

MASTER PROFESSIONNEL

CONCEPTION DE DISPOSITIFS INTERACTIFS MULTIMÉDIA POUR LA DIFFUSION ET L'APPROPRIATION DES SAVOIRS



LA GESTION DU RISQUE DANS LE TRAITEMENT DES INFORMATIONS SENSIBLES

DIRECTEUR DE MÉMOIRE
DIDIER PAQUELIN

PRÉSENTÉ PAR
NASSIM BEN GHMISS

ANNÉE UNIVERSITAIRE
2011-2012



Table des matières

Résumé.....	5
Introduction	6
Identité numérique.....	7
Théories de l'information	9
Sécurité informatique.....	11
Problématique.....	12
Enjeux	14
Information cachée	18
Dispositifs numériques	22
Cryptologie	24
Introduction	24
Cryptographie symétrique.....	26
Cryptographie asymétrique	27
Stéganographie	28
Législation	30
Communauté Européenne	31
France	32
Normalisation	34
Communauté Européenne	35
France	36
Hypothèses.....	38
Méthode de recherche	40
Interview d'experts	42
Protection de la vie privée	42

Complexité cryptographique	48
Secret de l'information	51
Vecteurs d'attaque.....	53
Tableau comparatif	58
Etude de cas	60
L'affaire VMWare	60
Le nucléaire Iranien	62
Le printemps arabe	65
Histoire de drones	68
Conclusion.....	70
Bibliographie.....	72
Annexes	77
Annexe 1	77
Annexe 2	78
Annexe 3	79
Annexe 4	80
Annexe 5	81
Annexe 6	86
Annexe 7	90
Annexe 8	92

Résumé

Ce mémoire s'attache au domaine de la sécurité de l'information. Il présente, de façon la plus exhaustive possible, les différents moyens de protection des données pour mieux comprendre l'impact qu'ont celles-ci sur nos vies.

Pour cela, une analyse large du domaine est réalisée en vue de proposer un outil de mesure du risque de corruption d'un système informatique. L'étude des aspects politiques, économiques, sociaux, techniques ou encore normatifs permettant de mieux comprendre les tenants et les aboutissants de la problématique de ce mémoire.

Celle-ci étant de savoir si la gestion actuelle du risque dans le traitement de l'information sensible est suffisante aux vues des différents cas concrets récoltés.

Ainsi donc, pour mieux y répondre, une analyse tant au niveau civil que militaire est réalisée. Cela dans l'objectif d'une meilleure classification des risques. Pour cela nous traitons de l'identité numérique par le biais de la protection de la vie privée pour ensuite nous intéresser aux travaux des grands théoriciens des sciences de l'information et de la communication, Claude Shannon et Andreï Kolmogorov.

Cette étude préliminaire nous amène donc directement dans le cœur du sujet qui touche à l'aspect sécuritaire des systèmes d'information.

La présentation des techniques cryptographiques et stéganographiques ne font leurs apparitions qu'après avoir vu l'aspect théorique de la question posée. Celles-ci étant quelque peu techniques, elles nécessitent un parcours historique de l'état de l'art.

Le volet protocolaire est traité grâce à un regard sur les normes mises en place au niveau européen mais aussi national. Pour ensuite présenter également la législation en vigueur au niveau européen et national.

Dans la suite, l'analyse à proprement parlé est réalisée auprès d'experts du domaine pour étayer nos éléments de réponse.

Enfin notre outil comparatif nous permet alors, à partird'un panel de cas représentatifs, de mesurer le risque de fuite d'informations sensibles.

Introduction

Depuis l'arrivée massive de nouvelles technologies dans notre quotidien, la gestion de la confidentialité de l'information a été un facteur de préoccupation majeur de nos sociétés contemporaines. En effet, celle-ci est devenue le vecteur essentiel de communication de l'ère de la révolution numérique. Nous sommes au cœur d'un système sur lequel de nombreux secteurs clés se reposent tels que l'économie, l'armée mais aussi les gouvernements.

Mais l'information n'est qu'un outil, et il nous incombe de savoir quels sont les usages que nous souhaitons en faire puisque bien que les systèmes informatisés soient de plus en plus efficents, cela reste à l'Homme de définir quel est le but à attribuer aux dispositifs numériques mis en place.

Comme nous pouvons le voir, les enjeux du traitement de l'information sont donc cruciaux pour nos sociétés du savoir et comme le dit si bien François Bacon "savoir c'est pouvoir". Or l'abus de pouvoir peut avoir tendance à mener vers des dérives de nombreuses sortes en ce qui concerne l'excès ou au contraire le laxisme en matière de contrôle de l'information.

Dans le cadre de ce Mémoire, nous allons donc étudier la gestion du risque dans le traitement des informations sensibles. D'un point de vue économique tout comme individuel. Pour cela nous nous attacherons à une approche pragmatique et macroscopique des enjeux possibles d'un tel contrôle et verrons au travers de cas pratiques les conséquences des dérives que cela peut occasionner. Nous analyserons également les méthodes actuelles mises en place pour éviter les risques de fuite d'informations.

C'est à la suite de cette ante-analyse que nous serons capable de mieux comprendre la problématique de notre domaine d'expertise. Par la suite, ce mémoire s'attachera donc à démontrer par le biais de différentes hypothèses comment gérer le risque de fuite d'informations. Pour cela nous prendrons un ensemble de cas pratiques que nous analyserons pour en tirer de possibles recommandations quant aux pratiques actuelles du traitement de l'information.

Nous nous attacherons également à étudier comment les informations du citoyen lambda sont-elles utilisées au sein de notre société et jusqu'à quel point peuvent elles être considérées comme sensibles.

Identité numérique

Les nouveaux usages introduits par l'émergence des dispositifs numériques auxquels nous sommes confrontés quotidiennement ont entraîné un profond changement social quant à l'appréhension des différentes interfaces virtuelles utilisées. De ce fait, malgré l'apparition de normes ergonomiques nouvelles nous y reproduisons les mêmes normes sociales. Nous avons toujours besoin de savoir, dans le cadre d'un échange, qui est notre interlocuteur et quel est son degré de confiance. D'où l'introduction d'informations personnelles réelles au sein de son identité numérique [5]. Ce qui nous amène à nous demander quelle est l'utilisation qui peut être faite de ces données et qui est en charge de son contrôle.

L'histoire nous a enseigné que la nature humaine est capable du pire comme du meilleur. En effet, au regard des évènements passés, l'humanité s'est rendue compte de sa capacité constructive tout comme destructive augmente de manière proportionnelle à l'évolution technologique. Il nous faut donc faire en sorte que le risque d'agissements à mauvais escient soit pris en compte pour pouvoir le pondérer. C'est pour cette raison que nous nous intéresserons aux données personnelles des citoyens pour mieux comprendre l'utilisation et les droits applicables.

Le véritable dilemme de l'identité numérique étant de savoir jusqu'où sommes-nous prêt à divulguer notre vie privée pour le bien de la société ? En effet, nous verrons dans ce mémoire comment mesurer le niveau de compromission d'un système donné par une classification de l'information ciblée et en quoi cela influe-t-il sur notre vie de tous les jours.

Il est également important de noter qu'en plus du contrôle de la divulgation, il existe également une autre approche consistant, tout simplement, à ne pas divulguer l'information ou du moins à la falsifier. Ainsi donc, l'identité d'une personne ne peut pas être déterminée. Ce que nous verrons sera que plus la science avance et plus il devient difficile de contrôler une identité dans le monde numérique.

Récemment un nouveau type de contrôle d'identité a été découvert, il s'agit de la biométrie qui introduit l'étude quantitative du vivant. Ainsi on introduit dans nos systèmes numériques les mêmes systèmes de perception cognitive du vivant.

Ce nouveau domaine dans le contrôle de l'identité nous fait entrer dans un tout autre niveau d'application puisqu'il permet de lier le vivant, par des éléments métaboliques, au

non-vivant. Une innovation par rapport à tout ce qui avait été mis en place précédemment. Cependant, comme tout système de sécurité, ce système possède ses limites et peut être contourné.

Mais, qu'en est-il de la vie privée des usagers de tels dispositifs permettant de lier la vie numérique à la vie réelle ? Imaginons qu'un individu souhaite effacer une

information compromettante par rapport à un évènement passé. Car aujourd'hui, le tout numérique enregistre et archive une quantité faramineuse de données ce qui peut constituer un réel frein à une telle démarche. Cela nous amène à l'hypothèse suivante : plus le contrôle sur les usagers est important, plus l'usager a le pouvoir sur ses données personnelles.

Théories de l'information

Depuis le début de ce mémoire nous utilisons souvent le terme information. Or cette terminologie revêt plusieurs concepts sous-jacents qu'il nous appartient de mieux définir pour bien comprendre la problématique. Pour cela, nous nous appuierons sur les travaux des théoriciens Claude Shannon [1] et Andreï Kolmogorov [4] touchant à la théorie de l'information [1].

Au sein de celle-ci nous différencions les données de l'information. La complexité d'une donnée ne dépend pas de la longueur de la donnée mais bel et bien de la complexité du message véhiculé. On parle alors d'entropie de l'information comme défini par Claude Shannon. Dans la théorie algorithmique de l'information [3] la complexité d'une donnée est définie par la taille du plus petit programme permettant de la fabriquer.

A travers des travaux de ces grands théoriciens, nous nous rendons compte que l'information est une notion bien plus complexe qu'il n'y paraît au premier abord. En effet, celle-ci a une signification contrairement à la donnée brute. Ainsi donc lorsque nous traitons de la confidentialité il faut prendre en compte les facteurs contextuels dépendant des cas applicables. Prenons le cas de la différenciation au niveau

de la législation française, sur laquelle nous reviendrons plus loin dans ce mémoire, applicable différemment en fonction du type de l'information traitée. Par type d'information on parle de sa contenance, de l'émetteur, du récepteur et de sa complexité.

De plus, il faut également prendre en compte les contraintes physiques du stockage de l'information. Certes une information est théoriquement considérée comme intemporelle mais les contraintes s'appliquant aux supports physiques sont on ne peut plus réelles. Il s'avère que tous les supports ont une durée de vie limitée. Cet aspect présenté au sein de la théorie de l'information sous la technique dite des codes correcteurs. Celle-ci introduit le principe de redondance, tant au niveau du stockage qu'au niveau de la transmission. Et ainsi s'assurer de sa pérennité.

L'inconvénient de cette technique étant qu'avec toutes les informations démultipliées, il devient encore plus difficile d'assurer son contrôle. Par contre, si une information a été créée à l'aide d'un algorithme complexe il est d'autant plus difficile de déchiffrer les données véhiculées par ce type d'information.

D'où le postulat suivant : Plus une information est complexe, tel que défini par Kolmogorov, plus elle est sûre.



D'après « *le guide interministériel sur les systèmes d'informations et applications sensibles* » [20], une information sensible est une donnée dont la compromission, l'altération, le détournement ou la destruction, est de nature à nuire à la continuité du fonctionnement des services de l'État et de l'exercice du pouvoir. On peut voir au travers de cette définition que les systèmes de gestion de l'information sont donc un point essentiel au bon fonctionnement de l'appareil d'État.

Il est donc intéressant de se pencher sur les méthodes de confidentialité utilisées au niveau national, de l'Union Européenne et de leurs applications pour ainsi développer une grille d'analyse pouvant mesurer le domaine technologique que nous étudions.

Dans le livre « *La guerre de l'information ou l'éloge de la paranoïa* » [9] écrit par Franck Boulot et Didier Volle, l'intelligence économique, en plus d'être étudiée par le biais de cas concrets, est présentée à l'aide d'une classification intéressante basée sur les niveaux d'accès à l'information.

Dans un premier temps, le renseignement ouvert qui est considéré comme public puis le renseignement semi-ouvert qui est accessible à un personnel autorisé seulement et enfin le renseignement fermé qui lui n'est accessible que par des méthodes alternatives pour les personnes non autorisées.

En outre, nous nous intéresserons au sein de ce mémoire aux risques d'espionnage industriel et des conséquences tout aussi désastreuse d'une mauvaise gestion des secteurs sensibles d'une entreprise industrielle.

Ainsi donc, la qualité d'un système de confidentialité est intrinsèquement liée à la complexité des données, telle que définie par Kolgomorov [4], transitant en son sein. Car comme nous l'avons vu précédemment dans ce document, la sécurité d'une information est fortement liée à la construction algorithmique lui correspondant.

Ceci nous tend à penser que plus une information est gardée secrète, moins il y aura risque de fuite d'information.

Problématique

La problématique à laquelle nous faisons référence dans ce mémoire comporte donc plusieurs volets comme nous avons pu le voir précédemment. Les points purement techniques, économiques, juridiques mais aussi sociaux sont à prendre en considération dans l'analyse de la problématique. Il nous incombe donc de bien définir le périmètre de recherche pour une étude la plus exhaustive possible.

Il existe un grand nombre de facteurs à prendre en compte dans l'étude de la problématique de ce mémoire mais qui se rapportent tous indirectement à la gestion du risque dans le traitement des informations sensibles. Nous ne étudierons également certains autres aspects de la problématique bien qu'ils ne seront traités que de manière superficielle pour mieux comprendre les implications sous-jacentes au contexte sécuritaire. Comme nous nous intéresserons principalement à l'aspect numérique, l'importance sera donné au contrôle numérique de l'information.

L'identité de l'émetteur d'une information est un point clé concernant l'authentification d'un message pour en assurer la confidentialité de l'émetteur au récepteur. Ce postulat, introduit par les théories développées par Claude Shannon et Andreï Kolmogorov,

est d'autant plus vrai aujourd'hui, avec les évolutions technologiques, il est d'autant plus vrai.

Prenons le domaine cryptographique et faisons l'analogie avec la théorie de la complexité de l'information que nous avons présenté plus tôt dans cet article. Les avancées mathématiques considérables qui ont été réalisées depuis la seconde guerre mondiale ont permis la découverte de méthodes de confidentialités nouvelles. Mais elles n'ont pu être mises en œuvre qu'à partir du moment où nous avons découvert les outils capables de mettre en application ces théories.

On peut citer en exemple l'arithmétique des polynômes qui a permis la découverte de la théorie des nombres premiers [24]. Celui-ci a donné naissance au cryptage RSA. De même pour la théorie des courbes elliptiques qui a donné naissance à l'ECC (Elliptic Curve Cryptography). Bref, aujourd'hui les méthodes de confidentialités sont très diverses, d'où une complexification du domaine qui rend la mise en place de procédés cryptographiques indispensable.

En plus des dispositifs numériques, il faut également prendre en considération la mécanique sociétale de fuite d'information induite par la surmédiatisation [5]. En effet, la société contemporaine est en permanence connectée avec le monde extérieur ce qui n'était pas le cas il y a à peine plus de cinquante ans. Cette surconnection entraîne une demande de plus en plus forte en matière d'actualités et de nouveautés. Ceci a pour effet de pousser les médias vers une surenchère de l'information et entraîne dans certains cas des dérives à tel point que la véracité des communiqués n'est pas toujours vérifiée. Il nous faudra donc toujours garder à l'esprit un risque de désinformation. Pour éviter cela nous nous appuierons sur les travaux de chercheurs ou intervenants renommés pour confronter ces différentes sources. Ceci améliorant grandement la qualité des cas d'analyses à défaut d'une étude quantitative difficile dans le domaine.

En somme, nous nous intéresserons donc aux méthodes de confidentialité actuelles et tenteront d'évaluer la pertinence de ces préconisations par le biais de cas pratiques. Ceci nous permettant de répondre à notre problématique qui pourrait être formulée de la forme suivante : La gestion actuelle du risque est-elle adaptée aux risques induits par le traitement des informations sensibles?

L'information revêt une importance cruciale dans nos sociétés moderne comme nous avons pu le voir précédemment. Or il est difficile de mesurer l'impact socio-économique de l'information sur nos sociétés contrairement à d'autres évènements facilement mesurables et quantifiables comme les catastrophes naturelles. Les prises de position et les changement sociaux qu'entraînent la manipulation de l'information ne sont jamais quantifiés. Nous allons donc parcourir quelques unes des conséquences directes ou indirectes du facteur précité. Pour cela, nous devons tout d'abord classifier les enjeux du contrôle de l'information pour nous concentrer sur certains d'entre eux. En effet, traiter ce sujet de manière exhaustive mérirait à lui seul un mémoire ce qui n'est pas le but de ce chapitre.

