C&ESAR 2010

Computer & **E**lectronics
Security **A**pplications
Rendez-vous

22 - 23 - 24 novembre 2010
Rennes - France

http://www.cesar-conference.fr/

C&ESAR 2010 : la cyberdéfense

Voici la dix-septième édition de la conférence C&ESAR (Computer & Electronics Security Applications Rendez-vous), organisée par le Ministère de la Défense (DGA-MI, connu antérieurement sous l'appellation de Centre d'Electronique de l'Armement). Le programme que nous vous présentons revisite en 2010 le vaste sujet de la cyber-défense, sept années après une première édition consacrée à ce sujet.

En 2003, l'agence européenne chargée de la sécurité des réseaux et de l'information était créée mais Facebook et bien sûr Twitter n'existaient pas encore. Gmail ne sera ouvert qu'en 2004. L'Estonie sera attaquée en 2007, banalisant les attaques en dénis de services distribués et l'usage des botnets. 2003, c'est aussi l'année de Blaster, et d'une panne électrique d'envergure affectant l'Est des Etats-Unis. Le ver n'était pas à l'origine de la panne généralisée mais il en a augmenté l'ampleur, soulignant déjà la dépendance des infrastructures critiques (centrales électriques, banques, centres de traitement des eaux usées, etc.) au bon fonctionnement des réseaux informatiques. Le monde numérique a été bouleversé durant ces sept dernières années, notamment dans les usages individuels et la croissance des cyber-attaques visibles ou non. Il connaîtra d'autres soubresauts dans le futur avec la généralisation du nomadisme, l'arrivée de l'informatique nébuleuse, de l'Internet des objets et la redistribution permanente de ses acteurs dans de complexes enjeux de pouvoir.

La prise de conscience des enjeux globaux de la cyber-défense, en dehors des cercles de spécialistes, est relativement récente. Dans le domaine de la cybersécurité, l'analyse du Livre Blanc sur la Défense et la Sécurité Nationale, publié au cours de l'été 2008, est particulièrement explicite et sans aucune ambigüité : « Les moyens d'information et de communication sont devenus les systèmes nerveux de nos sociétés, sans lesquels elles ne peuvent plus fonctionner. Dans les quinze ans à venir, la multiplication des tentatives d'attaques menées par des acteurs non étatiques, pirates informatiques, activistes ou organisations criminelles, est une certitude. Certaines d'entre elles pourront être de grande ampleur. S'agissant des attaques d'origine étatique, plusieurs pays ont déjà défini des stratégies de lutte informatique offensive et se dotent effectivement de capacités techniques relayées par des pirates informatiques. Dans ce contexte, les tentatives d'attaques dissimulées sont hautement probables. Des actions massives, menées ouvertement, sont également plausibles. ». La création en avril 2010 aux États-Unis du Cyber Command avec ses milliers de « cyber-warriors » participe de cette prise de conscience avec des moyens et des objectifs qui appellent le débat. Enfin, la récente déclaration du 2 novembre sur la coopération de défense et de sécurité entre le Royaume-Uni et la France qui intègre la cyber-défense démontre, s'il en est besoin, sa dimension supranationale : « Les cyber-attaques sont un défi croissant

pour la sécurité des États et les infrastructures nationales critiques, particulièrement en période de conflit. Nos infrastructures nationales dépendent de plus en plus des technologies de l'information en ligne et sur des réseaux informatiques. La France et le Royaume-Uni feront face ensemble aux menaces croissantes qui pèsent sur la sécurité de leurs systèmes d'information. C'est pourquoi nous avons agréé un cadre régissant notre coopération dans ce domaine crucial. Il permettra de renforcer la résilience de nos systèmes nationaux et communs. »

L'originalité de C&ESAR est de viser un objectif double, scientifique mais surtout didactique, en proposant à la communauté SSI, c'est à dire à une audience qui va des chercheurs aux praticiens et aux décideurs, un tour d'horizon sur la cyber-défense avec une vision prospective. L'appel à contribution a permis de sélectionner un premier lot de sujets, qui a ensuite été complété par un certain nombre de communications invitées, en fonction du périmètre envisagé par le comité de programme pour le thème de cette année. Nous souhaitons dès à présent remercier les membres du comité de programme ainsi que les experts sollicités, qui ont tous répondu présent à l'appel. C'est à eux que nous devons la richesse et la variété de ce programme reflétant bien la diversité et les multiples facettes du sujet, techniques, juridiques, culturelles, sociales et politiques.

Le programme est organisé en demi-journées articulées chacune autour d'une thématique :

- la matinée d'introduction va permettre de poser le problème, en confrontant approche et expérience publiques et industrielles en matière de cyber-défense.
- la Session 1 « Quel est le problème ? » fait le point sur les nouvelles formes de cybercriminalité, sur les stratégies de cyber-attaque, la place du renseignement, sur les dangers de l'Internet des objets et la place de la cyber-défense dans la protection des infrastructures vitales ;
- la Session 2 « Contre quoi se défendre ? » s'intéresse aux menaces touchant les environnements industriels, aux nouvelles formes d'espionnage numérique et de fuite d'information avec une première piste de solutions consistant à mieux détecter les vulnérabilités sur la Toile ;
- la Session 3 « Quelle cyber-défense ? » aborde les outils d'application d'une cyber-défense efficace, depuis les bonnes pratiques, la virtualisation des architectures, jusqu'au déploiement d'hyperviseurs ;
- la Session 4 « Comment s'organiser ? » donne un aperçu, dans une vision stratégique et internationale, des nouvelles doctrines et organisations qui sont le support nécessaire de la cyber-défense, avec des retours d'expérience ;
- la Session 5 « Et demain ? » organise une discussion libre autour du futur de la SSI et de nouvelles idées comme la défense en profondeur proactive d'une forteresse informatique partiellement investie par l'ennemi, ou l'intégration

dans les SICs d'une cyber-défense plus transparente à l'utilisateur dans le respect des libertés individuelles.

Nous espérons que ce programme brosse un bon panorama des divers aspects de la cyber-défense, et que les participants à cette conférence y trouveront un éclairage pertinent sur ce domaine en pleine évolution, ainsi que des réponses aux questions qu'ils peuvent se poser.

Nous souhaitons remercier à nouveau les contributeurs, que ce soit au travers des soumissions d'articles, des communications invitées ou des discours programmes, les membres du comité de programme pour leurs évaluations et leur apport à la construction du programme définitif, ainsi que les membres du comité d'organisation qui font que cette conférence peut se dérouler dans les meilleures conditions. Sans oublier les sponsors et soutiens divers (DGA, DGSIC, Orange, ANSSI, Technicolor) qui rendent possible ce rendez-vous annuel de la communauté SSI.

Bonne conférence C&ESAR 2010 à tous, et au plaisir de vous rencontrer !

Yves Correc (DGA-MI), Président du comité d'organisation.
Philippe Wolf (SGDSN/ANSSI), Président du comité de programme.

Partnaires

Direction générale de l'Armement, Direction Générale des Systèmes d'Information et de Communication, Orange Business Services, Technicolor, Supélec

Comité d'organisation

Jean-François Arnaud	DGSIC
Pascal Chour	SGDN/ANSSI
Yves Correc	DGA-MI, président du comité d'organisation
Olivier Heen	Technicolor, directeur de la publication
Ludovic Mé	Supélec
Eric Wiatrowski	Orange Business Services

Comité de programme

Jean-François Arnaud	DGSIC
David Bénichou	Ministère de la Justice
Mathieu Blanc	CEA
Pascal Chour	SGDN/ANSSI
Yves Correc	DGA-MI
Frédéric Cuppens	Telecom Bretagne
Hervé Debar	Telecom SudParis
Yves Deswarte	LAAS - CNRS
Victor Vuillard	SGDN/ANSSI
Stanislas de Maupéou	Thalès
Frédéric Raynal	Sogeti / Cap Gemini
David Simplot-Ryl	INRIA - LIFL
Pascal Sitbon	EDF - R&D
Eric Totel	Supélec
Eric Wiatrowski	Orange Business Services
Philipe Wolf	SGDN/ANSSI président du comité de programme

Site officiel : `http://www.cesar-conference.fr/`

Table des matières

I

II

III

Première partie

Cyberattaque 2.0 : comment mêler exploits techniques et manipulation humaine ?

Alban Ondrejeck[1], Pierre-Yves Gouardin[2], Florent Cottey[2], Arnaud Garrigues[2], Thomas Duval[3] et Antoine Coutant[3]

[1] Orange Business Services - Orange Consulting, 3, allée de Beaulieu 35700 Rennes, France
alban.ondrejeck(@)orange-ftgroup.com
[2] Orange Business Services - Orange Consulting, 114, rue Marcadet, 75018 Paris, France
{pierreyves.gouardin, florent.cottey, arnaud.garrigues}(@)orange-ftgroup.com
[3] Orange Business Services - IT&L@bs, 4 rue de la Châtaigneraie, 35510 Cesson-Sévigné, France
{thomas.duval, antoine.coutant}(@)orange-ftgroup.com

Résumé Un État souhaite déstabiliser un autre État. Pour cela, l'État attaquant va essayer de porter atteinte à une société énergétique alimentant l'État victime en exploitant les informations et les opportunités offertes par Internet et plus particulièrement le Web 2.0. L'attaquant va mettre au point un scénario qui nuira au bon fonctionnement de cette société et lui permettra de recueillir des renseignements pour parfaire son retard technologique notamment dans le cadre d'une réponse à appel d'offres. Pour ce faire, l'Etat attaquant manipulera une ONG écologique puissante qui sera aux yeux de tous à l'origine de cette crise et laissera la véritable source de l'attaque dans l'anonymat. Adossées à des pratiques de manipulation utilisant les réseaux sociaux, des attaques de nature plus techniques menées par des groupuscules plus agressifs vont permettre d'amplifier l'effet final recherché sur Nukepower. Au-delà des modalités d'action employées (techniques et organisationnels), c'est la collusion de fait entre deux acteurs très différents qui permet de révéler une forme d'agression plus pernicieuse. La dernière partie de l'article décrit une possible analyse "forensics" de l'attaque et montre que cette analyse peut attiser la crise. Enfin, ce scénario révèle les points faibles d'une organisation n'associant que trop les différents secteurs d'activité et notamment le partenariat public-privé tel qu'évoqué dans la publication d'Orange Business Services « Cyber défense des SI vitaux : quel partenariat public-privé ? »

Mots-clés: réseaux sociaux, web 2.0, cyber-défense, social engineering, ARP Poisoning, attaques iFrame, déni de service factice, CMS SPIP, Forensics.

Avertissement : Le présent article reflète simplement l'opinion de leurs auteurs et ne représentent pas une analyse ou des positions officielles d'Orange, Orange Business Services, France Télécom ou de l'une de ses filiales

1 Introduction

Un État (Risasu) souhaite mettre à mal le secteur énergétique d'un pays voisin (Victima). À cette fin, va mettre en place un scénario d'attaque. Ce scénario repose sur une opération de manipulation d'une Organisation Non Gouvernementale (Greenwar) contre le principal producteur d'électricité de source nucléaire

(Nukepower) de Victima. L'ONG deviendra ainsi inconsciemment alliée à l'attaquant. L'objectif de Risasu est multiple :

- faire de l'espionnage industriel afin de rattraper le retard technologique de son pays, et de concurrencer Victima dans le domaine de l'exportation énergétique ;
- décrédibiliser Nukepower, principal concurrent dans le cadre d'appels d'offres pour l'export d'énergie au sein de leur zone géographique d'influence ;
- indirectement déstabiliser Victima en regagnant de l'influence géopolitique grâce au développement de son secteur énergétique ;
- profiter des avancées technologiques dans le domaine nucléaire civil pour progresser dans le domaine de l'armement nucléaire.

Risasu cherche donc en priorité à obtenir des documents relatifs à la réponse à appel d'offre Śéléments commerciaux, technologies utilisées etc.) en cours à laquelle Nukepower répond

Pour produire son électricité, Nukepower a besoin de matière première, principalement d'uranium.

Risasu est conscient du niveau élevé de sécurité et de vigilance de Nukepower, c'est pourquoi son opération s'appuie sur différentes techniques et acteurs afin de rendre impossible la détection de certaines attaques et l'identification de la véritable source de ces attaques :

- veille stratégique ;
- manipulation humaine inconsciente ;
- création de buzz sur les réseaux sociaux ;
- utilisation d'un « écran de fumée » créé par des attaques iFrame via les actifs du buzz ;
- exploitation de vulnérabilités techniques pour l'intrusion sur les bases de données ;
- techniques d'analyse des logs et d'identification de la source de l'attaque (forensics).

Dans un premier temps, Risasu cherche à recueillir deux types d'informations compromettantes concernant Nukepower :

- informations stratégiques concernant le développement de projets qui s'avéreraient impopulaires notamment dans le milieu de la protection de l'environnement ;
- informations techniques qui identifient des équipements sensibles du SI de Nukepower et leurs potentielles vulnérabilités.

Pour cela, l'attaquant recueille des informations auprès de différentes sources, publiques et internes.

Les informations publiques permettent d'identifier et de manipuler une source interne à Nukepower afin de recueillir l'information désirée.

Dans un second temps, Risasu dévoile subtilement en préservant son anonymat, les informations impopulaires à l'ONG internationale Greenwar.

Cette dernière, forte de ces renseignements, effectue des actions de déstabilisation grâce à des campagnes de communication et d'appels à action sur le web 2.0 et plus particulièrement sur les réseaux sociaux. C'est en effet cette maîtrise des nouveaux médias de communication qui a orienté Risasu à choisir Greenwar comme opérateur à son insu.

Ce soulèvement populaire rendra plus discrètes les actions d'intrusions informatiques dans les bases de données de Greenwar.

L'analyse forensics accablera Greenwar sans pouvoir remonter au véritable attaquant à savoir Risasu.

2 Première étape : recueil d'informations compromettantes concernant Nukepower

2.1 Veille stratégique

Tout d'abord Risasu effectue des actions de veille stratégique et concurrentielle en suivant les activités de Nukepower. Ces actions doivent être anticipées car elles nécessitent une longue période de veille afin d'identifier les éventuelles stratégies de Nukepower.

Cette veille exploitera des informations publiques (dites ouvertes ou blanches) :

- presse généraliste locale et étrangère ;
- presse spécialisée ;
- sites, pages, blogs web officiels de Nukepower ;
- suivi des webforums spécialisés dans cette thématique ;
- articles, études scientifiques etc.

Ces actions ne seront pas que passives. En effet, Risasu pourra publier des messages sur les forums spécialisés permettant d'alimenter une discussion autour du sujet voulu ou d'identifier des collaborateurs de Nukepower possédant des informations intéressantes.

L'avènement des réseaux sociaux facilite le travail de notre attaquant :

- suivi des informations publiées sur les profils de réseaux sociaux officiels (le twitter @Nukepower, la page Facebook Nukepower etc.) ;
- analyse de contacts professionnels (sous-traitants, fournisseurs, clients, chercheurs etc.) des certains personnels clé de Nukepower grâce notamment à leurs profils Viadeo, LinkedIn etc.
- suivi des déplacements de ces personnels sur les sites de communautés de voyageurs ou sites tels que copainsdavant ;

– étude des CV publiés par certains collaborateurs de l'entreprise visée révélant des détails les projets actuels et passés réalisés etc.

La veille va également exploiter des informations semi-ouvertes ou dites grises. L'obtention de cette information nécessite certains privilèges mais ne relève pas d'actions illégales :

– droits d'abonnement à des lettres internes ;
– invitation à des conférences, colloques ou forums ;
– acceptation comme ami sur son profil de réseau social de type Facebook
– acceptation dans la communauté Nukepower sur des sites de type Yammer [4] en tant que partenaire ;
– accès aux annuaires d'écoles supérieures du domaine énergétique ;
– accès aux appels d'offres que Nukepower a émis ou ceux auxquels il a répondu etc.

L'analyse de ces multiples informations oriente Risasu vers différentes pistes dont celles d'un éventuel projet d'implantation de Nukepower au Nagikaria. Une éventuelle implantation d'un leader de l'énergie nucléaire dans cette zone écologiquement préservée et géopolitiquement instable provoquerait incontestablement l'ire de certains gouvernements, mouvements rebelles locaux et associations de protection de l'environnement.

Risasu décide donc de recouper ces informations et d'en savoir plus sur ce projet en menant des actions de manipulation humaine sur certains employés de Nukepower.

2.2 Manipulation humaine au sein de Nukepower

La veille a permis d'identifier des employés qui connaissent :

– les détails de ce projet ;
– d'éventuelles vulnérabilités permettant d'accéder à ces données.

Risasu est conscient que ses personnels clé ont été sensibilisés et sont donc vigilants aux actions de manipulations humaines. C'est pourquoi, l'attaquant décide de ne pas se risquer au recrutement de sources. En outre, l'attaquant ne maîtrise pas les délais pour recruter une telle source de façon subtile et discrète. La manipulation exploitera seulement des sources humaines inconscientes. En effet, une source consciente représenterait un risque trop élevé et pourrait compromettre Risasu et la suite de l'opération.

Les leviers de la rémunération financière directe ou de la compromission ne pourront donc pas être utilisés.

4. Yammer est un site de réseaux social de type Twitter mais qui regroupe les utilisateurs dans des groupes correspondant à leur entreprise d'appartenance. Ces tweets peuvent donc être partagés entre collègues ou avec ces partenaires professionnels.

La veille aura permis d'identifier d'éventuelles sources et plus particulièrement des collaborateurs de Nukepower indiquant vouloir changer de poste ou d'employeur. Ces personnes sont susceptibles :

- d'avoir un fort ego car ils considèrent qu'ils ne sont pas employés à leur juste valeur
- être attiré par un poste éventuellement plus rémunérateur

Risasu tente des approches sur différentes sources. Parmi ces dernières, Claude Durand, un des administrateurs du réseau interne de Nukepower attire particulièrement l'attention. En effet, fort de sa présence sur les réseaux sociaux, M. Durand indique clairement sa volonté de changer de travail.

Les attaquants, se font donc passer pour des chasseurs de tête en contactant cette cible.

M. Durand est très flatté d'être reçu en entretien. Il n'hésite pas à déballer sa rancoeur sur la mauvaise gestion de la sécurité du réseau interne en mentionnant certains exemples. Ces exemples aident les attaquants à identifier des vulnérabilités qui une fois exploitées faciliteraient l'accès à des bases de données internes au sein de Nukepower.

M. Durand est remercié et le faux recruteur lui indique qu'il va étudier son dossier et qu'il le recontactera ultérieurement [5].

À ce stade, Risasu possède :

- des indices concernant un éventuel projet au Nagikaria grâce à sa veille active ;
- des vulnérabilités liées aux accès à des bases de données internes de Nukepower.

2.3 Piratage de comptes mails de Nukepower

Les attaquants vont désormais chercher des preuves et des détails concernant le projet du Nagikaria.

Pour cela, Risasu a identifié un VIP de Nukepower, Jérôme Dumael ayant mentionné sur son profil copainsdavant qu'il s'est rendu au Nagikaria.

Ces différentes pages de réseaux sociaux dévoilent différentes informations le concernant, dont :

- célibataire
- passionné de golf
- rêve d'aller en Australie
- son parcours scolaire
- sa photo

5. Ce recruteur rappellera M. Durand une semaine plus tard pour lui indiquer qu'il n'a pas été retenu mais qu'il garde néanmoins son CV au cas où. Bien évidemment, le numéro de portable et le portable du recruteur sont anonymisés (par exemple : portable BIC, abonnement carte prépayée en liquide etc.)

Fort de ces informations, les attaquants vont créer de faux profils sur Facebook pour tenter d'être ami avec Jérôme. Un des premiers profils créés correspond à une femme de son âge, célibataire et ayant a priori été scolarisée dans le même collège.

Malheureusement, Jérôme est prudent et n'accepte que de très proches amis à partager ces informations sur Facebook. Cette acceptation, aurait permis aux attaquants d'avoir accès à d'autres informations telles que sa ville d'origine, ses contacts, sa date de naissance et surtout son adresse email personnelle.

Cependant, Risasu a remarqué que Jérôme est fan de golf. Les attaquants vont donc développer une application Facebook permettant de suivre les résultats de golf et de participer à des petits jeux concours.

Par le jeu des recommandations Facebook, les attaquants indiquent indirectement à Jérôme qu'une nouvelle application de golf est disponible. Jérôme ne résiste pas à installer cette application. À ce moment, les attaquants profitent des fonctionnalités offertes par les APIs de Facebook. En effet, ces APIs donnent accès aux développeurs à l'ensemble des informations renseignées sur les profils des personnes installant cette application mais également à l'ensemble des informations concernant les amis de cette même personne [6].

Les attaquants obtiennent donc :

- l'ensemble des informations renseignées par Jérôme sur Facebook (date de naissance, ville d'origine, liste d'amis, centres d'intérêts, mur Facebook, l'ensemble des photos, vidéos etc. et bien sûr l'adresse mail de Jérôme etc.)
- l'ensemble des informations auxquelles Jérôme a accès concernant ses « amis » Facebook.

Risasu va désormais essayer de pirater la boîte mail personnelle de Jérôme. Pour cela, les attaquants utilisent l'option mot de passe oublié. Les questions secrètes sont rarement personnalisables et souvent les suivantes :

- ville de naissance de votre mère
- lieu de rencontre de votre conjoint
- nom de votre premier animal de compagnie
- date de naissance sous la forme jj/mm/aaaa
- lieu de votre voyage de noces etc.

L'ensemble des informations publiées et accessibles sur les réseaux sociaux concernant Jérôme permettent aux pirates de trouver la réponse à la question secrète.

Les pirates ont désormais accès à la boîte mail personnelle de Jérôme. À la lecture des mails, les pirates trouvent les confirmations de création de comptes sur des sites Internet (e-Commerce, blogs, divers forums etc.). Ces mails de création de comptes comprennent le login et le mot de passe. Il suffit de peu de temps

6. La configuration des profils par défaut permet en effet aux développeurs d'avoir accès à l'ensemble de vos informations si vous ou un de vos « amis » Facebook avait installé une application.

aux attaquants pour se rendre compte que Jérôme utilise un unique mot de passe pour l'ensemble de ses comptes. Jérôme se sent certainement en sécurité car son mot de passe est réellement fort. Les pirates changent donc le mot de passe de son compte mail par celui trouvé. En effet, il y a des fortes chances que ce soit le même. Ainsi, Jérôme ne se sera pas aperçu du piratage de sa boîte, pour peu que les attaquants aient remis en ordre ses mails [7].

Dorénavant, il suffit aux pirates de chercher sur Google l'adresse du webmail de Nukepower, qui est référencé par ce moteur de recherche comme la plupart des webmails professionnels.

Il suffira alors aux pirates de renseigner l'adresse professionnelle de Jérôme de la forme prénom.nom@nukepower.com (ou d'une autre forme facilement trouvée sur Internet) et de renseigner le mot de passe trouvé.

Risasu a désormais accès à la boîte professionnelle d'un collaborateur de Nukepower se déplaçant régulièrement au Nagikaria. Les attaquants possèdent dorénavant des mails prouvant et détaillant le projet d'implantation d'une mine d'extraction d'uranium au Nagikaria dans une zone écologiquement protégée et géopolitiquement sensible. Cette implantation ne pourrait d'ailleurs se faire que grâce à la construction d'un barrage perturbant l'écosystème actuelle et la distribution d'eau vers son pays voisin.

Désormais, Risasu possède un renseignement qu'il va exploiter pour générer un nuage de fumée qui dissimulera l'exploitation des vulnérabilités identifiées grâce à Claude Durand afin de mener des actions d'intrusion sur les bases de données sensibles de Nukepower.

Cet écran de fumée va être provoqué par un buzz médiatique et une attaque utilisant des iFrames.

Enfin, il est important de noter, qu'à ce moment, Nukepower n'a eu aucun indice permettant de détecter ces premières actions et fuites d'informations.

3 Deuxième étape : Déstabilisation de Nukepower

3.1 Action 1 : manipulation et crise générée par l'ONG

Risasu va mener une action de manipulation de l'ONG Greenwar. Cette ONG doit croire en la fiabilité de la source et de l'information compromettante concernant Nukepower. C'est à cette condition que Greenwar se donnera tous les moyens pour déstabiliser médiatiquement Nukepower afin qu'elle mène une action médiatique à ce sujet.

En parallèle de ses actions contre Nukepower, Risasu a mené une opération d'infiltration au sein de Greenwar. Au moins un an avant l'opération, Risasu a

7. Certaines boîtes mail indiquent le jour et l'heure de la dernière connexion, mais elles restent rares et les utilisateurs qui prennent garde à cette indication le sont encore plus.

placé des agents au sein de cette ONG. Ces agents sont de simples adhérents bénévoles, faisant croire en leur bonne foi pour aider Greenwar. Certains d'entre eux participent à des actions sur le terrain.

Ces agents infiltrés ne vont pas diffuser telle quelle et directement l'information à l'état major de Greenwar car cela serait trop risqué et peu crédible.

Les « taupes » de terrain vont permettre à Risasu de comprendre comment Greenwar :

- s'organise pour obtenir de l'information,
- recrute et évalue ses sources
- estime la valeur ses informations, les exploite, les analyse

Ces agents seront éventuellement en contact avec certains informateurs. Fort de ces informations de collecte de renseignement, certains agents vont diffuser au compte goutte des informations concernant l'opération au Nagikaria. Des agents sur le terrain pourraient modifier les propos des informateurs pour ajouter certaines informations ou encore recommander un nouvel informateur qui s'avérerait en fin de compte être un autre agent de Risasu. Ces faux informateurs diffuseraient au début des informations fiables sur un autre sujet pour obtenir la confiance de Greenwar. Une fois jugés fiables, ces informateurs commenceraient à divulguer des informations concernant le projet de Nagikaria.

Ce type d'actions doit :

- être anticipé ; la confiance s'acquière au fil du temps ;
- reposer sur des informations provenant de différentes (fausses) sources. En effet, Greenwar peut se méfier d'une source, mais pas de multiples sources a priori sans lien. Les informations sembleront recoupées.

Au fur et à mesure de la montée en confiance, les fausses sources fourniront des renseignements plus précis apportant de plus en plus de preuves à Greenwar sur le projet de Nagikaria. La multitude de sources ne permettra pas à l'ONG de se croire manipulée.

Une fois, ces informations compromettantes récoltées par Greenwar, celle-ci décide de mener une campagne médiatique contre Nukepower.

Cette campagne va s'appuyer sur les réseaux sociaux, excellent vecteur de buzz. Greenwar va ainsi tenter de créer le buzz.

Cependant elle ne va pas publier cette information sous forme textuelle via un simple tweet. L'ONG va mettre en place une stratégie de communication en s'aidant de visuels. En effet, la forme du message est au moins aussi importante que la forme pour tenter de faire le buzz sur la Toile.

Pour cela, Greenwar va réaliser une parodie d'une publicité de Nukepower montrant comment cette société va mettre à mal un écosystème et risque de mettre à feu et à sang une région entière.

Ce film sera accompagné de goodies, comme des avatars communs qui permettront aux internautes d'afficher clairement leur soutien à cette cause.

Greenwar va donc diffuser ce clip parodique sur différentes plateformes de partage de contenu comme Youtube ou Dailymotion. La diffusion est programmée le vendredi soir. Cela permettra à Greenwar d'avoir deux jours d'avance sur la cellule communication de Nukepower partie en weekend. L'ensemble de ces sites, blogs et comptes de réseaux sociaux (principalement sur Twitter et Facebook) va relayer cette vidéo en appelant à rejoindre une page Facebook spécialement réalisé à cet effet. Cette page Facebook proposera le téléchargement de goodies, le suivi de l'actualité des actions menées par l'ONG, l'appel à la participation de ces actions, l'installation d'applications dédiées à la lutte contre le projet de Nukepower etc.

Greenwar essaie de créer un buzz en s'appuyant à la fois sur sa communauté avec qui elle maintient des relations depuis sa présence sur les réseaux sociaux et sur des contenus percutants, très visuels et d'excellente qualité. Avant cette action, Greenwar comme la majorité des grandes ONG possédait déjà au moins 15 000 fans sur sa page Facebook. C'est cette communauté de fidèles qui constitue le premier relais du buzz.

En effet, chaque profil Facebook possède en moyenne 100 contacts. Si 6 000 fans de la page Facebook de Greenwar installent l'application dédiée à cette opération ou deviennent fan de la vidéo, il y a 6 000 x 100 = 600 000 personnes [8] qui seront notifiées sur leur mur de l'existence de la vidéo ou de l'application et donc de la campagne de déstabilisation entreprise contre Nukepower. À partir de ce moment là, l'effet boule de neige s'enclenche et la page Facebook peut vite atteindre les 100 000 fans à la fin du weekend.

Greenwar s'appuiera également sur ses relations presse et sur les multiples chroniques télévisuelles relayant les nouveautés du Web pour diffuser au plus grand nombre son message.

Le lundi suivant, Greenwar profitera également des réactions de Nukepower prônant la censure pour créer un « effet Streisand [9] » qui ne fera que fédérer de nombreux internautes autour de la cause de Greenwar.

3.2 Action 2 : Ecran de fumée contre Nukepower par l'Etat attaquant via l'ONG

Risasu souhaite lancer une attaque informatique furtive sur le système d'information de Nukepower, mais les attaquants savent que les administrateurs face à eux sont bien préparés à réagir. Les pirates procèdent par étapes. D'abord ils génèrent un écran de fumée qui rendra inutilisable les logs des serveurs et qui monopolisera les administrateurs sur un problème complexe.

8. A ce chiffre il faut déduire les éventuels doublons correspondant aux amis communs.

9. L'effet Streisand est un phénomène Internet qui se manifeste par l'augmentation considérable de la diffusion d'information ou de documents faisant l'objet d'une tentative de retrait ou de censure.

Pour cela, Risasu met à profit les dizaines de milliers de visiteurs de la page Facebook de Greenwar pour mettre en oeuvre son attaque. Ces derniers, s'ils veulent consulter les articles sur Nukepower, visionner les parodies ou acheter des goodies, sont invités à se rendre sur le blog de Greenwar. Ce blog sera piégé au moment opportun.

L'effet recherché est de créer un déni de service, grâce aux iFrames, contre certains serveurs publics de Nukepower grâce à l'aide inconsciente des internautes surfant sur cette page. Ces attaques iFrames représentent l'écran de fumée masquant l'intrusion sur les serveurs de bases de données de Nukepower.

Ce piège se fonde sur des attaques iFrame qui feront exécuter des requêtes par tous les visiteurs vers des serveurs sensibles de Nukepower identifiés grâce à Claude Durand.

Le blog de Greenwar s'appuie sur le CMS SPIP. Une faille dans la configuration par défaut a été publiée sur la mailing-list full-disclosure et permet de modifier le code source des fichiers sur le serveur. Le pirate commandité par Risasu choisit d'altérer le code de l'entête du site car cet élément est affiché sur chaque page dynamique.

L'altération consiste à insérer plusieurs iFrame invisibles de 1x1 pixel menant vers les serveurs sensibles de Nukepower. Une fois ce fichier mis en ligne, chaque visite va déclencher dans le navigateur des internautes le chargement de pages web complètes, y compris les images, depuis les serveurs sensibles. À noter que Facebook a modifié le fonctionnement des iFrame en obligeant les utilisateurs à cliquer sur un bouton avant d'ouvrir le lien. Cela explique la nécessitée de transférer l'intérêt des internautes vers le blog de Greenwar.

L'objectif principal de cette attaque n'est pas forcement de faire tomber les services mis en ligne par Nukepower, mais de « polluer » le trafic à destination des adresses IP publiques de Nukepower. Les traces générées sur les différents serveurs de Nukepower auront l'air de venir de milliers de sources différentes sans aucun lien entre elles, entrainant le déclenchement d'une situation de crise chez Nukepower et la mobilisation de ses services IT et sécurité sur cette attaque.

Afin de complexifier la détection de l'origine de cette attaque de type « déni de service » servant à créer un écran de fumée, Risasu aura pris soin d'inclure une protection dans le code source de son code malveillant permettant de ne pas initier l'attaque depuis les adresses IP publiques de Nukepower. Sans cette protection les administrateurs auraient sans doute constatés que certaines connexions venaient de leurs utilisateurs. Ils auraient alors été en mesure d'identifier rapidement la source (blog de Greenwar) dans les logs de leur proxy par exemple ou en consultant l'historique du navigateur de ces employés.

Ce type d'attaque pourrait être relativement facilement détecté en temps normal mais la double crise informationnelle et informatique rencontrée par le Groupe peut ouvrir une « fenêtre d'action » permettant d'exploiter la vulnérabilité pu-

blique révélée par Claude Durand. Pour ne pas prendre le risque de rendre le serveur vulnérable indisponible, Risasu prend bien entendu soin de ne réaliser qu'une attaque par iFrame « light » auprès de l'adresse IP publique du serveur en question.

3.3 Action 3 : Intrusion dans les bases de données de Nukepower

À l'apogée de l'utilisation de l'écran de fumée ainsi créé, Risasu mène une attaque visant à infiltrer les bases de données de Nukepower. Cette attaque va exploiter les vulnérabilités indiquées par Claude Durand.

La vulnérabilité en question impact un serveur ColdFusion. Un directory traversal permet de récupérer le hash du compte administrateur, et de le rejouer, en manipulant le salt, auprès de la mire d'authentification. Avec ce compte il est possible de déposer sur le serveur un programme malveillant au format CFM. Les pirates ont alors le contrôle total du serveur.

Les premières commandes leur permettent de constater que le serveur est dans une DMZ et interagit avec une base de données qui est dans un autre sous-réseau. La consultation du code source du site Internet hébergé sur le serveur permet de connaître le type de base de données utilisée et de retrouver des identifiants pour s'y connecter.

Les attaquants fouillent alors la base à la recherche d'informations intéressantes, mais sans succès. Néanmoins la base de données est un Microsoft SQL Server 2005 et les tests montrent qu'elle accepte la commande xp_cmdshell. Ce serveur peut alors servir de rebond pour attaquer d'autres serveurs dans le réseau de l'entreprise.

Pour ne pas perdre de temps et profiter du fait que les administrateurs doivent se connecter sur tous les serveurs pour comprendre pourquoi leurs serveurs Internet remontent des alertes de performance, les pirates installent des keyloggers sur les deux serveurs compromis et récupèrent une heure après deux comptes du domaine AD de Nukepower.

L'objectif est maintenant de récupérer des informations relatives au projet ciblé. Pour ce faire Risasu se concentre sur les serveurs de messagerie et le serveur de fichiers.

Les agents de Risasu vont accéder au webmail de l'entreprise avec les comptes dérobés pour les vérifier. Ils se connectent sans problème et décident d'envoyer un e-mail à une adresse qu'ils contrôlent pour étudier les entêtes ajoutées au message. Ces entêtes leur révèlent l'adresse interne d'un serveur Exchange qui est dans le même sous-réseau que la base de données précédemment compromise. Ils peuvent donc utiliser cette dernière comme rebond pour atteindre le serveur. Ils n'ont pas besoin de pirater ce serveur de messagerie car les comptes subtilisés ont des droits d'administrateur également sur Exchange. Risasu a maintenant accès aux boîtes aux lettres (BAL) de tous les employés de Nukepower.

Ce serveur de messagerie faisant partie du domaine Windows privé de Nukepower, les communications RPC, SMB et Netbios sont autorisées à destinations du Primary Domain Controler (PDC). L'utilisation des commandes RPC pour lister les machines membres du domaine auprès de ce PDC vont permettre à Risasu d'identifier le serveur de fichier. Il ne reste plus aux attaquants qu'à mettre en place un rootkit, afin de pouvoir prendre la main quand bon leur semble sur ces serveurs tout en obfusquant ces connexions.

Risasu a donc maintenant tout loisir d'accéder aux BALs et aux partages du serveur de fichier afin de localiser des documents relatifs à l'appel d'offre. La PKI de Nukepower n'étant pas déployée à l'ensemble des cadres, des documents sensibles envoyés en clair et détaillant des solutions technologiques et des données commerciales

4 Collecte et analyse des traces

Aucun dispositif n'a permis de détecter le déroulement de l'opération avant la première vague d'attaques iFrame. C'est donc seulement suite à un problème de fiabilité et de performance de ses systèmes SCADA (généré par le déni de service servant à créer un écran de fumée) que Nukepower décide de mener son enquête par l'entremise de son RSSI (Responsable Sécurité des Systèmes d'Information). Celui-ci va devoir récupérer des informations concernant le problème détecté. Il peut comprendre alors rapidement que les systèmes ont été la cible d'une attaque de type déni de service et qu'il doit obtenir le maximum d'information sur cette attaque (origine de l'attaque, nombre d'assaillants, objectif final,. . .) et ceci malgré les contraintes liées aux plateformes industrielles (pas d'arrêt possible, OS/applications fermés ou très spécialisés, peu d'expert sur l'OS ou les applications cités ci-dessus, . . .). Partons du principe que les attaques iFrames ont été stoppées d'une quelconque manière. Nous allons voir dans les paragraphes suivants comment un RSSI pourrait réagir lorsque sa hiérarchie lui demande « Que s'est-il passé ? Qui a fait quoi ? ».

4.1 Analyse 1 : l'écran de fumée

Le RSSI analysera en premier l'écran de fumée généré par les iFrames, c'est l'attaque qui va révéler les autres attaques. Les logs seront très nombreux (voire trop nombreux) et l'analyse n'en sera que plus difficile. D'une part parce que les adresses IP seront complètement aléatoires et d'autre part parce que les attaques viennent certainement de différents pays mais avec une prédominance (a priori) pour Victima.

Contrairement à un déni de service classique, les IP appartiennent ici à de réelles connexions (l'IP correspond à un système informatique), celles des internautes connectés sur le site de Greenwar. Pour obtenir cette information, il suffit

d'effectuer un whois sur une partie des adresses IP servant à l'attaque. La plupart vont appartenir le plus souvent à des opérateurs téléphoniques ou à des entreprises (les internautes qui surfent sur le web depuis leur poste professionnel). Mais tout ce que verra le RSSI, ce sont des adresses IP sans lien apparent, venant de différents types de machines avec différents types d'OS. Le RSSI notera tout de même que l'attaque est dirigée sur des serveurs bien précis et bien particuliers de Nukepower. Peut-être remarquera t-il aussi que certains serveurs publics sont ignorés. Il devrait alors vérifier pourquoi. Mais certainement dans le feu de l'action, il se contentera de contenir l'attaque créant l'écran de fumée et de comprendre d'où vient celle-ci. Le RSSI pourrait se poser la question à ce moment là de savoir s'il y a eu fuite de données par l'un des employés de Nukepower.

On peut raisonnablement imaginer que certains employés de Nukepower, alertés par le buzz créé par Greenwar, vont aller sur le blog infecté de Greenwar. Mais comme les attaquants ont inclus une iFrame intelligente qui ne s'active pas pour les personnes dont l'adresse IP provient de Nukepower, les employés de Nukpower ne contribueront pas l'attaque factice par déni de service. Par contre, les attaquants ne pourront pas filtrer tous les réseaux des entreprises qui gravitent autour de Nukepower (clients, fournisseurs, etc.). Le RSSI trouvera bien un contact qui lui permettra d'enquêter directement sur un des réseaux émetteurs de l'attaque. Il se peut, néanmoins, que dans la multitude d'adresses IP contenue dans les logs, le RSSI ne voit pas les adresses venant de ce ou ces réseaux. Mais pour simplifier et permettre d'aller plus loin dans l'analyse, nous allons considérer d'une part que le RSSI a trouvé l'adresse IP externe du réseau de l'entreprise d'un des fournisseurs de Nukepower et d'autre part que ce dernier accepte de collaborer.

4.2 Analyse 2 : le navigateur web

Il est fort probable que le réseau de l'entreprise soit séparé de l'Internet par un pare-feu et un NAT. Dans un premier temps, le RSSI devra analyser les logs de cet élément frontière (si toutefois ces logs sont conservés). Il pourra alors récupérer les adresses IP du réseau interne qui ont générées ou qui génèrent encore des paquets qui participent à l'attaque. Deux cas se présentent alors, soit les stations ne génèrent plus de paquets (cas le plus défavorable pour le RSSI), soit les stations sont encore actives. Voyons les deux cas de figure.

Analyse d'une station inactive Le RSSI arrive sur une station qui n'alimente plus les attaques par iFrames. Aucune connexion réseau n'est visible au niveau de l'élément frontière ou au niveau de la machine. Les premières investigations seront :

- vérifier s'il n'y a pas de processus inhabituels
- vérifier s'il n'y a pas de services réseau inhabituels

– passer un anti-virus, anti-trojan, ...
– questionner l'utilisateur habituel de cette station

Le RSSI pourra éventuellement trouver un ou plusieurs virus sur la station mais se rendra vite compte que ce ou ces virus ne peuvent en aucun cas avoir générés ce trafic. Comme les paquets réseau alimentant le déni de service factice étaient sur le port 80 (supposition faite que l'attaque se fait sur le port 80 des serveurs sensibles de Nukepower), le RSSI va se tourner alors vers l'historique de navigation web de l'utilisateur de la station. La navigation web peut être générée par plusieurs applications :

– les navigateurs web standards (Internet explorer, Firefox, Chrome, etc.)
– les messageries instantanées (Messenger, Pidgin, ...)
– mises à jour (logiciels ou OS)
– widgets divers et variés sur le bureau de l'utilisateur
– aide en ligne d'un logiciel
– ...

Il existe donc une pléthore d'applications pouvant émettre des paquets réseau vers le port 80. Tout dépend de la politique de sécurité mise en place sur les réseaux et les machines de Nukepower. L'utilisateur peut avoir tous les droits (installation de logiciels, utilisation de n'importe quel protocole) ou il ne peut avoir accès qu'aux logiciels autorisés par la politique de sécurité sans avoir la possibilité d'en installer un autre. A priori, la première idée (la plus simple) du RSSI sera d'analyser le navigateur web en regardant l'historique de navigation de l'utilisateur. Si le RSSI avait dû analyser les autres logiciels, cela aurait été plus compliqué, notamment parce que l'historique n'est pas forcément disponible. Le RSSI pourrait analyser aussi la machine d'un utilisateur méfiant qui utilise la navigation privée ou une clé USB contenant un Firefox portable par exemple. Nous allons considérer que le RSSI analyse la machine d'un utilisateur lambda qui ne cache pas particulièrement sa navigation web.

Pour retrouver le générateur des attaques iFrames, le RSSI va tester toutes les pages vues par l'utilisateur une à une pour trouver celle qui génère ce trafic réseau. Il découvrira alors la page web de Greenwar et en analysant finement le contenu de cette page, il découvrira l'iFrame coupable.

Analyse d'une station active Le RSSI arrive sur une station qui alimente encore le déni de service factice. Ce cas est beaucoup plus simple que le cas précédent.

En vérifiant le processus qui génère des paquets réseau vers le port 80 des serveurs attaqués, le RSSI va s'apercevoir que c'est le browser web de la machine qui génère ces paquets. En analysant les pages en cours de visualisation, le RSSI va découvrir l'iFrame sur le serveur de Greenwar.

4.3 Analyse 3 : le dilemme

Nukepower se trouve désormais face à trois possibilités :

- Nukepower dévoile publiquement sa découverte et attise par conséquent la crise actuelle sans être conscient qu'un tiers les a manipulés. Cette solution ne permettra pas à Nukepower de résoudre entièrement l'affaire, l'attaque de Risasu restera cachée.
- Nukepower décide de tenter de résoudre cette affaire avec Greenwar pour ne pas attiser la crise publiquement. Encore faut-il que Greenwar accepte de collaborer, tout dépend de l'état d'esprit des dirigeants de Greenwar. Cette solution pourrait permettre de résoudre partiellement l'affaire, tout dépend des capacités des RSSI de Nukepower et de Greenwar à effectuer des analyses « forensics » On parle ici de résolution partielle car les RSSI arriveront très certainement à trouver qui a posé l'iFrame mais, par contre, il y a peu de chance que le RSSI de Nukepower arrive à trouver la provenance de la fuite liée au recrutement d'une source d'infrastructure (cf. ğ2.1).
- Nukepower fait appel aux services de police pour approfondir l'enquête. Ce choix permettrait peut-être d'identifier la source de l'attaque, à savoir Risasu. Cependant, le fait de porter cette affaire devant la justice la rendra publique tôt ou tard.

La meilleure solution serait très certainement la troisième. Faire appel aux services de Police permettrait une meilleure compréhension de l'attaque et aussi (et surtout) de comprendre les motivations réelles des attaquants. Cela permettrait aussi de remonter des alertes au niveau de l'État Victima pour que ce dernier puisse prendre des mesures face à ce type d'attaque.

4.4 Analyse 3 : l'attaque ciblée

La suite de l'analyse va dépendre des choix effectués par le RSSI. Prenons le cas le plus probable, une fois que le RSSI a bien la preuve d'une attaque ciblée sur les serveurs de Nukepower, il va faire appel aux autorités compétentes. Ces dernières vont alors devoir remonter la piste Greenwar. L'analyse des serveurs de Greenwar va permettre de trouver la faille sur le CMS SPIP. Avec un peu de chance, les forces de l'ordre trouveront dans les logs que celui qui a modifié l'entête du site de Greenwar ne fait pas partie de Greenwar (ce qui permet d'écarter cette association de la liste des suspects). Par contre, puisque Greenwar n'est plus suspecté, les enquêteurs vont chercher la ou les motivations de l'attaquant. Les attaques de type déni de service sont utilisées soit pour nuire à un réseau soit pour cacher une attaque plus ciblée.

Les enquêteurs vont alors retourner sur le site de Nukepower pour analyser tous les équipements informatiques qui ont un accès au réseau public. Selon la taille de l'entreprise (et donc de son réseau informatique), le travail peut être

considérable. Il faut alors procéder par étape et avec méthode. Les enquêteurs devront analyser en priorité les systèmes les plus critiques, c'est-à-dire ceux qui offrent un accès plus ou moins illimité au coeur du réseau. Si un attaquant bien renseigné essaye de pénétrer le réseau de Nukepower, il essaiera de prendre le contrôle d'un accès lui offrant le plus de possibilité. Les enquêteurs devront aussi analyser les systèmes qui ont un accès le plus direct à Internet (sans NAT par exemple). Ces systèmes sont les plus vulnérables. Ces analyses prendront énormément de temps aux enquêteurs et même s'ils trouvent le système qui a permis aux attaquants de pénétrer le réseau de Nukepower, il restera deux questions :

- est-ce les mêmes attaquants que ceux qui ont effectués les attaques créant l'écran de fumée ?
- est-ce que c'est la seule brèche ?

5 Conclusion

Alors que l'actualité se fait régulièrement l'écho des formes agressives que l'on rencontre dans le monde économique, parfois sous le vocable de « guerre économique », ce scénario montre comment un Etat peut avoir une action discrète mais génératrice de profondes perturbations sur un autre état en utilisant de multiples intermédiaires Cet état de fait est certainement aggravé par un monde dont les cycles de crises sont nombreux, parfois long et souvent très dommageables. Les entreprises nécessaires au bon fonctionnement économique d'un État sont donc une cible potentielle pour tout type d'agresseur : terroriste ou encore étatique.

Ces entreprises sont désormais au coeur de la cyberdéfense car, même si le coeur de leur activité est plus ou moins connecté, le monde est lui, en permanence interconnecté entrainant une fragilisation de ces « barrières ». La multiplicité des acteurs et l'interpénétration des méthodes font, très certainement, de ces organisations le coeur des prochains affrontements.

Ces affrontements, que la nature même d'Internet rend discrets, difficilement décelables obligent à la fois à une veille constante mais aussi à une préparation éclairée et à l'entretien d'une capacité de réaction. Une attaque organisée peut être difficilement décelable comme nous venons de le démontrer.

Nous pouvons ainsi imaginer qu'un État savamment organisé saura cacher ses traces d'effraction. Seule une coopération organisée, en confiance, et déjà mise à l'épreuve, pourra permettre de préparer la crise, de l'anticiper puis, celle-ci terminée, d'investiguer avec succès sur les attaques afin d'y répondre au mieux. Une attaque sur ce type d'infrastructure doit être traitée extrêmement rapidement, d'une part pour faciliter l'enquête ; nous avons vu que l'analyse de la station de l'utilisateur est très différente selon que la station émette encore ou pas des paquets pour le déni de service factice. D'autre part, la compréhension de l'attaque permet de prendre des contre-mesures plus rapides pour contrer l'objectif réel

des attaquants. Ce traitement de l'attaque doit être fait en collaboration avec les services de sécurité pour éviter une mauvaise compréhension de l'attaque. En effet, ces services auront une plus grande expérience de ce type de problème ainsi que le matériel d'analyse adéquat.

Les traces techniques sont difficiles à analyser pour remonter au véritable commanditaire de l'opération. Cependant, comme dans toute organisation, cette discrétion peut-être mise à mal par le personnel. En effet, l'opération a requis une importante organisation et des ressources humaines et principalement des compétences différentes du côté de Risasu. La moindre faille organisationnelle ou de gestion du personnel pourrait mettre à mal la confidentialité de l'opération. En effet, comme tous, Risasu n'est pas sûr à 100

6 Références

1 Intelligence Analysis, a Target-Centric Approach ; Robert M. Clark, Editions CQ Press

2 http://www.helium.com/items/1828138-why-former-anti-terrorism-czar-believes-a-cyber-attack-could-bring-us-collapse

3 http://chaptersinwebsecurity.blogspot.com/2009/07/ddos-attacks-in-korea-forensic-analysis.html

4 https://www.mag-securs.com/spip.php?article1543

5 http://fr.readwriteweb.com/2010/03/30/a-la-une/greenpeace-nestl-sur-facebook-lart-de-guerre/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+readwriteweb-france+%28ReadWriteWeb+France%29

Biographies

Alban ONDREJECK Ingénieur spécialisé dans la télécommunication et la détection, Alban Ondrejeck a effectué sept ans au sein des services de renseignement étatiques français après un stage de fin d'étude au CELAR.

L'avènement des réseaux sociaux l'ont aidé à effectuer des actions de renseignement économique et industriel.

Alban Ondrejeck met désormais à profit cette expérience offensive et cette expertise en intelligence économique au service des entreprises privées et organisations étatiques en leur conseillant des organisations leur permettant de maîtriser et protéger leur patrimoine informationnel.

Arnaud GARRIGUES Diplômé du Mastère Spécialisé en Management des Systèmes d'Informations et d'un Master en Relations Internationales/Sécurité-

Défense, Arnaud Garrigues a un parcours atypique qui l'a conduit à se passionner pour les questions liées à la Cyberdéfense. Consultant SSI au sein d'Orange Consulting, il intervient sur des questions techniques et organisationnelles liées à la sécurité des SI. Il a également travaillé au profit de la Direction des Affaires Stratégiques du Ministère de la Défense, sur les questions de lutte informatique offensive et défensive. Il est également auteur du blog « CIDRIS-Cyberwarfare » : `http://cidris-news.blogspot.com/` et du site `http://www.cidris.fr/` présentant des éléments de recherche et de veille sur les Relations Internationales, la Défense et la Sécurité et sur Internet, sa Gouvernance et le Cyberespace.

Pierre-Yves GOUARDIN Consultant en sécurité des systèmes d'information, Pierre-Yves Gouardin est ingénieur de l'Institut d'Ingénierie Informatique de Limoges.

Pierre-Yves Gouardin met à profit cette formation au service de l'équipe de test d'intrusion d'Orange Consulting.

Florent COTTEY Diplômé d'un Master Réseau, Système et Imagerie à la faculté de Reims et d'un Master Sécurité des Systèmes d'Information à l'Université Technologique de Troyes, Florent COTTEY intervient comme auditeur intrusif pour Orange Consulting. Ses 5 ans d'expérience dans le domaine de la sécurité des systèmes d'informations et de l'audit intrusif l'ont amené à travailler pour le CESTI OPPIDA en tant qu'évaluateur Critères Communs puis chez Areva avant de rejoindre Orange Business Services au sein d'Orange Consulting.

Thomas DUVAL Après avoir obtenu un diplôme d'ingénieur ESEO (informatique et réseau), Thomas Duval a effectué une thèse sur le thème des analyses forensiques (Supélec / DGA MI - ex CELAR) qu'il a soutenu en décembre 2005.

Depuis, Thomas Duval effectue des évaluations sur la sécurité des systèmes d'information (notamment selon les Critères Communs) au sein du CESTI Orange Business Services - Silicomp AQL. En marge de ces activités, Il met en oeuvre son expérience sur l'analyse forensique pour divers travaux au sein du CESTI.

Antoine COUTANT Responsable R&D du CESTI Orange Business Services / Silicomp AQL, Antoine Coutant est ingénieur CNAM en Calcul Scientifique. Après 8 années au sein des services de renseignement français dans un groupe spécialisé dans les cryptanalyses de systèmes cryptographiques, Antoine Coutant a intégré en 2008 le CESTI pour y réaliser des évaluations de sécurité ainsi que différentes analyses de sécurité.

Netglub : Le Renseignement d'Origine Source Ouverte pour ou contre la cyberdéfense

Éléments de réflexion au travers de la plate-forme Netglub

Guillaume Prigent[1]

Responsable et architecte du projet Netglub - diateam, 41 rue Yves Collet 29200 Brest
guillaume.prigent(@)diateam.net

Résumé Le renseignement d'origine source ouverte est une discipline récente dont toutes les richesses ne semblent pas encore exploitées. Nous tentons dans cette communication de fixer le contexte d'emploi de ce domaine et de donner une illustration d'outillage au travers de l'instrumentation de notre plate-forme Netglub. Nous commençons par rappeler ce qu'on entend communément par renseignement d'origine source ouverte afin d'en fixer les contextes d'emplois. Suite à l'exposition de quelques cas d'utilisation nous exposons les fondements de notre plate-forme, son architecture générale et quelques spécificités, avant d'ouvrir le débat et proposer quelques pistes d'études.

Mots-clés: OSINT, ROSO, *datamining*, théorie des graphes, *stream computing*, veille, reconnaissance numérique, signaux faibles, aide à la décision

Note de l'auteur : Dans le cadre de cette communication, l'auteur ne souhaite pas effectuer un état de l'art complet des techniques et méthodologies du renseignement d'origine source ouverte ni présenter cette discipline et ses outils d'un point de vue trop technique. Cela pourra faire l'objet d'une autre communication. Son objectif actuel est plutôt d'exposer démonstrativement et au travers de sa plate-forme quels sont les enjeux du domaine, aussi bien d'un point de vue d'un opérateur de la cyberdéfense que d'un attaquant. Principalement basé sur l'exemple et la démonstration lors de la future présentation qui sera faite, l'ambition de cet article est de montrer de manière plus structurée qu'il est tout à fait possible, en France, d'approfondir et d'outiller ce domaine aussi bien pour aider les problématiques de l'analyse de la menace que celles de la veille offensive.

1 Introduction

Avant de considérer ce que peuvent être les intérêts et les désavantages du renseignement d'origine source ouverte pour un cyberdéfenseur (et de façon duale, pour un cyberattaquant) il convient naturellement de préciser ce que nous entendons par « source ouverte ».

Si tout le monde s'accorde à définir les sources ouvertes comme les sources d'informations accessibles à tous au moyen de médias spécifiques (numériques, analogiques, papiers, rumeurs, ...) et éventuellement payantes (bases de données de Curriculum Vitae, informations financières, annuaires thématiques, ...) il en va autrement dès qu'on s'intéresse aux modalités spécifiques de mise en oeuvre de l'action de captation et d'agrégation de cette information. On peut ainsi se demander si certaines méthodologies triviales du renseignement d'origine humain (« *phoning*[1] », discussions orientées, recoupement de rumeurs ou d'observations sociales, ...) ne sont pas également des sources ouvertes, plus difficiles à trouver cependant.

À notre sens, toute source d'information (qu'elle soit totalement ouverte ou difficile à trouver, voire même réservée à certaines personnes) peut et doit s'intégrer dans le cadre d'une réflexion globale sur le renseignement. Cependant, afin de ne pas dévier du domaine d'étude pour le moment, nous retiendrons dans la suite de cette communication, le sens restrictif de tout ce qui est disponible « communément » et principalement dans l'espace numérique qu'est Internet.

Maillon essentiel et historique de l'intelligence économique et stratégique mondiale dans le secteur privé, il semble que toutes les richesses du renseignement d'origine source ouverte ne sont que partiellement exploitées, tout du moins en Europe et plus particulièrement en France. Le renseignement de source ouverte ne dispose historiquement que de peu de moyens dédiés, alors que la croissance constante de ses flux d'informations requiert des investissements technologiques conséquents, une mutualisation des moyens entre services et une concentration des efforts de collecte, de traitement et d'analyse[1]. Celà peut s'expliquer par l'origine Américaine du domaine où l'on parle publiquement depuis la fin des années 90 de l'*Open Source Intelligence* (OSINT), c'est à dire les techniques et les méthodologies d'analyse et de traitement des *Open Source InFormation*. Au niveau mondial, l'unité opérationnelle OSINT de plus haut niveau est probablement la branche de l'armée américaine d'intelligence de source ouverte du *Special Operations Command Joint Intelligence Center* (SOCJIC). Aux États-Unis, les plus hautes instances étatiques, comme le secrétaire de la Défense Donald Rumsfeld dans son discours au *Council on Foreign Relations*[2] en février 2006, reconnaissent l'importance des médias ouverts comme une composante de la sécurité nationale dans l'âge de l'information numérique. Il est bien sûr difficile de dresser un panorama mondial exhaustif dans un domaine tel que celui ci : en France, cette activité semble pratiquée et disséminée dans toutes les structures étatiques où la veille est un métier historique, mais sans véritable mutualisation ni effort de développement. Seul le Centre d'Enseignement et d'Etudes du Renseignement de l'Armée de Terre (CEERAT) créé en 2002 et basé à Saumur, affiche clairement parmi ses doctrines le « Renseignement d'Origine Sources Ouvertes » (ROSO)

1. Mot anglais qui désigne la prospection ou le démarchage téléphoniques.

et l'objectif de préciser la définition, l'intérêt et l'organisation du ROSO dans les forces terrestres françaises[3]. Dans la suite de cet article, nous tenterons de brosser le contexte dans lequel s'applique le Renseignement d'Origine Source Ouverte et nous effectuerons un focus opérationnel sur quelques cas d'utilisation. La seconde partie de cette communication s'attachera à présenter le cadre de conception de notre plate-forme Netglub destinée à mieux outiller et instrumenter le domaine du ROSO, au moins en France, et ceci à l'aide d'une plate-forme elle-même ouverte.

2 Contexte du renseignement d'origine source ouverte

Aujourd'hui, Internet est un moyen unique d'accès à une multitude de sources d'informations, dynamiques, a priori indépendantes et très hétérogènes. Mais d'un point de vue de la relation consommateur versus producteur d'information, les chemins sinueux d'il y a vingt ans sont devenus à la fois des autoroutes et des égouts de l'information. Dorénavant la société de l'internet oblige quasiment la totalité des organismes privés, publics, ou étatiques à migrer vers l'immense toile informationnelle qu'est l'internet. Les principes structurants de cette culture de l'affichage, de l'instantanéité et de l'interconnexion dépassent complètement nos capacités (et notamment notre échelle temporelle au niveau de nos prises de décisions) de compréhension convenable de ce système complexe (maillé, multi-niveaux, hétérogène, dynamique, ...). Pour parachever le tout, il n'a jamais été aussi facile, pour quiconque, d'assurer seul (pour un individu, une structure privée, une association, ...) sa production et publication d'information.

L'indépendance (relative) et surtout l'hétérogénéité des sources ouvertes d'information sont des atouts majeurs pour un prédateur informationnel ou simplement pour celui qui cherche à recouper de l'information [4] ou mieux comprendre le contexte numérique d'une entité (qu'il soit technique comme pour un serveur physique présent sur le web, économique comme pour l'image d'une entreprise ou encore social pour des utilisateurs de réseaux sociaux).

Pour autant, s'il est aisé d'effectuer quelques recherches manuelles et bien souvent simplement outillé d'un butineur hypertoile [2] et de quelques moteurs de recherches (voire de bases publiques « ouvertes »), il va autrement dès qu'il faut traiter rapidement un gros volume d'information de « source ouverte ».

Dès lors, le problème qui se pose est pluriel :

- les sources ouvertes sont multiples et toujours contextuelles (au niveau de la sémantique qu'elles manipulent) ;
- le ou les modi operandi d'acquisition de ces informations sont toujours spécifiques aux fournisseurs (les « sources ») ;

2. Plus communément appelé « *crawler Web* »

- la corrélation et le recoupement d'informations hétérogènes provenant de « sources » différentes sont très difficiles (au niveau structurel de l'information comme au niveau sémantique) ;
- la quantité d'informations disponible, le fameux facteur d'échelle, étouffe rapidement notre capacité à analyser la qualité de l'information (quantité versus qualité) ;
- la confiance à accorder (ou non) à chaque information ou à chaque « source ouverte » est très difficile à qualifier et/ou pondérer d'autant qu'elle peut varier dans le temps (et rétroactivement) ;
- même si on est en droit de se demander si l'internet a une mémoire, les « sources ouvertes » et les informations accessibles sont dynamiques ; une information possède intrinsèquement un ou plusieurs caractères temporels (date de création, date de publication, dernières dates de modification, etc.) et il est quasi impossible à ce jour d'en suivre les multiples évolutions (soit parce que ces facteurs ne sont pas toujours connus, soit parce qu'il s'agit de phénomènes qui se déroulent en « temps réel »).

Dès lors que le contexte et le champ d'investigation sont, au moins partiellement, brossés, il devient intéressant d'essayer d'en comprendre les intérêts et les richesses, aussi bien au niveau des enjeux dans un contexte de cyberdéfense que dans celui de l'analyse des menaces qui pèsent à ce niveau informationnel, c'est à dire la vision opposée, celle du cyberattaquant.

Afin de montrer, en négatif, les enjeux du renseignement d'origine source ouverte pour la cyberdéfense, nous prenons volontairement le point de vue opposé et nous privilégions, dans un premier temps, le point de vue de l'opérateur de renseignement qui souhaite exploiter au mieux les richesses de cette discipline et par extension directe, la menace.

3 Cas d'utilisations

Les motivations qui peuvent animer un opérateur du ROSO sont vastes, la surface d'attaque et de collecte est immense. A titre d'illustration et de manière non exhaustive, il peut s'agir :

- de collecter et d'analyser la « Blogosphère[3] » afin d'essayer de prédire le taux de pénétration potentiel d'un produit commercial comme un film ou d'un type de musique[5] ;
- d'analyser et de détecter les personnes « pivots » dans un groupe ou un réseau social[6] ;

3. Désigne indifféremment un ensemble de blogues ou l'ensemble de ses rédacteurs. L'expression « la Blogosphère » désigne ainsi l'ensemble de tous les blogues, c'est à dire un sous-ensemble du *World Wide Web*.

- de détecter des visages dans une large collection afin d'identifier « visuellement » et de recouper des informations concernant une personne « profilée »[7] ;
- d'utiliser les réseaux sociaux tels que Facebook pour tenter de récupérer des informations économiques précieuses par l'intermédiaire d'employés et de profils trop « ouverts »[8] ;
- d'analyser, de recueillir et d'agréger toutes les informations fiscales, de gestion, de brevets et de participations afin de mieux engager une Offre Publique d'Achat (OPA) hostile envers une société possédant des savoirs et/ou des savoir-faire critiques (cas de « l'affaire » Gemplus [4] en 2000) ;
- d'obtenir une meilleure perception de l'environnement technologique d'un produit considéré et en particulier d'identifier les interdépendances (et naturellement les maillons faibles) des entités en « relation » avec la cible, qu'il s'agisse d'un processus, d'un composant logiciel ou matériel, ou d'une idée ;
- d'effectuer une vaste phase de « reconnaissance » technique et organisationnelle avant un test d'intrusion pour mieux appréhender le contexte opérationnel de la cible (plages d'adresses IP, prestataires, zones géographiques, types de serveurs, types de services, ...)

La liste précédente peut s'enrichir de toute sorte de cas d'utilisation du moment que les méthodologies et techniques mises en oeuvres sont celles de l'intelligence et du renseignement « source ouverte », c'est à dire :

1. identifier le besoin (la question qu'on se pose, sur quoi et/ou qui) ;
2. identifier les « sources ouvertes » de collectes potentielles ;
3. acquérir ou extraire les éléments d'information unitaire dans leur contexte ;
4. analyser et normaliser l'information réellement utile ;
5. visualiser les dépendances produites et mieux comprendre leurs structurations ;
6. élaguer, éventuellement qualifier et enrichir les résultats ;
7. réitérer de proche en proche.

A peu de choses près, cette première vision correspond finalement au cycle classique de l'intelligence et du renseignement appliqué aux « sources ouvertes » (Fig. 1).

Ces démarches de collecte, d'analyse, de visualisation et d'enrichissement ne sont plus possibles manuellement (hormis quelques cas spécifiques bien particulier) face à la réactivité nécessaire et au volume des données disparates à traiter, aussi bien d'un point de vue de la veille (passif) que de la recherche d'informations ciblées (actif). Depuis quelques années, il existe plusieurs outils qui instrumentent

4. Entreprise française de fabrication de cartes à puce. Gemplus a fusionné avec Axalto en 2007 pour former le groupe Gemalto.

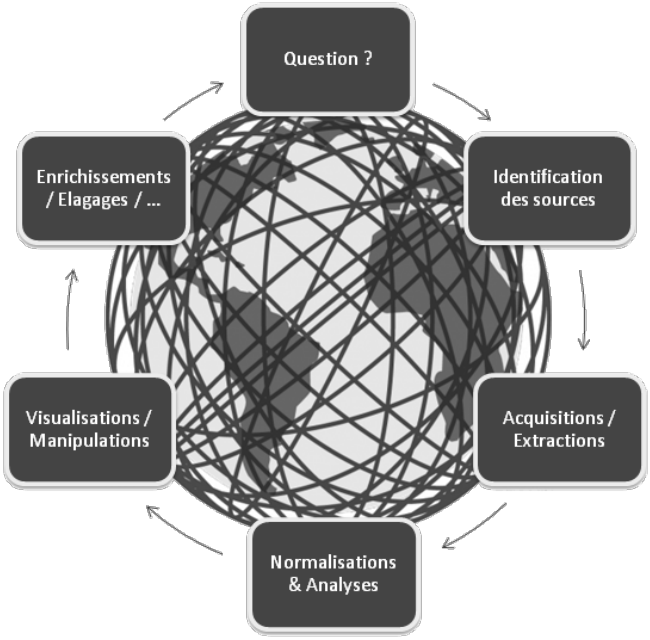


Figure 1. Cycle du renseignement adapté au ROSO

ces techniques et méthodes pour tenter de capter la richesse souvent inexploitée du renseignement issu de sources ouvertes. Les deux outils ou services les plus illustratifs de cette instrumentation du domaine sont à notre sens :

- *Analyst's Notebook* (actuellement en version 8.5) édité par la société i2 (Fig. 2) ;
- *Maltego* édité par la société Sud Africaine Paterva (Fig. 3).

S'il est donc vrai que ce domaine est déjà outillé (au moins partiellement), le plus souvent les briques technologiques utilisées sont réservées à quelques privilégiés qui préservent de manière propriétaire leurs plate-formes, leurs outils et leurs méthodologies (c'est le coeur de leur modèle). Au travers du projet Netglub présenté dans la section qui suit, nous avons souhaité montrer qu'il était tout à fait possible de concevoir, implémenter et utiliser une plate-forme distribuée de renseignement d'origine source ouverte, ergonomique, fonctionnelle et si possible elle-même libre.

4 La plate-forme Netglub

L'objet de cette section n'est pas de décrire dans les détails toutes les spécifications du projet et de notre plate-forme mais bien plus d'en montrer les principes fondateurs et ce qui peut la distinguer des autres solutions.

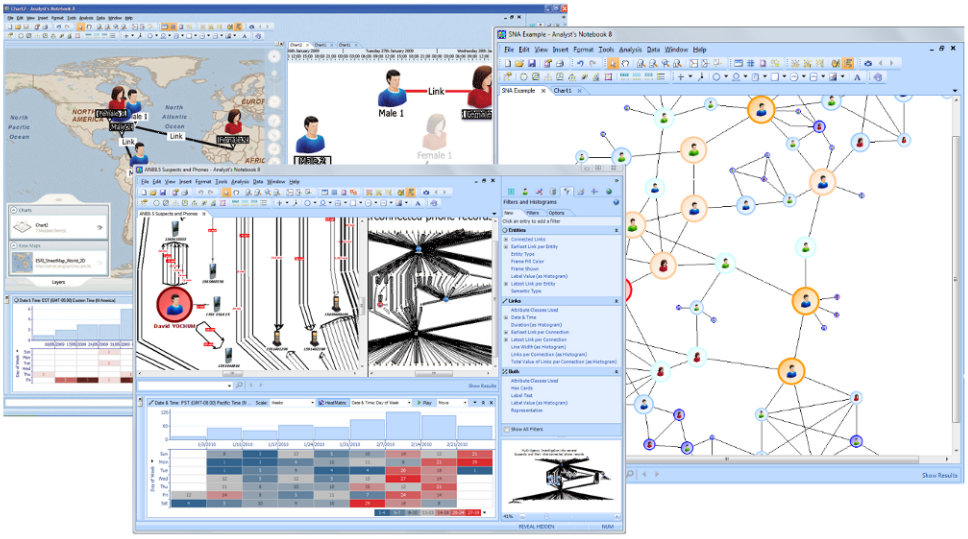


Figure 2. Interfaces visuelles de différents modules du logiciel *Analyst's Notebook 8.5*

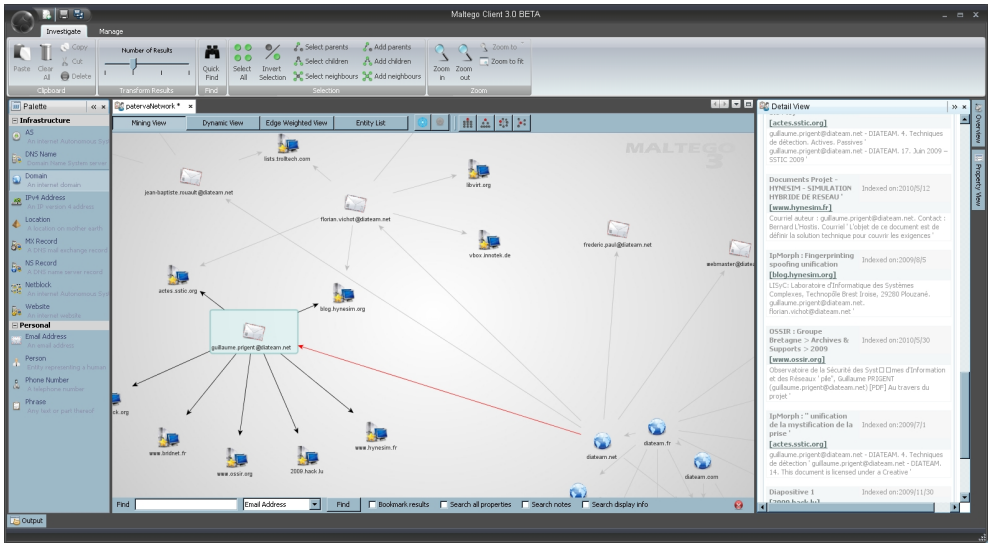


Figure 3. Interface visuelle du client Java *Maltego 3.0*

4.1 Cadre de conception

Aux Etats-Unis, et dès 1992, l'amiral William Studeman pose le cadre général de la création d'une plate-forme de renseignement d'origine source ouverte[9] :

> *The plan establishes the goal of creating an integrated Community open source architecture. The new architecture must provide, among other things :*
> – *flexible collection,*
> – *networked access to external data bases,*
> – *immediate user and customer feedback, and*
> – *automated, profiled delivery of collected open source information based on user requirements.*
>
> *We expect the centerpiece of the architecture will be an Open Source Information Exchange comprising a central switch and digital communications networks which interconnect all user organizations within the Community.*

Suivant ces principes, Netglub est, en l'état et à ce jour, un démonstrateur technologique complètement fonctionnel d'une plate-forme distribuée de renseignement d'origine source ouverte. La plate-forme Netglub est elle-même issue d'une réflexion de longue date et est conçue, développée et maintenue exclusivement par la société diateam.

Notre approche, comme habituellement dans la plupart des projets de recherche et de développement que nous menons, a été la suivante :

– analyser les offres disponibles et effectuer un état de l'art des différentes techniques de captation et d'extraction des sources ouvertes ;
– identifier les composants sur étagères qui peuvent nous aider à la mise en place d'une véritable infrastructure de ROSO ;
– privilégier les composants ou les outils sur leur origine *Open Source* (au sens cette fois du développement logiciel) ;
– identifier les verrous technologiques et les limitations des offres actuelles ;
– définir une architecture souple et évolutive sans nécessité de développements conséquents ;
– implémenter diverses Preuves de Concept [5] sur la faisabilité des différentes fonctionnalités nécessaires ;
– comparer nos résultats avec les autres outils du domaine ;
– réitérer et ainsi déboucher sur le démonstrateur complet.

Le fondement de notre raisonnement est le suivant ; chacun doit pouvoir contrôler complètement sa chaîne de renseignement d'origine source ouverte et

5. La Preuve de Concept (*Proof of Concept* - PoC) est une réalisation courte ou incomplète d'une certaine méthode ou idée pour démontrer sa faisabilité. La preuve de concept est habituellement considérée comme une étape importante sur la voie d'un prototype pleinement fonctionnel.

surtout ne doit pas dépendre d'un logiciel opaque (tels que des clients graphiques propriétaires ou des serveurs de ROSO classiques en mode hébergé hors de contrôle). Cette nécessité existe tout d'abord pour des raisons de confidentialité (chacun doit pouvoir contrôler complètement ce qu'il fait et être souverain sur sa mission) . En second lieu pour des raisons purement métier au sens ou chaque opérateur de la solution Netglub doit pouvoir rajouter librement ses « sources ouvertes » (ou même plus « hermétiques ») ainsi que ses propres moteurs d'extraction d'information.

Enfin, il nous semble primordial d'envisager les sondes d'acquisition d'information issue de source ouverte comme des éléments potentiellement « jetables » (au sens d'une adresse IP) et de ce fait permettre l'emploi d'une « grappe » extensible et malléable de serveurs Netglub qui rendent les services demandés suivant certaines spécifications (comme la possibilité d'anonymiser les requêtes d'acquisition et d'extraction au travers de chaînage de proxy ou de réseaux tels que Tor). Les différentes phases du cycle classique de l'intelligence et du renseignement doivent impérativement êtres scindées afin de pouvoir construire son propre système de manière modulaire tout en permettant un chaînage complet, distribué, sécurisé et redondant.

4.2 Fonctionnalités principales

Les fonctionnalités principales actuelles de la plate-forme Netglub sont :

- un catalogue d'entités et de transformations qui peut être vu comme l'ontologie des concepts manipulés (les informations qu'on manipule) et comme les actions unitaires d'acquisition et d'extraction sur les sources ouvertes que nous considérons ;
- un moteur de rendu de graphes qui possède de nombreuses vues et de nombreux « rendus » (hiérarchiques, radiaux, énergie basés, ...) afin de mettre en évidence rapidement les dépendances et relations entres les entités manipulées ;
- un moteur de script intégré qui permet d'automatiser et d'utiliser directement certaines fonctionnalités internes de Netglub. Ainsi, il est possible de manipuler programmatiquement (en ECMAScript [6]) des graphes, des entités et des transformations ;
- l'extensibilité offerte par l'ajout de nouvelles transformations afin d'étendre les fonctionnalités de Netglub. Il est ainsi possible de créer des transformations et de les ajouter à un esclave Netglub ou au client graphique directement (transformation locale) pour les utiliser ;

6. http://www.ecma-international.org/publications/standards/Ecma-262.htm

– une gestion fine des droits accordés aux utilisateurs selon les profils et les transformations autorisées sur certaines « sources ouvertes » (gestion et contrôle effectués sur le maître Netglub).

4.3 Éléments d'architecture

Comme présenté sur la figure 4, Netglub est une plate-forme distribuée architecturée en plusieurs niveaux. Au coeur de l'architecture, se trouve un serveur métier **maître** qui possède une grappe de serveurs **esclaves** à sa disposition. Il possède un catalogue de l'ensemble des entités et des transformations existantes ainsi qu'une base de données pour gérer entre autres les droits des utilisateurs.

Un serveur esclave est capable de réaliser des transformations (présentes sous la forme de plugins et de scripts). Il se connecte à un serveur maître quand il démarre et lui annonce la liste des transformations qu'il possède. Le programme du serveur esclave est massivement « multithreadé » afin qu'il soit capable d'exécuter de multiples transformations simultanément.

L'Interface Homme Machine (IHM) de Netglub est un client lourd qui se connecte au serveur maître par le biais d'une connexion sécurisée en SSL [7]. Il dialogue ensuite avec ce dernier à l'aide du protocole XML-RPC [8] pour récupérer les entités et les transformations disponibles, ou encore pour lui demander la réalisation de transformations sur des entités. Le maître se charge alors de répartir les transformations à exécuter sur ses différents esclaves, et renvoie les résultats au client quand ils sont disponibles sur les esclaves.

4.4 Quelques focus techniques

Hormis les transformations qui sont essentiellement des scripts python et php, l'ensemble de la plate-forme Netglub est développé à l'aide du framework C++ Qt4 [9] de Nokia. Bien que l'accent ait été mis sur l'utilisation de COTS, le protocole de communication entre le serveur maître et les esclaves a été développé spécifiquement pour Netglub, afin de supporter certaines fonctionnalités propres à ce dernier sans toutefois s'encombrer du code superflu d'une technologie existante.