Tout d'abord nous pouvons faire ressortir assez clairement les enjeux stratégiques. C'est à dire, l'intérêt qu'aurait un État de pouvoir contrôler ses informations stratégiques, de pouvoir les manipuler mais aussi et surtout de pouvoir accéder aux données des autres pays. Les intérêts en jeu peuvent être énormes, c'est pour cette raison que les États les plus influents dépensent sans compter dans le domaine de la sécurité intérieure. Pour preuve, il nous suffit de

lister les services de renseignement de ces États. Aux États-Unis, le Central Intelligence Agency (CIA), la National Security Agency (NSA), le Federal Bureau of Investigation (FBI). En Russie, la direction Générale des Renseignements (GRU), le Service des Renseignements Extérieurs (SVR), et le plus connu, le Service Fédéral de Sécurité (FSB). En Angleterre, le Secret Intelligence Service (SIS), le Security Service (MI5). Et en France, la Direction centrale du renseignement intérieur (DCRI) qui regroupe plusieurs services de renseignement. Comparons maintenant les budgets estimés des dépenses en matière de renseignement pour ces pays. Aux États-Unis, en 2010, Le bureau du Directeur de l'Intelligence Intérieure a présenté un budget de 53,1 milliards de dollars pour le programme d'intelligence intérieure [14] [15]. En France, ce budget s'élève à 34,3 millions d'euros d'après le projet de loi n° 2009-973 de règlement des comptes et rapport de gestion pour l'année 2008. Nous pouvons voir à travers ces données statistiques que les enjeux au niveau étatique sont pris très au sérieux et qu'il sont un vecteur stratégique essentiel à la prise de décision et à l'application du droit par les décideurs.

En plus du domaine gouvernemental, il y a également la dimension économique à prendre en compte. La majorité de nos sociétés contemporaines étant basée sur le capitalisme nous allons voir les enjeux concernant les biens et les savoirs sous-jacents. Le milieu financier, par exemple, est très friand des informations concernant les cours de la bourse. C'est pour répondre cette demande à cette problématique que sont nées les agences de notation permettant de connaître la qualité d'un placement boursier.

Aujourd'hui trois agences de notations se partagent 94% du chiffre d'affaire dans ce secteur : Moody's qui au quatrième trimestre 2010, a affiché des bénéfices de 137,4 millions de \$US. Standard & Poor's avec 153,8 millions de \$US. Fitch Ratings avec 145 millions de \$US. Avec un total de 436,2 millions de \$US ce qui montre l'importance attachée à l'information dans ce secteur primordial de l'économie.

Plus en avant, le domaine de la vie privée est un enjeu à prendre également en compte. Avec l'émergence de réseaux de tous types, il devient de plus en plus compliqué de garantir la confidentialité d'une information. En particulier celles à caractère personnel qui sont tout particulièrement recherchées par certaines organisations gouvernementales

et commerciales. Dans certains cas pourtant ces données peuvent revêtir une importance cruciale pour l'intégrité des citoyens comme dans le cas d'opposants politiques.

C'est pour cette raison que de nombreuses entreprises se sont créées dans ce secteur d'activités. Celui-ci pouvant être très large allant de la simple récupération d'adresses email jusqu'à la mise sous surveillance d'une partie de la population. Prenons l'exemple du réseau d'écoute planétaire dont l'existence a été révélée par le scandale du Watergate aux États-Unis. Cet évènement ayant conduit à la démission du président américain Richard Nixon en 1974, il a permis, grâce à l'enquête menée par le département de la justice des États-Unis, la mise en lumière un réseau d'écoute satellitaire d'envergure mondiale. Ce système ayant été déployé en Australie, au Canada, aux États-Unis, au Royaume-Uni et en Nouvelle-Zélande. Une délégation de la commission européenne a publié un rapport complet sur ce projet [11]. Au niveau national, un réseau d'écoute existe également et a été surnommé le réseau Frenchelon dont le but est également de capturer les communications écrites et audios en vue d'un archivage ou d'une analyse.

Ces réseaux possèdent une légitimité dans le domaine de la lutte antiterroriste puisqu'il a déjà démontré son utilité. Par contre, l'obscurantisme qui l'entoure entraîne toutes sortes de théories. Mais si nous prenons les faits, l'évolution des écoutes téléphoniques a été évalué à 5845 en 2002 pour passer à 35000 aujourd'hui. On peut voir alors que des systèmes initialement prévus pour le domaine militaire, en rapport avec la sécurité nationale, sont en partie détournés vers le domaine civil.

On peut citer le décret n° 2008-632 du 27 juin 2008 portant création d'un traitement automatisé de données à caractère personnel dénommé « EDVIGE » dont l'objectif tel que décrit dans le texte législatif lui-même est le suivant :

« Le ministre de l'intérieur est autorisé à mettre en œuvre un traitement automatisé et des fichiers de données à caractère personnel intitulés EDVIGE (Exploitation documentaire et valorisation de l'information générale) ayant pour finalités, en vue d'informer le gouvernement et les représentants de l'État dans les départements et collectivités :

1. De centraliser et d'analyser les informations relatives aux personnes physiques ou morales ayant sollicité, exercé ou exerçant un mandat politique,

syndical ou économique ou qui jouent un rôle institutionnel, économique, social ou religieux significatif, sous condition que ces informations soient nécessaires au Gouvernement ou à ses représentants pour l'exercice de leurs responsabilités ;

2. De centraliser et d'analyser les informations relatives aux individus, groupes, organisations et personnes morales qui, en raison de leur activité individuelle ou collective, sont susceptibles de porter atteinte à l'ordre public ; [...] »

On peut alors se demander qu'elle peut être l'utilisation fait d'un tel fichier et s'il n'y a pas un risque de fuite d'information. Surtout lorsqu'elles sont particulièrement recherchées par des sociétés privées dont les bénéfices reposent sur ce type d'activités. On peut citer en exemple la société ChoicePoint qui a commencé dès 1997 à récupérer des informations personnelles de citoyens américains et à revendre ces informations à l'industrie de l'assurance. L'évolution de l'entreprise fut fulgurante puisque sa valeur est passée de 500 millions de \$US avec un millier de clients à 4,1 milliards de \$US avec plus de 50 mille clients nous pouvons alors voir à quel point ces informations sont devenues importantes [12].

Pour finir, d'un point de vu social, la manipulation de l'opinion publique par le biais de la désinformation est une composante du contrôle de l'information. En effet, le terme même d'opinion publique est mis en doute dès 1971 par certains philosophes comme Pierre Bourdieu [16] lors de sa conférence d'Arras, on peut se demander alors si les sondeurs eux-mêmes ne sont-ils pas des créateurs de conscience.

Lors de sa présentation, Pierre Bourdieu annonce que le sondage d'opinion implique avant même de questionner les participants qu'il existe un consensus sur les problématiques à poser. Ainsi, les influences des institutions chargées des études d'opinion est un vecteur d'influence dans la fabrication d'une opinion publique imposant sa majorité. Ce thème est traité plus en profondeur par Noam Chomsky, Edward S. Herman dans l'ouvrage « *Manufacturing Consent: The Political Economy of the Mass Media* » [17] où les auteurs analysent 40 ans de lobbying médiatique aux États-Unis. De même que dans l'ouvrage de Lawrence R. Jacobs et Robert Y. Shapiro « *Presidential Manipulation of Polls and Public*

Opinion: The Nixon Administration and the Pollsters » [18] où les auteurs analysent en profondeur les coulisses de la création de sondage sous l'administration Nixon et les rapports entre les politiques et les instituts de sondage. On peut voir au terme de cet ouvrage que les opinions publiques qui ressortent de telles études sont très souvent biaisées par des intérêts différents de la restitution de la vérité. Au niveau national, cette opinion est appuyée par l'ouvrage de Patrick Champagne, « *Faire l'Opinion. Le nouveau jeu politique* » [19] où est démontré l'influence, qu'ont les spécialistes quant à l'analyse socio-politique de l'actualité, sur l'opinion publique.

Ainsi donc nous avons vu, dans ce chapitre, l'importance des enjeux derrière la confidentialité des informations. Certains gouvernements et certaines entreprises disposant de moyens que l'on peut qualifier de considérables sont très friands d'informations sensibles. Nous voyons alors clairement qu'une donnée est compromettante si et seulement si une entité connaît son existence et qu'elle est intéressée par ce qu'elle contient.

Information cachée

Après avoir vu les enjeux derrière la prise de contrôle de l'information nous allons nous intéresser maintenant à l'aspect quantitatif de la confidentialité de l'information.

En effet, lorsqu'une information est cachée elle est tout de même accessible aux individus connaissant son existence qui peuvent eux-mêmes avoir alors des niveaux d'accès différents à la même information. La question est donc de savoir s'il existe une corrélation entre le nombre de personnes ayant accès au renseignement avec le risque qu'une personne tiers se l'approprie.

Pour cela nous allons voir que cela dépend grandement de l'information en question et des moyens mis en oeuvre pour la récupérer. Mais avant cela il nous faut mettre en place une classification pour une meilleure analyse. Nous prendrons celle proposée par Franck Boulot et Didier Violle dans l'ouvrage "La guerre de l'information ou l'éloge de la paranoïa" quant aux niveaux d'accès à une donnée.

Dans cet ouvrage, les auteurs catégorisent trois types d'informations, le niveau le plus accessible étant la zone blanche correspondant à un renseignement ouvert, publiquement accessible, dont le recueil n'entraîne aucune infraction. Ce niveau

correspond à près de 90% des données qui circulent sur nos réseaux. S'ensuit la zone grise correspondant à un renseignement sensible dont l'accès est limité aux personnes autorisées mais dont le recueil n'est pas illégal bien que soumis à jurisprudence en fonction des cas. Ce niveau correspond à un pourcentage croissant d'informations circulant sur les réseaux. Pour finir, la zone noire correspondant à une information sensible dont l'accès est très limité et dont le recueil entraîne des poursuites judiciaires systématiques. On estime qu'elles correspondent à 10% de l'information circulant sur le réseau. Cette analyse nous montre clairement qu'en fonction du niveau de classification, l'accessibilité est plus ou moins grande, tout du moins sans risque de sanctions pénales. Mais bien que plus complexe et risqué à obtenir c'est le type de renseignement jugé à forte valeur ajoutée qui est recherché contrairement à l'information publique qui n'a peu ou pas d'intérêt. C'est pour cela que la protection de l'information est grandement assurée par des procédés de limitation d'accès.

Certaines organisations dissidentes ont appliqué ce principe de limitation de l'accessibilité cela fait déjà de nombreuses années. En exemple, nous pouvons citer les teutoniques, qui ont dès la création

de leur ordre, commencer à entourer de mystère leur existence avant de divulguer des informations au compte goûte pour se faire reconnaître par la papauté [10]. Les groupes terroristes utilisent aussi ce genre de pratique et sont répartis en cellules autonomes mais connectées entre elles. Cette pratique est également reproduite au sein de groupes criminels qui sont quant à eux soumis au secret souvent sous peine de condamnations de justice. La possibilité de récupérer des renseignements sur l'ensemble de l'organisation est donc grandement diminuée puisque seule une poignée de personnes a accès à l'ensemble des savoirs de la zone noire.

Par contre l'accès aux informations publiques est quant à lui beaucoup plus facile et offre, dans de nombreux cas, la possibilité d'accéder à un niveau supérieur de renseignement, la zone dite grise. C'est tout l'intérêt de l'analyse quantitative opérée par les services de renseignement à travers les réseaux précédemment cités tels que le projet Echelon ou encore Frenchelon au niveau national. Ils n'offrent pas l'accès direct au renseignement mais permettent de guider la recherche d'information de classification plus élevée.

Bien, nous avons vu que l'étude quantitative entraîne une plus-value intéressante pour une recherche de renseignement de qualité. Certes dans le cas d'un réseau organisé avec des limitations d'accès, cette technique est extrêmement efficace mais dans le cas où le renseignement est caché dans la zone blanche ? Et bien cette approche par l'étude quantitative se révèle être inefficace.

Pour mieux comprendre cela nous devons nous intéresser à une composante particulière du domaine de la cryptologie, la stéganographie. Il s'agit alors d'arriver à cacher un renseignement classifié dans une information au premier abord anodine. S'il existe un récepteur illégitime ne savant pas qu'il existe une information cachée dans le message, comment peut-il réaliser une étude qualitative dessus ?

La stéganographie existe depuis très longtemps puisqu'on a des traces de l'utilisation de cette dernière dès 1830 dans des courriers envoyés par Georges Sand à Alfred de Musset. Certes il s'agit d'une méthode stéganographique assez grotesque et qui pourrait être surtout détectée. Avec l'évolution technique contemporaine des systèmes d'information et de communication, il devient tout à fait envisageable de mettre en place un système de détection de tels

procédés sur une masse conséquente de données. D'où l'émergence de techniques de plus en plus poussées pour dissimuler un renseignement. Pour chaque média, il existe une technique lui correspondant : le format texte avec les techniques de l'acrostiche ou de l'eidesis mais aussi la photographie avec la technique basée sur le théorème chinois des restes [26] ou encore la manipulation de la palette de couleurs et bien d'autres.

L'information cachée est donc un moyen comme un autre de passer outre une étude quantitative tout en n'attirant pas l'attention par limitation d'accès. La difficulté résultant dans le fait que personne ne doit découvrir qu'il existe un renseignement caché. Dans ce dernier cas, il est tout à fait possible de combiner les techniques cryptographiques et stéganographiques pour que le message soit caché et que, même en cas de fuite, que le renseignement soit protégé.

Un autre intérêt d'inclure un message caché dans un média est de pouvoir vérifier la non altération du message initial. En effet, imaginons le cas où un texte contenant un message caché soit modifié par un intermédiaire n'étant pas conscient de sa présence. Le texte est mais le contenu caché ne seront altérés. Dans le domaine du numérique on appelle cela le tatouage

électronique. Il est utilisé dans de nombreux cas de signature numérique de documents. Dans l'imagerie il est possible de modifier une image en y ajoutant une marque invisible pour la protection du droit d'auteur.

Plus globalement on appelle cela la Gestion des droits numériques, ou encore, le Digital Rights Management (DRM). Cette limitation de diffusion d'une ressource sur les différents supports numériques a entraîné un vrai débat. Par exemple au sein de la communauté du logiciel libre, Linus Torvalds, fondateur du système d'exploitation GNU Linux, a créé un tollé en annonçant qu'il refuse d'adopter la licence GPL 3 (licence déclarant les sources d'un logiciel accessible et modifiable par tous) car celles-ci interdit le déploiement de systèmes de type DRM [11] :

« *On Wed, 25 Jan 2006, Chase Venters wrote:*
 > *This means that when the code went GPL v1 -> GPL v2, the transition was permissible.*
*Linux v1.0 shipped with the GPL v2. It did not ship with a separate clause specifying that «You may only use *this* version of the GPL» as it now does. (I haven't done any research to find out when this clause was added, but it was after the transition to v2).*

Bzzt. Look closer.

The Linux kernel has always been under the GPL v2. Nothing else has ever been valid. The «version 2 of the License, or (at your option) any later version» language in the GPL copying file is not – and has never been – part of the actual License itself. It's part of the explanatory text that talks about how to apply the license to your program, and it says that if you want to accept any later versions of the GPL, you can state so in your source code.

The Linux kernel has never stated that in general. Some authors have chosen to use the suggested FSF boilerplate (including the «any later version» language), but the kernel in general never has.

In other words: the default license strategy is always just the particular version of the GPL that accompanies a project. If you want to license a program under any later version of the GPL, you have to state so explicitly. Linux never did.

So: the extra blurb at the top of the COPYING file in the kernel source tree was added not to change the license, but to clarify these points so that there wouldn't be any confusion.

The Linux kernel is under the GPL version 2. Not anything else. Some individual files are licenceable under v3, but not the kernel in general.

And quite frankly, I don't see that changing. I think it's insane to require people to make their private signing keys available, for example.

I wouldn't do it. So I don't think the GPL v3 conversion is going to happen for the kernel, since I personally don't want to convert any of my code.

> If a migration to v3 were to occur, the only potential hairball I see is if someone objected on the grounds that they contributed code to a version of the kernel Linus had marked as «GPLv2 Only». IANAL.

No. You think «v2 or later» is the default. It's not. The default is to not allow conversion. Conversion isn't going to happen.

Linus »

Nous voyons dans son intervention que le choix ou non de protéger une oeuvre numérique ne revient pas aux développeurs mais aux artistes à l'aide des licences Creative Commons.

Dispositifs numériques

Dans la première partie de ce mémoire nous avons pu mieux cerner le périmètre de notre problématique. Sur le terrain numérique cette problématique nous force à nous porter vers l'aspect technique de la sécurisation de l'information.

En effet, l'informatique étant un domaine de hautes technologies et souvent en interactions avec la confidentialité de l'information nous allons faire un rapide tour des dispositifs numériques qu'il est possible de rencontrer durant notre analyse de la gestion du risque dans le traitement des informations sensibles.

Tout d'abord nous devons différencier les dispositifs physiques (hardware) des dispositifs logiciels (software). De plus, bien que nous nous intéressons à l'aspect numérique de la sécurité de l'information nous devons également prendre en compte les cas où l'exploitation d'une fuite d'information se fasse par le vecteur humain de la problématique.

Dans ce cas, le dispositif technique importe peu puisqu'il s'agit d'une motivation humaine qui peut être individuelle ou collective de corruption de données. Ce cas sera abordé dans ce mémoire mais ne prendra pas une part importante puisqu'il

implique un aspect plus psychologique. Ce qui relève d'un domaine d'expertise différent de celui que nous souhaitons aborder dans ce mémoire mais reste à prendre en compte.

Nous nous concentrerons donc plus sur le côté technique au sein de ce mémoire puisque nous souhaitons étudier les usages des dispositifs numériques ou plutôt de leur détournement à des fins non avouables. En effet, leur omniprésence, tant au niveau gouvernemental en ce qui concerne les informations d'état que au sein des entités économiques et financières ou encore en matière de gestion des informations personnelles, prend une place de plus en plus critique dans le traitement de l'information sensible.

Dans tous les cas, les méthodes de confidentialité sont applicables, à des niveaux de complexité différents, et nous devons donc nous y pencher pour une meilleure compréhension de la problématique. Le contrôle de l'information regroupe donc plusieurs domaines d'expertises et revêt des enjeux sociaux, économiques, gouvernementaux mais aussi militaires comme vu précédemment.

C'est pour cela que nous allons voir dans la suite quelles sont les réponses apportées par la normalisation des méthodologies appliquées au contrôle de l'information. Mais aussi les conséquences juridiques que cela implique au niveau des organisations gouvernementales Française et Européenne.

Mais avant cela, il nous faut mieux comprendre les mécaniques de contrôle de l'information. Celui-ci étant régit par trois grands principes : l'authenticité, la confidentialité et la sécurité.

L'authenticité permet de savoir si l'émetteur du message qui nous est transmis peut être considéré comme sûr. C'est pour cette raison que nous avons introduit la notion d'identité numérique à ce mémoire.

La confidentialité permet de s'assurer que le message transmis n'a pas été divulgué à un autre destinataire que celui à qui il était destiné. D'où l'introduction de la notion stéganographique en début de ce mémoire.

Et enfin la sécurité qui nous permet de nous assurer que personne d'autre que le destinataire n'a pu lire le message qui a été transmis. Cette dernière composante quant à elle est assurée par une autre branche des sciences de l'information et de la communication, la cryptologie.

Cryptologie

Introduction

Au fil de l'Histoire, la confidentialité des informations a été assurée par différents moyens que nous allons voir ci-après. Ces méthodes, toutes plus diverses et variées, ont souvent été le fruit d'un besoin de sécuriser les informations transmises en temps de crise. C'est ainsi que de nombreuses techniques pour assurer la sécurité de l'information ont été inventées.

[21]

L'un des premiers texte sur les procédés cryptographiques [22] [23] est daté du IV^e siècle avant J.C. Il s'agit du chapitre 31 de la Poliorcétique d'Enée le Tacticien. Ainsi donc les premières techniques de confidentialité de l'information étaient basées sur un système de transposition. Celui-ci fonctionne en remplaçant les groupes de lettres dans un message par d'autres puis il est ensuite possible de retrouver le message d'origine en effectuant le remplacement inverse. Pour cela il est généralement nécessaire d'avoir la clé qui a été utilisée pour crypter le message.

L'un des dispositif de cryptage basé sur cette technique est le code de César datant du le siècle avant J.C. Le principe est simple, il suffit de décaler toutes les lettres du message d'un nombre n :

si $n = 3$, A se transforme en D, B en E, etc... Ainsi si l'on connaît la valeur de n il est facile de décrypter le message. Malheureusement un tel cryptage est bien trop facile à décoder puisqu'il n'existe que 26 (autant de lettres que l'alphabet) possibilités de permutations.

Un autre système de cryptage révolutionnaire pour l'époque est le chiffre de Vigenère apparu en 1586 et décrit par le diplomate français Blaise de Vigenère. Cette technique de chiffrement utilise un mot de passe et une grille visible en Annexe 1. La technique du chiffre de Vigenère consiste à s'aider de la grille de la manière suivante : prenons le mot de passe « MYSTERE » et le texte à crypter suivant « VIGENERE ». A l'aide de la grille, nous allons chercher sur la première ligne la première lettre du texte à chiffrer V, sur la première colonne, la première lettre du mot de passe M. L'intersection des deux nous donne la première lettre du message crypté et ainsi de suite. Cette technique de cryptage n'a été décryptée qu'en 1854 soit près de 300 ans après son apparition.

Pour finir, nous parlerons brièvement du système de cryptage Enigma utilisé pendant la seconde guerre mondiale par la marine Allemande. Ce système de cryptage utilise une machine Enigma, visible en Annexe 2, qui permet de commuter les lettres du message de façon variable rendant le décryptage assez complexe.

A notre époque contemporaine, la technique aidant, les procédés se sont grandement complexifiés. Mais nous pouvons étudier deux aspects essentiels dans la compréhension de la problématique. La cryptographie symétrique et la cryptographie asymétrique. [25]



Cryptographie symétrique

La cryptographie symétrique est la forme la plus ancienne de cryptographie. Elle est basée sur l'échange d'une clé secrète que seules les deux parties se transmettent l'information et connaissent la constitution.

La clé peut revêtir plusieurs formes très diverses. Comme la clé n'est connue que des deux parties, on l'appelle clé privée.

De plus il existe plusieurs types de chiffrement symétrique : le chiffrement par bloc et le chiffrement par flot. L'un utilise un ensemble de données avant d'appliquer l'algorithme de chiffrement tandis que l'autre effectue le chiffrement par bloc de données.

Ces algorithmes utilisent principalement une technique mathématique basée sur la difficulté de factorisation de grands nombres premiers rendant le cassage du chiffrement très coûteux en temps de calcul.

Cette notion de secret partagé privé est très importante car avec l'apparition des nouvelles technologies est apparue la problématique de l'échange de cette clé privée de façon sûre. De ce nouveau besoin a donc découlé l'apparition de la cryptographie asymétrique qui introduit la notion de clé publique expliquée dans le chapitre qui suit.

Cryptographie asymétrique

La cryptographie asymétrique quant à elle se base sur des notions mathématiques plus récentes et tente de répondre à la problématique posée par l'échange de données de façon sécurisée. La cryptographie asymétrique fonctionne sur un système de paire de clés publique et privée. L'utilisateur génère une paire de clé, l'une est publique et peut être distribuée à des tiers ce qui leur permettra de chiffrer des messages et l'autre, privée, doit être conservée pour pouvoir déchiffrer les messages. Ce procédé est possible grâce à des propriétés mathématiques qui rendent le décryptage beaucoup trop long seulement avec la clé publique. Il est principalement basé sur la factorisation des nombres premiers.

Cette nouvelle méthode de cryptage entraîne une véritable révolution dans la communication cryptée. En effet, la possibilité de communiquer sa clé de cryptage publique à tout le monde permet d'être sûr de pouvoir être le seul à décrypter le message tout en diffusant de manière sécurisé sa clé publique.

Cette différenciation entre les deux cryptographies revêt un aspect essentiel pour la suite de cet article qui traitera brièvement de la législation en vigueur en matière de confidentialité de l'information.

Stéganographie

L'informatique étant intimement lié aux mathématiques, il paraît assez naturel de retrouver une analogie entre les systèmes cryptographiques et les mathématiques. [40] En effet, tout comme dans les langages formels, l'accès à l'information se soumet à certaines règles. Par analogie, une information chiffrée serait récessive au sens mathématique puisque l'information est alors considérable comme "finitiste" tandis que la stéganographie par déni, dont nous parlons ci-après, a des propriétés expansives. Puisque plus d'informations sont interceptées et plus il y a de scénarios de fuites possibles.

Comme nous avons vu précédemment, la stéganographie est une branche de la cryptologie. Elle consiste à assurer la sécurité d'une information par le secret plutôt que par la complexité. La stéganographie numérique consiste à transmettre un média au sein d'un autre média source tout en conservant la qualité du média d'origine. Le but étant de transmettre cette information cachée de manière transparente, il faut que le média d'origine paraisse le plus banal possible.

Il est possible de faire l'analogie avec un convoyeur de fond : le cryptage serait un convoyeur transférant de l'argent par le biais d'un camion blindé alors que la stéganographie serait un convoyeur utilisant une voiture banalisée pour le transfert. Enfin, il est tout à fait possible de combiner ces deux techniques, on aurait alors un convoyeur en camion blindé ayant été préalablement banalisé.

Il est également possible d'aller plus loin. En effet, si un émetteur cherche à transmettre un message sans que celui-ci ne soit intercepté, il est dans son intérêt de brouiller les pistes. Pour cela il suffit d'envoyer un ensemble de messages qui se ressemblent mais dont seulement un contient le secret désiré. Pour faire l'analogie, prenons notre convoyeur de fonds qui décide qu'avec ses collègues, chacun prendra un véhicule et chacun utilisera une route différente pour arriver au même point d'arrivée en même temps que notre convoyeur emmènera avec lui la marchandise à transporter. Il devient alors très compliqué d'intercepter tous les véhicules et de les vérifier un à un. Cette technique est appelée stéganographie par déni car elle permet, dans le cas où l'ensemble des informations est interceptée de nier la présence d'un message caché.

On peut citer certains outils permettant la mise en place de telles techniques. Par exemple l'outil spammimic qui permet de camoufler un message dans un mail ayant l'apparence d'un spam. Mais aussi l'outil OpenPuff qui est très complet puisqu'il permet de cacher un message sur des médias visuels, audio ou vidéo entre autres. Il est même possible de cacher des messages dans les instructions d'un programme informatique comme le propose l'utilitaire hydan. Pour aller encore plus loin, StegFS permet quant à lui de cacher des informations directement dans le système de fichier de l'ordinateur.

Ces techniques de communication cachées sont un plus non négligeable pour le respect de la vie privée. En effet nous avons vu dans

le chapitre des enjeux que l'information prend de plus en plus d'importance et que nos données privées sont extrêmement recherchées par les gouvernements et les industries de l'information. Malheureusement avec l'anonymat viennent aussi les risques intrinsèques au camouflage ou l'usurpation d'identité comme vu en début de mémoire. On peut citer en exemple un article paru dans le USA Today qui montre que dès 2001 le groupe terroriste Al-Qaida utilisait la stéganographie en cachant des messages dans des versets du coran ou dans des vidéos pornographiques postées sur internet [35]. Faits corroborés par le journal allemand Die Ziet dans un article paru le 1er Mai 2012. Ainsi comme tout dispositif technique, seul l'utilisateur final peut choisir la qualité de ses actions et son bien fondé.

Législation

Pour étudier d'un point de vu étatique le traitement des informations à risque, il nous faut aborder l'aspect législatif. En effet, la législation est l'outil permettant de mettre en place et de faire respecter les lois en matière de protection de données ce qui nous permet d'avoir une approche différente du sujet.



Communauté Européenne

Il est stipulé qu'en matière de confidentialité et d'accès à l'information, les directives Européennes [27] sont prioritaires par rapport aux législations en vigueur au sein des pays membres. C'est pour cette raison que nous nous intéresserons brièvement à la législation européenne en matière de gestion de l'information.

L'une des premières conventions établies par le Conseil de l'Europe est la convention de sauvegarde des Droits de l'Homme et Libertés fondamentales. En effet, Selon l'article 8 de cette convention, «toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance». S'en est suivi l'adoption des Résolutions 22 en 1973 et 29 en 1974 qui précisent les principes de la protection de données à caractère personnel. Mais c'est seulement en 1981 que la Convention 108 a été votée. Cette dernière prévoit un certain nombre de limitations quant aux données collectées mais également la possibilité de les communiquer aux autres gouvernements ayant ratifiés la Convention mentionnée précédemment. Elle est également accessible aux états non membres de l'Union Européenne.

Pour limiter alors les risques d'utilisation abusive d'informations à caractère privé, les différents états de l'Union Européenne sont aptes à définir une autorité compétente chargée de la protection des citoyens.

Comme la Délégation Fédérale à la protection des Données (BnD) en Allemagne ou encore la Commission Nationale de l'informatique et libertés (CNIL) et bien d'autres. Ces organismes indépendants sont donc des remparts importants pour la protection des citoyens européens.

France

En France, la loi du 26 Juillet 1996 qui fait référence à la protection des informations et au développement des communications et des transactions sécurisées, fut une des premières lois reconnaissant la légitimité de l'utilisation de la cryptographie par les citoyens. Autant dire que le domaine est extrêmement récent et a beaucoup évolué en très peu de temps. [33]

C'est ainsi qu'un certain nombre de législations diffèrent en fonction de l'utilisation des techniques cryptographiques. Il existe une séparation entre les fonctions d'authentification et d'intégrité des données et les fonctions de confidentialité. Les premières sont soumises à un régime plus libéral contrairement aux dernières. En effet, la loi introduit la notion de « tiers de confiance » en ce qui concerne la confidentialité des données. Ces tiers de confiance doivent donc être avalisés par l'état pour permettre le déploiement futur de certificats.

Historiquement, la législation prévoyait vers la fin des années 1990 et plus précisément par un arrêté du 13 Mars 1998 applicable au régime de déclaration, soit à un échange d'informations confidentielles, une limitation quant à la taille maximale des clés utilisées. Cette limite étant de 2 puissances

40 combinaisons, soit une clé de 40 octets au maximum. Autant dire qu'avec une telle limitation de taille de clé et la puissance de calcul actuel des ordinateurs personnels, le cryptage des informations serait très vite devenu obsolète. C'est pour cette raison que la loi a été revue.

La loi du 21 Juin 2004 pour la confiance dans l'économie numérique revient sur de nombreux points en matière de cryptographie. C'est ainsi que, dans un objectif de mise en confiance des usagers dans les moyens de confidentialité sur internet mais aussi pour une harmonisation avec la législation européenne, l'utilisation des moyens de cryptologie devient libre que ce soit pour des fonctions d'authentification, réalisées en général avec du cryptage asymétrique, et de confidentialité, souvent effectuées à l'aide d'un échange de clés privées.

Bien qu'un assouplissement des méthodes cryptographique ait été mis en place, les tiers de confiance, sont toujours soumis aux mêmes obligations. Secret professionnel et déclaration auprès d'un organisme d'état voire auprès du Premier ministre pour les sociétés proposant des prestations cryptographiques. [34]

Plus récemment plusieurs lois ayant trait aux informations personnelles ont vu le jour et ont été assez médiatisées. Le projet de loi Création et Internet qui a conduit à la création de la Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (HADOPI) ou encore la loi d'Orientation et de Programmation pour la performance de la sécurité intérieure (LOPSSI).

Au niveau professionnel, un certain nombre de lois ont été adoptées [28] pour protéger les salariés d'un risque de récupération de données par leurs employeurs, tout du moins pour les informations à caractère privées.

Normalisation

Les normalisations permettent de mettre en application l'ensemble des préconisations prévues par les spécifications concernant la gestion de l'information. De ce fait nous abordons le sujet pour permettre un tour d'horizon complet de la problématique.

D'après Marie-Anne Chabin, présidente d'Archive 17 [29] une normalisation est une spécification technique accessible au public qui a été approuvée par une organisation reconnue. Ce document est destiné à fournir un avantage optimal pour la communauté et favorise les échanges et la standardisation entre les différentes parties.

Concernant l'archivage des informations il existe deux domaines : la gestion de l'information et des archives électroniques puis l'archivage et la conservation numérique. Ce domaine est appelé par les anglophones le record management.