XML-RPC (avec libmaia [10]). Comme nous avons pu le voir dans la section précédente, la communication entre les clients et le serveur maître s'effectue en XML-RPC. Netglub intègre une version modifiée de la bibliothèque « libmaia » (une bibliothèque de XML- RPC développée à l'aide de Qt) à laquelle le support du

7. *Secure Socket Layer* est un protocole de sécurisation des échanges en réseau, et en particulier sur l'internet, devenu *Transport Layer Security* (TLS) en 2001
8. XML Remote Procedure Call.
9. `http://qt.nokia.com`
10. `https://frucman.frubar.net/libmaia`

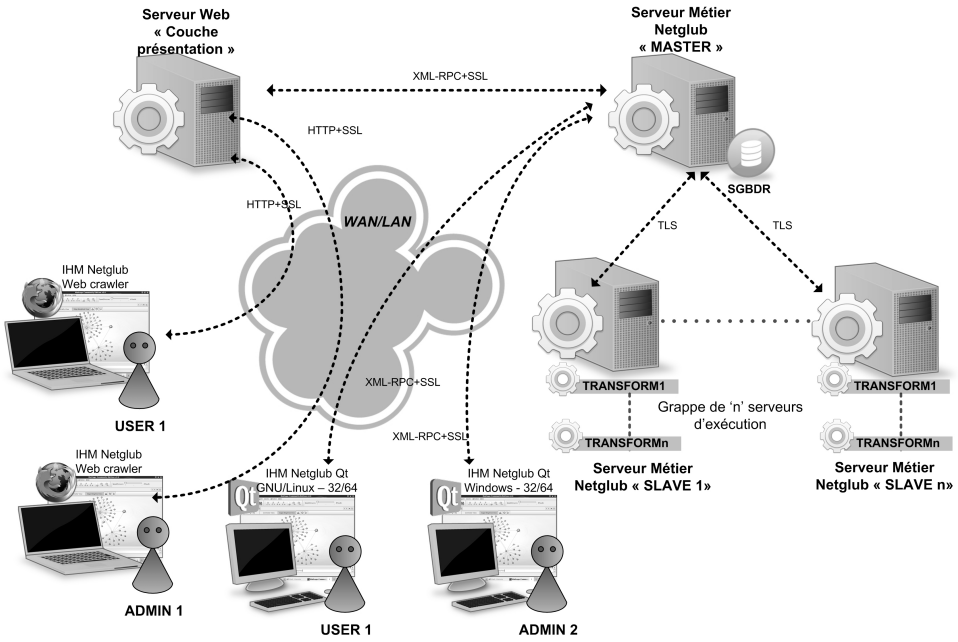


Figure 4. Vue d'ensemble de l'architecture générale réseau de la plate-forme Netglub

SSL a été ajouté afin que les communications entre clients et serveur soient chiffrées. De même nous utilisons le support de TLS pour la partie « grappe » entre les esclaves et le maître coordinateur.

Une IHM de contrôle : qng. L'IHM de Netglub, dont on peut voir une capture d'écran ci-dessous (Fig. 5), permet de créer de nouveaux graphes, d'y ajouter des entités et d'exécuter des transformations sur ces dernières à l'aide d'une interface graphique intuitive. Qng intègre le moteur de scripts dont nous avons parlé précédemment, et il est donc possible de visualiser « en temps réel » le résultat de l'exécution d'un chaînage de renseignement dans la zone d'affichage des graphes.

Rendu des graphes avec l'API C de Graphviz[11]. Le client graphique qng utilise la bibliothèque Graphviz pour effectuer les calculs d'agencement des graphes : l'ensemble des noeuds du graphe (les entités) ainsi que les arcs les reliant les uns aux autres sont fournis à Graphviz qui se charge de calculer les nouvelles positions de chaque noeud. Qng effectue ensuite un rendu graphique (Fig. 6) animé du changement d'agencement du graphe à partir des informations fournies par Graphviz et d'algorithmes réimplémentés (comme la *betweenness centrality*) afin de piloter le rendu graphique (notamment au niveau des « bounding box » des noeuds informationnels).

11. `http://www.graphviz.org`

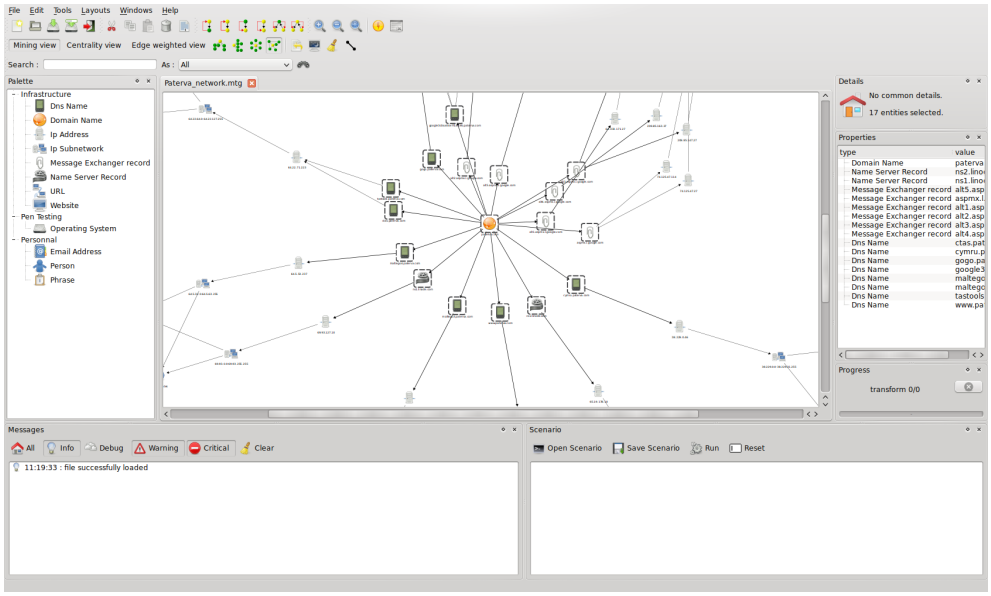


Figure 5. L'interface qng, une IHM de la plate-forme Netglub

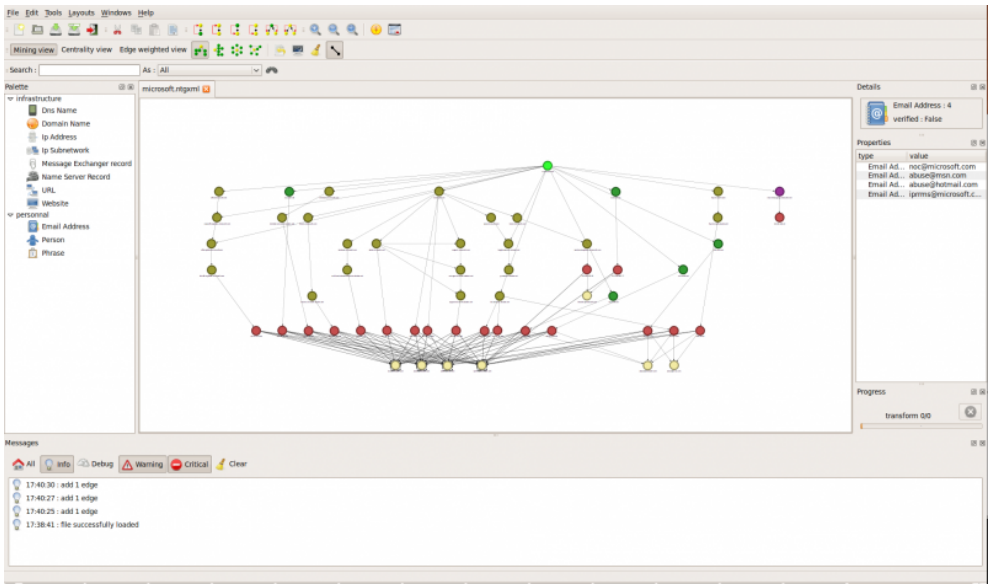


Figure 6. Différentes vues dynamiques de graphes dans l'IHM à l'aide de l'API C Graphviz et du support SVG

Outils métiers pour les transformations. Netglub expose de nombreuses entités (adresse IP, site internet, numéro de téléphone, phrase, ...) que l'utilisateur peut créer et manipuler en leur appliquant des transformations. De nombreux outils unitaires existent déjà et permettent d'obtenir une ou plusieurs « entité(s) » en relation avec ce qui leur a été donné en entrée. C'est pourquoi la plupart des transformations de Netglub utilise des outils « métiers » existants en les chaînant éventuellement entre eux afin d'obtenir les résultats attendus par l'utilisateur. Parmi ces outils, on peut citer :

- DNSenum [12] : pour obtenir des informations sur les noms de domaine ;
- Robtex [13] : récupération d'informations sur les noms de domaine (technique de *Web scraping* [14]) ;
- OpenCalais [15] : pour extraire des données « web sémantique » des documents ;
- Alchemy API [16] : même utilisation qu'OpenClais ;
- Metagoofil [17] : extraction de métadonnées disponibles dans des documents en ligne (pdf, doc, xls, ...) ;
- Nmap [18] : pour obtenir des informations sur les services ou le système d'exploitation d'une machine ;
- Scripts de recherches de bases « Web » (societe.com, inpi, fournisseurs de la défense, infogreffe) ;
- API des réseaux sociaux ;
- John the Ripper [19] : cassage de *hash* et de mot de passe ;
- WhatWeb [20] : identification de CMS [21] ;
- Wikipedia [22] : *Web scraping* pour identifier les adresses IP utilisées pour modifier des articles ;
- Google dorks ;
- etc...

En pratique, tout ce qui existe est directement intégrable dans le cadre d'application Netglub. En outre, il est important de noter que Netglub ne se contente pas de fournir l'ensemble des résultats retournés par ces différents outils, mais qu'un filtrage est effectué afin d'éliminer le maximum de faux positifs.

12. `http://code.google.com/p/dnsenum`
13. `http://www.robtex.com`
14. Extraction du contenu d'un site Web à l'aide d'un programme ou d'un script.
15. `http://www.opencalais.com`
16. `http://http://www.alchemyapi.com`
17. `http://www.edge-security.com/metagoofil.php`
18. `http://nmap.org`
19. `http://www.openwall.com/john`
20. `http://www.morningstarsecurity.com/research/whatweb`
21. *Content Management System*
22. `http://www.wikipedia.org`

5 Synthèse et perspectives

Au travers de cette première communication, nous avons souhaité montrer que le renseignement d'origine source ouverte était, en négatif (du point de vue d'un cyberattaquant), une discipline très riche, potentiellement utile et déjà bien instrumentée si elle est associée aux autres « typologies » du métier de l'intelligence et du renseignement. Dès lors, il devient évident que son caractère dual peut permettre à un cyberdéfenseur de mieux prendre en compte les menaces potentielles qui pèsent sur son organisation (qu'elle soit privée, publique, étatique) en effectuant lui même cette phase de collecte et de traitement sur ses propres signaux faibles disséminés dans l'internet.

Finalement et comme toujours dans la sécurité des systèmes d'information, tout est réversible. Le renseignement d'origine source ouverte peut être considéré comme un atout (voire une arme) pour un opérateur de renseignement comme une menace directe pour un cyberdéfenseur qui souhaite juguler et contraindre la dissémination de son patrimoine informationnel. Ce discours, qui peut sembler alarmiste, doit naturellement être pondéré. Aujourd'hui il existe encore de nombreux écueils techniques et structurels (voire même méthodologiques) comme la capacité à gérer la confiance des informations recueillies, la définition d'une ontologie suffisamment exhaustive, le caractère fondamentalement dynamique des informations et des sources numériques (évolution dans le temps) et le facteur d'échelle qui semble difficilement franchissable à l'heure actuelle.

Au mieux, correctement instrumentés (d'un point de vue technique) et convenablement utilisés (d'un point de vue de l'analyste humain qui fait le tri, qui sélectionne et qui pilote), les outils actuels permettent de se doter d'un aimant plus puissant dans une meule de foin chaque jour plus large et peuvent dans ce cas constituer une aide à la décision significative.

Au pire et mal outillé, il s'agit d'une nouvelle manière de se noyer plus rapidement dans un maelström d'informations automatiquement mises en relations sans expressivité significative ni quelconque plus-value (ou comment la machine gagne encore en anéantissant la qualité par la quantité).

Références

1. Zone d'Intérêt : Hérisson et OSINT, `http://zonedinteret.blogspot.com/2009/04/herisson-et-osint.html` (avril 2009)
2. Rumsfeld, D.H. : New Realities in the Media Age, Council on Foreign Relations, New York, `http://www.cfr.org/publication/9900/new_realities_in_the_media_age.html` (17 février 2006)
3. Centre d'Enseignement et d'Etudes du Renseignement de l'Armée de Terre (CEERAT) : Renseignement d'origine sources ouvertes (ROSO), `http://www.ceerat.terre.defense.gouv.fr/spip.php?rubrique31` (2010)
4. Loewenthal, J.F. : Le renseignement via les « sources ouvertes » (OSINT) : Une nouvelle discipline ? Centre Français de Recherche sur le Renseignement, `http://www.cf2r.org/fr/cyber-rens/le-renseignement-via-les-sources-ouvertes-osint-une-nouvelle-discip.php` (janvier 2008)

5. Fabian Abel, Ernesto Diaz-Aviles, Nicola Henze, Daniel Krause, Patrick Siehndel : « Analyzing the Blogosphere for Predicting the Success of Music and Movie Products », Social Network Analysis and Mining, International Conference on Advances in, pp. 276-280, 2010 International Conference on Advances in Social Networks Analysis and Mining (2010)
6. Esslimani, I. Brun, A. Boyer, A., « Detecting Leaders in Behavioral Networks », Social Network Analysis and Mining, International Conference on Advances in, pp. 281-285, 2010 International Conference on Advances in Social Networks Analysis and Mining, (septembre 2010)
7. iOSINT : « Face-recognition added in Picasa 3.6 - great OSINT processing tool », `http://iosint.wordpress.com/2010/03/31/face-recognition-added-in-picasa` (mars 2010)
8. Siciliano, R. « Using Facebook to Steal Company Data », `https://www.infosecisland.com/blogview/3579-Using-Facebook-to-Steal-Company-Data.html` (mars 2010)
9. Studeman, W. : Teaching the Giant to Dance : Contradictions and Opportunities in Open Source Within the Intelligence Community, First International Symposium on Open Source Solutions, `http://www.fas.org/irp/fbis/studem.html` (décembre 1992)

De Big Brother à small brothers : cyber guerre dans le nanomonde ?

De la surveillance à la sousveillance ?

Jean-Philippe Lelièvre

Thalès lelievre.jp(@)free.fr

Résumé Après avoir expliqué ce qu'est la RFID et rappelé son intérêt en matière de sécurité des systèmes d'information, nous étudions les interactions entre RFID et vie privée, notamment sous l'angle de la localisation et du traçage électronique des personnes. Après avoir présenté les solutions de protection existantes, nous convoquons la guerre électronique d'une part et la sécurité des systèmes d'information d'autre part pour améliorer cette protection car l'acceptation du public est la condition sine qua non du succès de la technologie RFID, de ses successeurs : Machine2Machine, Internet des objets et Ubimedia ainsi que de tous les secteurs dans lesquels la RFID est désormais implantée. Le but de ce document, est de susciter l'intérêt de spécialistes de la sécurité des systèmes d'information et de la guerre électronique afin qu'ils trouvent des solutions à cette problématique de protection non plus seulement des SIC et autres C4ISR étatiques et de l'infrastructure critique mais de l'individu et de ses libertés.

1 Introduction : la RFID

1.1 Qu'est ce que la RFID ?

La RFID est la lointaine mais directe descendante de l'IFF (Identification Friend or Foe) un moyen radio mis en oeuvre par l'aéronautique britannique durant la seconde guerre mondiale pour distinguer ses avions de ceux de ses ennemis allemands que le radar ne suffisait pas à discriminer. Dans l'acronyme RFID (Radio Frequency IDentification) ID signifie identification. Or l'identification, qui est l'affirmation sans preuve d'une identité, est plus faible que l'authentification qui, elle, apporte la preuve de ladite identité. Il y a donc inadaptation intrinsèque de la RFID à la sécurité. C'est pourtant sur ce socle branlant qu'est basée la sécurité de nombreux systèmes.

En 60 ans, du fait de la vertigineuse chute des prix des ordinateurs, et de leurs capacités exponentielles, nous sommes passés d'un ordinateur utilisé par N personnes à plusieurs ordinateurs/calculateurs par personne. La RFID accentue cette tendance en connectant des multitudes d'objets/êtres vivants par simple apposition d'une étiquette, d'une carte à puce sans contact ou d'un badge RFID à tout type d'objet de notre environnement.

1.2 La RFID comment ça marche ?

La RFID permet d'associer du virtuel à du réel. En effet, en collant une étiquette RFID sur n'importe quel objet on permet d'assigner des informations à cet objet. Une étiquette RFID peut être vue comme un petit système d'information (doté d'un processeur, de mémoire et éventuellement d'une batterie lorsque l'antenne n'apporte pas assez d'énergie). Une étiquette RFID ayant aussi un étage radio, elle peut donc aussi être vue comme un minuscule émetteur/récepteur. Suivant les pays et les usages, les fréquences utilisées en RFID peuvent se trouver dans les gammes suivantes :

- LF (basses fréquences),
- HF (hautes fréquences),
- UHF (ultra hautes fréquences),
- SHF (super hautes fréquences)

1.3 Composants d'une chaîne RFID

Les composants principaux d'une chaîne RFID sont : l'étiquette, la station de base, l'intergiciel et l'applicatif métier.

Etiquette (tag en anglais) : c'est la partie la plus visible/apparente et la plus nombreuse de l'ensemble de la chaîne

La station de base appelée aussi BTS, base station, portique, lecteur est la seconde partie émergée de l'iceberg RFID.

L'intergiciel gère spécifiquement la RFID : à quoi correspond cette étiquette, d'où vient-elle, où doit-on l'envoyer, que doit-on écrire dans sa mémoire ?

L'applicatif métier enfin est ce qui va donner du sens aux maillons précédents : et faire la différence entre le comptage de skieurs, de passagers dans un bus ou de vaches dans un champ...

1.4 En quoi la RFID concerne-t-elle la sécurité des systèmes d'information ?

La problématique de la sécurité des systèmes d'information intrinsèque à la RFID Comme nous l'avons vu, une étiquette RFID est un mini système d'information et de communication et donc, en tant que telle, elle relève de la sécurité des systèmes d'information.

La RFID est importante de par les quantités d'étiquettes en circulation Plusieurs milliards d'étiquettes RFID sont produites chaque année (environ 4 milliards d'étiquettes produites en 2009, davantage en 2010).

La RFID est importante car elle est déjà utilisée pour des applications sensibles Les passeports de dernière génération (dits biométriques), conformes au format de l'Organisation de l'Aviation Civile Internationale (OACI), sont dotés d'une étiquette RFID dans laquelle sont inscrits des éléments nominatifs, des images numérisées et des éléments biométriques (empreintes digitales...). Certains être humains se sont fait implanter des puces sous cutanées (applications permettant de localiser/retrouver des malades atteints d'Alzheimer, certains militaires US, et application plus futile et anecdotique, des habitués de certaines boîtes de nuit). Ces applications doivent être sécurisées.

La RFID est importante en tant que précurseur

La RFID est importante en tant que précurseur de l'Internet des objets
L'Internet du futur (comme en général le futur (sic)) n'est pas encore bien défini (Web 3.0, Web sémantique...) mais l'hypothèse que nous retenons et que nous allons commenter est que l'Internet du futur serait pour partie l'Internet des objets, M2M (Machine 2 Machine), WSN (Wireless Sensors Networks).

Aujourd'hui, chacun d'entre nous possède et utilise fréquemment une petite dizaine d'objets communicants (téléphone portable, PC portable, appareil photo, assistant personnel, GPS...). Ce nombre d'objets communicants va croître dans les prochaines années, mais la principale source de croissance du nombre d'objets devrait venir d'ailleurs, des objets de la vie courante. Chacun d'entre nous est déjà entouré par des centaines voire des milliers d'objets, dont plusieurs centaines lui appartiennent. En rajoutant des étiquettes RFID à certains de ces objets, on leur confère une capacité de communication avec entre autres Internet et... une autre dimension/utilité/vie : virtuelle. L'ajout de ces milliards d'objets communicants dimensionnerait alors l'Internet du futur qu'il faudra bien évidemment sécuriser.

La RFID précurseur des nanotechnologies... et peut-être d'une société de surveillance
Derrière la RFID se profilent les nanotechnologies (composants de l'ordre du nanomètre au confluent entre biologie et électronique) qui multiplieront les problèmes, notamment parce qu'elles sont souvent associées à une société de surveillance. La RFID peut apparaître comme précurseur d'une intensification de la surveillance dans la société car après les points prometteurs de la RFID vus précédemment, le dernier point est évidemment problématique et nous allons le creuser ci-dessous.

2 Problématique : interactions entre RFID et vie privée

2.1 La vie (privée) vaut-elle d'être vécue ?

Constatons qu'il est loin d'être évident que la vie privée ait encore un avenir, du moins aux yeux de certains, lorsque :

- l'on lit les déclarations d'Eric Schmidt, le président directeur général de Google pour justifier la mise en ligne et le non-retrait d'informations personnelles sur ses centaines de millions de clients *"If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place."*
- l'on voit la facilité avec laquelle des millions de personnes acceptent de remplir des descriptifs personnels sur les réseaux sociaux, incluant l'acceptation de sa propre localisation et le descriptif de ses activités en ligne (Twitter...) ainsi que l'affichage de ses opinions, ses goûts, ses préférences sexuelles...

Formulons néanmoins l'hypothèse que cette abolition de la vie privée soit un problème et qu'il vaille la peine de préserver ladite vie privée.

2.2 Le cas particulier de la localisation et du traçage

La vie privée est souvent vue sous l'angle de l'opinion, de la liberté d'expression : « qui suis-je ? Quelle est mon opinion ?... » Or, avec la technique, se développe une branche de la vie privée qui était longtemps restée secondaire, la position géographique : « Où suis-je ? » C'est à cette branche de la vie privée appelée géo localisation, traçage électronique,... que nous allons nous intéresser car c'est à ce niveau que se concentrent les interactions entre vie privée et RFID.

2.3 Etat actuel du traçage électronique sans RFID

Bruce Schneier :"we lose our individuality because everything we do is detectable and recordable"

La géo localisation est la technique qui permet de savoir où est une personne à un moment donné, d'où elle vient, combien de temps elle y reste, qui y est en même temps qu'elle, où elle se dirige... Pour ceux qui ne voient pas l'intérêt ni le danger que d'autres aient accès à ces informations et qui se disent : « qu'est-ce que ça peut faire ? Je n'ai rien à cacher ! » . Pour fixer les idées, demandez-vous si vous aimeriez devoir répondre aux questions suivantes ?

- Etiez-vous à la manifestation de la semaine dernière ?
- Aviez-vous préparé cette manifestation la semaine précédente ? Chez Monsieur X. ?
- Etes-vous allé dans un centre IVG ?
- Avez-vous consulté sur le SIDA ?

- Etiez-vous dans un hôtel à l'heure du déjeuner ? Avec votre secrétaire ?
- Etes-vous souvent vu à côté des bureaux de votre concurrent ? D'un cabinet de chasseur de têtes ?
- A quelle église, quel temple, quelle mosquée, quelle synagogue, quelle loge, quel bar gay allez-vous ?

Voyons ci-dessous quelques uns des éléments hors RFID qui contribuent au traçage électronique.

Rétention de données La directive européenne 2006/24/EC de 2006 impose aux opérateurs téléphoniques et Internet d'enregistrer tous les numéros appelés par les téléphones mobiles ainsi que tous les sites Internet visités, les courriels envoyés et reçus pendant une durée qui varie entre 6 et 24 mois suivant les pays européens.

Traçage/géo localisation (via les téléphones cellulaires : GSM, UMTS) L'opérateur téléphonique et les services d'ordre peuvent savoir où se trouve le détenteur d'un téléphone portable (que celui-ci soit en communication ou en veille) avec une précision de l'ordre de la taille d'une cellule téléphonique : soit au « mieux » quelques centaines de mètres en ville, à quelques kilomètres dans les zones moins peuplées. Si le téléphone est équipé d'un GPS, la précision peut tomber sous le mètre en extérieur.

Réseaux sociaux La version 2 du Web (Web 2.0) doit beaucoup aux réseaux sociaux (Facebook, Myspace, MSN, copains d'avant, LinkedIn...) dans lesquels les personnes remplissent leur « profil » avec des éléments biographiques, leurs activités, avis, préférences, amis, photos... Mention spéciale pour :

- Twitter dans lequel on déclare presque en temps réel ce que l'on fait et où on le fait, sur une base de volontariat,
- certains services Apple, Google, Facebook Places où l'on fournit sa position avec la précision du GPS en temps réel à son réseau de connaissance.

Caméras vidéo CCTV (Closed Circuit Tele Video) Un des pays les plus avancés en vidéo surveillance est la Grande-Bretagne qui est « couverte » de plusieurs millions de caméras de surveillance, dont quatre millions pour l'agglomération londonienne. Certains scénaristes TV laissent entendre qu'il serait possible pour les services de sécurité de prendre quelqu'un en filature dans Londres et sa périphérie seulement à l'aide des caméras de surveillance. La reconnaissance faciale amplifiera l'efficacité de ces outils.

Archivage des questions posées sur les moteurs de recherche et sur les portails géographiques Il se dit que Google archiverait toutes les questions

qui sont posées sur ses moteurs de recherche et Google maps et Google earth. A quelle fin ? Pour qui ? Jusqu'à quand ?

Et bien d'autres moyens... Il serait évidemment possible de donner d'autres exemples pouvant contribuer au traçage électronique (plaques minéralogiques...) mais l'élément le plus déterminant sont le croisement et la fusion des données recueillies par tout ou partie des systèmes ci-dessus.

Fusion/intégration des données ci-dessus Les différentes données ci-dessus prennent évidemment un relief particulier lorsqu'elles sont fusionnées entre elles et enrichies des relevés bancaires, de parking, de transport public, des factures d'alimentation... A cela s'ajoutent aussi des données issues de la RFID dont nous allons évaluer l'apport ci-dessous.

2.4 Etat actuel du traçage électronique avec RFID : traçabilité des animaux, des êtres humains et des objets

La RFID permet la traçabilité de nombreuses entités

Traçabilité des animaux

La traçabilité des animaux (domestiques, cheptel) existe depuis plusieurs dizaines d'années et est bien perçue par les humains car elle contribue à la traçabilité alimentaire (ce beefsteak provient du boeuf n° xyz qui a paît dans les prairies abc, def... a été traité tel jour avec tel médicament pour telle maladie, abattu tel jour dans tel abattoir) ainsi qu'à la sécurité de leurs animaux domestiques (suivi de leur identité, du nom du propriétaire, du dossier médical grâce à des puces sous-cutanées) ou de certains animaux sauvages (ours, loups réimplantés, oiseaux migrateurs...) .

Traçabilité des objets

En RFID, on distingue cycle fermé (une palette, un chariot qui est tracé à chaque fois qu'ils ont un nouveau contenu) de cycle ouvert dans lequel l'étiquette quitte le circuit (chez les détaillants par exemple). Tant qu'il s'agit de cycle fermé : charriots, palettes... cela reste dans le monde industriel et logistique et cette traçabilité d'objets pose rarement problème. Dans les cycles ouverts, l'étiquette RFID attachée à un produit quitte le cycle industriel et logistique à la sortie du magasin de détail et peut être associée à un acheteur/utilisateur du plein gré de ce dernier ou à son insu. Jusqu'à présent la traçabilité des objets n'a pas globalement été jugée critique.

Traçabilité des humains
La traçabilité humaine -que par convention nous appellerons traçage électronique dans la suite du document- est beaucoup plus sensible et surveillée que la traçabilité des objets et des animaux et ce d'autant plus que l'on se rapproche du corps humain et de ses caractéristiques biométriques. Les pièces d'identité peuvent contenir des puces RFID dont le contenu a fait débat dans les différents pays les utilisant qui le plus souvent est redondant des données typographiées sur la pièce d'identité. Le problème actuellement identifié comme le plus sensible est l'usage de puces sous-cutanées.

La RFID est utilisée dans quelques applications sensibles en terme de vie privée mais... La RFID est déjà présente dans de nombreuses applications logistiques ainsi que dans des applications de la vie privée : les titres de transports, les passeports électroniques, les badges d'accès aux immeubles (ex : Vigik), les porte monnaies électroniques, les clés de contact des voitures... Parmi ces applications, les plus « en vue » en matière de sécurité et notamment de localisation sont : l'identité numérique et notamment les nouveaux passeports conformes aux normes OACI, les cartes de transport public de type Navigo (Paris) ou Oyster (Londres...) les badges/clefs de contrôle d'accès Vigik qui commandent l'accès de nombreux immeubles dans les villes françaises

Il n'y a pas assez de standardisation effective Il existe plusieurs milliards d'objets dotés d'étiquettes RFID et il existe des standards RFID utilisables dans tous les pays, mais ils ne représentent pas encore une part suffisante des étiquettes RFID en service. De plus, beaucoup de lecteurs ne sont pas connectés à un système de centralisation et fonctionnent de façon autonome.

2.5 Evolutions possibles du traçage électronique avec RFID

La RFID contribue donc déjà au traçage électronique mais cette contribution n'est pas encore déterminante et est moins importante que celle du GSM, des réseaux sociaux, d'Internet, des comptes en banque... mais les facteurs énoncés dans les paragraphes qui suivent pourraient changer radicalement cet état de choses.

Partant des prévisions du marché de la RFID (source cabinet Idetechex et de notre vision du marché) nous formulons les hypothèses suivantes : multiplication des étiquettes, enrichissement des informations, multiplication des lecteurs connectés, permanence des traitements et de l'archivage.

Multiplication des étiquettes Comme nous l'avons vu, à un horizon prévisible, des milliards d'étiquettes seront produites chaque année et s'ajouteront à et

communiqueront avec celles déjà en service, augmentant ainsi la probabilité que nous en possédions et/ou les portions sur nous. Dans les pays développés, chacun d'entre nous porte déjà sur lui une demi-douzaine d'étiquettes RFID (passeport, carte navigo, carte de fidélité, badges de contrôle d'accès, clefs Vigik, étiquette de vêtements...) et ce nombre devrait continuer de croître dans les prochaines années.

Multiplication des lecteurs connectés, donc de la fréquence des contrôles Le nombre de lecteurs/BTS interconnectés devrait aussi fortement augmenter. Cette augmentation sera due notamment au remplacement/évolution des lecteurs de codes-barres par des lecteurs RFID dans la logistique et la grande distribution ainsi que de l'arrivée attendue de plusieurs centaines de millions de téléphones équipés de fonction NFC (Near Field Communication) qui pourront lire les étiquettes RFID, les badges... qui seront bien évidemment connectés aux réseaux cellulaires et à Internet. Le nombre de capteurs augmentera, les étiquettes que nous portons (et donc nous) serons donc vus de plus en plus de fois par jour par des lecteurs. L'augmentation de la quantité de lecteurs et d'étiquettes et leur standardisation contribueront à la finesse de la grille de détection, l'augmentation de la précision de localisation. Les mailles du filet du traçage électronique se resserreront.

A noter aussi qu'avec l'arrivée de capteurs dans le corps humain (ingérés, implantés...), la frontière entre ce qui nous trace et nous-mêmes se déplacera.

Standardisation accrue La standardisation en RFID, et même en NFC, va bon train et il existe maintenant :

- des fréquences utilisables partout dans le monde,
- une standardisation des contenus par l'organisme international EPCGlobal qui donne un identifiant unique équivalent à un numéro de série à chaque produit individuellement (le code-barres s'arrêtait au type de produit : une bouteille d'eau gazeuse de marque X et de contenance 1litre) avec la RFID et EPCglobal on suit/trace individuellement chacune des bouteilles.

Les étiquettes évoluent, permettant l'enrichissement des informations fournies La baisse continue des prix des composants électroniques et la miniaturisation de ceux-ci permettent d'ajouter des capteurs de grandeurs physiques (lumière, température, pression...) dans les étiquettes RFID et enrichissant ainsi les informations qu'elles fournissent.

La permanence de la collecte et de l'archivage de données : « persistent surveillance » Une étiquette RFID passive est principalement composée d'une

antenne métallique et d'une puce de silicium et n'a donc pas de date de péremption qui serait due à la destruction volontaire ou non d'un de ses composants. De ce fait, la durée de vie d'une étiquette RFID peut donc être quasi-infinie. Les capteurs plus sophistiqués qu'une simple étiquette RFID sont actifs et dépendent encore souvent de l'énergie électrique pour leur alimentation. S'il s'agit de capteurs sans fil, l'énergie provient pour l'instant d'une batterie qui a une durée de vie limitée. Cependant, les progrès en cours dans la capacité du capteur à récupérer de l'énergie dans son environnement (vibrations, changement de température, lumière) permettront aux réseaux de capteurs sans fils de vivre très longtemps en autonomie énergétique. Les capteurs sans fil pourront alors assurer comme les étiquettes passives une permanence de la collecte des données. De même, par la réduction des coûts de stockage, les données générées par les applications RFID et de réseaux sans fil, peuvent être -et sont souvent- archivées sans limite de temps. Ce stockage peut excéder la durée de vie des organismes les ayant opérés ainsi que des raisons ayant présidé à leur création (un peu comme les bombes/obus enfouies depuis une précédente guerre sont encore dangereuses des décennies plus tard).

Tout ceci fait que les données permettant le traçage ont donc une durée de vie... très longue.

Absence de bouton marche/arrêt L'étiquette RFID passive s'active automatiquement lorsqu'elle passe dans le champ du lecteur, elle n'a pas de bouton marche/arrêt, ce qui fait qu'elle peut être lue (voire réécrite) à l'insu de son possesseur car ce dernier n'est pas conscient de la présence d'ondes électromagnétiques.

Atomisation des traitements et déresponsabilisation où : comment se perdre dans les nuages Les traitements pourraient de plus en plus être externalisés comme c'est le cas avec le « cloud computing » dans lequel les données et les traitements sont « quelque part » ce qui posera évidemment des problèmes de juridiction et de déresponsabilisation. Un autre phénomène pourrait aussi compliquer la situation : la capacité grandissante de calcul de chacun des milliards de capteurs à qui sera confiée une partie des traitements. Cette capacité de stockage et de calcul de chacun de ces capteurs autorise une décentralisation/atomisation des traitements. Lesquels traitements deviennent donc difficilement visibles et détectables.

La RFID pourrait permettre le traçage électronique des êtres humains en s'affranchissant de l'aspect nominatif Avec la RFID, il est déjà possible d'effectuer le filtrage des citoyens sur leur identité numérique directe ainsi qu'en fonction de leurs habitudes de consommation : alimentaires, culturelles...

Le contrôle par des organismes de type CNIL fonctionne bien face à ce genre de danger individuel/ciblé/nominatif. Néanmoins, il y a des limitations : tout d'abord géographiques, car la CNIL a des prérogatives en France seulement, ensuite car les grands génocides du vingtième siècle n'ont pas eu besoin de descendre au niveau de finesse de l'individu, il a suffi aux génocidaires de cibler :

- des classes sociales,
- des religions,
- des ethnies,
- des membres de partis ou d'associations,
- des types de maladies,
- ...

Or, avec la RFID, ce genre de ciblage ne nécessitant pas de sélection nominative est possible. La nouveauté tient dans la possibilité de filtrer en se passant de l'identité directe. La multiplication de capteurs et leur association (ce pass navigo pourtant anonyme a été contrôlé plusieurs fois en même temps que le passeport de M.X et le n° de carte bancaire xyz de M.X + le pantalon n° xyz et la chemise n° zyx) permettent de générer des sortes d'empreintes/identité numérique indirecte qui peuvent être pistées même en l'absence de cartes sans contact/pièces d'identité de monsieur X. Il est donc possible de suivre certains des objets qui nous ont été liés à un moment ou à un autre (pass Navigo anonyme +pantalon n° xyz + chemise zyx). Car, comme nous l'avons vu, chacun d'entre nous possèdera de plus en plus d'objets communicants sophistiqués (assistant personnel, « smartphone » , GPS...) ainsi que des objets simples comme des étiquettes RFID et dans quelques années des réseaux de capteurs sans fil (à domicile, dans le véhicule...). Et ce de notre plein gré ou à « l' insu de notre plein gré » .

Multiplication des objets communicants + multiplication des moyens de contrôler/lecteurs = contrôle de plus en plus fréquent et de plus en plus fin/précis. Or nous pourrions arriver à des capteurs quasi éternels par milliards qu'on ne débranche plus et qui génèrent des données permanentes utilisées on ne sait par qui ni dans quel but. La RFID rend les contrôles économiques et invisibles. On ne verra plus ce qui nous trace (multitude de capteurs, sous quelle responsabilité ? Avec quelle autonomie ?...)

D'autant que ces possibilités de contrôle ne s'appliqueraient pas seulement à quelques délinquants équipés de bracelets électroniques mais à chacun d'entre nous, qu'il ait un casier judiciaire ou pas, qu'il ait quelque chose à se reprocher ou pas, qu'il enfreigne la loi ou pas...

Voilà qui pose plusieurs questions et soulève de nombreux problèmes car la protection de la vie privée est le grand enjeu conditionnant l'avenir de la RFID et constitue -à juste titre- la perception principale des citoyens et donc la clef du développement de cette technologie.

3 Solutions appliquées à la RFID pour la protection de la vie privée

Il n'y a pas si longtemps, à la fin du vingtième siècle, Andy Warhol annonçait *"In the future, everyone will be world-famous for 15 minutes"*. En ce début de vingt-et-unième siècle, certains -comme M. Banksy- reformulent *"In the future, everyone will be anonymous for 15 minutes"*

Face au problème ci-dessus, il existe des solutions individuelles et institutionnelles mais voyons déjà comment est perçue la RFID.

3.1 La perception actuelle de la RFID et de ses applications par les citoyens est mitigée

La perception des menaces sur la liberté individuelle que pourrait représenter la RFID semble assez liée :

- à l'âge des personnes sondées : les jeunes n'ayant globalement pas de crainte (c.f. la liberté avec laquelle ils remplissent leurs profils et narrent leurs activité sur les réseaux sociaux)
- du niveau de la démocratie dans le pays (les citoyens de pays démocratiques ne sont pas méfiants ni vis-à-vis de l'état ni encore moins vis-à-vis des entreprises à qui ils confient leurs données)

Il existe une perception globalement positive de la RFID Il existe des applications RFID déployant des étiquettes à plusieurs millions d'exemplaires (clefs Vigik, pass Navigo, Velib...) sans dysfonctionnement majeur, pour lesquelles : l'équation économique semble satisfaite et l'acceptabilité sociale semble acquise car il n'y a pas de réaction de rejet, plutôt une indifférence positive. Les citoyens apprécient les aspects positifs (notamment l'aspect pratique) et minimisent l'atteinte à la vie privée. Les avantages des applications RFID étant perçus comme plus concrets que les risques (vus eux comme virtuels) car en la matière il semble bien que la sécurité prime sur la liberté. Dans le monde futur de l'Internet des objets, protéger sa vie privée pourrait ainsi devenir un « sacrifice »

- Financier (exemple : surcoût pour obtenir un Pass Navigo anonyme, surcoût des communications cellulaires par cartes prépayées).
- En terme de confort et de facilité de la vie quotidienne (désormais qui se passerait de :
  - son GSM ?
  - tirer de l'argent au distributeur ?
  - son GPS en voiture ? En bateau ?

  Combien de franciliens ont demandé l'abonnement Navigo anonyme ?)

Notons que le fait qu'une grande partie des citoyens ne voient pas le problème que pose certaines atteintes à leur vie privée est en soi un problème voire... le problème.

Mais pour certains, il existe une perception très négative de la RFID
La RFID est souvent assimilée aux nanotechnologies et « diabolisée » par certains au même titre. On trouve ainsi des groupes d'opposants aux RFID :

- Pièces et main d'oeuvre
- Halte aux puces (France)
- Oblomoff (Oblomov)
- Caspian (US)
- Electronic Frontier Foundation (US)

Certains s'insurgent contre les possibilités accrues de surveillance, d'autres comme David Brin répondent à la vieille question de Juvénal « sed quis custodiet ipsos custodes ? » (qui surveillera les surveillants) en filmant avec téléphones portables et caméscopes les forces de police lors de leurs interventions et prônent une « sousveillance » comme moyen de lutte contre la surveillance policière. Ce concept est intéressant, mais si l'opposition magnétoscope/vidéo sur téléphone contre CCTV a un sens, quel serait son équivalent pour la RFID ?

Du fait de leur assimilation de la RFID aux nanotechnologies, certains des groupes ci-dessus risquent une exagération des dangers.

Or il n'est pas envisageable de :

- Lâcher dans la nature des objets/systèmes liberticides... surtout à des milliards d'exemplaires
- Condamner l'industrie entière de la RFID qui « pèse » déjà plusieurs milliards d'euro par un et cela sera encore plus avec l'Ubimedia et l'Internet des objets.
- Renoncer aux bienfaits potentiels de la RFID (malades d'Alzheimer, traçabilité alimentaire, sécurité des pièces d'identité...)
- Bloquer tous les secteurs bénéficiant de la RFID qui s'est déjà répandue dans toute l'industrie et une bonne partie de la société : logistique, transport...

3.2 Solutions institutionnelles

France

CNIL

La Commission nationale de l'informatique et des libertés (CNIL) est une institution indépendante chargée de veiller au respect de l'identité humaine, de la vie privée et des libertés dans un monde numérique. La CNIL s'intéresse particulièrement aux données suivantes : nominatives et biométriques ainsi qu'à la

finalité du recueil, des traitements et du stockage et à la proportionnalité. La CNIL rappelle que « le développement de ces technologies doit nécessairement s'accompagner d'une prise en compte des principes clés de la protection des données, à savoir les principes de finalité, de proportionnalité, de transparence et de sécurité » . Cette technologie soulève de nouvelles problématiques en matière de protection des données personnelles au premier rang desquelles figure leur invisibilité ou quasi-invisibilité. Comment garantir le respect de la loi en présence de technologies invisibles ?

Revenons à trois des points considérés essentiels par la CNIL :

- Données nominatives : mais nous avons vu plus-haut que les réseaux de capteurs n'ont pas besoin de données nominatives pour nuire aux individus porteurs d'étiquettes RFID ou de capteurs sans fil
- Données biométriques : idem
- Finalité : la finalité peut être inconnue du capteur et de celui qui l'opère et/ou avoir changé depuis l'origine. D'ailleurs, être confronté à un réseau de capteurs et plus globalement à l'Ubimedia/Internet des objets n'est pas forcément en être utilisateur. On comprend aisément qu'être détecté par un capteur infrarouge/capteur de mouvement ne signifie pas en être l'utilisateur. De même, lorsque votre passeport est détecté, ce n'est probablement pas vous qui êtes l'utilisateur/usager/bénéficiaire du système qui le « lit » , mais un service de police, un aéroport, une compagnie aérienne...

ANSSI

Les attaques informatiques/cybernétiques contre un état prennent deux formes :

- directe qui paralyse les Systèmes d'information et de Commandement (SIC) et les propres moyens de l'état,
- indirecte par manipulation des messages

De plus en plus souvent, l'état doit aussi prévenir les attaques sur le secteur privé qui, opérant 90

Union Européenne

Le principe de protection choisi par la commission européenne est la transparence des traitements ; les personnes informées doivent pouvoir :

- accepter,
- modifier

les données les concernant et la finalité doit être :

- légitime,
- explicite,
- connue.

Solutions préconisées par l'industrie

L'industrie de la RFID puis des M2M (machine 2 machine) est intéressée à

la résolution des problèmes liés à la vie privée car elle rencontrera un point de blocage si les étiquettes sont vues comme liberticides et de ce fait boycottées. Une information claire et précise des consommateurs sur l'usage des étiquettes, sur les traitements effectués ainsi que sur les moyens mis à leur disposition pour lire le contenu de la puce et vérifier si elle est ou non active devrait être disponible. La désactivation des étiquettes par choix du client « opt-in, opt-out » en sortie de magasin est envisagée mais un dispositif passif comme une étiquette ne peut pas être muni d'un bouton « marche-arrêt » contrairement à la volonté du législateur.

3.3 Bilan sur les solutions actuelles

La plupart des protections imaginées ci-dessus n'existe pas encore ; face à l'ampleur prévisible du problème, les autres sont inadaptées, inefficaces, pas applicables.... La riposte semble incomplète ou inadaptée, car accepter, modifier les données les concernant est faisable face à un être humain à un guichet mais le faire face à un détecteur infra rouge ou un portique de supermarché peut vite ressembler au sketch de Marc Jolivet où un homme essaie de négocier face à un Digicode.

4 Propositions

4.1 La vérité est ailleurs !

Comme nous venons de le voir, les bonnes solutions passeront par une prise de conscience individuelle relayée par un travail du législateur et une réflexion commune des parties prenantes (industriels, autorités, usagers...). Néanmoins, en attendant ces solutions qui dépassent les ambitions et les moyens de l'auteur, nous évoquons ci-dessous quelques pistes techniques.

Evangélisme sans angélisme
En parallèle aux réponses institutionnelles tant au niveau français qu'européen, une des réponses est la formation, l'éducation/information, qui permettra :

- d'isoler les vrais problèmes et de les redimensionner entre les deux extrêmes de ceux qui ne voient de problème et de ceux qui en voient des milliards
- mettre en place les outils pour (r)établir la confiance dans les RFID

4.2 Les pistes issues de la guerre électronique

Parce que la RFID est un champ d'application de toutes les composantes de la guerre électronique, on peut y retrouver la plupart des fonctions suivantes :

Ecoute/interception La fonction d'écoute peut s'appliquer en plusieurs parties de la chaîne : - L'exemple qui semble le plus prometteur en la matière est l'infrastructure mise en place par EPCglobal ; en consultant la hiérarchie de l'ONS il est possible de savoir à distance où et quand a été contrôlé telle étiquette et de la suivre. l'ONS est évidemment intéressant car étant en haut de la pyramide il permet de voir passer nombre d'informations intéressantes.

- surtout intéressante dans la liaison entre les étiquettes et le lecteur, la portée peut être grandement améliorée par l'usage de récepteurs de guerre électronique qui ayant une meilleure sensibilité peuvent écouter les communications à plus grande distance que les étiquettes et les lecteurs. Certaines cartes sans contact de type C sont aujourd'hui « protégées » contre l'écoute de par leur authentification active.

L'expérience de la guerre électronique pourrait bénéficier à la réalisation de stations de base multifréquences multi protocoles ainsi qu'à des petits systèmes détectant les lectures illicites des étiquettes RFID.

Goniométrie/localisation/traçage Avec l'augmentation du nombre de lecteurs pouvant lire au moins une des étiquettes présentes sur une personne donnée, la localisation gagne en précision et en nombre d'occurrences. En étendant ces recherches, il doit être possible pour une société d'exercer une surveillance permanente sur ses concurrents : leurs achats, leurs fournisseurs, leurs circuits de distribution, la localisation de leurs clients, leurs problèmes de SAV...

La localisation de badges existe déjà notamment

- dans les parcs d'attraction pour permettre aux membres d'une même famille de ne pas se perdre.
- pour localiser les forces de sécurité/pompiers dans une zone d'intervention dans l'obscurité, les flammes, la fumée...
- Dans des hôpitaux, pour localiser le mobilier, l'appareillage... les patients et les soignants.

Les techniques actuelles permettent une précision de quelques mètres pour des badges actifs détectables à plusieurs centaines de mètres. Ces outils de localisation gagneraient à être enrichis pas les algorithmes de la guerre électronique.

Brouillage/anti-brouillage destruction /Saturation/Déni de service/Intrusion Brouillage, anti-brouillage, ECM (electronic counter measures), ECCM (electronic counter counter measures), ECCCM... sont des composantes bien connues de la guerre électronique. Le brouillage est d'autant plus intéressant en RFID que lorsqu'un lecteur dialogue avec des étiquettes, elles répondent toutes sur la même fréquence et de ce fait, des algorithmes dits d'anti-collision ont dû être développés et sont appliqués. L'expertise de la guerre électronique en anti-brouillage serait ici aussi très bénéfique.

Pour protéger la vie privée contre des détections abusives, il pourrait être intéressant de développer l'équivalent des « yes card » des étiquettes qui répondent toujours présent à une demande d'identification quel que soit le numéro d'étiquette demandé par le lecteur et qui donc vont désinformer le lecteur. La saturation des lecteurs est aussi possible en passant des rouleaux de plusieurs centaines d'étiquettes (volume d'un verre à moutarde) sous le lecteur. L'intrusion a aussi été envisagée par certains groupes « d'hacktivistes » sur internet mais elle suppose que les étiquettes ne transmettent plus seulement des identifiants mais des ordres exécutables, ce qui n'est pas souvent le cas.

Equivalent d'un débranchement électrique du réseau (Impulsion électromagnétique (IEM) spécialisée ?) Les réseaux actuels peuvent être désactivés lorsque l'on débranche leur alimentation électrique. Les réseaux futurs seront pour partie indépendants des sources de courant électrique car ils seront autonomes et sans fil. Il faudrait envisager sur les réseaux sans fil et la RFID une action similaire au débranchement électrique. Une piste pourrait être l'impulsion électron magnétique. Lors des premières expérimentations nucléaires aux Etats-Unis les effets IEM ont été détectés et remarqués par leur capacité à détruire les appareillages électriques et électroniques. Des émetteurs de micro-onde de forte puissance pourraient être miniaturisés pour générer ces effets. Sur Internet certains conseillent de passer les étiquettes au four à micro-ondes pour les annihiler.

Une autre solution consisterait à concevoir une fréquence/forme d'onde/clef prévue d'origine pour désactiver certains réseaux, certaines étiquettes.

Avec par exemple des feuilles d'aluminium, il est assez facile de réaliser une cage de Faraday (de type portefeuille blindé) permettant ainsi de protéger contre des lectures intempestives/abusives les pièces d'identité contenant des RFID.

« Man in the middle » Des attaques de type relai ou "man in the middle" sont assez prisées pour attaquer les contrôles d'accès RFID et elles sont assez difficiles à déjouer. Les premières générations de cartes sans contact Mifare en ont fait les frais.

Bulle de protection Certains citoyens revendiqueront probablement qu'aucune émission n'émane d'eux ni qu'ils en reçoivent par les lecteurs. Ce qui est conforme à l'inquiétude vis-à-vis des radiofréquences surtout développée contre les réseaux de téléphonie cellulaire. Il faudrait analyser comment réaliser une « bulle de protection » individuelle ; par exemple : détection multi fréquences multi protocoles, alarme en cas de lecture, réponse pertinente si lecture autorisée, brouillage et/ou déni de service sinon.

4.3 Les pistes issues de la cryptologie et de la sécurité des systèmes d'information

Changement de paradigme La sécurité des systèmes des systèmes d'information est confrontée habituellement à la protection des infrastructures critiques (publiques, réseaux vitaux...) contre des pannes et des attaques. Cette logique peut encore s'appliquer à la protection de la chaîne RFID qui contribue de plus en plus à la chaîne logistique qui est devenue une infrastructure sensible. Il est évidemment important de savoir comment protéger des :

- étiquettes
- BTS
- infrastructure RFID qui contribue à la logistique.

Cas particulier de l'Object Name Server (O.N.S.) : l'Object Name Server est l'équivalent du Domain Name Server (DNS) de l'Internet actuel et, à ce titre, a les mêmes caractéristiques et présente donc des vulnérabilités similaires. L'ONS est contrôlé par les Etats-Unis mais il y a des velléités européennes et chinoises d'échapper à ce contrôle ou de le partager et notamment de savoir qui gère les clefs racines. Nous ne nous y intéresserons pas ici, bien que le sujet soit passionnant, car des solutions similaires à celles déjà appliquées pour le DNS devraient suffire.

Mais la nouveauté est ailleurs et la sécurité des systèmes d'information pourrait, du fait de la RFID, connaître un changement de paradigme.

Face aux risques liés aux réseaux de capteurs et à leur précurseur la RFID, le problème deviendrait : comment protéger chacun de nous de l'inquisition de réseaux qui ne mourraient jamais et dont on ne connaîtrait ni la finalité ni les bénéficiaires.

Le but de ce document, est de susciter l'intérêt de spécialistes de la sécurité des systèmes d'information et de la guerre électronique afin qu'ils trouvent des solutions à cette problématique de protection non plus seulement des SIC et autres C4ISR étatiques et de l'infrastructure critique mais de l'individu et de ses libertés individuelles. A cette fin, quelques pistes sont ébauchées ci-dessous.

Chiffrement En RFID comme ailleurs, la cryptographie contribue à protéger la confidentialité des communications.

Authentification forte (déploiement d'Infrastructure de Gestion des Clefs (IGC)) Une authentification mutuelle (basée sur une IGC) ferait qu'une étiquette n'accepterait d'être lue que par un lecteur autorisé qui relèverait de la même IGC que lui et dont il pourrait identifier la clef/signature. Cette authentification mutuelle requiert encore actuellement trop de transistors sur le circuit intégré et n'est pas encore compatible avec les prix de revient des étiquettes, mais la baisse des coûts du silicium devrait permettre d'intégrer ces fonctions à prix

raisonnable dans des étiquettes RFID (en suivant ce qui a été fait sur les cartes à puce) à assez court terme.

« Kill bit » (détruire certaines étiquettes) Sur l'inspiration de la carte à puce, il existe plusieurs schémas de destruction des étiquettes :

- Physiquement en en arrachant une partie, la rendant inopérante
- Logiquement en envoyant un « bit tueur » prédéfini qui va désactiver l'étiquette. Ce qui est notamment utile en « opt-in » « opt-out » à la sortie des magasins.
- Le « kill bit » ne serait protégé que par un mot de 32 bits, or tant que la lecture ne peut être détectée par le possesseur, le lecteur frauduleux peut tester les 2 puissance 32 possibilités.
- En allant au-delà, serait-il aussi possible de construire des étiquettes pour que leur durée de vie soit limitée d'origine ?

Duplication /Les identités masquées/pseudonymes/noms d'emprunt/Anonymisation/Usurpation d'identité /leurrage Il pourrait être intéressant de se raccrocher à des infrastructures pseudonymisantes Il devrait aussi être possible de rester au niveau de précision des codes-barres en masquant les derniers bits ne permettant ainsi pas d'aller jusqu'au numéro de série.

5 Conclusion

Les avantages de la RFID et de ses successeurs sont énormes à la fois pour l'individu et pour la société, les enjeux et les dangers le sont aussi. Sera-t-il possible de résister à la tentation d'utiliser une technologie comme la RFID parce qu'elle est disponible ?

Pourtant, sans défense des libertés individuelles, sans préservation de la vie privée, la RFID et ses technologies dérivées, pour innovantes qu'elles soient, et parce qu'elles repoussent sans cesse les limites, doivent être interrogées. Il nous faut réfléchir, former, informer, expérimenter, discuter collectivement sur les façons d'implémenter ce nouvel outil et donner plus de moyens aux organismes chargés de ces réflexions et peut-être aussi explorer les pistes ébauchées dans le présent document du côté de la guerre électronique et de la sécurité des systèmes d'information. Car, comme le dit M. Alberganti : « demain nous vivrons dans un nouveau monde, si nous ne voulons pas y être traités comme les objets qui nous entourent, il est urgent d'en fixer les règles. »

Cyber défense des SI vitaux : quel partenariat public-privé ?

Marie Barel, Arnaud Garrigues

Orange Business Services, Orange Consulting, 114 rue Marcadet 75018 PARIS
marie.barel(@)orange-ftgroup.com, arnaud.garrigues(@)orange-ftgroup.com

Résumé Dans le cadre de la cyberdéfense, la porosité entre le monde virtuel et le monde réel est tangible et fait craindre la réalisation de scénarios catastrophes mettant en jeu des pans entiers de notre économie nationale. Or, chacun des acteurs en présence ne peut s'occuper seul de la sécurité des systèmes d'information compris dans le champ de l'écosystème virtuel formé de l'ensemble des « systèmes d'importance vitale ». L'interdépendance des systèmes, qui supportent également souvent les mêmes vulnérabilités liées aux produits et équipements dont ils sont constitués, suppose en conséquence une coopération étroite des différents partenaires publics et privés. A cela doit s'ajouter la coopération extérieure et à terme une gouvernance de l'Internet désormais considérée comme une « infrastructure critique », adaptée aux évolutions. Un changement de vision doit donc s'opérer pour permettre de dépasser des stratégies de sécurité encore très largement « auto centrées » et entrer dans une approche de la sécurité de « tous par tous ».

Mots-clés: systèmes d'importance vitale - partenariat des secteurs public/privé - exemples étrangers (US, UK, GER) - dispositif et cadre juridique français - coopération supranationale - gouvernance de l'Internet

Avertissement : le présent article reflète simplement l'opinion de leurs auteurs et ne représente pas une analyse ou des positions officielles d'Orange, France Telecom ou de l'une quelconque de ses filiales.

1 Introduction

La possibilité d'une cyberattaque sophistiquée contre une infrastructure vitale, scenario largement exploité tant dans le domaine de la littérature [1] que par le

1. Comme le rappelle le dossier spécial de la revue Courrier International consacré à la Cyberguerre [1], *« le thème de la cyberguerre inspire. Plusieurs ouvrages, essais ou fictions, sont parus ces dernières années sur le sujet. Guy-Philippe Goldstein, Babel minute zéro, éd. Denoël. Un roman très documenté qui décrit comment la propagation d'un virus informatique à l'échelle mondiale peut conduire la planète au bord d'une guerre nucléaire totale. »* Voir aussi l'ouvrage *CyberWar* [éd. Ecco, 2010, inédit en français] par Richard Clarke, ancien coordinateur de la Maison-Blanche pour le contre-terrorisme et la cybersécurité, estimant qu'une gigantesque panne pourrait paralyser la planète en moins d'un quart d'heure. Dans son scénario, les virus informatiques s'attaquent aux systèmes de courrier électronique militaires ; les raffineries de pétrole et les oléoducs explosent ; les systèmes de contrôle aérien s'effondrent ; les données financières sont brouillées. La société se trouve alors totalement désorganisée et la nourriture vient à manquer.

cinéma [2], ressort bien aujourd'hui de la réalité La revue *The Economist* dans son numéro du 3 juillet 2010 [1] fait même remonter la chronologie de ce *« nouveau risque mondial »* à l'explosion d'un gazoduc soviétique qui était intervenue en juin 1982 (en plein coeur de la guerre froide) et avait abouti, selon les propos de Thomas Reed - ancien directeur de l'armée de l'air américaine - à *« l'explosion et l'incendie non nucléaires les plus gigantesques que l'on ait jamais pu voir depuis l'espace »*. L'accident était dû à une défaillance du système de contrôle informatisé que des espions soviétiques avaient subtilisé à une entreprise canadienne mais dont ils ignoraient que la CIA avait bidouillé le logiciel pour qu'il *« se détraque au bout d'un certain moment »*. C'était alors, comme le conclut l'article, l'une des premières démonstrations de la puissance de ce qu'on appelle une *« bombe logique »*.

Les dommages liés aux cyberattaques qui, comme le montrent les cas d'attaques menés ou, du moins, attribués à la Chine depuis 10 ans [2], utilisent des codes malicieux et recourent aux dernières techniques de *social engineering* pour cibler via les réseaux sociaux des personnes précises, s'expliquent plus particulièrement par la pervasivité et l'interconnexion croissantes des systèmes d'information et les effets de systémique (ou effets domino) que celles-ci impliquent. L'exemple (plus récent) du ver Stuxnet est à cet égard édifiant [3] : il constitue une première tentative d'agression sur un système informatique industriel. Malgré de très nombreuses suppositions parfois hasardeuses, l'analyse stricte du code révèle bel et bien l'exploitation concomitante de failles sur un système bureautique classique (Microsoft Windows) ainsi que sur des applications industrielles développées par un autre constructeur [4]. A ce jour, le ver ne semble pas avoir produit de quelconques dégâts, hormis les perturbations liée à sa réplication, mais il semble toutefois faire entrer dans une forme de réalité des menaces envers les OIV jusque là moins tangibles.

L'objet de cet article ne sera pas d'aborder les nombreuses et importantes questions que cette introduction a pu déjà insuffler dans l'esprit de ses lecteurs : comment déterminer un acte de cyberguerre ? Comment localiser les points primaires d'une cyberattaque et en identifier les auteurs ? Quelles règles d'engagement pour les actes de riposte ? ... Il sera plus spécifiquement d'étudier le partenariat public-privé qui constitue l'un des facteurs clés d'une cyberdéfense opérationnelle et résiliente contre les cyberattaques menées à l'échelle des nations (voire au-delà) et de leurs intérêts fondamentaux. En effet, face à la menace cybernétique, les États comme les organisations d'importance vitale ayant la responsabilité d'infrastructures critiques, n'ont pas la capacité de répondre de façon autonome et unilatérale et les politiques en matière de cyberdéfense admettent

2. Notamment « Die Hard IV » pour ne citer que cet exemple.
3. `http://www.wired.com/threatlevel/2010/10/stuxnet-deconstructed/`
4. `http://www.schneier.com/blog/archives/2010/10/stuxnet.html`

aujourd'hui communément qu'une synergie doit être recherchée entre les secteurs public et privé.

Cette synergie, au-delà d'un levier d'efficacité, devient une condition sine qua non, de la réussite du dispositif pour deux raisons essentielles : la dépendance des organisations (étatiques ou pas) aux systèmes d'informations sur lesquels reposent leurs activités d'une part et la posture agressive adoptée par nombre d'entre elles d'autre part. La solution à cette nouvelle équation qui pousse ainsi la plupart des Etats du monde à adopter une détection et une gestion plus proactive des attaques menées par le biais de l'Internet, lui-même considéré comme un « actif stratégique national » pour les Etats-Unis ou bien encore une « infrastructure vitale » [3] en France, consiste en particulier dans le développement de nouvelles coopérations public-privé.

Nous nous interrogerons donc tout de long de cet article sur les formes de ce partenariat, son efficacité et les orientations à prendre ou les efforts à poursuivre dans ce domaine ...

2 Exemples étrangers en matière de coopération public-privé

Parmi les exemples étrangers de partenariat public-privé et de modèle d'organisation en matière de protection des systèmes d'importance vitale, la Grande-Bretagne, l'Allemagne et les États-Unis figurent parmi les plus avancés. Sans préjuger ici d'un quelconque retard de la France en la matière, c'est une synthèse des dispositifs en vigueur dans ces trois États qui est proposée en premier lieu pour approfondir le sujet de cet article.

2.1 Grande-Bretagne

Au Royaume-Uni, le CPNI (*Centre for the Protection of National Infrastructure*[5]) - ex-NISCC, rattaché au *Home Office* - est l'organisme chargé de coordonner la protection des infrastructures nationales critiques contre les attaques électroniques [4]. Parmi les actions fortes développées sous l'impulsion du CPNI, on peut citer en particulier la **mise en place d'une plateforme d'échange, d'analyse et de diffusion de l'information autour des vulnérabilités des infrastructures vitales**[6]. De même, un **protocole d'accord** a également été formalisé **avec les éditeurs de produits sur le partage d'informations sur les vulnérabilités** articulé autour de neuf principes, dont l'objectif principal est de garantir la confidentialité absolue des informations transmises par le biais du CPNI.

5. Site officiel : `http://www.cpni.gov.uk/ProtectingYourAssets/informationSharing.aspx`
6. Lien profond : `http://www.cpni.gov.uk/ProtectingYourAssets/informationSharing.aspx`

Pour remplir sa mission d'information, de sensibilisation et d'alerte, le CPNI s'appuie ainsi sur différentes entités :

- l'UNIRAS [7] (CSIRT gouvernemental) : pour fournir aux opérateurs des infrastructures critiques des avis techniques, des informations sur les menaces, les vulnérabilités et les niveaux d'alerte ;
- des WARPs (*Warning, Advice and Reporting Points*) [5] : pour recueillir des alertes, fournir des conseils de sécurité et signaler des incidents (mais sans capacité d'intervention) ; à la différence des CERTs, les WARPs travaillent avec des communautés réduites et sur une base personnelle, ce qui permet d'établir des échanges de proximité avec ses membres et renforce l'efficacité des communications réalisées en adressant des sous réseaux et des organisations plus difficiles à atteindre pour les CERTs ;
- des ISACs (*Information Sharing & Analysis Centre*) : pour la diffusion des informations d'alerte et d'incident au sein d'une communauté donnée d'utilisateurs, généralement sur une base commerciale.

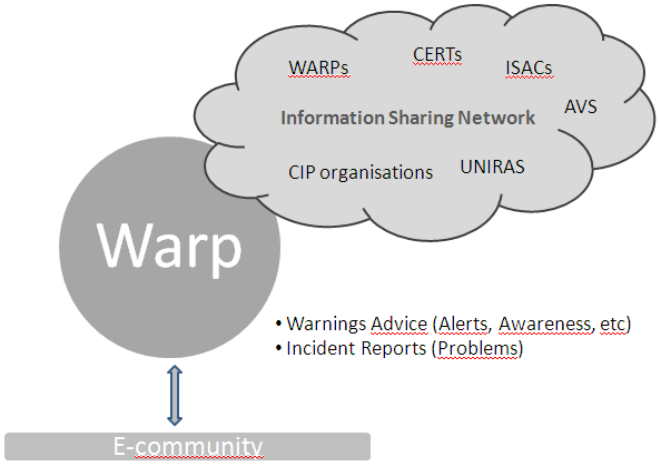


Figure 1. Vision du partage d'informations (*« Warp diagram »*), source :`http://www.warp.gov.uk/downloads/WARPs.pdf`

Plus récemment, le Royaume-Uni a mis en place plusieurs initiatives visant à renforcer la surveillance et la sécurité informatique des instances gouvernementales.

D'un point de vue doctrinal d'abord avec la **publication en 2009 de la « *Cyber Security Strategy* »** [6] qui reconnaît l'importance de la problématique de la sécurité informatique. Ensuite, au-delà de la doctrine de sécurité nationale

7. Site officiel : `www.uniras.gov.uk`

qui fait d'Internet un bien d'importance vitale, cette stratégie se focalise sur la sécurité des systèmes d'informations critiques et/ou vitaux. Elle met ainsi en avant l'importance du partenariat public-privé et met en place deux nouvelles organisations [7] :

- OSC (Office of Cyber Security) : son objectif est d'assurer la coordination et la persistance des politiques et stratégique de sécurité informatique au sein du gouvernement notamment ;
- CSOC (Cyber Security Operations Center) : son activité se rapproche plus de celle d'un CERT, tout en dépassant la seule analyse de machines compromises.. Il s'agit en outre de surveiller, « monitorer » , à la fois les activités sur le web dans le cyberespace susceptibles de porter atteintes aux actifs gouvernementaux mais également de surveiller les attaques et de traiter les alertes. On retiendra incidemment que le CSOC est hébergé dans les locaux du GCHQ britannique (UK Government Communications Headquarters) [8], une des agences britanniques de renseignement spécialisées dans les communications (satellites. . .) et plus généralement le SIGINT - Signal Intelligence. A noter également que lors de l'annonce de la création de ce centre, les britanniques ont affirmé être en mesure de conduire des actions offensives.

2.2 Allemagne

L'Allemagne a adopté dès juillet 2004 un *Plan national pour la protection des infrastructures d'information (NPSI)*[9] - remis à jour en 2009 [8] - qui s'appuie notamment sur l'homologue de l'ANSSI, le BSI (*Bundesamt für Sicherheit in der Informationstechnik* - office fédéral allemand pour la sécurité des informations).

Le BSI, qui exerce ses missions auprès des utilisateurs quels qu'ils soient (administration, entreprises, citoyens) et des fabricants de technologies de l'information, fournit en particulier, dans le cadre d'un partenariat très fort avec le privé, des conseils et des supports techniques.

Ainsi, parmi les réalisations du BSI, on peut citer, grâce à des efforts combinés avec les secteur privé des affaires, de l'industrie (Siemens, Daimler, Volkswagen, . . .), les associations professionnelles et la communauté académique, la publication de plusieurs **guides, documents de recommandations et instructions pratiques portant en particulier sur la protection des infrastructures critiques** (CIP, Critical Infrastructure Protection). Considérés à ce jour par les

8. http://www.gchq.gov.uk/press/csoc_newsitem.html

9. Document publié en 2005 : http://www.en.bmi.bund.de/cln_028/nn_148138/Internet/Content/Common/Anlagen/Nachrichten/Pressemitteilungen/2005/08/National__Plan__for__Information__Infrastructure__Protection,templateId=raw,property=publicationFile.pdf/National_Plan_for_Information_Infrastructure_Protection.pdf

entreprises et le gouvernement comme de véritables standards professionnels régulièrement remis à jour, les documents : « CIP - Baseline Protection Concept » (2006) [10] et « CIP - Risk and Crisis Management » [11] (2008), représentant à cet égard le socle des bonnes pratiques qui permettent de sécuriser des systèmes d'information vitaux et d'en gérer les risques.

Se poursuivent également des **exercices réguliers, à la fois sectoriels et transverses**, impliquant un panel renouvelé de participants issus des secteurs public/privé et permettant en particulier d'affiner les processus de communication et d'échange applicables pour la détection précoce des cyberattaques ou bien encore la gestion de crise. Ces processus de communication reposent en particulier sur le concept de SPOC (*Single Point of Contact*) [12] mis en place pour chaque secteur d'activité critique identifié, et constituant l'interface unique avec le Centre de Situation du BSI.

Enfin, le **Plan d'Implémentation du Plan national pour la Protection des Infrastructures Critiques** (*CIP Implementation Plan*) [13] publié en septembre 2007 a défini parmi les quatre principales actions à mener :

- des efforts en matière de sensibilisation et de formation des responsables et des personnels, de nature à favoriser la pérennité sur le long terme des mesures déjà entreprises ;
- le renforcement de la coopération extérieure, d'abord européenne et ensuite internationale, tendant en premier lieu à mettre en place une plateforme de discussion commune pour l'échange d'information et la création de structures supranationales.

2.3 Etats-Unis

Dès 1995, les experts américains ont envisagé un scenario de guerre informatique totale, connue alors sous le nom de « Pearl Harbor électronique » (et, de manière plus actuelle, de « 11 Septembre numérique »). Dans ce scenario catastrophe utilisant l'ensemble conjugué des infrastructures critiques pour créer le chaos, le succès de l'attaque résulte de la paralysie de la capacité de réaction et de riposte du défenseur. Récemment encore, la conférence « Defcon » 2010 voyait l'un de ses intervenants présenter un tel scénario avec une grande assu-

10. Document à télécharger sur le site du Ministère de l'Intérieur (BMI) : `http://www.bmi.bund.de/cae/servlet/contentblob/121746/publicationFile/13129/Basisschutzkonzept_kritische_Infrastrukturen_en.pdf`

11. Document à télécharger sur le site du Ministère de l'Intérieur (BMI) : `http://www.bmi.bund.de/cae/servlet/contentblob/131086/publicationFile/13133/Leitfaden_Schutz_kritischer_Infrastrukturen_en.pdf`

12. Présentation du Dr Mickael Pilgerman, réunion des experts CIP EU-US (Madrid, 2010) : `http://infrastructure-protection.net/files/docs/01-national/08-DE.ppt`

13. Document à télécharger sur le site du Ministère de l'Intérieur (BMI) : `http://www.bmi.bund.de/cae/servlet/contentblob/994784/publicationFile/63256/kritis.pdf`

rance ; ainsi, Charlie Miller [14], un ancien membre de la NSA, estime qu'avec 100 millions de dollars, deux ans de travail et une cyber armée composée d'une centaine d'hommes, il serait possible de mener une cyberattaque généralisée contre les Etats-Unis, en ciblant en particulier les réseaux de distribution d'électricité, les banques et les télécommunications [15].

Se montrant lui-même très conscient à la fois des potentialités et du niveau de dangerosité de l'Internet, le Président Obama a lancé dès son arrivée une profonde remise en cause du système de « cybersécurité » . Un audit établissant une liste de défaillances et d'objectifs a ainsi immédiatement été conduit par Mme Mélissa Hathaway, ancienne responsable cybersécurité au sein de la Maison Blanche.

Fait remarquable, l'approche du Président Obama est très globale et prend en compte l'ensemble des problématiques de la sécurité des systèmes d'information, que ceux-ci relèvent de systèmes « industriel » ou « de gestion » ou encore, appartiennent à des particuliers. Par ailleurs, les Etats-Unis ont affirmé à plusieurs reprises que l'infrastructure de télécommunications, **au sein duquel l'Internet est assimilé**, est sans aucun doute une infrastructure critique ou vitale. Cet aspect explique notamment l'activisme américain au niveau de la Gouvernance de l'Internet (voir sur point la section 4.2) mais également le fait que certaines organisations s'attachent à préserver l'*« information infrastructure »*.

Cette approche doctrinale américaine, dans laquelle la surprise stratégique est réellement problématique, est également une des causes de cette vision très globale qui sous-tend la « cybersécurité » . Or, si les Etats-Unis excellent à publier nombre de documents, la complexité de l'organisation et la masse de l'information rendent parfois délicate la compréhension du sujet. Une autre cause est une forme de perte de contrôle sur les infrastructures vitales nationales : à cet égard, **le GAO [16] estime qu'environ 85% de ces infrastructures sont actuellement gérées par le secteur privé** [17]. Cet article tente donc d'apporter une vision plus claire et précise de la situation aux Etats-Unis en répondant à trois questions :

- Quelles sont les organisations impliquées dans les questions de sécurité informatique des infrastructures vitales ?
- Quelles sont les problématiques auxquelles sont confrontées les Etats-Unis ?
- Quelles sont les leçons à tirer d'une expérience réelle de partenariat public-privé illustrée par le cas « Conficker » ?

14. https://www.defcon.org/html/defcon-18/dc-18-speakers.html#Miller
15. http://www.20minutes.fr/article/587011/High-Tech-Un-specialiste-affirme-etre-capable-d-envahir-l-Internet-americain.php
16. L'équivalent, en bien plus proactif, de notre « Cour des Comptes ».
17. Cybersecurity for Critical Infrastructure Protection - http://www.gao.gov/docsearch/repandtest.html

2.4 Descriptif des organisations impliquées dans la protection des infrastructures critiques américaines

Un des problèmes récurrents de l'administration américaine, notamment au niveau fédéral, est son manque de lisibilité et son entropie. Depuis les attentats du 11 Septembre 2001 puis la « guerre contre le terrorisme » , la multiplication des agences et l'augmentation des budgets attribués à la sécurité a créé une nébuleuse complexe. Parmi ces agences et autres bureaux, un grand nombre traitent de la cybersécurité. La lecture de nombreux documents a permis de dresser une liste, certainement non-exhaustive mais assez complète, de celles qui traitent des infrastructures critiques.

Pour plus de lisibilité, ces entités ont été regroupées en 4 catégories :

a. Celles relevant directement de l'autorité de la Maison Blanche et du Président

b. Celles relevant du domaine militaire ;

c. Celles relevant de la sécurité intérieure, et notamment du *Department of Homeland Security* (DHS), créé en 2002 ;

d. Une catégorie plus générique contenant les organismes de recherche ou les agences très spécifiques.

Comme nous pouvons le voir sur l'organigramme (figure 2), il existe pléthore d'organisations de nature diverse et variée impliquées directement ou non dans la question des infrastructures. Notons que la création du *Department of Homeland Security* (DHS) en 2002 a bouleversé le paysage de la sécurité. Encore aujourd'hui, le périmètre des responsabilités de ce « ministère » ne cesse de s'agrandir.

Plus généralement, nous pouvons estimer que les principales responsabilités sont partagées de la façon suivante :

a. Autour du Président s'agrègent plusieurs acteurs. Parmi ceux-ci, les conseils nationaux de sécurité (insérer : acronyme ou *désignation en anglais*) et économique (insérer : acronyme ou *désignation en anglais*) peuvent avoir un rôle important, notamment en ce qui concerne le premier. Le « CYBERCZAR » , Howard Schmidt, nommé le 21 décembre 2009, est une fonction spécialement créée par le Président. Il participe aux deux conseils susnommés. La prégnance de la question de la protection des infrastructures vitales est telle que le Président lui-même, ou son entourage, ont un rôle fort de coordination et d'impulsion comme peut le montrer leur position dans l'organigramme ci-dessus.

b. Les organisations de nature militaire ont plus particulièrement une fonction de protection des réseaux militaires. C'est ce qui ressort de l'audition du Général Alexander, commandant de la NSA et désormais également commandant du CYBER COMMAND. Chaque composant spécifique des forces

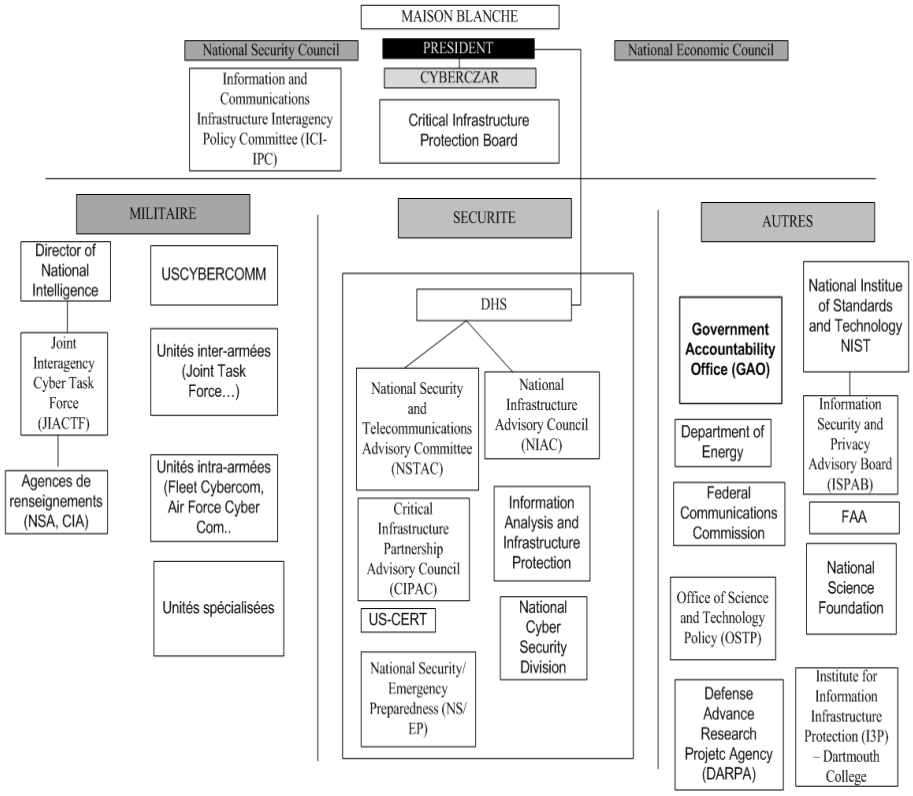


Figure 2. Représentation des entités traitant de la sécurité des infrastructures critiques aux Etats-Unis

armées américaines (Navy, Marines, Air Force et Army) dispose d'un commandement de haut niveau chargé spécifiquement de ces questions de protection et de diverses unités plus spécialisées sur les opérations d'information ou encore les opérations liées aux réseaux.

Les services de renseignement (CIA, NSA...) ont quant à eux également vocation à protéger les réseaux et les infrastructures vitales américaines, notamment en décelant de façon précoce les attaques et en agrégeant et analysant les informations s'y rapportant.