Le schéma en Annexe 3 présente un panorama des normalisations existantes. Nous nous intéresserons plus particulièrement au Moreq2 qui est une préconisation formulée par l'Union Européenne concernant l'archivage et la conservation des données. Au plan national, le standard NF Z42 013 fait référence en la matière.

Communauté Européenne

Les préconisations du Moreq2 sont très complètes quant à la gestion des données archivées (plus de 200 pages). Nous allons voir ici très brièvement quelques uns des points abordés qui correspondent à la problématique que nous souhaitons traiter.

Tout d'abord il est à noter que l'ensemble de cette standardisation tourne autour des ERMs (Electronic Records Managements System) qui proposent de relier le système d'archivage à d'autres dispositifs tiers ayant prouvé leur fiabilité.

Concernant la sécurité de l'information, le Moreq2 fournit des préconisations concernant l'accès aux informations, les données critiques, les outils et méthodes de sauvegarde et de récupération des données et enfin sur les systèmes d'enregistrement.

Par rapport au système d'accès, il est recommandé d'appliquer une politique de permissions par groupe et non par personne. Il faut également un compte administrateur capable de gérer les groupes

et les rôles attribués à ceux-ci. De plus, il est recommandé de ne pas fournir d'information à un utilisateur tiers sur les données des autres utilisateurs (via un outil de recherche ou autre) ainsi que d'autres préconisations comme montré dans l'Annexe 4.

Par rapport aux méthodes à appliquer à la gestion des informations vitales et à fortiori aux sauvegardes, l'accent est donné au rôle de l'administrateur. Celui-ci doit être le seul capable d'effectuer et de restaurer une sauvegarde de toutes les données du système.

Ces préconisations adoptent un point de vu théorique sur les mécanismes de prévention de fuite d'informations. Malheureusement on peut regretter le manque d'expertise dans les techniques cryptologiques de ce document. En effet la mise en application d'un système cryptographique n'est exprimée que brièvement ce qui, comme nous l'avons montré, est un facteur indispensable pour garantir l'intégrité de l'information.

France

Les précurseurs en matière d'archivage et de confidentialité d'accès à l'information sont un certain nombre d'archivistes reconnus tels que Jean-Yves Rousseau, Carol Couture mais aussi Luciana Durati avec son étude sur la gestion des documents intitulée « *The Odyssey of the Record Management* ». Ces travaux novateurs pour l'époque, début des années 90, introduisent la problématique de la gestion et de l'organisation des données archivées. D'où l'apparition d'un certain nombre de normes pour répondre à cette problématique.

En France, on peut citer la norme NF Z42-013 qui fait référence en la matière. Cette norme est directement tirée de l'ISO 15489 [30] qui elle est une standardisation internationale sur la gestion des données archivées. Elle reprend un certain nombre d'éléments de la MoReq2 précédemment citée. Parmi ceux-ci on peut citer l'assignation de responsabilités et de droits d'accès ainsi que la mise en place d'un système d'administration. On peut voir dès lors que les préconisations concernant la gestion des données au niveau national sont sensiblement les mêmes qu'au niveau européen.

D'un point de vu de sécurité nationale, il existe le RGS (Référentiel Général de Sécurité) [31] ainsi que la norme EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) qui sont des méthodologies d'amélioration de la sécurité des systèmes d'information. Le RGS a été créé conjointement entre la Direction générale de la modernisation de l'État (DGME) et l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Il décrit les différentes fonctions sécuritaire telles que la confidentialité, l'authentification, la signature électronique ou encore la politique de certification. Il permet de se familiariser avec les concepts de la sécurité informatique. L'EBIOS quant à lui est une méthodologie applicable dans la construction du référentiel de sécurité informatique et dans la gestion des risques. Cette méthodologie est plus un conseil sur les points importants à prendre en compte lors de la création de son système d'information avec une étude préalable du contexte, la mise en place de scénario d'attaque en découlant, l'analyse du risque induit, les méthodes de sécurisation et enfin les problèmes auxquels l'entité peut être confrontée à la suite de cela [7].

De manière moins étatique mais toujours au niveau national, le CLUSIF (Club de la Sécurité de l'Information Français) a développé la méthode MEHARI (méthode harmonisée d'analyse des risques). Cette méthode permet de bien identifier les entités du système d'information et donc de pouvoir choisir avec une meilleure granularité les règles sécuritaires à y appliquer.

Dès lors se posent les mêmes questions que pour les préconisations de niveau européen. Questions auxquelles nous tenteront de répondre en émettant un certain nombre d'hypothèses que nous nous appliquerons à mesurer en présentant la démarche utilisée.

Hypothèses

L'ensemble des points vus précédemment nous permettent un éclaircissement du terrain de recherche par une analyse histologique et pluridisciplinaire. Nous pouvons ainsi avoir un aperçu des travaux réalisés dans le domaine.

Grâce à ces différentes analyses recueillies parmi les travaux de certains théoriciens des sciences de l'information et de la communication, des sciences sociales ou encore économiques, nous voyons que l'intégrité numérique a une importance primordiale dans les secteurs sensibles diplomatiques, militaires, économiques et sociaux. La connaissance d'un secret, s'il est révélé à des personnes mal intentionnées, peut entraîner la perte d'un avantage ou une dégradation du niveau de sécurité. Il s'agit donc d'un domaine difficile d'étude en raison du manque d'accessibilité de données en la matière.

Malgré tout nous tenterons, en formulant un ensemble d'hypothèses, d'essayer de mesurer la gestion du risque dans le traitement des informations sensibles et personnelles. Pour cela nous établirons un ensemble de paramètres mesurables aidant à l'analyse et à la réduction du risque

de corruption d'un dispositif numérique. Pour cela il convient d'avoir une approche macroscopique englobant les vecteurs d'intrusion du plus au moins critique. Ceci permettant d'améliorer la sécurité des systèmes d'informations de n'importe quelle entité possédant une infrastructure informationnelle.

En ce qui concerne le domaine étatique, les risques sont quant à eux multiples. Les dommages provoqués par une fuite d'information au niveau national voir international peut entraîner des conflits diplomatiques. Mais il peut aussi être un risque bénéfique de transparence pour les citoyens. D'où l'introduction de la problématique première de ce mémoire portant sur la normalisation. Ce domaine fait clairement partie intégrante des concepts de sécurisation d'une information. En particulier en matière d'authenticité d'une information et d'identité numérique. Nous verrons donc comment les États Européens se sont équipés d'organismes en charge des données à caractère personnelles.

Ces organismes comme la CNIL, au niveau national, sont en charge de la protection du citoyen. Mais ont-ils les moyens suffisants

pour assurer leur mission ? Car avec l'augmentation croissante de la quantité de données diffusées et de la technicité d'utilisation des nouveaux médium de communication nous observons les limites de telles entités.

Ainsi donc, pour mesurer la qualité de la sécurité d'un système d'information il nous faut prendre en compte un certain nombre de vecteurs d'intrusion dont une forte proportion dépendant de la résistance du système cryptographique. Car comme nous l'avons vu précédemment dans ce mémoire, la sécurité d'une information est fortement liée à sa complexité telle que définie par Kolmogorov.

Grâce à cet éclaircissement du domaine de recherche que nous nous attachons à étudier, nous pouvons dès lors émettre un certain nombre d'hypothèses qui émergent de la problématique mise en exergue précédemment.

Notre première hypothèse touche à la gestion de la vie privée comme vu en début de mémoire. En effet, nous tenterons de savoir si plus le contrôle sur les usagers est important, plus l'usager a le pouvoir sur ses données personnelles. Ceci en reprenant

l'idée qu'aujourd'hui la frontière entre le monde virtuel et le monde réel est de plus en plus ténu.

La seconde hypothèse quant à elle touche à la sécurisation intrinsèque d'une information et part du postulat que plus une information est complexe, tel que défini par Kolmogorov, plus est est sûre. En effet, la base de la sécurisation d'une information est qu'elle ne peut être intelligible que par son émetteur et son récepteur légitime.

La dernière hypothèse quant à elle nous entraîne dans le domaine du secret qui est très présent en matière d'espionnage. C'est pour cette raison que nous postulons que plus une information est gardée secrète, moins il y aura de risque de fuite d'information.

La réponse à ces hypothèses nous permettra d'ailleurs d'amorcer un élément de réponse à la problématique introduit en début de mémoire concernant la gestion actuelle du risque dans le traitement des informations sensibles. Bien sûr cet élément de réponse sera étayé par une analyse de phénomènes concrets en rapport direct avec le domaine d'étude.

Méthode de recherche

Comme vu précédemment, le secret est un moyen de protection souvent utilisé dans le domaine de la protection des systèmes d'informations. Ceci entraîne une difficulté certaine quant à l'analyse du sujet. En effet, le recueil d'informations viables ne peut se faire qu'en passant par des experts du secteur entraînant un risque de divulgation d'informations confidentielles ce qui n'est pas envisageable.

C'est pour cela que nous allons adopter une méthode d'analyse particulière plus adéquat au sujet traité. Pour avoir une vision d'ensemble de la problématique nous traiterons plusieurs hypothèses qui de manière empirique sont en corrélation directe avec le thème principal de ce mémoire. Cette méthodologie d'étude hypothèse par hypothèse de notre problématique nous permettra de parcourir le sujet de manière la plus exhaustive possible tout en s'attachant à approfondir certains points. Nous aurons donc un point de vue micro et macroscopique du domaine de recherche.

Nous allons commencer cette étude par l'aspect contrôle de l'information personnelle. Ces informations qui sont glanées par différentes entités étatiques ou économiques ont une valeur de plus en plus

grande dans nos sociétés de l'information comme nous l'avons vu précédemment. Pour mieux comprendre cela nous analyserons une conversation vidéo sur le sujet tenu par des experts du domaine : Julian Assange qui est un des fondateurs de WikiLeaks, Andy Müller-Maguhn porte-parole du Chaos Computer Club, Jérémie Zimmermann qui est un des fondateurs de la Quadrature du Net et enfin Jacob Appelbaum qui est un des principaux collaborateur du projet The Onion Router et membre de l'association Cult of the Dead Cow. Ces personnalités représentent l'esprit d'ouverture et de transparence de l'information et ce qui est intéressant dans cette vidéo c'est le débat lancé sur l'utilisation qui est fait des données personnelles numériques des usagers.

A la suite de quoi, nous analyserons l'aspect cryptographique de la problématique correspondant à notre seconde hypothèse. Pour un avis expert sur la question nous avons effectué une interview auprès d'Emmanuel Fleury, maître de conférences au sein du Master Cryptologie et Sécurité Informatique de Bordeaux 1. Nous nous efforcerons donc à partir de ce contenu de développer le sujet et ainsi pouvoir répondre à notre seconde hypothèse sur la complexité d'un algorithme.

Nous poursuivrons notre réflexion par une analyse macroscopique des vecteurs d'intrusion les plus courants dans les cas de fuite de données. Ceci nous permettra d'avoir un aperçu complet de la problématique de la fuite d'information et du risque encouru.

Nous allons également nous appuyer sur les travaux d'experts en sécurité informatique pour proposer dans un premier temps une catégorisation des cas possibles de corruption d'un système informatique. Puis, dans un second temps, une taxonomie des principaux risques encourus.

Le but étant de définir une grille d'analyse applicable à nos cas pratiques pour une mesure du facteur risque et ainsi quantifier

le niveau d'exigence sécuritaire pour un système d'information en fonction de son environnement. La grille d'analyse sera ensuite appliquée à un panel de cas représentatifs ce qui nous permettra de donner un ordre de grandeur quant au type d'intrusion subit.

Cette méthodologie de recherche par l'exemple et l'analyse nous offrira une vision réaliste sur le sujet et permettra d'anticiper les évolutions à venir dans ce domaine. Le but étant de présenter au lecteur une analyse large du sujet avec des experts pour étayer nos hypothèses en se basant sur des cas concrets. Pour au final, savoir si la gestion actuelle de l'information sensible est suffisante au niveau sécuritaire.

Interview d'experts

Protection de la vie privée

Comme vu précédemment nous allons tout d'abord présenter le cas de l'identité numérique. Pour cela nous allons étudier un débat diffusé sur la chaîne "Russia Today" dans le cadre de l'émission "The Julian Assange Show". La conférence que nous étudions correspond à l'épisode 8 de la série. Cet épisode est en deux parties respectivement intitulées "Cypherpunks, stumbling block in the way of total surveillance" diffusée le 05 Juin 2012 et "Taking back our information" diffusée le 11 Juin 2012. Les adresses de ces vidéos sont disponibles en [1] et [2].

Cette vidéoconférence présente les dangers à laquelle est confrontée la protection de la vie privée avec la montée du contrôle de l'information dans nos médiums de communication. C'est pour cela que l'on y retrouve Julian Assange qui est fondateur de Wikileaks. Bien qu'il s'agisse d'un personnage controversé, il est indéniable qu'il est aujourd'hui un des acteurs dans la guerre du numérique. Bien qu'en général ces acteurs soient pour une opacité de l'information, Julian Assange et le mouvement amorcé par Wikileaks est pour une plus grande transparence de l'information. Cette idéologie cypherpunk

assume qu'il existe une asymétrie entre le contrôle des citoyens sur leur vie privée et les informations dont disposent les états. Il est à noter que Julian Assange est également un programmeur informatique et a participé à la création du système de chiffrement par Denis déjà présenté dans ce mémoire ainsi qu'à d'autres projets du monde du logiciel libre.

Au moment de la conférence, Julian Assange est assigné à résidence en Grande-Bretagne car il est accusé de viol par la justice suédoise. Il est à noter que ces accusations de viols sont apparues quelques temps après la diffusion le 25 Juillet 2010 de documents confidentiels sur la guerre en Afghanistan ce qui a provoqué la fureur du Pentagone, le quartier général du département de la Défense des États-Unis. Depuis, Julian Assange a été condamné par la justice de Grande-Bretagne à être extradé vers la Suède où il serait de facto emprisonné puisque le système pénal suédois ne prévoit pas de liberté conditionnelle avant le jugement. Pour éviter donc d'aller en prison, ce dernier s'est réfugié à l'ambassade d'Équateur en Grande-Bretagne.

1. <http://assange.rt.com/cypherpunks-episode-eight-full-version-pt1/>

2. <http://assange.rt.com/cypherpunks-episode-eight-full-version-pt2/>

Egalement présent Andy Müller-Maguhn qui est porte parole du Chaos Computer Club dont il est membre depuis 1986. Le Chaos Computer Club est incontestablement l'un des groupes le plus influent dans le monde cypherpunk. Pas tant au niveau technique mais plus au niveau philosophique et aujourd'hui politique puisqu'il est, parmi d'autres, à l'origine du Parti Pirate lui-même présent dans une centaine de pays. L'association a été indirectement impliquée dans la première affaire de cyberespionnage en 1989. Pour la petite histoire, un pendant du Chaos Computer Club Français a été créé en 1989 mais il s'agissait en réalité d'une fausse association montée par la Direction de la Surveillance du Territoire (DST) qui a aujourd'hui fusionnée avec la DCRI présentée précédemment dans ce mémoire.

Egalement présent, Jacob Appelbaum, qui est enseignant chercheur au sein de l'Université de Washington. Il est également une figure emblématique de la communauté du logiciel libre et un des principaux contributeurs au projet The Onion Router (TOR) permettant de naviguer de manière anonyme sur internet. Il est également connu pour avoir été représentant de Wikileaks à la Hope Conference de 2010. Ce qui lui a valu par la suite d'avoir été arrêté une dizaine de fois par la police aux frontières lors de ses

voyages à destination des États-Unis. De plus, il est membre de l'association Cult of the Dead Cow également très influent au sein de la communauté hacker. Cette association a été créée en 1984 au Texas et a mis à disposition du grand public un certain nombre de logiciels de contrôle de l'information comme le logiciel TorPark qui fournit une version modifiée de Firefox pour naviguer de façon anonyme. Pour la petite histoire, Jacob Appelbaum a été représentant de Wikileaks à la Hope Conference 2010 car Julian Assange n'aurait pas souhaité s'y rendre après avoir appris l'arrestation de Bradley Manning, son principal informateur, analyste militaire responsable de la fuite des documents confidentiels sur la guerre en Afghanistan et des câbles diplomatiques. Celui-ci est actuellement emprisonné en attente de jugement et risque jusqu'à 50 ans de prison.

Pour finir, est également présent à cette conférence, Jérémie Zimmermann, cofondateur de la Quadrature du Net qui est une association défendant les droits et les libertés des citoyens sur Internet. Ses actions marquantes ont été d'informer les responsables politiques français sur le traité ACTA, un accord international anti-contrefaçon. Pour ce faire, l'organisation publie, grâce à une fuite d'information,

le texte consolidé de l'accord. Ce qui a entraîné le rejet de celui-ci au niveau du gouvernement des États-Unis et devant le parlement Européen.

On voit grâce à cette courte présentation des différents protagonistes de cette vidéo que chacun d'eux possède une expertise dans le domaine de la confidentialité de l'information ou dans la protection de la vie privée. Au delà, ils ont pour la plupart l'expérience personnelle de l'influence que peut avoir une identité numérique sur la vie quotidienne.

Les deux séquences mises à la suite faisant près de 50 minutes, nous ne prendrons que certaines parties en rapport direct avec notre hypothèse. Une retranscription écrite originale en anglais est disponible à l'Annexe 5.

Pour mieux comprendre cette vidéo il nous faut dans un premier temps amener le contexte du tournage. Tout d'abord cette vidéo a été diffusée sur la chaîne Russia Today qui est un média mainstream basé en Russie et est donc soumis à la législation de ce pays. Ensuite, Julian Assange tout comme son ami Jacob Appelbaum sont sous le coup d'une procédure judiciaire de la part des autorités des États-Unis. Il faut donc prendre

le message de cette vidéo avec précaution. Malgré tout, cette vidéo par la présentation d'exemples concrets et par la présence de protagonistes d'horizons différents que ce soit d'un point de vue géographique, idéologique ou professionnel nous offre un aperçu objectif sur la question de la protection de la vie privée. Surtout que sur plusieurs thèmes s'instaure un jeu de rôle durant la conférence où un des intervenants se positionne à l'opposé de la conversation pour mieux faire ressortir les arguments de chacun.

Dans un premier temps, la vidéo commence par une présentation du sujet et la présentation des intervenants. S'ensuit une entrée directe dans le vif du sujet, les libertés fondamentales. Le concept variant beaucoup entre les pays, Julian Assange propose de prendre trois libertés fondamentales : la liberté de communication qui par analogie fait référence à la liberté d'opinion, d'expression et d'information présent dans la Déclaration universelle des droits de l'Homme. Tout comme la liberté de circulation qui est également citée dans la constitution française et enfin la liberté d'interaction économique. Cette dernière peut surprendre dans un tel débat mais il s'avère que Julian Assange en tant que fondateur de WikiLeaks est directement lié

à une restriction de cette liberté puisqu'en effet, les compagnies Visa, Mastercard et Paypal ont refusé d'encaisser des paiements à destination de l'association Wikileaks en décembre 2010. Puis, comme le fait remarquer Andy Müller-Maguhn, il est question dans le débat de la nature des capitaux sur le réseau internet. Il s'avère que sur le réseau ceux-ci ne sont représentés que par des impulsions électromagnétiques et somme toute ne sont que des données ayant un caractère financier. On peut alors se demander si grâce au contrôle opéré par les organisme de télépaiement cités précédemment, Wikileaks avait un meilleur contrôle sur ses informations financières ?

Plus loin durant cette vidéo conférence, il y a un point important à prendre en compte dans le reste de ce mémoire. Il s'agit de la séparation des domaines civil et militaire comme le fait remarquer Jérémie Zimmermann. En effet, l'ensemble des protagonistes s'accordent sur le fait que sur le réseau internet a lieu une cyber guerre, ce que nous verrons plus tard dans ce mémoire, or la création de cyber armes a un coût bien moindre tant au niveau financier qu'humain. Ceci a donc entraîner une surenchère dans ce secteur par les organisations militaires comme le fait remarque Julian Assange. En effet, la National Security Agency (NSA) avait, il y a 10 ans,

seulement 10 partenaires privés. Il y a deux ans on dénombrait un millier de contrats passés avec des entreprises du domaine privé. Ce qui nous montre également que le contrôle de l'information et des usagers sur internet est effectivement en augmentation. L'exemple le plus frappant de ce contrôle a atteint son paroxysme durant le printemps arabe. Comme indiqué dans l'interview, le système EAGLE vendu par la société Amesys au régime de Kaddafi lui a permis d'avoir un contrôle total sur les communications nationales. Nous verrons également que durant la révolution en Tunisie, le principal fournisseur d'accès du pays a tenté de récupérer les identifiant Google, Yahoo et Facebook de nombreux citoyens tunisiens pour vérifier leurs communications.

Par la suite, une prise de position intéressante en faveur des industriels du monde de l'information est prise. Julian Assange défend le lobbying pratiqué par les grands groupes en matière de protection du droit d'auteur. En justifiant cela par le fait que ce sont ces grands groupes qui sont les principaux créateurs de richesse et donc qu'ils devraient avoir des lois facilitant leur productivité. Par cette prise de position envers le capital, nous entrons dans un système idéologique entraînant une possession de l'esprit, de l'immatériel. En

effet, étymologiquement l'information bien que venant du radical informatum signifiant donner forme, il peut également avoir une autre signification du fait de son préfixe in représentant à la fois le don dans le sens de l'appartenance (innover) ou l'enlèvement dans le sens privatif (interminable). Si nous prenons ce second postulat, alors, le sens même du mot n'est pas de donner forme mais au contraire de ne pas avoir de forme, dans notre cas physique. Ainsi donc, le contrôle se fait non plus sur des matières mais sur des idées. Or comme le note à très juste titre Jérémie Zimmermann, en fin de retranscription, l'ensemble des acteurs majeurs sont nés grâce à l'innovation dans le domaine de l'information immatérielle. Or les grands groupes tels que Google, Apple ou encore Microsoft sont nés à partir d'idées dont l'objectif premier n'était pas forcément qu'elles soient lucratives ce qui démontre que cet argument est faussé par la nature même du terme information.

Si nous en revenons à notre hypothèse spéculant que plus le contrôle sur les usagers est important, plus il a le pouvoir sur ses données personnelles et faisons l'analogie avec l'étude de cette conférence d'experts.

Il en ressort que si l'on considère par usager un citoyen lambda, que ce soit dans une société à régime totalitaire, oligarchique ou démocratique, à partir du moment où une institution cherche le contrôle sur ses ressortissants il y a un archivage qui est mis en place. La seule issue devient alors la protection de la vie privée par la mise en place d'un contre pouvoir juridique et donc d'un appareil judiciaire indépendant. D'où l'importance, comme le souligne Jérémie Zimmermann, de l'éducation technologique des instances politiques pour un vote en adéquation des lois dans le domaine de l'information et de la communication. Ce qui semble, au niveau national et aux vues de l'évolution des législations et de la technique sur les précédentes vingt dernières années, être en bonne voie comme présenté plus haut dans ce mémoire.

Mais il ne faut pas oublier qu'il existe différents tribunaux en fonction de la nature de l'inculpation. En effet, dans le monde civil il existe le droit pénal et le droit civil qui sont traités dans des tribunaux différents. Il existe aussi le droit militaire qui lui est traité de manière totalement différente au sein de tribunaux militaires.

Malheureusement comme présenté dans la vidéo-conférence, la frontière entre le monde civil et le monde militaire est de plus en fine et dans certains cas il arrive que des usagers retrouvent leurs données étalées au sein de réseaux non désirés. C'est alors que le pouvoir des utilisateurs sur leur propres informations est annihilé. La difficulté de réponse à cette hypothèse ne réside donc pas tant sur l'accessibilité de l'information mais bel et bien sur la nature des risques

encourus surtout lorsque la portée devient de type militaire puisqu'à partir de ce moment l'usager n'a plus ou peu de recours possible. On peut donc dire que plus il y a de contrôle au niveau militaire des usagers et moins ceux-ci ont de pouvoir sur leurs informations. Bien sûr cette conclusion entre dans le cadre d'un état de droit qui n'est pas soumis à des conditions exceptionnelles comme une dictature ou une occupation où de facto la loi martiale est appliquée.



Complexité cryptographique

Notre seconde hypothèse concerne la complexité, telle que définie par Kolmogorov, d'une information. Nous appliquons donc cette théorie, par analogie, aux concepts induits par la cryptographie. Nous verrons qu'il y a une imbrication de ce concept dans le domaine précédemment cité pour pouvoir ensuite mesurer les paramètres de notre hypothèse. Bien sûr, nous restons dans l'aspect macroscopique de la problématique. Pour étayer notre argumentation, nous nous appuierons sur les différents points présentés précédemment dans ce mémoire mais aussi sur le recueil d'une entrevue avec le professeur Emmanuel Fleury, maître de conférence au sein du master Cryptologie et Sécurité de l'Université de Bordeaux 1 et chercheur au Laboratoire Bordelais de Recherche Informatique (LaBRI). Une transcription écrite est disponible en Annexe 6.

Tout d'abord il faut savoir que dans le domaine de la cryptanalyse, depuis les années 1980 est appliqué le principe de Kerckhoffs un postulat stipulant qu'un cryptosystème doit être sûr même si tous les éléments le constituant, sauf sa clé, sont accessibles publiquement. En effet,

dès 1883 dans les numéros de Janvier et de Février du Journal des sciences militaires, Auguste Kerckhoffs alors cryptographe et professeur de langue à l'Ecole des Hautes Etudes Commerciales à Paris énonce les six grands principes suivants :

- Le système doit être matériellement, sinon mathématiquement, indéchiffrable
- Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi
- La clé doit pouvoir être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants
- Il faut qu'il soit applicable à la correspondance télégraphique
- Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes
- Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer

Le postulat premier est alors repris à posteriori par Claude Shannon dans sa théorie de l'information par la maxime "l'ennemi connaît le système". Ceci oblige donc à vérifier la robustesse d'un algorithme, il ne doit fournir aucun détail sur le secret protégé comme le fait remarquer Emmanuel Fleury durant notre interview. Cela rejoint notre troisième hypothèse, que nous développerons plus loin dans cette analyse, disant que plus une information est gardée secrète moins il y aura de risque de fuite d'information.

Dans le cas de la cryptanalyse, il convient donc que certains pré-requis soient respectés mais pas seulement. En effet, pour assurer une bonne analyse il faut que l'algorithme soit réellement accessible au plus grand nombre, ce qui n'est pas forcément le cas encore aujourd'hui. Cette idée de la sécurité par l'obscurantisme, consistant à cacher un algorithme pour éviter qu'il soit analysé, était utilisé il y a quelques années alors que la majorité des cryptographes compétents étaient employés par des Agences Nationales de sécurité, que ce soit aux États-Unis, en Russie ou en France. Mais aujourd'hui avec ce mélange du domaine militaire au domaine public et la meilleure accessibilité de l'information induit par les nouvelles technologies nous voyons que de plus en plus d'analystes cryptographes enseignent

dans des Universités ou travaillent, des fois en tant qu'indépendants, au sein de structures économiques civiles. Or, avec cette augmentation d'expertise qui n'est pas soumise au secret, on a vu de plus en plus de cas d'algorithme "rétro-ingénieré". Un exemple marquant a été celui du cryptage par flux A5/1 utilisé dans le standard GSM de nos téléphones portables. Par le biais de fuites d'informations et d'analyses, il a été prouvé qu'il contenait plusieurs vulnérabilités [36].

Nous voyons donc que la garantie de robustesse ne passe pas par la sécurité par l'obscurantisme. Mais comme le fait remarquer également notre interlocuteur durant l'interview cela ne passe pas non plus par une accessibilité maximale de l'algorithme. À cela, nous pouvons argumenter par le fait que la majorité des vulnérabilités au sein d'algorithmes cryptographiques ont été découvertes par des experts dans le domaine réalisant des travaux financés par différentes entités, agences de sécurité ou universités entre autres. Alors bien qu'un algorithme soit accessible, cela ne veut pas dire qu'il soit robuste tant qu'une expertise n'a pas été effectuée. On peut citer l'exemple du Data Encryption Standard, un algorithme de chiffrement de données, développé durant les années 1970 par IBM puis diffusé au

grand public en 1977. Il a fallu attendre les années 1990 avec les travaux de Eli Biham et Adi Shamir sur la cryptanalyse différentielle pour se rendre compte qu'il était vulnérable dans le cas de l'utilisation d'une table de valeur statique faible. Or durant la création de l'algorithme, les experts de la NSA ont collaboré à sa création et ont fourni une table statique de valeurs recommandées. Et il s'est avéré près de trente ans plus tard que l'utilisation de ces tables permettait de se prémunir contre ce type de cryptanalyse. Les experts de la NSA avaient donc une vingtaine d'années d'avance sur la cryptographie civile et la mise à disposition de l'algorithme au grand public n'a pas changé cet état de fait.

Enfin la corrélation se fait au travers de programmes introduisant une forte complexité dans le traitement des données à cacher. Comme nous l'avons déjà vu, le

cassage d'un crytage est fortement lié à des propriétés mathématiques complexes dans le sens que le nombre d'étapes permettant de résoudre le problème est très grand. Cette définition rejoint d'ailleurs totalement la théorie de la complexité des algorithmes présentée par Donald Knuth dans sa série de livres "The Art of Computer Programming". Ainsi donc, si l'on applique une analogie avec la définition de la complexité telle qu'énoncée par Kolmogorov on peut dire que plus une information est complexe, plus elle est sûre. Un exemple concret étant la création du cryptage par courbe elliptique présenté précédemment dans ce mémoire à partir de l'interview du professeur Emmanuel Fleury. Avec l'augmentation de la capacité de calcul des processeurs, les chercheurs s'orientent vers ce type de cryptage [37] plutôt que la factorisation.

Secret de l'information

Jusqu'à présent nous ne nous sommes intéressés qu'à l'aspect algorithmique de la cryptographie et donc des étapes rendant inintelligible le message véhiculé pour les non-initiés, ceux qui n'ont pas la clé ou le secret de décryptage. Mais qu'en est-il alors lorsque l'on doit justement transmettre cette clé ? Comme présenté précédemment ce problème a été résolu grâce à la cryptographie asymétrique mais il existe d'autres méthodes de transmission de secret. Nous entrons alors dans le domaine de la stéganographie qui lui agit sur l'étape de transmission d'une information. On arrive donc à notre troisième hypothèse citée préalablement concernant le fait de garder une information secrète.

Comme vu dans le chapitre précédent, la protection par obscurantisme n'est pas suffisante dans un cadre purement fonctionnel. On part alors du postulat que l'information restera pour toujours secrète ce qui, dans la pratique, n'est presque jamais le cas. Comme indiqué durant l'interview, aujourd'hui, avec cette frontière toujours plus fine entre le monde militaire et civil, de plus en plus de systèmes de communication intègrent des dispositifs cryptographiques. Prenons l'exemple des cartes de paiement,

dans les années 1990 des chercheurs se sont penchés sur son fonctionnement et ont découvert que le système d'authentification était basé sur l'algorithme DES munis d'une clé de 8 octets. De même pour la console de jeu Playstation 3 qui elle utilise l'algorithme RSA pour l'authentification. Mais aussi les nouveaux smartphones de la marque Apple. Bref, ces procédés sont de plus en plus prégnants dans nos sociétés de l'information, ce qui montre que le nombre d'informations qui sont gardées secrètes par ces mécanismes augmente. Toute la subtilité de la stéganographie étant de ne pas faire savoir qu'il existe de telles données au sein d'un système d'information et de communication. Il s'agit alors non pas d'une protection par obscurantisme mais plutôt d'une protection par la minorité puisque seul une poignée d'initiés connaît le secret. Arrive alors la problématique de la confiance déjà présentée plus tôt dans ce mémoire, si quelqu'un se fait passer pour un récepteur légitime de l'information, dans un premier temps il pourra découvrir qu'il existe un renseignement caché mais aussi, dans le pire des cas, le décoder. Ainsi donc, entre en jeu, les notions de confidentialité et de confiance. La solution trouvée à cette demande a donc été la mise en place

d'un système d'autorités compétentes fournissant des certificats permettant de prouver son identité numérique aux autres et que celle-ci n'est pas falsifiée. Mais au delà de la simple certification, il s'agit d'instaurer une relation de confiance entre l'émetteur et le récepteur comme présenté en début de mémoire car si elle est rompue alors le certificat n'a plus aucune valeur. Prenons un exemple concret pour illustrer ce cas. Le 08 Août 2012 la société Websense ThreatSeeker a détecté une attaque sur plusieurs sites internet du gouvernement Népalais. Le but de cette attaque était d'installer un logiciel espion sur les ordinateurs de certains sites gouvernementaux. Il s'est avéré que ce logiciel espion était certifié par l'autorité VeriSign qui avait délivré ce certificat au fournisseur d'accès 360.cn. Le logiciel se faisait donc passer pour un logiciel légitime grâce à ce certificat qui a probablement été volé.