Tout ceci ne concerne que l'aspect défensif mais chaque unité peut avoir aussi un volet offensif que, cependant, nous ne traitons pas ici. Ainsi le Général HAYDEN, ancien directeur de la CIA puis de la NSA, faisait remarquer lors de la dernière conférence « Black Hat USA » (Las Vegas - 28-29 juillet 2010) [18] que, selon lui, environ 90% des efforts de la NSA sont actuellement tournés vers l'offensive.

18. `http://www.blackhat.com/html/bh-us-10/bh-us-10-briefings.html`

c. Les organisations de sécurité civile sont, pour la plupart, dans le giron du DHS ou en lien direct avec lui. Cette très importante organisation ne cesse de croitre et de se voir attribuer de nouvelles fonctions. L'US-CERT, de même que la National Cyber Security Division, sont intégrés en son sein. Il existe par ailleurs plusieurs branches dévolues à la protection des infrastructures critiques.

On notera que le DHS, qui a émis un document de référence intitulé *« National Strategy to Secure Cyberspace »* [9], a la vocation particulière d'être le conseiller particulier du Président en matière de cybersécurité et de protection des infrastructures vitales, notamment via 2 comités représentés sur le schéma :

- National Security and Telecommunications Advisory Committee (NSTAC)
- National Infrastructure Advisory Council (NIAC)

d. Enfin, parmi les organisations civiles diverses se trouvent deux acteurs particulièrement engagés : le *Government Accountability Office* (GAO) et le monde de la recherche représenté ici par la *National Science Foundation*, ou encore la *Defense Advance Research Project Agency*, plus particulièrement chargée des réseaux du futurs intégrant directement des fonctions de sécurité.

Le GAO, qui possède des fonctions analogues à notre Cour des Comptes, a adopté un comportement très proactif quels que soient les sujets. Il n'hésite ainsi jamais à pointer du doigt régulièrement les défauts dans l'organisation et la gestion des problématiques d'envergure nationale. Plus encore, les documents du GAO sont généralement bien renseignés et n'hésite pas à aborder les aspects techniques. Enfin, l'organisation publie très régulièrement ces rapports continuant à mettre en avant les objectifs, le chemin parcouru et les besoins.

Dans un rapport publié en 2004, « *Cybersecurity for Critical Infrastructure Protection* » , l'organisation n'hésite pas à proposer des outils tels que les « Smart Tokens » , à évoquer les avantages et inconvénients des différents moyens et outils de chiffrement ou encore à réaffirmer l'importance des outils d'audit, de monitoring et de *forensics*. Les travaux du GAO offrent donc une vision assez intéressante de l'état d'avancement des Etats-Unis en la matière et notamment les problèmes rencontrés associés aux solutions proposées.

Enfin, il existe également, dans cette dernière catégorie d'organisations, des institutions dédiées à la coopération et à l'échange. C'est le cas du « *Institute for Information Infrastructure Protection* » (I3P) dont le *Dartmouth College* est l'organisme de rattachement. Initialement organisme de recherche, l'I3P est un exemple intéressant d'initiative privée visant à dynamiser le partenariat public-privé autour de questions de cybersécurité. En effet, tout en restant relativement

neutre [19], l'I3P a développé une activité de forum de coopération, rassemblant nombre d'acteurs publics ou privés comme la RAND Corporation, le NIST, le DHS ..., offrant ainsi un cadre d'excellence avec un ensemble d'instituts de recherches de pointes et des liens avec l'ensemble des acteurs impliqués dans la protection des infrastructures vitales.

Si les capacités de lutte informatique des Etats-Unis sont avérées, il n'en reste pas moins que le nombre et la dispersion des organisations chargées de la sécurité pose problème. Régulièrement, articles et rapports (notamment ceux du GAO), font état de cette incapacité à organiser correctement la sécurité des systèmes. S'il fallait une preuve de plus, on se souviendrait des déclarations du sous-secrétaire d'Etat, W. Lynn, dans un article publié dans la revue « *Foreign Affairs* » , révélant les vols d'information pratiqués au Pentagone via une clé USB.

2.5 Descriptif des problématiques clés et leçons tirées du cas Conficker pour le partenariat public-privé

Le suivi de l'actualité de la « cybersécurité » aux Etats-Unis a permis de déterminer que cinq problématiques clés constituaient le coeur des débats outre-Atlantique :

a. Approche globale

b. Définition d'un cadre législatif adéquat

c. Définir les modalités du partage d'informations

d. Recherche et développement

e. Exercices et sensibilisation

a. L'approche globale prônée par les Etats-Unis se définit différemment de ce que l'on peut comprendre de l'approche française bien que celle-ci évolue également profondément. Ainsi, nous faisions référence ci-dessus à une approche commune comprenant à la fois l'aspect « sécurité informatique » des infrastructures vitales mais également celui des réseaux et systèmes d'information industriels et de gestion plus traditionnels.

Par ailleurs, une des différences notables est également de considérer Internet et l'ensemble des réseaux informatiques comme une infrastructure vitale. Enfin, on note une approche très large révélée notamment par les documents de la GAO :

19. Ce qui suppose une capacité rare que possèdent a priori les institutions éducatives américaines qui leur permet d'avoir ce rôle bien particulier...

Table 1: Critical Infrastructure Sectors Defined in Federal CIP Policy

Sector	Description
Agriculture	Includes supply chains for feed and crop production.
Banking and finance	Consists of commercial banks, insurance companies, mutual funds, government-sponsored enterprises, pension funds, and other financial institutions that carry out transactions, including clearing and settlement.
Chemicals and hazardous materials	Produces more than 70,000 products essential to automobiles, pharmaceuticals, food supply, electronics, water treatment, health, construction, and other necessities.
Defense industrial base	Supplies the military with the means to protect the nation by producing weapons, aircraft, and ships and providing essential services, including information technology and supply and maintenance.
Emergency services	Includes fire, rescue, emergency medical services, and law enforcement organizations.
Energy	Includes electric power and the refining, storage, and distribution of oil and natural gas.
Food	Covers the infrastructures involved in post-harvest handling of the food supply, including processing and retail sales.
Government	Ensures national security and freedom and administers key public functions.
Information technology and telecommunications	Provides information processing systems, processes, and communications systems to meet the needs of businesses and government.
Postal and shipping	Includes the U.S. Postal Service and other carriers that deliver private and commercial letters, packages, and bulk assets.
Public health and healthcare	Consists of health departments, clinics, and hospitals.
Transportation	Includes aviation, ships, rail, pipelines, highways, trucks, buses, and mass transit that are vital to our economy, mobility, and security.
Drinking water and water treatment systems	Includes about 170,000 public water systems that rely on reservoirs, dams, wells, treatment facilities, pumping stations, and transmission lines.

Source: GAO analysis based on the President's national strategy documents and HSPD-7.

A titre d'exemple, le cas de la « Smart Grid » fait partie des sujets récurrents dans la littérature outre-Atlantique. Réseau électrique évolué, ce futur système de gestion de l'électricité implique plus fortement les réseaux informatiques de gestion « intelligents » , c'est-à-dire capable de gérer automatique la répartition des charges, la récupération des informations sur les compteurs... Au vu des coupures d'électricité ayant affecté les Etats-Unis, de fortes craintes sont régulièrement évoquées par les acteurs. Le NIST, organisme de standardisation, a récemment publié un document traitant de la Cybersécurité au sein de la Smart Grid. Ce rapport fleuve (d'environ 500 pages), s'il constitue un effort remarquable du GAO, ne fait cependant que s'incliner devant le tropisme de l'approche américaine : le respect d'une norme avec les incitations associées. Or, nos développements montrent bien que les acteurs locaux pointent du doigt l'échec de la FISMA (ou encore du PCI-DSS [20]) et rien n'assure que cette norme complexe et longue puisse réellement conduire à l'adoption des mesures nécessaires au niveau de sécurité souhaité.

Cette approche globale comprend également toute la dimension « Menace » comme le montre les rapports du GAO [21]. Il apparait cependant que la première menace, en termes de probabilité, reste encore de leur point de vue le hacker indépendant et en second, l'employé mécontent.

20. Le vol, en 2009, de très nombreux numéros de cartes de crédits a été commis au sein d'organisations certifiés PCI-DSS : `http://www.lemonde.fr/technologies/article/2009/08/20/130-millions-de-cartes-bancaires-piratees-aux-etats-unis_1230199_651865.html`

21. Emerging Cybersecurity Issues Threaten Federal Information Systems - GAO

Table 7: Likely Sources of Cyber Attacks According to Respondents to the CSI/FBI 2003 Computer Crime and Security Survey

Potential source	Percentage of respondents
Independent hackers	82%
Disgruntled employees	77%
U.S. competitors	40%
Foreign governments	28%
Foreign corporations	25%

Source: 2003 CSI/FBI Computer Crime and Security Survey.

Table 6: Threats to Critical Infrastructure

Threat	Description
Criminal groups	International corporate spies and organized crime organizations pose a threat to the United States through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent.
Hackers	Hackers sometimes crack into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use. According to the Central Intelligence Agency (CIA), the large majority of hackers do not have the requisite tradecraft to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.
Hacktivists	Hacktivism refers to politically motivated attacks on publicly accessible Web pages or e-mail servers. These groups and individuals overload e-mail servers and hack into Web sites to send a political message. Most international hacktivist groups appear bent on propaganda rather than damage to critical infrastructures.
Insider threat	The disgruntled organization insider is a principal source of computer crimes. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a victim system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors.
National governments and foreign intelligence services	Several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that could affect the daily lives of U.S. citizens across the country. The threat from national cyber warfare programs is unique because they pose a threat along the entire spectrum of objectives that might harm U.S. interests. According to the CIA, only government-sponsored programs are developing capabilities with the prospect of causing widespread, long-duration damage to U.S. critical infrastructures.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence. However, traditional terrorist adversaries of the United States are less developed in their computer network capabilities than other adversaries. Terrorists likely pose a limited cyber threat. The CIA believes terrorists will stay focused on traditional attack methods, but it anticipates growing cyber threats as a more technically competent generation enters the ranks.
Virus writers	Virus writers are posing an increasingly serious threat. Several destructive computer viruses and worms have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, and Blaster.

Source: GAO analysis based on data from the FBI, CIA, and CERT/CC.

Enfin, on note une évolution intéressante dans la description du risque qui prend en compte l'interdépendance entre opérateurs critiques par exemple. Ainsi, un opérateur vital pour les télécommunications est dépendant de celui qui fournira l'électricité. On trouve également un exemple de 2003 qui met en avant les effets collatéraux sur le traitement des eaux, d'une importante panne électrique [22].

22. Ibid.

Par ailleurs, on peut observer une prise de conscience sur les problématiques des systèmes dits « SCADA » et notamment en raison de l'interconnexion croissante, maitrisée ou non, de ces systèmes avec d'autres réseaux.

Outre la recherche et le développement, plusieurs éléments de réponse sont proposés pour pallier à ces problématiques :

- on voit ainsi apparaitre la notion d'une chaine de sécurité prenant en compte, pour l'Internet et les réseaux, l'importance des FAI qui entrent désormais de plein pied dans la catégorie des infrastructures vitales ;
- de même apparait également une notion de maitrise des fournisseurs et de la « *supply chain* » des équipements informatiques, réseaux et logiciels. Il s'agit ici de maitriser les systèmes d'informations de bout en bout en évitant, par exemple, les problématiques de portes dérobées sur les matériels réseaux ou les logiciels informatiques. Cette notion est également perceptible en France, assez nettement dans les milieux spécialisés et de plus en plus dans la sphère politique et stratégique ;
- enfin, la notion de globalité impose également une définition plus précise et plus efficiente des relations avec le secteur privé, les organisations internationales (G8, ONU, ISO, UIT, OTAN...) et les états alliés partageant des vues similaires.

b. Cependant, le **cadre législatif pose encore problème**. L'approche « conformité » telle que contenue dans la FISMA (« *Federal Information Security Management* Act ») a fait long-feu car, à de nombreuses reprises, des audits ont pu mettre en avant le fait que des agences publiques, bien que conformes, étaient faillibles à de nombreux niveaux. La loi est d'ailleurs en cours de réexamen.

Un autre problème est la lisibilité ou encore le partage des responsabilités. Les textes traitant de ce point sont nombreux et leur nombre ne décroit pas. La dé-classification de la « *Comprehensive National Cybersecurity Initiative* » prise sous la présidence de G.W.Bush ou bien encore le récent « *Protecting Cyberspace as an National Asset Act* »[23] ne font qu'ajouter à la longue liste

23. Pour mémoire, ce projet de loi initié au mois de juin 2010 par Joe Lieberman propose la création d'un bureau « chargé de la politique du cyberespace » et dont la mission sera de travailler avec les entreprises pour mettre au point des paramètres de sécurité adaptés en cas d'attaque, notamment en ce qui concerne les réseaux électriques et l'Internet. Le président des États-Unis pourrait prendre, en cas d'urgence, « des mesures de protection critique d'Internet » et « donner un ordre aux responsables des grandes infrastructures de prévoir un plan de secours d'urgence en cas de cyber-attaque généralisée » . (source : `http://www.desaunay.com/Protecting-cyberspace-as-a-national-asset-Act_a399.html`). A cet égard, on notera une précision à apporter : la nouvelle loi précitée de protection du cyberespace a fait frémir la communauté des observateurs car elle donnerait au Président la capacité de « couper » Internet. Or, cela est à la fois vrai et faux puisque le Président des Etats-Unis dispose de ce droit depuis 1934 comme l'atteste la loi américaine, droit applicable en temps de guerre ou de désastre national : `http://cidris-news.blogspot.com/2010/06/breve-sur-le-cybersecurity-bill.html`

des textes (ou projets de textes) régissant (ou visant à régir) le statut des infrastructures vitales.

Une troisième question concerne enfin les aspects financiers et fiscaux. En effet, il s'agit à la fois d'inciter les opérateurs privés ainsi que les agences publiques à se conformer à des obligations de nature à élever le niveau de sécurité. Pour cela, un système d'incitation à bases de taxes et d'exemptions d'impôts est envisagé comme pour de nombreux autres domaines. En ce qui concerne les agences, c'est leur budget qui est visé, avec un droit de regard attribué à différents acteurs. Cependant, ce système d'incitation n'est encore que peu ou mal défini et ne rend pas les services attendus. Une des problématiques actuelles est donc de refondre un système pour en obtenir les effets désirés. Pour autant, dans la vision américaine, rien ne sera possible sans un effort budgétaire conséquent des Etats-Unis. Il faut donc prévoir des fonds en quantité suffisante pour financer notamment la protection de ces infrastructures mais également la recherche et le développement des outils et moyens de sécurité de demain.

c. Le dernier problème reste l'encadrement juridique des échanges d'information et constitue également, la troisième problématique-clé.

En effet, à de nombreuses reprises, il est fait allusion au **partage d'informations**. Cette problématique ne concerne pas seulement les Etats-Unis puisque lors de conférences sur la protection des infrastructures vitales, en France, des acteurs ont demandé une réévaluation du dispositif considérant qu'il n'est pas assez automatique ou encore efficace.

A de nombreuses reprises, les éléments tirés de la bibliographie ou de la veille ont mis en évidence des déclarations faisant état de carences au niveau du partage d'informations entres les acteurs impliqués dans la protection des infrastructures critiques. Ces carences sont notamment organisationnelles car les processus à priori existants ou le cadre juridique applicable manque encore d'efficacité.

Cet aspect est primordial car il semble focaliser l'ensemble des difficultés liées à la gestion des infrastructures vitales. En effet, il porte une grande partie de la nature des relations à venir entre les acteurs publics et privés. Or, le secteur public de la sécurité est par nature et tradition, peu enclin à partager ses informations et le monde privé a parfois une gestion laxiste de ses propres informations. Peu de choses plaident donc pour une forme de cogestion apaisée.

On peut pourtant tirer profit de quelques expériences où les différents acteurs ont été obligés de communiquer.

La « faille » Kaminsky fut ainsi un des cas ayant joué un rôle de catalyseur dans la mise en place du DNSSEC (« *Domain Name System Security Extensions* »).

La gestion de la problématique « Conficker » est également très intéressante en ce que plusieurs acteurs ont souhaité rédiger des retours d'expérience explicitant alors les enseignements à tirer de la question. On dispose ainsi d'un document rédigé par un officiel de l'ICANN, plus particulièrement chargé des questions de sécurité. Celui-ci est intéressant car l'infrastructure DNS s'est retrouvée au centre de la problématique car le vers utilisait de nombreux noms de domaines associés à de très fréquents changements. De nombreux acteurs de nature diverses ont alors été impliqués : ICANN, fournisseurs de produits de sécurité, communauté du renseignement, registres, bureaux d'enregistrement, chercheurs, gouvernements...

Une des problématiques majeures posées par le ver a été la souplesse. Celui-ci a été développé en au moins cinq versions délivrées en réaction aux mesures de sécurité. Il s'agissait donc que l'ensemble des acteurs puissent rapidement réagir à toute nouvelle version afin, par exemple, de bloquer les domaines utilisés par le vers.

Par ailleurs, la complexité croissante du ver est allée de pair avec une augmentation de sa diffusion et un nombre grandissant de noms de domaine utilisé. Cela impliquait donc de plus en plus d'organisations dont l'intégration devenait obligatoire.

En réponse à cette problématique ont été développés différents processus dont certains ont été conservés. C'est le cas des « *Expedited Registry Security Request Process (ERSR)* » , processus d'information des registres vers l'ICANN [24] afin de remonter des alertes sur des incidents de sécurité.

Cette formalisation des processus de sécurité est donc issue, pour l'ICANN, des leçons tirées de la gestion des dérives de Conficker et constitue un vrai apport.

La dernière leçon de l'épisode Conficker concerne le partage d'informations. Au-delà du processus cité ci-dessus, les acteurs réaffirment que les modes de partage de l'information tel que le « *best effort* » ou encore l'informel ne peuvent suffire à prévenir ou gérer des crises.

La crise Conficker enseigne donc le besoin du partage d'informations, la nécessité de définition des processus et le besoin de souplesse entre organisations.

d. Parmi les problématiques encore abordées notamment par le GAO, **la Recherche et le Développement dans le domaine informatique et sécurité** figurent en bonne place. Le GAO y consacre d'ailleurs un rapport entier [25] qui fait état de différents problèmes. Sujet sensible en France, il est également préoccupant outre-Atlantique.

24. `http://www.icann.org/en/registries/ersr/`

25. CYBERSECURITY - Key Challenges Need to Be Addressed to Improve Research and Development

Si le GAO pointe ici un manque de recherche dans le domaine de la « cybersécurité » , elle ne fait pas allusion à d'autres éléments préoccupants. Les Etats-Unis connaissent, comme le reste du monde, un phénomène de désertion des filières scientifiques [26] qui rend incertain la capacité du pays à préserver un leadership et un fort contrôle dans le domaine de la cybersécurité. Parmi d'autres problèmes, c'est notamment cette question qui est jugée préoccupante.

Le GAO fait également état de deux autres aspects jugés dommageables :
- le manque de leadership et d'impulsion globale qui rend cohérente une politique de recherche ;
- les carences du partage d'informations : si l'on a vu qu'il existe de nombreux organismes rassemblant l'ensemble des acteurs, cela parait encore insuffisant à la Cour des Comptes américaine qui juge encore trop aléatoire le partage des connaissances et demande un encadrement plus poussé.

e. Dernière problématique clé, la question **de la sensibilisation et des exercices** est également abordée.

Le GAO réclame en premier lieu plus de sensibilisation et propose d'utiliser des outils dont l'efficacité est prouvée en s'appuyant sur des campagnes de sensibilisation telles que « *Smokey Bear* » lancée pour prévenir les feux de forêts et qui a montré sa capacité à sensibiliser les esprits. Pour autant, cette analogie laisse songeur notamment parce que les gestes impliqués sont bien plus techniques et les populations concernées bien plus hétérogènes en ce qui concerne leurs compétences en informatique.

Ensuite, dans l'optique de tester l'état actuel de son degré de préparation, les Etats-Unis ont déjà organisés, à la fois au niveau national et international, **plusieurs exercices** susceptibles de lui conférer une longueur d'avance par rapport aux nations et autres organisations interétatiques (UE, OTAN) :
- Cyberstorm I (2006) : incluant outre les Etats-Unis, la Grande-Bretagne, le Canada, l'Australie et la Nouvelle-Zélande, ces exercices tendaient à tester les procédures en vigueur ainsi que leur résistance aux attaques ;
- Cyberstorm II (2008) : incluait l'hypothèse que l'attaquant pouvait pénétrer n'importe quel réseau, dégrader le réseau Internet et les systèmes SCADA (sur lesquels reposent en quasi-totalité la protection des infrastructures vitales dans les différents secteurs d'activité concernés : eau, gaz, électricité, carburants, transports, télécommunications, urgences, etc.) ;
- Cyber Shock Wave (2010) : cette attaque - simulée par les Américains le 16 février dernier - aurait, d'après les commentateurs, plongé dans le noir la plus grande partie des Etats-Unis, montrant ainsi la fragilité du secteur énergétique.

26. http://www.assemblee-nationale.fr/12/rap-info/i3061.asp

– Cyberstorm III [27] s'est déroulé à la fin du mois de septembre 2010. Cet exercice se concentrera sur la question des infrastructures critiques avec le test d'environ 1500 scénarios d'attaques informatiques concoctés notamment par la NSA et le Pentagone. De nombreux pays ont été invités dont les alliés proches des Etats-Unis. Plusieurs ministères ainsi qu'une soixantaine d'entreprises privées de tous les secteurs, participaient également à cet évènement d'une durée de 4 jours environ.

En définitive, les Etats-Unis, depuis l'élection du Président Obama, ont développé un fort activisme en matière de protection des infrastructures vitales. Celles-ci, cependant, sont définies de façon relativement différente, intégrant par exemple Internet. La dimension « cybersécurité » contient par ailleurs, une notion de sécurité informatique propre aux infrastructures vitales qui n'est pas traitée de façon identique en France. Enfin, les problèmes rencontrés sont très proches des nôtres et les solutions imaginées sont également instructives pour l'approche nationale.

3 Dispositif et cadre juridique français

Les diverses organisations décrites ci-dessus ont permis de mettre en avant les avantages et les inconvénients dans le traitement de la problématique des infrastructures critiques. Particulièrement bien dotés en termes d'organisations, les Etats-Unis se distinguent toutefois par une organisation complexe, lourde et dont le poids ne donne pas forcément toutes les garanties souhaitées.

Par ailleurs, Anglais, Allemands et Français partagent aujourd'hui certains réseaux propres aux infrastructures critiques : acheminement d'hydrocarbures, électricité... Régulièrement, des pannes sont constatées sur des régions géographiques proches mais appartenant à des Etats différents [28]. Cette intégration des réseaux suppose donc également une vision européenne commune ainsi qu'une capacité française déjà établie. La directive « CIIP » de mai 2009 [29] semble en prendre la direction et n'est pas sans rappeler, plus de 10 ans plus tard, le décret SAIV de 1996. Mais cette intégration des réseaux suppose d'abord une véritable capacité française de protection des infrastructures dites vitales.

27. http://cidris-news.blogspot.com/2010/09/cyber-storm-iii.html
28. On pense aux coupures d'électricité qui affectent l'ouest de l'Allemagne et le Nord et/ou l'Est de la France.
29. http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm

3.1 Une organisation française et un partenariat avec les OIV efficace ?

Présentation du dispositif français en vigueur Comme l'explique fort pédagogiquement Matthieu Grall, expert conseil du bureau Assistance et Conseil de l'ANSSI, dans une interview donnée à la revue Mag Securs consacrant un dossier à la sécurité des industries sensibles [10], le principe général du dispositif français pour la sécurité globale des infrastructures vitales repose sur un « *dispositif à étages, par secteur, par opérateur et par site* » :

1. Par secteur : 1er étage du dispositif, les « SAIV » (Secteurs d'Activités d'Importance Vitale) sont répartis en 12 secteurs fixés par arrêté du 2 juin 2006 et coordonnés chacun par un ministre. Chaque SAIV fait l'objet d'une Directive Nationale de Sécurité (DNS), sorte de politique générale de sécurité pour le secteur concerné mettant en évidence les risques globaux auxquels le SAIV est exposé et des mesures graduées par niveau d'alerte. Conformément au décret n° 2006-212 du 23 février 2006, « *un secteur d'activités d'importance vitale est constitué d'activités concourant à un même objectif qui :*

   (a) Ont trait à la production et la distribution de biens ou de services indispensables ;
   - *a. A la satisfaction des besoins essentiels pour la vie des populations ;*
   - *b. Ou à l'exercice de l'autorité de l'Etat ;*
   - *c. Ou au fonctionnement de l'économie ;*
   - *d. Ou au maintien du potentiel de défense ;*
   - *e. Ou à la sécurité de la nation ;*

   Dès lors que ces activités sont difficilement substituables ou remplaçables ;

   (b) Ou peuvent présenter un danger grave pour la population.

   » En outre, comme déjà mentionné en introduction, le Livre Blanc adopté en 2008 [2] parle d'un Internet crucial pour notre sécurité et considère également le réseau des réseaux comme une « *infrastructure vitale* » (p.58 - 2ème partie du Tome 1).

2. Par opérateur : 2ème étage du dispositif, chacun des OIV (Opérateurs Importance Vitale) - environ 250 - nomme un délégué pour la défense et la sécurité de l'opérateur qui a la charge d'élaborer un PSO (Plan de Sécurité Opérateur) pour décliner la ou les DNS dont relève l'Opérateur. Le statut d'OIV repose sur deux conditions qui sont définies dans l'Instruction Générale Interministérielle du 26 septembre 2008 (IGI/6600/SGDN/PSE/PPS) :
   - *que son activité s'exerce en tout ou partie dans un secteur d'activités d'importance vitale ;*
   - *qu'il gère ou utilise au moins un établissement, un ouvrage ou une installation dont le dommage, l'indisponibilité ou la destruction risquerait de*

quelque manière que ce soit d'avoir des conséquences majeures sur les capacités de la Nation ou sur la santé de la population.

3. Par site : 3ème et dernier étage du dispositif, les PIV (Points d'Importance Vitale) désignent des sites sensibles tels une centrale nucléaire. Identifiés sur proposition des OIV et regroupés en zones aux menaces et mesures de sécurité similaires, ils doivent faire l'objet d'un Plan de Protection Particulier (PPP) et d'un Plan de Protection Externe (PPE, élaboré par le Préfet de départements), qui déclinent de façon opérationnelle les PSO.

Des lacunes persistantes constitutives d'autant d'axes de progression Comme présenté dans le rapport d'information au Sénat de juillet 2008 [11], plusieurs lacunes affectent l'efficacité de l'organisation de la France en matière de cyberdéfense, difficultés encore persistantes à différents degrés en 2010 :

– la dispersion des différents acteurs en charge de la sécurité des systèmes d'information : à cet égard, la complexité du schéma inséré ci-après, est loin cependant d'égaler celle de l'organisation américaine présentée plus haut (2). De plus, la création de l'Agence Nationale pour la Sécurité des Systèmes d'Information (ANSSI) le 7 juillet 2009 [30] permet de concentrer toutes les compétences en matière de sécurité au profit des administrations et des opérateurs d'importance vitale.

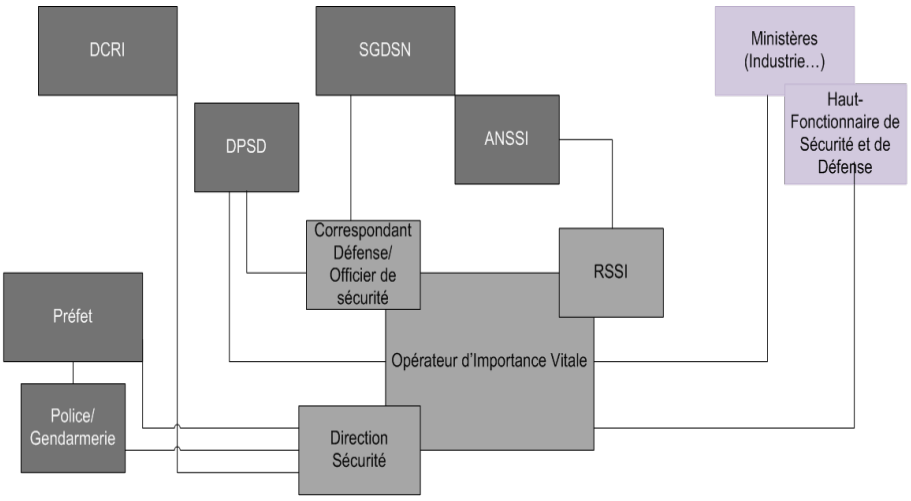


Figure 3. Schématisation des acteurs français impliqués dans la protection des infrastructures vitales

30. Créée par décret n° 2009-834, la nouvelle agence est rattachée au secrétaire général de la défense et de la sécurité nationale, en lien direct avec le cabinet du Premier ministre.

- la très large autonomie des directions administratives pour la mise en oeuvre de leur politique de sécurité : le caractère non contraignant des recommandations édictées en la matière conduit nécessairement à un manque d'harmonisation au sein de l'Administration ;
- des ressources humaines insuffisantes : malgré des efforts de recrutement importants ces derniers mois et donc un rattrapage progressif (l'objectif 2012 étant fixé à 250 agents [31]), un effectif encore trop réduit au sein du service pivot, l'ANSSI, en comparaison de ses homologues britannique et allemand, rend difficile l'atteinte de tous ses objectifs comprenant à la fois la sensibilisation, le conseil, l'évaluation, la surveillance et la qualification de produits sécurisés ;
- l'absence de capacité centralisée de surveillance et de détection des flux de données transitant entre les administrations et l'Internet : c'est ici un besoin d'approche centralisée avec un acteur unique de coordination qui ne prendrait ni la place, ni les compétences des différents acteurs impliqués qui est identifié dans le Rapport Romani ;
- l'insuffisance de l'action des pouvoirs publics en direction du secteur privé en matière de sensibilisation et de conseil : de ce point de vue, le Livre Blanc ayant souligné l'importance de disposer de relais sur l'ensemble du territoire pour sensibiliser les principaux acteurs de la société de l'information et diffuser les mesures de protection préparées par l'ANSSI, un réseau territorial d'experts est mis en place actuellement au sein d'observatoires zonaux (les « OzSSI » au nombre de 7) placés auprès des préfets de zone.

S'agissant du partage d'informations déjà évoqué dans l'exposé des exemples étrangers (section 2) comme un besoin et une problématique-clé, le sujet est régulièrement évoqué en France notamment lors de colloque spécialisés. Une des leçons tirées de la « crise Conficker » a été que le mode « partage informel » ou « best effort » n'était pas suffisant à la fois avant mais aussi pendant la crise. On peut donc imaginer qu'une plus grande lisibilité de l'organisation et des processus mieux définis permettraient de mieux gérer les relations avec les différents acteurs.

Identifiées également comme des axes d'améliorations, la communication et la sensibilisation apparaissent comme très importantes. A cet égard, l'absence de communication et de publicité plus large sur les exercices conduits ne rend pas forcément compte du niveau de préparation atteint. Rappelons que la France organise des exercices réguliers de crise informatique appelés « Piranet » , qui demeurent cependant, culture du secret oblige, bien plus discrets que les exercices outre-Atlantique. Invitée cette année à participer à la campagne de tests américains « *Cyberstorm III* » , la France est également partie prenante dans d'autres exercices internationaux organisés par l'OTAN (« *Cyber coalition* »).

31. Présentation de l'ANSSI par Nathalie Favier, lors des journées de l'AFSIN (Troyes, 28-30 septembre 2010).

Par ailleurs, la sensibilisation s'applique à l'ensemble des acteurs, de l'individu au grand groupe et reste encore trop peu imposée au sein des organisations. Un acteur de coordination imposant une politique globale apporterait sans doute un plus à ce niveau.

En définitive, à certaines exceptions près, les entreprises françaises paraissent insuffisamment armées face à la menace informatique, celles-ci étant en outre souvent confrontées à une difficulté dans la définition et l'appréciation de la menace. S'agissant en particulier des PME, qui représentent en elles-mêmes un part très importante du patrimoine scientifique et technique de la France et qui pourraient donc être considérées dans leur ensemble comme un actif critique, les efforts de sensibilisation de la DCRI, la DPSD ou encore la Gendarmerie nationale pour créer une synergie public-privé dans la lutte pour la protection du patrimoine informationnel, correspondent à des actions trop ponctuelles et non coordonnées pour pouvoir se révéler pleinement efficaces.

3.2 Difficultés et évolution du cadre juridique français

Comme l'ont montré les exemples étrangers développés à la section 2, le partenariat public-privé conduit plus particulièrement à développer des échanges d'information autour des vulnérabilités d'une part et des incidents de sécurité d'autre part. Malgré les réticences naturelles qui opèrent en la matière, le cadre juridique français continue de s'adapter pour converger progressivement vers ces nouveaux besoins ...

Divulgation des vulnérabilités Pour caractériser l'environnement juridique et l'état d'avancée des partisans de la « sécurité par la transparence » (*full disclosure*), on se souviendra ici d'anciennes affaires très médiatisées, tant dans l'Hexagone (cas « Serge Humpich » [32] - février 2000) qu'à l'étranger (cas Dimitri Sklyarov [33] - Las Vegas, juillet 2001 ; cas « *DVD Jon* » [34] - Norvège, 2002), ou bien encore d'affaires plus récentes (affaires « Zataz » [35] et « Vupen » [36] - sept.-octobre

32. Pour un rappel des faits : `http://www.legalis.net/spip.php?page=breves-article&id_article=1201`.

33. Programmeur russe employé de la société ElcomSoft, il est connu pour avoir été arrêté à l'issue d'une conférence intitulée « eBook's Security - Theory and Practice » à la convention DEF CON à Las Vegas en juillet 2001 et poursuivi par la société Adobe qui lui reprochait d'avoir développé pour sa société un logiciel destiné à contourner des mesures de protection logicielles, selon les termes du Digital Millennium Copyright Act (DMCA)...

34. Surnom donné à Jon Lech Johansen, adolescent norvégien impliqué dans la diffusion du logiciel DeCSS et inculpé en 2002... Pour en savoir plus : `http://fr.wikipedia.org/wiki/Jon_Lech_Johansen`

35. Pour une présentation de l'affaire : `http://www.legalis.net/breves-article.php3?id_article=2739`

36. Texte de la décision : `http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2791`

2009) dans lesquelles il a été respectivement reproché aux prévenus d'avoir divulgué une faille de sécurité ou bien encore mis à disposition, sans motif légitime, un exploit (c'est-à-dire un élément de programme permettant à un individu d'exploiter une faille de sécurité informatique dans un système d'information ou un logiciel ceci, par exemple, afin de prendre le contrôle d'un ordinateur, de permettre une augmentation de privilège d'un logiciel ou d'un utilisateur, ou d'effectuer une attaque par déni de service).

Partant du principe suivant lequel le risque résiduel le plus fort se situe dans le délai qui sépare la découverte d'une faille de sécurité dans un système et la disponibilité d'un correctif et son installation effective [37], une divulgation responsable passe, comme le recommande d'ailleurs (en l'état du projet) la proposition de norme ISO/CEI 29147 « Responsible Vulnerability Disclosure » [38], par une information préalable et une collaboration étroite avec l'éditeur pour résoudre la vulnérabilité concernée. Dès lors que l'on s'écarte de ce « schéma idéal » , les facteurs qui peuvent être retenus pour évaluer son « risque judiciaire » en cas de divulgation d'une faille de sécurité sont notamment :

- détails/nature de la divulgation (ex. données permettant d'exploiter directement la vulnérabilité)
- faible/haut niveau d'expertise requis
- système/environnement/logiciel standard (répandu) ou plutôt exotique ou complexe
- nombre d'utilisateurs potentiellement impactés
- criticité ou sévérité de la vulnérabilité
- divulgation avec/sans solutions de contournement
- divulgation à public restreint ou au contraire très large (ex. site ou publication à forte audience)
- public visé : grand public, professionnels, communauté scientifique, ...
- divulgation précédée de l'information de l'éditeur, avec ou sans délai, avec ou sans assistance, à titre gratuit ou onéreux
- ...

En définitive aujourd'hui, dans le cadre du partenariat public-privé justifié par la protection des infrastructures d'importance vitale, c'est bien par le biais de structures et de canaux d'information dédiés (réseau de CERTs) que la communication sur les vulnérabilités peut s'effectuer tout en éludant ces risques judiciaires. Par ailleurs, la coopération avec les éditeurs et surtout l'évaluation des produits font partie des missions de l'ANSSI qui se prononce sur la sécurité des dispositifs et des services, offerts par les prestataires nécessaires à la protection des systèmes d'information. Elle favorise également la prise en compte de la sécurité dans le

37. On parle communément de « fenêtre d'exposition » pour désigner ce délai.
38. Projet de normalisation soutenu par la société Microsoft...

développement des technologies de l'information.3.2.2 Signalement des incidents de sécurité

Dans tous les cas, que ce soit les administrations ou les entreprises, la mauvaise publicité conséquente au dévoilement d'une vulnérabilité ou d'un incident de sécurité est globalement trop négative et angoisserait clients ou usagers, actionnaires, partenaires et fournisseurs, si bien que les organisations restent très réticentes à révéler a fortiori les attaques dont elles ont été victimes.

Pourtant, la culture du secret qui prévaut toujours en France va bientôt connaître une première brèche sous l'impulsion des derniers textes européens relatifs à la protection des données à caractère personnel dans le domaine des communications électroniques. En effet, dans le cadre des négociations du « Paquet Télécoms » qui se sont achevées fin 2009, la directive « E-privacy » 2009/136/CE [39] (ci-après « la Directive »), qui modifie notamment la directive 2002/58/CE « Vie privée et communications électroniques » , introduit à son tour [40] une obligation de signalement des incidents ayant entraîné une violation de la sécurité de ces données [12]. Si le Conseil de l'Union Européenne souhaitait restreindre cette obligation aux seuls opérateurs télécoms, le texte définitif adopté le 25 novembre 2009 - qui vise les « *fournisseurs de services de communication électronique accessibles au public* » -, semble l'avoir généralisé à l'ensemble des acteurs de l'Internet et a pour ambition de l'appliquer « *quel que soit le secteur ou le type de données concerné* » (Considérant 60 de la Directive).

Si, comme le commente Me Eric Caprioli [13], le texte soulève encore plusieurs interrogations - en particulier : notion de « *sans retard indu* » à interpréter de manière circonstanciée en fonction de la taille de l'entreprise, l'existence ou non d'un CIL et de procédures formalisées de notification ; notion de « violation des données » dont il faut définir les critères déclencheurs de la notification (ex. sensibilité des données affectées, préjudice causé) ; modalités pratiques de contenu, forme et modalités à respecter ; question du partage de responsabilités en cas de sous-traitance et du droit applicable dans les situations de notification extraterritoriales -, la transposition dans les Etats membres est prévue au plus tard le 25 mai 2011.

39. Directive publiée au JOUE du 18 décembre 2009 : `http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:FR:PDF`

40. Le principe de la notification de la violation des données a été initié dès 2002 en Californie (Senate Bill 1386), puis repris progressivement dans 44 Etats américains et adopté au niveau fédéral dans certains secteurs tels que les finances, avant d'être implémenté en Allemagne par le biais de la loi fédérale du 20 décembre 1990 (Bundensdataschutzgesetz).

Dépassant d'ores et déjà les objectifs de cette directive [41], la proposition de loi Detraigne-Escoffier [14], adoptée en 1ètre lecture par le Sénat puis transmise à l'Assemblée nationale le 24 mars 2010, prévoit elle-même (article 7) une double obligation de notification pesant ici sur tous les « responsables de traitement » [42] et consistant à avertir, sans délai, le CIL - ou à défaut de celui-ci, la Commission Nationale Informatique et Libertés (CNIL) - de toute « violation » d'un traitement de données à caractère personnel et, le cas échéant, informer les personnes physiques concernées dont les données auraient été affectées par la violation. En l'état de la proposition de loi, il semble donc que toute atteinte, volontaire comme involontaire, doive déclencher une notification, l'absence de nécessité de justification d'un préjudice par les personnes concernées par la violation tendant en outre à favoriser le « tout » notifier, ce qui paraît inenvisageable ... Gageons ici que la loi qui sera adoptée et ses textes d'application permettront de mettre en place un dispositif efficace, qui contribuera à la fois à une gestion plus responsabilisante des données à caractère personnelle d'une part et à plus de transparence en matière de sécurité d'autre part.

Enfin, s'agissant plus spécifiquement des incidents affectant les systèmes d'information de l'Etat, l'ANSSI met en oeuvre un système de détection des évènements susceptibles d'affecter la sécurité de ces systèmes et coordonne la réaction à ces évènements. Elle recueille les informations techniques relatives aux incidents affectant les systèmes d'information de l'Etat via le « COSSI » , Centre opérationnel de la SSI regroupant notamment un centre de veille, le CERTA et un centre de détection ...

4 Quelle cible de coopération ?

Les différents acteurs (publics [43] comme privés [44]) s'accordent aujourd'hui sur deux cibles prioritaires (pour ne pas dire impératives) :

41. Parmi les nouvelles dispositions envisagées : la clarification du statut de l'adresse IP en tant que donnée à caractère personnel (article 2), la désignation d'un CIL (Correspondant Informatique et Libertés) rendue obligatoire pour les organismes ayant recours à un traitement soumis à autorisation ou auquel plus de 100 personnes y ont directement accès ou sont en charge de sa mise en oeuvre (article 3), le renforcement des obligations relatives au devoir d'information des personnes (article 6)...

42. Au sens de la loi Informatique et Libertés du 6 janvier 1978, il s'agit de la personne ou de l'entité qui détermine la finalité et les moyens attachés à un traitement de données à caractère personnel.

43. En ce sens par exemple les propos tenus lors du FIC 2010 dans le cadre de la table ronde sur la cyberdéfense « *quelles coopérations public/privée dans le cadre du livre sur la défense et la sécurité nationale ?* » ou bien encore le discours tenu par M. Pascal Pailloux lors de son intervention dans le cadre du premier sommet mondial consacré à la cyberdéfense (Dallas, 3-5 mai 2010) - 01net.entreprise, 06/05/2010.

44. Ainsi Michael Dell, CIO de Dell, et Jim Stikeleather, CIO de Dell Services, ont eux aussi lancé au récent sommet international sur la cybersécurité un avertissement aux experts sur l'urgence de repenser la cybersécurité au niveau mondial - Le Monde Informatique, 10/05/2010. Ceux-ci estiment d'une part que les gouvernements n'ont pas fait suffisamment de choses en matière de cybercriminalité (dans laquelle ils incluent la criminalité économique et les menaces directes pesant sur les infrastructures

- la coopération internationale d'une part, qui s'inscrit pour l'heure :
  - soit dans le cadre de l'Union européenne : on peut notamment souligner ici le rôle de l'ENISA (*European Network for Information Security Agency*) qui, bien que n'ayant aucun pouvoir d'action dans la lutte contre les cyberattaques, oeuvre en tant que plateforme d'expertise ;
  - soit dans le cadre de l'OTAN : après avoir officialisé en 2008 sa politique sur la défense cybernétique, l'Organisation a mis en place, suite aux cyberattaques dirigées contre l'Estonie entre avril et mai 2007, un Centre d'Excellence (*CCD CoE Talinn*= - opérationnel depuis avril 2008) qui est une plateforme intellectuelle et un forum d'échange d'informations ; en parallèle, a été également mise en service une autorité de contrôle (*Cyber Defense Management Authority -CDMA*) - accréditée depuis octobre 2008, qui incarne ici la capacité opérationnelle, responsable pour le déclenchement ainsi que la coordination de l'action immédiate de la cyberdéfense en cas d'attaque imminente ou en cours [45] ;
- une nouvelle gouvernance de l'Internet permettant de dépasser la gestion très « américano centrée » en vigueur et de l'adapter pour répondre aux changements qui vont modifier l'utilisation de l'Internet dans les années à venir. Ainsi l'exposé portera notamment sur les failles ou manquements justifiant l'évolution souhaitée. En outre, cette nouvelle gouvernance devra à la fois préserver le pré-carré stratégique des Etats tout en réservant une place de choix à l'Europe. A cet égard, on notera l'implication sans réserve du Conseil de l'Europe présent régulièrement aux colloques internationaux de la Gouvernance Internet.

4.1 Enseignements de la coopération extérieure...

...en matière de lutte contre la criminalité organisée La réponse de l'Union européenne dans la lutte contre le crime organisé est à la fois globale (touchant de nombreux domaines d'action et politiques de l'Union), ciblée (visant notamment les trafics d'armes ou de drogue, la criminalité économique et financière, la corruption ou encore le blanchiment d'argent ainsi que les nouvelles dimensions que sont le cyberterrorisme ou la criminalité environnementale), et or-

critiques de l'Internet) et ont considéré ce problème de manière étroite, en le limitant souvent à la sphère nationale et ,d'autre part, qu'il faudrait peut-être revoir la manière dont les Etats-Unis dirigent l'Internet : « *les gouvernements et le secteur privé doivent travailler ensemble pour élaborer un cadre international approprié pour sécuriser le cyberespace. Nous devrions tous faire en sorte que le système nerveux central de l'information mondiale soit intouchable et sûr.* »

45. Informations présentées par Bart Smedts, dans son article « *Cyberguerre et cyberdéfense dans le cadre de l'OTAN et de l'UE* » , paru à la revue Défense Nationale du mois de juin 2010, pp.31-38.

ganisée (s'appuyant le plus souvent sur des agences et offices européens [46] chargés de coordonner les actions autorisées par les différents protocoles d'accord).

L'approche intégrée qui guide l'action de l'Union s'étend de la prévention à la répression et repose essentiellement sur une coopération entre les services des États membres, incluant en particulier la désignation de points de contact, l'échange régulier d'informations à un stade précoce et l'entraide en matière par exemple de perquisitions, saisies et de confiscations.

Prenant l'exemple particulier de la coopération en matière de lutte anti-terrorisme, on peut également relever parmi les mesures préconisées dans la Communication de la Commission [15] sur un programme européen de protection des infrastructures critiques (décembre 2006) [47] :

- la mise en place d'un réseau d'alerte concernant les infrastructures critiques (CIWIN) : complémentaire des réseaux existants (ex. système ARGUS de la Commission pour les messages d'alerte rapides), le réseau visé doit consister en une plate-forme (homologuée) pour un échange sécurisé des meilleures pratiques ;
- le recours à des groupes d'experts nationaux en la matière au niveau de l'UE : groupes spécialement constitués pour examiner des questions clairement définies et favoriser le dialogue entre les secteurs public et privé en matière de protection des infrastructures critiques ;
- des procédures de partage des informations relatives à la protection des infrastructures critiques.

. . . en matière d'espaces internationaux : cas du droit de la mer Le droit maritime international nous apporte l'expérience du régime applicable aux eaux internationales. Ainsi, on relève en particulier que les eaux internationales, qui sont comprises dans la Convention de Montego Bay ou CMB [Convention des Nations Unies sur le Droit de la Mer - CNUDM, 1982 ; convention signée par la Communauté européenne] dans le champ de définition de la « haute mer » (partie VII), constituent en premier lieu, comme nous pourrions l'écrire pour l'Internet ou le cyberespace :

46. Pour exemple, citons : Europol, l'office européen de police ; Eurojust, chargé de renforcer la coopération judiciaire entre Etats ; OLAF, l'office européen de lutte anti fraude ; ou encore, Frontex, l'agence européenne pour la gestion de la coopération opérationnelle aux frontières extérieures des États membres de l'Union européenne.

47. Rappel de l'historique de ce texte : le Conseil européen de juin 2004 a demandé l'élaboration d'une stratégie globale visant à renforcer la protection des infrastructures critiques (PIC). La Commission a adopté, le 20 octobre 2004, une communication intitulée « Protection des infrastructures critiques dans le cadre de la lutte contre le terrorisme », dans laquelle elle a proposé des mesures en vue de renforcer la prévention, la préparation et la réponse de l'Union européenne face aux attaques terroristes contre des infrastructures critiques (IC). La présente communication expose les principes, les procédures et les instruments proposés pour mettre en oeuvre le programme européen de protection des infrastructures critiques (EPCIP).

– un espace de liberté, ouvert à tous (article 87),
– où aucune revendication de souveraineté (territoriale) par un Etat n'est légitime (article 89).

Dans le cadre de cet espace maritime international, force est de souligner que la lutte contre la criminalité organisée, en particulier le trafic illicite de stupéfiants et substances de psychotropes (article 108 CMB), repose entièrement sur la coopération internationale.

Bien sûr, la simple transposition des règles juridiques existantes telles que celles du droit maritime international citées par analogie, ne paraît pas envisageable car elle ne permettrait pas de prendre en compte des spécificités du cyberespace telles que la nécessité en particulier d'élaborer des normes régissant le fonctionnement, les moyens et l'utilisation, dans le cadre d'opérations de lutte informatique, des infrastructures mondiales de l'information et des prestataires techniques qui sous-tendent l'Internet.

Ce retour d'expérience permet néanmoins de confirmer le caractère incontournable de la voie de la coopération internationale comme mode de pacification du cyberespace, la construction du cadre juridique applicable à l'espace numérique mondial ayant déjà été entamée dans le domaine de la lutte informatique « en temps de paix » (cadre judiciaire et policier), au travers de différentes conventions internationales et d'accords de coopérations, notamment la **Convention des Nations Unies contre la criminalité transnationale organisée** (2000) [48].

Dans le domaine de la cybercriminalité C'est le chapitre III de la Convention de Budapest adoptée en 2001 [49] et entrée en vigueur en France en 2006 [50], qui traite des aspects liés à la « coopération internationale » et qui pose les principes d'une entraide internationale aux fins notamment d'investigation et de recueil des preuves sous forme électroniques.

A cet égard, la Convention prévoit plus particulièrement qu'une Partie à la Convention peut demander à une autre :

– d'ordonner ou imposer la conservation rapide, à titre conservatoire, de données stockées au moyen d'un système informatique se trouvant sur son territoire ;

48. Texte de la Convention : `http://www.uncjin.org/Documents/Conventions/dcatoc/final_documents_2/convention_french.pdf`. Cette convention est le premier instrument global - et juridiquement contraignant des Nations Unies - de lutte contre la criminalité transnationale organisée, nécessitant une action concertée au niveau mondial. L'objectif principal de la convention est de promouvoir la coopération et, au niveau européen, de renforcer l'espace judiciaire afin de combattre plus efficacement ce phénomène.

49. `http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm`

50. La France avait signé la Convention le 23 novembre 2001 puis adopté la loi de promulgation du 19 mai 2005 en autorisant l'approbation. Un an après cette loi, les décrets n° 2006-580 et n° 2006-597 du 23 mai 2006 permettant la publication et l'entrée en vigueur de la Convention et du protocole additionnel, sont adoptés...

- de donner un accès rapide aux données de trafic se rapportant aux échanges électroniques objet d'une investigation ;
- dans la limite permise par les lois internes applicables, collaborer aux opérations d'interception en temps réel de données relatives au contenu des communications spécifiques transmises au moyen d'un système informatique.

Enfin, l'article 35 de la Convention a également conduit à la mise en place d'un « réseau 24/7 » dans le cadre duquel chaque Partie désigne un point de contact joignable vingt-quatre heures sur vingt-quatre, sept jours sur sept, afin d'assurer une assistance immédiate pour, le cas échéant (en fonction du droit et de la pratique interne) :

- apporter des conseils techniques ;
- conserver des données ;
- recueillir des preuves, apporter des informations à caractère juridique et localiser des suspects.

Dans la pratique, les cas d'information spontanée, eux aussi encouragés par la Convention, sont plutôt rares et les procédures à suivre encore trop lourdes pour assurer en particulier l'accélération des transmissions d'information (réseaux professionnels encore trop peu développés, demandes de confirmation de l'Etat, ...), même si les agences européennes Europol et Eurojust montent peu à peu en puissance.

Surtout, il est notable de rappeler que si 43 Etats sont signataires de la Convention (dont quatre non membres du Conseil de l'Europe : les Etats-Unis, le Japon, le Canada et l'Afrique du Sud), seuls 14 pays ont procédé à son approbation. Si ce niveau de ratification est décevant, cet accord a néanmoins déclenché une tendance dans le sens d'une harmonisation des législations. Comme le cite en exemple Alexandre Seger à l'occasion de la conférence plénière d'ouverture du FIC 2010 « *La mobilisation européenne et internationale pour la lutte contre la cybercriminalité* » [51], le Sénégal et l'Inde ont ainsi adopté une législation conciliable avec la Convention de Budapest et Les Nations Unies proposent en ce moment l'élaboration d'une nouvelle convention au sujet de la cybercriminalité.

4.2 Vers une gouvernance de l'Internet adaptée

L'insertion d'une étude de la gouvernance Internet dans la présente publication résulte d'un constat simple : il s'agit d'un système assez unique, réellement multi-acteurs, gérant une ressource commune, complexe et désigné par plusieurs pays comme critique ou vitale.

L'histoire de l'Internet place sa genèse aux Etats-Unis. On sait aujourd'hui que cela est plus complexe et que les travaux de nombreux scientifiques, dont

51. `http://www.fic2010.fr/pdf/2010/conf_ouverture.pdf`

certains français, ont aidé à la naissance du réseau des réseaux. Il est tout à fait vrai néanmoins que le démarrage et l'évolution la plus rapide du réseau à ses débuts fut observée aux Etats-Unis et que ceux-ci ont très tôt pris les initiatives nécessaires à la mise en place d'un embryon de gestion qui deviendra par la suite la Gouvernance Internet.

Dans ce paragraphe, nous nous attacherons donc à dresser tout d'abord un panorama de la Gouvernance, de ses acteurs et de ses organisations. Par la suite, nous verrons quels sont les axes de progression et problématiques rencontrées par la forme actuelle de gouvernance de l'Internet.

Définition et acteurs de la gouvernance Internet

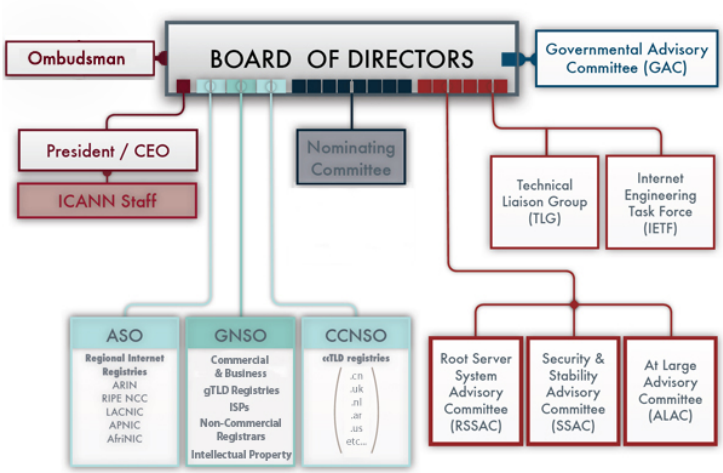
i) Définition La Gouvernance Internet est constituée de :

Processus Ex. : les différents processus d'échange d'informations, de mises à jour des zones, des serveurs entre registres et bureaux d'enregistrement.

Acteurs appelés « *multi stakeholders* » , les acteurs de la gouvernance Internet sont très divers et interviennent à différents niveaux au titre de leurs diverses qualités. Ex. : un individu peut intervenir à l'ICANN au titre de sa société, un bureau d'enregistrement par exemple, mais également à l'IETF au titre de sa compétence technique propre.

Organisations de nombreuses organisations émaillent la gestion de l'Internet. On notera cependant que certaines sont réellement au coeur tandis que d'autres gravitent à un niveau de périphérie plus ou moins proche. C'est donc un système cohérent qui gère et se coordonne pour gérer les aspects les plus cruciaux d'Internet, qu'ils soient politiques ou techniques. A cet égard, et considérant la diversité des acteurs impliqués et la diversité des questions traitées, la Gouvernance Internet fournit un microcosme très intéressant pour la gestion des infrastructures critiques.

ii) Fonctionnement de la Gouvernance a) ICANN



Source : ICANN

Cette vision de l'ICANN permet d'avoir un aperçu de l'ensemble des acteurs présents dans le système de la Gouvernance Internet. Notons cependant l'absence d'un acteur déterminant, IANA, pour Internet Assigned Numbers Authority qui correspond à la gestion plus opérationnelle de l'ICANN et de son périmètre. Ainsi, elle est chargée notamment de la gestion et de la maintenance du système DNS : elle constitue le point d'entrée unique pour tout changement notamment au niveau des root-servers et assure notamment le respect de règles prises par l'ICANN.L'organisation s'assure également de la gestion des autres « nombres » de l'Internet et notamment les adresses IP et les numéros d'AS (Autonomous Systems). Elle conserve la base de données de référence d'attribution des adresses IP et des numéros d'AS et constitue l'interlocuteur privilégié des attributeurs locaux d'adresses que sont les RIR (Regional Internet Registries), eux-mêmes regroupés dans l'Adress Supporting Organization (ASO, présente dans le schéma ci-dessus). C'est en dernier lieu l'organisation responsable de la gestion de ces ressources.

En revanche, l'IANA ne gère pas elle-même ces serveurs qui sont gérés par d'autres opérateurs parmi lesquels des organisations privées (ISC, Cogent Communications...), publiques (Department of Defense des USA, NASA) et même des universités. Ainsi, le A-root, racine du système DNS est géré par une organisation privée, Verisign qui gère par ailleurs un autre root-server ainsi que les domaines « .com » et « .net » [52].

Contrairement à une croyance répandue, il n'y pas « 13 serveurs racines de l'Internet ». Les besoins de sécurité du système ont induit une multi-

52. `http://www.root-servers.org/`

plication des serveurs en tant que tels et ils sont aujourd'hui 206 [53]. Il y a cependant encore moins de gestionnaires de root-serveurs puisque certains opérateurs en gèrent 2. Par ailleurs, certains organismes relèvent directement de l'autorité des Etats-Unis et en particulier la NASA et le DOD.

Au sein de l'ICANN, quatre autres acteurs sont remarquables :

- Le GAC pour *Government Advisory Committee* : cette organisation regroupe les représentants des différentes nations souhaitant s'investir dans la Gouvernance Internet. Cependant, la nature du comité (Advisory Committee) rend aléatoire sa capacité à faire adopter certaines mesures car il n'a pas lui-même une capacité de décision.
- L'ALAC pour *At-Large Advisory Committee* qui accueil des représentations des utilisateurs. Ainsi, des organisations de nature diverses assurant la transmission de la voix des utilisateurs se réunissent au sein de ce comité. Par ailleurs, et contrairement au « SO » (*Supporting Organization*), l'ALAC ne possède donc aucune capacité de décision en propre.
- gNSO et ccNSO : ces deux organisations possèdent une capacité d'action beaucoup plus importante notamment pour édicter des règles applicables au sein de leur communauté respective : les noms de domaines génériques (.com, .org...) et les noms de domaines correspondants au pays (.fr, .de,...). Le gNSO accueillera des entreprises privées, registres et bureaux d'enregistrement tandis que le ccNSO accueillera également des entités publiques impliquées dans la gestion des extensions « pays » .

b) ISOC et IETF L'ISOC est une organisation au positionnement intermédiaire. Sa mission principale consiste à mener des actions d'éducation et de sensibilisation, notamment auprès des pays et populations défavorisées pour les aider à entrer dans le monde numérique et à en utiliser ces opportunités pour leur développement. Cependant, l'ISOC est également détentrice du titre de registre du « .org » dont la gestion effective est assurée par une autre entité, PIR (*Public Internet Registry*). Par ailleurs, l'ISOC assure également les éléments d'organisation et offre un accueil pour les processus de l'IETF.

L'*Internet Engineering Task Force* (IETF) est une organisation de standardisation à qui l'on doit une majorité des standards utilisés d'Internet. Son format de publication est le RFC (*Request For Comments*). Très ouverte dans son fonctionnement elle aborde depuis peu des sujets moins techniques. Cette ouverture qui permet à tout utilisateur techniquement apte de suivre les débats pose cependant quelques difficultés car ce fonctionnement ne permet pas de compenser les effets de lobbying menés par

53. Source : `http://www.root-servers.org/`.Ces serveurs sont les points d'entrée sur l'Internet (*Gateway Internet eXchange* ou *Gix*) et, d'après *l'European Internet Exchange Association*, il existe 11 de ces serveurs principaux en France.

les constructeurs et éditeurs souhaitant voir la rédaction de tels standards prendre telle ou telle direction.

c) ONU, FGI et ITU L'ONU a souhaité s'impliquer plus récemment dans les questions de gouvernance Internet. Cette implications s'est faite en plusieurs étapes et ne peut être considérée comme achevée. Il est à noter d'ailleurs que dans le cadre de l'ONU et de façon relativement discrète, ont débutés des pourparlers entre la Russie et les Etats-Unis pour concevoir un traité relatifs aux attaques et à la prolifération des armes informatiques.

Dans le cadre de l'ONU les US et la Russie ont entamé des discussions relatives à la prolifération des armes informatiques.

Les deux « Sommet Mondial sur la Société de l'Information » ou SMSI ont ouvert une réflexion plus large encore entre les acteurs déjà évoqués au sein de l'ICANN. En 2003, puis 2005, à Genève puis Tunis ces deux sommets ont permis à de nombres organisations et acteurs se rencontrer.

Si la valeur opérationnelle de ces rencontres reste faible, ils ont permis la création du Forum sur la Gouvernance d'Internet (FGI) ainsi que d'autres initiatives plus sectorielles comme la lutte contre le SPAM ou l'accès à l'éducation numérique. Il est à retenir que d'autres SMSI ont eu lieu depuis 2006, avec moins de publicité, et notamment en 2010, à Genève.

Le FGI possède un mandat de 5 ans mais il est fort probable qu'il devrait être reconduit. Il permet à de nombreuses organisations d'échanger sur la Gouvernance Internet et son avenir. Le Conseil de l'Europe y participe par exemple depuis quelques années, notamment pour mettre en valeur son action en matière de lutte contre la cybercriminalité. Bien que très généraliste, le FGI ne possède aucun pouvoir de décision comme le prévoit l'Agenda de Tunis, ce qui laisse parfois songeur sur son utilité et son avenir.

FGI et SMSI relèvent chacun de l'ITU (*International Telecommunication Union*) qui gère notamment les relations entre Etats et opérateurs nationaux de télécommunications à propos des aspects techniques nécessitant une approche globale : fréquences, orbites satellitaires, fibres sub-océaniques.

Notons cependant, comme le font remarquer des habitués du « monde » de la gouvernance [54], que l'ITU a un fonctionnement assez lourd, typique des organisations internationales inter-étatiques et a été soigneusement tenu à l'écart des processus de la gouvernance Internet sur lesquels elle n'a que peu d'influence.

Au-delà de ses actions politiques, l'ITU souhaite se positionner comme un acteur incontournable de l'Internet en développant une activité de RIR (registre attributeur d'adresse) pour Ipv6. Par ailleurs, selon les mots de son secrétaire général, Hamadoun Touré [55], l'ITU souhaite se positionner comme une « Organi-

54. http://www.bortzmeyer.org/uit-rir.html

55. http://www.lemonde.fr/technologies/article/2010/02/03/la-seule-facon-de-gagner-la-cyberguerre-c-est-de-l-eviter_1300757_651865.html

sation des Nations-Unis du Cyberespace » permettant négociations et rencontres diplomatiques en vue d'éviter la cyberguerre.

Problématiques-clés Le système de gouvernance Internet est donc un système complexe où la multitude d'acteurs rend difficile les prises de décisions et les évolutions. Cependant, on ne peut nier que le système reste tout de même fortement résilient vis-à-vis des différentes crises qu'il a pu connaître et qu'il su faire preuve de capacités d'évolution non négligeables comme en témoigne la mise en place de DNSSEC.

En revanche, il est délicat de nier que la gouvernance aborde mal voire refuse d'aborder certaines questions. Si le paragraphe précédent a pu mettre en avant les succès de ce système et les solutions associées, celui-ci s'attardera donc aux questions non ou mal traitées.

Aspects techniques

De façon générale, on peut estimer que trois aspects de nature technique sont très mal approchés par la Gouvernance :

a. le routage

b. l'évolution de l'adressage

c. les capacités d'interconnexion

a. Le routage sur Internet demeure à ce jour un problème pour plusieurs raisons. D'une part, il oblige à une évolution constante et couteuse de matériels aptes à supporter notamment des bandes passantes croissantes mais des tables de routage de plus en plus lourdes.

De plus, la sécurité et la stabilité du routage reste encore aléatoire. Si, au sein des AS (*Autonomous System*), le routage reste une question plus facile à gérer, ce sont les zones intermédiaires qui posent problème. Ainsi, on connait bien les « failles » ou problématiques du protocole BGP. Plusieurs évènements restent ainsi en mémoire : celui de l'AS 7007 ayant annoncé en 1996 l'ensemble des routes de l'Internet. Très vite, le réseau s'effondre laissant les utilisateurs démunis. Plus récemment, en 2008, le Pakistan souhaitant bloquer Youtube a commis une erreur bloquant le site de vidéos pour une bonne partie de la planète.

Si un système actif de veille permet notamment de pallier à ce genre de problèmes, il reste un « best effort » . La création des points d'échanges pour Internet et leurs règles de gestion est ainsi un effort remarquable de gestion du trafic. Cependant, ces efforts ne peuvent rien contre les attaques contre BGP permettant notamment de détourner du trafic [56]. Même si l'IETF a pu

56. `http://blogs.orange-business.com/securite/2008/09/detournement-de-trafic-internet-via-protocole-bgp-fonctionnement-de-lattaque-partie-23.html`

rédiger d'autres versions plus sécurisées du protocole comme Secure BGP, certaines sont plus abouties que d'autres.

Le problème vient donc bien du système de gouvernance de l'Internet, *a priori* incapable d'imposer une évolution qualitative du routage.

b. On peut également faire une remarque identique à propos de l'adressage. La raréfaction des Ipv4 est depuis longtemps connue et le protocole successeur est finalisé depuis un certain temps aussi. Il s'agit bien évidemment d'Ipv6.

On peut extrapoler ici deux problèmes. Le premier est que la Gouvernance a échoué ici à impulser une politique de changement vers le nouvel adressage, la réaction naturelle des utilisateurs étant de conserver un adressage Ipv4 et en utilisant souvent des mécanismes de translation (NAT). Or, ces mécanismes de translation sont limités pour l'utilisation de certains protocoles.

Plus encore, l'interopérabilité des deux protocoles d'adressage est limitée ce qui oblige l'ensemble des acteurs (constructeur de matériels, de solutions, de logiciels. . .) a revoir la totalité de leurs produits. Et, si des fournisseurs d'accès peuvent avoir une politique éclairée en proposant dés à présent un adressage Ipv6, celui-ci reste limité et ne permet pas d'aller « directement » sur Internet. On en conclut sur la seconde incapacité de la gouvernance dans l'adressage : ne pas avoir su développer un protocole que l'on pouvait facilement adopter.

c. La dernière « faille » de la gouvernance concerne les capacités d'interconnexion. Tout d'abord, il est vrai que cet aspect relève notamment de l'ITU et que cette organisation n'a pas ou mal été intégrée à la gouvernance, limitant de fait, les capacités à coordonner certains efforts. Cependant, l'actualité encore récente a indiqué que plusieurs experts s'inquiétaient des capacités d'interconnexion pour le futur, au vu de la croissance forte de la bande passante induite par les nouveaux usages. Plus exactement, on constate une baisse constante du ratio de la bande passante utilisée sur la bande passante disponible.

Enfin, on notera que pendant très longtemps, l'Afrique a été victime d'un monopole sur une unique infrastructure de fibre optique « entourant » le continent et limitant la diversité des offres. Cet état de fait devrait prochaine changer mais a longtemps perduré, rendant ainsi les offres Internet par satellite plus abordable.

Légitimité

Le système actuel de la gouvernance Internet présente actuellement une forme persistante de crise de légitimité. Cette crise provient, selon notre analyse, de trois causes :

a. les relations privilégiées avec les Etats-Unis

b. le manque d'efficacité

c. l'apparition de formes sévères de conflictualité

a. **L'ICANN notamment, a toujours eu des liens assez forts avec le gouvernement des Etats-Unis et en particulier, le *Department of Commerce.*** Le renouvellement, sous une forme allégée sans doute, d'un document contractuel n'a pas su dissiper les inquiétudes. Plus encore, les opérateurs des root-servers restent encore profondément ancré aux Etats-Unis voire même sont des acteurs déterminants de la dite administration (Department of Defense, NASA). Enfin, le système de gestion du tout premier des root-server bénéficie d'un encadrement contractuel encore flou dont on trouve très peu de traces dans les archives légales de la gouvernance. Cette relation n'est donc pas de nature à renforcer la confiance en ce système, confiance qui parait pourtant essentiel et donc l'absence a pu être une des causes de certains échecs signalés ci-dessus (adressage par exemple).

   Par ailleurs, cette crise a encore été très visible lors de la mise en place du système de gestion des clés de chiffrement utilisées pour DNSSEC ou encore lors de la mise en place des noms de domaine internationalisés.

   Cette problématique de confiance et de légitimité pose un problème de capacité du système de gouvernance à relever les défis à venir pour la gestion d'Internet Ainsi, pour Stanislas de Maupeou, ancien chef du CERT-A et actuellement chef du projet « Cyberdéfense » chez Thalès, le temps est venu de ne plus dépendre de l'Icann pour la gouvernance de l'Internet, et *de s'appuyer sur une organisation internationale et supranationale reconnue par tous (. . .), chaque pays gérant par subsidiarité ses propres noms de domaine.* » [16]

b. **Le manque d'efficacité** du système de Gouvernance Internet est régulièrement pointé du doigt, souvent pour marquer le manque d'avancement d'un projet important ou pour indiquer que le statu quo est dommageable pour l'ensemble des utilisateurs.

   On ne peut nier que l'ICANN reste une institution produisant nombre de documents et de propositions et dotée d'une certaine capacité de réaction. Dans le cas de la pratique dite de « *domain testing* » dommageable pour l'ensemble des acteurs et constitutive d'une fraude, les différents acteurs ont pu réagir relativement rapidement pour proposer et mettre en place diverses solutions.

   Ces critiques d'inefficacité renvoient pour partie à des aspects techniques comme la question de l'adressage ou du routage dont le statu quo préserve une situation dangereuse à court ou moyen terme. Elle peut également concerner des politiques mal orientées comme celle de la gestion des clés de chiffrement de DNSSEC ou encore les choix faits pour les noms de domaine internationalisés.

   Plus généralement toutefois, c'est une forme d'immobilisme et d'inflation organisationnelle qui est condamnée. Ainsi, la création du SMSI puis du FGI ainsi que de multiples organisations sectorielles conduisent à un nombre sans

cesse grandissant de rencontres et autres forums dont les résultats ne sont pas forcément tangibles. Ainsi, après 5 ans de FGI, les résultats concrets se font toujours attendre et l'ICANN reste encore très liée au gouvernement des Etats-Unis malgré les demandes répétées de plusieurs pays.

On trouve cependant un discours différent défendant notamment le statut particulier de l'ICANN contre celui de l'ITU par exemple. Cette opinion défend ainsi le fait qu'une organisation internationale traditionnelle serait tout à fait incapable d'être aussi réactive que peut l'être l'ICANN. Il n'en reste pas moins qu'un nouveau modèle plus neutre encore constitue une attente forte.

c. Cette neutralité reste une demande forte alors que de nouvelles formes de conflictualité apparaissent de plus en plus nombreuses. De nombreux analystes pointent ainsi un retour en force du politique sur Internet, que ce soit pour l'aspect militaire (lutte informatique offensive et défensive) ou policier (lutte contre les trafics, la cybercriminalité). Ce retour du politique est causé notamment par la prégnance de l'outil Internet mais également par l'incapacité du système de gestion actuelle à réguler ces usages déviants.

Ainsi en est-il des différents accords en cours de négociation entre différents pays, notamment Russie et Etats-Unis pour le règlement l'usage des « armes » dans le cyberespace. L'OTAN s'est également fortement impliquée dans ces questions avec la création d'un centre d'expertise à Tallynn en Estonie et la récente création d'une division « Défis de Sécurité Emergents » prenant en compte la « cybersécurité » .

Si la sécurité a été largement prise en compte par les membres de l'IETF dans de très nombreux travaux, cette organisation s'est par exemple toujours refusée de prendre un parti politique quelconque. Toute discussion de ce type y est bannie.

Au contraire, l'ICANN est assez fortement politisée mais le monde de la « cybersécurité » ne s'y retrouvait pas forcément jusqu'à la nomination de son actuel dirigeant. Rod Beckstrom, en effet, a été un temps dirigeant du NCSD (*National Cyber Security Division*) du DHS, que nous évoquions ci-dessus. Ce « mélange des genres » n'est donc pas de nature à conforter l'équilibre délicat de la Gouvernance notamment vis-à-vis d'un système qui attire très fortement des acteurs politiques peu concernés par le système de gouvernance.

La « Gouvernance Internet » représente donc un système multi-acteurs de gestion tout à fait original et unique en son genre. Capable de faire travailler ensemble de très nombreux acteurs très divers, il a réussi à maintenir et à faire évoluer tant bien que mal un système technique relativement complexe et cependant non prévu pour atteindre une telle dimension. En cela, elle fournit des leçons à retenir pour la gestion complexe de tout système critique.

Bien que ses succès soient incontestables, la Gouvernance Internet est également faillible en de nombreux points, fournissant ainsi des pistes d'améliorations pour tout gestionnaire global des infrastructures vitales. Elle constitue, en dernier lieu, un point d'intérêt absolu pour toute autorité qui devrait reconnaître la nature vitale dudit système.

5 Conclusion

Les preuves indiquant que des cybercriminels pourraient provoquer des pannes majeures et menacer des pans entiers de nos infrastructures vitales avec un minimum d'efforts ne manquent pas et il est aisé de construire des scenarii d'attaques mettant en oeuvre des moyens réalistes. Ainsi, réclamé depuis plusieurs années et désormais avec de plus en plus de force par tous les acteurs, le partenariat public-privé doit aujourd'hui monter en puissance. En effet, la présente étude aura montré plus précisément en quoi les dispositifs en vigueur dans ce domaine ne sont que partiellement efficaces, chacun des schémas présentés possédant bien sûr des qualités mais aussi des insuffisances (voire des lacunes) persistantes. Ainsi conscients des limites inhérentes aux approches proposées, et en particulier à la dimension internationale de la problématique visée ici qui constitue l'un des écueils majeurs à dépasser, une seconde entreprise aura permis de tirer des enseignements sur des domaines particuliers dont la régulation nécessite une coopération effective entre de multiples partenaires internationaux (droit de la mer, gouvernance Internet ...).

En définitive, ces développements nous conduisent peu à peu à dessiner les contours de la nécessaire approche de la sécurité des OIV. En effet, la vision actuelle de la sécurité, notamment informatique, se conçoit comme une approche globale mais qui reste encore une sécurité largement « auto centrée » . Or, dans le cadre des organismes d'importance vitale, les scénarios d'attaques mettent généralement en lumière l'interdépendance des acteurs impliqués et invitent en conséquence à repenser la sécurité, qu'elle soit informatique ou autre, dans une approche non seulement globale (physique, informatique, logique, humaine...) mais également dans une approche multi-acteurs. Au final, dans cette approche de la sécurité de « tous par tous » , où la sécurité de l'un garantit alors, pour partie, la sécurité de l'autre, le partenariat public-privé se veut un axe de réponse déterminant pour renforcer la résilience des organismes, et pour lequel des efforts importants doivent encore être rapidement investis.

Références

1. The Economist, « Cyberguerre, la menace venue d'Internet » - couverture du numéro du 3 juillet 2010 repris dans la revue Courrier International (n° 1034 - 26 août au 1er septembre)
2. Larcher S.. : La Chine est en cyber-guerre de puis 10 ans. Dans : Mag Securs n° 26, pp. 10-11 (2ème trimestre 2010). Article s'appuyant lui-même sur le rapport américain : Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation (octobre 2009) - http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf [FR]
3. Livre blanc sur la Défense et la Sécurité nationale. Sous : http://www.livreblancdefenseetsecurite.gouv.fr/information/les_dossiers_actualites_19/livre_blanc_sur_defense_875/index.html

UK National Security Strategy of the United Kingdom (2008) - http://interactive.cabinetoffice.gov.uk/documents/security/national_security_strategy.pdf

UK An Information sharing vision to improve Internet Security : the Warps (2002) - http://www.warp.gov.uk/Marketing/WARPs.pdf

UK Cyber Security Strategy (2009) -

UK Sur les OCS et les CSOC : http://www.cabinetoffice.gov.uk/media/216620/css0906.pdf, http://www.cabinetoffice.gov.uk/reports/cyber_security.aspx

GER National strategy for Critical Infrastructure Protection (CIP strategy), juin 2009 - http://www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf

US DHS, National Strategy to Secure Cyberspace - Sous : http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf

4. Ciupa D., La sécurité des industries sensibles, un sujet . . . sensible. Dans : Mag Securs n° 26, pp. 23-26 (2ème trimestre 2010)
5. Rapport 2007-2008 de M. Roger Romani : « Cyberdéfense, un enjeu de sécurité nationale » : chapitre II (pp. 20 et suivantes), « La France est encore insuffisamment organisée et préparée »
6. Rasle B., La sécurité des données personnelles enfin prise au sérieux ? - AFCDP, février 2010. Sous : http://www.globalsecuritymag.fr/IMG/pdf/Article_Bruno_Rasle_Notification_Atteintes_Donnees_Personnelles_28_fevrier_2010.pdf

7. Caprioli E., Les notifications de violation de données à caractère personnel et le droit : des questions en suspens. Dans : Communication Commerce Electronique, revue mensuelle LexisNexis Jurisclasseur, mai 2010.
8. Dossier législatif relatif à la proposition de loi Detraigne-Escoffier : `http://www.senat.fr/dossier-legislatif/ppl09-093.html`
9. Communication de la Commission sur un programme européen de protection des infrastructures critiques (décembre 2006) - `http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:FR:PDF`
10. De Maupeou S., Internet, nouvelle infrastructure vitale ! : revue Défense nationale et Sécurité collective, pp.57-65 (mars 2009)

Rappel des principales abréviations applicables au schéma français

ANSSI Agence Nationale de la Sécurité des Systèmes d'Information

DNS Directive Nationale de Sécurité

OIV Opérateurs d'Importance Vitale

PIV Point d'Importance Vitale

PSO Plan de Sécurité Opérateur

PPE Plan de Protection Externe

PPP Plan Particulier de Protection

SAIV Secteur d'Activité d'Importance Vitale

Deuxième partie

Cyber Security of Process Control Systems in Critical Infrastructure

Igor Nai Fovino

EC DG JRC IPSC, Ispra, Italie Igor.Nai(@)jrc.ec.europa.eu

Industrial Critical infrastructures and systems (power plants, energy grids, oil pipelines etc.) are today exposed not only to traditional safety and availability problems, but also to new kinds of security threats. These are mainly due to the large number of new vulnerabilities and architectural weaknesses introduced by the extensive use of information and communication technologies (ICT) into such complex systems. Today the process control network of most Critical Installations is integrated with broader information and communication systems, including the company business network. Most maintenance services on process control equipment are remotely performed. There has been a qualitative leap in the last years regarding the need to safeguard those installations against malicious activities by actors as terrorism, organized crime or violent extremism. On the one hand, security conditions suffered a drastic change the after September 11, 2001. On the other, the intensive use of ICT has opened new ways for carrying out attacks.

The paradox is that the more ICT systems are used, the more opportunities there are for intrusions by external and internal malicious actors. A violation of the integrity, availability or even the confidentiality of data might produce significant damage to assets of the company and be part of a broader aggressive action involving material offense. These situations cannot be ignored because the potential consequences of an incident can be severe (e.g. the cost of a power plant shutdown is huge and release of pollutants from a plant in the environment can provoke vast damages).

The core of Industrial Critical Infrastructures is the so called Supervisory Control and Data Acquisition (SCADA) system. The ICT security of control systems is an open and evolving research field. Adam and Byres [1] presented an interesting high level analysis of the possible threats to a power plant system, a categorization of the typical hardware devices involved, and some high level discussion about the intrinsic vulnerabilities of common power plant architectures. A more detailed work on the topic of SCADA security, is presented by Chandia, Gonzalez, Kilpatrick, Papa and Shenoi [2]. In this work, the authors describe two possible strategies for securing SCADA networks, underlying that several aspects have to be further improved. What is evident in primis is that communication protocols used in such systems, (e.g. Modbus, DNP3 etc.) were not conceived for dealing with typical ICT threats. This is due to the fact that when they were designed, the world of industrial control systems was completely isolated

from public networks, and then ICT based intrusion scenarios were considered completely negligible. Some work has been done regarding the security of such specialized communication protocols : for example, Majdalawieh, Parisi-Presicce and Wijesekera [3] presented an extension of the DNP3 protocol, called DNPsec, which tries to address some of the known security problems of those control protocols (i.e. integrity of the commands, authentication, non repudiation etc.). A similar approach was presented by Heo, Hong, Ju, Lim, Lee and Hyun [4], while Mander, Navhani and Cheung [5] presented a proxy filtering solution aiming at identifying and avoiding anomalous control traffic.

All those papers underline how SCADA systems, and generally speaking industrial process control systems, are at the moment exposed to ICT threats. These attacks can be categorized into two classes :

1. Classic ICT attacks : attacks that take advantage of vulnerabilities typical of general purpose ICT systems. Those attacks can be usually mitigated by adopting ICT countermeasures like firewalls, antivirus, patches etc.
2. Specific industrial ICT attacks : attacks that take advantage of vulnerabilities which are specific of industrial ICT systems. Example of these vulnerabilities can be for example the lack of authentication and integrity check of several of the most used SCADA communication protocols [6].

The recent detection of Stuxnet, the first known malware developed to directly impact on process control systems taking advantage of the peculiar vulnerabilities of those installations, brought the attention of government bodies on the cyber-exposure of Critical Installations to cyber-threats.

Due to the peculiarities of industrial systems, traditional ICT countermeasures cannot always be deployed efficiently in all environments, or worst - as in the case of attacks of the second class described before - are totally inadequate. Moreover, even in the case in which countermeasures are successfully deployed, the risk of exposure to new unknown attacks, for which traditional signature based security applications are not effective, always exists. Considering the role in the life of the citizen of the so called ŞCritical InfrastructuresŤ, this exposure is unacceptable.

Under the light of the previous considerations, the Cyber Protection of Critical Installations at global level has to go through three mandatory steps :

1. In deep study and understanding of the interdependencies among different critical infrastructures (Energy-Telecommunication-Transport etc.), i.e. need for systematic approaches in the analysis of complex systems of systems. [7]
2. In deep vulnerability analysis and testing of critical infrastructures. This implies the design and development of protected environments where reproduce on field tests allowing to gather as much information as possible on the effects of new attacks against process control systems. [8]

3. Design of new ad-hoc tailored countermeasures to protect those systems (e.g. lightweight cryptographic schemes for SCADA protocols, Critical State based intrusion detection mechanisms etc.) [9]

Bibliography

[1] Creery, A., Byres, E. : Industrial Cybersecurity for power system and SCADA networks. IEEE Industry Apllication Magazine (July-August 2007)

[2] Chandia, R., Gonzalez, J., Kilpatrick, T., Papa, M., Shenoi, S. : Security Strategies for Scada Networks. In : Proceeding of the First Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, Dartmouth College, Hanover, New Hampshire, USA, March 19-21 (2007).

[3] Majdalawieh, M., Parisi-Presicce, F.,Wijesekera, D. : Distributed Network Protocol Security (DNPSec) security framework. In : Proceedings of the 21st Annual Computer Security Applications Conference, Tucson, Arizona, December 5-9 (2005)

[4] Hong, J.H.C.S., Ho Ju, S., Lim, Y.H., Lee, B.S., Hyun, D.H. : A Security Mechanism for Automation Control in PLC-based Networks. In : Proceedings of the ISPLC 2007. IEEE International Symposium on Power Line Communications and Its Applications, Pisa, Italy, March 26-28, pp. 466-470 (2007)

[5] Mander, T., Nabhani, F., Wang, L., Cheung, R. : Data Object Based Security for DNP3 Over TCP/IP for Increased Utility Commercial Aspects Security. In : Proceedings of the Power Engineering Society General Meeting, Tampa, FL, USA, June 24-28, pp. 1-8. IEEE, Los Alamitos (2007).

[6] I. Nai Fovino, A. Carcano, M. Masera, A. Trombetta : Experimental Proof of Malware Attacks on SCADA Systems. International Journal of Critical Infrastructure Protection. Ed. Sujeet Shenoi. Vol. 2, Issue 4, pp. 135-144, 2009, Elsevier.

[7] I. Nai Fovino, M. Masera, A. DeCian : Integrating Cyber Attacks within Fault Trees. International Journal of Reliability engineering & System Safety. Ed. Terje Aven, Elsevier 2009. Volume 94, Issue 9, September 2009, Pages 1394-1402.

[8] I. Nai Fovino, M. Masera, L. Guidi and G. Carpi :An Experimental Platform for Assessing SCADA Vulnerabilities and Countermeasures in Power Plants. In Proceedings of the IEEE 3rd International Conference on Human System Interaction, May 13-15, 2010, Rzeszow, Poland.

[9] A. Carcano, I. Nai Fovino and M. Masera : Modbus/DNP3 State-based Filtering System. In Proceedings of the IEEE International Symposium on Industrial Electronics. July 4-7, 2010, Bari, Italy

Du profilage commercial à l'espionnage industrialisé

Dominique L.R. Chandesris

ANSSI

Résumé Il est rappelé ici comment, malgré une résistance importante exprimée par es consommateurs internautes [ref1] la collecte systématique et le profilage de leurs activités marchandes et non marchandes a été maquettée et réalisée sur le web et l'internet que nous connaissons aujourd'hui pour s'inscrire dans le web des applications qui commence avec tablettes et ordiphone. Comme il n'y a pas de séparation nette recommandée entre les activités professionnelles et les activités personnelles sur internet, du moins dans la pratique, il apparaît que cette récolte d'information peut servir beaucoup d'autres objectifs centrés sur l'activité industrieuse (celle des professionnels) [ref2]. Peu d'éléments échappent à une analyse continue sans oubli de l'activité quotidienne d'une personne si on la relie à son activité professionnelle ou celle de son entreprise et ce bien au-delà des remarques faites par les médias sur le profilage pour le recrutement. La gestion du consentement [ref3] est probablement la prochaine étape de notre asservissement à la société marchande : le modelage de l'expression de la pensée à travers les outils de l'interactivité en réseau semble prometteur pour nos apprentis sorciers [ref4] captology]. Y a-t-il une raison de vouloir échapper à cette douce et confortable tyrannie : probablement la dignité du charbonnier qui paie par son isolement l'accès à une pensée autonome qui prend le temps de mûrir avant de mourir et à la défense des sans voix. Y a-t-il des moyens de retourner ce pouvoir de l'innervation par les réseaux, sans que le coût du compromis à notre dignité individuelle et collective soit trop élevé ? Des moyens techniques circonstanciels, une prudence de bêta, un retournement des affirmations utilisées, voire une quête des motivations sont utiles mais ne remplacent pas la recherche inlassable du sens et le retrait indispensable (accepter d'être et de rester un plouc) au décalage créateur préparant ou anticipant le futur.

Avertissement: Cette petite étude de technicien ne s'adresse qu'au grand public et ne traite aucunement le cas de l'entreprise ou de l'organisation dont les données critiques ou stratégiques sont explicitement ciblées y compris à travers son personnel.

1 Introduction

Si la protection des systèmes d'information, extensions mécanisées de l'organisation des activités humaines, repose d'abord sur le maillon humain, celui-ci est victime d'agressions spécifiques mécanisées préparées par un profilage systématique sur internet qui s'industrialise progressivement.

L'activité du commerce et de la publicité justifierait aux yeux de certains l'extraction d'informations concernant la sensibilité à la publicité ciblée et le potentiel d'achat (impulsif ou non) des personnes. Par ailleurs, la facilité d'accès au contenu des échanges, indexés et filtrés par certains services en échange de

la gratuité (pensez à GMail [ref5]) fait l'objet non de phantasmes mais de réalités opérationnelles uniquement limitées par le coût des puissances de calcul non numérique disponible.

Il semble apparemment que l'internet fut un bénéfice pour l'accès aux communication des centres de recherche puis des entreprises. D'une part l'instabilité du réseau internet pouvait permettre dans les années 80 et 90 le détournement de communications internet hors du territoire français ou européen et le transit de communication internet de l'Europe vers l'Extrême-Orient se faisait à travers l'Amérique du Nord. Plus tard l'oligopole des moteurs de recherche Google-Bing, sauf en Chine, a permis un suivi de la dynamique des intérêts des internautes à la fois sur les éléments commerciaux et sur les sujets généraux (grippe porcine, ...).

Alors comment maintenir cette collecte si juteuse commercialement et utile pour comprendre des vagues de fond sinon par une diversification des moyens de collecte qui s'enrichit maintenant des applications :

- les premiers éléments sont des applications/services gratuits comme GMail qui accède lui explicitement aux contenus,
- la deuxième étape est constituée des éléments d'applications dites de réseaux sociaux (Orkut, Myspace,Twitter, Facebook„ ...) qui transforment les forums ("newsgroup") en base de données à la propriété incertaines
- la troisième est constituée des applications fermées sur les tablettes dont les remontées d'informations sont bien moins visibles et contrôlables que celles qui sont présentes dans les navigateurs.

Le conflit entre les opérateurs dépossédés de leur avantage en bande passante et leurs prédateurs, acteurs du service à valeur ajoutée comme Google, Skype et d'autres (FaceBook, Twitter, ..) traduit clairement la fuite en avant d'un modèle économique instable et bricolé. (voir l'affaire Phorm/NebuAd, ainsi que toutes les discussions autour de la neutralité de l'internet).

Une analyse sémantique, technique et économique de cette tendance à la capture de profils d'intérêts dynamiquement remis à jour est nécessaire pour mieux comprendre et maîtriser ce qui nous attend , voire que nous subissons déjà.

Comment préserver le caractère privé de mes activités et de mes relations, le droit à à la recherche et l'exploration sans être victime de jugements à l'emporte-pièce ? Comment ne pas transmettre les sélections d'articles de pages et la dynamique associée aux fournisseurs de services fussent-ils gratuits ?

Si je n'ai rien à cacher, je ne me sens cependant pas à l'aise, corseté dans les définitions élaborées à partir des données recueillies, à mon insu, sur ma personne et mes activités car je ne contrôle plus mon image.

La situation est telle qu'une refonte de la protection des données personnelles est lancée aux USA par l'industrie, par peur de la régulation qui se profile, en Europe par la Commission Européenne. Certains envisagent même, au delà du traité

de Budapest sur la cybercriminalité et son annexe, un traité internet qui comprendrait nécessairement des règles concernant ce type de collectes d'information touchant au respect des personnes humaines et de leurs organisations

2 Le web n'est pas limité au portail Google : voilà !

La pratique observée de l'usage naïf de l'internet est tout simplement : "je ne sais pas, je mets un mot dans Google et je trouve quelque chose qui peut me convenir" : c'est tout simplement considérer Google comme le portail sur Internet.

La conséquence claire est que l'on ne s'interroge pas naturellement sur les limites de Google : sur ce que l'on ne trouve pas, sur pourquoi on ne le trouve pas ...ni sur le prix qu'on paye pour cela (y a-t-il vraiment des déjeuners gratuits ?)

Il faut lire à ce sujet deux excellents ouvrages critiques sur Google (il faut aussi attendre ou bien écrire un ouvrage équivalent sur Bing ex LiveSearch de MicroSoft) :

Ce que nous montrent ces ouvrages c'est comment Google détiendrait aujourd'hui un pouvoir excessif de façonner les flux d'informations qui parviennent aux internautes qui acceptent par confort le filtrage par les services offerts gratuitement.

En effet, en recueillant les informations recherchées et en utilisant des statistiques sur les éléments trouvés pertinents, il façonne non seulement une opinion moyenne en tolérant des anomalies nombreuses, mais il profile les intérêts de l'internaute et leur dynamique. Ce mécanisme est certes un pas vers une intelligence en coopération, mais montre rapidement ses limites par exemple en assistance à la traduction quand on compare avec des outils plus professionnels victimes d'une concurrence par la médiocrité due aux limites des statistiques.

Ce qui n'est pas vu directement à travers Google, qui déguise son indexation très rapide en exhaustivité, peut souvent être trouvé sur Internet avec un peu d'opiniatreté, de perspicacité, de jugement, de sens linguistique -le choix des mots- et de sens pratique.

Parfois même, ces techniques permettent de retrouver des éléments intentionnellement effacés, comme par exemple la trace des maîtres d'ouvrage des systèmes de billettique qui auraient fait un emploi imprudent des puces Mifare Classic selon leur producteur NXP et seraient seuls responsables des vulnérabilités systémiques associées et encore présentes.

3 Le règne des applications, des ordiphones et des tablettes : la nouvelle violence commerciale

Apple, Androïd, BlackBerry, Nokia, et les magasins d'applications et de données - AppStore- : qui contrôle quoi au service de quels objectifs ?

Sur les tablettes et les ordiphones, coexistent pour l'instant des navigateurs internet quasi-classiques et des applications fermées offrant un plus grand confort de lecture et de mémorisation, mais pouvant conduire à des achats impulsifs. Sachez que votre carte bancaire est connectée en permanence à votre iTunes Apple Store (verrouillez le donc doublement) ou autre magasin.

Plus que cela, les services rendus font l'objet d'une commercialisation (ou d'une gestion de la sécurité) très différente voire dérangeante : sur Amazon Kindle comme ordiphone Androïd, les objets virtuels ne sont pas les vôtres : leur mise à disposition est révocable pour raison juridique [Kindle] ou sécuritaire [Androïd]. Le terminal semble complètement contrôlé par les prestataires de services mais d'abord pour leurs besoins propres.

L'exemple de la localisation est le plus caractéristique : alors que le suivi du parcours d'une personne est perçu par tous comme une intrusion grave dans sa vie privée, sous des prétextes de confort et de commodité ("best user experience") ce type d'information est accessible aux prestataires de service dont certains [Androïd Apps] ont la politesse de solliciter une autorisation générale [Apple iPhone], et mais jamais spécifique à chaque requêtece qui semblerait tout à fait normal [CNIL] mais légèrement inconfortable.

De plus les applications et les services associés sont conçus, construits et fournis au moindre coût c'est à dire parfois sans souci suffisant de protection des données détenues (y compris personnelles [RockYou 2009]) faute d'obligation légale, en particulier dans l'univers anglo-saxon : le nombre des incidents ayant touché FaceBook et certaines applications est là pour en attester.

Une solution partielle utille : pourquoi ne pas couper son ordiphone portable dans la plupart des circonstances, créant ainsi des blancs dans les données dont vous faites cadeau à vos prestataires de service (réunions, rendez-vous, visites privées) sans compter la protection contre la transformation en micro intempestif pour les personnes vraiments ciblées ou paranoïaques ?

La vraie question reste la suivante : comment tracer et identifier les flux sortants et entrants dans des tablettes et des ordiphones ? comment installer une application vraiment utilisable pour ce faire dans le système de communication de l'ordiphone ou de la tablette ? (sur le terminal ou le serveur d'accès). L'opérateur ou les prestataires de services ont-ils un intérêt à le faire ? voire à le permettre ?

Une utilisation des réseaux locaux avec outils (filtres et journaux) ? Des gardes barrières personnels pour les appareils terminaux ? Un dialogue organisé entre les techniciens spécialistes et grand public ?

4 Les moyens de la dignité : comprendre les mécanismes techniques et les mécanisme de pousse à l'achat (séduction)

La liberté de parole absolue souvent revendiquée aux États-Unis au nom du premier amendements n'existe pas, il existe une limite liée au respect de la dignité des personnes perçue et pratiquée de façon différente entre les continents [Whitman 2004]. Si les systèmes du droit sont différents des deux côtés de l'Atlantique, et les pratiques différentes, les valeurs essentielles promues au nom de l'humanité sont-elles exactement identiques ? Quelles en sont les conséquences techno-économiques et juridiques ? (probablement plus importante que la séparation du thème racisme et xénophobie dans une annexe du traité de Budapest , facultative)

1. Les mécanismes économiques évoluent
2. Les supports techniques s'affinent
3. L'important est de rester un agriculteur de l'internet : pour y produire et consommer des informations, il faut maîtriser ses propres outils et leurs principes, parfois complètement, en maintenant une distance critique ; y conserver une activité industrieuse (typique de l'agriculture confer Arrighi) comme dans sa propre bibliothèque ou dans une bibliothèque publique.
4. Comment détecter les fuites d'informations
5. Comment freiner, voire interdire, ces fuites d'informations
6. Comment ne pas être dupe du potentiel d'industrialisation de ces processus.

5 L'action patiente et le retournement des moyens

La vigilance des spécialistes et des techniciens ne suffit plus si elle reste absolument nécessaire pour détecter les pratiques douteuses, et inventer les moyens de les dénoncer, de les freiner, sinon de les empêcher.

Il n'est pas question ici des mécanismes de mise à jour des applications et des systèmes qui doivent être disséqués par des spécialistes et expliqués aux utilisateurs pour que ces derniers puissent faire des choix éclairés.

Par contre, il est intéressant de signaler que la chasse à la collecte déloyale de données de parcours ou de manifestation d'intérêts des internautes s'affirme et s'outille, malgré la mobilité ingénieuse de certains prestataires de services.

L'action publique :

L'action technique : Bloquer les requêtes qui transmettent des informations sans l'accord de l'internaute. **Seul ce qui est nécessaire à l'obtention du service demandé, fut-il gratuit, doit être dispensé d'autorisation explicite de l'internaute.**

- le blocage des requêtes indésirables par un filtre technique au niveau de l'appareil (bloquer le port 443 :HTTPS, ou mieux n'autoriser que les ports et les @IP dont on est sûr : liste blanche). La fonction est réalisée par des gardes-barrières personnels voire spécifiques par applications. Bien sûr ceux-ci ne doivent pas augmenter la fragilité du terminal ni obérer sa facilité d'emploi.
- le blocage des requêtes indésirables par un filtre sur les noms symboliques dans le navigateur ou par application,
- la journalisation des décisions, des blocages et des passages réalisés pour examens éventuels par des spécialistes.

Aujourd'hui bien plus qu'un antivirus, ou un antispam qui se préoccupent de ce qui entre et serait déjà reconnu comme dangereux ou gênant, la surveillance des sorties de données par application est l'élément critique de la protection sur Internet que ce soit sur poste de travail, sur ordiphone ou sur tablette.

Les applications qui existent soit sous forme autonome (gardes barrières avec filtres par applications) soit sous forme d'extensions à des navigateurs Firefox, Safari e.g. AdBlockPlus, Ghostery, ...) progressent vers des facilités d'emploi acceptables malgré la réflexion nécessaire et irréductible à toute décision qui parasite le travail en cours.

Google a rendu les dispositifs qui s'appuient sur la seule adresse IP obsolètes : l'accès à certains services gratuits de recherche n'a plus été possible dans le cas l'on bloque certains accès (dont le nom symbolique restait clair) aux actions indésirables : en effet les serveurs correspondants n'étaient pas spécialisés

quelques tableaux sont données en annexe : Attention les données varient très rapidement au cours du temps, et, pour l'instant, les collectes de données restent visibles avec un effort moyen. en annexe A des données recueillies par Little Snitch en annexe B des marqueurs repérés sur des pages caractéristiques

6 Conclusion : de l'origine des pouvoirs aveugles ou du mauvais usage des statistiques

Pour pouvoir influer légèrement sur l'évolution harmonieuse des forces en présence un gouvernement se doit de les comprendre et d'anticiper leurs mouvements : le recueil de leur expression naissante à travers les personnes (individu statistique) peut se révéler utile si le travail sur le sens est effectué à un niveau de qualité suffisant.

Or dans l'univers de l'internet qui désarticule celui de la télévision canal primitif de l'audiovisuel, les pressions de conformité sont transmises par des mécanismes plus subtils. Il est fait appel à la fugacité (règne de l'immédiat), à la rareté des informations (des informations disparaissent : confer l'enquête sur le non respect par la puce de sécurité MiFare du principe cryptographique de Kerckhoff -"le seul

secret cryptographique doit être la clé"- qui révèle le partage de responsabilités effacé sur internet)

L'analyse des émotions immédiates dans les éléments de micro-bloc-notes (Twitter, identi.ca) est aujourd'hui industrialisée sous deux aspects : l'indexation rapide (en temps-réel), et l'analyse statistique.Si elle n'est pas complée par des analyse de sens, il peut se produire des incidents regrettables résulatnt de jugement à l'emporte-pièce.

Les personnes, en particulier les citadins, ont apprécié le relatif anonymat de la ville ; sur internet, ils se retrouvent à la campagne observés de toutes parts, il vont donc prendre des précautions et ne pas se laisser piéger par des mécanismes qui les conduisent à exposer l'intégralité de leurs pensée à travers leurs mouvements et leurs actions.

Qui connait la liste des livres que vous empruntez en bibliothèque ? Qui connaît et conserve vos équations de recherche sur Internet et vos réactions exprimées ? Qui peut anticiper vos futures réactions ? Pour quel raison ou cible financer tout cela ?

Évaluer la sécurité face au risque stéganographique

Johann Barbier[1] et Emmanuel Mayer[2]

Novetix, laboratoire de stéganographie
5, rue du Général Leclerc, 35 580 Guichen, France
johann.barbier(@)novetix.fr

DGA Maîtrise de l'Information, département Analyse de la Menace Informatique
La Roche Marguerite, BP 57 419, 35 174 Bruz Cedex, France
emmanuel.mayer(@)dga.defense.gouv.fr

Résumé Dans cet article, nous présentons les concepts généraux de la stéganographie et montrons comment elle peut permettre la compromission d'information stratégique pour l'entreprise. Nous détaillons ensuite les méthodes génériques pour évaluer le risque de fuite d'information et mettons en évidence les limites des techniques de détection d'information cachée. Nous expliquons enfin le concept *d'indistinguabilité indéniable* et mesurons l'impact de celui-ci dans l'évaluation des dommages lorsque des incidents de sécurité mettant en cause l'utilisation de techniques de stéganographie sont détectés.

Mots-clés: stéganographie, sécurité, indistinguabilité indéniable.

Introduction

Loin de ses origines philanthropiques ancrées dans la communication et le partage des connaissances, Internet a trouvé sa place au centre d'un nouveau modèle économique amenant la mondialisation à la portée de tous les acteurs économiques. Aujourd'hui, le producteur local a ainsi la possibilité de vendre et se faire connaître aisément à l'international *via* un simple site internet. Dans ce contexte hautement concurrentiel, la maîtrise de l'information est vitale pour s'adapter à un marché qui évolue vite et où l'innovation et le savoir faire sont les clés de la réussite. C'est ainsi que l'on parle de guerre économique. Cette guerre est relayée sous diverses formes sur la toile : attaques virales, en disponibilité de services, en désinformation et en piratage en tous genres. Ce sont les structures les plus petites qui sont visées, en tant qu'acteurs innovants et compétitifs. Malheureusement, ces acteurs n'ont pas toujours les moyens d'une protection en profondeur et sont donc les plus vulnérables. Le plus souvent, ce sont des PME constituées autour d'une technologie spécifique et convoitée. La protection de ce savoir faire est donc vital. Parmi nombre de techniques employées pour faire secrètement fuir de l'information stratégique, il y a la stéganographie.

La stéganographie offre des fonctionnalités pour camoufler de l'information (texte, image, ...) dans n'importe quel support numérique (image, vidéo, son, ...). Elle vise, en plus de garder secrète l'information échangée, à dissimuler l'existence même de la communication. Pour ce faire, les supports contenant de l'information cachée sont rendus ressemblants à n'importe quel autre support. Dans ce contexte, afin d'empêcher toute fuite d'information qui serait invisible à l'œil nu, il est primordial de disposer de détecteurs automatiques capables de dire si un support contient ou non de l'information cachée. De plus, l'utilisation de telles techniques par un collaborateur peu scrupuleux est d'autant plus aisée qu'Internet regorge de logiciels faciles à mettre en œuvre. On en dénombre environ deux cents. Le risque stéganographique est donc sérieusement à considérer lors de l'élaboration d'une politique globale de sécurité. Néanmoins, il faut garder à l'esprit que le coût de déploiement d'une protection efficace pour ce prémunir contre ce risque est élevé. D'autre part, les détecteurs stéganographiques possèdent des limitations intrinsèques. Pour bien comprendre leur utilisation et leur paramétrage, il est nécessaire de s'attarder sur la notion de sécurité en stéganographie. Cette notion quantifie à la fois l'efficacité des détecteurs et la furtivité des algorithmes de stéganographie. Tandis qu'en cryptographie l'étude de la sécurité dimensionne le temps nécessaire à un adversaire pour avoir accès à l'information claire, en stéganographie, elle dimensionne la probabilité qu'un médium stéganographié avec un algorithme donné soit détecté par un détecteur spécifique.

Dans cet article, nous présentons tout d'abord en partie 1 les concepts généraux de la stéganographie et de son pendant, la *stéganalyse* (ensemble des techniques qui statuent si un support contient ou non de l'information cachée). Nous détaillons ensuite dans une seconde partie, la notion de sécurité en stéganographie afin de bien comprendre les limites des détecteurs stéganographiques. Nous expliquons, en s'appuyant sur des fondements théoriques, comment mesurer l'efficacité en pratique de tels détecteurs. Enfin, dans une dernière partie, nous discutons de l'exploitation des résultats issus des détecteurs et présentons une technique générique pour cacher indépendamment deux messages dans un même support.

1 Stéganographie et Sécurité

1.1 Principes de base en stéganographie

La stéganographie est un domaine scientifique aussi ancien que celui de la cryptologie, sinon plus. Bien que souvent confondus, ces deux domaines sont très différents tant dans l'esprit que dans la forme mais ils n'en restent pas moins complémentaires. Tandis que la cryptographie vise à assurer, entre autres, un service de confidentialité des données, la stéganographie a pour objectif de

dissimuler l'existence même de la communication entre deux protagonistes. La stéganographie moderne prend ses racines au début des années 80 dans l'article fondateur de G.J. Simmons [1] qui introduit et définit les canaux *subliminaux* en s'inspirant du problème des prisonniers.
Ce problème met en jeux Alice et Bob, deux prisonniers autorisés à communiquer entre eux exclusivement sous la surveillance de Wendy, une gardienne. Si Wendy a le moindre doute sur un potentiel projet d'évasion, Alice et Bob seront envoyés en isolement et perdront ainsi le privilège de correspondre. Pour mener à bien leur projet d'évasion ils ne doivent pas éveiller les soupçons de Wendy. Bien évidemment, l'emploi de cryptographie dans ce contexte est à proscrire. Un message chiffré rendrait Wendy suspicieuse ; elle contraindrait alors l'un des deux à lui fournir leur clé secrète. Alice et Bob n'ont pas d'autres solutions que de rendre non seulement le contenu de leur correspondance mais aussi le fait même qu'ils communiquent hors du cadre légal ; ils doivent alors établir un canal de communication invisible pour Wendy. Ce canal est qualifié de subliminal.

Pour ce faire, nous supposons tout d'abord qu'Alice et Bob se sont échangés au préalable une clé secrète cryptographique ainsi qu'une clé secrète stéganographique. Nous appelons par la suite *médium support* ou *support de couverture* le médium vierge d'information cachée et *stégo médium* tout médium en contenant. Par abus de langage, nous utilisons aussi le terme de support et nous le qualifions de *stégo* si c'est un stégo médium et *non stégo* dans le cas contraire. La mise en œuvre d'un schéma de stéganographie s'effectue alors en deux étapes distinctes. Pour envoyer un message à Bob, Alice effectue les opérations suivantes :

1. elle compresse son message et le chiffre avec la clé cryptographique,
2. elle génère un support de couverture,
3. l'algorithme de stéganographie sélectionne les sous-parties du support favorables à la dissimulation,
4. il dissimule ensuite aléatoirement, à l'aide de la clé stéganographique, le message chiffré dans les parties favorables,
5. Alice envoie le stégo médium par un canal classique.

Cette étape, appelée aussi *dissimulation*, est illustrée par la figure 1. Pour lire le message d'Alice, la procédure est totalement symétrique et Bob effectue alors les opérations suivantes :

1. Bob reçoit le stégo médium par le canal classique,
2. l'algorithme de stéganographie sélectionne les sous-parties du support favorables à la dissimulation,
3. il retrouve la position du message chiffré dans les parties favorables, à l'aide de la clé stéganographique,

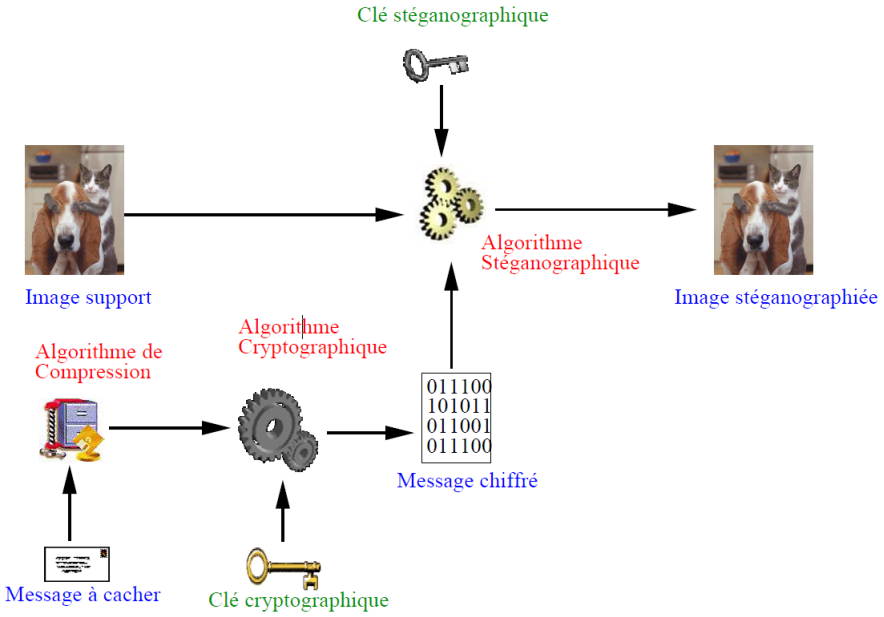


Figure 1. Étape de dissimulation pour une image fixe

4. Bob déchiffre le message à l'aide de la clé cryptographique et le décompresse.

Cette étape est appelée *extraction*. La mise en œuvre de schémas de stéganographie nécessite les précautions d'usage suivantes [2]. Tout d'abord, c'est l'émetteur qui génère le support. Celui-ci doit n'être utilisé qu'une seule fois et détruit après utilisation, afin d'éviter les attaques par différence. En effet, tout attaquant possédant le support original est capable avec une probabilité égale à 1 de détecter tout stégo médium issu du support. De même, pour éviter les attaques visuelles, l'algorithme de stéganographie ne doit pas détériorer visuellement le support. En général, les valeurs du support que l'algorithme de stéganographie modifie pour insérer l'information possèdent une distribution uniforme (par exemple les bits de poids faible (LSB)). Chiffrer permet d'une part d'assurer la confidentialité et d'autre part d'uniformiser la distribution des bits du message effectivement dissimulés. Le but étant d'obtenir une distribution des valeurs du stégo médium identique à celle des valeurs du support. De plus, afin de se prémunir contre des attaques classiques sur les moments d'ordres supérieurs, comme un test du χ^2 par exemple, on demande aux algorithmes de stéganographie de conserver les statistiques des valeurs qu'il modifie, à l'ordre 1 et supérieur. Enfin, la quantité d'information à dissimuler doit être petite. Le support peut être en effet considéré comme un canal au sens de Shannon [3], avec une capacité limitée. Intuitivement, plus on dissimule d'information dans un support, plus celui-ci subit de changements et plus le stégo médium risque d'être détecté. Dans le domaine

de la dissimulation d'information, il faut composer avec un compromis entre la *capacité*, c'est-à-dire la quantité d'information que l'on peut insérer dans un support, *l'indétectabilité*, c'est-à-dire la probabilité que le stégo médium soit déclaré non stégo par un attaquant et la *robustesse*, c'est-à-dire la quantité d'information dissimulée résiduelle après un certain nombre de transformations sur le stégo médium.
Le problème du prisonnier illustre parfaitement la complémentarité entre la cryptographie et la stéganographie et met précisément en avant toute la difficulté à laquelle doit faire face un attaquant. Nous percevons à travers cet exemple combien il est difficile de mettre en place des contre mesures pour lutter contre l'emploie de telles techniques au sein d'une entreprise. Une première conséquence pour limiter un tel risque est de conserver la maîtrise du système informatique en interdisant notamment l'exécution de tout logiciel non approuvé par la politique de sécurité mise en place. Le lecteur intéressé pourra se référer aux ouvrages suivants [2,4,5,6,7,8] pour compléter ou approfondir les notions présentées ici.

1.2 Détecter l'information cachée

Par essence même des techniques de stéganographie, la mise en place d'une protection s'avère extrêmement compliquée. Tout d'abord parce que tout support informatif peut donner lieu à une technique de stéganographie et par ailleurs, la surveillance de tous les canaux de communication de l'entreprise est techniquement impraticable. Il faut donc restreindre la surveillance à un nombre limité de canaux et donc faire l'hypothèse qu'avec forte probabilité, la compromission n'empruntera pas les autres canaux. La détection d'information cachée consiste à analyser tous les média transitant sur un canal de communication et à répondre à la question suivante : « le médium analysé contient-il de l'information cachée ? ». Pour bien comprendre les protections à mettre en place pour répondre à cette première question, nous en donnons ici une définition formelle. Le lecteur intéressé par une formalisation plus complète des détecteurs en stéganographie, pourra se référer à [9,10].
L'étape d'analyse correspond à un ensemble de mesures à effectuer sur le médium. En pratique, ces mesures ne doivent pas prendre trop de temps. De plus, comme elles sont effectuées sur un grand nombre de média, on s'intéresse à leur distribution statistique. Cette étape est appelée extraction des caractéristiques ou *features extraction* en anglais.

Définition 1 *Soit Σ un schéma de stéganographie. Nous appelons extraction de caractéristiques, la donnée d'une fonction*

$$\begin{aligned} V : \quad & \mathcal{I} \longrightarrow \mathcal{V}_1 \times \cdots \times \mathcal{V}_n \\ & I \longrightarrow V(I) = (V_1(I), \ldots, V_n(I)), \end{aligned}$$

où V_i est une variable aléatoire définie sur $\mathcal{I}$ à valeurs dans $\mathcal{V}_i$ et calculable en temps polynomial, $\mathcal{I}$, l'ensemble des média et I le médium à analyser.

L'extraction des caractéristiques est équivalente à la donnée de n mesures, coordonnées d'un *vecteur statistique*. Une extraction est utile si elle permet de distinguer $\mathcal{C}$, l'ensemble des supports de couverture, de $\mathcal{S}$, l'ensemble des stégo média produits par Σ, ou de façon équivalente $V(\mathcal{C})$ de $V(\mathcal{S})$. C'est à partir de cette capacité à distinguer ces deux ensembles que nous pouvons classer le médium à analyser comme stégo médium ou comme support de couverture et ainsi répondre à la question. Ce critère de distinction entre $\mathcal{C}$ et $\mathcal{S}$ trouve ses fondements dans la théorie de l'information et notamment les travaux de C. Cachin [11,12,13] relayés par ceux de R. Chandramouli [14,15,16]. D'un point de vue plus formel, une extraction de caractéristiques est efficace si et seulement si elle vérifie au moins l'un des deux critères suivants.

- Il existe $i \in [1, n]$ tel que $P_{V_i(\mathcal{C})} \neq P_{V_i(\mathcal{S})}$,
- il existe $i \in [1, n]$ tel que $P_{V_i|\{V_k,\, k\neq i\}(\mathcal{C})} \neq P_{V_i|\{V_k,\, k\neq i\}(\mathcal{S})}$.

Le premier critère implique que $I \longrightarrow V_i(I)$ est aussi une extraction de caractéristiques efficace, ce qui n'est pas le cas pour le second. Si $V_i(I)$ n'est pas une extraction efficace, cela signifie que nous devons aussi observer les autres coordonnées de V pour obtenir de l'information sur I à partir de V_i.

Une extraction efficace permet alors d'obtenir des distributions que l'on peut distinguer, encore faut-il construire un distingueur qui exploite cette capacité à différentier les ensembles $\mathcal{C}$ et $\mathcal{S}$, c'est à dire les distributions marginales, P_{V_i}, ou conditionnelles, $P_{V_i|\{V_k,\, k\neq i\}}$, évaluées sur les ensembles $\mathcal{C}$ et $\mathcal{S}$.

Définition 2 *Soit Σ un schéma de stéganographie et V une extraction de caractéristiques. Nous appelons distingueur compatible avec V, la donnée d'une fonction définie par*

$$D_V : \mathcal{V}_1 \times \cdots \times \mathcal{V}_n \longrightarrow \{0, 1\},$$

calculable en temps polynomial. Par convention 0 est associé à non stégo et 1 à stégo.

Celle-ci nous permet alors d'énoncer la définition de la *stéganalyse par discrimination*, qui est la stéganalyse la la plus usitée dans la communauté.

Définition 3 *[9] Soit Σ un schéma de stéganographie. Nous appelons stéganalyse par discrimination contre Σ tout couple (V, D_V), où V est une extraction de caractéristiques et D_V un distingueur compatible avec V.*

En pratique, il est vraiment onéreux de mettre en place des détecteurs sur tous les canaux communication sortant de l'entreprise. De surcroît, pour détecter l'utilisation d'un seul algorithme de stéganographie, il existe de nombreux détecteurs.

D'autre part chaque détecteur est spécifique à un format donné. On imagine alors aisément un investissement en ressources nécessaires prohibitif pour une analyse en coupure et en temps contraint. Le plus souvent ce n'est qu'*a posteriori* et dans un cadre d'investigation numérique qu'ils sont mis en œuvre.

2 Évaluer la sécurité en stéganographie

Le nombre croissant de schémas de stéganographie mais aussi la complexité des attaques auquel ils doivent résister renforce la nécessité d'une méthodologie commune pour quantifier l'efficacité des détecteurs et donc la furtivité des algorithmes de stéganographie. Ce point pose la question de la définition de la sécurité en stéganographie. Trois objectifs de sécurité doivent être considérés. Le premier est la sécurité contre un adversaire qui vise à détecter la présence d'information cachée dans un support. Cet aspect de la sécurité en stéganographie doit composer avec le compromis incontournable entre la capacité et la détection en gardant à l'esprit que « plus nous cachons d'information, plus celle-ci sera détectable». Le second est la sécurité contre un adversaire qui cherche à extraire l'information cachée qu'il a précédemment détectée. Extraire cette information sans connaissance *a priori* est équivalent à une recherche exhaustive sur la clé stéganographique. Enfin, le dernier objectif est la sécurité classique en confidentialité contre un adversaire qui a accès au texte chiffré et dont le but est d'obtenir le texte clair. Dans cet article, nous nous limiterons au premier niveau de sécurité, *i.e.* en détection.

2.1 Des modèles théoriques

C. Cachin [11,12,13] puis R. Chandramouli [14,15,16] ont été les premiers à s'intéresser à la notion formelle de la sécurité en stéganographie. Pour la quantifier, nous définissons traditionnellement l'adversaire auquel le schéma de stéganographie doit résister. Chaque adversaire est ensuite associé à un modèle de sécurité qui définit les actions qu'il est capable d'effectuer ainsi que les règles qu'il doit respecter. De nombreux modèles ont été proposés. Certains pour les schémas à clés privées [12,17,18,19] et d'autres pour ceux à clés publiques [20,13,21]. D'autre part, différentes catégories d'adversaires ont été considérées comme les adversaires passifs [12,18,21,20] ou actifs [13,22]. La thèse de N. Hopper [23] représente peut-être les travaux les plus complets sur le sujet. Plus récemment, dans la même direction, A.D. Ker [24] et J. Barbier [10,9] on tenté de réduire le fossé entre les adversaires réels et ceux définis dans les modèles classiques de sécurité. Nous nous appuierons sur les travaux de ce dernier.

L'adversaire le plus souvent considéré est un adversaire passif qui intercepte les média qu'il voit passer sur un canal de communication. Celui-ci a la connaissance du schéma de stéganographie Σ employé par les différents protagonistes.

En revanche, il ne connaît pas la clé secrète partagée par les participants. Pour chaque médium qu'il intercepte, il doit répondre à la question suivante : «le médium contient-il de l'information cachée ?». Nous supposons sans perte de généralité que celui-ci dispose de ressources et de temps finis. À partir de cet adversaire réaliste, qui correspond par exemple à des détecteurs mis en place en coupure sur un réseau, nous définissons un modèle d'adversaire et de sécurité [10,9] ; le modèle IND-SSA (indistinguashability specific steganalysis attack), *i.e.* modèle en indistinguabilité contre un adversaire mettant en œuvre des stéganalyses dédiées. Dans ce modèle, l'adversaire A est modélisé par un couple d'algorithmes probabilistes polynomiaux (A_1, A_2). Pour mesurer l'efficacité de cet adversaire, nous le faisons jouer contre à un challenger. Ce jeu se déroule en deux étapes.

Étape 1 : le challenger génère aléatoirement une clé secrète. L'adversaire peut générer ses propres clés mais ne connait pas celle du challenger. Il peut tester le schéma de stéganographie avec ses propres clés et ses propres ensembles de média. Il teste ensuite ensuite ses stéganalyses et essaie d'obtenir de l'information sur le comportement du schéma de stéganographie pour pouvoir le distinguer ultérieurement. À la fin de cette étape, il stocke toute la connaissance qu'il a apprise dans une variable s.

Étape 2 : le challenger choisi aléatoirement un bit, un message et un médium dans son ensemble de média (connu de lui seul). Si le bit vaut 1, il stéganographie le message dans le médium et le renvoie à l'adversaire sinon il lui renvoie le médium ainsi sélectionné sans modification. Ce médium constitue le challenge. L'adversaire reçoit donc un médium. À la fin de cette étape celui-ci doit statuer si le médium reçu contient ou non un message caché.

Le jeu associé au modèle de sécurité est noté $\mathbf{Exp}_{\mathbf{\Sigma}}^{\mathbf{IND\text{-}SSA}}(\mathbf{A}, \mathbf{k})$ et est résumé sur la figure 2. Le paramètre k est la paramètre qui détermine la taille de la clé secrète. Dans ce contexte, la sécurité est alors évaluée en comptabilisant le nombre de fois ou A a correctement répondu au challenge. Plus formellement,

Définition 4 [9] *L'efficacité d'un attaquant A de type IND-SSA contre Σ est défini par son avantage $Adv_{\Sigma}^{IND\text{-}SSA}(A, k)$ tel que*

$$Adv_{\Sigma}^{IND\text{-}SSA}(A, k) = 2|\mathcal{P}r\left(Exp_{\Sigma}^{IND\text{-}SSA}(A, k) = 1\right) - \frac{1}{2}|.$$

L'avantage quantifie la puissance de l'attaque, *i.e.* la proportion de fois où l'attaquant répond correctement relativement à un tirage à pile ou face.

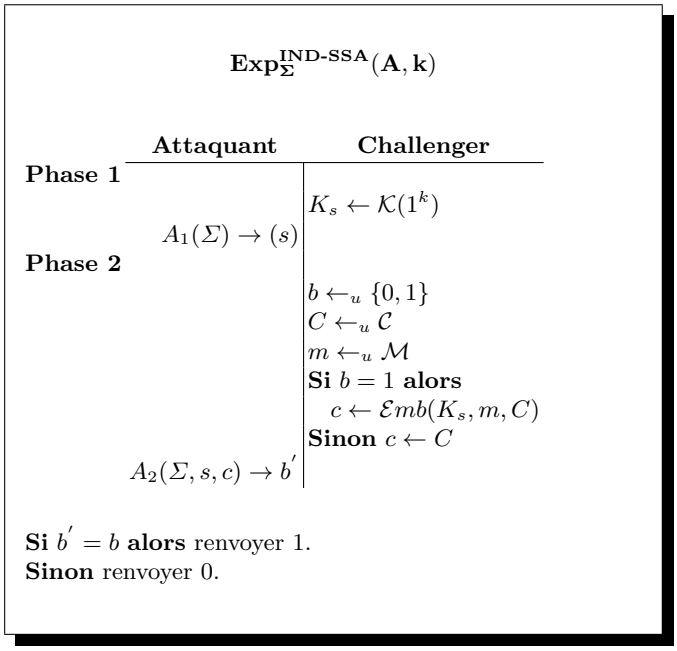


Figure 2. Expérience en indistinguabilité avec un attaquant A de type IND-SSA contre Σ

2.2 De la théorie à la pratique

Dans le jeu IND-SSA, l'adversaire A reçoit le challenge c et doit faire une hypothèse sur c parmi H_1, « c est un stégo médium » et H_2, « c est un support de couverture ». Nous rappelons que $\mathcal{C}$ est l'ensemble des supports de couverture et $\mathcal{S}$ l'ensemble des stégo média. Nous sommes dans un cas classique de test à deux hypothèses. Le lecteur intéressé par ce pan du domaine des statistiques peut se référer à [25]. Les définitions classiques suivantes en sont issues. Pour évaluer la « réussite » de l'attaquant, nous différencions deux configurations :

1. c est un support de couverture,
2. c est un stégo médium.

Dans la configuration 1, nous calculons tout d'abord $\mathcal{P}r(A \text{ répond } H_1 \mid c \in \mathcal{C}) = \mathcal{P}_{fp}$, *la probabilité de faux positifs*, aussi appelée *probabilité de fausse alarme* ou encore *erreur de 1ère espèce*. Nous en déduisons alors $\mathcal{P}r(A \text{ répond } H_2 \mid c \in \mathcal{C}) = \mathcal{P}_{vn}$, *la probabilité de vrais négatifs*, aussi appelée *spécificité*. Bien évidemment, nous avons

$$\mathcal{P}_{fp} + \mathcal{P}_{vn} = 1.$$

Dans la configuration 2, nous calculons tout d'abord $\mathcal{P}r(A \text{ répond } H_2 \mid c \in \mathcal{S}) = \mathcal{P}_{fn}$, *la probabilité de faux négatifs*, aussi appelée *probabilité de non détection*

ou encore *erreur de 2ème espèce*. Nous en déduisons alors $\mathcal{P}r(A \text{ répond } H_1 \mid c \in \mathcal{S}) = \mathcal{P}_{vp}$, *la probabilité de vrais positifs*, aussi appelée *sensibilité*. Là encore,

$$\mathcal{P}_{fn} + \mathcal{P}_{vp} = 1.$$

De plus, si le détecteur reçoit n_s challenges c, média stéganographiés et n_c challenges c, supports de couverture, alors la *probabilité de succès*, $\mathcal{P}_{suc}$, du détecteur est donnée par

$$\mathcal{P}_{suc} = \frac{1}{n_c + n_s} \left(n_s \mathcal{P}_{vp} + n_c \mathcal{P}_{vn} \right).$$

Traditionnellement, le détecteur est évalué avec autant de challenges de $\mathcal{C}$ que de $\mathcal{S}$, *i.e.* $n_c = n_s$. Dans ce cas particulier, la probabilité de succès est donc la moyenne de la sensibilité et de la spécificité.

Les performances des détecteurs dépendent d'un seuil qui impacte les probabilités de détection, de faux positifs et de faux négatifs. Traditionnellement, on trace les courbes ROC *(Receiver Operating Characteristic)* représentant la probabilité de vrais positifs en fonction de la probabilité de faux positifs. Elles mettent ainsi en évidence le compromis à faire lors du choix du seuil. Généralement, on se fixe une probabilité maximum de faux positifs, puis on choisit le seuil en conséquence. Intuitivement, plus la courbe ROC est proche du coin supérieur gauche et meilleur est le détecteur. En stéganographie, on limite au maximum les faux positifs car ils sont plus coûteux que les faux négatifs. En effet, une fois qu'un stégo médium est détecté, on essaie d'extraire l'information cachée. D'autre part, le compromis illustré entre la capacité et la détection, montre que les performances des détecteurs stéganographiques dépendent de la quantité d'information dissimulée. Pour prendre en compte ce paramètre, les stéganalystes fixent le taux stéganographique et évaluent la courbe ROC pour ce taux. Pour un détecteur donné, nous obtenons ainsi une famille de courbes ROC, comme l'illustre la figure 3. Cette démarche est équivalente à attaquer avec la même stéganalyse les schémas de stéganographie Σ_r, correspondant au schéma Σ dissimulant au taux stéganographique constant r. Enfin, si nous notons α la probabilité de fausse alarme et β la probabilité de faux négatifs, nous pouvons montrer [10] que

$$Adv_{\Sigma}^{\text{IND-ATK}}(A, k) = |1 - (\alpha + \beta)|. \tag{1}$$

Cette équation relie la sécurité au sens des modèles théoriques à des valeurs pratiquement mesurables. D'autre part, la plupart des algorithmes de classification nécessitent une phase d'apprentissage, c'est à dire qu'ils doivent connaitre un ensemble de stégo média et un ensemble de supports de couverture pour être configurés. Or, leur efficacité, et donc celle du détecteur associé, dépendent fortement de la proximité de ces ensembles d'apprentissage avec ceux observés dans l'étape de challenge. Pour être réellement efficaces, les logiciels de détection doivent pouvoir apprendre sur des ensembles que l'on choisit nous même.

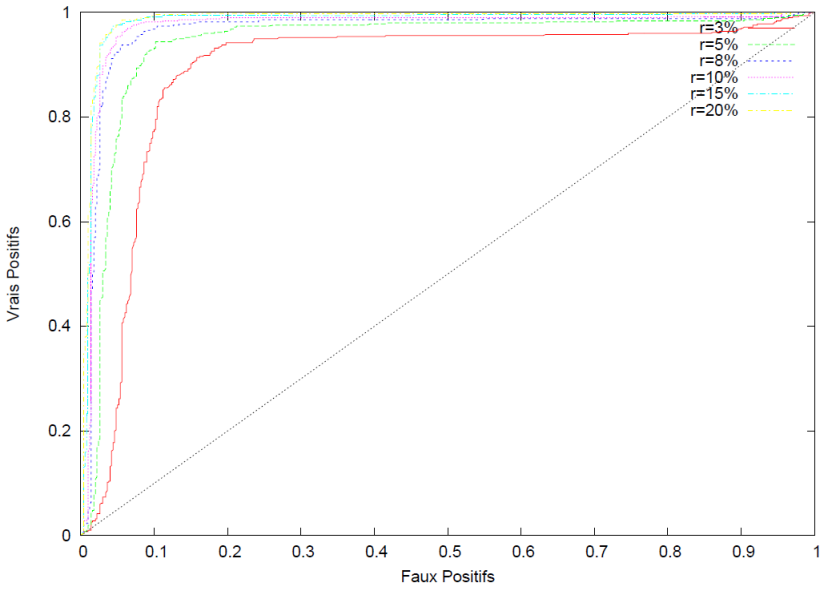


Figure 3. Famille de courbes ROC d'un détecteur

3 L'indistinguabilité indéniable

3.1 Concept et impacts

Lorsque l'on évalue la sécurité en stéganographie, l'adversaire est considéré comme gagnant dès lors qu'il est capable de dire si un médium contient ou non de l'information dissimulée. Maintenant, imaginons le scénario suivant. Nous souhaitons faire sortir des documents stratégiques d'une entreprise en employant des moyens de stéganographie. Celle-ci analyse automatiquement tout document sortant et dispose par ailleurs du détecteur qui ne se trompe jamais. De plus, l'extraction d'un message dissimulé est une simple lecture du support et ne permet pas de retrouver le support de couverture tel qu'il était avant l'insertion. Enfin, supposons maintenant que nous sommes capables de cacher avec deux clés indépendantes et dans un même support deux messages ; le premier qui ne soit pas incriminant et le second qui le soit. Alors, lorsque nous passerons le détecteur, nous révèlerons la première clé associée au message non incriminant. À ce stade, comme l'extraction du premier message est une opération de lecture, le support est inchangé ; le détecteur le considérera alors toujours comme un stégo médium. En conclusion, le détecteur est incapable de faire la différence entre un support qui contient un message caché et un support qui en contient plus d'un. Cette propriété est appelée *indistinguabilité indéniable* [9].
Cette propriété est importante car aucun détecteur aussi bon soit-il n'est capable

d'apporter une preuve de notre culpabilité voire même d'éveiller les soupçons. Il reste un doute sur lequel on ne peut statuer. Cela pose évidemment la question de l'utilisation de techniques de stéganalyse dans le cadre d'une expertise légale. Au-delà de l'aspect technique qui associe à chaque médium une probabilité qu'il contienne de l'information cachée, il reste aujourd'hui un problème ouvert : quelle doctrine d'emploi pour des détecteurs stéganographique ? Dans le cadre d'un déploiement de détecteurs en entreprise, ces derniers ne peuvent être que des indicateurs faisant remonter des alertes mais ne peuvent malheureusement pas être utilisés pour confondre d'éventuels coupables. Néanmoins, cette propriété repose sur une hypothèse forte qui nécessite la capacité à cacher deux messages dans un même support avec deux clés indépendantes. Aujourd'hui peu de schémas de stéganographie offrent cette fonctionnalité.
Pour pallier cette difficulté, à l'instar des travaux initiés par Fridrich *et al* [26], la communauté scientifique s'intéresse à mettre en évidence des estimateurs statistiques de la quantité d'information cachée. De ce fait, une simple comparaison entre la longueur du message extrait et la longueur estimée peut révéler la présence d'information cachée non encore révélée. Néanmoins, de tels estimateurs sont bien plus difficiles à mettre en évidence que les détecteurs usuels. D'autre part, la méthodologie d'évaluation de la sécurité en stéganographie doit être adaptée. Pour ce faire, deux pistes peuvent être explorées. La première consiste à utiliser les mesures nécessaires à l'estimation comme extraction de caractéristiques ; la seconde à ne prendre que la valeur de l'estimation comme caractéristique. Dans ces deux cas nous appliquons alors la méthodologie présentée dans la partie 2. De plus, en tant qu'estimateurs ils doivent être aussi évalués de manière usuelle en calculant notamment leur bais, l'erreur quadratique moyenne, l'erreur relative et l'intervalle de confiance. L'étude des estimateurs statistiques montre que pour retrouver la propriété d'indistinguabilité indéniable face à un estimateur, la longueur relative du second message doit appartenir à l'intervalle de confiance pour une probabilité proche de 1 de l'estimation de la longueur du premier message. Dans le cas des estimateurs, l'indistinguabilité indéniable n'est plus garantie.

3.2 Vers une construction générique

Nous présentons ici une construction générique pour atteindre la propriété d'instingabilité face à des détecteurs. L'objectif auquel nous voulons répondre consiste à cacher dans un même support C, deux messages secrets M_1 et M_2, de longueur respective l_1 et l_2, avec deux clés stéganographiques K_1 et K_2 indépendantes. Pour ce faire, nous avons besoin d'une fonction de MAC_K (Message Authentification Code) sur 128 bits, d'un algorithme de chiffrement E_K sur 128 bits et d'un générateur pseudo-aléatoire dont l'état interne est de 128 bits, noté GPA. Nous noterons enfin iv, iv_1 et iv_2 trois vecteurs d'initialisation de 128 bits fournis ou générés par ailleurs. Dans un premier temps, C est décomposé

en $C = U \cup \overline{U}$, où U est l'ensemble des bits utiles pour la stéganographie (par exemple les bits de poids faible des pixels d'une image) et $\overline{U}$ son complémentaire. Pour chaque clé K_i, $i = 1, 2$, nous tirons pseudo-aléatoirement un ensemble de 384 positions P_i dans U sous l'hypothèse que $P_1 \cap P_2 = \emptyset$.

$$GPA(MAC_{K_i}(\overline{U})) \rightarrow P_i. \tag{2}$$

Cette hypothèse est peu bloquante en pratique car la probabilité qu'un tel évènement se produise est proche de 1. Si d'aventure $P_1 \cap P_2 \neq \emptyset$ alors nous changeons de support ou l'une des clés. Nous générons ensuite une permutation pseudo-aléatoire des positions de $U \setminus (P_1 \cup P_2)$:

$$GPA(iv) \rightarrow P. \tag{3}$$

Nous tirons ensuite pseudo-aléatoirement une position de P que nous notons pos_1. Nous noterons pos_2 la position de P située à $256 + l_1$ positions de pos_1. À la position pos_1, nous insérons $E_{K_1}(l_1)||E_{k_1}(iv_1)$. Nous générons ensuite une permutation des l_1 positions suivantes de P :

$$GPA(iv_1) \rightarrow P_1^{'}, \tag{4}$$

puis nous insérons aux positions de $P_1^{'}$ le message M_1. Nous insérons exactement de la même manière l_2, iv_2 et M_2 à partir de la position pos_2. Enfin, aux positions P_i, nous insérons le message de 384 bits composé de

$$E_{K_i}(MAC_{K_{\bar{i}}}(\overline{U}))||E_{K_i}(iv)||E_{K_i}(pos_i). \tag{5}$$

où $\bar{i}$ vaut 1 si i vaut 2 et réciproquement. Ces 384 bits constituent l'en-tête pour la récupération du message M_i. La procédure d'insertion est résumé dans la figure 4. L'extraction d'un des deux messages ne fournis pas d'information sur la présence ou non d'un autre message. Elle se décompose selon les étapes suivantes. À partir de la clé K_i nous calculons P_i tel que $GPA(MAC_{K_i}(\overline{U})) \rightarrow P_i$. P_i nous donne les positions pour retrouver l'en-tête. En extrayant l'en-tête (5) puis en déchiffrant avec K_i, nous obtenons $MAC_{K_{\bar{i}}}(\overline{U})$, iv et pos_i. $MAC_{K_{\bar{i}}}(\overline{U})$ nous permet de retrouver $P_{\bar{i}}$ et d'avoir les positions de l'en-tête de M_i. Ceci est la seule information que nous avons sur un éventuel message supplémentaire, l'accès étant protégé par un chiffrement. À ce stade, nous sommes donc incapables de différencier l'en-tête $P_{\bar{i}}$ d'une suite de positions non stéganographiées. Néanmoins, la connaissance de $P_{\bar{i}}$ est nécessaire pour calculer P selon (3). Enfin, à la position pos_i nous extrayons puis déchiffrons l_i et iv_i. Ces valeurs permettent le calcul de $P_i^{'}$ selon (4) et l'extraction de M_i. Les paramètres de sécurité (128) sont donnés à titre indicatifs mais peuvent être augmentés si nécessaire.

Procédure d'insertion de deux messages dans un support

Entrées : C un support,
K_1, K_2 deux clés stéganographiques,
M_1, M_2 deux messages de longeur l_i,
iv, iv_1, iv_2 vecteurs de 128 bits.

Sortie : C contenant M_1 et M_2

1 $C = U \cup \overline{U}$
2 $GPA(MAC_{K_i}(\overline{U})) \rightarrow P_i$, $i = 1, 2$
3 **Si** $P_1 \cap P_2 \neq \emptyset$ **alors** changer K_i ou C et **retourner** en 1
4 $GPA(iv) \rightarrow P \subset (U \setminus (P_1 \cup P_2))$
5 **Choisir** $pos_1 \in P$
6 $(256 + l_1)^{\text{ème}}$ position après pos_1 dans $P \rightarrow pos_2$
7 **Insérer** $E_{K_i}(l_i)||E_{k_i}(iv_i)$ dans P à partir de pos_i, $i = 1, 2$
8 $GPA(iv_i) \rightarrow P_i^{'} \subset [pos_i + 256, pos_i + 256 + l_i]$ positions de P, $i = 1, 2$
9 **Insérer** M_i dans $P_i^{'}$, $i = 1, 2$
10 **Insérer** $E_{K_i}(MAC_{K_{\overline{i}}}(\overline{U}))||E_{K_i}(iv)||E_{K_i}(pos_i)$ dans $P_i^{'}$, $i = 1, 2$
11 **Retourner** C ainsi modifié

Figure 4. Procédure d'insertion de deux messages

Conclusion

Dans cet article, nous avons présenté les principes généraux de la stéganographie et de la stéganalyse. Nous avons ensuite étudié les fondements théoriques de l'analyse de la sécurité en stéganographie et les avons reliés à des mesures pratiques pour évaluer l'efficacité des détecteurs d'information cachée. Cette approche ouvre la porte à une méthodologie d'évaluation commune et admise par la communauté. Nous avons enfin présenté la notion d'indistinguabilité indéniable qui montre clairement la limite de l'approche par détecteurs. Nous avons discuté d'une approche alternative, dite *quantitative*, plus difficile à mettre en évidence mais aussi plus efficace en terme de détection. Nous avons proposé une méthode générique pour atteindre la propriété d'indistinguabilité.
Lorsque la recherche d'information cachée s'effectue à partir de détecteurs statistiques, la propriété d'indistinguabilité ne permet pas de confondre un coupable mais seulement de faire remonter des alarmes. Aujourd'hui, le déploiement à grande échelle de solutions d'analyse et de recherche systématique de contenu dissimulé n'est pas à la porté de toutes les entreprises, notamment les TPE et PME. Paradoxalement, ce sont ces petites structures moteurs de l'innovation qui sont le plus touchées par des actions visant à acquérir leur savoir faire et leur technologie. De plus, s'il existe des techniques pour détecter des média stéganographiés, l'extraction pose encore un problème. Avoir accès à l'information insérée

nécessite sans *a priori* une recherche exhaustive sur la clé stéganographique. Le coût prohibitif d'une telle procédure pousse à configurer les détecteurs en réduisant au maximum les fausses alarmes. Dans ces conditions, il est quasi impossible d'évaluer même *a posteriori* le sujet et l'ampleur d'une compromission par fuite d'information sur un canal subliminal. Nous sommes juste capables d'alerter sur une fuite d'information non identifiée.

Références

1. Simmons, G. : The prisoners' problem and the subliminal channel. In : Proc. CRYPTO'83. (1983) 51–67
2. Barbier, J. : La stéganographie moderne : d'Hérodote à nos jours. In : Computer & Electronics Security Application Rendez-vous, CESAR 2007, Rennes, France (2007)
3. Chandramouli, R. : Data hiding capacity in the presence of an imperfectly known channel. In : Proc. SPIE Security and Watermarking of Multimedia Contents II. Volume 4314. (2001)
4. Johnson, N., Jajodia, S. : Exploring steganography : Seeing the unseen. IEEE Computer **31** (1998) 26–34
5. Judge, J. : Steganography : Past, Present and Future. SANS (2001)
6. Kahn, D. : The Codebreakers. MacMillan, New York (1967)
7. Kipper, G. : Investigator's guide to steganography. Information Security. Auerbach (2004) ISBN : 0-8493-2433-5.
8. Raynal, F., Petitcolas, F., Fontaine, C. : L'art de dissimuler les informations. Pour la Science (2002) Dossier " L'art du secret ".
9. Barbier, J. : Analyse de canaux de communication dans un contexte non-coopératif. Application aux codes correcteurs d'erreurs et à la stéganalyse. PhD thesis, École Polytechnique, Palaiseau, France (2007)
10. Barbier, J., Alt, S. : Practical insecurity for effective steganalysis. In : Proc. of 10th International Workshop on Information Hiding, IH 2008. Lecture Notes in Computer Science, Santa Barbara (CA), USA, Springer (2008)
11. Cachin, C. : An information-theoretic model for steganography. In Aucsmith, D., ed. : Proc. Information Hiding, 2nd International Workshop. Volume 1525 of Lecture Notes in Computer Science., Portland, Oregon, USA, Springer (1998) 306–318
12. Cachin, C. : An information-theoretic model for steganography. Information and Computation **192** (2004) 41–56
13. Cachin, C. : Digital steganography. In van Tilborg, H., ed. : Encyclopedia of Cryptography and Security. Springer (2005) ISBN : 978-0-387-23473-1.
14. Chandramouli, R. : Mathematical theory for steganalysis. In : Proc. SPIE Security and Watermarking of Multimedia Contents IV. (2002)
15. Chandramouli, R., Kharrazi, M., Memon, N. : Image steganography and steganalysis : Concepts and practice. In Kalker, T., Cox, I.J., Ro, Y.M., eds. : Proc. Digital Watermarking, Second International Workshop, IWDW 2003. Volume 2939 of Lecture Notes in Computer Science., Seoul, Korea, Springer (2003) 35–49 ISBN : 3-540-21061-X.
16. Chandramouli, R., Memon, N. : Steganography capacity : A steganalysis perspective. In : Proc. SPIE, Security and Watermarking of Multimedia Contents V. Volume 5020., Santa Clara, CA, USA (2003) 173–177
17. Dedić, N., Itkis, G., Reyzin, L., Russel, S. : Upper and lower bounds on black-box steganography. In : Proc. 2nd Theory of Cryptography Conference (TCC 2005). Volume 3378 of Lecture Notes in Computer Science., Springer (2005)

18. Hopper, N., Langford, J., von Ahn, L. : Provably secure steganography. In Yung, M., ed. : Proc. Crypto 2002. Volume 2442 of Lecture Notes in Computer Science., Santa Barbara, CA, USA, Springer (2002) 77–92 ISBN : 3-540-44050-X.
19. Katzenbeisser, S., Petitcolas, F. : Defining security in steganographic systems. In : Proc. SPIE Security and Watermarking of Multimedia contents IV. Volume 4675. (2002) 50–56
20. von Ahn, L., Hopper, N.J. : Public-key steganography. In Cachin, C., Camenisch, J., eds. : Proc. Eurocrypt 2004. Volume 3027 of Lecture Notes in Computer Science., Interlaken, Switzerland, Springer (2004) 323–341 ISBN : 3-540-21935-8.
21. Levan, T., Kurosawa, K. : Efficient public key steganography secure against adaptative chosen stegotext attacks. In : Proc.Information Hiding, 8th International Workshop, Old Town Alexandria, Virginia, USA (2006)
22. Hopper, N. : On steganographic chosen covertext security. In : Proc. International Colloquium on Automata Languages and Programming, ICALP 2005. Volume 3580 of Lecture Notes in Computer Science., Lisboa, Portugal, Springer (2005) 311–323 ISBN : 3-540-27580-0.
23. Hopper, N. : Toward a Theory of Steganography. PhD thesis, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, USA (2004)
24. Ker, A. : The ultimate steganalysis benchmark ? In : MM&Sec '07 : Proceedings of the 9th workshop on Multimedia & security, Dallas, Texas, USA, ACM (2007) 141 – 148 ISBN : 978-1-59593-857-2.
25. Saporta, G. : Probabilité, Analyse des Données et Statistiques. Technip (1990)
26. Fridrich, J., Hogea, M.G.D., Soukal, D. : Quantitative steganalysis of digital images : Estimating the secret message length. ACM Multimedia Systems Journal **9** (2003) 288–302 Special issue on Multimedia Security.

Amélioration de la détection de vulnérabilités Web par classification automatique des réponses

Anthony Dessiatnikoff[1,2], Rim Akrout[1,2], Éric Alata[1,2], Vincent Nicomette[1,2], and Mohamed Kaâniche[1,2]

[1] CNRS ; LAAS ; 7 avenue du Colonel Roche, F-31077 Toulouse, France
[2] Université de Toulouse ; UPS, INSA, INP, ISAE ; LAAS ; F-31077 Toulouse, France {adessiat, rakrout, ealata, nicomett, kaaniche}@laas.fr

Résumé La sécurité des serveurs et applications Web est plus que jamais d'actualité. Les attaques d'injection de code (SQL, JavaScript, etc.) se multiplient et font désormais partie des menaces les plus fréquentes sur le réseau Internet. Les scanners de vulnérabilités Web sont des outils permettant de détecter les vulnérabilités des serveurs Web, à l'aide de l'envoi de requêtes HTTP spécialement formattées. Même si ces outils permettent effectivement de révéler plusieurs vulnérabilités, les algorithmes qu'ils utilisent restent souvent trop limités et peuvent générer des faux positifs et faux négatifs. Nous proposons dans cet article un nouvel algorithme de détection de vulnérabilité basé sur des techniques de classification de pages. Nous montrons son efficacité comparé aux algorithmes des outils usuels au travers d'une expérimentation.

Mots-clés : scanner, application Web, détection de vulnérabilités

1 Introduction

La sécurité des serveurs et applications Web est un problème désormais récurrent. Le nombre de vulnérabilités recensées dans ce type de logiciels s'accroît constamment [1]. On peut l'expliquer par plusieurs raisons : la complexité croissante des technologies du Web, les délais sans cesse plus courts de mise sur le marché de logiciels, les compétences limitées et le manque de culture de sécurité des développeurs. Il est donc important de fournir à la communauté Internet les moyens leur permettant d'améliorer aisément la sécurité de leurs serveurs, sans pour autant leur demander une culture importante en sécurité. En réponse à ce besoin, un certain nombre de méthodes et d'outils ont été mis en place. Ils sont destinés aux développeurs d'applications Web et aux administrateurs en charge de la sécurité du système informatique. Ces méthodes et outils peuvent être utiles en phase de développement pour détecter et éliminer les vulnérabilités des applications Web mais aussi en phase opérationnelle pour protéger les applications vulnérables contre d'éventuelles attaques :

– L'analyse statique de code [2,3,4] consiste à analyser le code source de l'application Web (ASP, PHP, Java, ...) de façon à découvrir les vulnérabilités incluses dans ce code. L'avantage d'une telle méthode est qu'elle permet d'éliminer les fautes dans le logiciel avant que celui-ci ne soit déployé.

- L'interception des requêtes émises par le client avant qu'elles n'atteignent le serveur permet de protéger une application Web d'éventuelles attaques. Les outils qui emploient cette technique assainissent toute donnée suspecte envoyée au serveur. Ces outils peuvent être installés soit directement sur le serveur ([5,6,7]) soit entre le client et le serveur, sous forme de *proxy*. Un exemple d'un tel outil est `Noxes`[8]. Potentiellement, tout type de pare-feu applicatif peut réaliser ces vérifications.
- La détection de vulnérabilités permet de localiser, au sein des pages d'un site, la vulnérabilité, aussi bien avant le déploiement du site qu'en phase opérationnelle. Les outils qui implémentent cette technique sont en général nommés *scanners de vulnérabilités Web*. Afin de détecter les vulnérabilités, ils envoient des requêtes avec un format particulier et analysent les réponses correspondantes retournées par le serveur. En fonction de ces réponses, les scanners avertissent de la présence d'une vulnérabilité ou non.

Cet article se focalise sur les outils de détection de vulnérabilités et, plus particulièrement, sur les vulnérabilités de type injection SQL. Les scanners de vulnérabilités sont nombreux, comme illustré par exemple par la liste disponible sur le site `sectools.org` [9]. De par la complexité des sites Web d'aujourd'hui et les multiples fichiers qu'ils incluent, une analyse manuelle seule n'est pas envisageable. Ces outils sont donc indispensables. Malheureusement, les algorithmes qu'ils utilisent ne sont pas toujours assez efficaces, comme illustré dans plusieurs travaux tels que [10,11,12]. Il est souvent nécessaire qu'un expert en sécurité intervienne manuellement pour en vérifier les résultats. Cette limite constitue un frein à l'automatisation du processus d'analyse de vulnérabilités. En particulier, on constate que bon nombre d'outils, lorsqu'ils essaient de détecter la présence de vulnérabilités permettant l'injection de code de type SQL ou Javascript, génèrent de nombreux faux positifs et ne fournissent aucune requête permettant l'exploitation réelle de la vulnérabilité. Dans cet article, nous proposons un nouvel algorithme permettant une détection automatique de vulnérabilités pouvant être exploitées par des attaques de type injection SQL. Cet algorithme est en particulier capable de fournir la requête lui permettant d'affirmer que l'injection de code est possible.

Cet article est organisé comme suit : la partie 2 présente le fonctionnement général des outils de détection de vulnérabilités et donne un certain nombre de définitions utiles pour la suite. La partie 3 se focalise sur trois outils en source libre et analyse en détail leur algorithme de détection de vulnérabilités afin d'en présenter les faiblesses. La partie 4 propose un nouvel algorithme de détection de vulnérabilités permettant de combler ces faiblesses. La présentation de l'algorithme est réalisée sur la base des vulnérabilités de type injection SQL. La partie 5 présente une expérimentation permettant de mettre en évidence l'efficacité de

notre algorithme, comparé aux algorithmes des outils présentés dans la partie 3. Enfin la partie 6 propose une conclusion et quelques perspectives.

2 Principe des outils de détection de vulnérabilités

Les attaques les plus courantes concernant les serveurs Web sont les attaques d'injection SQL (lorsque le serveur Web est connecté à une base de données SQL) et Javascript (réalisées sous la forme d'attaques de type *Cross Site Scripting* ou XSS). Ces injections de code proviennent de l'exploitation du même type de vulnérabilité des serveurs Web : l'absence de test de conformité des paramètres d'URL ou des données fournies dans les champs des formulaires.

Pour vérifier si ces attaques d'injection de code sont possibles, les outils de détection de vulnérabilités envoient des requêtes particulières et analysent les réponses retournées par le serveur. Un serveur peut répondre avec une page de *rejet* ou une page d'*exécution*. La page de *rejet* correspond à la détection par le serveur de valeurs d'entrées malformées ou incohérentes (par un test de conformité de paramètres). Une page d'*exécution* correspond à la page renvoyée par le serveur suite à l'activation réussie de la requête. Elle peut corrrespondre soit au scénario "normal", dans le cas d'une utilisation légitime du site, soit à un détournement de son exécution via l'exploitation réussie d'une injection de code (avec des entrées non conformes).

Pour identifier les vulnérabilités d'un site Web, les outils soumettent au site des requêtes contenant des données non conformes correspondant à des attaques potentielles. Les réponses sont alors analysées par les outils afin d'identifier les pages d'*exécution*.

Tout le problème vient donc de l'analyse des réponses pour déterminer s'il s'agit réellement d'une page de *rejet* ou d'une page d'*exécution*. Les approches adoptées par les outils que nous avons analysés consistent à rechercher des motifs particuliers dans la page retournée par le serveur (correspondant par exemple à des messages d'erreurs) ou bien à analyser la similarité entre les pages associées à différentes requêtes. Ces approches ne sont pas toujours efficaces comme nous allons le montrer dans la section suivante.

Prenons l'exemple d'une page d'authentification qui utilise une base de données SQL pour conserver les couples *nom d'utilisateur / mot de passe* valides. Un outil de détection de vulnérabilités doit déterminer si la page d'authentification est vulnérable à une injection SQL (une telle injection permettant à un attaquant de contourner l'authentification). Ce type d'attaque est très fréquent [13] et peut permettre à un attaquant d'obtenir par exemple le contrôle complet sur une base de données. A la requête d'authentification soumise, le serveur peut retourner deux types de réponses : succès ou échec de l'authentification. Ces deux catégories de réponses se traduisent généralement par l'affichage de deux pages

différentes au niveau du navigateur du client en terme de code HTML de façon à ce que l'utilisateur puisse constater qu'il a entré un couple valide ou pas. Ces pages peuvent varier dans leur forme, en fonction du langage utilisé, du site lui-même, du développeur, etc. Les outils de détection de vulnérabilités doivent donc automatiquement classifier la réponse retournée afin de déterminer de façon correcte si la vulnérabilité est présente ou pas. Les exemples de la section suivante montrent que les analyses réalisées par les outils actuels sont souvent imprécises.

Dans la suite de cet article, nous appelons *faux positif* le fait qu'un outil de détection de vulnérabilités détecte la présence d'une vulnérabilité dans une page du site qu'il a balayée alors que cette vulnérabilité n'existe pas. De même, nous désignons par *faux négatif* le fait qu'un outil de détection de vulnérabilités ne détecte pas la présence d'une vulnérabilité dans une page du site qu'il a visitée alors qu'elle existe.

3 Analyse de trois scanners de vulnérabilités

Nous présentons dans cette section trois outils de détection de vulnérabilités connus dont les sources sont libres sur Internet et réalisons une analyse critique de leur algorithme de détection de vulnérabilités.

3.1 W3af

`W3af` [3] a été créé par Andres Riancho en 2006. Il est considéré comme l'un des plus performants[9]. Il est libre et écrit en Python. Son architecture modulaire permet aux utilisateurs d'importer et modifier facilement les différents modules qui le composent.

En particulier, le module `sqli` peut détecter des injections SQL dans les formulaires d'authentification, composés d'un champ permettant la saisie d'un nom d'utilisateur et d'un champ permettant la saisie du mot de passe. Plus précisément, il utilise trois requêtes formées à partir de l'injection SQL `d'z"0` (ou `d%2Cz%220` encodé en ASCII [4]). Par exemple, pour détecter si le serveur Web est vulnérable à une injection SQL au travers du fichier `login.php`, à l'aide de la méthode POST et des paramètres `login` et `password`, `W3af` envoie les trois requêtes HTTP suivantes :

```
request("POST","login.php","login=&password=d%2Cz%220")
request("POST","login.php","login=d%2Cz%220&password=")
request("POST","login.php","login=&password=")
```

Les trois réponses correspondantes sont ensuite analysées. Si elles contiennent des messages d'erreur SQL, `W3af` informe l'utilisateur que l'application est vulnérable

3. `http://w3af.sourceforge.net`
4. Ce qui est nécessaire avant d'envoyer une requête HTTP contenant des caractères spéciaux.