Nous avons donc pu voir que la sécurité par le secret est une solution possible dans le cas où la confiance dans le canal de communication est totalement assurée. Ceci est donc directement en corrélation avec le nombre de personnes susceptibles d'accéder au canal de communication. Plus il y aura de personnes pouvant falsifier l'identité du récepteur légitime. Dans cette continuité on peut alors imaginer l'utilisation en conjonction des deux techniques présentées. Notre hypothèse postulant que plus une information est gardée secrète moins il y aura de risque de fuite sera alors proportionnée au nombre de dispositifs ayant accès au canal de communication.

Vecteurs d'attaque

Nous avons vu précédemment les bases de la sécurité informatique selon les théories de l'information telles que définies par Claude Shannon ou encore Andreï Kolmogorov.

Nous allons maintenant nous intéresser aux autres facteurs de risque qui eux sont de qualité plus techniques mais tout aussi importants.

Comme vu précédemment pour mieux comprendre les risques liés au traitement d'une information sensible il faut être en mesure de classifier les données transmises. Cette classification aidant ensuite à savoir si le niveau de sécurité appliqué est en accord avec le besoin. Tout d'abord comme nous avons vu précédemment il nous faut savoir si la nature de l'information est d'origine militaire ou civile ce qui entraîne des conséquences très différentes tant au niveau juridique que de la technicité des attaques.

Il nous faut ensuite déterminer le niveau d'accès autorisé. Nous reprendrons pour cela la classification décrite par Franck Boulot et Didier Volle : l'information dite ouverte est accessible à tous, celle dite semi-ouverte est accessible par des canaux publics et secrets et enfin celle dite fermée n'est disponible

que par des méthodes alternatives et souvent illégales. Ceci nous permettant de mieux définir l'aspect protocolaire de la transmission.

Il nous faut ensuite nous intéresser à la nature de la fuite d'information. C'est à dire les vecteurs d'attaques possibles pour l'accès à l'information. Il en existe de très nombreux c'est pour cette raison que nous ne proposerons qu'une classification généraliste la plus élargie possible. Revenons donc au risque de fuite, celui-ci induit tout le temps au moins une faiblesse dans une ou plusieurs des fonctions de sécurité telles que définie par la Méthode Harmonisée d'Analyse de Risques précédemment citée. Cela peut être une atteinte à la confidentialité, à l'intégrité regroupant l'authenticité ou encore la disponibilité de l'information [6].

Plus en avant il nous faut considérer les vulnérabilités d'un système. Celles-ci sont multiples et pour mieux mesurer le danger il nous faut connaître la nature du risque. Pour cela nous allons les catégoriser et ainsi pouvoir faire une comparaison du danger le plus prégnant dans notre panel d'analyses.

Commençons tout d'abord par les failles humaines qui sont quelque peu hors de notre sujet mais qu'il faut prendre en compte car elles peuvent être nombreuses. Le facteur humain est à prendre en compte car il est tout à fait possible d'obtenir de manière volontaire ou non de transmettre des informations secrètes à un interlocuteur.

Dans le jargon cela est appelé l'ingénierie sociale.

Il existe également les failles matérielles qui elles sont intrinsèques à tout matériel électronique. Il est tout à fait possible pour une personne mal intentionnée, si elle a un accès physique, d'exploiter un point faible directement au niveau matériel. On peut citer en exemple le crackage de la Playstation 3 par George Hotz (geohot). Celui-ci a réussi par le biais de la technique appelée attaque par perturbation (glitch) à outrepasser le système d'authentification développé par Sony pour pouvoir installer des logiciels non autorisés sur la console. La technique d'attaque par perturbation consiste à générer délibérément des mal fonctions matérielles pour modifier le cours d'exécution d'un programme. Il est possible de catégoriser ces attaques en trois grands groupes, les attaques invasives consistant à agir physiquement sur le matériel

pour l'analyse. Cette technique offre des résultats rapides mais coûte assez cher, ou les attaques non-invasives consistant à glaner des informations sur le matériel sans en modifier l'intégrité. Il existe aussi les attaques de type semi-invasives mêlant les deux techniques suscitées.

Plus en avant, nous avons les failles logicielles qui elles sont encore plus nombreuses puisque l'étude de celles-ci ne nécessitent qu'un faible investissement. Nous pouvons regrouper ces failles applicatives en plusieurs sous catégories pour une granularité plus fine dans notre étude. Pour cela il faut prendre en compte le contexte d'exécution d'un programme. Le programme peut être soit dans un fonctionnement local, c'est à dire sur une machine unique, ou à distance, pouvant ainsi contaminer plusieurs machines. Cette différentiation est importante car elle introduit la notion de réseau et donc de protocole sécuritaire. Ensuite, comme vu précédemment, la sécurité d'un système d'information passe par la mise en place d'une politique de gestion de droits pour limiter les accès des différents codes machine. Or, dans certains cas, des vulnérabilités logicielles entraînent une élévation de privilège, ce qui peut être extrêmement dangereux.

Nous nous intéressons ensuite à l'auteur de la tentative d'exploitation. Car aujourd'hui, avec l'évolution permanente de la capacité de traitement de nos processeurs, il existe des algorithmes complexes capables d'exploiter de manière automatique ce vecteur. On les appelle des malwares. Comme ces programmes sont automatisés, ils ont un rayon d'action et une rapidité d'exécution bien plus grande qu'un humain. Par contre ce genre d'attaque ne représente pas le risque le plus important car elle n'est pas évolutive et difficilement ciblée. Malgré tout elle représente la part la plus importante dans les cas de fuite d'information.

C'est pour cela que nous allons présenter une taxonomie pour ce type d'attaque. Il s'agit de la taxonomie présentée par Joanna Rutkowska dans sa présentation « *Introducing Stealth Malware Taxonomy* » [39]. Cette taxonomie présente 4 types de programmes malicieux cachés :

- Le Type 0 où le programme malicieux s'exécute de manière indépendante par rapport aux autres processus du système. C'est le cas d'un grand nombre de ces programmes.
- Le Type 1 quant à lui désigne les programmes effectuant des modifications dans les sections

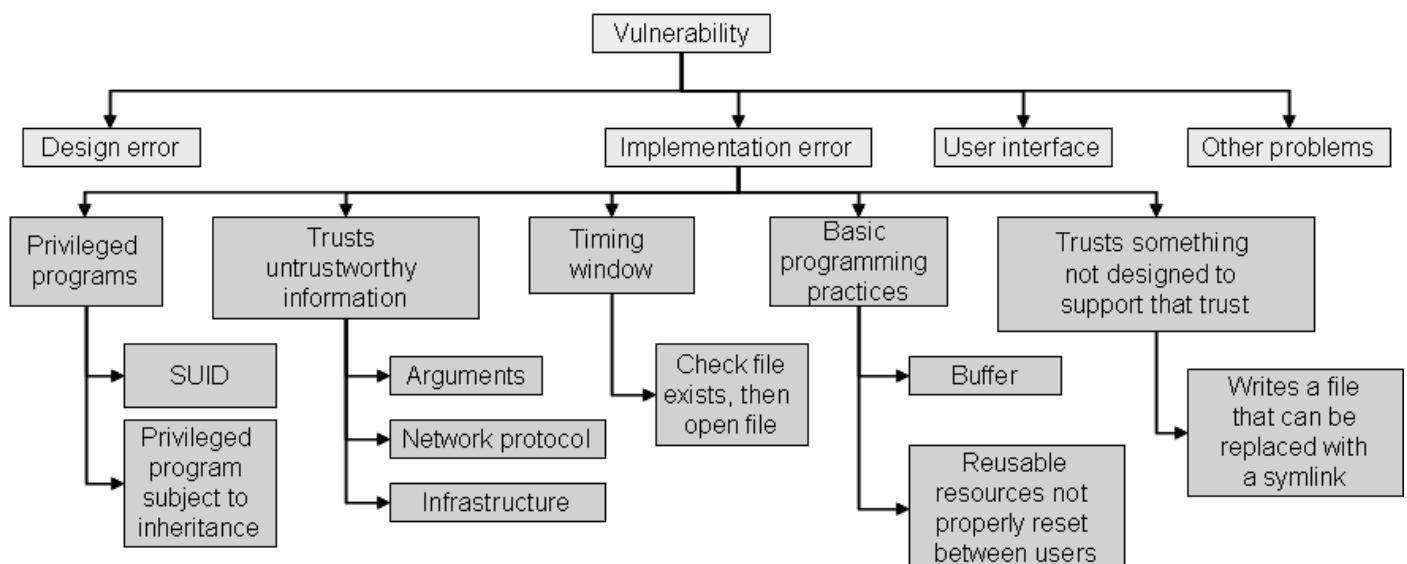


dynamiques des autres processus. Comme la modification de l'ordre d'exécution des instructions d'un autre programme par exemple.

- Le Type 2 est un peu plus complexe à comprendre car il concerne les programmes effectuant des modifications dans les sections statiques du système d'exploitation. Cela peut être des adresses d'appel de fonctions ou de zones mémoires. Ce qui les rend particulièrement difficiles à détecter.
- Et enfin le Type 3 qui consiste en un programme fonctionnant au-dessus du système d'exploitation qui pourrait alors intercepter absolument tous les appels au matériel. Ce type de programme n'effectue aucune modification du système ce qui le rend quasi indétectable.

Grâce à cette taxonomie, plutôt que de nous intéresser au type de fonctionnement du programme malicieux, nous nous intéressons au degré de corruption du système cible et donc à la difficulté de désinfection qui est directement en corrélation avec le risque de fuite d'informations.

Enfin, il existe un autre vecteur de fuite de données étant proéminent dans le domaine sécuritaire. Il s'agit des fuites d'informations dues à une mauvaise architecture du système d'information et de communication. Ce type de vulnérabilité est appelée faille réseau puisque les informations sont détournées en dehors de la machine, directement dans le canal de communication. Celles-ci ont souvent des conséquences très graves sur l'ensemble de l'organisation puisqu'aucune des machines légitimes du



CERT Taxonomie sur les vulnérabilités

réseau n'est corrompu, d'où la difficulté de les détecter. De plus, ce type d'attaque porte souvent atteinte à la disponibilité des systèmes d'informations ce qui peut être pénalisant pour certaines entités étatiques ou économiques.

Nous séparerons donc ce type de vulnérabilité en trois catégories différentes pour mieux les classifier. Tout d'abord nous avons le risque d'abus de confiance introduisant

la notion d'usurpation d'identité qui est souvent induit par une anomalie au sein même du protocole de communication ou encore par une mauvaise architecture du système d'information. Les failles réseau d'implémentation dont l'origine étant l'algorithme de traitement. Et enfin, celles concernant l'interface utilisateur.

Tableau comparatif

Nous avons donc défini notre taxonomie concernant les risques d'attaques sur les systèmes d'informations. Le but de cette classification est de parcourir la plus grande surface de vecteurs de fuites possible. Mais nous avons vu plus tôt dans notre argumentation que toutes les attaques n'entraînent pas le même niveau de compromission du système. C'est pour cette raison que nous avons mis en place une grille de notation proportionnellement au risque encouru et des conséquences de la compromission.

Pour commencer, la notation générale dépendra de l'objectif visé par l'attaque, puisque nous pouvons convenir que les conséquences de la compromission d'un sous-marin nucléaire sont plus importantes que celles de l'ordinateur d'un particulier. Une attaque de domaine militaire sera donc l'objet d'un facteur de 4.

La classe d'information ayant été compromise entraîne également une différence de risque. Prenons l'exemple de la falsification d'une information sur Wikipédia, on peut considérer que ceci n'est pas aussi grave que la compromission d'une image satellite d'un objectif militaire. Le risque étant exponentiellement proportionnel à la nature

de l'information corrompue, nous utiliserons un facteur exponentiel. Si la donnée est ouverte, le facteur sera exponentiel 1, si elle est semi-ouverte le facteur sera de exponentiel 2 et enfin si l'information est fermée, il sera de exponentiel 3.

Par la suite, nous prendrons également comme facteur aggravant l'exploitation d'une faille au niveau humain ou matériel par rapport à une attaque logicielle. Puisque souvent cela entraîne une compromission plus difficile à localiser et à réparer. Nous prendrons un facteur de 4 pour ces éléments. Au niveau logiciel, nous avons également les vulnérabilités distantes et celles entraînant une élévation de privilège qui sont un facteur aggravant. Nous prendrons un facteur de 2 pour ces premières et un facteur de 4 pour ces dernières.

A la suite de cela, nous prenons également plus au sérieux l'attaque si l'auteur est un humain et n'utilise pas d'outils automatisés puisque cela veut dire que la personne a clairement choisi sa cible. Il en est de même pour les programmes mal intentionnés de niveau 2 ou 3 car très difficile à détecter. Nous appliquerons un facteur de 2 à ce type d'attaques.

Le type d'atteinte quant à lui nous permet juste de mieux comprendre la nature de l'attaque. Il n'a donc pas de facteur risque associé puisque le risque encouru est le même.

Enfin concernant la partie réseau il apparaît clair que les vulnérabilités de type architecturales sont celles à prendre le plus en considération. Nous attribuons donc un facteur de 4 à celles-ci.

Atteinte	Confidentialité	Intégrité	Disponibilité	Légendes
Objectif	Militaire ⁴	Civil ¹		¹ facteur de 1 ² facteur de 2 ⁴ facteur de 4 ⁵ exposant de 0 ⁶ exposant de 1 ⁷ exposant de 2
Information	Ouverte ⁵	Semi ouverte ⁶	Fermée ⁷	
Auteur	Humain ²	Automate type 0 ¹ type 1 ¹ type 2 ² type 3 ²		
Réseau	Architecture ⁴	Implémentation ¹	Interface ¹	
Vulnérabilité	Humaine ⁴	Matérielle ⁴ invasive non invasive semi invasive	Logicielle locale ¹ pas d'élévation de privilèges ¹ distante ² avec élévation de privilèges ⁴	

Tableau d'évaluation du risque de fuite d'information

Etude de cas

L'affaire VMWare

Le premier cas que nous allons étudier concerne une fuite d'apparence bénigne qui concerne la solution VMWare qui permet de faire de la virtualisation haut niveau. Or il est apparu le 20 avril 2012 que le code source de l'un des fichiers était disponible en ligne (une partie du fichier est en Annexe 7). Très vite, le responsable de cette fuite s'est fait connaître, il s'agissait d'une personne agissant sous le pseudonyme Hardcore Charlie [1]. En réponse, la société américaine VMWare a indiqué que cela ne représentait pas un grand risque quant à l'intégrité de sa solution qu'un seul fichier soit diffusé. Ce que ne savait pas la société c'est que le pirate n'avait pas seulement récupéré un seul fichier mais qu'il avait bien l'ensemble du code source de la solution en sa possession et surtout, qu'il avait récupéré ces informations sur le réseau de la société chinoise "China Electronics Import & Export Corporation" (CEIEC). Le protagoniste va jusqu'à dire qu'il a pu récupérer le code source de tous les logiciels de la compagnie

EMC Corporation qui édite des logiciels en tout genre dont certains concernent l'aspect sécuritaire. Mais ce n'est pas tout, il apparaît probable que cette personne ait récupéré des compte-rendus d'opérations militaires des États-Unis en Afghanistan dont un exemplaire est visible en Annexe 8. Plus en avant, lors d'une interview avec le journal The Inquirer, Hardcore Charlie affirme que ces informations sont transmises par le gouvernement chinois par le biais de la société Petrovietnam aux officiels Russes et Ukrainiens. Bien que ce n'est pas été totalement vérifié, il y a tout du moins quelques documents officiels ayant fuité dans cette affaire [2]. Malheureusement nous n'avons aucun détail sur la méthode employée pour obtenir ces informations, nous savons tout du moins qu'il s'agit d'une attaque logicielle avec élévation de privilèges étant donné le nombre d'informations sensibles ayant été récupérées. Certes certains documents ayant filtrés sont d'origine militaire il n'en reste que le système corrompu est du domaine civil.