à une injection SQL. Pour détecter la présence d'un tel message, cet outil effectue une recherche, dans la page, de motifs caractéristiques des messages d'erreur SQL provenant d'une base de données (en l'occurrence `Mysql_` et `Mysql_fetch_array()`). Aucun mécanisme supplémentaire n'est implémenté pour vérifier si la vulnérabilité existe réellement ou pas. Or, un tel message d'erreur ne provient pas nécessairement du serveur de bases de données lui-même. Il peut très bien avoir été produit par le serveur Web lui-même en analysant les données en entrée. Et même si le message a été généré par le serveur SQL, il n'est pas possible d'affirmer avec certitude à la réception de ce message qu'une injection SQL est possible. En effet, ce message signifie que pour cette requête, les données en entrée n'ont pas été assainies. Mais il ne signifie pas pour autant que le serveur n'assainie pas systématiquement toutes les requêtes.

Un algorithme plus performant est utilisé par `W3af` dans le module `formAuthBrute`. Ce module réalise une attaque par dictionnaire sur un formulaire d'authentification (il tente un grand nombre de couples *nom d'utilisateur / mots de passe*). L'algorithme fonctionne en deux temps. Tout d'abord, il envoie deux requêtes construites de la manière suivante [5] :

```
request("POST","login.php","login="+randomChar(8)+"&password="+randomChar(8))
request("POST","login.php","login="+randomChar(8)+"&password=")
```

Les noms d'utilisateur et mots de passe associés à ces requêtes sont générés aléatoirement. Les réponses à ces deux requêtes (notées `refA` et `refB`) seront donc vraisemblablement des pages de *rejet*. Elles sont conservées et serviront de témoins. Ensuite, le module réalise l'attaque par dictionnaire. Durant cette attaque, les requêtes sont formées à partir d'un dictionnaire, par exemple :

```
request("POST","login.php","login=admin&password=azerty")
```

Chaque réponse (notée `respC`) est comparée aux témoins `refA` et `refB`. Cette comparaison s'appuie sur une distance mesurant la différence entre deux chaînes de caractères. Elle est calculée à l'aide de la distance de Levenshtein[14] et renvoie une valeur dans l'intervalle $[0, 1]$. Cette distance est basée sur l'évaluation du nombre de transformations nécessaires pour obtenir la première chaîne à partir de la seconde (ajout d'un caractère, suppression d'un caractère, etc.). Si la distance vaut 0, les pages sont identiques. Si la distance vaut 1, les pages sont complètement différentes. `W3af` considère que la page `respC` est une page d'*exécution* si les distances entre cette page et les pages `refA` et `refB` sont supérieures à $0,65$. Sinon, cette page est considérée comme une page de *rejet*. La valeur $0,65$ peut être configurée par le développeur de manière empirique.

Cependant, cet algorithme peut générer des faux négatifs si les pages renvoyées par le serveur suite à une authentification réussie ou échouée sont très proches (cf. section 5 pour un exemple).

5. La fonction `randomChar(num)` génère aléatoirement une chaîne de `num` caractères alphanumériques.

3.2 Skipfish

`Skipfish`[6] est un outil développé par Google, qui permet de détecter un grand nombre de vulnérabilités sur des serveurs Web. Il parcourt le site et collecte toutes les pages qui lui semblent stables. Les autres sont ignorées. Pour détecter si une page est stable, `Skipfish` envoie 15 requêtes identiques et compare les réponses correspondantes. Si les réponses sont similaires, la page est considérée stable. Ensuite, plusieurs tests sont réalisés sur ces pages stables.

En particulier, un de ces tests concerne les injections SQL. Cette vulnérabilité est testée grâce à 3 requêtes incluant chacune une injection SQL : *A*) `'"`, *B*) `\'\"` et *C*) `\\'\\"`. Les réponses à ces 3 injections SQL sont comparées deux à deux dans le but d'identifier la présence d'une injection SQL. Selon `Skipfish`, une vulnérabilité est présente si les réponses associées aux injections A et B ne sont pas similaires et si les réponses associées aux injections A et C ne sont pas non plus similaires. Le test de similarité utilise les fréquences d'apparition des mots dans les réponses.

Cette méthode présente les deux inconvénients suivants. Tout d'abord, le nombre de requêtes envoyées au serveur est faible. Or, il n'est pas inhabituel de trouver un site qui retourne des pages de *rejet* différentes. Par exemple, une page qui réagit à la requête A par une page de *rejet* contenant le message `saisie incorrecte`, et qui réagit aux requêtes B et C par une autre page de *rejet* contenant un message d'erreur SQL, sera considérée vulnérable à tort. Il est donc nécessaire d'utiliser plus de réponses pour réaliser une comparaison plus efficace.

Le second inconvénient provient de l'importance de l'ordre des mots dans un texte, qui est ignoré par la distance utilisée dans `Skipfish`. Ignorer l'ordre des mots peut amener à ignorer la sémantique d'une page et à nouveau peut amener à mal estimer si deux pages sont identiques ou non. Par exemple, les pages suivantes partagent le même vocabulaire, mais elles correspondent à une authentification réussie et échouée respectivement :

Your are authenticated, you have not entered a wrong login.

Your are not authenticated, you have entered a wrong login.

3.3 Wapiti

Wapiti est un outil développé en Python, en source libre[7]. Il est capable de détecter des injections SQL, des injections XSS, des mauvaises manipulations de fichiers, des injections LDAP, CRLF et des exécutions de commandes du système d'exploitation à partir d'une URL. Pour trouver ces vulnérabilités, il envoie des requêtes permettant d'exploiter des vulnérabilités et recherche des motifs correspondant à des messages d'erreur type dans les réponses produites. Cette recherche

6. `http://code.google.com/p/skipfish`
7. `http://wapiti.sourceforge.net`

est utile lorqu'une erreur, générée par exemple par le serveur de base de données, est propagée au client, par le site, sans modification. Par contre, si ce message d'erreur est modifié par le site, par exemple pour le rendre compréhensible par le client, alors cette recherche sera inefficace et ne pourra détecter de façon fiable la présence d'une vulnérabilité. Autrement dit, une recherche de motif correspondant à un message d'erreur n'est pas une technique suffisante pour s'assurer de la présence de vulnérabilités sur un site. En résumé, l'algorithme utilisé par cet outil présente les mêmes limites que celui utilisé par `W3af`.

4 Notre algorithme de détection de vulnérabilités

Notre algorithme de classification nécessite, en entrée, un *point d'injection*, c'est-à-dire une entrée d'une page dans laquelle il est possible d'injecter du code : un paramètre d'une URL ou un champ d'un formulaire. Dans la suite, sans perte de généralité, nous supposons que cette entrée est un champ d'authentification et nous nous intéressons uniquement aux injections SQL.

4.1 La classification de pages

Notre objectif est d'identifier, parmi un ensemble d'injections SQL à notre disposition, celles qui permettent effectivement de contourner l'authentification. Le principal défi réside dans l'automatisation de ce processus.

Nous proposons une méthode qui vise à réduire à la fois le nombre de faux positifs et faux négatifs, comparé aux solutions des outils que nous avons analysés.

L'expérience montre plusieurs points : *a*) les pages de *rejet* sont différentes des pages d'*exécution* en terme de contenu textuel, *b*) deux pages de *rejet* peuvent être différentes et *c*) deux pages d'*exécution* peuvent être aussi différentes. Pour s'en rendre compte, il suffit d'accéder à une page d'authentification d'un site et de tester la saisie de données valides et invalides. Par exemple, les réponses associées à des données valides contiendront des messages de bienvenue et les réponses associées à des données invalides contiendront des messages d'erreur PHP ou des messages d'erreur SQL. Le point important est l'existence de différences entre les pages de *rejet* et les pages d'*exécution*.

Notre approche vise à étudier ces différences afin de déterminer, parmi des réponses différentes, lesquelles sont des pages d'*exécution*. Pour débuter cette classification, nous avons besoin de requêtes initiales dont nous connaissons le type des réponses associées (*rejet* ou *exécution*). Clairement, il est plus facile de générer des requêtes qui engendrent une page de *rejet*. Il suffit par exemple de générer aléatoirement les noms d'utilisateur et mots de passe permettant de renseigner le formulaire d'authentification. Un autre exemple concerne les requêtes malformées générant des erreurs SQL. Les requêtes initiales seront donc de telles requêtes.

Dans notre approche, nous distinguons les trois ensembles de requêtes suivants :

R_{ea} est l'ensemble des requêtes générées à partir de mots aléatoirement choisis dans la liste [a-zA-Z]+. Vraisemblablement, ces requêtes engendrent des pages de *rejet*. Par exemple :
http ://address/directory/page.php ?login=ABCDEF&pass=ABCDEF

R_{ii} est l'ensemble des requêtes d'injection SQL inappropriées pour le *point d'injection*. Elles correspondent à des requêtes SQL qui sont syntaxiquement invalides. Elles sont construites de façon à ce que le serveur SQL qui interprète ces requêtes génère une erreur. Cette erreur peut être propagée au client ou capturée par le serveur web qui peut alors la reformuler et renvoyer un message d'erreur plus parlant pour le client. Par exemple :
http ://address/directory/page.php ?login=' ' '&pass=' ' '

R_{it} est l'ensemble des requêtes d'injection SQL qui sont construites dans le but de générer des pages d'*exécution*. Les réponses associées doivent donc être comparées aux réponses associées aux requêtes des ensembles R_{ea} et R_{ii}. Par exemple :
http ://address/directory/page.php ?login=test&pass=' or '1'='1

Nous notons également S_{ea}, S_{ii} et S_{it} les réponses associées aux requêtes R_{ea}, R_{ii} et R_{it} respectivement. Le principe de notre algorithme est alors le suivant : les requêtes R_{it} dont les réponses ne sont similaires à aucune des réponses S_{ii} et S_{ea}, sont considérées comme des injections SQL valides. Pour évaluer la similarité entre les pages renvoyées par les différentes requêtes, nous utilisons une technique de classification basée sur la distance présentée au paragraphe suivant.

4.2 La distance utilisée

Rappelons que la séquence des mots dans une réponse a une grande importance. En effet, les mêmes mots dans un ordre différent peuvent complètement changer la sémantique de la réponse. Aussi, pour calculer la distance, nous choisissons d'utiliser la différence normalisée entre deux réponses. L'opérateur de différence que nous utilisons est une version légèrement modifiée de la version de la commande Unix diff[15]. Soit a et b deux réponses de longueur n and m. La distance est formalisée ainsi [8] :

$$\mathsf{diff}(a_i, b_j) = \begin{cases} n - i + m - j & i = n+1 \text{ ou } j = m+1 \\ \mathsf{diff}(a_{i+1}, b_{j+1}) & a_i = b_j,\ i < n,\ j < m \\ \mathsf{diff}(a_{i+1}, b_{j+1}) & a_i = b_j,\ i < n,\ j < m \\ 1 + \min(\mathsf{diff}(a_{i+1}, b_j), \mathsf{diff}(a_i, b_{j+1})) & a_i \neq b_j,\ i < n,\ j < m \end{cases}$$

8. L'implémentation de diff ne respecte pas strictement cette définition. Elle est plus optimisée.

$$d(a,b) = \frac{\mathsf{diff}(a_1, b_1)}{(n+m)}$$

Cette distance permet de déterminer si deux réponses correspondent à des requêtes du même type ou pas. Pour cela, un seuil est nécessaire. Ce seuil peut varier d'un *point d'injection* à l'autre. En effet, il dépend de la taille des réponses et de la quantité de données qui changent entre deux réponses associées à des requêtes du même type. Nous choisissons ce seuil de façon empirique : la plus petite distance entre *i*) la distance la plus longue entre deux réponses dans S_{ea} et *ii*) la distance la plus longue entre deux réponses dans S_{ii} [9]. En utilisant ce seuil, nous sommes en mesure d'identifier des groupes de réponses qui sont similaires appelés grappes. Nous utilisons la technique de regroupement hierarchique [16].

A partir de cette classification, nous sommes en mesure d'identifier le type des requêtes. En sachant qu'une requête est associée à une réponse et vice versa, nous pouvons donc identifier le type de réponses. Pour identifier le type des requêtes dans R_{it}, l'algorithme suivant est utilisé :

1. Une requête faisant partie d'une grappe qui contient également une requête de R_{ea} ou de R_{ii} est une injection SQL invalide.
2. Une requête faisant partie d'une grappe qui ne contient aucune requête de R_{ea} et de R_{ii} est une injection SQL valide.

Cette méthode est illustrée dans la figure 1 suivante. Elle a été obtenue en utilisant l'algorithme de Kamada et Kawai [17] pour placer les points représentant les pages et l'algorithme de Graham [18] pour représenter la forme autour des grappes.

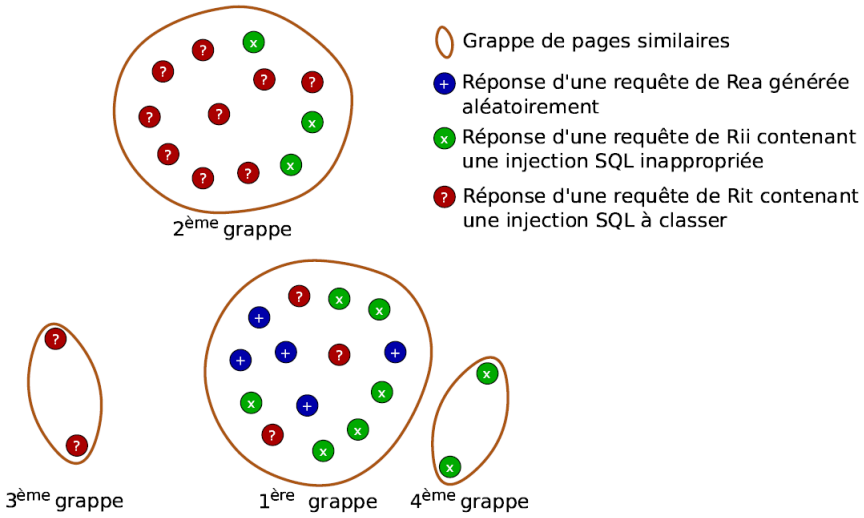
Dans cet exemple, la troisième grappe contient seulement des requêtes de R_{it} : ce sont des injections SQL valides. Cet exemple montre que notre approche présente moins de faux positifs que les approches existantes. En effet, dans la première grappe, nous trouvons à la fois des requêtes de R_{ea} et R_{it}. Cependant, cette grappe n'est pas la seule qui est associée à des requêtes qui engendrent des pages de *rejet* : il existe donc différents messages d'erreur pour cette page du site. D'autres outils (comme *Skipfish*) peuvent considérer les pages incluses dans la seconde grappe comme un succès simplement parce qu'elles sont éloignées des requêtes de la première grappe, qui, elles, auront été testées par ces approches. Cela mène à des faux positifs. Notre approche les évite.

5 Expérimentation

Dans cette section, nous présentons un cas d'étude de détection de vulnérabilités réalisé sur 5 applications à l'aide des 4 outils : `W3af`, `Skipfish`, `Wapiti` et un

9. Notons qu'il aurait été étrange d'établir ce seuil en nous basant sur les réponses S_{it}.

Figure 1. Exemple de classification des requêtes



outil implémentant notre algorithme. Dans un premier temps, nous présentons les 5 applications. Ensuite, nous détaillons les résultats de l'expérimentation.

5.1 Description des applications web et des vulnérabilités

phpBB-3. Cette application [10], est un gestionnaire de forum écrit en PHP et utilisant une base de données MySQL. Nous l'avons modifiée pour qu'elle contienne une vulnérabilité.

`v1` Cette vulnérabilité peut être exploitée par une injection SQL sur le formulaire d'authentification. Elle permet à un attaquant de contourner l'authentification et d'accéder à l'interface d'administration du forum. Par contre, si l'injection SQL employée par l'attaquant est inappropriée, une erreur liée à la base de données SQL est générée et transmise telle quelle au client. Ce dernier est alors face à un message difficile à comprendre s'il n'a aucune notion de programmation Web, SQL et de sécurité.

SecurePages. Cette application [11], écrite en PHP, est un coupe-feu permettant de protéger l'accès d'un site par authentification. Les couples valides pour cette authentification sont stockés dans une base de données. Nous avons volontairement ajouté une vulnérabilité (`v2`).

10. `http://www.phpbb.com`
11. `http://www.01php.com/fiche-scripts-126.html`

`v2` Cette vulnérabilité s'exploite par une injection SQL sur le formulaire d'authentification. Elle permet à un attaquant de contourner l'authentification et d'accéder directement au site protégé.

HardwareStore. Cette application est développée par nos soins en PHP-5. Elle permet, après authentification, d'enregistrer du matériel informatique dans une base de données MySQL et d'effectuer des recherches dans la description du matériel avec des expressions régulières. Nous avons injecté cinq vulnérabilités dans cette application.

`v3` Cette vulnérabilité s'exploite par une injection SQL dans le champ de recherche. L'application accède à la base de données en utilisant le compte `root` de MySQL. Ce compte dispose des droits `FILE`. Par conséquent, l'attaquant peut lire l'ensemble de la base de données et télécharger l'ensemble des fichiers du système en exploitant correctement la vulnérabilité.

`v4` Cette vulnérabilité s'exploite par une injection SQL dans le formulaire d'authentification. Elle permet de contourner l'authentification en fournissant, comme mot de passe, `x' or '1'='1` par exemple.

`v5` Cette vulnérabilité s'exploite par une injection SQL sur un paramètre de la requête. Contrairement aux précédentes vulnérabilités, le caractère apostrophe n'est pas nécessaire. De plus, nous avons fait le choix de suivre les recommandations de sécurité de PHP : nous avons désactivé l'affichage des erreurs au client.

`v6` Cette vulnérabilité est similaire à la vulnérabilité `v4` mais elle est utilisée dans des conditions différentes (les mêmes conditions que pour `v5` : désactivation de l'affichage des erreurs au client).

`v7` Cette injection SQL s'exploite sur la page de recherche des produits. Elle n'est accessible qu'après authentification réussie ou après l'exploitation de la vulnérabilité `v4`.

Insecure. Cette application a été développée en `Ruby` dans le cadre du projet Dali [12]. Elle correspond à un site de commerce en ligne, avec un système de gestion de panier virtuel et un système de saisie de commentaires. Elle contient volontairement une vulnérabilité de type SQL.

`v8` Cette vulnérabilité est une injection SQL exploitable depuis le formulaire d'authentification. Le seul détail qui la différencie de `v4` est le post-traitement des messages d'erreur : il est différent de celui réalisé par `Apache`.

12. Projet ANR du programme ARPEGE (2009-2011) (http ://dali.kereval.com)

Damn Vulnerable Web Application (DVWA). Cette application [13] est écrite en PHP et utilise un serveur MySQL. Elle contient volontairement plusieurs vulnérabilités. Nous nous focalisons sur l'une d'entre elles.

`v9` Cette vulnérabilité est une injection SQL qui permet à l'attaquant qui l'exploite de parcourir l'ensemble de la base de données. Elle est comparable à la vulnérabilité `v3`.

5.2 Expérimentation

		Outils de détection de vulnérabilités			
		`Skipfish`	`W3af`	`Wapiti`	Notre outil
Vulnérabilités	v1 `phpBB3`	×	×	✓	✓
	v2 `SecurePages`	×	×	✓	✓
	v3 `HardwareStore`	✓	✓	✓	✓
	v4 `HardwareStore`	✓	✓	×	✓
	v5 `HardwareStore`	✓	×	×	✓
	v6 `HardwareStore`	×	×	×	✓
	v7 `HardwareStore`	-	-	-	✓
	v8 `Kereval`	✓	✓	×	✓
	v9 `DVWA`	✓	✓	-	✓
Nombre de détections		5	4	3	9

✓ Vulnérabilité détectée par l'outil
× Vulnérabilité non détectée par l'outil
\- Vulnérabilité ignorée par l'outil

Figure 2. Synthèse des tests

Le tableau de la figure 2 résume la campagne de tests réalisée à partir des 5 applications présentées précédemment et des 4 outils de détection. Dans ce tableau, une vulnérabilité est considérée détectée si l'outil a effectivement détecté sa présence, indépendamment de la démarche suivie pour arriver à cette conclusion. Une vulnérabilité est considérée non détectée si l'outil a testé la présence de cette vulnérabilité sur le *point d'injection* correspondant, sans la détecter. Une vulnérabilité est considérée ignorée par l'outil si le *point d'injection* n'a pas été testé par l'outil. Dans ce dernier cas, la vulnérabilité ne peut pas avoir été detecté par l'outil correspondant.

Rappelons que les outils `W3af` et `Wapiti` utilisent des algorithmes basés sur une recherche de motifs d'erreur. Le tableau nous montre que, au delà des vulnérabilités ignorées par `Wapiti`, ces deux outils présentent des performances comparables. En particulier, `Wapiti` détecte les vulnérabilités `v1` et `v2`, tandis que `W3af`

13. `http://www.dvwa.co.uk`

ne les détecte pas. Inversement, `W3af` détecte les vulnérabilités `v4` et `v8` tandis que `Wapiti` ne les détecte pas. Par contre, notre outil nous permet de couvrir toutes ces vulnérabilités. Nous pouvons en conclure que notre approche apporte une meilleure couverture que les algorithmes utilisés par ces deux outils. Cela confirme les limites que nous avions énoncées concernant ces algorithmes.

Pour les vulnérabilités `v1` et `v2`, nous avons vérifié manuellement les injections testées par `Skipfish` (`'"`, `\'\"` et `\\'\\"`) et conservé les pages retournées correspondantes (respectivement `A`, `B` et `C`). `Skipfish` considère entre autres que les pages `A` et `C` doivent être différentes pour qu'une vulnérabilité soit présente. Or, pour ces deux *points d'injection*, ce n'est pas le cas. Les réponses correspondent à des messages d'erreur SQL qui se ressemblent. `Skipfish` ne détecte donc pas ces vulnérabilités. Cette situation confirme qu'il est important de diversifier les tests réalisés et, par conséquent, d'utiliser une technique de classification pour analyser les résultats.

Concernant les vulnérabilités `v5` et `v6`, elles sont incluses dans des pages PHP pour lesquels nous avons volontairement désactivé les rapports d'erreur (à l'aide de la directive `error_reporting(0)`). Cette désactivation est notamment conseillée dans le fichier de configuration de PHP5 [14]. On constate, dans cette configuration, que les 3 outils `Skipfish`, `W3af` et `Wapiti` ne sont plus capables de détecter les vulnérabilités puisqu'ils s'appuient sur ces messages d'erreur.

Un dernier point important à noter concerne la vulnérabilité `v7`. Non seulement notre outil est le seul à l'avoir détectée, mais en plus les autres outils n'ont pas testé le *point d'injection* correspondant. Ce *point d'injection* n'est accessible qu'après avoir franchi la page d'authentification soit avec le bon couple *nom d'utilisateur / mot de passe* soit par l'exploitation de la vulnérabilité `v4`. Notre outil étant capable d'identifier précisément une requête permettant d'exploiter cette dernière, le *point d'injection* est devenu accessible à notre outil automatiquement, sans notre intervention. Pour les autres outils, il est nécessaire d'intervenir manuellement pour leur permettre de franchir la page d'authentification. Notons que `Wapiti` ne pouvait pas détecter cette vulnérabilité puisqu'il ne détecte pas `v4`.

Dans cette expérimentation, nous n'avons pas approfondi l'étude des faux positifs. Ces travaux sont en cours. Néanmoins nous avons constaté un cas intéressant concernant un des champs de recherche d'une page de notre application `HardwareStore`. En effet notre application considère que ce champ peut contenir le méta-caractère (`'`) qui permet d'effectuer des recherches contenant des chaînes de caractères avec des espaces. Cette possibilité peut être inhibée à l'aide du caractère *backslash* (\). Le comportement de cette page satisfait le critère de `skipfish` sans pour autant correspondre à une vulnérabilité (cf. Section 3.2).

14. "For production web sites, you're strongly encouraged to turn this feature off, and use error logging instead".

6 Conclusion

Dans cet article, nous avons présenté un nouvel algorithme permettant d'automatiser et d'améliorer la détection de certaines vulnérabilités des sites Web. Cet algorithme utilise des techniques de classification de pages et est capable de fournir la requête d'injection de code permettant l'exploitation de la vulnérabilité détectée. Nous avons présenté une expérimentation préliminaire qui nous a permis de montrer la pertinence de notre approche, et de montrer certaines limites des trois scanners de vulnérabilités usuels en source libre que nous avons testés.

Cet algorithme n'a pour le moment été testé que pour des vulnérabilités de type injection SQL. Nous comptons à présent l'étendre à tout type d'injection de code, l'expérimenter à plus large échelle en considérant d'autres applications vulnérables et mener une campagne visant l'étude des faux positifs.

Remerciements

Ces travaux ont été partiellement réalisés dans le cadre du projet ANR DALI [15] (*Design and Assessment of application Level Intrusion detection Systems*) du programme ARPEGE. Nous tenons à remercier aussi Yves Deswarte, Karama Kanoun et Hélène Waeselynck pour leur contribution à ces travaux.

Références

1. Christey, S., Martin, R., *Vulnerability type distributions in CVE*, Mitre report, May 2007 `http://cwe.mitre.org/documents/vuln-trends/index.html`[accessed on 02/22/10]
2. Huang, Yao-Wen and Yu, Fang and Hang, Christian and Tsai, Chung-Hung and Lee, Der-Tsai and Kuo, Sy-Yen, *Securing web application code by static analysis and runtime protection* .WWW '04 : Proceedings of the 13th international conference on World Wide Web, , p-p 40–52, New York, USA, 2004.
3. Y. Minamide *Finding Security Vulnerabilities in Java Applications with Static Analysis*. In WWW '05 : Proceedings of the 14th International conference on World Wide Web, 2005.
4. V. B. Livshits, and M. S. Lam *Static approximation of dynamically generated Web pages*. In Proceedings of the 14th Usenix Security Symposium, Aug. 2005.
5. Huang, Yao-Wen and Huang, Shih-Kun and Lin, Tsung-Po and Tsai, Chung-Hung. *Web application security assessment by fault injection and beh avior monitoring*, WWW '03 : Proceedings of the 12th international conference on World Wide Web, p-p 148–159, 2003.
6. T. Pietraszek and C. V. Berghe. *Defending Against Injection Attacks Through Context-Sensitive String Evaluation* . In Recent Advances in Intrusion Detection 2005 (RAID), 2005.
7. A. Nguyen-Tuong, S. Guarnieri, D. Greene, J. Shirley and D. Evans. *Automatically Hardening Web Applications Using Precise Tainting* . In IFIP Security 2005, 2005.
8. Kirda, Engin and Kruegel, Christopher and Vigna, Giovanni and Jovanovic, Nenad. *Noxes : a client-side solution for mitigating cross-site scripting attacks*, SAC '06 : Proceedings of the 2006 ACM symposium on Applied computing, p-p 330–337, New York, USA, 2006.

15. `http://dali.kereval.com`

9. Top 10 vulnerability scanners, Sectools Website
URL : `http://sectools.org/web-scanners.html`[accessed on 02/22/10]
10. J.Fonseca, M. Vieira and H. Madeira, *Testing and Comparing Web Vulnerability Scanning Tools for SQL Injection and XSS Attacks*. In PRDC '07 : Proceedings of the 13th Pacific Rim International Symposium on Dependable Computing, pp. 365-372, Victoria, Australia, 2007.
11. J. Bau, E. Bursztein, D. Gupta, J. Mitchell, State of the art : Automated black-box web application vulnerability testing, IEEE Symposium on Security and Privacy, Oakland, USA, 2010
12. A. Doupé, M. Cova, G. Vigna, Why Johnny can't pentest : An analysis of black-box web vulnerability scanners, DIMVA 2010
13. Owasp Top ten, Owasp Website
`http://www.owasp.org/images/0/0f/OWASP_T10_-_2010_rc1.pdf`[accessed on 02/22/10]
14. Levenshtein, V., *Leveinshtein distance*, 1965
`http://en.wikipedia.org/wiki/Levenshtein_distance`[accessed on 02/22/10]
15. J. W. Hunt and M. D. McIlroy, *An Algorithm for Differential File Comparison*, Tech. Report CSTR 41, Bell Laboratories, Murray Hill, NJ, 1976.
16. S. C. Johnson, *Hierarchical Clustering Schemes*, Psychometrika Journal, pp. 241-254, Volume = 2, 1967.
17. Kamada, T. and Kawai, S., *An algorithm for drawing general undirected graphs*, Inf. Process. Lett., Volume 31, Number 1, pp. 7-15, issn=0020-0190, Elsevier North-Holland, Inc., 1989.
18. Ronald L. Graham, *An Efficient Algorithm for Determining the Convex Hull of a Finite Planar Set*, Inf. Process. Lett., Volume 1, Number 4, pp. 132-133, 1972.

Exemple d'application de la cyberdéfense

Julien Sterckeman

ANSSI/COSSI/BIS

Résumé Cet article propose d'illustrer, à travers un système d'information d'exemple, l'aspect technique de la cyberdéfense. Plutôt que se de concentrer sur la réaction face à une attaque, cet article détaille des mesures techniques préventives, relativement peu complexes à mettre en œuvre et peu coûteuses financièrement et humainement si elles sont appliquées dès la conception d'un réseau, d'un système ou d'une application. Elles ont pour but d'empêcher les compromissions, d'en limiter l'impact ou de permettre de les détecter, en appliquant le principe de la défense en profondeur.

1 Contexte

Les principes évoqués dans cet article seront illustrés au travers d'un système d'information d'exemple, reposant sur une architecture représentative pour un réseau déconnecté. L'hypothèse de travail est que ce système d'information traite des informations sensibles et est, à ce titre, isolé physiquement d'autres réseaux. Son but est de partager des informations, provenant de l'extérieur, entre les utilisateurs de plusieurs entités distinctes pour générer de nouvelles données (le schéma 1 représente le processus fonctionnel d'utilisation).

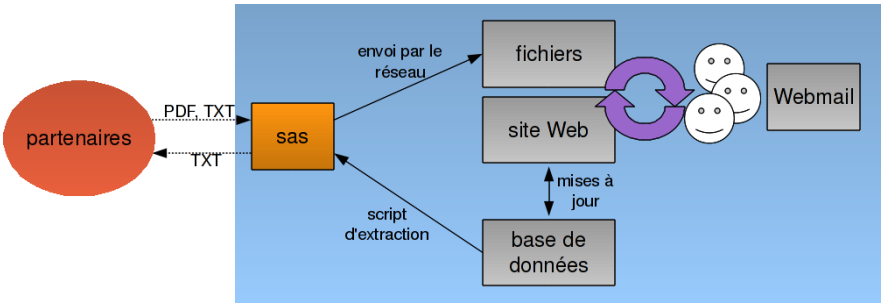


Figure 1. Processus fonctionnel du système d'information d'exemple

Les postes de ce réseau, sous Windows XP, sont ainsi répartis sur plusieurs sites, reliés par un nœud central (correspondant à une architecture en étoile). Ce site central héberge :

- des serveurs d'infrastructure (domaine Active Directory) ;
- un serveur de gestion de base de données ;

– un serveur Web hébergeant l'application principale (permettant de modifier les données de la base de données et offrant une traçabilité des modifications effectuées par les utilisateurs) et un Webmail ;
– un serveur de fichiers ;
– un sas.

Certaines entités disposent également d'un serveur de fichiers interne.

Les imports de données provenant de partenaires extérieurs ne doivent se faire qu'à travers le poste dédié à la fonction de sas, accessible uniquement aux administrateurs sur le site central. Les fichiers, de format PDF ou texte, déposés sur le sas sont ensuite transférés sur le serveur de fichiers. Les utilisateurs ne doivent pas pouvoir importer eux même des données, en particulier par clé USB ou CD-ROM.

Les exports de données, à destination des même partenaires extérieurs, sont réalisés grâce à un script qui extrait des informations de la base de données pour générer un important fichier texte, qui sera importé dans un autre réseau par un opérateur avec un support amovible.

Le schéma 2 présente l'architecture simplifiée du réseau d'exemple.

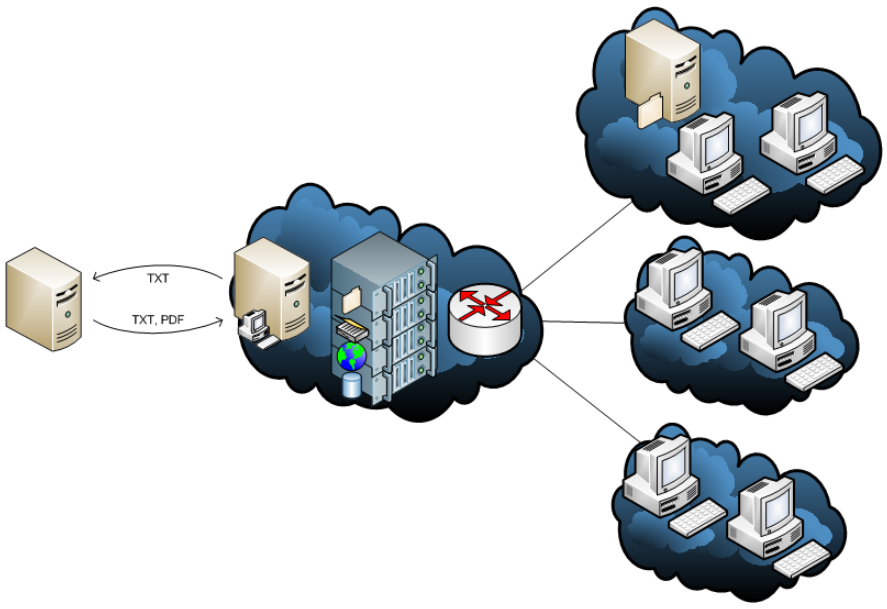


Figure 2. Schéma réseau simplifié du système d'information d'exemple

2 Démarche

La cyberdéfense ne se limite pas aux procédures et aux méthodes de supervision et de réaction : des méthodes de protection doivent être mises en place afin de diminuer le nombre d'incidents, en réduisant la surface d'attaque. Même si ce concept peut paraître évident, la réalité sur le terrain montre que la fonctionnalité *autoplay*[1] des périphériques amovibles est encore activée sur beaucoup de postes sous Windows, que les comptes par défaut des serveurs de gestion de base de données ne sont pas désactivés ou que leur mot de passe par défaut n'est pas changé, que beaucoup d'applications Web sont sujettes à des vulnérabilités de type *injection SQL*, que des serveurs et postes de travail se font encore compromettre à cause de vulnérabilités dont le correctif est disponible depuis plusieurs mois ou *via* des fichiers PDF malveillants utilisant du code JavaScript alors que tous les lecteurs permettent de désactiver cette fonctionnalité très peu utilisée. Ces faits ne sont pas acceptables du point de vue technique et organisationnel, puisque des contre-mesures, souvent triviales et sans impact fonctionnel significatif, existent mais ne sont simplement pas appliquées.

Lorsque l'on parle de sécurité, plusieurs fausses conceptions ressortent régulièrement :

- « *nous n'avons pas besoin d'une sécurité quasi-militaire.* » Que ce soit un réseau sensible ou public, les techniques de protection de base sont à appliquer. Les besoins de sécurité sont généralement mal qualifiés et beaucoup de personnes ignorent par exemple les problèmes de responsabilité et les obligations légales ;
- « *la sécurité coûte cher.* » La sécurité est souvent vue comme un ensemble de « briques » onéreuses (antivirus et outil de détection d'intrusion sur chaque poste, outil de *Data Loss Prevention* ou de contrôle des clés USB, système de détection d'intrusion réseau, etc.). Or, plutôt que d'ajouter des composants souvent inutiles qui n'augmentent pas significativement le niveau de sécurité (ces outils ne détectent pas tout et sont parfois trivialement contournables ou difficiles à configurer), il est préférable de commencer par activer les mécanismes de protection déjà intégrés dans les systèmes et les outils utilisés. Il vaut mieux mettre en place des moyens efficaces et simples, plutôt que des produits complexes, mal maîtrisés et pas toujours adaptés ;
- « *mettre en place des protections est inutile, puisqu'il y aura toujours des failles de sécurité et qu'une personne arrivera toujours à entrer.* » S'il est vrai qu'obtenir un très haut niveau de sécurité est difficile, il est toujours possible de corriger les vulnérabilités les plus simples et d'élever le niveau

1. Fonctionnalité de Windows réalisant l'exécution automatique d'un programme sur un support amovible lors de l'insertion de celui-ci, ou affichant à l'utilisateur plusieurs actions possibles, dont certaines dépendent du contenu du support.

nécessaire de compétence de l'attaquant. Il y a une grande différence entre une possible compromission réalisable en quelques secondes par une personne connaissant peu la sécurité et une possible compromission réalisable en quelques jours par une personne ayant des outils spécifiques (codes d'exploitation non publics, connaissance approfondie du fonctionnement d'une application, etc.). Si l'attaque est plus compliquée, elle prendra plus de temps et laissera plus de traces, ce qui augmentera les chances de la détecter. Ce raisonnement est identique à celui qui consisterait à dire qu'il est inutile de mettre des extincteurs dans des bureaux puisque ceux-ci ne permettent pas d'éteindre tous les types de feu.

Avant même de mettre en place des moyens de détection des attaques et de prévoir des procédures de réaction, il est nécessaire de s'assurer que les attaques de masse et les compromissions les plus simples ne soient pas réalisables. L'expression « *il vaut mieux prévenir que guérir* » s'applique également à l'informatique.

3 Analyse de risques

La première étape pour sécuriser le réseau est de réaliser une analyse de risques pertinente.

Dans le cas du réseau d'exemple, les besoins de sécurité correspondent à la confidentialité des données échangées (informations contenues dans la base de données, sur les serveurs de fichiers et dans les courriers électroniques), ainsi que leur intégrité et la traçabilité des actions des utilisateurs (notamment pour les ajouts et modifications dans la base de données). La disponibilité peut être également importante, mais elle ne sera pas prise en compte dans cet article.

En reprenant la terminologie EBIOS 2010, les sources de menace pertinentes sont :

- source humaine interne, malveillante, avec de faibles capacités : un utilisateur soudoyé ;
- source humaine interne, malveillante, avec des capacités importantes : un prestataire travaillant sur le réseau ;
- source humaine externe, malveillante, avec de faibles capacités : une personne intéressée par les informations traitées (concurrent avec des faibles moyens) ;
- source humaine externe, malveillante, avec des capacités importantes : une personne ayant la possibilité de faire importer des fichiers PDF par les administrateurs système et de récupérer une partie des données extraites automatiquement (concurrent direct) ;
- virus non ciblé : un programme importé involontairement par le sas.

Les principaux scénarios d'attaque envisageables sont :

- scénario 1 : un administrateur qui importe involontairement par le sas un virus (infectant automatiquement les fichiers présents sur les clés USB), à travers un document ou programme vérolé, effaçant ou modifiant des données ;
- scénario 2 : une personne malveillante branchée sur le réseau local d'une entité (prestataire ou utilisateur) qui accède à des données auxquelles elle ne devrait pas en compromettant un élément du système (postes de travail ou serveurs), en exploitant une vulnérabilité de celui-ci ou en utilisant des comptes valides ;
- scénario 3 : une personne connectée sur le réseau local d'une entité qui accède aux données de la base de données ou y exécute des actions non tracées en exploitant une vulnérabilité dans l'application Web ;
- scénario 4 : un utilisateur (ou programme s'exécutant dans son contexte) qui récupère des données de connexion (mot de passe du compte administrateur local, etc.) et les rejoue sur d'autres postes pour accéder à d'autres informations ;
- scénario 5 : une personne non autorisée qui accède physiquement au réseau, en utilisant un poste du réseau, en se connectant sur le réseau local d'une entité ou à une interconnexion entre les sites, dans le but de récupérer des données ;
- scénario 6 : une personne pouvant faire importer des fichiers sur le système par les administrateurs (typiquement sur le réseau d'où proviennent les fichiers importés par le sas) qui compromet un poste utilisateur grâce à un fichier PDF malveillant et qui tente de faire fuir de l'information grâce au script d'extraction automatique pour l'export ;
- une personne qui récupère à distance des informations traitées en récupérant des signaux parasites compromettants. Cette menace ne sera pas prise en compte dans le reste de cet article.

Il faut donc trouver des moyens de se protéger contre chacune de ces menaces, en mettant en place des mesures de sécurité multiples agissant à différents moments des scénarios d'attaques. L'application la plus large du principe de défense en profondeur (principes de prévention, de blocage, de tolérance et de détection [2]) permettra de répondre à ce besoin mais également de réduire les risques liés à des scénarios non identifiés au moment de l'analyse.

4 Prévention des vulnérabilités

Le premier axe de protection consiste à essayer d'empêcher les compromissions. Il faut ainsi agir sur l'origine des scénarios redoutés en supprimant des vulnérabilités, par exemple en réduisant la surface d'attaque.

2. Le dernier axe de la défense en profondeur, la réaction, ne sera pas abordé ici.

4.1 Accès physique au réseau par un tiers (scénario 5)

Pour prévenir les accès physiques non autorisés au système d'information (connexion directe sur le réseau ou accès à un poste de travail), plusieurs mesures doivent être mises en place, pour couvrir différents positionnements de l'attaquant :

- utilisation de chiffrement pour les liaisons non maîtrisées entre les sites ;
- mise en place de protections physiques pour limiter l'accès aux postes de travail, aux serveurs, aux équipements actifs et aux chemins de câbles ;
- utilisation d'une méthode d'authentification robuste pour l'ouverture de session sur les postes, en protégeant les éléments secrets lorsqu'ils ne sont pas utilisés ;
- interdiction de démarrer les systèmes sur un autre périphérique que le disque dur, en configurant le BIOS et en y définissant un mot de passe unique et complexe. Un scellé doit être apposé sur le boîtier pour détecter son ouverture *a posteriori*.

Avec ces quatre mesures, sous réserve de leur implémentation effective correcte, l'accès illégitime est fortement restreint.

4.2 Compromission des serveurs et des postes de travail (scénario 2)

Pour empêcher un utilisateur branché sur le réseau d'une entité de compromettre les serveurs ou des postes de travail, les principes de base de la sécurité informatique doivent être appliqués :

- utiliser des systèmes d'exploitation et des services maintenus (Windows XP SP3, Windows 2003 SP2, Oracle 11, etc.), pour disposer de correctifs de sécurité de la part de leur éditeur. Cela nécessite également d'effectuer une veille pour déterminer quand un composant deviendra obsolète [CERTA-2005-INF-003-009] et pour planifier sa migration. Il faut aussi garantir une non adhérence des applications utilisées vis-à-vis des systèmes d'exploitation ;
- appliquer les correctifs de sécurité des systèmes d'exploitation, des services et des applications, pour ne pas souffrir de vulnérabilités publiques dont les codes d'exploitation sont généralement disponibles sur Internet. Un serveur WSUS [UPDATEMS] devra pour cela être installé en central et un processus de qualification devra être mis en place pour valider le bon fonctionnement du système après chaque mise à jour, ainsi que la gestion des correctifs d'urgence ;
- définir des mots de passe complexes pour chaque service et chaque interface d'administration (Oracle, Webmail, commutateurs, routeurs, etc.). Il faudra auparavant déterminer les possibilités d'accès réseau à chaque composant utilisé.

Les techniques classiques de sécurisation des systèmes d'exploitation permettent également de réduire la surface d'attaque. Les postes de travail sous Windows XP SP3 doivent ainsi faire l'objet d'un durcissement de configuration [XPSECGUIDE] :

- suppression des protocoles réseau inutilisés : il faut par exemple désactiver NetBIOS sur TCP/IP (ports TCP 137, UDP 138 et TCP 139) qui n'est plus utilisé par SMB, celui-ci étant désormais directement transporté par TCP (port 445) ;
- désactivation des services Windows inutilisés :
  - « Explorateur d'ordinateur » : le voisinage réseau n'est pas utilisé dans un réseau professionnel, les répertoires partagés sont accessibles par des lecteurs réseau ;
  - « service de découvertes SSDP », « hôte de périphérique universel plug-and-play », « webclient », « configuration automatique sans fil », etc. : ces protocoles ne sont pas utilisés dans un réseau professionnel ;
- décochage de « partage de fichiers et d'imprimantes » dans la liste des protocoles des connexions réseau : les postes utilisateur n'ont pas vocation à partager des répertoires. Cette mesure rendra inaccessible le service « serveur » depuis le réseau. Il est intéressant de noter que le ver Conficker s'est répandu à l'origine en exploitant une vulnérabilité accessible grâce aux services « explorateur d'ordinateur » et « serveur » ;
- désactivation des sessions nulles, du stockage sous format LM des empreintes des mots de passe, etc.

Pour les serveurs, un travail identique doit être mené, même si plus de fonctionnalités doivent être accessibles (partage éventuel de fichiers, etc.).

Ainsi, les méthodes triviales pour compromettre une machine distante ne seront plus utilisables (exploitation d'une vulnérabilité dont le correctif est disponible, détermination d'un mot de passe par essais successifs et absence d'authentification pour certains accès).

4.3 Compromission du site Web (scénario 3)

Pour limiter les informations accessibles aux utilisateurs et pour empêcher qu'ils n'abusent l'application Web, il faut :

- que celle-ci gère des comptes utilisateur, des profils et des droits d'accès dans l'application Web ;
- mettre à jour son code si des correctifs sont disponibles ;
- développer l'application en respectant des critères de développement sécurisé pour éviter les vulnérabilités Web les plus courantes ;
- réaliser une évaluation incluant des audits de code source, voire des tests d'intrusion.

4.4 Rejeu des éléments d'authentification (scénario 4)

Un scénario classique de compromission consiste à rejouer des éléments d'authentification, préalablement obtenus sur d'autres systèmes. Aucune exploitation logicielle n'est nécessaire, le but est d'utiliser les fonctions d'accès à distance avec des éléments d'authentification valides. Sous Windows, lorsque le compte administrateur local est compromis, d'autres éléments d'authentification peuvent être récupérables, par exemple les mots de passe des comptes des administrateurs du domaine ou leur empreinte (en mémoire ou en modifiant les services auxquels ils se connectent).

Ainsi, la compromission du compte administrateur local par les utilisateurs (élévation locale de privilèges) doit être évitée. Il faut pour cela :

- appliquer les correctifs de sécurité du système d'exploitation ;
- restreindre au maximum les droits des utilisateurs. Plus les utilisateurs disposent de droits et de privilèges d'administration, plus ils pourront en abuser et plus l'impact d'un code malveillant déclenché involontairement sera important. Sous Windows, les utilisateurs ne doivent pas appartenir aux groupes « administrateurs » et « utilisateurs avec pouvoir » (ce dernier permet aisément de devenir administrateur grâce aux droits sur des fichiers système). Si certaines applications nécessitent des droits particuliers sur le système (écriture dans certains répertoires ou dans certaines parties de la base de registre, etc.), les ACL correspondantes doivent être positionnées. L'outil Microsoft [PROCMON] peut être utilisé pour déterminer les droits nécessaires d'une application sur les objets système. Il faut également s'assurer que le contrôle d'accès sur les fichiers système est correct [ACCESSENUM] ;
- empêcher le démarrage du système sur un autre périphérique que le disque dur (cf. scénario 5) ;
- limiter les logiciels installés au strict nécessaire. Dans le cas présent, un antivirus sur chaque poste de travail n'est pas nécessaire puisque les utilisateurs ne peuvent pas utiliser de clés USB. Les programmes de configuration des composants matériels qui sont lancés au démarrage (carte son, carte graphique, etc.) et non nécessaires doivent être déterminés [AUTORUNS] et désactivés. L'application du principe de minimalisation permet de diminuer la surface d'attaque locale et les risques de mauvaise configuration.

Dans le contexte de l'exemple, l'utilisation des clés USB doit être interdite sur les postes de travail. Plutôt que d'utiliser un logiciel tiers, qu'il faudra mettre à jour et qui peut entraîner des instabilités (un pilote noyau est toujours complexe à écrire) et des vulnérabilités, il est préférable d'utiliser la fonctionnalité de Windows le permettant [KB555324]. Pour empêcher l'utilisation des clés USB U3, la désactivation du support des CD-ROM est nécessaire [KB555324].

4.5 Compromission d'un poste grâce à un fichier PDF malveillant (scénario 6)

Dans le système d'information d'exemple, en l'absence d'antivirus sur les postes client, le seul logiciel de ceux-ci qui manipule des fichiers provenant de l'extérieur, donc potentiellement malveillants, est le lecteur de fichiers PDF. Pour réduire le nombre de ses vulnérabilités, il est nécessaire :

- d'utiliser une version maintenue du lecteur PDF ;
- d'appliquer le plus rapidement possible les correctifs de sécurité de ce logiciel.

4.6 Import involontaire de virus (scénario 1)

Un administrateur, en important les fichiers PDF, texte et exécutables (notamment pour la mise à jour du parc), peut infecter involontairement le sas. Pour limiter ce risque, il faut :

- appliquer rapidement les correctifs de sécurité du système et des applications ;
- désactiver toute fonctionnalité d'exécution automatique des supports amovibles sur le sas [KB967715] ;
- supprimer tout autre programme que l'antivirus et le programme d'épuration des fichiers PDF du sas.

5 Blocage des attaques

Le deuxième axe de protection consiste à bloquer les tentatives d'exploitation des vulnérabilités ou à rendre plus difficile leur succès.

5.1 Accès physique au réseau par un tiers (scénario 5)

Pour diminuer la quantité d'informations issue du site Web principal et du Webmail pouvant être recueillie par détournement de trafic réseau, le chiffrement applicatif (certificats serveur TLS valides reconnus par une autorité de certification incluse dans les navigateurs) est nécessaire. En plus d'empêcher un éventuel homme du milieu sur les réseaux locaux des entités de récupérer les informations accédées par les utilisateurs ciblés, ce mécanisme l'empêche aussi de pouvoir s'introduire dans la session HTTP des utilisateurs et donc d'effectuer des requêtes à leur place. Si la charge de travail supplémentaire est acceptable, une authentification par certificat des clients peut être mise en place. Dans le cas contraire, il est préférable d'activer sur le serveur Web l'authentification implicite native de Windows [WINDOWSAUTH], doublée éventuellement d'un mot de passe applicatif pour les accès aux ressources les plus sensibles. Il est à noter que la plupart

des navigateurs permettent d'activer l'utilisation de l'authentification intégrée de Windows.

Il est également nécessaire d'imposer une authentification pour l'accès à toute donnée (notamment sur les serveurs de fichiers). Des protocoles d'authentification éprouvés et ne faisant pas transiter en clair les secrets doivent être utilisés : il est inutile d'imposer des mots de passe complexes si ceux-ci sont facilement récupérables. Les comptes génériques doivent également être proscrits.

5.2 Compromission des serveurs et des postes de travail (scénario 2) et élévation locale de privilèges (scénario 4)

La compromission des postes passe souvent par l'exploitation d'une faille logicielle. Pour rendre plus difficile l'implantation d'un code malveillant, il est nécessaire d'activer :

- les mécanismes intégrés de Windows pour lutter contre l'exécution de code (DEP en mode permanent [KB875352]) ;
- les stratégies de restriction logicielle [SRP] : ce mécanisme intégré depuis Windows XP permet de limiter les possibilités d'exécution de programmes, par exemple d'après leur emplacement. Ainsi, si l'exécution de programmes n'est autorisée que depuis des répertoires sur lesquels les utilisateurs n'ont pas les droits en écriture, il leur sera impossible de lancer un exécutable qu'ils auraient réussi à importer (clé USB, CD-ROM, partage réseau, etc.). Selon les cas, cette protection peut être contournée en cas d'exécution de code arbitraire (par exemple avec un *shellcode* utilisé lors de l'exploitation d'une vulnérabilité logicielle), mais un exécutable éventuellement déposé dans un répertoire utilisateur ne pourra pas être lancé automatiquement au démarrage. Cette fonctionnalité a été remplacée par AppLocker depuis Windows 7.

Même si la majorité des services ouverts mais inutiles sur les postes et de travail et les serveurs a été désactivée dans la partie précédente, il est prudent d'activer le pare-feu intégré des postes en n'autorisant que les flux entrants réellement utilisés.

5.3 Compromission d'un poste grâce à un fichier PDF malveillant (scénario 6)

Pour réduire les risques d'exploitation d'une vulnérabilité du lecteur PDF, il est nécessaire :

- de le configurer de manière stricte, en désactivant les fonctionnalités non nécessaires : désactivation de l'interprétation du code JavaScript, du support des animations Flash et 3D, de la gestion de fichiers intégrés, etc. [ACROBAT] ;

– d'activer les mécanismes intégrés de Windows pour lutter contre l'exécution de code (DEP en mode permanent [KB875352]) ;
– d'épurer les fichiers PDF sur le sas, en convertissant temporairement le fichier en un autre format (par exemple PS), en modifiant les fichiers (suppression du code JavaScript [PDFID]) ou en refusant les fichiers PDF suspects (présence de fonctionnalités spéciales, de techniques d'obscurcissement, etc.).

L'application du principe de la multiplication des mécanismes de sécurité (d'une part la suppression du code JavaScript des fichiers PDF sur le sas et d'autre part la désactivation de l'interprétation dans les visualisateurs) permet de résister à une attaque si la configuration d'un seul élément est contournée.

5.4 Import involontaire de virus (scénario 1)

Dans le but de bloquer les éventuels virus présents sur des clés USB ou CD-ROM introduits dans le sas, il faut :
– installer un logiciel anti-virus à jour et renouveler régulièrement sa base de signatures ;
– appliquer des stratégies de restriction logicielle [SRP] (cf. section 5.2) ;
– idéalement, utiliser un autre système d'exploitation que celui des serveurs et postes de travail.

6 Tolérance aux compromissions

Le troisième axe de protection consiste à essayer de diminuer l'impact de l'exploitation réussie d'une vulnérabilité. Ainsi, toutes les techniques de cloisonnement, de diminution des informations accessibles et de contrôle des informations sortantes permettront de tolérer une compromission.

6.1 Accès physique au réseau par un tiers (scénario 5) et compromission d'un élément (scénario 2)

Si une personne arrive à se brancher sur le réseau local d'une entité, la présence d'un cloisonnement réseau peut l'empêcher d'accéder aux autres ressources :
– l'installation et la configuration d'un pare-feu ou de listes de contrôle d'accès sur le routeur central peut permettre, s'il est bien configuré, de limiter les rebonds entre les entités (les flux d'un site distant vers un autre doivent être bloqués). Du filtrage réseau entre la zone des clients et des serveurs permet également de ne pas exposer certaines interfaces (le serveur SQL ne doit pas être accessible directement depuis les clients par exemple). La liste complète des flux nécessaires doit être déterminée et formalisée. Enfin, la

séparation des postes des utilisateurs de ceux des administrateurs peut éviter des attaques par détournement de trafic pouvant permettre de récupérer des informations de connexion ;
- l'utilisation de *private VLAN*[3] au sein de chaque entité peut protéger les postes clients entre eux, aucune connexion directe entre deux postes utilisateur n'étant nécessaire ;
- l'activation sur les commutateurs de mécanismes de protection contre les attaques par empoisonnement de cache ARP [DIACISCO] permet d'éliminer une partie des risques de détournement de trafic, si la configuration des *private VLAN* n'est pas possible. Toutefois, ces mécanismes nécessitent généralement d'activer DHCP et le détournement de trafic est toujours possible par d'autres moyens. La configuration en statique des tables ARP est également envisageable si le nombre de postes de travail est restreint.

Concernant le partage de fichiers Microsoft, aucun mécanisme n'est disponible pour assurer la confidentialité des fichiers transmis sur le réseau, mis à part l'utilisation d'IPsec. Cette solution paraît cependant lourde à appliquer. Le cloisonnement réseau avec des *private VLAN* ou la protection contre l'empoisonnement de cache ARP sera à défaut la seule barrière technique contre ce scénario. Il convient alors, dans la mesure du possible, d'éviter d'accéder trop souvent aux informations sensibles des répertoires partagés.

6.2 Compromission du site Web (scénario 3)

Pour limiter les risques d'accès non autorisés à la base de données en cas d'exploitation réussie d'une vulnérabilité du site Web, il est possible :
- de supprimer ou désactiver les fonctions ou *packages* dangereux (par exemple la procédure stockée `xp_cmdshell` sur les versions anciennes de Microsoft SQL Server et les fonctions UTL sous Oracle), ou d'enlever les droits des utilisateurs sur ces fonctionnalités.
- de configurer des droits restreints pour les utilisateurs du SGBD (voire de créer un compte par utilisateur, sans compte générique) ;
- de n'utiliser que des procédures stockées, en spécifiant des droits, et d'interdire les accès directs aux tables.

6.3 Rejeu des éléments d'authentification (scénario 4)

De mauvaises méthodes d'administration peuvent introduire des vulnérabilités facilement exploitables une fois l'attaquant introduit dans le réseau.

3. Fonctionnalité permettant d'isoler les ports physiques d'un commutateur entre eux, en ne permettant que les communications avec un port défini.

La liste des comptes locaux (système ou applicatif) des postes utilisateur et des serveurs doit être établie. Le mot de passe qui leur est associé doit être suffisamment complexe et respecter la politique de gestion des mots de passe. Il faut également empêcher que la compromission d'un poste permette la compromission d'autres postes en utilisant ses comptes locaux (en particulier le compte local « administrateur »). Pour cela, plusieurs solutions peuvent être envisagées :

- spécifier des mots de passe différents pour chaque système, avec la lourdeur que cela implique pour les retrouver ;
- empêcher la connexion par le réseau des comptes locaux [ACCESRESEAU] et n'utiliser que des comptes du domaine pour l'administration.

Enfin, pour éviter que l'empreinte du mot de passe d'un compte du domaine trop privilégié ne soit récupérée dans la mémoire d'un poste de travail, il est préférable de ne pas utiliser le compte du domaine « administrateur », mais de placer temporairement un compte utilisateur peu privilégié dans le groupe « administrateurs » du domaine, le temps d'effectuer l'opération. Cette méthode est un peu contraignante mais efficace.

6.4 Compromission d'un poste grâce à un fichier PDF malveillant (scénario 6)

Le risque lié à la fuite d'informations potentielle du fait de l'utilisation du script d'extraction automatique peut difficilement être réduit. En effet, seule une vérification humaine peut garantir l'absence d'informations sensibles dans les données qui seront échangées. Cette vérification ne peut se faire que si l'utilisateur peut réellement décider de cette absence d'informations sensibles. Le format des données doit donc être simple (uniquement du texte ASCII ou type XML restreint) et les informations doivent toutes être visibles et vérifiables (caractères ASCII affichables uniquement, contrôle des métadonnées).

Un mécanisme de signature des données texte importées (labellisation « à la source ») pourrait également être mis en place pour permettre leur export sans vérification si leur intégrité est vérifiée. Cette méthode nécessite toutefois de pouvoir faire confiance au mécanisme de labellisation et d'analyser les problèmes de canaux cachés.

6.5 Import involontaire de virus (scénario 1)

Pour limiter les conséquences de l'exécution d'un virus sur le sas, il faut utiliser un compte non privilégié.

Enfin, pour empêcher qu'une compromission du sas (notamment en exploitant une vulnérabilité du moteur anti-virus) ne contamine automatiquement les fichiers importés auparavant, il faut que ces derniers soient rendus inaccessibles à partir

du sas. Il faut pour cela les transférer vers le serveur de fichiers en utilisant un mécanisme demandant explicitement un authentifiant (pour éviter la récupération automatique) et en utilisant un autre compte utilisateur (pour pouvoir gérer les droits d'accès de manière fine). Il est par exemple possible d'utiliser SFTP pour déposer les fichiers dans un répertoire temporaire du serveur de fichiers et de les déplacer ensuite dans la bonne arborescence, en utilisant un compte sur le serveur depuis une autre machine que le sas.

7 Détection des compromissions

Le dernier axe concerne la détection des compromissions. Le but n'est pas de détecter les tentatives d'intrusion, mais les signes d'une compromission avérée ou d'un comportement déviant.

Avant d'ajouter de la complexité et d'autres équipements réseau ou d'autres logiciels, il est préférable de commencer par tirer partie des journaux déjà présents :

- *a minima* les erreurs 403, 404 et 500 des serveurs Web ;
- les paquets rejetés par les pare-feux ;
- les échecs et dates de succès des authentifications sur les systèmes d'exploitation (comptes locaux et du domaine) ;
- les requêtes DNS sur des noms inexistants, ainsi que les demandes de transfert de zone ;
- les échecs de connexion sur le SGBD ;
- les journaux applicatifs Web (authentification et autorisation).

Pour faciliter le traitement des évènements suspects, il est nécessaire de mettre en place un système de centralisation des journaux. Il existe souvent des protocoles propriétaires pour envoyer les journaux vers une machine distante (avec WMI pour Windows par exemple), mais il préférable d'utiliser un protocole commun et public. Bien que toutes les implémentations disponibles ne permettent pas l'utilisation de TLS, le protocole `syslog` fait figure de standard :

- les routeurs et les pare-feux disposent presque tous nativement de cette fonctionnalité ;
- il existe des programmes sous Windows pour envoyer régulièrement les journaux d'évènements vers un serveur `syslog` ([AGENTSNARE] ou [NTSYSLOG]) ;
- il est envisageable d'adapter le code d'un client libre existant pour gérer d'autres formats de fichiers de journaux (journaux applicatifs Web, journaux du SGBD, etc.) ;
- des serveurs `syslog` libres sont disponibles sous Windows, si l'installation d'un autre système d'exploitation pour ce serveur n'est pas envisageable, bien qu'un peu d'hétérogénéité maîtrisée soit préférable.

À partir des évènements récoltés, stockés dans des fichiers plats ou dans une base de données SQL, il est possible d'écrire des scripts simples, à lancer régulièrement, qui ignorent les faux-positifs récurrents (erreur 404 sur l'icône d'un site Web par exemple) et qui envoient un courrier électronique aux personnes pertinentes avec les évènements restants.

La plupart des actions malveillantes seront détectées par ces mécanismes simples, qui ne nécessitent pas d'investissement lourd ni une charge d'exploitation trop importante.

8 Analyse des risques résiduels

L'analyse des risques résiduels permet de connaître les scénarios d'attaque envisageables de manière effective après la mise en place de toutes les contre-mesures évoquées précédemment. Le niveau requis de l'attaquant et la probabilité associés au scénario peuvent donc plus facilement être déterminés.

Voici par exemple l'analyse du scénario 1 et du scénario 6.

Concernant l'import involontaire de virus sur le sas, le risque résiduel est créé au final par un virus :

↪ connu : *checkmark* bloqué par l'antivirus dont la base de signatures est à jour

↪ **nouveau**

- ↪ se propageant par autoplay : *checkmark* protégé par la désactivation de l'autoplay
- ↪ s'exécutant automatiquement depuis la clé USB : *checkmark* bloqué par la configuration des stratégies de restriction logicielle (SRP)
- ↪ ayant infecté un document bureautique : *checkmark* protégé par l'absence de lecteurs sur le sas, mais scénario envisageable dans un second temps sur les postes utilisateur
- ↪ **ayant infecté un exécutable** : *bigtimes* impact *a priori* limité par le compte peu privilégié, par l'impossibilité d'accéder automatiquement aux fichiers importés auparavant et par la configuration des SRP.

Ainsi, les virus se propageant automatiquement par clé USB (de type *Conficker* ou *Stuxnet*) seront inopérants et seuls les exécutables infectés par un nouveau virus et copiés par l'utilisateur du sas lui-même auront une chance de fonctionner (cas d'une mise à jour vérolée).

Pour la compromission d'un poste par un fichier PDF malveillant, il faudrait que celui-ci :

↪ exploite une faille corrigée : *checkmark* protégé par le lecteur PDF à jour

↪ **exploite une faille non corrigée**

↪ dans le traitement d'une fonction JavaScript : *checkmark* bloqué par la désactivation du JavaScript dans les lecteurs et par l'épuration sur le sas

↪ **dans la structure PDF**

↪ avec une fonctionnalité particulière : *checkmark* bloqué par l'épuration sur le sas (ou la conversion dans un autre format) et par la désactivation des fonctionnalités inutiles du lecteur. La présence de vulnérabilités dans le programme d'épuration ou de conversion peut néanmoins rendre ce scénario exploitable.

↪ **sans fonctionnalité particulière**

↪ en utilisant JavaScript (par exemple pour du *heapspray*[4]) : *checkmark* bloqué par la désactivation du JavaScript dans les lecteurs et par l'épuration sur le sas

↪ **sans utiliser JavaScript**

↪ avec une technique d'exploitation simple : *checkmark* bloqué par l'activation de DEP

↪ **avec une technique d'exploitation contournant DEP**

↪ écrivant dans un répertoire système : *checkmark* bloqué par les droits de l'utilisateur non administrateur

↪ exécutant un programme : *checkmark* bloqué par la configuration des SRP

↪ **exécutant un programme en contournant les SRP** : *bigtimes* impact limité par le compte peu privilégié et la configuration des SRP pour le lancement au démarrage suivant

Le niveau requis de l'attaquant devant réaliser ce genre de document malveillant est ainsi élevé et la portée de son attaque n'est pas très étendue.

9 Conclusion

En conclusion, le volet technique de la cyberdéfense peut être implanté par des moyens simples (qui existent et ne demandent qu'à être appliqués), à condition d'avoir une analyse de risque pertinente et des mesures adaptées mises en place dès la conception. Certains contextes nécessiteront toutefois l'implantation de solutions plus riches, par exemple pour la détection de scénarios élaborés d'attaque.

Il faut privilégier des systèmes simples qui utilisent des protocoles standards et interopérables, en profitant de toutes les fonctionnalités intégrées (y compris pour

4. Technique consistant à remplir la mémoire, à l'aide de chaînes de caractères JavaScript, pour fiabiliser une exploitation logicielle, si certaines adresses mémoire ne sont pas prédictibles.

la détection). La maîtrise du système et des applications (flux de communication, configuration possible et fonctionnement interne) est nécessaire pour cela.

Le principe de défense en profondeur et la multiplication des mesures de protection rendra le système robuste, même en cas de compromission d'un élément. Tout le travail de supervision, de détection et de réaction servira alors à gérer les réels problèmes d'attaques interactives et de compromission plutôt que les attaques de masse, bloquées par les défenses mises en place.

Il est nécessaire de mettre en place un processus continu d'amélioration et d'affinement des contre-mesures, en analysant les techniques de contournement utilisées par les attaquants, en trouvant des moyens pour les reconnaître et les bloquer.

Enfin, la démarche est identique quel que soit le système d'exploitation : ce n'est pas parce qu'il y a moins d'exploits publics sur certains systèmes que des exploits privés n'existent pas (ceux dont la « cyberdéfense » veut se protéger).

Références

[CERTA-2005-INF-003-009] *Les systèmes et logiciels obsolètes*
`http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/index.html`

[UPDATEMS] *Guide Microsoft des mises à jour de sécurité*
`http://www.microsoft.com/downloads/details.aspx?FamilyID=c3d986d0-ecc3-4ce0-9c25-048ec5b52a4f&displaylang=fr`

[KB555324] *555324 : HOWTO : Use Group Policy to disable USB, CD-ROM, Floppy Disk and LS-120 drivers*
`http://support.microsoft.com/kb/555324`

[ACCESSENUM] *AccessEnum*
`http://technet.microsoft.com/fr-fr/sysinternals/bb897332.aspx`

[AUTORUNS] *AutoRuns pour Windows*
`http://technet.microsoft.com/fr-fr/sysinternals/bb963902.aspx`

[ACROBAT] *Acrobat enhanced security*
`http://www.adobe.com/go/acrobat_security` et `http://learn.adobe.com/wiki/download/attachments/64389123/Acrobat_EnhancedSecurity.pdf`

[KB875352] *KB875352 : Description détaillée de la fonctionnalité Prévention de l'exécution des données*
`http://support.microsoft.com/kb/875352`

[PDFID] *Outil pdfid permettant d'analyser des fichiers PDF et de supprimer le code JavaScript*
`http://blog.didierstevens.com/programs/pdf-tools/`

[KB967715] *KB967715 : Procédure de désactivation de la fonction d'exécution automatique dans Windows*
`http://support.microsoft.com/kb/967715`

[SRP] *Using Software Restriction Policies to Protect Against Unauthorized Software*
`http://technet.microsoft.com/en-us/library/bb457006.aspx`

[XPSECGUIDE] *Guide de sécurité Windows XP*
`http://technet.microsoft.com/fr-fr/library/dd548379.aspx`

[DIACISCO] *Configuring Dynamic ARP Inspection*
`http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.1/19ew/configuration/guide/dynarp.html`

[WINDOWSAUTH] *Mod_ntlm module pour Apache*
`http://modntlm.sourceforge.net`

[PROCMON] *Process Monitor*
`http://technet.microsoft.com/fr-fr/sysinternals/bb896645.aspx`

[ACCESRESEAU] *Refuser l'accès à un ordinateur à partir du réseau*
`http://technet.microsoft.com/fr-fr/library/cc758316(WS.10).aspx`

[AGENTSNARE] *SNARE - Auditing and EventLog Management*
`http://sourceforge.net/projects/snare/`

[NTSYSLOG] *NTsyslog*
`http://ntsyslog.sourceforge.net/`

De l'importance de l'ergonomie dans la Cyber Défense

Sébastien Héon et Louis Granboulan

EADS

1 Défense : un triptyque

1.1 Introduction

Un système d'information (SI) est complexe et en évolution constante. Tous les jours, des serveurs et des stations de travail sont remplacés ou déplacés, des applications sont mises à jour, des disques durs et des alimentations électriques tombent en panne. Le SI est presque un organisme vivant qui évolue au rythme de l'organisation qu'il soutient et qui a, sinon une histoire, au moins un historique. Le Livre blanc sur la défense et la sécurité nationale le compare d'ailleurs au système nerveux de nos sociétés et note que « dans les quinze ans à venir, la multiplication des tentatives d'attaques menées par des acteurs non étatiques, pirates informatiques, activistes ou organisations criminelles, est une certitude ». [1]

En effet, les SI subissent des attaques informatiques de plus en plus nombreuses et sophistiquées car l'attaquant n'a pas besoin de matériel évolué pour les conduire et il ne risque quasiment pas d'être démasqué. S'il est délicat de chiffrer avec précision les préjudices dus à ces attaques (indisponibilité de services, vols de secrets, vol d'identité, chantage, ...), le ver Stuxnet vient de démontrer qu'elles pourraient avoir un impact majeur sur notre vie quotidienne en perturbant le fonctionnement de sites industriels sensibles. [2]

Des exemples plus anciens avaient déjà montré la fragilité de nos infrastructures critiques face aux cyber attaques. Le projet américain Aurora avait prouvé en 2007 qu'une attaque informatique pouvait conduire à l'explosion d'un générateur électrique. De même, en janvier 2008, la CIA annonçait : *"We have information, from multiple regions outside the United States, of cyber intrusions into utilities, followed by extortion demands. [Ě] We have information that cyber attacks have been used to disrupt power equipment in several regions outside the United States. In at least one case, the disruption caused a power outage affecting multiple cities".* [3]

1. Le Livre blanc sur la défense et la sécurité nationale - p. 53
2. Voir par exemple : http ://fr.wikipedia.org/wiki/Stuxnet
3. Voir `http://www.sans.org/newsletters/newsbites/newsbites.php?vol=10&issue=5`

1.2 Une sécurité qui évolue

Face à ces attaques potentiellement dangereuses, les SI doivent être protégés. Leur complexité et leur évolution constante, tant au niveau de l'architecture que des applications qu'il héberge, tendent à aggraver ses vulnérabilités. En l'état, il est illusoire d'espérer un SI intrinsèquement sûr et dénué de toute faiblesse, de même qu'il est illusoire de vouloir cartographier les faiblesses de manière exhaustive pour les réduire définitivement.

Les premières recommandations de la sécurité des systèmes d'information consistaient à assurer une protection périmétrique de son SI, voire de l'isoler au maximum pour empêcher toute intrusion. Mais les évolutions sociétales, nos manières de travailler et de communiquer ont forcé leur ouverture progressive sur l'extérieur. L'apparition puis la banalisation des clés USB a accéléré la porosité des SI en facilitant l'entrée et la sortie d'informations.

En parallèle, on a réalisé la fragilité d'une défense périmétrique des SI pouvant conduire à recréer des *lignes Maginot* de l'informatique : une seule barrière, un exosquelette dans le meilleur des cas, qui, une fois contournée, laisse le coeur sans défense. Le concept a donc évolué de la défense périmétrique à la défense en profondeur qui « consiste à exploiter plusieurs techniques de sécurité afin de réduire le risque lorsqu'un composant particulier de sécurité est compromis ou défaillant ».[4] La défense des SI s'est donc structurée progressivement.

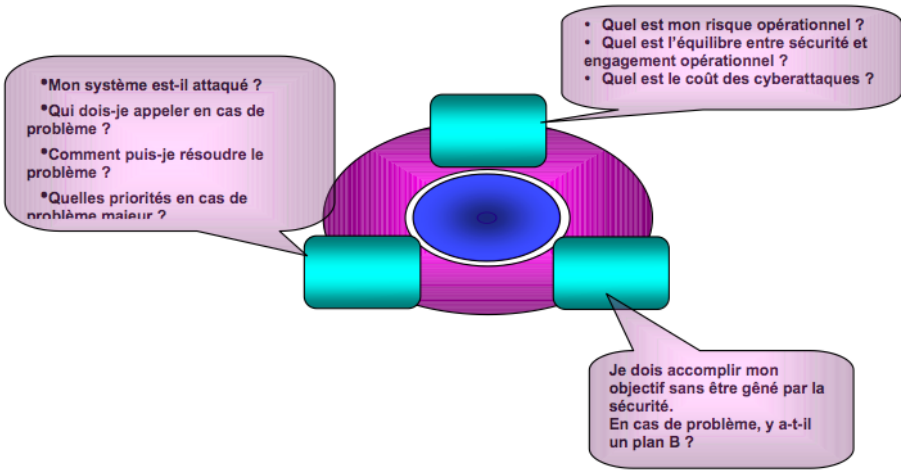
Face à une menace technologique, il était tentant d'apporter d'abord une réponse technologique. Contre les virus, des antivirus, contre les intrusions, des firewalls, contre l'écoute, le chiffrement, etc. Mais cette logique de l'épée et du bouclier, cette accumulation de boîtiers, a rapidement prouvé ses limites.

1.3 Apporter à chacun l'information pertinente

En effet, cela révèle une vision à court terme des enjeux de sécurité, sans stratégie aucune. Il n'y a pas d'approche holistique permettant d'évaluer les risques, de planifier les investissements, et de mesurer la sécurité. Pour pallier cette approche *par le bas*, des méthodes formelles d'analyse de risque, dont la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité), ont été développées et sont dorénavant couramment utilisées en complément d'une politique globale de sécurité des systèmes d'information (PSSI).

Mais, la politique de sécurité, vision formelle à long terme, n'a pas le même cycle de vie que la supervision technique de la sécurité qui demande, elle, une capacité de réaction rapide. Assurer la cohérence entre ces deux aspects est pourtant essentiel pour apporter à chaque acteur du SI l'information dont il a besoin.

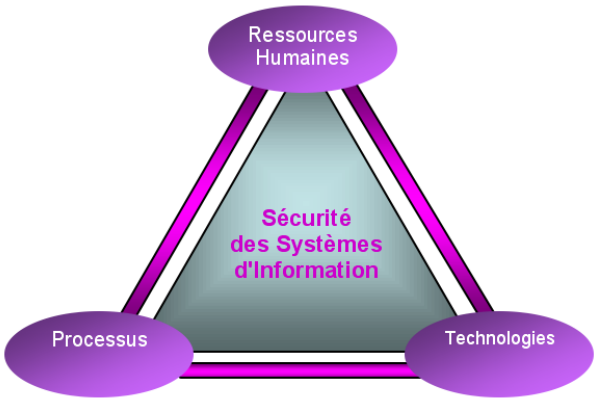
4. http://fr.wikipedia.org/wiki/D\%C3\%A9fense_en_profondeur



La figure ci-dessus illustre quels sont les différents angles d'approche de la sécurité des SI. L'opérateur qui supervise la sécurité s'intéresse au *quoi* (technique) et au *comment* (processus métier). En cas d'alerte, il doit savoir comment réagir et comment fixer ses priorités avant de corriger les problèmes techniques. La vision stratégique et l'aide à la décision (le *pourquoi* et le *combien*) doit être apportée au décideur de manière à ce qu'il puisse définir le juste équilibre entre risque opérationnel et investissements dans la sécurité. Enfin, l'utilisateur final, quant à lui, souhaite que la sécurité ne le bride pas dans ses activités quotidiennes. Il doit simplement savoir comment réagir en cas d'incident.

1.4 La place de la technologie : vers un nouvel équilibre ?

Afin de s'adapter à ces différentes problématiques, la sécurité des SI doit franchir un palier et s'abstraire des couches technologiques basses pour venir s'intégrer tout au long de la chaîne de traitement de l'information, utilisateurs, techniciens et décideurs. Il faut donc une vision globale qui s'appuie sur trois composantes indissociables : des technologies de pointe, des processus opérationnels formalisés, et des ressources humaines efficacement formées et entraînées. Ce triptyque garantit une gestion de la sécurité des systèmes d'information adaptée à l'organisation et à ses acteurs.



2 Attaque : la menace existe

Nous ne décrirons pas dans cet article les techniques d'attaques, courantes ou bien originales, qui menacent les systèmes d'information, mais elles sont nombreuses et variées.

Les attaques sont en réalité une petite partie des comportements anormaux d'un système d'information, et la plupart des comportements anormaux peuvent être négligés. La visualisation d'une attaque doit donc commencer par éliminer le bruit, ce qui se fait habituellement grâce à des outils de corrélation regroupant ensemble les nombreux événements pouvant être ignorés. Il faut ensuite relier entre elles les différentes étapes de l'attaque, ce qui se fait souvent aussi au moyen d'un corrélateur. La visualisation de l'attaque permet alors de qualifier l'intention et l'impact de l'attaque.

Il est important, lorsqu'on prépare une Cyber Défense, de bien considérer que la source de l'attaque n'est pas nécessairement externe. Il n'y a pas de statistiques fiables sur les attaques, d'une part parce que les meilleures attaques sont celles qui n'ont pas été détectées, et d'autre part parce que les attaqués en font rarement la publicité. Mais on peut sans aucun doute affirmer que le nombre des attaques est en grande augmentation, et que la technicité des meilleures attaques est en constante progression.

3 Technologie : l'artisanat et le commerce

Il est autant de façons de mettre en place la technologie nécessaire à la surveillance d'un système d'information que de systèmes d'information. Aux deux extrêmes, il y a l'approche artisanale développée entièrement par le responsable de la sécurité du système, et l'approche commerciale où est installé un produit standard configuré par le vendeur. Entre ces deux extrêmes, on trouve des com-

promis parfois malheureux, qui récupèrent les défauts des deux approches. C'est pour éviter cela que nous mettons ci-dessous en valeur ces défauts.

3.1 L'approche commerciale pêche par sa standardisation

Une solution de Cyber Défense facile à déployer, bien documentée, commercialisée avec un support, pourrait apparaître comme étant idéale. C'est ce que déploient en général les particuliers, qui se contentent d'installer l'antivirus recommandé par le fabricant ou par des connaissances. L'équivalent pour un réseau d'entreprise est l'installation d'un firewall, d'un IDS, d'un analyseur de logs, et de tout autre boîtier ayant bonne presse. À cela, il convient d'ajouter des mises à jour de sécurité aussi fréquentes que nécessaire.

Malheureusement, l'attaquant peut lui aussi avoir accès à la documentation de cette solution de Cyber Défense, et vérifier que son attaque est indétectable avant de lancer la dite attaque. En réalité, le système n'est protégé que contre les attaques standardisées, qui sont en effet nombreuses et souvent non ciblées (par exemple la dissémination de vers tels que Conficker) ou bien de technicité faible (les attaques de *script-kiddies*[5]).

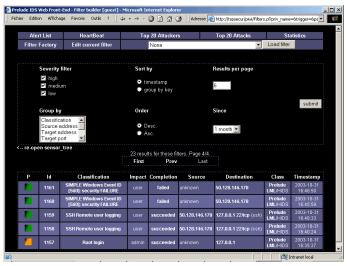
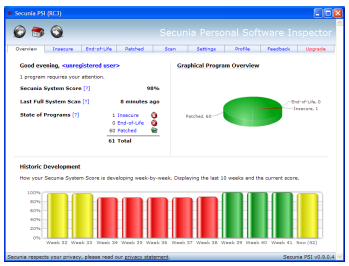
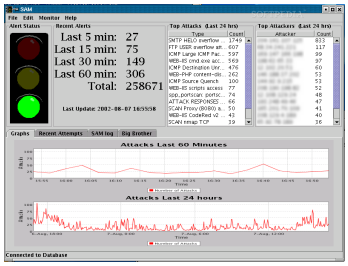
De plus, il n'est pas rare qu'on ne puisse pas protéger ainsi l'ensemble du système d'information : certains équipements ne sont pas compatibles avec la solution standard, et ne peuvent être remplacés. Le cas le plus courant est celui des équipements ne pouvant accepter de mises à jour de sécurité, pour des raisons techniques ou bien des raisons contractuelles. Il est parfois tentant de vouloir protéger ces équipements en les isolant, mais l'expérience montre qu'il reste souvent des chemins d'accès qui n'ont pas été coupés, et qu'il faut donc inclure ces équipements dans le périmètre surveillé.

Le troisième gros défaut de cette approche est que sa réactivité est limitée par la réactivité des fournisseurs de sécurité. La menace étant évolutive, il importe de pouvoir faire évoluer la protection aussi vite que possible. Mais les fournisseurs doivent garantir à tous leurs clients que toute évolution est sans risque sur les fonctionnalités de leurs systèmes. Cela impose des procédures de test très lourdes, dont la lenteur peut être illustrée par la lenteur avec laquelle les éditeurs de logiciels corrigent les failles de sécurité qui leur ont été révélées. [6]

Enfin, l'installation des quelques boîtiers de sécurisation dans un but de protection du système va souvent de pair avec une sous-estimation du coût (principalement humain) d'exploitation de ces boîtiers. Un risque de cette approche est donc de négliger les deux autres pieds du triptyque de la Cyber Défense.

5. http://en.wikipedia.org/wiki/Script_kiddie

6. Jusqu'à sept ans avant la découverte de la faille et sa correction, dans certains cas http://blogs.technet.com/b/msrc/archive/2008/11/11/ms08-068-and-smbrelay.aspx

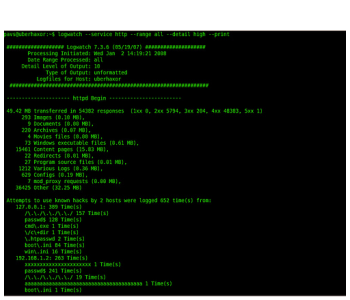
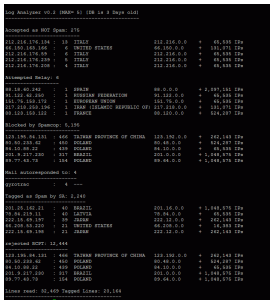
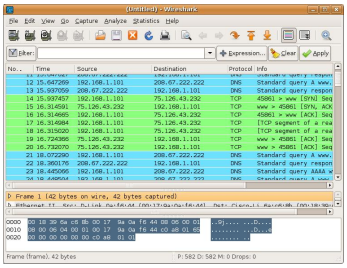
3.2 L'approche artisanale pêche par son ergonomie

À l'opposé, il y a les administrateurs qui utilisent leur propre système de surveillance, fait maison. Cela va d'un grep occasionnel des fichiers de logs, à des sondes finement adaptées à tout les équipements connectés, pouvant être mis à jour de façon extrêmement réactive en cas d'évolution de la menace, qui peuvent ainsi détecter des intrus avant que les intrus ne les détectent.

Souvent, ces systèmes de surveillance ont été développés selon la méthode *agile*, c'est-à-dire en réagissant aux circonstances, de façon incrémentale et sans spécification du besoin. Il est même assez courant que malgré l'installation de boîtiers de sécurité, la surveillance du système d'information se fasse de façon artisanale, à partir des données fournies par ces boîtiers.

Un premier défaut de l'approche artisanale est sa grande dépendance à présence du concepteur de ces outils et méthodes : seul lui sait comment et pourquoi ils ont été conçus, et est capable d'en interpréter les résultats. Il lui est possible de former sur le tas d'autres utilisateurs, mais pas de leur en transférer la maîtrise, en particulier par manque de documentation.

La visualisation des informations est quant à elle assez rudimentaire, reposant sur l'expertise de l'administrateur de sécurité.

Par ailleurs, l'architecture de ces outils et méthodes développés de façon agile n'est en général pas formalisée. En conséquence, ces outils manquent la modularité qui leur permet de s'adapter à de grosses évolutions du système d'information. Tant qu'il n'y a que de petits changements, ils évoluent de façon incrémentale, mais à chaque refonte ou fusion du système d'information, il faut tout redévelopper.

Il y a plusieurs exemples de cas où l'approche artisanale, avec un outil développé d'abord pour les besoins propres du développeur, est devenu un produit commercial, souvent en passant par une étape open-source. On peut citer par exemple Prelude-IDS, Sourcefire/Snort, ClamAV, ... Mais, dans ces cas là, les défauts de l'approche commerciale sont apparus en même temps que l'industrialisation.

3.3 Comment obtenir le meilleur des deux !

Il s'agit donc d'éviter une trop grande standardisation, une non-adaptation à certains équipements, une mauvaise réactivité, et aussi une difficulté à maintenir, un manque de modularité, ...

Pour cela, il importe de pouvoir utiliser l'existant, au maximum de ses possibilités, qu'il ait été installé de façon standard ou bien développé de façon anarchique. Il s'agit donc d'une approche d'intégrateur (mot clef : l'existant) avec un soin particulier apporté à l'ergonomie, en particulier l'ergonomie de configuration et celle de visualisation (mot clef : utiliser).

Ainsi, on favorisera un système qui présentera une ou plusieurs vues synthétiques de l'état de sécurité, avec la possibilité d'entrer dans les détails de chacun des outils intégrés. Ces vues synthétiques doivent non pas se focaliser sur la technologie utilisée ou sur l'architecture du système d'information surveillé, mais sur l'état des services rendus par le SI. Ainsi, ces vues sont indépendantes des outils qui ont été intégrés, et sont compréhensibles par des non-experts en sécurité informatique.

En revanche, ce système ne cherchera pas à remplacer l'existant. Il s'agit de laisser les boîtiers protéger contre les menaces classiques, et de laisser les outils artisanaux avoir leur flexibilité et leur réactivité. Ainsi, l'intégration se fait en ajoutant une dimension métier, et en laissant la dimension technique accessible aux experts.

4 Processus : le passage à l'échelle

4.1 La complexité du système d'information

L'informatique n'est désormais plus un outil neuf, et l'urbanisation du système d'information laisse voir plusieurs strates dont certaines ne sont pas entièrement enfouies. Il y a donc en permanence des incohérences, des migrations en cours, des éléments obsolètes mais toujours utilisés. Et dans le cas d'un SI d'une entreprise ayant connu des réorganisations ou des fusions, il reste en général des traces de logiques contradictoires qui n'ont pas encore été unifiées.

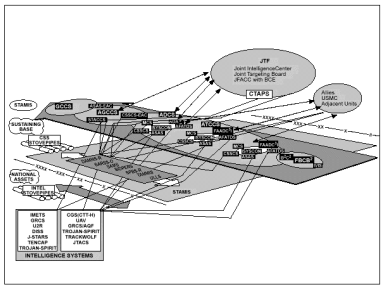
De plus, malgré une volonté de centraliser la gestion du SI, nous sommes à l'ère de l'ordinateur individuel (le PC) avec donc des utilisateurs ayant une

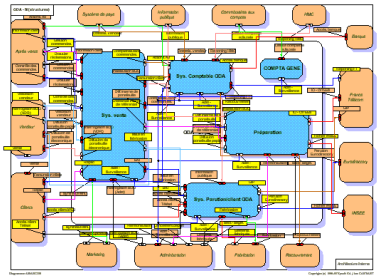
certaine autonomie. Tout élément du SI est ainsi susceptible d'être compromis, encore plus avec les ordinateurs portables qui sont une partie du temps connectés à des réseaux domestiques... Les politiques de sécurité autoritaires sont toujours contournées pour des raisons d'efficacité, et donc le nombre d'éléments du SI qu'on peut considérer de confiance est faible.

Et aussi, chaque élément du SI est complexe ; les imprimantes sont des ordinateurs presque complets, les éléments de réseau sont intelligents, les serveurs sont tous interconnectés (par exemple pour avoir du single-sign-on), etc.

Une tâche difficile est de faire correspondre la réalité du système d'information et la représentation qu'en ont les personnes et outils chargés de la sécurité du SI. Une solution pourrait être de mettre en place des systèmes automatiques de découverte de l'architecture du SI, mais il y a le risque que ces outils aient la même signature qu'un attaquant cherchant à détecter les points faibles du SI.

En conclusion, il faut prendre en compte dans la mise en place d'une Cyber Défense le fait que la connaissance du SI à protéger est incomplète. Une direction de recherche qui n'a pas encore abouti vise à quantifier la complexité du SI, et in fine à quantifier la connaissance que l'on a du SI. [7]





En pratique, la surveillance du SI ne peut donc qu'être alignée sur un découpage du SI en éléments surveillés indépendamment et localement, et la complexité du SI se traduit en la complexité de la coordination de ces surveillances locales. Cette problématique de l'interopérabilité de la Cyber Défense de systèmes fortement interconnectés se retrouve à toutes les échelles, jusqu'à l'intergouvernemental.

4.2 La complexité de la défense du SI

La responsabilité de la défense d'un système d'information d'entreprise est principalement chez le RSSI, mais celui-ci n'a pas tous les leviers sa disposition, en particulier juridiques. En effet, en interne, il y a une obligation de respect de la vie privée qui empêche certaines surveillances, et en externe il y a le respect de la propriété industrielle des fournisseurs, qui empêche certaines analyse de sécurité.

7. Une telle recherche est par exemple menée au NIST : `http://www.nist.gov/itl/math/measurement-science.cfm`

Ces deux aspects sont partiellement adressés par voie contractuelle, en faisant signer des chartes aux utilisateurs et en faisant signer des engagements de qualité aux fournisseurs, mais ni les uns les autres ne peuvent être considérés comme fiables.

Il est généralement accepté que tout humain est faillible, et donc les mots de passe et autres token ne sont pas des éléments d'authentification absolus. La Cyber Défense doit donc viser à minimiser à la fois l'impact de ce risque (en cloisonnant les droits) et l'occurence de ce risque (en particulier en fournissant à chaque utilisateur les moyens de délégation qui lui éviteront d'avoir à divulguer ses codes d'accès).

De même, il est généralement accepté que tout logiciel a des bugs, et des failles de sécurité. Il est donc important que les procédures de mise à jour de sécurité puissent être mises en oeuvre rapidement, et de choisir des fournisseurs ayant une bonne expérience de la réaction à des failles de sécurité. Pour cela, il serait utile d'avoir des métriques de la qualité sécuritaire des logiciels, afin que les critères d'achats puisse les prendre en compte. Les évaluations de type Critères Communs ou CSPN ne sont pas une réponse adaptée, car elles apportent une réponse binaire sur une cible de sécurité dont l'adéquation aux besoins opérationnels n'est pas quantifiée. En pratique, le choix est souvent de suivre la majorité, car c'est un choix qui même en cas de problème de sécurité ne sera pas reproché.

Outre ces aspects juridiques, la complexité de la défense du SI apparaît aussi dans les relations nécessairement conflictuelles entre les acteurs de la Cyber Défense et leurs collègues.

D'une part, la défense est un coût récurrent, alors que le coût induit par les attaques contre lesquelles on a été protégé n'est pas quantifié. Il est donc utile que le système de défense serve non seulement à fournir un protection, mais aussi à fournir une indication sur les coûts évités grâce à cette protection. Ces coûts sont de deux types : des coûts directs (inaccessibilité du SI, nettoyage d'une infection, ...) et des coûts indirects (fuite d'information sensible, impact sur l'image, ...)

D'autre part, la défense apparaît sous la forme de contraintes, les comportements risqués étant interdits. Or, il est nécessaire d'obtenir l'adhésion des utilisateurs, sinon ceux-ci mettront en place des techniques de contournement de la sécurité.

5 Humain : la formation

5.1 Une nouvelle gestion des ressources humaines

Cette nouvelle manière d'appréhender la sécurité des SI appelle une nouvelle gestion des ressources humaines.

Il y a peu, la SSI restait le parent pauvre lors de la conception de nouveaux SI. Les experts étaient sollicités très en aval pour apporter après coup une “couche de

sécurité" réglementaire, dans un contexte budgétaire toujours contraint et avec des délais d'exécution toujours trop courts. Des oppositions naissaient de ces situations conflictuelles dans lesquelles les chargés de la sécurité faisaient systématiquement figure de *monsieur non* et pointant du doigt les insuffisances et les non conformités, retardant les déploiements et empêchant, in fine, les opérationnels d'utiliser leur nouveau système.

Quand des attaques survenaient sur des systèmes existants, les experts étaient sollicités en urgence par les décideurs pour évaluer la situation. Malheureusement, leurs approches respectives, très technique pour les uns, stratégique pour les autres, avaient du mal à se rencontrer. A la question : « que se passe-t-il ? », l'expert explique le fonctionnement de l'attaque alors que le décideur attend une évaluation de l'impact. Ce hiatus renforçait l'isolement, voire l'enfermement dans une tour d'ivoire de la SSI.

Aujourd'hui, grâce au développement d'outils et de concepts de supervision de la sécurité capables d'apporter l'information nécessaire à chaque acteur, cette incompréhension tend à diminuer. Mais, si les outils sont maintenant disponibles, il faut accompagner ce changement par de la formation.

De l'opérateur à l'expert, de l'utilisateur final au décideur, chacun doit être sensibilisé à la sécurité pour ce qui le concerne. La formation doit être parfaitement adaptée au public visé : il est inutile voire contre-productif de vouloir imposer un cours théorique de SSI à un décideur ou à un simple utilisateur qui attendent davantage des informations pratiques et de l'aide à la décision. L'expert doit lui aussi se former régulièrement. Dans ce domaine qui évolue extrêmement vite, les compétences doivent être entretenues en permanence. Les procédures de réactions aux incidents évoluent elles aussi au rythme rapide des déploiements et de l'installation de nouveaux matériels. Les opérateurs et les administrateurs système doivent recevoir un entraînement régulier qui leur permettra de rester à jour.

5.2 Développer les exercices

La formation continue doit en plus être mise en pratique régulièrement. Pour cela, des exercices spécifiques se mettent en place. En France, au niveau national, Piranet est un exercice majeur dont la dernière édition s'est déroulé en juin 2010. Conduit par l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI), cet exercice « visait tout d'abord à tester le nouveau plan gouvernemental d'intervention PIRANET, qui fixe l'organisation et les grands principes de réponse à une crise provoquée par des agressions informatiques de grande ampleur ». [8]

On constate que Piranet permet d'exercer les **processus métier**, ce qui était déjà mis en exergue dans le Plan de Renforcement de la SSI de l'Etat du 10

8. http://www.sgdsn.gouv.fr/site_article98.html

mars 2004 qui identifiait l'objectif de Piranet comme étant de s'assurer de la « disponibilité en toute circonstance de liaisons sécurisées, annuaire de correspondants, pleine maîtrise par tous les acteurs des mesures à appliquer, disponibilité d'équipes mobilisables sans délai et capables de mener 24h sur 24 un programme opérationnel dans la durée ». [9]

Cette activité qui apparaît très clairement au niveau interministériel doit aujourd'hui se généraliser à l'ensemble des acteurs des SI. Par analogie, on peut comparer avec les exercices incendies qui sont obligatoires au moins tous les 6 mois (Article R 232-12-21 du Code du travail - Livre 2 - Section 4) pour tous les établissements définis à l'article L.231-1 du code du travail (publics, industriels, commerciaux, etc.). Pourquoi n'en serait-il pas de même pour la sécurité des systèmes d'information ?

5.3 Conclusion

La probabilité de subir une attaque informatique de grande ampleur est désormais très élevée [10], avec un impact sans doute important sur notre vie quotidienne. Dans ce contexte, il faut mettre en place une sécurité des SI intégrée à chaque niveau de l'organisation et qui atteigne le juste équilibre entre une technologie de pointe, des processus métiers régulièrement exercés et des acteurs bien formés. Cette vision globale apporte la capacité de planifier l'engagement financier nécessaire afin d'atteindre l'optimum réaliste.

9. Plan de Renforcement de la SSI du 10 mars 2004, paragraphe 2.3, page 4/18
10. Le Livre blanc sur la défense et la sécurité nationale - p. 53

Hynesim : virtualisation de systèmes d'information pour la cyberdéfense

Bernard L'Hostis[1], Guillaume Prigent[2], and Jean-Baptiste Rouault[3]

[1] Département AMI DGA Maîtrise de l'information bernard.l'hostis(@)dga.defense.gouv.fr
[2] Responsable et architecte du projet Hynesim - diateam ⋆ guillaume.prigent(@)diateam.net
[3] Développeur principal du projet Hynesim - diateam ⋆ jean-baptiste.rouault(@)diateam.net

Résumé La sécurisation des systèmes d'information est un domaine ancien où l'outil de simulation n'apparait que très rarement. Cette communication fait le point sur une série de travaux initiés à la division SSI du centre DGA Maîtrise de l'information (ex CELAR) et dont le but est de disposer d'un outil de simulation réaliste d'un système d'information. Cet outil de simulation permet de modéliser un système d'information puis de l'instancier en mixant des instances de systèmes d'exploitation virtualisés, émulés voire simulés, des simulations d'équipement et de liens réseaux et enfin d'utilisateurs virtuels en interaction avec ces équipements. Ces différents systèmes simulés ou virtualisés peuvent être connectés à une partie réelle. L'outil peut ainsi être utilisé dans différents contextes :
– Veille, comme plastron pour la surveillance et la collecte d'information ;
– Alerte, comme un champ de tir électronique pour augmenter le niveau d'expertise ;
– Réponse, comme outil d'entrainement pour former les acteurs de la sécurité informatique.
Un premier retour d'expérience ainsi que le futur de ce projet seront présentés comme synthèse.

Mots-clés: Sécurité des systèmes d'information, simulation, simulation hybride, Hynesim, virtualisation.

Note des auteurs : Dans le cadre de cette communication, les auteurs souhaitent effectuer une démonstration d'emploi de la plateforme Hynesim en s'appuyant sur un scénario de cyberdéfense déjà réalisé.

Abstract : Financed by the MinDef/DGA/Celar, the Hynesim project's goal is to provide the open source community with an information systems hybrid simulation platform. The purpose of this network oriented project is to integrate low and high interaction hosts in complex topologies, based on a massively distributed simulation. The major advantage of this system is the interconnection between real and virtual machines, as well as its ability to simulate life on the network through production of lifelike data-flows, based on the concept of virtual users. The aims of this platform are to offer an all-in-one solution allowing preparation, construction, simulation and operation of a virtual information system, so as to observe the evolution of its security. Based as much as possible on pre-existing Open Source components (COTS), the Hynesim project will provide the ISS community with a way of deploying large virtual information system at a low cost. Beyond the innovative concepts of hybrid simulation and distributed nature of such a tool, many technical features must be implemented to make sure all these components integrate smoothly into the plateform. Many aspects, such as remote control of high interaction hosts, lifelike data-flows generation, dynamicity of the topology, and the distribution of

⋆. diateam, 41 rue Yves Collet, 29200 Brest

models on a server cluster running the simulation require a true reflection on design, and the use of original system and network techniques. The foundations of the Hynesim project are based on 10 years of thinking on the subject, and on the lessons learned from a first approach through the BridNet project (http ://www.bridnet.fr). Beyond the technological and conceptual framework of the project, the members of the Hynesim project wish to bring genuine expertise on tools such as Honeyd, VirtualBox, Qemu, by sharing the experience gained through their usage and development in the field of hybrid network simulation. The "Hybrid" in "Hynesim : Hybrid network simulation" stands for two things : first, Hynesim will be hybrid because it will allow for real machines to interact transparently with simulated ones, and secondly because these simulated machines will be of two sorts : either high or low interaction, meaning that they will either be simulated by a honeypot system (in our case Honeyd) or using a virtualized OS. We will also develop a guest manager, to handle all the different OSes to virtualize, using prepared disk images, as well as a virtual and distributed software switch, to route all traffic to its destination, entirely bypassing the IP stack of the OS running the simulation, to ensure complete control over the flowing data, and to allow for very complex topologies. We will also provide the possibility of generating fine-grained lifelike data flows in between any machines, be they real or virtual. Data flows can range from SNMP traps to emails with attachments or web surfing, and can be customized in content, frequency, origin, destination etc... Also, we will provide all the most common network interfaces to interact with the simulation : Ethernet, but also WiFi and Bluetooth. This should result in an all-in-one platform, with all components completely integrated.

1 Introduction

Depuis plus de dix ans, le département AMI (Analyse de la Menace Informatique) de DGA Maîtrise de l'information (ex CELAR), a initié une série de travaux qui visent à développer l'utilisation de la simulation dans le processus de la SSI [4]. Cet article présente de manière générale les besoins et l'état d'avancement de ces études et plus précisément le cadre d'emploi en cyberdéfense de la plateforme hybride de simulation d'architecture réseau Hynesim.

Nous exposerons dans la prochaine section les attentes et les besoins qui devront être couverts afin d'instrumenter le domaine de la SSI et de la cyberdéfense avant de poursuivre en section 3 par la description des orientations techniques qui ont permis la conception et la réalisation de l'architecture Hynesim développée par la société diateam [5] en association avec Orange IT&L@BS. L'architecture actuelle et le fonctionnement de cette plateforme y seront décrits en essayant de s'affranchir de la lourdeur d'un exposé technique et en privilégiant plutôt un exposé clair des fonctionnalités proposées. Enfin, dans le cadre d'emploi « cyberdéfense », nous effectuerons la synthèse de ces travaux en présentant nos premiers retours d'évaluations et d'expérimentations d'Hynesim et nous exposerons pour conclure les évolutions souhaitables et le futur envisageable de cette plateforme.

4. Sécurité des Systèmes d'Information

5. `http://www.diateam.net`, `contact@diateam.net`. diateam est une société d'ingénierie numérique et un véritable laboratoire de recherche et développement en informatique, tout particulièrement dans le domaine de la sécurité des systèmes d'information

Afin de bien comprendre l'état actuel de notre réflexion et l'aboutissement à la plateforme Hynesim, il convient d'exposer nos besoins historiques et le cadre d'emploi attendu.

2 Besoins de la défense nationale

Le département AMI travaille de longue date à explorer la capacité à outiller le domaine de la SSI en outils de simulation. Le but de ces études est principalement de doter les experts en systèmes d'information d'un outil dynamique, pluridisciplinaire, qui participe à combler les défaillances des méthodologies actuelles. Ces outils doivent permettre de créer un modèle de base représentatif d'un système d'information et de conduire des expérimentations de différentes natures.

L'objectif est de décrire le système par ses éléments constituants principaux et d'observer et d'analyser les interactions de ses composants élémentaires pour faire apparaître des comportements macroscopiques des systèmes observés.

En phase amont, la connaissance plus fine des menaces doit permettre une conception plus précise et plus rationnelle des systèmes et des éléments de sécurité. Durant la phase d'intégration et de test, le système doit être soumis à tous les types d'agressions envisageables. L'analyse des comportements globaux doit permettre d'éclairer les conditions d'emploi opérationnel et d'améliorer l'expérience des utilisateurs. De plus, durant la phase d'emploi opérationnel, ces techniques doivent permettre de renforcer les capacités d'analyse pour l'homologation et d'améliorer les actes réflexes des acteurs opérationnels.

Ces actions doivent être réalisées sous contraintes (on parle de ŞstressŤ du système) et intégrer la dynamique des échanges et des interactions. En effet, le développement du stress du système (composantes technique et humaine), ne doit pas augmenter la prolifération des outils et des savoir-faire d'attaque (cloisonnement). Elle doit permettre de tenir compte du contexte d'emploi du système (utilisateur, flux métier, interconnexion de systèmes étrangersĚ) et de minimiser les ressources nécessaires (nature et nombre des matériels informatiques à mettre en oeuvre, trafic et évènements courants du système, pertinence des éléments de vieĚ). De plus il n'est bien souvent pas envisageable d'effectuer ces expérimentations sur des systèmes complets en fonctionnement opérationnel. Cette nécessité conduit à développer des moyens de simulation qui puissent être directement mis en interaction avec le système réel (on parle de couplage « hybride » pour la connexion virtuel/réel).

Le département Analyse de la Menace Informatique a décliné ses axes de développement « métier » en objectifs précis, dans le cadre général des missions relatives à la sécurité des systèmes d'information. À ce titre, le simulateur doit permettre :

- la conduite et la génération des flux représentatifs des attaques informatiques dans un processus construit et global (opposition entre une vulnérabilité unitaire et un chemin global d'attaque) ;
- la génération de tous les autres flux, représentatifs de la vie du système et des comportements de ses acteurs ;
- l'intégration d'une composante physique réelle d'un système (composant, sous-système, entité) cible du stress nécessaire à sa qualification ;
- la mise en situation sous stress de l'acteur humain pour capturer et analyser ses comportements dans le cadre du déroulement de scénarios d'attaque ou de perturbations du système étudié.

Principalement, la plateforme souhaitée doit permettre de simuler un système d'information afin :

- d'évaluer le niveau de sécurité d'un système futur (prototypage) ;
- de mettre en concurrence plusieurs architectures alternatives (analyses comparatives) ;
- d'augmenter la pertinence et le réalisme des travaux sur les systèmes d'information ;
- de fournir un outil d'analyse adaptatif, pluridisciplinaire dans le cadre de la maîtrise des systèmes d'information.

La section suivante s'attache à présenter les pistes technologiques étudiées et les choix effectués afin de déboucher sur l'architecture générale de la plateforme actuelle pour en présenter son fonctionnement général.

3 Choix technologiques et éléments d'architecture

3.1 Axes d'études technologiques

La simulation d'un système d'information se décompose en deux problèmes dont les maturités technologiques sont très différentes :

- La simulation des parties matérielle et logicielle du système d'information.
- La simulation de la partie humaine en interaction avec le système d'information.

Pour valider les pistes et les choix technologiques liés aux parties matérielles et logicielles, des travaux ont été menés depuis 2000 sous la direction technique de M. Éric Bornette. Parmi les résultats de ces travaux, on peut citer deux maquettes GIMLI et BRIDNET[1] issues d'une étude de définition réalisée entre 2003-2005. Ces maquettes ont mis en évidence deux axes de solutions possibles.

La solution du simulateur numérique pur : Pour ce type de solution, le système à étudier est entièrement simulé. Il peut être raccordé à un système réel (couplage mixte réel/virtuel). Des échanges de flux sont réalisés entre les deux. Cette solution nécessite la réalisation d'un logiciel de simulation de système. Elle

permet de dématérialiser l'ensemble des composantes d'un système et possède de nombreux avantages :

- la minimisation de la composante physique d'un système ;
- la compression du temps de vie du système simulé ;
- la facilité de mise en oeuvre ;
- la diminution des effets de bords des attaques déroulées.

Ce type d'approche pose cependant plusieurs problèmes épineux :

- la difficulté de fixer le bon niveau d'abstraction par rapport à la pertinence des comportements attendus. Il est parfois nécessaire de « tout simuler » avec des niveaux de granularité multiples et importants ;
- la contrainte de développements importants et « propriétaires » (au sens d'une implémentation spécifique et locale) à chaque évolution ou à chaque phénomène spécifiquement désiré ;
- la quasi impossibilité de validation et les difficultés de qualification du simulateur dans son fonctionnement global.

La solution dite hybride : Dans ce cas, c'est le niveau de granularité qui détermine le niveau de la répartition des tâches entre le « réel complet » et le « tout virtuel ». Cette solution repose donc sur un découpage du système suivant plusieurs niveaux d'abstraction :

- réel : composante du vrai système ;
- virtuel ou émulé : c'est le cas des machines virtuelles qui permettent de simuler plusieurs ordinateurs (les invités) sur une seule machine physique (l'hôte) et qui utilisent des logiciels réels ;
- simulé : l'ensemble des éléments représentatifs et des flux sont simulés mais physiquement perceptibles et interconnectés avec les éléments réels et virtuels (cas du routage des paquets dans des liens physiques par exemple).

Les évènements qui donnent l'illusion d'un système réel (commutation, topologie, latence des liens, ...) sont réalisés par des outils de simulation complets (des instances de modèles). La diminution de la composante hardware est réalisée par l'emploi d'outils de type « machine virtuelle » ou d'émulation. Enfin, quand le besoin de réalisme est très important, les éléments réels prennent le relais.

Au cours de ces travaux d'études préliminaires, le réalisme de la simulation est devenu un objectif fonctionnel prépondérant. Cela a orienté la conception et le développement de l'architecture actuelle vers une solution dite « hybride » complète qui forme le coeur du système de simulation. La facilité de modélisation et de configuration de cette solution numérique s'est montrée plus souple, plus réaliste et plus évolutive pour les besoins visés.

Nous traiterons de la simulation de la composante humaine dans la section dédiée aux « Évolutions souhaitées ».

3.2 La plateforme Hynesim V1

Cadre de conception

Hynesim peut être qualifié de plateforme distribuée de simulation hybride de systèmes d'information. Distribuée tout d'abord car il est possible de répartir l'ensemble de la simulation sur plusieurs machines réelles, ce qui permet une forte extensibilité : il est aisé d'ajouter un serveur supplémentaire si nécessaire. Simulation ensuite car tout est contrôlé par Hynesim et il est donc possible de mettre en pause, sauvegarder, ou encore charger des simulations. Hybride enfin, du fait de la possibilité de relier le système d'information simulé à un système réel. Hynesim est également une plateforme de simulation multi-niveaux, permettant de simuler aussi bien des composants à interaction faible que des composants à interaction forte.

La plateforme Hynesim a été conçue en essayant de privilégier au maximum l'intégration d'outils existants (COTS [6]) afin d'éviter des développements redondants tout en s'efforçant de réaliser une architecture modulaire et sans dépendance forte sur un outil ou une technologie en particulier. Hynesim est un projet open source sous licence GPLv3, et le choix a été fait de s'impliquer dans les projets des divers outils utilisés, que ce soit pour corriger des bugs ou ajouter de nouvelles fonctionnalités.

S'il est aisé de manipuler une seule machine virtuelle, les manipulations sont en revanche nombreuses et non triviales lorsqu'il s'agit d'en relier plusieurs les unes aux autres. Un souci tout particulier a donc été apporté à la simplicité d'utilisation et à l'ergonomie de l'interface de contrôle d'Hynesim afin que l'utilisateur puisse rapidement créer une simulation de système d'information plus ou moins complexe.

Il faut également noter qu'en plus d'être une plateforme logicielle, Hynesim est aussi une plateforme matérielle. Comme on peut le voir sur la figure 1, un important travail d'intégration a été effectué pour obtenir un support matériel transportable pour effectuer des simulations hybrides Hynesim (cinq serveurs, KVM [7], onduleur, équipement sans-fil, commutateurs Gigabit Ethernet...).

Fonctionnalités

Simulation de composants réseaux : Pour simuler un système d'information, il faut pouvoir relier les machines entre elles. Il est donc nécessaire d'avoir des briques réseaux basiques : fils, cartes réseaux, commutateurs et concentrateurs... Les fils sont un peu particuliers puisque leurs deux extrémités ne sont pas forcément sur la même machine physique. Tous ces composants sont entièrement simulés par

6. Components off the Shelf
7. Keyboard, Video, Mouse

Figure 1. Plateforme matérielle

des objets C++ natifs ce qui permet, par exemple, de simuler un phénomène de latence pendant le transfert des données.

Composants réseaux hybrides : Nous avons pu voir dans la section précédente que la simulation pure ne suffit pas et qu'il est parfois intéressant de pouvoir y relier des systèmes réels. C'est pourquoi nous avons doté la plateforme Hynesim de composants réseaux hybrides qui permettent de relier le virtuel et le réel via des ports RJ45, du Wi-Fi ou encore du Bluetooth.

Interaction avec les machines virtuelles Simuler un système d'information ne présente que peu d'intérêt si on ne peut pas interagir avec ce dernier. De ce fait, la plateforme Hynesim permet à l'utilisateur d'obtenir facilement un déport d'écran sur les machines simulées depuis l'interface graphique de contrôle. Un canal de communication entre les machines virtuelles et l'hôte est également présent et permet de commander, depuis l'hôte, l'exécution de commandes sur l'invité.

Mystification de la prise d'empreinte TCP/IP Il peut être important de pouvoir simuler de nombreuses machines utilisant le système d'exploitation Windows, dans un cas d'utilisation de type « pot de miel hybride » par exemple. Afin de limiter les ressources nécessaires, l'idéal serait de pouvoir lancer un grand nombre de machines virtuelles à interaction faible (de type Linux) qui soient vues comme des machines Windows depuis l'extérieur. C'est pourquoi nous avons intégré un outil de mystification de la prise d'empreinte TCP/IP qui permet de tromper un attaquant sur les systèmes d'exploitation réellement employés.

Architecture générale Comme le montre la figure 2, on peut envisager la plateforme selon deux angles :

- Un angle d'administration qui permet de préparer, de contrôler et d'interagir avec Hynesim via le bus d'administration. L'ensemble des serveurs de la plateforme matérielle Hynesim sont reliés sur ce bus par une connexion Gigabit Ethernet. Le bus d'administration sert à la communication des différentes instances d'Hynesim entre elles ainsi qu'au partage des données nécessaires à la simulation (images disques, sauvegardes...). Les différents postes qui permettent de contrôler la simulation par le biais d'une IHM [8] sont également reliés à ce bus.
- Un angle de simulation qui permet de se connecter au système d'information simulé depuis un système réel via le bus de communication « hybride ».

La figure 3 présente une vue plus détaillée de l'architecture de la plateforme. Un point primordial dans le cadre de la simulation était qu'elle paraisse la plus réelle possible pour un utilisateur connecté à une machine simulée. Par conséquent, le bus d'administration d'Hynesim et le système d'information simulé sont

8. Interface Homme Machine

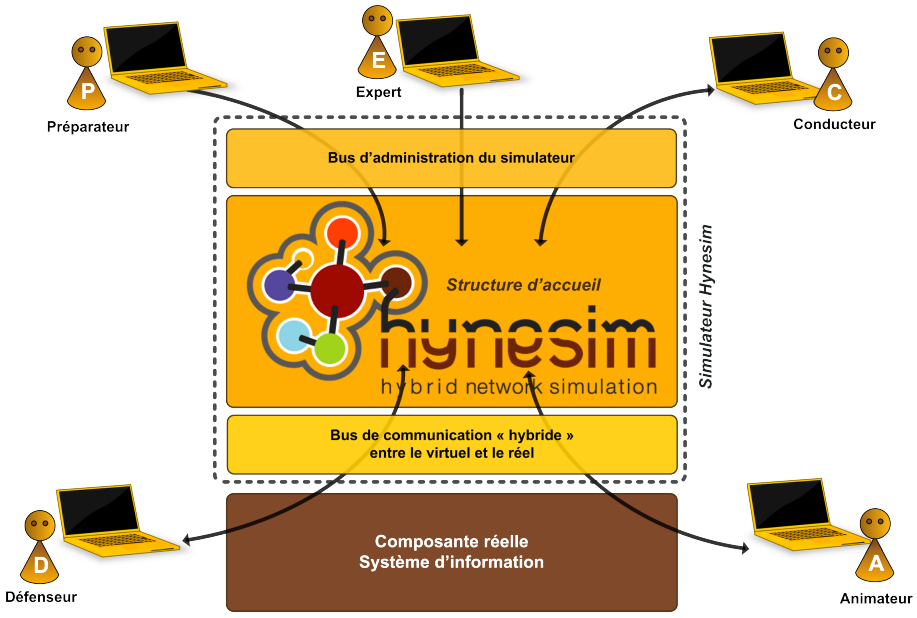


Figure 2. Architecture générale

complètement isolés l'un de l'autre : aucun flux de commande n'est visible depuis la simulation. On remarque également la présence de Bluetooth (dongles USB) et de Wi-Fi (point d'accès matériel) sur le bus hybride.

Une simulation distribuée : Comme la simulation d'un système d'information peut nécessiter d'importantes ressources matérielles, Hynesim a principalement été conçu pour être un simulateur distribué et se comporte comme un ORB [9]. L'ensemble des objets correspondants aux entités virtuelles sont répartis sur un ensemble de noeuds (le *mesh*) présents sur le réseau. Grâce à un concept d'objets « proxys », il est aisé d'appeler des fonctions sur des objets distants. Les noeuds sont capables de s'auto-découvrir grâce à un mécanisme d'annonces sur le réseau, ce qui permet de faciliter la formation du *mesh*, et en particulier, l'ajout de nouveaux noeuds en cas de nécessité. Tous les noeuds sont interconnectés afin d'éviter d'introduire des latences supplémentaires dues au passage par un serveur central. Afin de permettre à plusieurs utilisateurs de simuler des systèmes d'information simultanément sur un seul et même *mesh*, nous avons souhaité intégrer un mécanisme de session qui cloisonne les objets de ces différentes simulations.

Dans notre terminologie, un noeud est une instance d'Hynesim identifiée par un hash et existant dans un *mesh* unique. Chaque noeud possède un certain nombre de capacités qui définissent les types d'objet qu'il est capable d'instancier (hôtes à interaction faible ou forte, composants réseaux hybrides...). Chaque *mesh*

9. Object Request Broker

possède un noeud particulier appelé « maître » qui possède des objets singletons pour toute la simulation tels que le gestionnaire de sessions, le catalogue des machines virtuelles disponibles, ou encore le gestionnaire d'adresses MAC. Un noeud peut également être « spectateur », c'est à dire qu'il n'est pas possible de lui demander d'instancier des objets ; il peut cependant créer et contrôler des objets sur les autres noeuds. Les noeuds **Hyneview**, l'interface graphique de contrôle d'Hynesim, font partie de cette catégorie de noeuds. Chaque noeud vérifie à intervalle régulier que les autres noeuds du *mesh* sont toujours « vivants ». Si un noeud ne répond pas à ces vérifications, il est marqué comme « déconnecté » et les tentatives d'appels distants vers lui sont alors immédiatement bloquées.

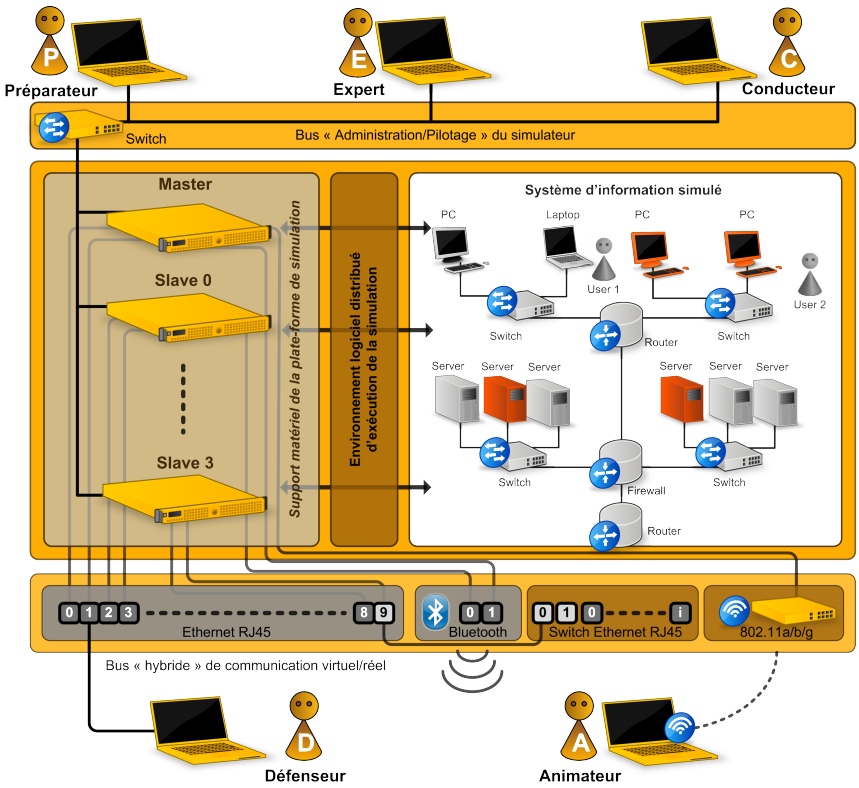


Figure 3. Vue d'ensemble de la plateforme

Socle technologique

Bien que nous ayons essayé de privilégier l'utilisation de COTS, nous avons fait le choix de redévelopper un ORB spécifique à nos besoins plutôt que d'intégrer des

technologies existantes comme CORBA [10], Ice [11] ou encore Xml-RPC [12]... L'intégralité de la plateforme réseau est développée à l'aide du framework C++ Qt4 de Nokia[2]. Pour faciliter les appels de méthodes distantes, nous avons développé un outil capable de générer des classes « proxys » : **proxygen**. Ce programme utilise *doxygen* [3] pour parser les classes existantes facilement et générer ensuite d'autres classes encapsulant toute la logique des appels distants. La figure 4 présente les composants matériels et logiciels types d'un noeud de calcul Hynesim. On remarque qu'Hynesim utilise divers composants logiciels dont nous parlerons plus en détail dans la suite de ce document.

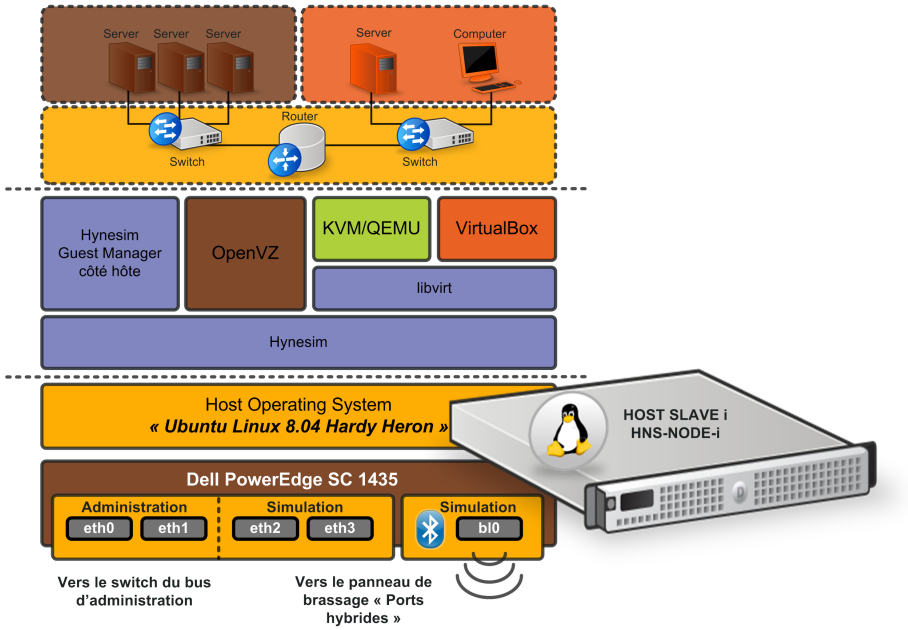


Figure 4. Noeud type

Virtualisation : À l'heure actuelle, trois outils de virtualisation sont utilisés pour simuler des machines de type PC dans une simulation Hynesim :

– **VirtualBox[4] :** un logiciel multiplateforme de virtualisation d'architectures x86. VirtualBox est gratuit et une version open source est disponible. La version propriétaire supporte en plus le RDP [13] ainsi que les périphériques USB. VirtualBox est principalement utilisé dans Hynesim pour vir-

10. Common Object Request Broker Architecture
11. Internet Communications Engine
12. Xml-Remote Procedure Call
13. Remote Desktop Protocol

tualiser des machines de bureau possédant des systèmes d'exploitation avec une interface graphique.

- **KVM/QEMU[5] :** couplé au module noyau KVM [14], l'émulateur et virtualisateur QEMU est capable de virtualiser des machines avec des performances quasi natives. KVM/QEMU est entièrement open source et permet d'effectuer des déports d'écran en utilisant le système VNC [15]. Les cas d'utilisation dans Hynesim sont identiques à ceux de VirtualBox.
- **OpenVZ[6] :** une technique de virtualisation pour linux basée sur des conteneurs. OpenVZ est constitué d'un noyau linux modifié ainsi que d'un ensemble d'utilitaires en ligne de commande. Cet outil permet de virtualiser avec peu de ressources car l'espace noyau de la machine hôte est partagé entre tous les conteneurs et seul les espaces utilisateurs sont isolés. Du fait de ce partage, seuls des systèmes linux peuvent être virtualisés à l'aide d'OpenVZ. Les hôtes dits à interaction « faible » (routeurs, serveurs...) sont simulés par ce biais dans Hynesim.

Afin de limiter le développement de code spécifique à chacun de ces outils de virtualisation, Hynesim utilise l'API [16] **libvirt**[7]. Projet open source Red Hat développé activement depuis 2005, libvirt fournit entre autres une API en C exposant un certain nombre de fonctions pour contrôler des machines virtuelles. Nous l'utilisons actuellement pour les invités VirtualBox et KVM/QEMU et avons contribué au driver OpenVZ de libvirt pour y ajouter des fonctionnalités manquantes.

Hyneview, l'interface graphique de contrôle : Afin de permettre à l'utilisateur d'Hynesim de créer des topologies de systèmes d'information à simuler et de pouvoir contrôler et interagir facilement avec les entités virtuelles, nous avons développé l'interface graphique **Hyneview**. Cette dernière est multiplateforme (Linux, Windows) et relativement simple d'utilisation. On peut voir sur la figure 5 deux zones essentielles de l'IHM : le cadre à gauche liste les différents composants qu'il est possible d'instancier. Pour ce faire, il suffit alors de les glisser-déposer dans la zone centrale où il sera ensuite possible de les relier par des fils. Un menu contextuel sur chaque entité instanciée permet d'interagir avec cette dernière afin de changer son état (démarrer, arrêter...), d'obtenir un déport d'écran ou encore de capturer les paquets réseaux.

Le Guest Manager : Dans un souci de réalisme, nous avons souhaité permettre aux utilisateurs d'Hynesim de générer du trafic de vie, c'est à dire de générer du trafic plus ou moins réaliste entre les différents hôtes simulés. De ce fait, la plateforme Hynesim intègre un utilitaire permettant d'interagir avec les machines virtuelles

14. Kernel-based Virtual Machine
15. Virtual Network Computing
16. Application Programming Interface

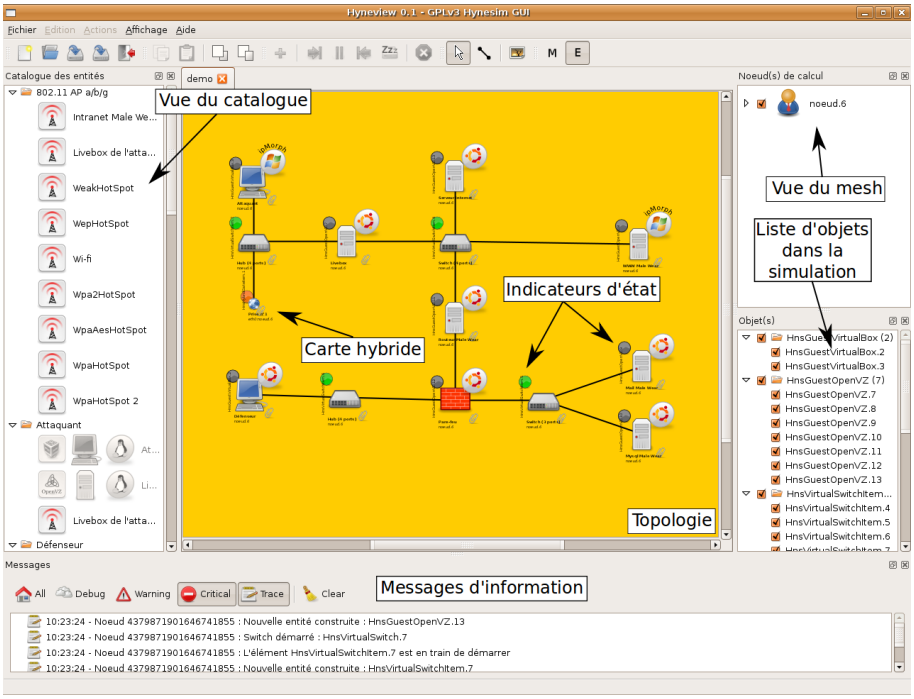


Figure 5. Hyneview

depuis l'extérieur de la simulation : le Guest Manager. Ce dernier se compose d'un ensemble de classes C++ (côté machine réelle), ainsi que d'un programme destiné à s'exécuter dans la machine virtuelle. La communication s'effectue par le biais d'un fichier partagé entre le noeud et l'entité virtuelle. Il est alors possible depuis l'extérieur de la machine virtuelle d'automatiser l'exécution de commandes diverses et variées et d'en récupérer les résultats.

IpMorph[8] : Afin de mystifier des outils de détection de systèmes d'exploitation tels que nmap, nous avons développé un logiciel de contre-reconnaissance qui se présente sous la forme d'une pile TCP/IP en espace utilisateur qui assure le suivi de session et la réécriture des paquets réseaux à la volée. La configuration d'IpMorph s'effectue en lui fournissant ce que nous appelons une « personnalité » : c'est un ensemble de signatures de différents outils de détection (nmap, sinFP, xprobe2...) qu'IpMorph va ensuite utiliser pour se faire passer pour une machine correspondant aux signatures en question.

4 Retours d'expérience en cyberdéfense

La plateforme a été utilisée dans plusieurs expérimentations dont on peut voir figure 6 un exemple simple qui a été déployé lors du salon Milipol 2009. Cet

exemple, non protégé par le secret défense, est malgré tout représentatif puisqu'il a utilisé l'ensemble des fonctionnalités d'Hynesim pour simuler les systèmes d'information d'une entreprise. Cette entreprise disposait d'un site INTERNET de vente en ligne sur lequel plusieurs scénarios d'intrusion ont pu être mis en oeuvre.

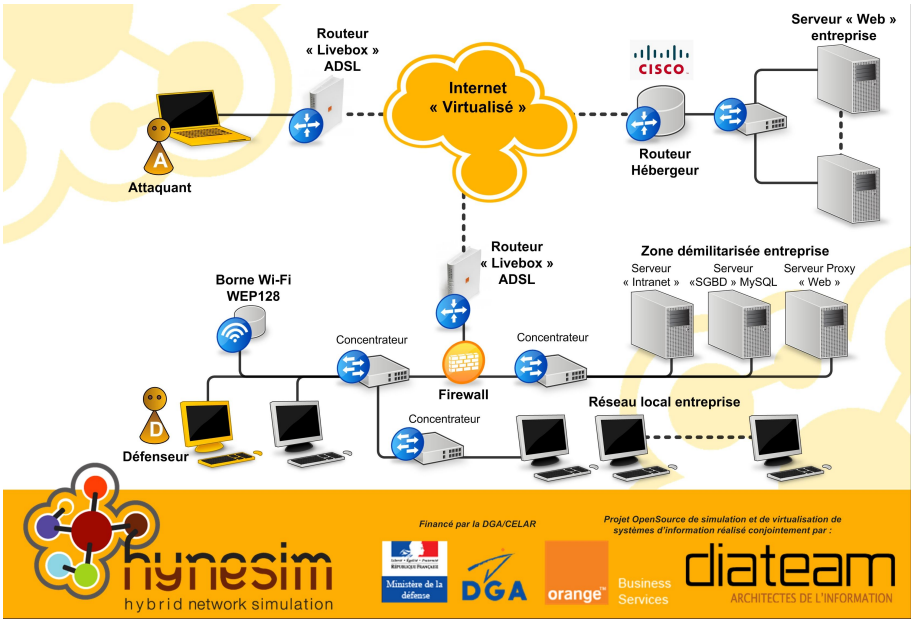


Figure 6. Scénario Hynesim de « cyberdéfense » dans le cadre de MILIPOL09

Ces expérimentations ont permis de vérifier l'intérêt de ce système et ont mis en exergue les points forts :

- La flexibilité du système permettant une configuration simple une fois les images des systèmes d'exploitation créées.
- L'intérêt des possibilités de disposer de plusieurs niveaux de représentativité : le réel, le système d'exploitation virtualisé ou la simulation du système par une instance d'OpenVZ. Il est à noter, pour ce dernier mode, l'utilisation indispensable de la fonctionnalité de mystification de la pile IP par l'outil IpMorph.

Ces expérimentations ont mis en évidence des besoins d'évolutions (voir paragraphe suivant) et ont permis d'appréhender la complexité de la phase de préparation. Hynesim permet (de manière très caricaturale) de déployer rapidement une architecture réseau à partir d'un catalogue d'images de systèmes d'exploitation banalisé. Cependant, pour, par exemple, permettre d'évaluer des solutions de cyberdéfense d'une architecture par rapport à des intrusions réalistes, il faudra :

– Configurer finement les systèmes d'exploitation (création de domaine « Windows », ajout d'utilisateurs, démarrage de services, etc...).
– Remplir les différentes mémoires du système de données antidatées (événement système, événement utilisateur, données utilisateurs) hors phase de test.
– Pendant les expérimentations, animer le système de manière réaliste.

5 Évolutions programmées

Les évolutions se décomposent en deux axes techniques. Le premier axe concerne les extensions des fonctionnalités d'Hynesim dans le domaine matériel parmi lesquelles on peut citer dans celles en cours de réalisation :

– le support des outils de virtualisation VMware ;
– la possibilité d'intégrer des systèmes d'exploitation de routeurs type Cisco ;
– la possibilité d'intégrer les systèmes d'exploitation Mac Os ;
– les études sur l'intégration des systèmes d'exploitation d'outils nomades.

Le deuxième axe concerne la simulation d'utilisateurs. Elle permet de peupler les machines virtuelles (ou réelles) d'utilisateurs interagissant avec les logiciels informatiques réels. La version actuelle d'Hynesim permet déjà de générer des flux réseaux représentatifs (cf. section 3.2). Les extensions prévues sont représentées dans la figure 7.

– Une bibliothèque d'actions perceptions permettra d'interfacer les interfaces hommes machines des logiciels courants. Dans l'exemple présenté, le logiciel de messagerie est démarré et la liste des courriers reçus dans la boite aux lettres est extraite. Il est à noter que chaque logiciel est à instrumenter de manière spécifique.
– Un outil de gestion de scénarios permettant le chainage des actions perceptions précédentes avec des possibilités de structuration (boucle, test conditionnel, etc...). Ces deux items permettront de se passer d'animateur dans de nombreux cas d'utilisation.
– Le dernier niveau « Modélisation du comportement humain » aura pour but d'évaluer les retombées d'une faille humaine et organisationnelle. Les tests conditionnels de l'outil seront évalués par l'outil de modélisation en prenant en compte les paramètres de la personne modélisée.

6 Synthèse

La première version de l'outil Hynesim a montré tout l'intérêt du choix de la simulation hybride dans les premières expérimentations. Son orientation technologique de plus en plus marquée vers une structure d'accueil des meilleures technologies de virtualisation/simulation va permettre une montée en puissance

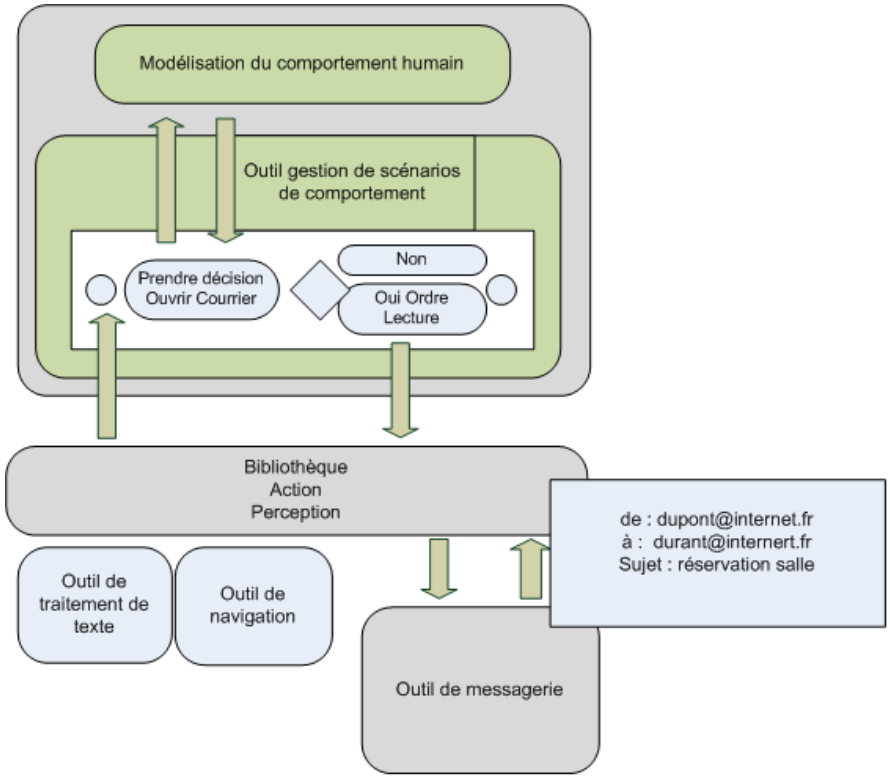


Figure 7. Simulation d'utilisateurs

rapide en terme de périmètre fonctionnalité. Il est appelé à devenir une brique indispensable d'un futur laboratoire technico-opérationnel de cyberdéfense.

En parallèle, cette architecture est également open source et cette disponibilité doit permettre d'étendre le cadre d'utilisation de cet outil de son périmètre de naissance vers d'autres acteurs de la sécurité et des réseaux.

Références

1. Prigent, G., Harrouet, F., Tisseau, J., Frédéric, P. : Simulation hybride de la sécurité des systèmes d'information - Vers un environnement virtuel de formation
   http://actes.sstic.org/SSTIC05/Simulation_hybride_de_la_SSI/SSTIC05-article-Prigent-Simulation_hybride_de_la_SSI.pdf
2. Qt by Nokia : a cross-plaftorm application and UI framework
   http://qt.nokia.com/
3. Doxygen : A source code parser and documentation generator http://www.doxygen.org
4. Oracle VM VirtualBox : A powerful x86 and AMD64 virtualization product
   http://www.virtualbox.org
5. KVM : a full virtualization solution for Linux on x86 hardware
   http://www.linux-kvm.org
6. OpenVZ : A container-based virtualization solution for Linux
   http://wiki.openvz.org
7. libvirt : The virtualization API
   http://www.libvirt.org
8. Prigent, G., Vichot, F., Harrouet, F. : IpMorph : unification de la mystification de prise d'empreinte
   http://actes.sstic.org/SSTIC09/IpMorph-unification_de_la_mystification_de_prise_d_empreinte/SSTIC09-article-G-Prigent-F-Vichotet-F-Harrouet-IpMorph-unification_de_la_mystification_de_prise_d_empreinte.pdf

Un coupe-feu adapté aux enjeux de l'informatique industrielle

Arnaud Tarrago, Pierre Nguyen, Pascal Sitbon

EDF R&D prenom.nom@edf.fr

Résumé Les systèmes d'information des infrastructures industrielles critiques font face à deux exigences difficiles à concilier.. D'un côté, les attentes en matière de cyber sécurité se renforcent, conduisant à une segmentation des systèmes d'information (SI) et à une mise en place d'un filtrage strict entre ces zones. De l'autre, la complexité des systèmes industriels à exploiter pousse à mettre en place de nouveaux échanges d'information entre SI de niveaux de confiance différents pour accroître la qualité et la rigueur d'exploitation, et faciliter la tâche de l'exploitant.

Les solutions de coupe-feu logiques ou de diode unidirectionnelles habituelles ne permettent pas de résoudre cette contradiction lorsqu'il s'agit de sanctuariser des systèmes réellement critiques :

- Les coupe-feu proposent un niveau de sécurité insuffisant. Leur efficacité à assurer la séparation et la communication entre des systèmes d'information de niveaux de confiance différents n'est assurée que par leur sûreté d'implémentation et leur bonne maîtrise des protocoles de communication. Indépendamment de cette sûreté logicielle, une mauvaise application de la politique de sécurité ou une erreur dans la configuration de ces dispositifs lors de leur administration a un fort impact sur le niveau de sécurité. Ce risque entraîne donc une nécessité de surveillance et d'audit permanent des éléments mis en place, sans pour autant que ces mesures suffisent à garantir la sécurité.
- Les diodes unidirectionnelles répondent seulement à une partie des besoins. Du fait de leur unidirectionnalité et en l'absence de retour d'information vers la source, elles ne permettent pas de vérifier que la transmission s'est faite correctement. Cette solution impose la mise en place de logiciels spécifiques ayant une adhérence forte avec un type de matériel et de système les hébergeant. De plus cet équipement ne répond pas aux besoins de faire remonter de l'information d'une zone moins sensible vers une zone plus sensible.

Une autre solution consiste à séparer physiquement les systèmes d'information en utilisant des réseaux disjoints. Cependant, dans un contexte industriel, cette séparation répond mal aux évolutions du métiers (notamment en dédoublant l'exploitation) et présente d'autres risques, car elle ne peut jamais être « totale ». Elle pousse alors à trouver des solutions « hors ligne » pour échanger de l'information, souvent sous la forme de supports amovibles (clés USB, etc.). Ce type de réponse présente donc des risques significatifs de transmissions de programmes malveillants d'un niveau de confiance à l'autre.

A la vue de la non correspondance entre les besoins industriels d'EDF et les solutions du marché, EDF R&D a conçu, breveté et réalisé DESIIR (Dispositif d'Echange Sécurisé d'Information sans Interconnexion Réseau) qui permet de transmettre des informations entre deux systèmes de niveaux de confiance différents, et en particulier d'une zone moins sensible vers une zone plus sensible, tout en garantissant un très haut niveau de sécurité. Il devient possible, par exemple, de faire transiter une information d'un réseau de gestion vers un réseau industriel (plan de production) ou d'un réseau non sûr vers un réseau industriel (remontée d'un réseau de capteurs sans-fil vers la supervision), tout en conservant un haut niveau de sécurité du côté du process.

Le principe de DESIIR est de garantir que seule une information répondant strictement au format attendu peut passer vers la zone destinataire. Le paramétrage du dispositif

est figé matériellement à sa fabrication, ce qui permet aussi une mise en service directe sans configuration ni administration. Une information ne respectant pas le format attendu sera rendue inoffensive et détectable par le système destinataire de l'information. DESIIR empêche également une prise de contrôle directe d'une zone vers l'autre. Plug & Play, le dispositif est supporté nativement par les systèmes (Windows, Linux, Ĕ). Afin d'apporter une preuve indépendante du niveau de sécurité, DESIIR a obtenu en avril 2010 la Certification Sécurité de Premier Niveau délivrée par l'ANSSI (certificat CSPN-ANSSI-2010/03).

Ce dispositif permet ainsi, d'établir des nouveaux flux d'information à forte valeur ajoutée vers un système sanctuarisé, de renforcer le niveau de sécurité et de simplifier les architectures coupe feu pour des flux d'information existant.

Cet article présente la conception et les mécanismes de sécurité du dispositif DESIIR, la cible de sécurité correspondant à la certification obtenue, ainsi que les perspectives d'évolution de ce dispositif.

1 Les besoins spécifiques des métiers industriels

De nos jours, les systèmes informatiques peuvent difficilement s'affranchir des fonctionnalités et des performances apportées par certaines interconnexions pour répondre aux enjeux métiers. Cependant, dans certains cas, en particulier pour les infrastructures critiques, il est de la responsabilité des opérateurs d'apporter l'assurance d'un haut niveau de sécurité informatique. Cette responsabilité est actuellement en cours d'organisation depuis le décret n° 2006-212 du 23 février 2006 relatif à la sécurité des activités d'importance vitale définissant les Secteurs d'Activité d'Importance Vitale (SAIV), déclinées par la suite en Directives Nationales de Sécurité (DNS). L'Agence Nationale Sécurité des Systèmes d'Information (ANSSI) a depuis 2009 comme mission supplémentaire d'aider à répondre aux enjeux de sécurité des infrastructures vitales.

Par ailleurs, une contrainte spécifique des sites industriels est le fait de disposer de peu d'expertise en réseaux et sécurité sur place. De fait, les architectures nécessitant ces compétences pour la surveillance, l'administration et l'exploitation sont difficilement intégrables en pratique.

On distingue deux besoins principaux d'échange du monde industriel :

- La publication d'information depuis une zone sensible vers l'extérieur, sans possibilité d'accès inverse (communication unidirectionnelle sortante)
- Le transfert d'informations situées dans une zone externe vers une zone sensible, avec des contraintes fortes sur les types de données (format connu à l'avance)

Des exemples sont données au chapitre « les cas d'usage industriels du dispositif ». Les enjeux dans le monde industriel sont nettement différents des enjeux classiques de l'informatique de gestion. Nous cherchons dans les deux cas d'usage précités à apporter une protection très élevée des zones sensibles. Par exemple, la politique actuelle n'autorise aucun flux informatique à entrer dans une zone sensible, y compris un flux retour (ex : acquittement de transfert). Ces contraintes

particulières font que des solutions usuelles sont rarement utilisables telles quelles en environnement industriel sensible. Plus formellement, nous définissons les besoins du dispositif comme suit :

B.1 : besoin d'un très haut niveau de sécurité

- B.1A : garantir que le niveau de protection reste maîtrisé même en cas de vulnérabilité logicielle ou d'erreur de configuration
- B.1B : protéger le système destinataire contre des attaques de contenu. En particulier, les fichiers mal formés, non conformes aux spécifications, les auto-exécutables et virus doivent être détectés et rendus inoffensifs.

B.2 : besoin de fiabilité et de garantie de transfert. L'émetteur doit savoir si le transfert qu'il a initié a fonctionné. B.3 : besoin de confort. La solution doit pouvoir être utilisée pour effectuer des échanges réguliers basés sur une interaction applicative.

- B.3A : le dispositif doit fonctionner sur les différents systèmes avec le minimum d'impact (donc sans installation supplémentaire) et être nativement interopérable avec ces systèmes (plug & play)
- B.3B : des connaissances basiques sont suffisantes pour installer et utiliser le dispositif. En particulier il ne doit pas nécessiter de compétences sécurité et réseau élevées pour son exploitation et son administration sur site industriel.

2 Les solutions existantes ne couvrent pas ces besoins

Les solutions existantes ne répondent pas à tous les besoins évoqués, mais avec la difficulté de combiner haute sécurité et fiabilité / « utilisabilité ». Les besoins exprimés au paragraphe précédent (cf. B.1, B.2 et B.3) impliquent les caractéristiques principales qu'une solution cible doit mettre en oeuvre :

- séparation « physique », c'est-à-dire sans flux réseau de bout en bout ;
- validation du format des données échangées ;
- absence de point unique de défaillance ou de malveillance ;
- confort d'utilisation élevé ;
- garantie de délivrance de l'information ;
- mise en place simplifiée et utilisation sans connaissance technique particulière.

La protection des réseaux peut être assurée par des dispositifs dont la sécurité repose sur leur sûreté d'implémentation et la bonne maîtrise des protocoles de communication. C'est le cas notamment des dispositifs classiques « coupe-feu », des relais applicatifs, des produits segmentant les réseaux (VLAN, 802.1Q). De nombreuses failles [1][2][3] ont été révélées dans ce type de dispositifs entraînant la compromission du réseau qu'ils étaient censés protéger. Ces failles logicielles peuvent également se retrouver dans les mécanismes d'inspection protocolaire des

Solution	Avantages	Inconvénients	Besoins		
			B.1	B.2	B.3
Architecture DMZ classique	Solution disponible sur le marché et très répandue	Niveau de sécurité généralement jugé insuffisant en contexte industriel	Non	Oui	Partiel
Diode physique	Haute sécurité (unidirectionnel au niveau physique)	Ne permet pas d'assurer une garantie de délivrance d'une information, le poste à protéger n'a pas l'initiative de l'échange, exposé aux contenus malveillants	Partiel	Non	Partiel
Transfert par un support physique	Pas de connectivité physique entre réseaux	Difficilement utilisable en pratique, nécessite le déplacement d'un intervenant à chaque nouvel échange, exposé aux contenus malveillants	Partiel	Partiel	Non

Figure 1. Comparaison des types de solutions existantes pour la publication d'informations

Solution	Avantages	Inconvénients	Besoins		
			B.1	B.2	B.3
Architecture DMZ classique	Solution disponible sur le marché et très répandue	Niveau de sécurité généralement jugé insuffisant en contexte industriel	Non	Oui	Partiel
Diode physique	*Non applicable*		*Non*	*Non*	*Partiel*
Transfert par un support physique	Pas de connectivité physique entre réseaux	Difficilement utilisable en pratique, nécessite le déplacement d'un intervenant à chaque nouvel échange, exposé aux contenus malveillants	Partiel	Partiel	Non
Transfert « papier »	Pas de connectivité réseau, ni d'entrée de données numériques	Difficilement utilisable en pratique, complexe à gérer, peu de fiabilité (erreurs de saisie, etc.).	Oui	Non	Non

Figure 2. comparaison des types de solutions existantes pour le transfert d'informations d'une zone « moins sûre » vers une zone « plus sûre »

coupe-feu évolués, d'autant plus qu'ils peuvent être basés sur des bibliothèques extérieures non maîtrisées (par exemple : bibliothèque XML[4]).

Indépendamment de cette sûreté logicielle, une mauvaise application de la politique de sécurité ou une erreur dans la configuration de ces dispositifs a potentiellement un fort impact sur le niveau de sécurité. Ce risque entraîne donc une nécessité de surveillance et d'audit permanent des éléments mis en place, sans pour autant que ces mesures suffisent à garantir la sécurité.

Certaines solutions de haut niveau de sécurité existent mais n'apportent généralement pas le confort d'utilisation et la fiabilité nécessaires aux environnements industriels. C'est par exemple le cas des « diodes physiques » unidirectionnelles [5], qui permettent de faire passer de l'information d'un niveau de confiance plus exigeant vers un niveau moins sévèrement protégé. Ce type d'équipement ne couvre cependant que partiellement les besoins, d'une part du fait de son unidirectionnalité (il ne permet pas de protéger des échanges d'une zone « moins sûre » vers une zone « plus sûre ») et d'autre part du fait de l'absence de retour d'information vers la source qui ne permet pas de vérifier que la transmission s'est faite correctement. De plus, il impose la mise en place de logiciels spécifiques ayant une adhérence forte avec un type de matériel et de système les hébergeant.

3 La conception d'un dispositif innovant : DESIIR

Comme nous venons de le voir, les solutions existantes ne sont pas satisfaisantes. Afin de répondre aux besoins métiers et de proposer un dispositif innovant permettant de dépasser les problématiques inhérentes à la mise en place d'architectures coupe-feu, nous avons conçu DESIIR : un *Dispositif d'Echange Sécurisé d'Informations sans Interconnexion Réseau*.

3.1 Les principes de DESIIR

DESIIR est un dispositif connecté via un port physique (type USB ou S-ATA) à chacune des machines, permettant d'échanger des informations sans interconnexion réseau. Les échanges entre DESIIR et les machines connectées sont restreints par les capacités physiques de ce type de connexion. La sécurité repose donc en premier lieu sur la nature même du dispositif, indépendamment de la qualité d'implémentation ou de sa configuration.

La figure 3 ci-dessous, représente le branchement de DESIIR à l'aide de ports USB. Ce branchement occasionne une découverte de matériel de la part des systèmes connectés. DESIIR y est vu comme un disque dur USB (unité de stockage de masse) et les drivers natifs au système connecté sont utilisés (Windows, Linux, OS industriel, Ĕ) . Aucune installation de logiciel n'est à effectuer.

La machine de la zone A peut déposer des fichiers dans cette unité de stockage en toute transparence en utilisant les commandes de copie/écriture de son système

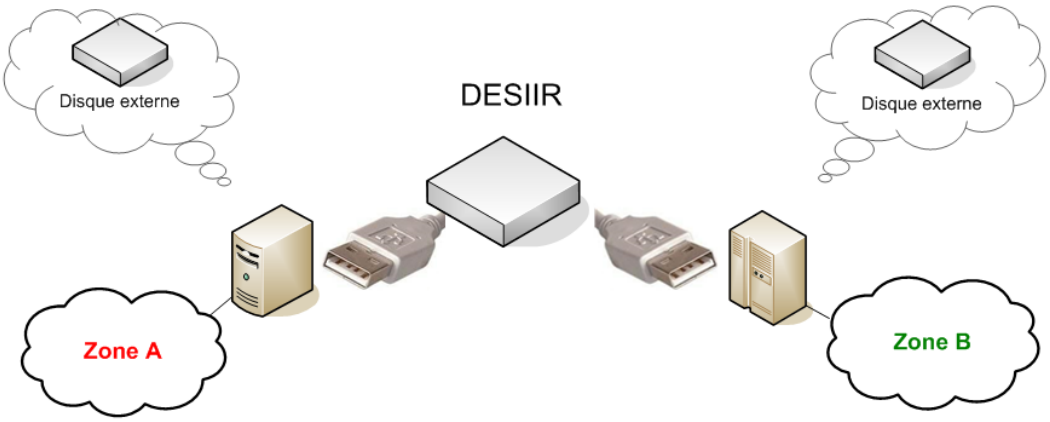


Figure 3. Concept général de DESIIR

d'exploitation. Le dispositif se charge d'analyser les données déposées, de les rendre inoffensives (liste d'extension de fichiers autorisés, transformation des noms et du contenu en certains caractères ASCII avec vérification de leur syntaxe) et de les présenter à l'autre extrémité si elles correspondent à la politique de sécurité du dispositif. La machine de la zone B n'aura ainsi que la visibilité sur des fichiers permis et sains et pourra, à son initiative lire ce fichier pour le traiter (cf figure 4).

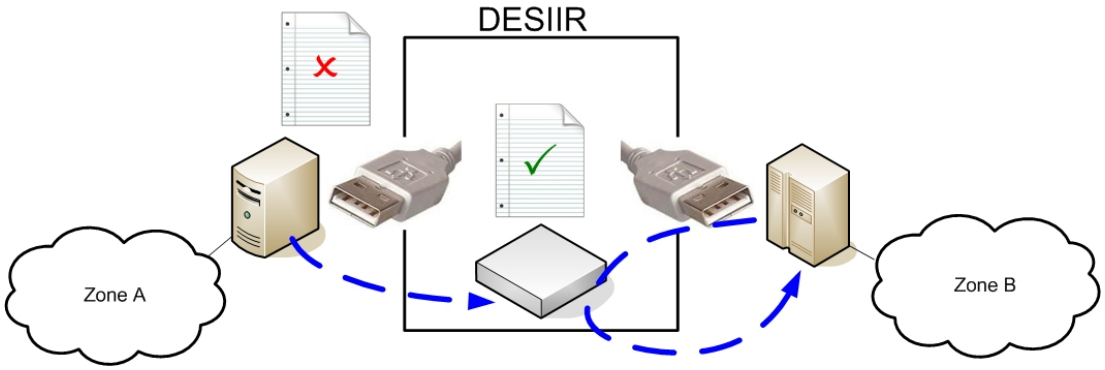


Figure 4. Principe général de fonctionnement de DESIIR

DESIIR peut ainsi assurer le passage d'une information filtrée et contrôlée d'une zone à une autre. Mais ce dispositif est principalement conçu pour sécuriser les flux d'information en provenance d'une zone « moins sensible » (zone A sur la fig. 3&4) et à destination d'une zone « plus sensible » (zone B sur la fig. 3&4).

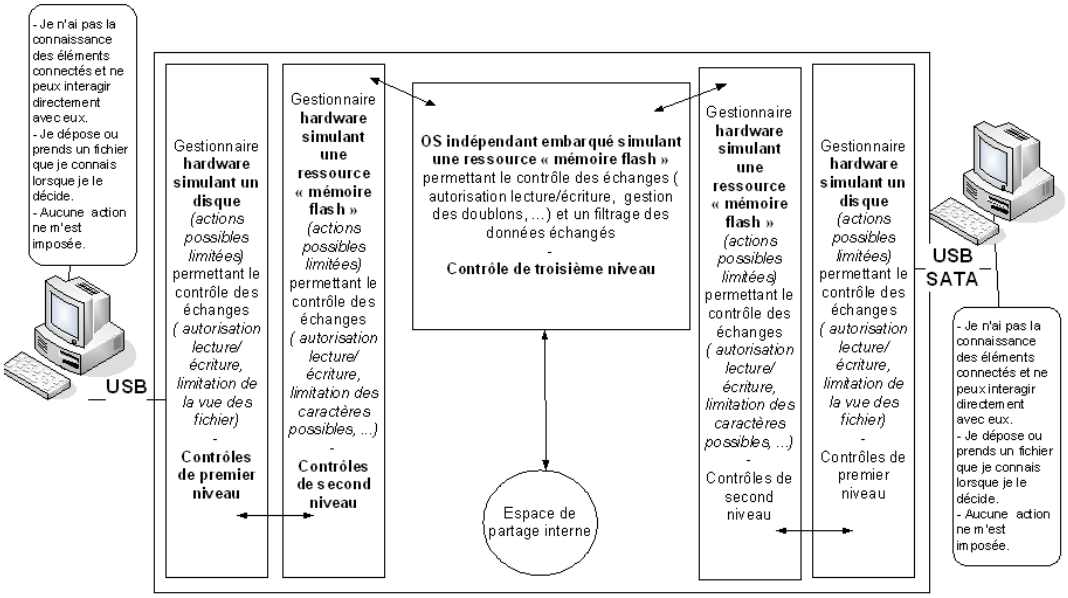


Figure 5. Détails de conception de DESIIR (mode de fonctionnement générique)

Son architecture interne est conçue comme une chaîne coupe-feu, comprenant un élément de coupure asynchrone, des contrôles d'accès redondants, des implémentations et des conceptions de filtres différents sur des architectures physiques différentes. Les composants ne se connaissent pas et ne se font pas confiance. Un transfert d'information est contrôlé sous différents aspects par plusieurs composants avec des implémentations différentes. Il permet ainsi d'embarquer dans un dispositif plusieurs concepts de sécurité que nous allons détailler.