Ce qui nous donne la grille d'analyse suivante catégorisée en une corruption de la confidentialité et de l'intégrité du système d'information.

Nous obtenons alors un degré de corruption de 33,77 qui ramené sur vingt nous donne

une note de 10,1. La note obtenue est assez basse étant donné la nature des informations ayant filtrées mais cela vient certainement du manque d'informations quant à la véracité des dires du protagoniste et aux techniques d'intrusion utilisées.

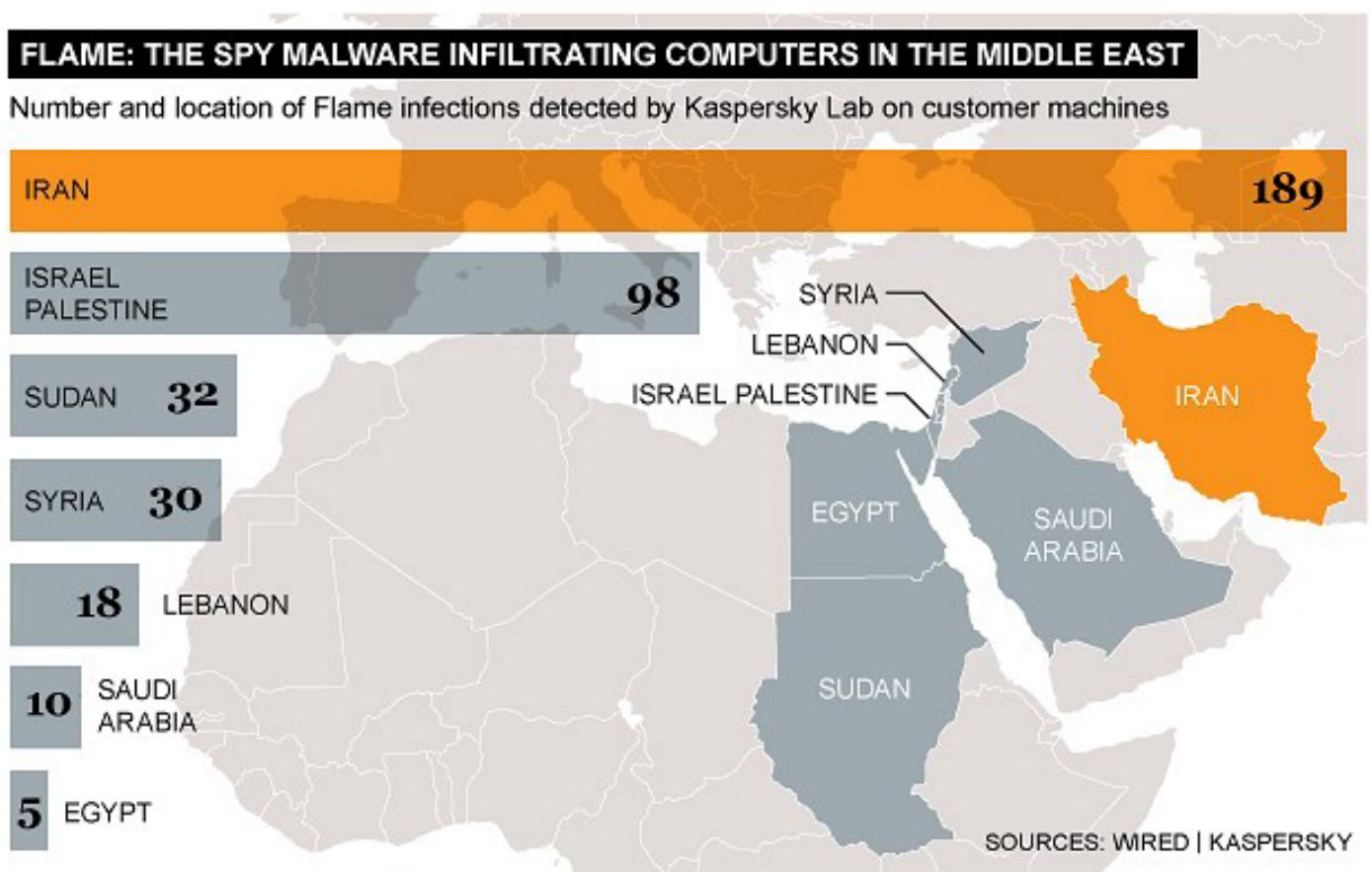
Atteinte	Confidentialité	Intégrité	Disponibilité	Légendes
Objectif	Militaire ⁴	Civil ¹		¹ facteur de 1 ² facteur de 2 ⁴ facteur de 4
Information	Ouverte ⁵	Semi ouverte ⁶	Fermée ⁷	⁵ exposant de 0 ⁶ exposant de 1 ⁷ exposant de 2
Auteur	Humain ²	Automate type 0 ¹ type 1 ¹ type 2 ² type 3 ²		
Réseau	Architecture ⁴	Implémentation ¹	Interface ¹	
Vulnérabilité	Humaine ⁴	Matérielle ⁴ invasive non invasive semi invasive	Logicielle locale ¹ pas d'élévation de privilèges ¹ distante ² avec élévation de privilèges ⁴	

1. « Anonymous' Hardcore Charlie on the VMware leak and why he did it », <http://www.theinquirer.net/inquirer/news/2171100/anonymous-hardcore-charlie-vmware-leak>
2. China mil contractor owned, <http://pastebin.com/ctLbRKVL>

Le nucléaire Iranien

Le second cas que nous allons étudier date de Juin 2010. Il s'agit de la date de découverte d'un programme malicieux appelé Stuxnet. Ce logiciel, dont on ignore l'origine, avait pour cible première les systèmes Microsoft Windows sans différenciation. Ce qui était déjà remarquable c'est le nombre de vulnérabilités utilisées par le programme, quatre, encore

inconnues à l'époque. Mais la véritable particularité de Stuxnet était qu'après avoir corrompu une première machine, il lançait un autre programme qui lui était chargé d'infecter des systèmes d'exploitation basés sur Siemens Supervisory Control and Data Acquisition (SCADA) en utilisant une autre faille encore inconnue sur ce type



Infection par région du malware Flame

d'environnement utilisé principalement dans des domaines industriels comme l'industrie gazière ou nucléaire. Plus en avant, après avoir réussi son transfert, le programme modifiait les vitesses de rotation des turbines centrifugeuses. De plus, pour éviter qu'aucune anomalie n'apparaisse sur les écrans de contrôle, les valeurs de rotation des turbines étaient falsifiées. Plusieurs experts s'attachent sur le point que le développement d'un tel programme a dû mobiliser une équipe de plus de 15

personnes durant au moins 6 mois, ce qui démontre la complexité de l'attaque. A noter également, que le logiciel était signé avec des certificats volés aux entreprises JMicron et Realtek toutes deux situées à Taïwan.

L'autre point intéressant étant qu'il ne ciblait les turbines de deux fabricants seulement, Vacon basée en Finlande et Fararo Paya situé en Iran. D'où un taux d'infection record en Iran avec 58,8% quelques jours après la découverte du virus.

Mais ceci n'est qu'un début, car un autre programme dont la découverte a été annoncée le 1er Septembre 2011 a été surnommé Duqu. Il comportait des similarités au niveau des cibles visées, des vulnérabilités utilisées, et du fait que le programme malicieux était également signé avec un certificat volé. Les experts considèrent ce programme tout aussi dangereux que Stuxnet [1] car son niveau de complexité est équivalent. La preuve en est, les analystes ont mis un certain temps ne serait-ce que pour déterminer en quel langage avait été programmé l'un des modules le composant [2]. Même si la cible de Duqu était équivalente, son but était assez différent puisqu'il ne faisait qu'espionner les communications pour les

remonter à un serveur de commande. De plus le programme était configuré pour s'autoeffacer après 36 jours d'activités ce qui rend son analyse encore plus complexe.

Stuxnet a également été en partie utilisé en mai 2012 par le programme surnommé Flame, notamment son module de propagation par USB. Par contre ce programme malicieux rejoint l'objectif de Duqu. En effet, les experts ont démontré que son but principal était l'espionnage des communications qu'elles soient vidéo, audio ou écrites pour les archiver. D'après l'étude fait sur le logiciel, il serait vingt fois plus complexe que Stuxnet [3] ce qui donne une idée de l'investissement nécessaire à un tel projet. Il utilise deux des mêmes vulnérabilités uniques de son prédecesseur sur les systèmes Microsoft Windows pour s'étendre. A noter également l'utilisation d'une nouvelle technique permettant de générer des certificats considérés comme légitimes pour faire croire que le programme malicieux n'en est pas un. A ce jour, les experts n'ont pas réussi à découvrir l'identité des auteurs de ces logiciels car ceux-ci utilisent une architecture de communication internationale complexe [4].

Nous prendrons ces trois attaques ensemble pour donner une notation à l'aide de notre grille d'analyse. Ce qui nous donne une grille catégorisée selon un risque au niveau de la confidentialité, l'intégrité et la disponibilité :

Nous arrivons alors à un total de 54,8 soit une note ramenée sur 20 de 16,4. Pour la petite histoire, ces attaques répétées contre les systèmes gouvernementaux d'Iran ont forcé le pays à déconnecter d'internet le réseau sécuritaire national [5].

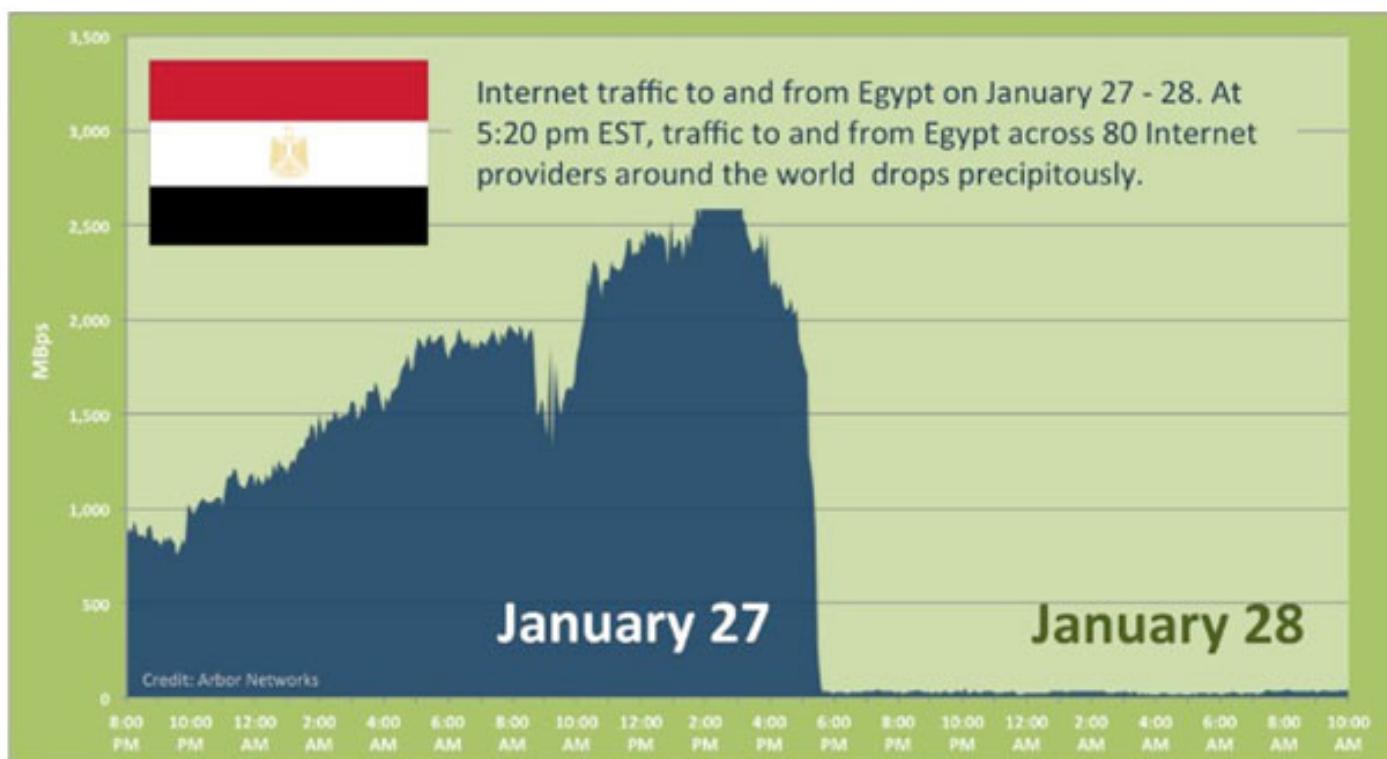
Atteinte	Confidentialité	Intégrité	Disponibilité	Légendes
Objectif	Militaire ⁴	Civil ¹		¹ facteur de 1 ² facteur de 2 ⁴ facteur de 4
Information	Ouverte ⁵	Semi ouverte ⁶	Fermée ⁷	⁵ exposant de 0 ⁶ exposant de 1 ⁷ exposant de 2
Auteur	Humain ²	Automate type 0 ¹ type 1 ¹ type 2 ² type 3 ²		
Réseau	Architecture ⁴	Implémentation ¹	Interface ¹	
Vulnérabilité	Humaine ⁴	Matérielle ⁴ invasive non invasive semi invasive	Logicielle locale ¹ pas d'élévation de priviléges ¹ distant ² avec élévation de priviléges ⁴	

1. W32.Duqu : The precursor to the next Stuxnet, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf
2. Son of Stuxnet Found in the Wild on Systems in Europe, <http://www.wired.com/threatlevel/2011/10/son-of-stuxnet-in-the-wild/>
3. Flame: world's most complex computer virus exposed, <http://www.telegraph.co.uk/news/worldnews/middleeast/iran/9295938/Flame-worlds-most-complex-computer-virus-exposed.html>
4. The Mystery of Duqu: Part Six (The Command and Control servers), http://www.securelist.com/en/blog/625/The_Mystery_of_Duqu_Part_Six_The_Command_and_Control_servers
5. Iran Took Systems Offline After Cyber Attack Hit Oil Industry, <http://www.securityweek.com/iran-took-systems-offline-after-cyber-attack-hit-oil-industry>

Le printemps arabe

A présent nous allons étudier un cas de fuite d'information au niveau national ne ciblant pas cette fois le domaine militaire bien que, nous le verrons encore, celui-ci s'entremêle avec le monde civil. Cette histoire commence le 05 Juillet 2010 durant la révolution en Tunisie. Le gouvernement de l'ex-président Ben Ali faisait alors face à une contestation populaire grandissante. C'est alors qu'il mit en place un système de filtrage au niveau national. En effet, c'est à cette date que Slim Amamou publie un

billet, sur le blog GlobalVoices Advocacy [1] dont le but était de défendre la liberté d'expression sur internet, indiquant que les connexions à destination de Google étaient détournées. Plus tard, le 04 Janvier 2011, le journal en ligne The Tech Herald publie un article [2] sur le phénomène qui confirme qu'une technique de "phishing", un détournement de trafic internet, était en place en Tunisie pour les sites Google, Yahoo et Facebook. L'article explique également qu'un détournement d'une telle



Graphique des connections entrantes et sortantes de l'Egypte les 27 et 28 Janvier 2011

envergure n'a pu être mis en place que par l'unique fournisseur d'accès à internet du pays, l'Agence Tunisienne d'Internet (ATI). Théorie confirmé deux jours plus tard, le 06

Janvier 2011 puisque ce jour, Slim Amamou est arrêté par le gouvernement Tunisien confirmant ainsi les soupçons faisant foi que le gouvernement tentait alors de récupérer

les identifiants et mots de passe des citoyens. Par la suite certaines grandes compagnies ont pris des mesures [3] pour empêcher ces informations d'être récupérées de manière illégitime.

Dans la suite des évènements du printemps arabe, en Tunisie, a eu lieu une révolte populaire en Egypte sous le gouvernement Moubarak. Durant cette période assez trouble, il s'est avéré le 27 Janvier 2011 que toutes les connections internet entrantes et sortantes du pays étaient bloquées [4] comme le montre le graphique.

Les citoyens sur place rapportent même que les communications par SMS sont bloquées. En effet le Vendredi 27 Janvier avait lieu une grande manifestation sur la place

Tahrir au Caire. Les experts en ont déduit que les autorités cherchaient à bloquer les communications via téléphone, Twitter ou Facebook pour empêcher les informations de fuiter hors du pays et cela malgré la présence de plus de 200 fournisseurs d'accès à internet dans le pays. Nous retrouvons là des éléments communs à l'analyse fait de la vidéoconférence sur les cypherpunk.