3.2 Séparation physique, sans flux réseau de bout en bout

DESIIR est un dispositif permettant de faire de la rupture protocolaire. Les informations en transit peuvent être acheminées via des protocoles réseaux (TCP/IP) sur les machines connectées au dispositif et lues ou écrites via le protocole USB/SCSI sur le disque DESIIR.

Le dispositif est vu sur les systèmes « hôtes » comme une mémoire de masse et adopte donc un comportement similaire à celui d'un disque dur externe.

Ce mode de connexion évite l'installation de logiciel spécifique sur les postes et d'être indépendant du système d'exploitation à partir du moment où il supporte les connexions « USB Mass Storage » (disque dur USB).

Le disque dur interne est un élément de coupure, il permet de l'échange d'information sans qu'à un moment, les postes connectés puissent s'échanger direc-

tement des flux (de quelque nature que ce soit). Il jouerait un rôle similaire à un « proxy applicatif » dans un coupe-feu traditionnel.

Ce mode permet de s'assurer également que les différents systèmes connectés à DESIIR ne subissent pas l'arrivée d'un flux d'information : la lecture ou l'écriture d'un fichier se fait à l'initiative de chaque système avec une connaissance préalable des fichiers à prendre en compte (élément choisi). Plusieurs mécanismes de sécurité rendent inopérants les fichiers de type auto-exécutable (autorun, Ĕ).

Indépendamment du niveau de sécurité de l'implémentation de DESIIR, le poste destinataire est maître de sa sécurité et peut (doit) lui-même mettre en place des mécanismes de protection (vérification applicative du format de fichier, etc.).

3.3 Dispositifs de contrôle redondants et d'implémentations différentes

Le premier niveau de contrôle est pris en charge par le contrôleur de ports physiques du dispositif. Dans notre première implémentation, c'est un contrôleur USB que nous avons réécrit afin d'être sûr du code implémenté et de ne pas dépendre d'un code dont nous n'avons pas la maitrise. N'ont été implémenté et programmé que le minimum de commandes afin de réaliser des actions de contrôle simple (interdiction d'écriture depuis le poste destinataire, écriture sur une clef qui apparaît comme vide, Ĕ). Le contrôleur ne connaît pas le deuxième niveau et il a l'impression d'écrire sur une mémoire Flash.

Le deuxième niveau de contrôle est une implémentation faite sur un composant intelligent mais figé. Il a pour but de simuler une mémoire Flash au contrôleur de premier niveau et n'est donc pas connu des postes utilisateurs et des autres composants internes du dispositif. Il applique un filtre « basiqueż sur les caractères (restriction des caractères dans un sous ensemble de la table ASCII) et la longueur de la ligne. Ce filtre ne comprend pas ńla structure d'un fichier », il applique la procédure de filtre ASCII automatiquement quelle que soit l'entrée. Cette non - connaissance permet au dispositif de ne pas être sensible à des attaques se servant de la structure de fichier ou du contenu comme support d'attaque. Il revérifie les droits d'écriture ou de lecture, notamment en ne possédant pas le code d'écriture lorsque la diode est paramétrée pour un sens de communication figée. Cela signifie donc que même si un attaquant parvenait à lui demander de faire une action d'écriture, le composant ne sait pas ce que « écrire » signifie, il n'a pas de code correspondant. Il ne connaît pas le troisième niveau et à l'impression d'écrire sur une mémoire Flash.

Le troisième niveau est une implémentation faite sur un composant intelligent et évolutif. Il simule une mémoire au contrôleur de deuxième niveau et n'est donc pas connu des postes utilisateurs et des autres composants internes du dispositif. Il applique un filtre « intelligent » sur les caractères, la longueur de lignes, les extensions de fichier et le contenu (grammaire d'analyse du contenu de fichier).

3.4 Limitation physique des opérations réalisables

Les opérations pouvant être effectuées sur les fichiers sont déjà limitées par le type de connexion de DESIIR. Néanmoins, en fonction des cas d'usage du dispositif, nous avons choisi de limiter en plus le code présent dans certains composants électroniques internes. Ainsi, les fonctions ne devant pas être accessibles (par exemple, la lecture d'un fichier lorsque seule l'écriture est permise) ne sont pas présentes dans le composant interne de deuxième niveau. Le dispositif DESIIR possède donc une limitation physique des opérations réalisables.

3.5 Validation du contenu des informations échangées

DESIIR a été conçu pour filtrer le contenu des fichiers échangés de plusieurs façons :

- substitution à la volée par un caractère de contrôle, des caractères ne correspondant pas à des caractères choisis (par exemple caractères compris dans l'intervalle ASCII 0-128) avec une double vérification de ces caractères lors de l'écriture du fichier
- contrôle du nombre de caractères maximum par ligne avec le cas échéant une césure de la ligne.
- contrôle et modification à la volée du nom et de l'extension des fichiers, en fonction d'une liste blanche ou d'une liste noire
- analyse du contenu afin de valider que chaque ligne correspond à une syntaxe connue (par exemple : ligne commençant par une référence alphanumérique de 8 caractères, suivi d'un indicateur d'état de deux caractères numériques, etc.). Afin de mesurer la robustesse de notre dispositif, la version certifiée CSPN a porté sur un boitier ne faisant pas d'analyse syntaxique. Si cette analyse est mise en place, le niveau de sécurité sera renforcé mais la solution devient adhérente à un usage spécifique

Ces contrôles et analyses permettent de valider la cohérence des fichiers échangés et donc de bloquer les tentatives d'écriture d'exécutables ou de scripts qui pourraient endommager les systèmes connectés. Ces éléments sont renforcés par des interdictions d'écriture. Il est, par exemple, impossible d'écriture à la racine du dispositif interdisant, de faite, toute tentative d'utilisation d'auto exécutable.

3.6 Virtualisation des ressources

Indépendamment des modifications faites « à la volée » sur les fichiers déposés via DESIIR (limitation des caractères utilisés, longueur de ligne maximum, etc.), le dispositif contrôle la façon dont les informations sont échangées afin de protéger les machines connectées de différentes attaques possibles. Ainsi, les ressources accessibles sur le disque n'apparaissent qu'à partir du moment où elles

sont permises et validées. Cela correspond à une sorte de virtualisation : Chaque poste connecté a une « vue différente » des fichiers présents sur le disque USB Mass Storage présenté par DESIIR.

3.7 Synthèse des dispositifs de protection

Les différents dispositifs peuvent être représentés sous deux thèmes, sécurité physique (rebond ou intrusion extrêmement difficiles) et sécurité logique (contrôle de contenu), chacun implémentant le principe de défense en profondeur. Il est important de noter que, conformément aux bonnes pratiques, le niveau de sécurité du dispositif dépend de la conception et de l'implémentation du dispositif mais ne repose pas sur un quelconque secret. Le schéma ci-dessous ne précise pas le lieu de ces différents contrôles et filtrages, il indique juste que ces derniers sont redondants.

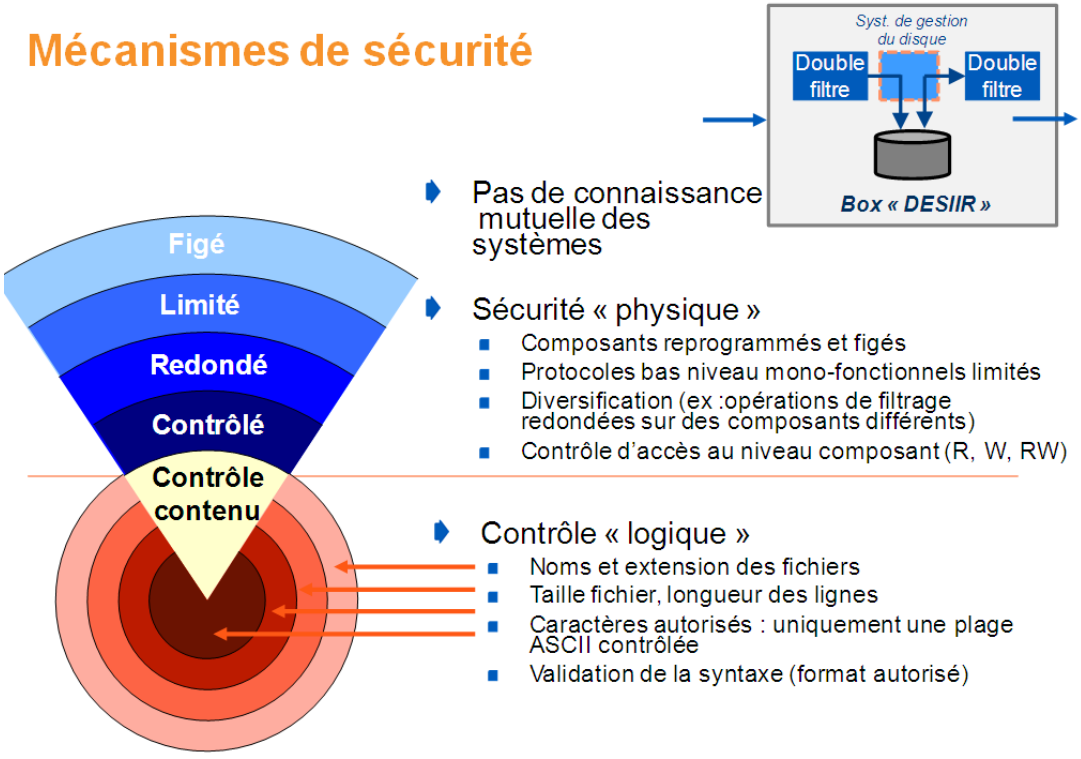


Figure 6. Synthèse des mécanismes de sécurité de DESIIR

Le dispositif DESIIR respecte le cahier des charges initial et permet de répondre aux besoins B.1, B.2 et B.3 (cf. paragraphe « Les besoins spécifiques des métiers industriels »). En particulier, il apporte :

- Une séparation « physique », sans flux réseau de bout en bout et sans même que le système d'exploitation sache qu'un échange de données est en cours ;
- Une validation du format et du contenu des données échangées ;
- Une absence de point unique de défaillance ou de malveillance ;
- Un confort d'utilisation élevé ;
- Une garantie de délivrance de l'information ;
- Une mise en place simplifiée sans connaissance technique particulière et sans administration

Il possède donc des avantages certains sur l'ensemble des solutions existantes.

4 DESIIR est conforme par conception à l'état de l'art des architectures coupe-feux

Le dispositif DESIIR vient en remplacement ou « en simplification » des dispositifs coupe-feu réseau existant. Nous avons voulu concevoir un dispositif respectant « l'état de l'art » des règles et principes de sécurité informatique appliqués aux infrastructures réseaux de confiances. Une architecture coupe feu doit être en mesure de protéger un système d'information tout en lui permettant de communiquer avec l'extérieur. L'état de l'art en sécurité suppose par ailleurs que l'architecture vérifie un certain nombre de critères : au moins 2 dispositifs de filtrage, pas d'accès direct sur les équipements de filtrages, un hébergement à étages avec filtrage inter niveaux, un cloisonnement des zones d'hébergement, une barrière de routage, des règles de gestion et d'administration de l'architecture ńnon modifiables », une rupture de protocole et la non-implémentation. Ces critères sont détaillés ci-dessous.

4.1 Au moins 2 dispositifs de filtrage

Il est recommandé d'utiliser au moins 2 dispositifs filtrants de conception technologique différente afin que les lacunes ou failles du premier soit compensées par le second dispositif, ou en tous cas que le même type d'attaque ne soit pas susceptible de mettre à mal l'architecture globale. DESIIR tient compte et implémente cette recommandation.

4.2 Pas d'accès direct sur les équipements de filtrages

Il est recommandé de ne pas rendre les plates-formes hébergeant les coupe-feux visibles depuis les zones connectées (Internet, réseaux internes), particulièrement lorsque ceux-ci sont de fabrication étrangère, afin d'éviter non seulement l'utilisation d'éventuelles portes dérobées, mais plus pratiquement de rendre plus difficile l'exploitation d'une faille découverte sur le dispositif. DESIIR tient compte et

implémente cette recommandation : les systèmes et les fichiers internes de configuration ne sont pas accessibles par les ports du dispositif (USB sur la première implémentation).

4.3 Hébergement à étages avec filtrage inter niveaux

Les zones d'hébergement sont étagées sur les différents composants de l'architecture coupe feu ; afin de permettre la répartition des composants applicatifs, et de disposer ainsi de gradients de sécurité croissants. Un filtrage doit être mis en oeuvre entre chaque zone de telle sorte que seuls les flux nécessaires et suffisants au bon fonctionnement de l'application soient autorisés entre deux de ses étages consécutifs. DESIIR implémente cette recommandation : il y a cinq niveaux de contrôle dans DESIIR avec trois implémentations différentes sur les trois composants physiques internes de nature différente.

4.4 Cloisonnement des zones d'hébergement

Sur les zones d'hébergement, les serveurs sont logiquement isolés les uns des autres de telle sorte que la compromission de l'un d'entre eux ne soit pas un facteur de risque pour le reste de la communauté. Des échanges entre zones logiques peuvent exister pour des besoins applicatifs, mais selon les mêmes modalités que les échanges applicatifs entre zones physiques (Cf. ğ précédent). DESIIR implémente cette recommandation : les cinq éléments filtrant ne se connaissent pas.

4.5 Barrière de routage

La ńbarrière de routage » est une protection extrêmement importante, visant à ce que les routes IP vers les réseaux internes ne soient pas connues depuis Internet, mais uniquement des quelques composants de l'infrastructure, ayant, pour leur fonction, besoin de cette information (typiquement les relais). Si la route n'est pas connue, le flux ne pourra transiter, ce qui rend inutile le filtrage. Toutefois, par précaution, un filtrage par défaut interdisant tout échange sera toujours présent pour pallier la mise en oeuvre erronée ou la création « malicieuse » de règles de routage. DESIIR, par conception, respecte ce principe.

4.6 Règles de gestion et d'administration de l'architecture « non modifiables »

Plusieurs problèmes se posent généralement avec une infrastructure coupe-feu classique. Avec ce type d'infrastructure, la conception et l'architecture applicative sont primordiales. Néanmoins, la configuration, l'administration et le maintien en condition opérationnelle de ces dispositifs sont tout autant vitaux. Une grande

partie des failles ou des éléments remontés dans les audits de sécurité fait par exemple, apparaître des problématiques de cohérence de filtres, des règles d'administration non maintenues ou encore un manque d'administration système. Dans la conception de DESIIR, nous voulions remplacer avantageusement les infrastructures existantes par un dispositif simple, robuste et sécurisé pouvant apporter un grand nombre de simplification. DESIIR est conçu avec des éléments programmables « physiquement » mais dont la modification a été rendue quasi-impossible. Il possède deux niveaux de filtrage : un filtrage basique assurant que les caractères des fichiers sont bien limités à une certaine plage prédéfinie de la table ASCII ; et un filtrage évolué portant globalement sur le contenu des fichiers (extensions de fichier autorisé, vérification du format et de la cohérence des données). La gestion, la surveillance, l'audit des fichiers de configuration n'est pas nécessaire : l'ensemble des filtres, prédéfinis suivant le cas d'usage métier, est figé en usine à la fabrication du dispositif.

4.7 Versions, correctifs des systèmes et architecture de pré production

De façon générale, les composants impliqués de quelque façon que ce soit dans l'infrastructure de filtrage et de cloisonnement, de même que les serveurs accueillant les applications doivent fonctionner avec une version système récente (voire la version stable la plus récente) corrigeant les failles de sécurité connues. En cas de détection de faille, les correctifs doivent être apportés dès leur publication, avec une rapidité proportionnelle à la sensibilité de la zone où la vulnérabilité a été détectée. Il est recommandé de valider préalablement la mise en oeuvre du correctif sur une architecture de pré production représentatif de la chaîne en exploitation. Lors de la mise en place de ces correctifs, une procédure d'exploitation spéciale est mis en oeuvre : un plan prévisionnel est mise en place avec une prévision des « retours arrières » et des procédures de sauvegarde avant et après la mise en place des correctifs. DESIIR apporte une protection par concept avec une implémentation minimaliste. Il n'est ainsi pas assujetti à la mise en place de correctifs. Si cela devait se passer (correction de bugs, Ĕ) un remplacement physique du dispositif sera alors opéré. Le branchement de DESIIR ne nécessitant aucun paramétrage ou configuration, il suffit de remplacer l'ancien par le nouveau dispositif (et réciproquement) : le retour arrière est donc simple et immédiat.

4.8 Rupture de protocole

La notion de « rupture de protocole » est une protection importante et très rarement mise en oeuvre. Le concept est simple : l'utilisation d'un protocole donné d'un bout à l'autre d'une chaîne de sécurité est souvent sujet à des comportements non prévus initialement ou à des faiblesses. Par exemple l'utilisation du protocole IP sans restriction, a permis un grand nombre d'exploitation de failles dues à des

problèmes de conception de ce protocole. Des failles comme le « source routing » (la possibilité de mettre « le chemin de retour » dans les paquets, permettant des usurpations d'adresse) ou la fragmentation IP (possibilité de modifier un paquet réassemblé par le destinataire final, permettant de passer les coupe-feux sur des connexions interdites) sont connues. Pour éviter qu'un problème sur un protocole ne se diffuse tout au long de sa chaîne d'utilisation, les architectures coupe-feu mettent en place des « coupures » protocolaires (proxy, passerelle, architectures 3 tiers, Ĕ). Ces éléments de coupures ne représentent pas vraiment de rupture protocolaire qui correspond à une utilisation d'un autre protocole pour la même fonction en mettant en oeuvre des passerelles de conversion. Ainsi chaque option particulière à un protocole ne franchira pas la passerelle de conversion puisque qu'elle n'aura vraisemblablement pas d'équivalent dans le deuxième protocole. DESIIR a été conçu pour ne pas utiliser de protocole réseau. Il représente une rupture protocolaire pour des informations transportées de part et d'autre par le protocole IP. Dans sa première implémentation, il est connecté via des ports USB utilisant le protocole SCSI, protocole de lecture et d'écriture de données.

4.9 La non-implémentation

La plupart des dispositifs de sécurité interdisent une fonctionnalité ou une action par configuration. DESIIR a été conçu pour s'adapter sur mesure à un cas d'usage. Il est ainsi possible de décliner le dispositif en plusieurs versions spécialisées qui implémentent ou non les fonctionnalités désirées selon les cas d'usage : les fonctionnalités ou actions seront ainsi de facto interdites par fabrication et non plus par configuration.

5 Contraintes et limitations de DESIIR

Comme tout dispositif technique, la bonne utilisation de DESIIR nécessite de respecter des contraintes globales de fonctionnement :

- La mise en oeuvre du dispositif doit respecter des règles d'utilisation, en particulier ne pas inverser les branchements (cela n'entraîne cependant pas un risque de compromission mais plutôt un risque de mauvais fonctionnement) ;
- Une entité de confiance doit contrôler la chaine logistique (fabrication, transport) pour éviter tout risque de piégeage du dispositif (exemple : remplacement d'un composant ou modification du code embarqué) ;
- Les deux machines à interconnecter doivent être relativement proches (limitation liée à l'USB de l'ordre de 60m de chaque côté de DESIIR), cependant il est possible de déporter le port USB d'une machine via le réseau en cas de besoin pour s'affranchir de cette limitation de distance ;

A ces contraintes, s'ajoutent quelques limitations et précautions d'usage plus spécifiques :

- DESIIR, ne connaissant pas la logique métier sous-jacente, ne protège pas le processus métier associé. Le dispositif peut bien évidemment, si nécessaire, être complété par un processus de validation humaine confirmant la pertinence métier de l'information transmise, au-delà de son innocuité et de sa conformité au format attendu ;
- Une modification du cas d'usage métier de DESIIR nécessite de remplacer physiquement le dispositif (exemple : le format de fichier autorisé à été modifié) ;
- Dans la version actuelle, l'intégrité des données transférées n'est pas assurée nativement par le dispositif dans le cas où le fichier déposé ne correspond pas aux règles de filtrages établies. Cependant des mécanismes additionnels peuvent permettre de palier à ces défauts, notamment avec l'utilisation de mécanismes de signature,

6 Evaluation externe : la certification CSPN

Afin d'apporter une confiance dans le niveau de sécurité du dispositif de manière indépendante, une validation gouvernementale en CSPN (Certification de Sécurité de Premier Niveau) a été obtenue. Cette évaluation est validée par l'ANSSI. La CSPN donne une mesure de l'assurance que l'on peut avoir dans le dispositif :

- Sur la conformité du produit par rapport à ses spécifications
- Sur l'efficacité des fonctionnalités de sécurité prévues

EDF R&D a décidé de rendre publique, à la fois la certification et la cible de sécurité. Elles sont disponibles sur le site de l'ANSSI [6]. Cette cible de sécurité [7] a été élaborée avec le laboratoire d'évaluation et a été validée par l'ANSSI. Elle garantit que le produit est évalué en fonction des propriétés de sécurité communément attendues de la part de ce type de produit. La cible de sécurité choisie appartient **à la catégorie 6 : la gamme des coupe-feux**. Les hypothèses prises en compte sont :

- Le dispositif DESIIR doit être utilisé dans un environnement considéré comme physiquement sûr (local à accès contrôlé, de même niveau de confiance que la zone haute) au niveau du produit et de la machine haute. Ainsi, le produit ne prend pas en compte de sécurité particulière au niveau de malveillances matérielles et/ou utilisant un accès physique au produit.
- Le dispositif DESIIR est entièrement configuré lors de sa fabrication, donc avant sa livraison. Les fonctions du produit sont figées et ne sont plus modifiables par la suite.

- Les seules actions d'administration sont le raccordement des interfaces USB et la mise sous tension du dispositif. Les deux rôles distincts existant sont donc le rôle utilisateur côté machine basse et le rôle utilisateur côté machine haute.
- L'utilisateur de la machine haute est considéré de confiance. De ce fait, l'attaquant situé côté machine basse ne peut pas disposer de complice ayant accès à la machine haute.

L'agent menaçant est tout utilisateur pouvant se connecter sur la machine basse ou à la place de la machine basse. Les menaces contre lesquelles protège le dispositif DESIIR sont les suivantes :

- Tentative de prise de contrôle de la machine haute depuis la machine basse via le dispositif DESIIR.
- Transfert de données non autorisées depuis la machine basse vers la machine haute
- Modification de la configuration du dispositif via les seules interfaces accessibles du dispositif, à savoir le câble USB.
- Transfert illicite de données depuis la machine haute vers la machine basse

DESIIR a obtenu en avril 2010 la Certification Sécurité de Premier Niveau délivrée par l'ANSSI (certificat CSPN-ANSSI-2010/03). Ce certificat apporte l'assurance d'un haut niveau de sécurité de manière indépendante des concepteurs, et de fait conforte son usage pour un nombre important de processus industriels du Groupe EDF, et plus généralement pour toute industrie sensible telle que les Opérateurs d'Importance Vitale (OIV) définis par la Directive Nationale de Sécurité (DNS). Déjà industrialisable dans sa version actuelle, différentes évolutions et variantes du dispositif sont actuellement en prototypage : augmentation des capacités de transfert, version embarquée sur une carte interne de PC, version avec interfaces réseau à la place des interfaces USB actuelles.

7 Les cas d'usage industriels du dispositif

Le dispositif a été prévu pour les cas « métiers » lié aux infrastructures industrielles

7.1 Remontée d'information de réseaux exposés (capteurs)

Ce cas d'usage concerne la remontée d'informations provenant de réseaux exposés (réseaux de capteurs sans fil). En effet, il est envisagé d'installer des capteurs de mesure d'instrumentation complémentaires, reliés avec des technologies sans fil ou situés dans des zones moins protégées physiquement. La remontée de ces données peut donc potentiellement représenter un risque d'intrusion via une porte d'entrée plus facile à franchir. Dans ce cas, DESIIR permet de récupérer ces données de capteurs sans exposer le réseau connecté.

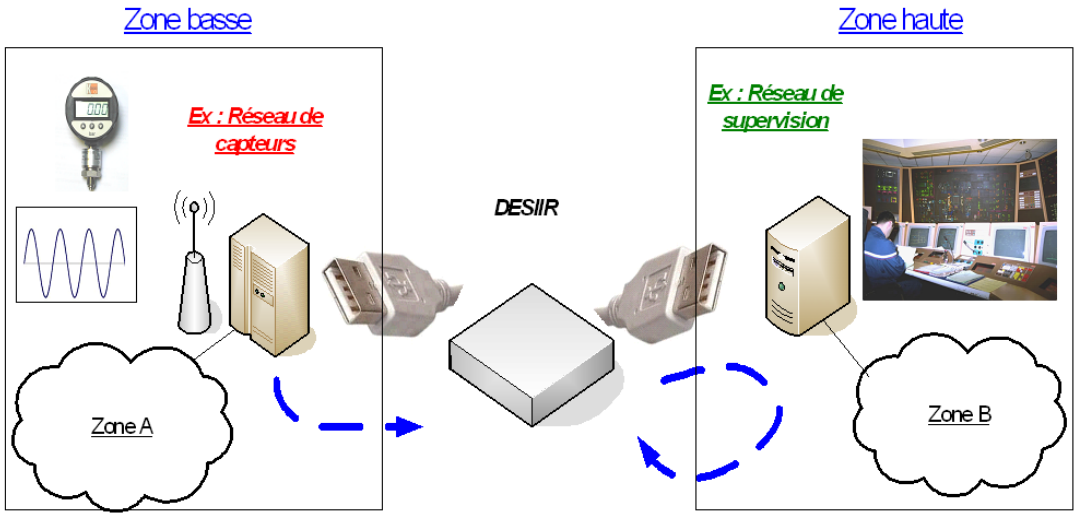


Figure 7. remontée d'information de réseau de capteurs

7.2 Fiabilisation des diodes physiques

Le principe ici est d'utiliser la diode physique pour la publication de gros volumes de données à une vitesse de transmission importante, tout en bénéficiant via DESIIR d'une information sur les données effectivement reçues côté B. On peut tout à fait restreindre le format accepté par DESIIR en n'autorisant qu'un certain type de message, correspondant par exemple à une indication des numéros de paquets d'information non reçus et en remontant régulièrement un message d'acquittement global.

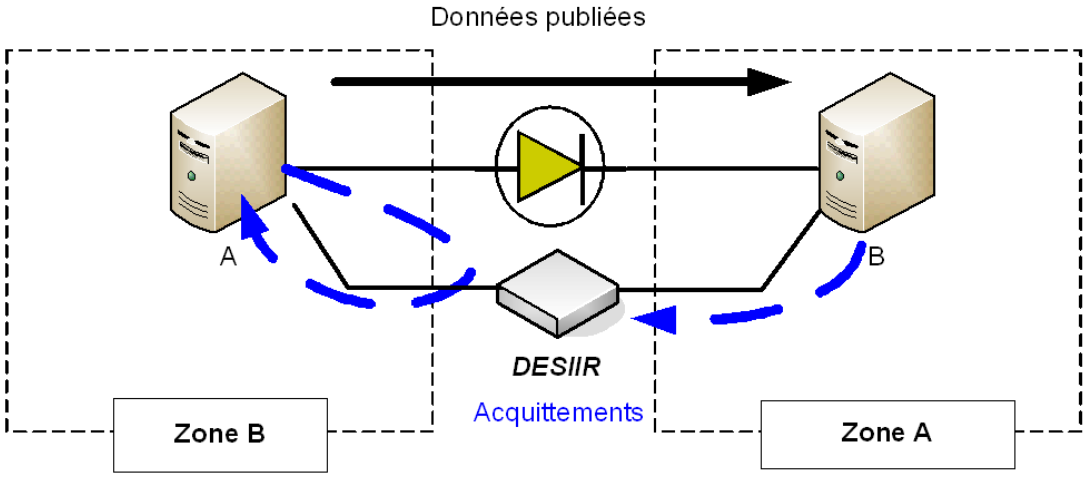


Figure 8. Utilisation combinée de diode physique et DESIIR

7.3 Autres cas d'usage possibles

Les applications vont au-delà des usages définis ci-dessus. En effet, si la solution a été conçue pour l'échange d'information sécurisé des réseaux sensibles industriels, elle est aussi utilisable avantageusement, par exemple dans les cas suivants :

- pour des applications de télémaintenance (récupération des états et journaux d'évènements, modification de configuration),
- pour des applications de publication d'informations pour la communication institutionnelle d'entreprise (publication d'images publicitaires sur des systèmes isolés dans des locaux publics, etc.).

Ce dispositif simplifie les architectures coupe-feux traditionnelles et permet un échange sécurisé d'information entre des réseaux non connectés.

8 Conclusions

EDF R&D a conçu, breveté et réalisé un dispositif coupe-feu qui permet de transmettre des informations entre deux systèmes de niveaux de confiance différents, y compris d'une zone moins sensible vers une zone plus sensible, tout en garantissant un très haut niveau de sécurité. Il devient possible, par exemple, de faire transiter une information d'un réseau de gestion vers un réseau industriel en conservant un haut niveau de sécurité du côté du process. Ce dispositif intègre différents concept de sécurité et cache leur complexité à l'utilisateur en adoptant un comportement naturel de type support de stockage. Il simplifie ainsi considérablement la mise en place d'architecture coupe-feu ou d'architecture de sécurité. En particulier, il répond aux besoins industriels pour lesquels actuellement aucune solution sur étagère n'est satisfaisante :

- Besoin d'un très haut niveau de sécurité, en garantissant que le niveau de protection reste maîtrisé même en cas de vulnérabilité logicielle ou d'erreur de configuration et en protégeant le système destinataire contre des attaques de contenu. En particulier, les fichiers mal formés, non conformes aux spécifications, les auto-exécutables et virus doivent être détectés et rendus inoffensifs.
- Besoin de fiabilité et de garantie de transfert. L'émetteur doit savoir si le transfert qu'il a initié a fonctionné.
- Besoin de confort, et utilisable pour des échanges réguliers basés sur une interaction applicative. Le dispositif fonctionne sur les systèmes différents avec le minimum d'impact (pas d'installation de logiciel supplémentaire) et est nativement interopérable avec ces systèmes (plug & play). Des connaissances basiques sont suffisantes pour installer et utiliser le dispositif. Le dispositif ne nécessite pas d'exploitation ni d'administration.

L'évaluation CSPN a mis en évidence la bonne conception de l'équipement utilisant une défense en profondeur. L'ensemble des fonctions de sécurité s'avèrent robustes et non contournables. Le boîtier permet une mise en place simplifiée rendant improbable une mauvaise utilisation. Une attaque a été trouvée mais ne remet pas en cause la cible de sécurité et est d'or et déjà corrigée dans sa version actuelle (version V1.1 devant être de nouveau évaluée). Ce dispositif permet une amélioration sensible de l'exploitation des processus industriels en toute sécurité en alliant simplification d'utilisation et pérennité du niveau de sécurité choisit. Une légère adaptation du dispositif permet également de filtrer les clefs USB permettant ainsi à ce dispositif d'éviter la propagation des virus par clef USB (CONFICKER , STUXNET). Ce dispositif peut également être intéressant pour des cas d'usage similaires pour d'autres opérateurs d'importance vitale. Plusieurs autres déclinaisons de ce dispositif peuvent également être pertinentes comme, par exemple, celles intégrant des mécanismes cryptographiques dans DESIIR qui permettraient d'authentifier, de signer ou de vérifier des signatures de fichier pour le transfert de fichiers binaires.

Références

[1] A Stateful Inspection of FireWall-1 , Thomas Lopatic, John McDonald TÜV data protect GmbH http://www.monkey.org/~dugsong/talks/blackhat.pdf

[2] Anatomy of an IP Fragmentation Vulnerability in Linux IPChains : Investigating Common Vulnerabilities and Exposures (CVE) Candidate Vulnerability CAN-1999-1018 http://www.sans.org/reading_room/whitepapers/threats/anatomy_of_an_ip_fragmentation_vulnerability_in_linux_ipchains_investigating_common_vulnerabilities_and_exposures_cve_candidate_vulnerability_can1_1110

[3] VLAN Security White Paper by CISCO http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml

[4] Researchers find large-scale XML library flaws, http://www.securecomputing.net.au/News/152193,researchers-find-largescale-xmllibrary-flaws.aspx

[5] An Analysis of Two New Directions in Control System Perimeter Security, Ludovic Pièrtre-Cambacédès, Pascal Sitbon, Scada Security Scientific Symposium (S4) 2009 http://digitalbond.com/s4papers/2009/edf/an-analysis-of-two-new-directions-in-control-system-perimeter-security/

[6] Certification ANSSI 2010/03 : http://www.ssi.gouv.fr/site_rubrique54_certificat_cspn_2010_03.html

[7] Cible de sécurité http://www.ssi.gouv.fr/IMG/cspn/anssi-cspn-cible_2010-03fr.pdf

[8] Enabling Secure Information Exchange from a less Secure Zone to a Control System Zone in a Critical Infrastructure, Pascal Sitbon, Arnaud Tarrago, Pierre Nguyen, Scada Security Scientific Symposium (S4) 2010

L'hypervision ou le Cyber C4ISR

Stanislas de Maupeou[1]

Thales Communications

Le livre blanc sur la défense et la sécurité nationale, la stratégie américaine ou celle de l'OTAN pour faire face aux attaques informatiques sont sans ambigüité : la dépendance des organisations avec leurs systèmes d'information et le choix de postures agressives de certains pays ou organisations, imposent de passer d'une défense passive à une défense active. Nous sommes là au cœur de la cyber-défense. Cependant, la défense active exige au risque de rester vaine, à la fois un lien vers les processus métiers pour le traitement des risques et une vue globale d'une situation de sécurité.

C'est l'objet de l'hypervision de délivrer de tels services afin d'effectuer un traitement dynamique du risque. Tout centre opérations (militaire ou civil) a besoin de cette vue globale d'aide à la décision apportée par les C4ISR (Command Control Communication Computer Intelligence Surveillance reconnaissance) ; l'hyperviseur apporte cette capacité C4ISR au centre opération de cyber défense.

***

L'idée principale est qu'il est préférable de gérer les prémices d'une attaque, voire de l'anticiper, plutôt que de ne réagir qu'à l'apparition des impacts. L'enjeu est donc de se doter d'une capacité de détection des attaques associée à des capacités d'analyse et de réaction.

Cette défense active, que le ministre adjoint du DoD décrivait comme un des cinq piliers de la cyberdéfense aux USA (Bruxelles septembre 2010), doit permettre d'une part de détecter les attaques de façon précoce, et d'autre part de traiter le risque sous un angle des métiers et non plus seulement sous l'angle technique (débordement d'une pile IP). En effet, la cyber-défense ne restera qu'un concept opérationnel limité aux seuls experts si nous ne parvenons pas à faire comprendre l'impact d'un fait technique sur un processus métiers.

La sécurité ne guide pas la conception et l'exploitation d'un système d'information, elle n'en est pas sa finalité. La finalité du SI est de délivrer un service au travers de processus métiers. La sécurité en revanche apporte un service. Dans ce contexte, la cyber-défense doit apporter une mesure du risque sur les processus métiers afin que les mesures de prévention et de réaction soient comprises et appliquées. L'expérience montre que c'est le contraire qui se passe...les RSSI passant une partie de leur temps à alerter sans être entendus. Les récents exemples de propagation de codes malveillants sont des exemples de cet autisme.

Ainsi la cyber-défense doit être vue comme une défense active par une surveillance permanente des activités réseaux et applicatives, mais elle doit aussi se comprendre dans la dimension métiers du risque.

Cette capacité de traitement de bout en bout du risque du fait technique (buffer overflow) jusqu'aux processus métiers impactés ne peut être aujourd'hui assurée par les outils existants. En effet, les outils de détection d'intrusion et les systèmes de collecte et de corrélation d'événements sécurité n'établissent pas le lien entre une analyse de risque du type EBIOS et des vulnérabilités techniques. Il est impératif pour un vrai traitement dynamique du risque de raisonner sur les impacts métiers.

D'autre part, la réaction à l'attaque s'effectue nécessairement dans un contexte de stress, inhérent à l'attaque. Il est donc indispensable d'apporter à l'opérateur tous les outils lui permettant une identification rapide des vrais enjeux de l'attaque, en lui permettant de se concentrer sur les enjeux de l'organisation, et par sur l'analyse technique de l'attaque.

L'hyperviseur, en prenant à sa charge le lien entre les conséquences techniques de l'attaque et ses impacts opérationnels, permet à l'opérateur de se concentrer sur les actions de riposte et/ou de protection des actifs de l'organisation. Il contribue ainsi directement à faire de la sécurité un apport à la sauvegarde du patrimoine, justifiant la pertinence de la mise en œuvre et de l'exploitation de ce type d'outil.

***

Par ailleurs, dans un monde largement interconnecté où la convergence vers l'IP prime sur tout à des fins d'interopérabilité et de coûts, la supervision de sécurité devient de plus en plus complexe. Comment assurer la délivrance en temps réel d'une situation de sécurité pour des systèmes à grande échelle, largement répartis, sachant que les sources d'informations sont hétérogènes ? L'expérience de Thales dans le monde des transports nous a amenés à développer des solutions d'hypervision permettant de délivrer des capacités de fusion d'informations hétérogènes.

L'hypervision est un solution permettant d'assurer une vue globale des risques à partir d'informations issues de sources variées, afin de fournir des éléments de décision et de réaction à un chef opérations. Cette solution, basée sur un *framework* d'échanges de données, ne modifie pas les applications sous-jacentes qui aliment l'hyperviseur via des connecteurs.

Par ailleurs, l'expérience montre qu'il est nécessaire d'adapter les situations de sécurité en fonction des besoins (vue technique d'architectures réseaux, vue des processus métiers, vue des risques, vue sous l'angle *log management*, etc.).

Dans ce contexte, nous proposons un démonstrateur d'une solution d'hypervision afin d'apporter à un chef opération des capacités de décision et de réaction

dans le cadre d'une attaque informatique. Cette solution est bâtie autour d'un framework, qui accueille les informations nécessaires qui sont collectées et fusionnées pour délivrer une alerte ou un événement. La solution s'adapte aux besoins des opérations.

***

L'hypervision apporte des capacités de traitement dynamique du risque en délivrant une vue globale d'une situation de sécurité, en appréciant l'impact d'une attaque sur les métiers et les organisations, et en proposant des meures de réaction appropriées. Il s'agit d'un outil d'aide à la décision face à des situations humainement et techniquement complexes du fait notamment du volume et de la nature des informations à traiter.

Troisième partie

United against Cybercrime

Annemarie Zielstra

Program Manager NICC, National Infrastructure against Cybercrime, ICTU, P.O. Box 84011, 2508 AA The Hague, The Netherlan annemarie.zielstra(@)ictu.nl

Résumé Tracking down and prosecuting cybercrime ? Extremely important but not the real solution for the problem. Prevention is better. That is why the NICC programme has brought public and private organizations together in the National Infrastructure against Cybercrime. The beating heart of this National Infrastructure is the Cybercrime Information Exchange. Within it, private and public organizations foght against cybercrime side by side."

Cyber défense : quelles « armes » ?

Stéphane Sciacco[1]

Orange Business Services, Direction de la Sécurité,9 rue du Chêne Germain 35510 Cesson-Sévigné
stéphane.sciacco(@)orange-ftgroup.com

Résumé Cet article décrit l'arsenal de mesure mis à la disposition d'un cyber-défenseur afin de contrer les cyber-attaques. Cette arsenal s'appuie sur un modèle de défense et sur une liste non exhaustive d'activités qui doivent assurer la suppression des points d'appuie d'une attaque.

Mots-clés: Analyse de risque, certification ISO 27001-2005, Security Opertions Center, CyberDefenseur, gouvernance, audit de sécurité

Avertissement: Le présent article reflète simplement l'opinion de leurs auteurs et ne représente pas une analyse ou des positions officielles d'Orange, France Telecom ou de l'une quelconque de ses filiales.

1 Introduction

Au jeu du chat et de la souris l'attaqué (notre malheureuse souris) peut elle échapper à l'attaquant (le malicieux chat) ? Quels « moyens de défense » notre souris peut elle mettre en oeuvre pour déjouer les plans machiavélique de notre gros matou ?

Cette courte image introduit le sujet de cet article à savoir quels sont « les moyens de défense » ou « arsenal de défense » à disposition d'un cyber-défenseur pour tenter de minimiser, détecter et éradiquer, les attaques en provenance d'un Cyber-attaquant/Cyber-Criminel.

1.1 Modèle de défense

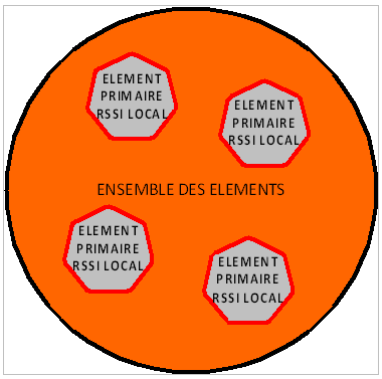
Avant de décrire l'ensemble de l'arsenal du Cyber-Défenseur et à partir du constat suivant : « il ne semble pas possible de protéger l'ensemble des biens d'une entreprise », il nous a paru important d'introduire une notion qui reviendra tout au long de cette exposé : « la posture de défense prioritaire ». Cette notion sera définie dans un modèle qui, à partir de l'ensemble des biens d'une société, fournit les « éléments primaires critiques et prioritaires » qui doivent obligatoirement protégés par notre Cyber-Défense.

Ce modèle sera axé autours de la sélection des « éléments primaires critiques et prioritaires » et de la désignation de responsable sécurité de ces composants équivalent d'un RSSI local. Au final la mise en place d'arme de Cyber-Défense aura pour but de réduire la surface d'attaque d'un « éléments primaires ». Nous

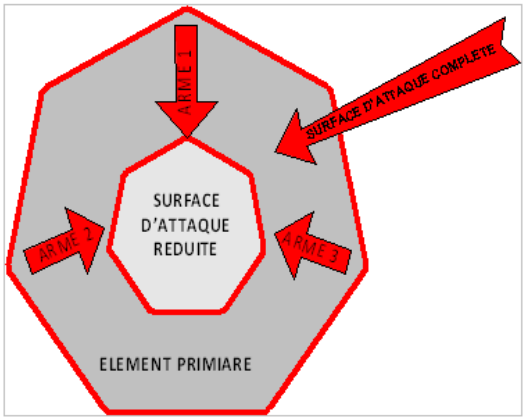
de décrivons pas en détail le modèle, en effet, le but de cette exposé est bien de présenter l'arsenal du Cyber-Défenseur et non la sélection des « éléments primaire » mais il nous paraît tout de même utile de lister ici quelques uns de ces critères :

- Application TOP-SOX
- Hébergement de donnés à caractère médicale ou bancaire
- Ensemble des portails clients
- Services business « critiques »
- Hébergement de donnés à caractère « étatique »

Le schéma ci-dessous fournit une description du modèle :



Le schéma ci-dessous fournit une description de la réduction de la surface d'attaque :

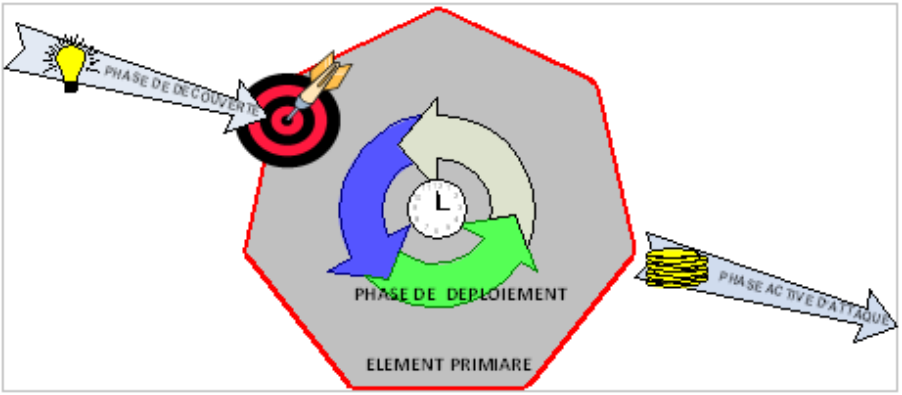


1.2 Modèle d'attaque

Une dernière notion à introduire avant la description de la « panoplie » du Cyber-défense (n'y voyez en rien une résurgence de ma petit enfance) le : « modèle d'attaque ». Ce modèle (il en existe bien d'autres) se décompose en trois temps fort qui sont :

- La phase de découverte : elle se définit par la prise de renseignement sur la cible à attaquer,
- La phase de déploiement/planification de l'attaque : c'est l'intrusion dans le système
- Enfin l'attaque à proprement parler : vol d'information, déni de service,...

Nous proposons par la suite des contre-mesures (l'arsenal de notre cuber-défenseur) en corrélation avec le modèle et qui tente d'éradiquer une à une les différentes phases du modèle d'attaque. Le schéma ci-dessous fournit une description du modèle.



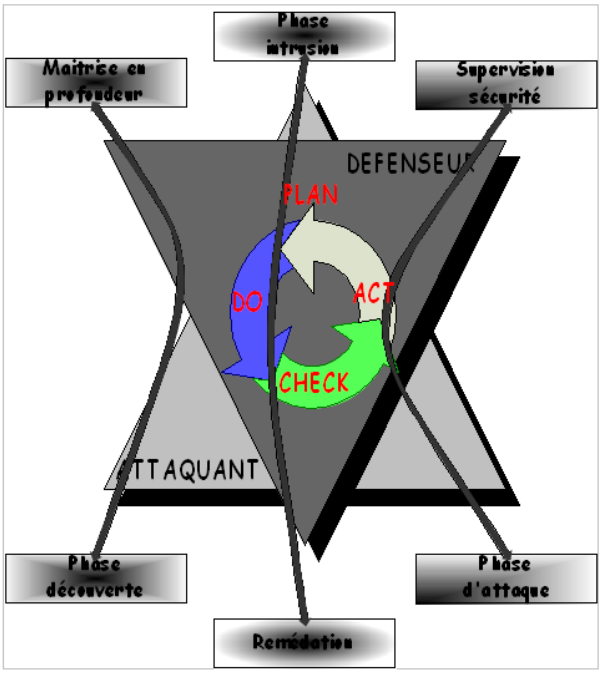
Sans avoir la prétention de décrire l'ensemble des contre-mesures qui peuvent exister la panoplie du Cyber-Défenseur proposée tente de contre balancer les 3 phases d'une attaque. Le lecteur aura donc une foultitude de moyen supplémentaire à rajouter dans cette panoplie.

Mais revenons à l'arsenal qui doit permettre de contenir les attaques sur les éléments critique à protéger. Cette panoplie sera composée de 4 grandes étapes ou « armes ».

1. La première étape une nommée « maitrise en profondeur » (analogie simpliste au célèbre et fameux concept de défense en profondeur) est constituée de :
   - L'analyse de risque.
   - L'audit organisationnel ou technique.
   - Cette étape doit permettre de réduire la phase de découverte du modèle d'attaque.
2. Vient ensuite une étape de déploiement d'un « service » de supervision de la sécurité. Ce service est une contre mesure possible à la phase active d'attaque.
3. La troisième étape décrit les méthodes de remédiation qui doivent être activées rapidement afin de pallier à la phase déploiement d'une attaque.
4. Enfin, nul n'étant sensée être omniscience la mise en place d'un processus de certification participera au processus d'amélioration continue de notre arsenal.

Cette action permet de garantir l'efficacité des contre-mesures proposées. Elle doit s'inscrire dans la durée, à l'inverse par exemple des audits qui sont par essence une photo prise à un instant T du niveau de sécurité (ou d'insécurité) d'une surface à protéger.

Le schéma ci-dessous résume le mapping entre l'arsenal du Cyber-Défenseur et le modèle d'attaque proposé.



2 Maitrise en profondeur

La première « arme », ou « batterie » dans ce cas précis d'arme, qui est à la disposition du Cyber-Défenseur sera appelée « la maîtrise en profondeur ». Cette arme tente de pallier à la phase de découverte du modèle d'attaque (prise de renseignent sur la cible à attaquer). Cette « batterie » est composée de 2 éléments primaire qui sont :

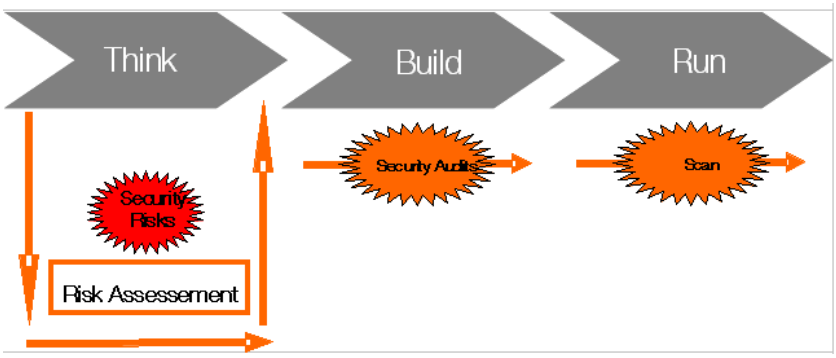
- L'analyse de risque,
- L'audit organisationnel ou technique.

2.1 L'analyse de risque

Abordons tout d'abord l'analyse de risque. Loin de dérouler l'intégralité de cette méthode, nous précisons juste la place et la portée qu'une analyse de risque devrait prendre dans l'arsenal fourni au Cyber-Défense.

Il nous paraît efficace de placer au tout début du processus de création d'un « éléments primaire » cette analyse de risque, par exemple lors d'une phase communément désignée « THINK ».

Nous indiquons dans le schéma ci-dessous la place d'une analyse de risque au sien du processus de création d'un service.



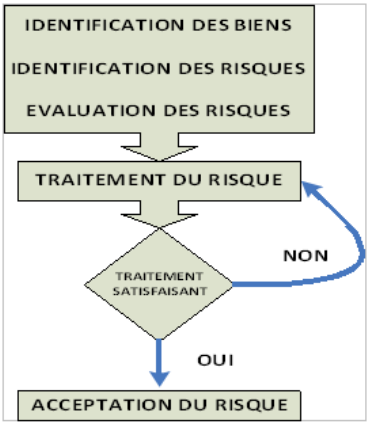
Parlons maintenant de la portée d'une analyse de risque. Dans notre cas elle doit permettre au Cyber-Défense de réduire la surface d'attaque. Attention réduire la surface d'attaque ne veut pas dire, la faire disparaître complètement. Il serait illusoire de croire que, suite à une analyse et à la prise en compte des mesures visant à réduire les risques, la totalité des attaques échoueront.

L'emploi de cette arme rencontre une difficulté tout de même. Même si nous avons réduit les éléments primaires, le coût, l'expertise requise et la complexité des méthodes d'analyse de risque peuvent parfois démotiver l'utilisation de cette arme par le Cyber-Défenseur.

Une solution pour contourner, par exemple la complexité, passe par la mise au point d'une méthode « light » (quelle soit EBIOS ou autre). Ces méthodes « light » prennent en compte au minimum les étapes suivantes :

- Identification du périmètre critique et des biens qui le composent,
- Identification des menaces/vulnérabilités qui pèsent sur les biens du périmètre,
- Critère « acceptance » des risques,
- Validation des risques et mise en place de mesures correctives.

Le schéma ci-dessous indique les phases minimum d'une analyse de risque « light ».



En conclusion, nous avons placé l'analyse de risque comme première « arme » disponible dans notre arsenal du Cyber-Défenseur puisqu'elle ce situe au tout début d'une réflexion sur les moyens de défense d'un élément primaire identifié comme critique.

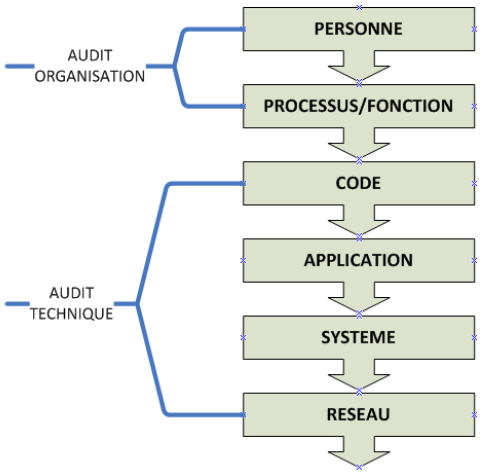
2.2 L'audit

Deuxième « sous arme » qui compose la phase « Maitrise en profondeur » l'audit. Qu'il soit technique ou organisationnel, l'audit à pour objectif de visualiser à un instant T, le niveau de sécurité ou d'insécurité d'un « élément primaire ». Cette visualisation doit impérativement déboucher sur d'un plan d'action de correction des failles identifiées (sinon notre audit n'a aucun intérêt et vous avez jeté de l'argent par la fenêtre). Mais faire corriger n'est pas toujours une chose aisée. Des contraires de charges, de ressources, de perturbations du service opérationnel... peuvent retarder la mise en place du plan d'action. Une phase de négociation peut être mise en place entre l'auditeur et l'audité pour étaler dans le temps le plan d'action par exemple, en fonction de priorités lié à la criticité des failles identifiées.

Mais il y a une limite aux audits. Nous avons précisé en effet, audit à un instant T et à l'instant T+1 que valent les résultats de cet audit ? Plus rien ou plus grand chose, sauf dans un monde idéal ou sur le « système » audité nous ne découvrons plus de vulnérabilités. Conduire des audits récurent à fréquence élevée sur un « élément primaire » nous semble illusoire. Pour tenter de pallier à cette impossibilité nous introduisons le concept, peut être simpliste, d'audit récurent sur un périmètre limité : la découverte de nouvelle vulnérabilité. Le périmètre étant réduit, il est aisé d'automatiser ces audits afin de maintenir en bonne condition opérationnel le système d'un point de vue sécurité. Cette action, peut être réalisée par une cellule « d'auditeur » via des outils spécifiques utilisés en mode fréquence haute (tout les mois par exemple). Cette équipe est en charge :

– De qualifier le résultat des tests (faux positif),
– D'établir et de suivre le plan d'action des corrections.

Ces tests de vulnérabilités ne devraient pas se limiter aux couches système ou applicatives, mais aussi, sur les codes développés. Le schéma ci-dessous indique les différents niveaux d'audit possible.



3 Supervision de la sécurité

3.1 Le Security Operations Center

Dans l'hypothèse probable ou malgré la phase de maîtrise en profondeur, il existe encore des trous de sécurité dans notre « éléments primaire » à sécuriser et suivant la phase de découverte, notre attaquant va tenter de s'introduire sur le système cible sans se faire détecter.

Lors d'une attaque par déni de service, la détection est « relativement simpliste » : « allo je n'arrive pas à me connecter sur le site alpha ». La remédiation l'est moins. Mais dans le cas d'une intrusion plus sophistiquée ou l'attaquant cherche une surface furtive maximale (je vol et je ne laisse aucune trace de mon effraction), comment le détecter ? Un moyen possible passe par la mise en place d'une structure de supervision de la sécurité un S(ecurity) O(peration) C(enter).

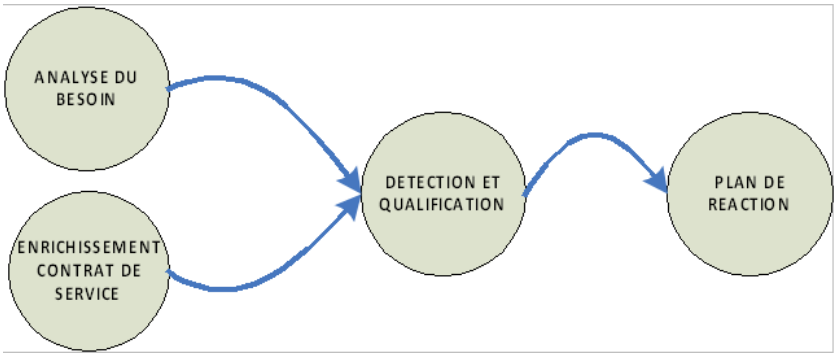
Mais que ce cache derrière cet anachronisme SOC. Dans notre contexte un SOC n'est pas une équipe :

– De « prise d'appel client »,
– Qui intervient en opérationnel sur des équipements de sécurité ou pas afin de modifier la configuration ou réaliser des mises à jour.

Le terme SOC définit ici l'équipe qui assure pour un « élément primaire » à protéger les fonctions suivantes :

– La prise en compte du besoin de supervision,
– La détection/qualification d'un événement de sécurité,
– La fourniture d'un plan de réaction.

Cette définition correspond au contexte présenté mais certain pourront confier d'autres fonctions de sécurité à cette équipe.



3.2 Le cahier des charges du SOC

Détaillons un peu plus maintenant, la manière de construire un service de supervision de la sécurité. Ce service est avant tout constitué d'une équipe d'ingénieurs sécurité (toutes compétences confondus système, réseau, codage, . . .) qui au travers de son expertise et à l'aide d'outil, assure la détection en temps réel des attaques sur le périmètre mis en supervision de sécurité. Il s'appuie sur des processus métier. Au final le SOC produit des alertes de sécurité et des tableaux de bord à destination des RSSI « locaux ».

Pour construire notre SOC nous avons indiqué qu'il s'appuyait sur des processus métier qui sont :

– L'expression du besoin de supervision de sécurité,
– Le déploiement de la solution de supervision de sécurité,
– La détection/qualification des événements de sécurité.

Le premier processus : l'expression de besoin de supervision de sécurité s'inscrit dans la démarche d'identification des « éléments primaires » critique à défendre. En effet, tous les services internes ou externes d'une entreprise ne peuvent être placés en supervision de sécurité. Il faut donc faire un choix en fonction de critères. Ces critères, sont regroupés dans le document d'expression du besoin (un cahier des charges) fourni par le demandeur de la mise en supervision de son « élément primaire ».

Ces critères peuvent être : Demande de supervision par le marketing, suite à la réponse d'appel d'offre d'un « éléments primaire »,

– Supervision de sécurité liée au respect de la réglementation,
– Approche de certification, incluant un contrôle de supervision de sécurité,

– Sensibilité des données nécessitant une supervision de sécurité.

Le demandeur doit aussi fournir des éléments techniques et organisationnels qui guideront les experts dans la mise en place de la solution technique. Ces éléments sont :

– La description technique du « service » à superviser (l'architecture),
– L'identification des barrières de sécurité déployées,
– La version des systèmes et des applications,
– contact HO/HNO en cas de détection,
– criticité des biens (application TOP SOX, annuaire d'entreprise...),
– cellule de crise à mettre en œuvre...

Sans ces informations le SOC est incapable de qualifier un événement de sécurité et d'identifier si oui ou non, la cible est impactée par le scénario d'attaque qui se déroule sous ses yeux. Les experts du SOC en fonction de toutes ces données pourront alors :

– Identifier les signatures de base à embarquer dans les IDS,
– Valider ou écrire des règles de corrélation (d'un simple agrégat à des scénarii en passant pas des modèles comportementaux).

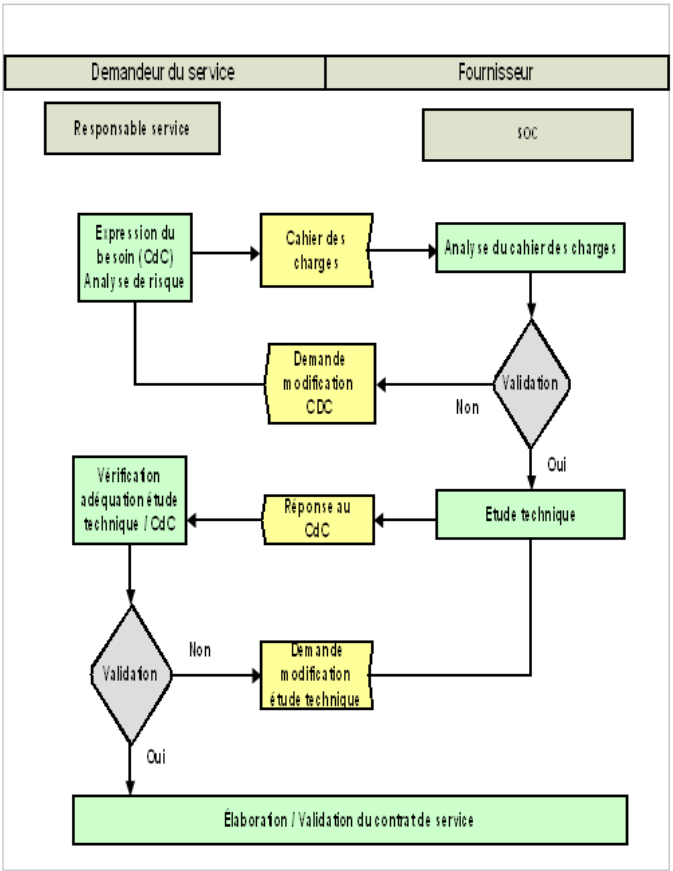
Enfin une étude approfondie des documents d'architecture de « l'élément primaire » permet une identification optimale de l'emplacement des capteurs.

Sans ces informations le SOC est incapable de qualifier un événement de sécurité et d'identifier si oui ou non, la cible est impactée par le scénario d'attaque qui se déroule sous ses yeux. Les experts du SOC en fonction de toutes ces données pourront alors :

– Identifier les signatures de base à embarquer dans les IDS,
– Valider ou écrire des règles de corrélation (d'un simple agrégat à des scénarii en passant pas des modèles comportementaux).

Enfin une étude approfondie des documents d'architecture de « l'élément primaire » permet une identification optimale de l'emplacement des capteurs.

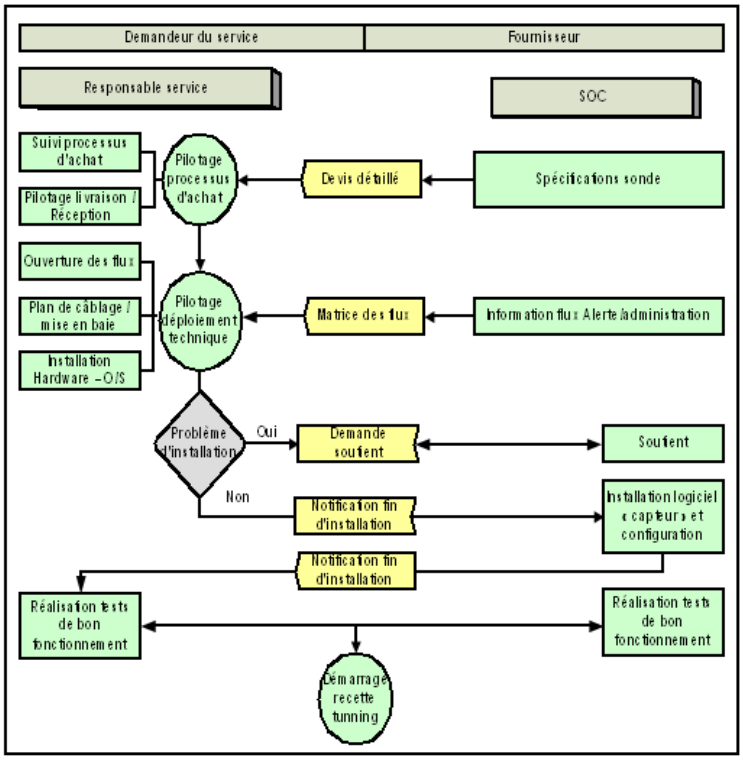
Le schéma suivant présente le processus expression du besoin



3.3 Le déploiement et le tuning du SOC

Vient ensuite le processus métier déploiement de la solution de supervision de sécurité. Ce processus est constitué par les phases d'achat, d'installation et de tuning des capteurs sécurité. Ces capteurs sont des IDS, des collecteurs de log, des sondes réseau...

Le schéma suivant présente le processus de déploiement.



Noter particulièrement la phase de tuning. Cette phase est à la fois la plus complexe et la plus importante de ce processus (installer une sonde Snort ne présente somme toute qu'un intérêt limité).

Lors de cette phase, les experts vont affiner les règles de sécurité embarquées dans les capteurs. Cette phase permet d'ajouter, de retirer, de récrire des règles installées sur les capteurs, afin de réduire les faux positifs. Elle permet aussi de tuner les règles de corrélation embarquées dans l'outil de supervision de sécurité. Certain fournisseurs embarquent de plus en plus des éléments additionnels permettant de faciliter cette action (proposition de jeux de règle suite à une analyse des « flux » à superviser).

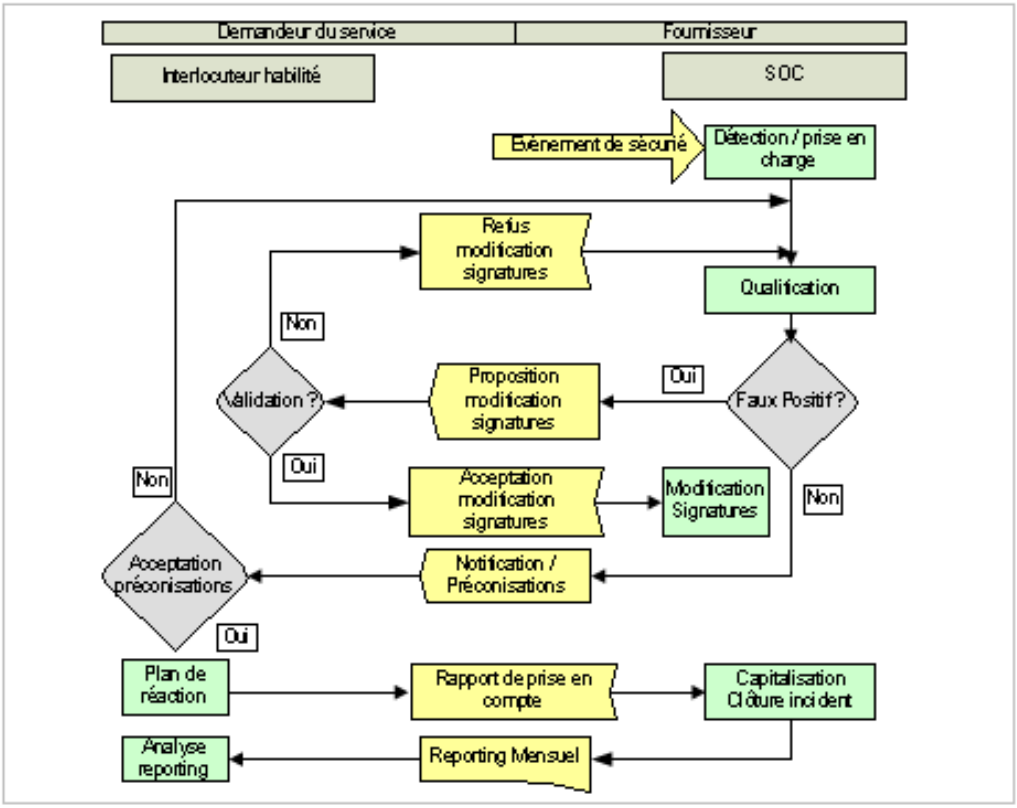
3.4 La détection des événements de sécurité

Dernier processus métier et non des moindres, la détection des événements de sécurité.

- Le processus ce décompose en 5 grandes phases qui sont :
- La prise en charge d'un événement sécurité,
- La qualification de l'événement,
- La notification et la préconisation,
- la mise en place du plan de réaction
- Le reporting.

La prise en charge d'un événement sécurité permet d'attribuer une priorité à un événement en fonction de la criticité de celui-ci. La qualification de l'événement et le processus qui garanti que l'attaque n'est pas un faux positif via le travail d'expertise des ingénieurs du SOC. La notification et la préconisation assurent la communication vers le propriétaire de « l'élément primaire » supervisé, de la détection d'une attaque et des recommandations pour la stopper. La phase de mise en place du plan de réaction à la charge du propriétaire de « l'élément primaire » est suivie par le SOC à des fins de support et de capitalisation.

Enfin, le SOC construit un reporting à destination du RSSI « local » pour qu'il puisse mesurer l'efficacité du service rendu.



3.5 Les outils du SOC

Nous avons abordé ce qui me semble le plus important à savoir, l'organisation du service de supervision de sécurité mais il faut tout de même parler un petit peu des outils utilisés par les experts du SOC. Il est évidemment recommandé de mettre en place un outil de type SIM/SIEM. Ce type d'outil assure :

- La fonction de console de supervision,
- Fournit des services de corrélation et d'enrichissement.

Le choix d'un SIM/SIEM est délicat. En effet, ces outils complexes et chers doivent être en adéquation avec les « éléments primaires » à mettre en supervision. La complexité de ces outils est introduite par les fonctions de corrélation (mais aussi la complexité d'installation et de paramétrage). L'écriture des règles de corrélation un est exercice de style particulièrement périlleux au résultat parfois critiquable.

Parlons rapidement aussi des capteurs de sécurité qu'il est possible de déployer. Quatre grands types peuvent être utilisés séparément ou ensemble, ce sont :

- Des IDS, IPS,
- Cleanpipe, Blackholing (nettoyage),
- Des collecteurs de log,
- Des honeypots (pots de miel),
- Des journaux d'événements.

Ces différents capteurs sont les « yeux » de l'expert sécurité. Ils lui remontent des événements de sécurité qu'il devra qualifier, en triant le bon grain de l'ivraie. Même si ces événements sont collectés puis corrélés par l'outil SIEM, l'expert reste le décideur final de l'activation ou pas, d'une véritable alerte sécurité.

Il faut noter que ces capteurs de sécurité nécessitent une expertise complexe au niveau du paramétrage des signatures embarquées. Ces capteurs doivent aussi impérativement être sous responsabilité de l'équipe SOC, en effet l'expert du SOC est incapable de qualifier une attaque s'il n'a pas la maîtrise complète des signatures implémentées dans les capteurs (qu'il soit IDS ou LOG).

Quelques remarque : concernant les IDS, l'introduction de solution de virtualisation dans nos architectures, nous obligent à revoir leur place, au sien des infrastructures. De même, des solutions d'enrichissement de l'information par analyse dynamique des flux améliorent les capacités de détection des IDS. Pour l'analyse de log, les solutions visualisation de la sécurité via des outils comme PICWIZ nous paraissent une approche à étudier, surtout lorsque un nombre important de log est à analyser. Côté détection des dénis de service, les solutions de détection par analyse comportemental (basée sur Netflow) des flux puis, de nettoyage (CleanPipe) complète la liste des « capteurs » disponibles pour le SOC.

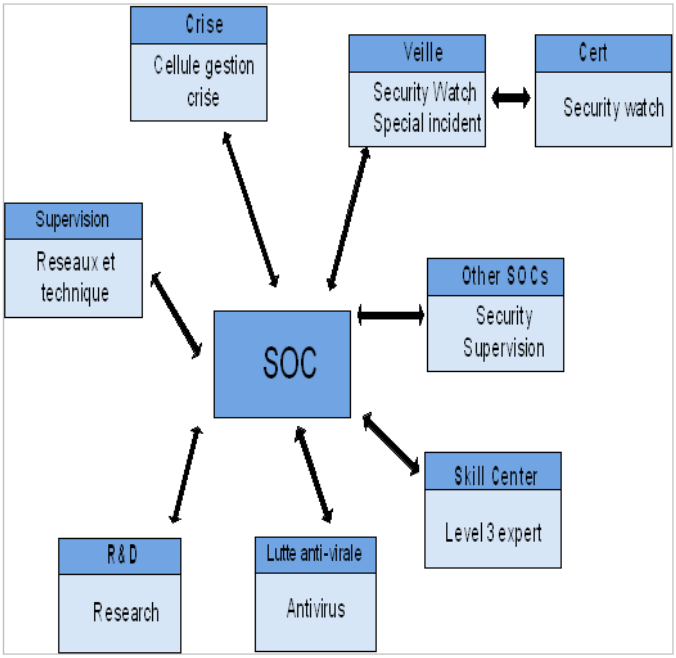
3.6 Les partenaires du SOC

Autre point à traiter, une équipe de supervision de sécurité ne doit pas vivre en autarcie. Elle doit s'interfacer avec d'autres cellules de sécurité voire d'autres SOC de (périmètres différents et complémentaires)

Nous ne décrivons pas ici les connexions multiples que le SOC doit avoir avec d'autres entités qui travaillent sur la sécurité ou pas. Une liste non exhaustive de connexion est proposée ci-dessous :

– L'équipe de veille,
– La cellule de lutte anti-virale,
– Les experts de niveau 3 (systèmes, réseaux, applications),
– La supervision technique (réseaux ou systèmes),
– La cellule sécurité R&D
– La cellule de gestion de crise

Le schéma suivant indique quelques liens externes :



4 « Remédiation »

La troisième arme à la disposition du Cyber-Défenseur et la remédiation. Loin de faire une liste à la Prévert des différents armes qu'ils seraient possible de déployer faisons un focus sur 4 d'entre eux :

– Patch management,
– Architecture de filtrage et d'authentification,
– Durcissement des OS et Applications,
– Campagne de sensibilisation

4.1 Patch management

« L'arme » patch Management est le moyen de remédiation en théorie le plus simple à mettre en oeuvre et pourtant il est souvent le moins utilisé. Logiquement faire les mises à jour de « sécurité », devraient faire partie du processus « release »

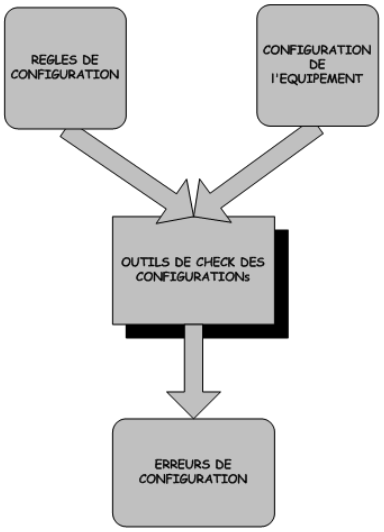
classique d'un « élément primaire », et être de facto inclus dans le processus métier des équipes d'ingénierie qui suivent de bout en bout le cycle de vie de celui-ci. De plus, cette tâche ne consomme pas des ressources importantes et devrait donc être utilisée systématiquement. Cette arme peux utilisée laisse donc au Cyber-attaquant une porte grande ouverte sur « l'élément primaire » attaquer. Mauvaise communication sur la portée cette arme, désamours coté ingénierie qui la considéré comme ayant peu de valeur ajouté « intellectuelle ».

4.2 Architecture de filtrage et d'authentification

Probablement l'arme la plus utilisée/déployée. La multiplication des barrières de défense qui reposent sur cet unique moyen en apportent la preuve. Ainsi, on ne compte plus les niveaux de filtrage déployés au sein d'un « éléments primaire ». Nous n'allons donc pas décrire une énième fois en détail une architecture de filtrage classique, mais une fois n'est pas coutume, émettre une petite critique sur l'utilisation qui pourrait paraître comme outrancière pour certains décideurs. Non sans vouloir prôner l'éradication des architectures de filtrage, une rationalisation de ce type d'arme semble opportune. Cet empilement de filtrages pourrait être mieux rationalisé si une vision globale des architectures était disponible via par exemple une cartographie complète des barrières de filtrage. Un autre moyen, peut être plus réaliste : le choix de déploiement d'un filtrage assujetti à une analyse de risque de l'environnement d'évolution technique de « l'élément primaire » à protéger. Bref un filtrage de sécurité adapté aux enjeux sans sur-consommation.

4.3 Durcissement des OS et applications

La notion de durcissement bien connu (en informatique mais hérité de l'électronique est une arme bien documentée et largement utilisée. Des guides fournis par le NSA pour les équipements CISCO par exemple au « hardering book », la liste des documents qui permettent de durcir tel ou tel système est pléthorique sur Internet. Un peu moins connu et déployé sont les outils qui contrôlent que les règles de « hardering » sont toujours activées sur l'équipement. Ces outils prennent en entrée les règles de durcissement liées au contexte et les configurations des équipements. L'outil compare les différences entre la réalité de la configuration et ces règles. En sortie l'indication des erreurs de configuration et fournit.



4.4 Campagne de sensibilisation

Même si certain pense que les actions de sensibilisation à la sécurité sont une mauvaise idée, il serait dommage de ne pas utiliser cette arme dans notre panoplie. Quelle soit véhiculée par des campagnes d'affichage, du push mail, des sessions de formation voire maintenant des serious games, la sensibilisation est l'élément qui permet d'interpeler à un moment ou un autre l'ensemble du personnel.

5 Certification

Dernière arme, dans le dispositif du Cyber-Défenseur la « certification ». Plus qu'un bouclier, nous prenons la certification comme un outil de validation par un tiers externe de l'efficacité et de l'amélioration continue de toute ou partie des axes « Maitrise en profondeur », « Supervision de sécurité » et « remédiation ». De façon rapide :

- Ces certifications (issues de normes) doivent démontrer « le niveau de sécurité » d' un « élément primaire » donnée (« cible de sécurité »).
- Elles assurent logiquement l'établissement de bonnes pratiques en matière de sécurité sur la cible de certification.
- Enfin, elles permettent d'augmenter le niveau de confiance que peu avoir un client (interne/externe) vis à vis de l'élément primaire certifié (pour peu que l'audit de certification soit rigoureusement conduit).

Nous ne faisons pas ici un catalogue des certifications de sécurité existantes. Nous nous contenterons à partir d'une certification bien précise (certification ISO 27001-2005) de détailler les phases que doit conduire le Cyber-Défenseur pour implémenter celle ci.

Pour commencer la certification de type ISO 27001-2005 et basée sur le célèbre modèle Plan Do, Check et Act issu des normes de qualité. Ce modèle est inclus dans la norme ISO 27001-2005 qui décrit toute les étapes à prendre en compte pour sécuriser un « élément primaire » : de la définition de celui-ci à la planification des campagnes de sensibilisation en passant par l'analyse de risque. Les étapes nécessaires cette certification sont :

- La définition de « éléments primaire » appelé périmètre en ISO 27001
- La rédaction du document de politique du SMSI
- L'analyse de risque sur le périmètre
- L'établissement du Statement of Applicability
- Quelques étapes supplémentaires

Chaque étape sera rapidement détaillée par la suite. Le lecteur averti pourra passer directement à la section qui décrit « les difficultés d'implémentation d'une telle certification ».

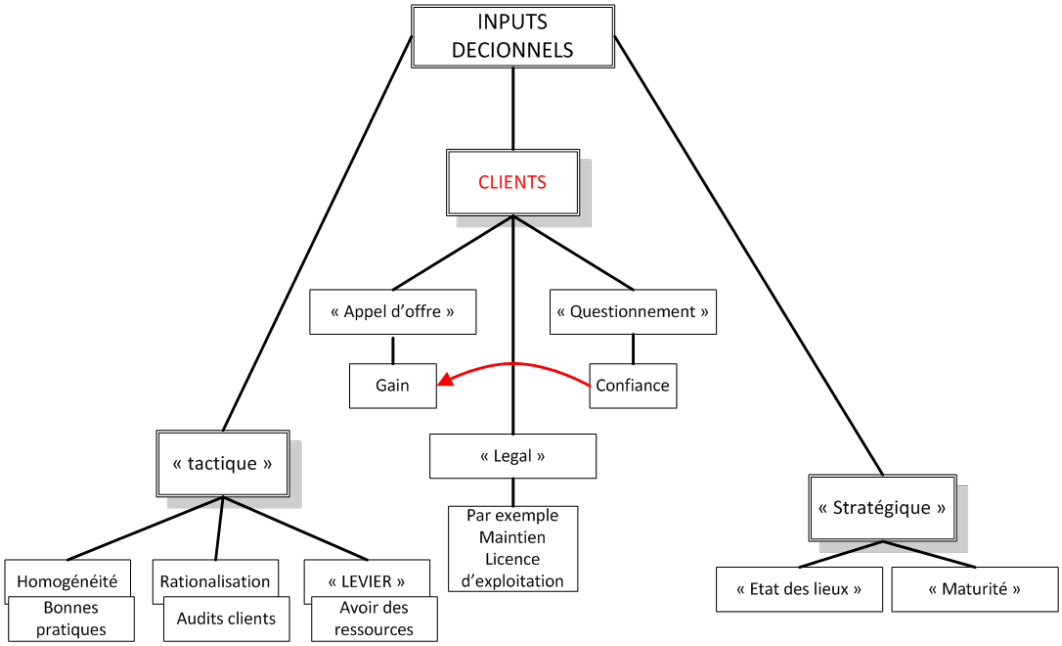
Première étape à effectuer : la définition du périmètre qui doit être certifié. Ce périmètre peut être :

- Un Data center,
- Des plates-formes critiques,
- Un service sécurité ou pas...

Une fois le périmètre fixé, les limites du périmètre doivent être justifiées. Les exclusions peuvent être, les personnes, les bâtiments, les services... qui ne participent pas à la création, mise à jour, administration des composants de la cible. Le périmètre devra être ensuite validé au niveau du top management afin de garantir l'adhésion de tous dans cette démarche.

Attention à des périmètres trop grands (difficultés pour rassembler toutes les preuves) ou trop petit (pas de pertinence des clients par exemple). Il n'existe pas de recette miracle, juste une piste simpliste : pour une certification externe, regarder quel est le périmètre le plus représentatif des besoins sécurité des parties prenantes externes (par exemple questions sécurité régulières sur la sécurité posées par les clients sur un ou des services) Il faut aussi identifier le besoin de réalisation de ce type de certification.

Le schéma ci-dessous indique quelques éléments de décision pour lancer une certification.



Vient ensuite l'écriture d'une politique du système de management à certifier. Un document court, qui indique entre autre les engagements de la direction à fournir les ressources. Ce document doit impérativement contenir les choix suivant :

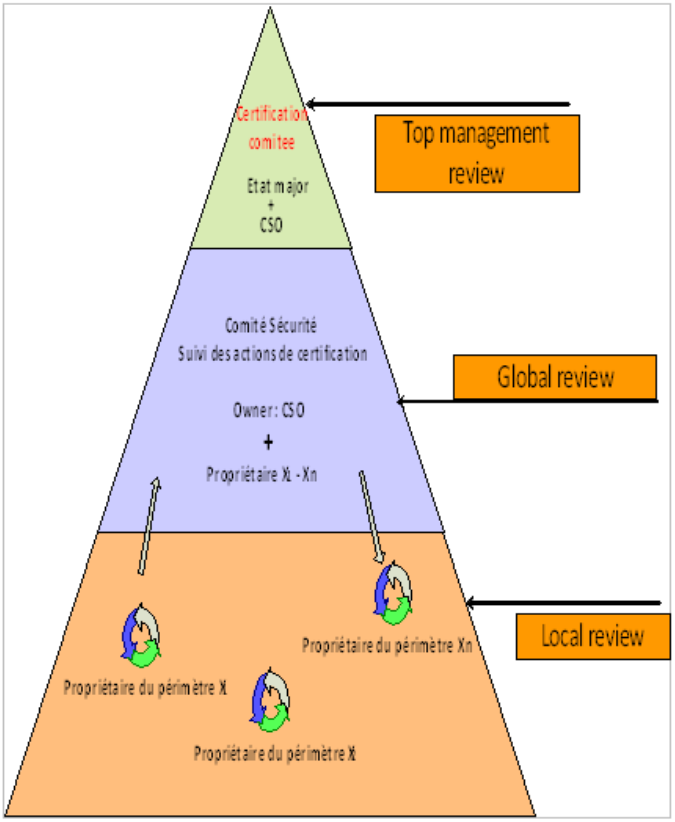
- Le modèle de gouvernance,
- La méthode d'analyse de risque,
- Les éléments de stratégie d'audit et de sensibilisation,
- Les indicateurs de suivi du système de management.

Nous allons commencer par détailler le modèle de gouvernance. Ce modèle doit contenir l'ensemble des niveaux décisionnels nécessaires à la mise en place, puis à l'amélioration du Système de Management. Ces instances décisionnelles se réunissent à des fréquences qui sont en adéquation avec le niveau hiérarchique des personnes qui constituent l'instance.

Enfin pour être efficace chaque instance doit être alimentée par des entrées et fournir en retour des sorties. Les entrées peuvent être les résultats :

- Les audits techniques ou organisationnels,
- Les campagnes de sensibilisation,
- Les retours d'enquêtes clients.
- Les sorties peuvent être :
- l'ajout d'un « élément primaire » à certifier,
- La mise en place ou le suivi des plans d'actions suite aux audits,
- La prise en compte des résultats d'enquêtes de satisfaction externe/interne,
- La mise en place de campagnes de sensibilisation...

Le schéma ci-dessous fournit une vue sur le modèle de gouvernance :



L'étape suivante est la conduite d'une analyse de risque sur le périmètre. Cette phase comporte :

- La définition de l'ensemble des grilles utiles à l'évaluation des risques,
- L'identification des biens sensibles et des propriétaires,
- Les menaces et vulnérabilités qui pèsent sur ces biens.

Une fois l'ensemble des risques identifiés et typés (faible, modéré, élevé, critique) il nous reste à mettre en place et faire valider par le top management les plans d'action nécessaires à la « réduction » des risques.

En parallèle il est possible d'établir la phase de sélection des mesures de sécurité qui sont déployées sur le périmètre. Le maintenant célèbre Statement Of Applicability comporte 133 points de contrôle. Chaque mesure sélectionnée doit faire l'objet de fournitures de preuves (politique, tableau de bord, audit, enregistrement...). Toutes les mesures non sélectionnées doivent aussi être justifiées. L'auditeur contrôlera à la fois, la pertinence du choix des contrôles et la véracité des preuves fournies pour chaque contrôle.

Les actions d'audits internes ou techniques, de campagnes de sensibilisation, de gestion des incidents... serviront à alimenter les instances décisionnelles afin quelles prennent les mesures nécessaires pour améliorer la sécurité du périmètre à certifier.

Au final, l'audit de certification conduit par un organisme externe, certifiera ou pas le système de management proposé. A noter aussi que l'ISO 27001-2005 s'inscrit dans la durée. Des audits de surveillance puis un audit de renouvellement seront réalisés tout au long de la vie du périmètre certifié.

Nous indiquons pour conclure quelques obstacles à la mise en place d'une certification de type ISO 27001-2005.

La première difficulté rencontrée est tout simplement la norme ISO 27001-2005 elle même. C'est une phase d'appropriation/décryptage de la norme qui sans être nécessairement longue demande un certain niveau de compréhension.

Le deuxième obstacle est le choix du périmètre. Un périmètre trop grand sera difficile à certifier, un périmètre trop petit n'aura pas d'intérêt. Le choix du périmètre dépendra de l'objectif visé, certification business (demande des clients), réglementaire (certain pays demande ce type de certification pour opérer sur leur territoire)

Une difficulté liée au Statement Of Applicability car la sélection des contrôles peut être un exercice périlleux. Le décryptage des termes employés pour décrire la mesure de sécurité à mettre en place est quelques fois soumis à des interprétations variées de la part de l'implémenteur. De même trouver l'ensemble des preuves qui assurent qu'une mesure est bien implémentée peut se révéler difficile.

Enfin, une certification ISO 27001-2005 n'est pas figée dans le temps. Un audit initial puis des audits de contrôle et enfin un audit de renouvellement (et on recommence pour un tour) sont inscrits dans le schéma de certification. Il faut réussir à maintenir et faire évoluer dans le temps l'ensemble des éléments obligatoires à la mise en place du système de management certifié.

6 Gouvernance du modèle

Un point hors panoplie reste à traiter et non des moindres : gouvernance de cette arsenal. Sans une instance de coordination, les armes mises à la disposition du Cyber-Défense agissent de manière automne sans possibilité de liaison interarmes ce qui diminue l'efficacité de l'arsenal déployé.

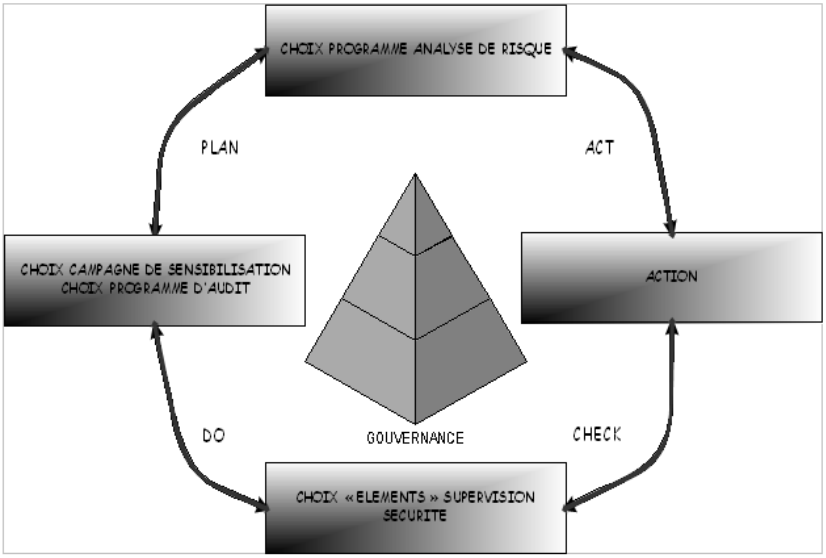
Une réponse possible à cette difficulté est la mise en place d'une cellule que nous appellerons « Direction de la Sécurité ». Équivalent des contrôleurs aériens, cette entité aura pour rôle de coordonner/guider l'ensemble des moyens mis à la disposition du Cyber-Défenseur.

De manière succincte cette direction au regard d'objectifs spécifiques (stratégique) assure une coordination entre toutes les armes décrie précédemment. Attention en aucun cas cette entité ne joue un rôle opérationnel.

De plus un processus de veille doit impérativement faire partie de ces activités. Quelle soit technique, organisationnelle, normative, juridique ou concurrentielle le résultat de cette veille doit alimenter les actions stratégiques de cette équipe.

Enfin, il est possible à partir de la célèbre boucle PDCA de construire un modèle, qui définit l'ensemble des actions coordonnées par cette entité.

Le schéma ci dessous décrit ce modèle.



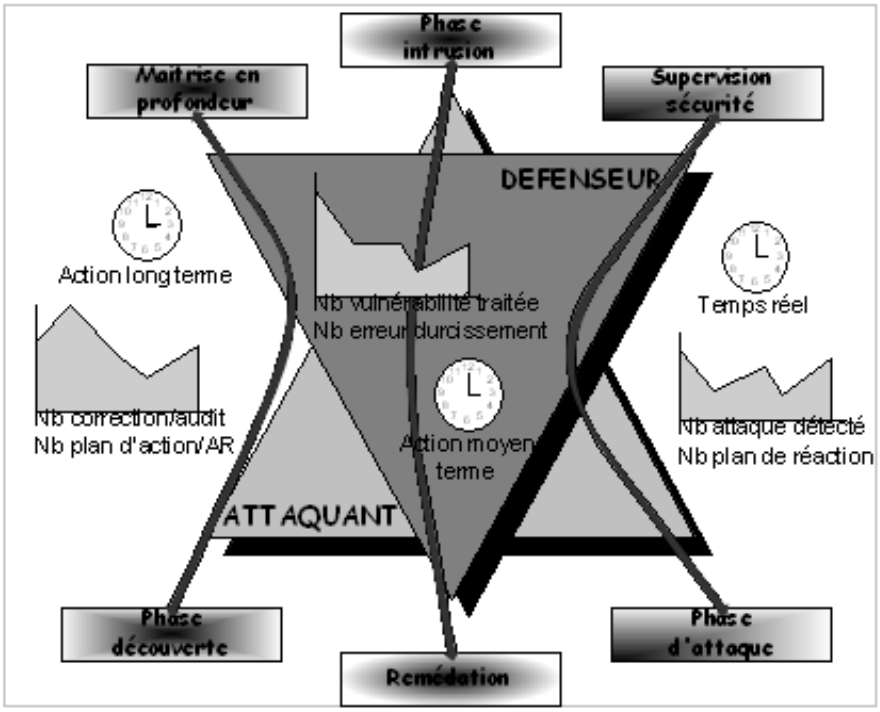
7 Conclusion

Nous avons décrit dans le présent article les quatre armes mis à la disposition du Cyber-Défense pour rappel sont : La maitrise en profondeur : propose la mise en place d'audits, l'engagement d'actions correctives et le déploiement d'un processus d'analyse de risque sur les « éléments primaires ».

- La supervision de sécurité prévoit :
- L'identification du besoin de supervision de sécurité, le déploiement du projet de supervision et enfin la détection/qualification des événements de sécurité.

Le remédiation est essentiellement axée sur le durcissement des « éléments primaires ». La certification prend toute sa place dans la panoplie du Cyber-Défenseur en jouant le rôle de super contrôleur des actions précédemment décrites. Nous pourrions aussi rajouter comme arme la mise en place d'outils qui englobent des aspects techniques et organisationnels comme une PKI ou un processus de type IAM. Cela renforce notre propos sur le fait, que la liste des armes du Cyber-Défenseur proposée n'est nullement exhaustive bien au contraire. Comme l'imagination des attaquants est sans limite, il serait absurde de limiter l'arsenal du Cyber-Défenseur. Il serait même suicidaire d'être dogmatique et d'imposer une liste restreinte des contre-mesures. Enfin, un point important dans le dispositif de Cyber-Défenseur reste la gouvernance des actions de sécurité déployées sur les

« éléments primaires » assurée par une « Direction de la Sécurité » sorte de tour de contrôle. Pour finir un schéma qui introduit les notions de temps/indicateurs sur le modèle d'attaque/défense.



Démarche OIV Télécom - Retour d'Expérience (RETEX)

Stéphane Lemerle[1], Pierre-Dominique Lansard[2]

[1] Orange Business Services, 9 rue du Chêne Germain 35 512 Cesson-Sévigné
stephane.lemerle(@)orange-ftgroup.com
[2] France Télécom Orange, 6 place d'Alleray 75505 Paris cedex 15
pierredominique1.lansard(@)orange-ftgroup.com

Résumé Dans le cadre du décret N° 2006-212 du 23/03/2006, certains opérateurs ont été associés à l'effort de vigilance, de prévention et de protection afin de faciliter l'application de plans gouvernementaux contre le terrorisme. Comment cette nouvelle démarche de « sécurité globale » pourrait être mise en place chez un opérateur de télécom comme France Télécom, selon quel protocole de dialogue régulier avec les autorités ? Quelles implications contractuelles ? Premier bilan d'étape « pratique » pour aider à redéfinir les enjeux de la cyberdéfense

Mots-clés: systèmes d'importance vitale - Opérateur d'Importance Vital (OIV) - Directive Nationale de Sécurité (DNS) - Plan Particulier de Protection (PPP) -

Avertissement: le présent article reflète simplement l'opinion de leurs auteurs et ne représente pas une analyse ou des positions officielles d'Orange, France Telecom ou de l'une quelconque de ses filiales.

La démarche SAIV (Secteur d'Activité d'Importance Vitale) a permis à l'Etat de déterminer par secteur, les Opérateurs d'Importance Vital (OIV) et de leur notifier leur statut. Par secteur (ou sous-secteur) l'Etat a bâtit une Directive Nationale de Sécurité (DNS) qu'il a communiquée à chaque OIV.

L'OIV ainsi désigné a deux ans pour se conformer à cette DNS. Il appartient à l'opérateur d'importance vitale de prendre les dispositions nécessaires vis-à-vis de son sous-traitant ou de son fournisseur, notamment dans les spécifications du contrat les liant, pour que celui-ci concourt à la réalisation des objectifs de sécurité de l'opérateur [3]

Le nouveau dispositif de sécurité des activités d'importance vitale constitue le cadre permettant d'associer les opérateurs, publics et privés, au système national de protection contre le terrorisme, d'analyser les risques et d'appliquer les mesures de leur niveau en cohérence avec les décisions des pouvoirs publics. Il vise à améliorer l'articulation des dispositifs que mettent en œuvre les pouvoirs publics et les opérateurs en particulier dans le cadre du plan VIGIPIRATE.

3. INSTRUCTION GENERALE INTERMINISTERIELLE RELATIVE A LA SECURITE DES ACTIVITES D'IMPORTANCE VITALE N° 6600/SGDN/PSE/PPS du 26 septembre 2008 : http://www.circulaires.gouv.fr/pdf/2009/04/cir_1338.pdf

Le statut d'Opérateur d'Importance Vitale (OIV) repose donc en France sur deux conditions :

- que son activité s'exerce en tout ou en partie dans un secteur d'activité d'importance vitale, cette démarche dite « Secteurs d'Activité d'Importance Vitale » est orchestrée par le SGDSN (Service du Premier Ministre). Elle est régie par un décret du 23 Février 2006. Ce décret a été incorporé au Code de la Défense en 2008. Il y a 12 secteurs en France couvrant l'ensemble des activités.
- qu'il génère ou utilise au moins un établissement, un ouvrage ou une installation dont le dommage, l'indisponibilité ou la destruction risquerait de quelque manière que ce soit d'avoir des conséquences majeures sur les capacités de la Nation ou sur la santé de la population.

Il ne s'agit pas forcément « d'infrastructures » à proprement parler mais cela peut être un équipement, ou un processus, voire même un groupe humain.

Dans ce contexte France Télécom Orange a défini les notions suivantes afin d'éviter toute confusion. Premièrement : un équipement, un processus, une fonction est critique s'il est essentiel ou vital. Deuxièmement : un équipement, un processus, une fonction est essentiel si il est impliqué dans plan de continuité d'activité (PCA) retenu par l'entreprise. Troisième net : un équipement, un processus, une fonction est vital s'il est impliqué dans une démarche de demandes des autorités nationales. Ainsi un équipement, un processus, une fonction peut être à la fois essentiel et vital pour un opérateur.

France Télécom Orange a tout d'abord traduit la DNS en un Plan de Sécurité Opérateur (PSO) puis proposé une liste de Points d'Importance Vitale (PIV) que l'Etat a accepté. Pour chaque PIV accepté, France Télécom Orange doit mettre au point un Plan Particulier de Protection (PPP) et à chaque PPP l'Etat répondra par un Plan de Protection Extérieur (PPE). Ainsi la sécurité résulté d'une collaboration entre l'acteur économique et l'Etat.

France Telecom Orange a d'abord mis en place un groupe de travail pour analyser le contenu de la DNS en insistant surtout sur les menaces à retenir et les « valeurs d'impact » (ex : nombre de clients impactés par la destruction de tel ou tel type de centre et existence d'un backup)

Puis nous avons mis en place un groupe projet pour passer en revue nos différents services afin de déterminer les entités qui pourraient être retenues comme PIV proposés. Pour chacun de ces points nous avons fait une analyse de risque de type EBIOS et nous avons pu ainsi les retenir ou non.

De nombreux échanges ont été nécessaires avec le HFDS (Haut Fonctionnaire de Défense et de Sécurité) de notre Ministère de référence pour expliquer nos choix et les justifier à l'aide notamment de présentations détaillées du fonctionnement de nos réseaux supports et de nos services.

En parallèle de la conception de notre PSO, nous avons commencé à mettre au point un PPP générique commun à l'ensemble de nos PIV. Notre HFDS a de son côté mis au point un PPP standard sur lequel nous avons fait des commentaires.

Exemples de quelques questions posées ?

- Quels sont les niveaux de robustesse de mes équipements ?
- Quel est le niveau de résilience de ma solution ?
- Quelles menaces me demande-t-on de prendre en compte ?
- Quelle est la stratégie de mon client (interne ou externe) ?
- Quelle est ma politique de Backup ?

Ensuite, nous avons demandé une réunion de l'ensemble des OIV du sous-secteur pour harmoniser nos PPP.

Finalement nous avons décliné la version générique harmonisée du PPP à l'ensemble de nos PIV et nous avons planifié de présenter les PPP ainsi réalisés au Préfet de chaque département concerné. Nous sommes actuellement dans l'attente des PPE miroir.

Les difficultés rencontrées ont été :

- une connotation très orientée terrorisme de la DNS
- l'impossibilité d'une concertation, avant l'écriture du PSO avec les autres OIV du sous-secteur
- des délais assez longs (plus de 8 mois) pour l'acceptation de notre PSO par le HFDS, et une procédure de mise à jour de la liste des PIV assez peu détaillé qui peu introduire des délais supplémentaires
- bien faire apparaître pour l'Etat la séparation à établir entre ce qui est du domaine SAIV pour un opérateur et ce qui du domaine contractuel
- l'absence d'un niveau standard uniformisé de PPP pour les PIV et de référentiel de sécurité associé
- l'absence de réglementation sur ce qui peut être construit près d'un PIV (exemple : « zone de sécurité » pour les sites SEVESO)

Les impacts sur les fournisseurs sont aujourd'hui difficilement quantifiable, mais si il y a environ une dizaine d'OIV pour les 12 secteurs nous pouvons en déduire un total d'au moins 200 OIV, chaque OIV transmet à ses fournisseurs ses obligations en matière de degré de résilience à satisfaire, et ainsi de suite Ĕ c'est donc, dans les deux ans, de très nombreuses entreprises qui seront impactées, et tout particulièrement les sociétés utilisant beaucoup d'informatique puisque les SCADA (System for Control And Data Acquisition) sont au centre du dispositif.

Pour que cette démarche SAIV puisse jouer pleinement son rôle, à savoir :

- faciliter l'application du plan VIGIPIRATE
- associer pleinement les opérateurs à l'effort de vigilance, de prévention et de protection
- sélectionner rigoureusement les points devant faire l'objet d'une protection efficace adaptée au niveau de la menace

L'organisation d'un dialogue constant doit s'instaurer entre l'OIV et les préfectures, ce dialogue devra se ponctuer d'audit des sites et surtout d'exercices communs sur les différents PIV (au niveau local plans « VIGIPIRATE » zonaux et départementaux, et au niveau gouvernemental les plans « PIRATE ») En outre, il nous apparaît nécessaire qu'une pédagogie ciblée puisse accompagner les OIV, et les délégués pour la défense et la sécurité pour les aider dans la retranscription des exigences de sécurité (issues des Analyses de Risque) dans les contrats avec leurs sous-traitants ou leurs fournisseurs.

Prospectives des doctrines françaises en matière de cyberdéfense

Par l'Association Nationale des Auditeurs Jeunes de l'Institut des Hautes Etudes de Défense Nationale

Arnaud Guarrigues[1] Emeric Laroche[2] Raphael Marichez[2]

[1] Orange
[2] Hervé Schauer Consultants - HSC

Résumé bien que la cyberdéfense française soit mentionnée par plusieurs textes officiels (Livre Blanc, avis et rapports parlementaires...), il n'existe pas de doctrine établie, c'est-à-dire d'ensemble cohérent décrivant en globalité la stratégie de cyberdéfense en France. Avec une approche très concrète, les auteurs, auditeurs jeunes de l'IHEDN, proposent d'abord, par une synthèse des organisations de cyberdéfense en France et à l'étranger, de rappeler les éléments de doctrine déjà présents mais disséminés. Des pistes alternatives d'améliorations à court-terme sont proposées, en se plaçant dans le domaine de la défense nationale : militaire, civile, économique. Cet exposé visite différents thèmes : économiques (innovation, normalisation et oligopoles), sociaux (subversion, multiplication des identités), militaires (emploi offensif de l'informatique), régaliens (régulation des réseaux, infrastructures vitales), et bien sur légaux (limitation des armes informatiques, autorités de régulation).

Quatre axes sont retenus en conclusion, concernant, successivement : le frein lié au secret dans la SSI des activités d'importance vitale ; l'adhésion nécessaire de la société civile pour une cyberdéfense globale ; le manque de présence française en normalisation et régulation internationale ; enfin l'élargissement des objectifs d'emploi de la cyberdéfense à la stratégie diplomatique et la défense globale, dépassant le secteur de l'informatique.

Introduction

L'émergence d'une stratégie française de cyberdéfense est plus ancienne que le Livre Blanc sur la Défense et la Sécurité Nationale paru en 2008. Ce dernier constitue toutefois le premier texte officiel de haut niveau qui identifie formellement la nécessité d'une stratégie. Il mentionne en effet la menace d'attaques contre les réseaux informatiques et encourage le déploiement de mécanismes de prévention de la cyberguerre. La cyberdéfense, tout comme la cyberguerre ou les cyberattaques, ne sont pas définies officiellement : pour notre étude, nous prendrons de la cyberdéfense une définition large et flexible, autorisant les remises en question. La stratégie concernant l'organisation et les moyens de mise en oeuvre des mécanismes de prévention des cyberattaques formera pour nous la doctrine de cyberdéfense française.

Cette doctrine est nécessairement à construire. En effet, la doctrine de cyberdéfense ne peut s'appuyer sur les concepts de défense classiques. L'agresseur

n'est plus aisément identifiable, ce qui complique les possibilités de dissuasion. De plus, la territorialité sur Internet ne répond pas aux modèles traditionnels : les frontières étatiques n'y sont pas établies, et de nombreux pays mettent en avant la « neutralité du net » . Les éventuelles possibilités d'actions étatiques n'y seraient donc a priori possibles que dans le cadre de traités internationaux pour le moment rares, limités dans leur couverture du sujet, et inégalement appliqués.

Pour traiter le thème de l'émergence d'une doctrine de cyberdéfense française, nous nous proposons de rappeler d'abord les différents textes officiels qui définissent et mettent en oeuvre des éléments de stratégie de cyberdéfense nationale.

Une comparaison avec quelques doctrines étrangères permet ensuite d'identifier des divergences de nature à nourrir le débat, enfin, nous proposons des évolutions de la doctrine française actuelle.

Les informations présentées dans l'exposé ne proviennent que de sources ouvertes et de présentations officielles. Les opinions émises par les auteurs, en revanche, intègrent divers retours d'expérience professionnelle et personnelle. Les idées avancées sont volontairement ambitieuses et permettrons nous l'espérons d'alimenter le débat.

Cyberdéfense en France

Doctrines actuelles

Aucun texte n'est en soit une doctrine de cyberdéfense française. Mais plusieurs éléments participent à la construction d'une telle doctrine.

Le Livre blanc sur la défense et la sécurité nationale Le Livre blanc sur la défense et la sécurité nationale, paru en juin 2008, présente un classement des risques à prendre en compte. Les systèmes d'information sont aujourd'hui vulnérables à des « ruptures accidentelles ou a des attaques intentionnelles » . Le risque que représente une attaque sur ces systèmes est évalué en numéro deux des menaces contre la France, avec une probabilité maximale et une ampleur faible à forte.

- Menaces
  - Il existe un risque de ruptures stratégiques brutales dans le domaine de l'informatique où des avancées exceptionnelles peuvent remettre en cause l'ensemble des défenses mises en place
- Défense
  - Les stratégies suivantes doivent être mises en place : « défense en profondeur, protection intrinsèque des systèmes, surveillance permanente, réaction rapide et action offensive » . Elles seront pilotées par l'État qui

devra développer son expertise en SSI, sa capacité de gestion de crise et d'après-crise (continuité des activités et poursuite des agresseurs). Enfin une dimension de lutte dans le cyberespace doit être définie.
- Des moyens de détection précoce des attaques informatiques doivent être mis en place.
- Le développement de produits de sécurité et de réseaux de confiance doit être encouragé chez les industriels français
- L'ANSSI est créée afin mettre en oeuvre un dispositif de détection centralisé et de défense contre les attaques informatiques. L'agence doit par ailleurs assurer la protection des réseaux sensibles de l'État et sensibiliser et conseiller le secteur privé et les SAIV (Secteurs d'Activités d'Importance Vitale). Elle sera par ailleurs le relais avec nos partenaires européens d'une politique de sécurité des réseaux de communication à l'échelle européenne.
- Ceci implique l'adaptation du dispositif français de lutte contre le terrorisme à la protection des systèmes informatiques sensibles et à précéder la progression de la menace.
- Une coopération opérationnelle entre états partenaires doit être créée pour détenir des capacités de réaction et des obligations de résilience pour nos opérateurs.
- L'efficacité de l'agence européenne ENISA doit être améliorée et contribuer à l'intégration de la SSI dans les réalisations des institutions européennes
- La lutte informatique offensive doit permettre d'engager l'agresseur et de neutraliser les sources d'attaques. La doctrine d'emploi de la LIO reste à préciser.
- Des capacités interarmées de lutte informatique doivent être mises en place.

Autres sources doctrinales Plan de renforcement de la sécurité des systèmes d'information de l'État (2004 2007) (mai 2004)

Le plan de renforcement de la sécurité des systèmes d'information de l'État [3] a été rédigé suite aux difficultés persistantes dans l'amélioration de la sécurité des systèmes d'information. Ce plan fixe plusieurs objectifs, dont certains ont été réalisés.

- Sécuriser les moyens de transmission des Hautes Autorités. Le SGDN propose différents moyens de générations différentes : MAGDA V2 (messagerie) et RIMBAUD (téléphonie, télécopie, éventuellement avec du surchiffrement) sont largement déployés ; ISIS (intranet homologué pour le transport

3. www.ssi.gouv.fr/archive/site_documents/PRSSI/PRSSI.pdf

d'informations classifiées de défense), plus récent, reliant pour l'instant un nombre restreint de sites.
- Sécuriser les systèmes d'information des administrations avec une attention particulière pour les nouvelles fonctions de l'administration électronique. Rédiger les politiques de sécurité.
- Mettre en place les capacités opérationnelles de réponse aux attaques informatiques via l'application des plans Piranet et Vigipirate SSI. Piranet fait notamment l'objet de plusieurs exercices théoriques ou pratiques, mais sans qu'aucun détail n'en soit publié.
- Inscrire la démarche de sécurisation des SI dans le cadre de la politique de sécurité de l'Union européenne.

Ce plan fixe douze mesures pour atteindre ces objectifs. De nombreuses mesures sont aujourd'hui appliquées mais certains points non-traités subsistent.
- Au regard de la formation, le plan prévoit le développement des compétences en sécurité des systèmes d'information au sein des administrations, la mise en place d'exercices pour tester la sécurité et son organisation, la sensibilisation des hauts responsables ainsi que la qualification des prestataires privés en SSI.
- Concernant l'organisation, le plan prévoit l'affectation des rôles et responsabilité en termes de sécurité à tous les niveaux de l'administration, la mise en place de permanences opérationnelles en cas d'application des plans Piranet et/ou Vigipirate et la mutualisation de services de sécurité des systèmes d'information.
- Pour les équipements, le plan prévoit l'acquisition d'infrastructures et de moyens techniques adaptés aux enjeux de sécurité, l'accroissement du nombre de produits qualifiés en sécurité, la garantie d'une diversité d'approvisionnement en produits de sécurité et l'adaptation des capacités d'évaluation et de certification aux besoins.
- Enfin, sur le plan juridique, le plan propose l'adaptation des textes réglementaires. Il s'agit notamment d'expliciter la politique interministérielle de sécurité des systèmes d'information.

Rapport de Pierre Lasbordes sur la Sécurité des Systèmes d'Information (2006)

Le rapport Pierre Lasbordes [4] reconnait l'enjeu crucial, « majeur » , que représente la sécurité des systèmes d'informations en France. Il met en avant 6 axes de développement :
- Sensibiliser et former à la sécurité des systèmes d'information
- Responsabiliser les acteurs via des chartes d'utilisateurs et la labellisation des acteurs SSI.
- Renforcer la politique de développement de technologies et de produits SSI

4. www.lasbordes.fr/IMG/pdf/26_novembre_doc_definitif.pdf

- Rendre accessible la SSI à toutes les entreprises
- Accroitre la mobilisation des moyens judiciaires
- Assurer la sécurité de l'État et des infrastructures vitales

Ce rapport semble être le point de départ ayant conduit à la transformation de la DCSSI vers l'ANSSI

Rapport d'Information du Sénat par Roger Romani (2008)

Ce rapport [5] est un grand état des lieux de la cyberdéfense et pointe, 2 ans après le rapport Lasbordes de nombreuses lacunes. Il indique également des points concrets à mettre en oeuvre pour une amélioration :

- Porter les moyens de l'ANSSI au niveau de ceux de ses homologues britanniques et allemands
- Donner plus de force à la politique de la sécurité des systèmes d'information en augmentant notamment les prérogatives de l'ANSSI
- Renforcer le partenariat avec le secteur économique via le développement des labels et le financement de la recherche

Le CEDF (Centre de Doctrine et d'Emploi des Forces) a également publié des doctrines [6] en mai 2008, concernant les opérations d'influence et les opérations d'information mais sans aborder la sécurité informatique proprement dite.

Le thème de la cyberdéfense est par ailleurs évoqué dans les travaux parlementaires suivants :

- La loi n° 2009-928 relative à la programmation militaire 2009-2014 [7] et son rapport annexe.
- L'avis n° 1970 [8] de la commission des affaires étrangères sur le projet de loi de finances pour 2010, dont nous retenons l'extrait suivant : « Cet événement [Conficker] est venu rappeler l'importance prise aujourd'hui par la menace cybernétique. Celle-ci est prise en compte depuis longtemps par d'autres États. La France, constatant son retard, a adopté plusieurs mesures pour renforcer ses capacités défensives et offensives dans ce domaine. »
- L'avis 2085 [9] de la commission des affaires étrangères de l'assemblée nationale ğ I-D-3 sur « les armes cybernétiques » , et III-B-3 sur « les attentats cybernétiques » .

Ces rapports depuis 2004 démontrent non seulement une manque d'amélioration entre chaque rapport mais plus encore, un relatif retard de la France dans le domaine de la cyberdéfense face aux enjeux de protection et aux moyens mis

5. www.senat.fr/rap/r07-449/r07-4491.pdf
6. www.cdef.terre.defense.gouv.fr/publications/doctrine/no_spe_fonct_ops/version_fr/fonct_ops/art8.pdf http://www.cdef.terre.defense.gouv.fr/publications/doctrine/no_spe_fonct_ops/version_fr/fonct_ops/art9.pdf
7. www.assemblee-nationale.fr/13/ta/ta0299.asp
8. www.assemblee-nationale.fr/13/budget/plf2010/a1970-tIV.asp#P470_78671
9. www.assemblee-nationale.fr/13/rap-info/i2085.asp#P476_141747

en oeuvre. Les pays de taille comparable souvent mentionnés en exemple sont le Royaume Uni et l'Allemagne.

Applications concrètes de la doctrine Protection des systèmes d'information

La protection des systèmes d'information en France est assurée par plusieurs entités. De manière globale, c'est l'ANSSI [10], agence rattachée au SGDN qui coordonne la sécurité des systèmes d'information au sein des administrations. Ses missions, publiques, ne sont pas rappelées ici.

Au ministère de la défense, cette protection, qui prend le nom de « LID » (lutte informatique défensive), est assurée par des fonctions de veilles, alertes et réponse aux vulnérabilités, menaces et incidents via l'OPVAR (Organisation permanente de veille, alerte et réponse). Cette organisation est aussi responsable de l'application des plans Vigipirate SSI et Piranet.

Au ministère de l'intérieur, la toute récente DPPSN [11] est chargée de l'élaboration, de l'actualisation et du suivi des plans. Elle élabore les instructions en vue de leur application territoriale, qui sont relayées par les OzSSI (Observatoires Zonaux de la Sécurité des Systèmes d'Information). Elle est aussi chargée de la définition de la PSSI interne au ministère.

La DCRI [12] contribue également à la protection de nos systèmes d'information. Elle travaille notamment à la sensibilisation des entreprises et à l'investigation, de concert avec la cellule d'intelligence économique à Bercy.

Lutte informatique offensive (LIO) dans le cadre de la défense

Dans un cadre non nécessairement militaire, il peut être utile aux enquêteurs de police et de justice d'acquérir de l'information sur les systèmes attaquant nos intérêts, à des fins d'identification des agresseurs, ou d'anticipation des attaques. En France, la future LOPPSI va autoriser les enquêteurs à déployer des dispositifs de captation de données informatiques, aussi bien en France qu'à l'étranger, dans des cadres stricts. Il n'est pas encore clair jusqu'où pourront aller les enquêteurs en matière d'intrusion proprement dite sur les systèmes d'information : s'agira-t-il d'intrusion réelle menée à distance ou d'installation des dispositifs sur place par les enquêteurs ?

Dans le cadre militaire, très peu d'informations sont disponibles sur la LIO en France. Depuis la parution du livre blanc de la défense nationale il y a deux ans, seules les présentations publiques du directeur technique de la DGSE au SSTIC (juin 2010) et à l'ARCSI (septembre 2010) affirment l'existence d'une telle activité en France. Par ailleurs, les diverses sources parlementaires précisent que la doctrine d'utilisation n'était toujours pas définie fin 2009 [13].

10. `www.ssi.gouv.fr`
11. La direction de la prospective et de la planification de sécurité nationale a succédé le 27 août 2010 à la DPSN, elle même n'ayant été créée qu'en 2008 à la suite du Livre Blanc
12. Direction Centrale du Renseignement Intérieur
13. `www.assemblee-nationale.fr/13/budget/plf2010/a1970-tIV.asp#P495_88312`

Enfin, l'éventualité technique et juridique de déployer des logiciels de prise de contrôle à distance sur des équipements potentiellement hostiles appelle à des réflexions que nous développerons dans un chapitre ultérieur sur la LIO.

Comparaison à l'international

A l'heure actuelle, de nombreux pays, développés ou engagés dans un développement rapide et intense, ont étudié, se préparent et considèrent sérieusement les questions de guerre de l'information ou cyberguerre. Bien que ces évolutions associées à plusieurs événements encore récents (Estonie, Géorgie, Corée du Sud, « Aurora » ...) commencent à gagner la sphère diplomatique, il n'existe à l'heure actuelle qu'un seul texte international traitant de sujets pouvant être rattachés à la cyber-défense : la Convention de Budapest. Cette « Convention sur la Cybercriminalité » du Conseil de l'Europe, signée et ratifiée par plusieurs pays, propose des mécanismes de coopération étendus mais se limite aux incriminations délictuelles liées au terme « cybercriminalité » et relevant de sécurité intérieure. Cependant, cette Convention pourrait être complétée sous peu par d'autres traités.

États-Unis d'Amérique

Les États-Unis disposent d'une organisation complexe assortie de doctrines variées.

Organisation Pour rappel, l'organisation américaine participant à la cyberdéfense s'étale sur quatre niveaux (politique, stratégique, état-major, opérationnel) et plusieurs domaines (civil, militaire, administration).

On retiendra, sans la détailler ici, une très profonde complexité qui ne garantit pas l'efficacité. On remarquera également que l'ensemble des domaines sont couverts : LIO/LID, sécurité et défense, cybercriminalité, protection des infrastructures, exercices et gestion de crise, unités à vocation stratégiques, complétude de la notion de guerre de l'information (guerre électronique, opération d'information, cyber défense, opérations « réseaux-centrés »)... Tout cela fait des États-Unis, sans doute le pays le mieux armé en matière de lutte informatique mais pas nécessairement de la manière la plus efficace.

Problématiques clés de la cyberdéfense américaine : Pour autant, la cyberdéfense américaine doit encore traiter certaines problématiques :

- Élever le niveau de sécurité global : le choix s'est porté sur une approche de type conformité ou encore « compliance » matérialisé par le FISMA, qui suscite de nombreuses critiques quant à son efficacité.

- Problématiques militaires : la récente création de l'US CYBERCOM dirigé par le Général K. Alexander en charge également de la NSA a suscité des critiques quant au périmètre de cette nouvelle fonction. A ce sujet, la problématique majeure demeure la capacité et la légitimité du Cyber Command à protéger les infrastructures et les réseaux « civils » .
- Lutte entre deux approches NETWORK CENTRIC vs. CYBER CENTRIC :
  - « Network Centric » : recommandée par le « cyberczar » américain, Howard Schmidt ainsi que par le Général K. Alexander. Cette approche réfute la logique de la cyberguerre en tant que telle et se concentre sur la sécurité des réseaux sans négliger les menaces actuelles. La notion même de cyberguerre a d'ailleurs été rejetée par Howard Schmidt,
  - « Cyber Centric » : relayée par l'Amiral McDonnel, ancien directeur du renseignement américain. Elle s'appuie sur une rhétorique assez dure et conçoit assez simplement la cyberguerre. Plus généralement, c'est la tendance qui ajoute du « cyber » à tous les mots et qui est soutenue par toute l'industrie de défense et de sécurité américaine.

Russie et Inde

Ces deux pays présentent des caractéristiques communes : ils sont fréquemment mis en avant dans le cadre de la lutte informatique ou sont des pionniers dans des domaines liés à l'informatique. Ils sont donc des acteurs déterminants de la cyberdéfense ou des cyberconflits.

En revanche, et contrairement aux États-Unis, les publications rares et les secrets bien gardés ne nous permettent qu'une évaluation de leur cyberdéfense.

Inde L'Inde, avec son acquisition de la capacité nucléaire et ses affrontements avec le Pakistan, est décidée à défendre sa place et son rang dans le système international.

En matière de lutte informatique, le Chief Admiral Sureesh MEHTA a pu ainsi dire en août 2009 [14] : « les forces armées indiennes sont de plus en plus impliquées dans des opérations réseaux-centrées, seules ou en interarmées. On ne peut se permettre d'être vulnérable aux cyber-attaques. Les TICS sont le point fort de l'Inde et il est de notre intérêt que de faire de ce levier un outil afin de développer de formidables capacités tant offensives que défensives dans le domaine de la cyberguerre » .

Les sources de doctrine ayant trait à la cyberdéfense auxquelles le lecteur peut se référer pour l'Inde sont :

- IT ROADMAP (1998-2008)

14. Federal Information Security Management Act, implementation project : csrc.nist.gov/sec-cert/

- « Challenges pour la gestion de la sécurité nationale » (2001)
- Doctrine de Sécurité Indienne (2004 - MAJ 2009)
- Doctrine de Guerre non-conventionnelle. Chapitre : « Cyber-Terrorisme et Guerre de l'information » (2007)
- Exercice de type « war game » en 2009 intitulé « Divine Matrix » : évaluation de la capacité de réaction indienne face à une cyberattaque précédent une attaque nucléaire chinoise en 2017
- Développement de leur propre OS afin de garantir leur souveraineté [15], annoncée en Octobre 2010.

Les lacunes de l'Inde en matière de sécurité ne doivent pas masquer l'existence d'une élite bien formée et des capacités informatiques avérées. De plus, l'histoire récente et parfois violente du pays, ainsi que les récents efforts de doctrines et d'organisation indiquent une véritable capacité de lutte informatique en construction. Si, à l'heure actuelle, cette capacité ne peut être comparée à celle des États-Unis ou de la Chine, l'Inde, sera très certainement une future « puissance informatique » .

Russie La Russie est un pays dont on attend beaucoup en matière de lutte informatique et de doctrine, notamment à cause de son passé qui a su forger un outil de formation et d'éducation de qualité mais également en raison de nombreux événements récents (Estonie, Géorgie, état de la cybercriminalité) qui démontrent des capacités russes réelles en matière de lutte informatique.

Cependant, comme en témoignent plusieurs déclarations de responsables militaires russes ou encore la stratégie de sécurité jusqu'en 2020, l'accent est mis sur la « guerre informationnelle » qui se conçoit plus largement. Plus encore, la Russie semble avoir une vision tout à fait innovante en la matière puisque elle sait utiliser l'ensemble de ses capacités diplomatiques au profit d'une action de tendance juridique de régulation de « guerre informationnelle » .

Les sources de doctrine ayant trait à la cyberdéfense auxquelles le lecteur peut se référer pour la Russie sont :

- Doctrine de sécurité russe 2020
- Doctrine concernant la sécurité de l'information pour la Fédération de Russie
  - Accord des services de sécurité de la CEI
  - Approche plus générale de la guerre informationnelle incluant les différents éléments propres aux concepts, informatiques et « sémantiques »
- Développement de leur propre OS afin de garantir leur souveraineté.
- Activisme diplomatique en faveur d'un traité de contrôlé des armements dans le cyberespace

15. economictimes.indiatimes.com/infotech/hardware/India-to-develop-its-own-futuristic-computer-operating-system/articleshow/6719490.cms

La Russie présente aujourd'hui un profil plus tranché que l'Inde : il ne subsiste aucun doute sur ses grandes capacités en matière de lutte informatique. Tant ses capacités informatiques, que son histoire ou encore son implication dans les affrontements récents prouvent un niveau avancé en matière de lutte informatique. On peut toutefois nuancer le propos en soulignant que rien n'a permis pour le moment de faire la preuve des capacités de lutte informatique défensive ou encore que ses approches doctrinales restent parfois étonnantes. Ainsi, son insistance à aborder la « diplomatie informatique » par le biais de l'arme informatique ou encore de la subversion par Internet.

Cette utilisation de l'arme informatique à des fins de géostratégie globale nous invitera à considérer la nécessité de positionner notre cyberdéfense dans un cadre d'emploi également global.

Suisse

Au contraire des pays précédemment cités, l'approche suisse est d'avantage similaire à l'approche française.

La Suisse se démarque en revanche par sa capacité à communiquer publiquement sur sa situation en matière de cyberdéfense, les incidents d'envergure et les conseils aux utilisateurs, notamment par le rapport semestriel « MELANI » (Centrale d'enregistrement et d'analyse pour la sûreté de l'information).

OTAN

Parallèlement aux efforts entrepris par les pays cités ci-dessus en matière de lutte informatique et guerre de l'information, l'OTAN s'est également saisi de la question notamment après les attaques informatiques contre l'Estonie. Elle devait par ailleurs prendre des mesures en réaction aux attaques informatiques dont l'organisation serait victime et face aux doctrines émergentes prenant en compte le concept de cyber-guerre. La stratégie publique de l'OTAN sur ce sujet ne concerne qu'un volet de cyberdéfense, qu'il soit actif ou passif. Il n'y a actuellement aucune information sur le développement ou sur une volonté de développement de capacité offensive dans le cyberespace. Cette absence de visée offensive n'interdirait pas, pour autant, l'attaque de réseaux illégitimes tiers à des fins de défense.

Suite au sommet de Bucarest en 2008, un centre de cyberdéfense (NATO CCDCOE) a été mis en place à Tallinn. Son objectif est de réunir l'expertise en matière de risque « cybernétique » , d'élaborer une doctrine, de partager des retours d'expérience et de former des experts tant au sein de l'OTAN que dans les différents pays membres. Par ailleurs, une autorité chargée de la cyberdéfense (CDMA) a été mise en place à Bruxelles afin de coordonner les efforts en cyberdéfense et de prévenir, détecter et dissuader les attaques.

De manière plus globale, l'OTAN est en cours de révision de ses concepts stratégiques à horizon 2020. Le rapport préliminaire sur les concepts stratégiques [16] identifie la faiblesse actuelle de l'organisation dans le domaine de la cyberdéfense comme une vulnérabilité inacceptable et de plus en plus dangereuse. Il suggère qu'une haute priorité soit accordée à la mise en place de mesures.

D'après ce rapport préliminaire, les actions consistent à :

- renforcer la surveillance des réseaux critiques de l'OTAN
- renforcer le rôle du centre de Tallin dans l'aide aux pays membres quant à leur programme de cyberdéfense
- mettre en place des capacités d'alerte rapide grâce à des capteurs et des noeuds de surveillance au sein de l'organisation
- développer et fournir les moyens de remédier aux vulnérabilités identifiées.
- mettre en place une équipe d'expert pouvant aider en urgence un État membre frappé ou menacé par une cyber-attaque majeure
- développer des moyens actifs et passifs de cyberdéfense adaptés

Nous relevons que le NATO Consultation, Command and Control Agency (NC3A), travaille actuellement sur des systèmes de détection d'intrusion et d'analyse de risques temps réel. Cette agence propose déjà divers services de sécurité aux états membres.

La consultation du nouveau concept stratégique de l'OTAN pose la question de l'adaptation de l'Art. 5, qui fonde la défense et la sécurité collective en permettant aux alliés d'intervenir si l'un d'entre eux est agressé, aux cas de cyber-attaques.

Organisations internationales et diplomatie Depuis quelques temps, on peut observer une recrudescence de l'activisme dans le monde diplomatique vers les problématiques de lutte informatique et les domaines connexes. L'UIT [17], en particulier, longtemps écartée de la Gouvernance Internet, souhaite établir un traité international contraignant chaque état à : protéger ses concitoyens des cyber-attaques, ne pas abriter de cyber-terroriste sur son territoire et ne pas lancer d'attaques contre d'autres pays. Ce projet suscite de nombreuses réserves quant à sa faisabilité.

Par ailleurs, l'ONU fournit depuis quelques temps le cadre légal des négociations russo-américaine sur la régulation des « armes informatiques » .

De cet activisme diplomatique, certaines initiatives sont plus perceptibles et avancées que d'autres. En voici un résumé :

- Les négociations américano-canadiennes actuellement en démarrage. On a pu constater que des négociations ont débuté avec le Canada. Il s'agirait dans ce cas de développer une cyberdéfense commune justifiée par le partage de visions, de doctrines et surtout d'infrastructures. On pense ainsi, par

16. www.nato.int/strategic-concept/strategic-concept-report.html
17. www.irsem.defense.gouv.fr/IMG/pdf/Intervention_Paris_15_juin-2.pdf

exemple, aux infrastructures de RIM (Blackberry) particulièrement utilisées aux États-Unis.

– Des négociations russo-américaines portent sur un traité pour l'encadrement de la lutte dans le cyberespace. Depuis au moins un an, délégations russes et américaines se rencontrent pour établir une forme de traité de non-agression sur Internet. Les positions étaient d'abord très éloignées : les américains préférant une approche de police, orientée lutte contre la cybercriminalité et le partage d'informations tandis que les russes prônaient une approche « arms control » . Un round de négociations s'est conclu le 14 mai 2010 et a vu ensuite les positions se rapprocher : les américains tendant à adopter la vision russe. Le dernier point notable reste la présence du représentant américain à l'ICANN, lors de ces négociations, M. Sadowsky.
– L'actualité de la convention de Budapest. A ce jour, la Convention de Budapest est entrée en vigueur dans la plupart des pays signataires. Cependant, il subsiste au moins encore 16 états dont la signature n'a pas été suivie de ratification et 30 état qui l'ont ratifié. Sur ces 30 ratifications, la Convention est entrée en vigueur partout. On rappelle qu'il existe plus de 200 états dans le monde. Cela permet d'avoir une vision assez précise de l'actualité de la Convention, un des rares textes juridiques internationaux à vocation opérationnelle.

Notons cependant que le Conseil de l'Europe reste une des rares organisations à s'être préoccupée assez rapidement des menaces sur Internet. Malgré les limites de la Convention sur la Cybercriminalité, traitant plutôt de sécurité intérieure, le Conseil est particulièrement impliqué notamment dans les processus de la gouvernance internet témoignant ainsi d'une ouverture et d'une continuité que d'autres organisations ont tardé à montrer.

Contrairement au Conseil de l'Europe et à l'OTAN, l'Union Européenne pourrait, pour sa part, imposer des évolutions législatives sur les états membres et ce dans la continuité de la directive 20/31/CE. En matière de sécurité informatique, au sein de l'UE, l'ENISA n'a pour l'instant pas de rôle opérationnel et une évolution de ses compétences est attendue. En matière de cyberdéfense, une synergie avec la PESD reste à trouver.

Limites et évolutions

Certains thèmes, qui nous semblent essentiels ou appelés à le devenir, ne font encore l'objet d'aucune stratégie établie.

Lutte informatique offensive

Différents contextes d'emplois de la LIO pourraient être les suivants.

Prépositionner des accès sur les principaux vecteurs menaçants A l'heure actuelle les vecteurs menaçants sont principalement les botnet. Ces botnet constitués à partir d'ordinateurs infectés peuvent être compromis. Disposer d'accès dans ces réseaux permettrait :

- de recueillir du renseignement concernant la préparation d'attaques ou les capacités techniques d'un agresseur potentiel ;
- de rendre simplement inopérants les armes ;
- d'en prendre le contrôle pour, en cas d'attaque sur une cible française ou un intérêt vital, interrompre cette attaque ;
- d'utiliser ces vecteurs pour lancer d'autres attaques.

Le CCDCOE (OTAN) a par exemple mené une première formation [18] dans le domaine de la prise de contrôle d'un botnet en septembre 2010. Les réflexions qui en découlent sont prometteuses. En particulier, le même centre appelle [19] à des discussions politiques urgentes pour définir les autorisations nécessaires et la faisabilité légale de ces actions.

Le prépositionnement par intrusion des botnets trouve sa limite face à des botnets très limités en dispersion, mais ayant une capacité de nuisance considérable avec l'arrivée des fibres optiques. Les opérateurs et hébergeurs sont évidemment des alliés privilégiés pour détecter et désactiver les éléments de botnet sur leur réseau. La future LOPPSI participe également à cette convergence public-privé, en obligeant les fournisseurs d'accès à interdire certaines adresses réseaux fournies par le ministère de l'intérieur à des fins de lutte contre la pédopornographie.

Se doter d'une capacité de dissuasion informatique Il n'y a pas de consensus sur la possibilité et la doctrine d'emploi d'une dissuasion informatique réaliste. D'après nous, la dissuasion à laquelle nous sommes habitués, à savoir la capacité démontrée d'infliger à l'agresseur des dégâts qui dépassent son intérêt potentiel à nous attaquer, est inapplicable en matière informatique.

En effet, cela exige d'identifier rapidement et avec certitude l'agresseur, ce qui reste irréaliste dans de nombreux cas, rendant donc inopérante ce type de dissuasion qui doit être permanente et totalement fiable. Cependant, une dissuasion avec un sens plus large reste envisageable, sous réserve que son cadre d'emploi soit clairement défini. Par exemple, nous pouvons envisager une dissuasion sous forme de menace d'attaque informatique en réponse à une agression dans un autre domaine (agression dans le domaine économique ou militaire conventionnel). Il n'est pas non plus nécessaire de viser, dans la dissuasion, l'agresseur. La dissuasion pourrait aussi viser des intérêts de l'agresseur, ses alliés, ou plus généralement une cible dont l'attaque informatique aurait des effets indirects sur l'agresseur.

18. www.ccdcoe.org/190.html
19. www.ccdcoe.org/cyberwarfare/images/146.pdf

Considérons à l'extrême la notion d'attaques aveugles qui évacue le problème d'identification de l'agresseur. En effet, il s'agit d'attaquer sans discernement les adresses relevées comme source. Cette approche d'une riposte, rapide, brutale, non mesurée et non intelligente, ne parait pas inconcevable lorsqu'on songe aux États-Unis. Au contraire, les pays auraient tendance à investir dans une plus grande sécurité pour se protéger d'éventuels retours de bâtons ! Il s'agit d'une approche théoriquement plus acceptable qui parait cependant ne pouvoir résister que difficilement à l'épreuve de la réalité.

Concernant la difficulté d'identification de l'agresseur, on voit qu'il ne s'agit pas d'un passage obligé : les motivations d'emploi de l'arme (revendications, effets recherchés, contexte plus global) fournissent de nombreux éléments pouvant, dans certains cas, définir une cible pertinente pour notre capacité de dissuasion. Il faut donc s'affranchir de la vision nucléaire de la dissuasion et rechercher des cadres d'emplois plus globaux ou progressifs.

En tout état de cause, une dissuasion efficace nécessite :

- une doctrine d'emploi, affichée et claire
- des capacités d'emploi affichées, notamment via des exercices dont les résultats sont publiés

Concernant la doctrine d'emploi, aucune information n'est publiée à l'heure actuelle. En revanche, les capacités, du moins techniques en l'absence d'autorisations légales, existent en France. Par exemple, des experts en intrusion se mesurent aux équipes internationales chaque année au challenge de Defcon (Las Vegas), avec un succès réel (l'équipe francophone est régulièrement deuxième), mais sans être médiatisés pour autant, ni revêtir une investiture officielle de l'État.

Force offensive informatique en soutien à la défense militaire Concernant l'acte offensif en lui-même, l'utilité d'une force offensive informatique dans un cadre de guerre conventionnelle (soutien aux opérations militaires) a déjà fait ses preuves (conflit Russo-Géorgien). Dans ce sens, la frontière entre guerre électronique et guerre informatique commence déjà à s'estomper très sensiblement.

Emploi en dehors du domaine militaire ? La LIO aurait également pu être un moyen, notamment pour un acteur du domaine de l'économie ou de la recherche, de protéger voire renforcer sa compétitivité internationale. Cet aspect non-militaire de l'attaque informatique a donné lieu, en France, a deux étapes majeures d'évolution du code pénal (1988, 2004) punissant ces pratiques :

- en 1988, la loi Godfrain punit l'intrusion dans un système informatique, l'altération et le déni de service (323-1 et suivants du code pénal).
- en 2004, l'acquisition, la détention et la fourniture d'outils conçus pour réaliser une intrusion deviennent également punissables (323-3-1 du code pénal).

Pour de nombreuses raisons, à commencer par la difficulté à mener les enquêtes techniques et l'absence de frontière sur internet, cette évolution n'a pas pour autant fait cessé les attaques informatiques entre entreprises ou institutions. Aussi, ces organismes ne peuvent se reposer sur cette protection pénale : ils doivent également mettre en oeuvre une cyberdéfense à leur niveau.

La subversion, la désinformation et la communication

Il s'agit de prendre en compte les actions subversives, d'information ou de désinformation, via internet lors des conflits. En particulier, la contestation dans la société civile peut avoir des répercussions directes sur les conflits armés. Cet aspect est déjà évoqué par le Livre Blanc (pages 52 et 190), et repris par le CDEF (centre de doctrine d'emploi des forces) et le CICDE (centre inter-armée de concepts, de doctrines et d'expérimentations).

Un organe centralisant la communication des différentes structures de l'État serait bénéfique à l'image des institutions. D'une part, un tel organe permettrait d'anticiper les réactions contestataires à des évolutions telles que, en 2004, la LCEN, aujourd'hui le projet de loi LOPPSI ou encore le projet de décret pour l'art. 6 de la LCEN. En effet, s'il est rassurant que la société civile s'interroge sur les dérives potentielles liées à la LOPPSI (liste noire d'adresses IP, dispositifs de captation de données). Il serait néfaste à nos capacités juridiques de la cyberdéfense que cette évolution soit remise en cause sur des fondements irrationnels.

De manière générale, la régulation des usages d'internet, étape nécessaire pour appliquer un minimum de cyberdéfense sur internet, se heurte nécessairement à l'opposition des partisans d'un internet libre et totalement ouvert. En effet, des actions de contestation, de désinformations voire de subversion via internet, allant du simple militantisme à l'altération de sites web institutionnels, visent à délégitimer le pouvoir et attiser certaines défiances. En ce sens, les actions des « hacktivistes » portent atteinte à l'efficacité de nos dispositifs législatifs et réglementaires. La prévention de ces atteintes participe directement à la cyberdéfense. Pour cela, l'identification et l'infiltration des noyaux de contestation s'avéreraient déterminantes.

D'autre part, les dissonances dans la communication de l'État, tant du fait de la multiplicité des acteurs que des vecteurs de communications (presse, web, blogs, réseaux sociaux, twitter...) pourraient être évitées. Cet organe central, toutefois, doit conserver une certaine indépendance de l'exécutif afin de conserver une crédibilité dans ses discours à destination de la société civile. Par exemple, l'ANSSI bénéficie aujourd'hui d'une opinion généralement très bonne au sein du milieu professionnel et d'une compétence non discutée. Il est toutefois regrettable que le site web securite-informatique.gouv.fr ne soit pas connu par les responsables informatiques et décideurs qui ne sont pas experts SSI. La promotion de ce site et

sa mise en avant médiatique lors des situations intenses, comme lors de Conficker ou actuellement avec Stuxnet, pourrait bénéficier à l'image des institutions.

En outre, cet organe pourrait être chargé de s'assurer que nos institutions ne sont pas exagérément exposées sur les réseaux sociaux, par l'intermédiaire de leurs représentants qui publient sur Facebook, Viadeo, LinkedIn, etc. On se rappellera des conséquences opérationnelles en Israël suite à la publication par un soldat de ses prochaines activités militaires sur profil de réseau social.

Outre un organe central, la prévention de la désinformation et de la subversion passe également par un maillage du territoire réalisé aujourd'hui par des structures décentralisées : OzSSI, réservistes, groupes de réflexion (IHEDN). De fait, le fonctionnement actuel des OzSSI ne leur permet pas de tisser des liens réels avec la société civile. En revanche, le tissu des réservistes et les instituts menant des réflexions sont en première ligne, tant pour remonter aux autorités des tendances de fond de la société civile, que pour y faire redescendre un discours rationnel et cohérent. Au Royaume-Uni par exemple, les WARP (Warning, Advice and Reporting points) participent à cette mission avec un maillage territorial similaire au tissu de nos réservistes.

Multiplicité des identités

Le cyberespace favorise notoirement les multiples identités, que ce soit dans des jeux à tendance social (MMORPG, Second Life...), dans un blog, sur Facebook, etc. Au-delà de ces usages légitimes, chaque internaute peut également avoir une activité malveillante et donc ajouter quelques identités à son « portefeuille » : pirate, cybercriminel...

Plus encore, le personnel militaire ou employé des services de renseignement possède également une vie sociale privée dont on peut trouver des traces sur Internet. Souvent cause de la « malveillance interne » , cette problématique porte, selon notre étude, sur la multiplicité des identités que l'individu utilise au cours de sa journée. Le cas de Bradley Manning, qui aurait diffusé à Wikileaks des informations de première main, pourrait ainsi trouver des causes dans cette multiplicité des identités.

La conséquence est que l'individu va adopter des codes et des valeurs morales éventuellement différentes en fonction de l'endroit et de l'identité qu'il aura.

De même, un État pourra utiliser et manipuler des groupes et ou des individus dans l'intention de les faire commettre des actes répréhensibles (DoS, intrusion, vol d'informations..).

Si nous transposons ces résultats à un objectif de « cyberdéfense » , nous nous apercevons que l'État est la cible directe des acteurs existants sur le net, que ce soit consciemment ou non. Les ressources informatiques d'une multinationale pourraient ainsi servir à des malveillances informatiques à cause d'un employé plus intéressé par une cause idéologique que par la loyauté envers son employeur.

Toute analyse stratégique qui identifierait la menace se verrait contrainte par la définition de l'acteur impactant de fait les contre-mesures. Cela doit donc conduire à de meilleurs modes d'action en matière de défense des institutions militaires, la pratique policière et celle du renseignement paraissent parfois les meilleures solutions. Or la multiplicité des identités des acteurs impliqués renforce la complexité de l'analyse des modes d'actions et de « l'ennemi » .

Deux moyens d'actions nous semblent éventuellement adaptés : l'infiltration des groupes menaçants sur internet et la coordination du renseignement. De la même manière que le renseignement permet de prévenir des attentats terroristes, on conçoit sans problème que des unités puissent être affectées à la prévention des attaques informatiques d'ampleur par l'identification des groupes ayant une tendance plus marquée au « passage à l'acte » .

Lutter contre la prolifération des armes, source d'asymétrie dans la lutte informatique

La législation actuelle [20] qui interdit « sauf motif légitime » , le développement des outils, reste peu précise. La jurisprudence permet une adaptation correcte du droit en fonction de l'appréciation de ce « motif légitime » exonératoire (cf. cass. 27 octobre 2009), mais l'incertitude juridique reste encore réelle et cela menace la recherche en sécurité informatique. En outre, d'autres évolutions législatives [21] ont également restreint la liberté de recherche sur les logiciels (rétro-ingénierie).

Évidemment, la détention et la circulation illégitime d'armes informatiques doivent être réprimées, mais cela ne doit surtout pas entraver la recherche en sécurité, en particulier lorsqu'il s'agit d'utiliser les outils permettant de tester ses propres réseaux et systèmes afin d'anticiper les attaques, ou d'échanger au sein de cercles restreints sur les dernières possibilités techniques d'attaque. L'utilisation ou la vente de programmes offensifs n'étant pas punissable sur l'ensemble du monde, il est illusoire de pense que l'art. 323-3-1 du code pénal suffira à réduire la prolifération des armes informatiques. Or aujourd'hui, l'ANSSI dit régulièrement que les états sont moins équipés que les particuliers en armes informatiques : l'asymétrie est flagrante.

Nous pensons qu'une loi pénale plus stricte accentuerait encore cet effet. Sans remettre en cause l'intérêt de ce cadre pénal, aujourd'hui, nous bénéficierions grandement d'un texte plus clair, moins ambigu, décrivant le champ d'application du « motif légitime » exonératoire de l'art. 323-3-1 du code pénal.

En Allemagne, à cause des craintes liées à un champ d'application trop flou, lorsque l'équivalent de l'article 323-3-1 du code pénal français a été introduit dans le code pénal fédéral allemand (section 202c), plusieurs développeurs d'outils de

20. Art. 323-3-1 du code pénal (issu de la LCEN, loi n° 2004-575 du 21 juin 2004)
21. Telle que la loi dite "DADVSI" n° 2006-961 du 1er août 2006

sécurité ont déménagé leurs sites web à l'étranger voire ont cessé leur activité publique [22]. Il est donc urgent que le législateur ou la cour de cassation définisse plus précisément les conditions entourant ce « motif légitime » .

La régulation des produits informatique et les situations de monopoles

Dans tous les domaines, une majorité de fournisseurs ne s'aligne pas sur les exigences de sécurité les plus basiques. La présence de monopoles industriels complique encore plus les capacités à réagir, les clients ne pouvant dès lors se tourner vers un concurrent offrant de meilleurs services en sécurité.

On pourrait aussi se poser la question de la confiance accordée aux produits ou services mondialisés. Différents fournisseurs étrangers ou institutions se sont imposés dans des secteurs clés de l'informatique : Cisco, Huawei (routeurs), HP (constructeurs), Microsoft (systèmes d'exploitation), Oracle (SGBD), SAP, quelques éditeurs d'antivirus (qui disposent de potentielles portes dérobées et peuvent prendre le contrôle de la plupart des ordinateurs), ICANN (gouvernance des noms de domaine), Google, etc.

La labellisation des produits de sécurité, et notamment le CSPN, est un bon début, mais une action encore plus en amont semble nécessaire. Dans son rôle régalien, l'État devrait, pour qu'un produit soit vendu sur le territoire français, imposer des fonctions minimales de sécurité sous forme d'une check-list de mesures incontournables. Le non respect de ces quelques exigences pourrait, pour l'efficacité du dispositif, être soumis à sanctions. Nous considérons la liste suivante comme un minimum :

- Tout logiciel en support du produit doit pouvoir être mis à jour dans les deux mois après la sortie de la mise à jour et ce, sans perte du support et sans surcoût ;
- Il ne doit pas exister de mot de passe par défaut à moins que celui-ci ne soit changé à l'installation et maîtrisé et modifiable par le client ;
- Tous les flux de communication à l'origine ou en destination du produit doivent être identifiés formellement ;
- Pour toute télémaintenance, la connexion au produit doit passer par un serveur de rebond avec authentification personnelle sur le sol français, effectuant une traçabilité complète et auditable par le client ;
- Lorsqu'une vulnérabilité sur son produit, lui est rapportée ou que celle-ci est publiée, l'éditeur/constructeur doit proposer sous un délai de deux mois des mesures permettant de réduire cette vulnérabilité et un correctif dans un délai de 6 mois ;

22. Parmi d'autres, Phenoelit et KisMAC ont cessé d'être distribués (www.phenoelit.de/202/202.html, http ://kismac.de)

– Nous envisageons enfin la possibilité que tout éditeur/constructeur vendant des produits sur le sol français, dès lors qu'une vulnérabilité lui est rapportée directement, rémunère le chercheur.

En particulier, pour les opérateurs d'importance vitale, même si les DNS n'abordent pas ou peu le risque informatique, ceux-ci devraient avoir l'obligation de protéger leurs systèmes d'information efficacement. Cette obligation devrait a priori être intégrée au plan de sécurité opérateur, mais les compétences des services préfectoraux [23] en matière d'audit SSI sont-elles à la hauteur ?

Nous proposons plutôt la création d'une Autorité Administrative Indépendante ou l'adaptation d'une AAI existante avec pouvoir de sanction, chargée des contrôles SSI dans ces secteurs clé.

Certes, l'ANSSI soutient les ministères coordonnateurs des SAIV et dispose de la compétence pour auditer la SSI des OIV. L'ANSSI peut également agir au sein de l'administration par la voie ministérielle. Cependant toute sanction, pénale ou administrative, en matière de SSI, n'est possible que par une décision judiciaire sur un fondement pénal (loi Godfrain, violation du secret défense...), ou par une décision administrative (CNIL, ASN...) pour un manquement à une obligation spécifique. Nous pensons donc que la SSI dans son ensemble, gagnerait à ce qu'une AAI soit capable de sanctionner, dans des limites prévues par la loi, les personnes de droit privé, de manière plus souple et réactive que l'autorité judiciaire, lors de certains manquements essentiels en SSI.

La régulation d'internet et des réseaux

Les réseaux de communication électroniques, au premier plan desquels figure internet, sont progressivement soumis à un conflit entre un besoin de régulation et volonté citoyenne d'un réseau neutre et libre. Les autorités sont en effet amenées à imposer des contraintes aux opérateurs privés et à se doter de capacités de décision et d'investigation. La loi impose déjà la conservation des données de connexion [24] et des données d'identification des contributeurs aux créations de contenu [25], bien que le décret pour l'application de ce dernier point ne soit malheureusement toujours pas publié à cause des oppositions émanant des communautés sur internet. La LOPPSI, quant à elle, apportera des outils utiles aux enquêteurs. Chaque évolution législative, réglementaire ou administrative restreignant la liberté d'utilisation des réseaux s'accompagne d'un militantisme en faveur d'un internet neutre et libre. Le débat lancé en février 2010 par la secrétaire d'État chargée de la prospective et du développement de l'économie numérique, Nathalie Kosciusko-Morizet, a d'ores et déjà permis d'officialiser le fait que la neutralité du

23. Le préfet de département ou l'autorité militaire peut saisir l'autorité judiciaire sur le fondement de l'article L1332-7 du code de la défense en cas d'inapplication des mesures protections prévues.

24. Art. L34-1 du code des postes et des communications électroniques

25. Art. 6-II de la loi n° 2004-575 du 21 juin 2004 dite LCEN

net n'interdisse pas de bloquer certains contenus ou de différencier leur traitement en fonction de leur nature.

Le Livre Blanc prévoyant qu'internet « devra être considéré comme une infrastructure vitale » et qu' « un effort important devra être mené pour améliorer sa résilience » , les capacités décisionnelles sur l'évolution de nos réseaux nationaux doivent s'inscrire dans une coopération européenne et faire l'objet de fondements juridiques impliquant les opérateurs privés. A cette fin, en liaison avec l'ANSSI (agence gouvernementale) qui participe aux négociations internationales, le régulateur ARCEP (autorité administrative indépendante) devrait prendre position dans le domaine de la résilience et s'investir du sujet dans ses relations avec les opérateurs privés. Si nécessaire, ses compétences pourraient être étendues par le législateur, se rapprochant ainsi de l'autorité que nous proposions précédemment, tout en se limitant aux réseaux de communications. L'organisation actuelle, avec un poste unique récemment pourvu au sein du bureau conseil de l'ANSSI, mériterait d'être complétée par des dispositifs plus ambitieux.

La normalisation internationale

Les États-Unis et, de plus en plus, la Chine sont très présents dans les centres de décision : l'administration et des entreprises privées emploient des personnes à temps plein pour être présentes aux groupes de normalisation. Il s'agit aussi bien de connaître à l'avance les futures spécifications qui vont prévaloir sur le marché, que d'influer sur la future norme en sa faveur. En France, nous manquons d'une capacité d'agir sur ces structures de normalisation et de gouvernance. Les activités associées s'appellent le lobbying, les réseaux d'influence, ou tout simplement la participation d'industriels ou d'autorités Françaises aux groupes de normalisation internationaux en matière d'informatique.

On peut finalement souligner [26] l'effort imposé à l'AFNOR sur l'assouplissement formulé par décret [27] des conditions de participation aux groupes de travaux de normalisation. Cet axe d'action dépasse le cadre informatique et est du ressort du HRIE.

Secteurs d'Activité d'Importance Vitale (SAIV) et Opérateurs d'Importance Vitale (OIV)

Les Directives Nationales de Sécurité et la réglementation des SAIV n'ont pas vocation à être centrées sur la SSI, cependant, le livre blanc met très sérieusement l'accent sur la menace SSI. Or les OIV dans la gestion de la défense de leurs infrastructures doivent respecter un niveau de classification défense contraignant. Cela entrave gravement le travail des RSSI qui ne peuvent faire appel à

26. Revue Défense en 2009 et Newsletter HSC en décembre 2009
27. Décret 2009-697 du 16 juin 2009

des compétences expertes SSI internes ou externes, si elles ne sont pas habilitées. Il est évidemment néfaste que les experts SSI soient tenus à l'écart des Politique de Sécurité Opérationnelles et Plan de Protection Particulier. Si la volonté est de conserver une classification de défense autour du travail sur les DNS, il faut impérativement prévoir d'habiliter le personnel SSI. Cette première option aurait également le mérite d'assurer que les experts SSI et les sous-traitants font l'objet de vérifications. A l'inverse, il est aussi possible d'assouplir la politique de classification des informations afin d'améliorer le travail en commun au sein de l'OIV. Cette seconde option a l'avantage de faciliter les échanges entre différents organismes du même secteur d'activité, et, surtout, entre les différentes nations européennes, notamment lorsque l'OIV est un industriel transnational. En effet, le fonctionnement des DNS est globalement commun aux différents pays de l'Union et la protection des réseaux informatiques ne s'entend qu'à l'échelle internationale.

Quel droit pour quelle doctrine ?

L'absence des définitions liées à la cyberdéfense rend les Conventions Internationales comme celle de Budapest capitales car elles sont seules à pouvoir définir des embryons de droit dans ce domaine.

Pour autant, un tel vide juridique rend aussi plus probable les tentatives bilatérales de négociation comme en témoignent les négociations russo-américaines sur le sujet.

De façon générale, les négociations devront en principe répondre aux trois questions suivantes, à l'instar des règles de droit international en matière de conflits :

- *Jus in bello* : Quels sont les interdits ? Comment attaque-t-on ? Quelles sont les règles d'engagement ? Quelles sont les limites des opérations militaires ?
- *Jus ad bellum* : Quelles sont les circonstances permettant à un pays de se déclarer agressé ? Comment déclare-t-il une éventuelle guerre après des attaques informatiques (sous l'hypothèse que l'agresseur a été identifié).
- *Jus contra bellum* : quelles sont les règles, lois et traités permettant d'éviter l'entrée en guerre par exemple ?

Conclusions

Nous retiendrons quatre grands thèmes d'évolution pour notre cyberdéfense.

Une culture excessive du secret nous semble d'abord préjudiciable à l'action des acteurs de la SSI. En particulier dans les Secteurs d'Activité d'Importance Vitale (SAIV), la surclassification des documents, à commencer par la directive nationale de sécurité, entrave la coordination de la sécurité des activités vitales.

En matière de SSI, la culture du partage des bonnes pratiques SSI doit être développée par exemple au moyen de forums transverses non seulement aux opérateurs d'importance vitale, mais aussi et surtout entre les quatorze SAIV qui sont interdépendants.

L'adhésion de la société civile à l'intérêt que représente la cyberdéfense nous semble ensuite nécessaire. Intéressons-nous aux expériences britanniques des WARP pour mailler le tissu citoyen ou au rapport MELANI en Suisse en matière de communication publique. Encourageons l'ANSSI à publier sur ses exercices PIRANET.

La France souffre d'une représentation insuffisante dans plusieurs domaines : normalisation internationale, équipementiers informatiques et éditeurs de logiciels, régulation internationale des réseaux. La régulation au niveau national d'un niveau de sécurité minimal (certifications et obligations) participerait également à améliorer la robustesse de nos activités. La création d'une autorité administrative indépendante (AAI) chargée de la SSI, ou l'adaptation d'une AAI existante, serait chargée du contrôle et des sanctions.

Enfin, une doctrine d'emploi claire de nos capacités de cyberdéfense devra s'appuyer sur une compréhension globale de la « diplomatie informatique » au sein de la défense nationale : emploi des armes, pré-positionnement, dissuasion, communication, formation. Cette maturité est nécessaire pour être au premier rang parmi les acteurs d'une coopération internationale (traités internationaux ou communautaires, législation) sans omettre l'utilité des relations bilatérales.

Remerciements

Nous souhaitons remercier, pour le temps qu'ils nous ont accordés :
– M. Yves Correc et l'IGA Philippe Wolf
– Le colonel. Stanislas de Maupeou
– Nos employeurs respectifs, Hervé Schauer Consultants (HSC) et Orange
– L'ANAJ-IHEDN et les membres du comité cyberdéfense