Ainsi donc, nous avons là deux exemples d'atteinte à la liberté d'expression par le biais d'une corruption de la confidentialité et de la disponibilité des communications comme le montre notre grille d'analyse. Nous n'avons pas choisi la catégorie intégrité car en l'occurrence, il n'y a pas d'atteinte à l'intégrité des dispositifs des particuliers.

Notre analyse nous donne une évaluation à 46,2 points de risque de fuite d'information. Ce qui nous donne une note de 13,8 sur 20. On voit grâce à cette étude que notre grille d'analyse donne un risque plus élevé que le premier cas ce qui est logique quant à l'ampleur de la fuite de renseignement.

La note obtenue est également inférieure au deuxième cas étudié car le risque est moindre du fait d'un ciblage moins critique du point de vu militaire. De plus la technicité de ce dernier cas n'est pas aussi poussé que précédemment.

Atteinte	Confidentialité	Intégrité	Disponibilité	Légendes
Objectif	Militaire ⁴	Civil ¹		¹ facteur de 1 ² facteur de 2 ⁴ facteur de 4
Information	Ouverte ⁵	Semi ouverte ⁶	Fermée ⁷	⁵ exposant de 0 ⁶ exposant de 1 ⁷ exposant de 2
Auteur	Humain ²	Automate type 0 ¹ type 1 ¹ type 2 ² type 3 ²		
Réseau	Architecture ⁴	Implémentation ¹	Interface ¹	
Vulnérabilité	Humaine ⁴	Matérielle ⁴ invasive non invasive semi invasive	Logicielle locale ¹ pas d'élévation de privilèges ¹ distante ² avec élévation de privilèges ⁴	

1. Mass Gmail Phishing in Tunisia , <http://advocacy.globalvoicesonline.org/2010/07/05/mass-gmail-phishing-in-tunisia/>
2. Tunisian government harvesting usernames and passwords , <http://www.thetechherald.com/articles/Tunisian-government-harvesting-usernames-and-passwords/12429/>
3. The Inside Story of How Facebook Responded to Tunisian Hacks , <http://www.theatlantic.com/technology/archive/2011/01/the-inside-story-of-how-facebook-responded-to-tunisian-hacks/70044/>
4. Internet Access & SMS Blocked in Egypt as Protests Escalate , <http://mashable.com/2011/01/27/egypt-protests/>

Histoire de drones

Pour finir nous allons présenter un cas d'espionnage entre les États-Unis et l'Iran. Il s'agit d'une affaire ayant commencée le Jeudi 8 Décembre 2011. Ce jour, la télévision Iranienne diffuse des images d'un drone américain top-secret qui aurait été capturé à l'aide d'un détournement comme le dit le responsable de la division aérospatiale Amir Ali Hajizadeh [1]. Ce drone porte la référence RQ-170 et est destiné à des opérations furtives de renseignement.

Les autorités américaines ont indiqué que l'Iran avait récupéré cet appareil suite à un crash ce qui paraît assez peu probable vu l'état du drone. Par contre, il paraît également peu probable que les iraniens avaient la technologie et les connaissances pour réaliser un tel détournement. Il existe une technique permettant ce genre d'opération qui est connu sous le nom de GPS Spoofing [2] dont le but est de falsifier la position GPS reçue par l'appareil et ainsi modifier sa destination. Cela est possible



Photographie du drone RQ-170 Sepahnews/AP

car le signal reçu par les satellites est extrêmement faible. En envoyant un signal plus facile à capter sur la même bande de fréquence, on arrive à surcharger le signal

satellite. Malgré tout, il y a d'autres moyens de protections embarqués dans le drone qui nécessitent des connaissances au sein même des structures américaines comme certaines clés de cryptage. On en vient alors à se demander si l'Iran a agit seul ou s'il n'a pas eu un appui extérieur, mais tout cela reste de la pure spéculation. Les faits par contre montrent qu'un document [3] expliquant comment il est possible d'utiliser cette faille a été diffusé en Octobre 2011.

Pour ce cas précis, notre grille d'analyse est catégorisée dans la confidentialité et la disponibilité car l'intégrité du système n'a pas été affectée durant l'opération comme l'atteste l'état général du drone.

Nous obtenons donc un score de 40,7 selon notre grille ce qui nous donne 12,2 sur 20. Nous voyons donc que notre grille d'analyse offre un résultat en concordance avec le risque de corruption post mortem. En effet, ce résultat est au dessus de notre premier cas mais en dessous d'un filtrage des communications au niveau national. Ceci nous réconforte également dans l'idée qu'il est possible d'appliquer cette analyse sur de nombreux cas de fuite d'informations sensibles.

Atteinte	Confidentialité	Intégrité	Disponibilité	Légendes
Objectif	Militaire ⁴	Civil ¹		¹ facteur de 1 ² facteur de 2 ⁴ facteur de 4
Information	Ouverte ⁵	Semi ouverte ⁶	Fermée ⁷	⁵ exposant de 0 ⁶ exposant de 1 ⁷ exposant de 2
Auteur	Humain ²	Automate type 0 ¹ type 1 ¹ type 2 ² type 3 ²		
Réseau	Architecture ⁴	Implémentation ¹	Interface ¹	
Vulnérabilité	Humaine ⁴	Matérielle ⁴ invasive non invasive semi invasive	Logicielle locale ¹ pas d'élévation de privilège ¹ distante ² avec élévation de privilège ⁴	

- Iran hijacked US drone, <http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video>
- Sat-nav systems under growing threat from ‘jammers’, <http://news.bbc.co.uk/2/hi/science/nature/8533157.stm>
- On the Requirements for Successful GPS Spoofing Attacks, <http://www.syssec.ethz.ch/research/ccs139-tippenhauer.pdf>

Conclusion

La gestion du risque dans le traitement des informations sensibles est un sujet complexe impliquant des tenants et des aboutissants souvent attachés au secret. C'est pour cette raison que le sujet est assez difficile à traiter mais aussi très intéressant. En effet, comme l'ont montré certaines affaires récentes comme le cas de Wikileaks, l'information est un vecteur extrêmement important dans les appareils d'état. Il convient donc de s'intéresser au problème et analyser les conséquences au niveau de la communication sur la scène nationale et internationale.

De plus une analyse de la façon dont sont gérées les informations personnelles concernant les citoyens d'un pays est aussi intéressante. Cela nous permet de mieux comprendre la problématique de la protection de la vie privée. Un point important sur lequel nous nous devons d'appliquer un regard critique. Il est arrivé par le passé, en particulier durant l'époque de la guerre froide, que certaines des parties utilisent de la désinformation faussant la vérité. D'où l'importance de la confrontation des opinions et des renseignements pour une analyse objective du sujet.

Il nous était donc important dans un premier temps de connaître les leviers en place sur cette thématique et de les traiter pour obtenir une vision globale des mécanismes concernant la gestion de l'information. Nous avons après cela, développé une analyse de la problématique par le biais des différentes hypothèses proposées pour ainsi pouvoir mesurer le phénomène.

Ainsi donc, nous avons pu, à travers quelques cas pratiques, nous rendre compte que les mondes militaires et civils sont en réalité de plus en plus liés ce qui se retrouve d'ailleurs dans les techniques de combat contemporaines. Aujourd'hui ce ne sont plus des armées qui se font la guerre, ce sont plus généralement des groupes rebelles qui sont en face d'armées régulières. Comme internet est le reflet de nos sociétés nous retrouvons la même organisation au niveau de l'autoroute de l'information, certaines données militaires sont détenues par des sociétés civiles et vice-versa. En tenant compte de cette évolution des pratiques et en nous appuyant sur l'analyse que nous avons réalisée dans ce mémoire, nous pouvons dire que dans le domaine militaire, le risque de fuite est bien plus important d'où une politique sécuritaire très forte. Ce qui n'est pas le cas dans le monde civil,

puisque'il existe un appareil judiciaire assez complet pour protéger les citoyens, tout du moins au niveau national. Par contre aux États-Unis, un certain nombre de lois du Patriot Act signé en Octobre 2001, peu après les attentats du 11 Septembre, font entrer dans le domaine militaire des données civiles d'où un risque plus grand pour les citoyens.

Le but de ce mémoire était de proposer un outil de mesure adapté aux différents cas de fuite d'information permettant une évaluation du risque cohérente pour

répondre à la problématique. Cet outil pourra être utilisé dans de nombreux cas principalement grâce à sa portée globale dans l'analyse du problème. Nous pouvons donc conclure que la gestion actuelle du risque dans le domaine militaire n'est pas adaptée aux risques induits par le traitement de telles informations comme le démontrent les cas que nous avons étudiés. Par contre, dans le domaine civil français les solutions possibles de protection de la vie privée tant au niveau technique que législatif paraissent être en adéquation avec le risque encouru.

Bibliographie

1. Claude Shannon, « *A mathematical theory of communication* », Bell System Technical Journal, vol. 27, pp. 379–423 and 623–656, July and October, 1948
2. Claude Shannon, « *A Mathematical Theory of Cryptography* », Bell System Technical Journal, 1 Septembre 1949
3. G. J. Chaitin, « *Algorithmic Information Theory* », Cambridge University Press, 1987
4. A. N. Kolmogorov, « *Logical basis for information theory and probability theory* », IEEE Trans. Inform. Theory, vol. IT-14, pp. 662–664, 1968
5. Olivier Iteanu, « *L'identité numérique en question* », Eyrolles, Avril 2008
6. Yves Deswarthe, Ludovic Mé, « *Sécurité des réseaux et des systèmes répartis* », Hermès Lavoisier, 2002
7. Sous la direction de Jean-François Lemettre, « *Risque, information et organisation* », L'Harmattan, 2008
8. Solange Ghernaouti-Hélie, « *Sécurité internet : Stratégies et technologies* », Dunod, 2000
9. Franck Boulot et Didier Violle, « *La Guerre de l'information ou l'éloge de la paranoïa* », Broché, 1 novembre 2005
10. Jean Jeanné, « *La Rose Croix Jonnanite* », 1960, Omnium Littéraire
11. Linus Torvalds, « *GPL V3 and Linux – Dead Copyright Holders* », 25 Janvier 2006, en ligne : <https://lkml.org/lkml/2006/1/25/273> (Page consultée le 17/06/2012)

12. Robert O'Harrow Jr., « *In Age of Security, Firm Mines Wealth Of Personal Data* », Washington Post Staff Writer, 20 Janvier 2005
13. Gerhard Schmid, « *Rapport final de l'enquête du Parlement européen sur le réseau Echelon* » le 11 juillet 2001.
14. Office of the Director of National Intelligence, « *DNI Releases Budget Figure for 2010 National Intelligence Program* », 28 Octobre 2010.
15. Department of Defense, « *DOD Releases Military Intelligence Program 2010 Topline Budget* » 28 Octobre 2010.
16. Pierre Bourdieu, « *L'opinion publique n'existe pas* ». Conférence (Arras, janvier 1971) dont le texte fut publié dans la revue Les temps modernes (n°318, janvier 1973, pp.1292–1309), puis repris dans Questions de sociologie, Les éditions de Minuit, Paris, 1980, p. 222–235.
17. Noam Chomsky, Edward S. Herman, « *La fabrique de l'opinion publique: la politique économique des médias américains* », Le Serpent à Plumes, 2003
18. Lawrence R. Jacobs and Robert Y. Shapiro, « *Presidential Manipulation of Polls and Public Opinion: The Nixon Administration and the Pollsters* », Political Science Quarterly, Vol. 110, No. 4 (Winter, 1995–1996), 519–538, The Academy of Political Science
19. Patrick Champagne, « *Faire l'opinion : le nouveau jeu politique* », Les éditions de minuit, 24 octobre 1990
20. Premier Ministre « *Guide Interministériel sur les systèmes d'information et application sensibles* », 13 Janvier 1997, en ligne : <http://www.circulaires.gouv.fr/pdf/2009/04/>

cir_1986.pdf

21. Wikipédia, « *Histoire de la cryptographie* », en ligne : http://fr.wikipedia.org/wiki/Histoire_de_la_cryptographie (Page consultée le 01/03/2011)
22. Simon Singh, « *Histoire des codes secrets* », Lattès, 1999.
23. Communication de M. Jean-Louis Greffe, « *Histoire des codes secrets* », 15 Octobre 2004, en ligne : <http://www.academie-stanislas.org/pdf04-05/Greffé.pdf> (Page consultée le 10/03/2011)
24. Jean-Paul Delahaye, « *Merveilleux nombres premiers* », Éditions Belin – Pour la Science, 2000.
25. David Pointcheval, « *Le Chiffrement Asymétrique et la Sécurité Prouvée* », 17 Juin 2002, en ligne : http://www.di.ens.fr/~pointche/Documents/Slides/2002_HDRThesis.pdf (Page consultée le 10/03/2011)
26. Dinu COLTUC, Alain TREMEAU, « *Stéganographie d'images basées sur le théorème chinois des restes* », Groupe d'Etudes du Traitement du Signal et des Images, 2005
27. Parlement Européen, « *DIRECTIVE 1999/93/CE DU PARLEMENT EUROPÉEN ET DU CONSEIL du 13 décembre 1999* », Journal officiel n° L 013 du 19/01/2000 p. 0012 – 0020
28. Conseil des Ministres, « *Recommandation sur la protection des données à caractère personnel, collectées et traitées à des fins statistiques* », 30 Septembre 1997
29. Marie-Anne CHABIN, « *Rôle et Applicabilité des normes* », Actes de la Ve conférence

- du DLM-Forum (Toulouse, 10–12 décembre 2008), volume 1, pp 43–51, en ligne : http://www.dlmforum.eu/index.php?option=com_jotloader§ion=files&task=download&cid=114_68b3bab2c0185eb1e62bb6f9789d799b&Itemid=75&lang=en (Page consultée le 10/06/2011)
30. Daniel Ducharme, « *Technologies et Normes archivistes* », Août 2005, en ligne : <http://www.otracuba.org/ressi/?q=isoducharme02> (Page consultée le 10/03/2012)
31. Agence nationale de sécurité des systèmes d'information, « *Référenciel Général de Sécurité* », Version 1.0, 6 mai 2010
32. Comité d'experts sur la protection des données sous l'égide du Comité européen de coopération juridique, « *Les numéros personnels d'identification : leur mise en oeuvre, leur utilisation et la protection des données* », Strasbourg 1991, en ligne : http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Pins_1991.pdf (Page consultée le 10/04/2011)
33. Maître Jean Baret, « *Législation française en matière de cryptologie* », modifié le 5 Mai 2010, en ligne : <http://knol.google.com/k/jean-baret/l%C3%A9gislation-fran%C3%A7aise-en-mati%C3%A8re-de/48a1rj5olrv8/12#> (Page consultée le 13/03/2011)
34. Maître Valérie Sedallian, « *Les problèmes posés par la législation française en matière de chiffrement* », Revue Droit de l'informatique et des télécoms, 1998/4 p. 23
35. Jack Kelley, « *Terror groups hide behind Web encryption* », 05 Février 2001, en ligne : <http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen.htm> (Page consultée le 25/06/2012)

36. Jeremy Quirke, « *Security in the GSM system* », 1er Mai 2004, en ligne : http://www.it.iitb.ac.in/~kavita/GSM_Security_Papers/Security%20in%20the%20GSM%20system%2001052004.pdf (Page consultée le 01/08/2012)
37. INRIA, CESAM, « *Les Courbes Elliptiques pour la Sécurité des Appareils Mobiles* », Octobre 2006
38. Farhat Ullah Khan, Surbhi Bhatia, « *A novel approach to genetic algorithm based cryptography* », White Globe Publications, International Journal of Research in Computer Science – Volume 2 Issue 3 (p. 7-10)
39. Joanna Rutkowska, « *Introducing Stealth Malware Taxonomy* », COSEINC Advanced Malware Labs, November 2006, en ligne : <http://www.net-security.org/dl/articles/malware-taxonomy.pdf> (Page consultée le 10/08/2012)
40. Yves Michaud, « *Université de tous les savoirs – Qu'est ce que l'Univers – volume 4* », Editions Odile Jacob , février 2001

Annexes

Annexe 1

THE TABLEAU DE VIGENERE

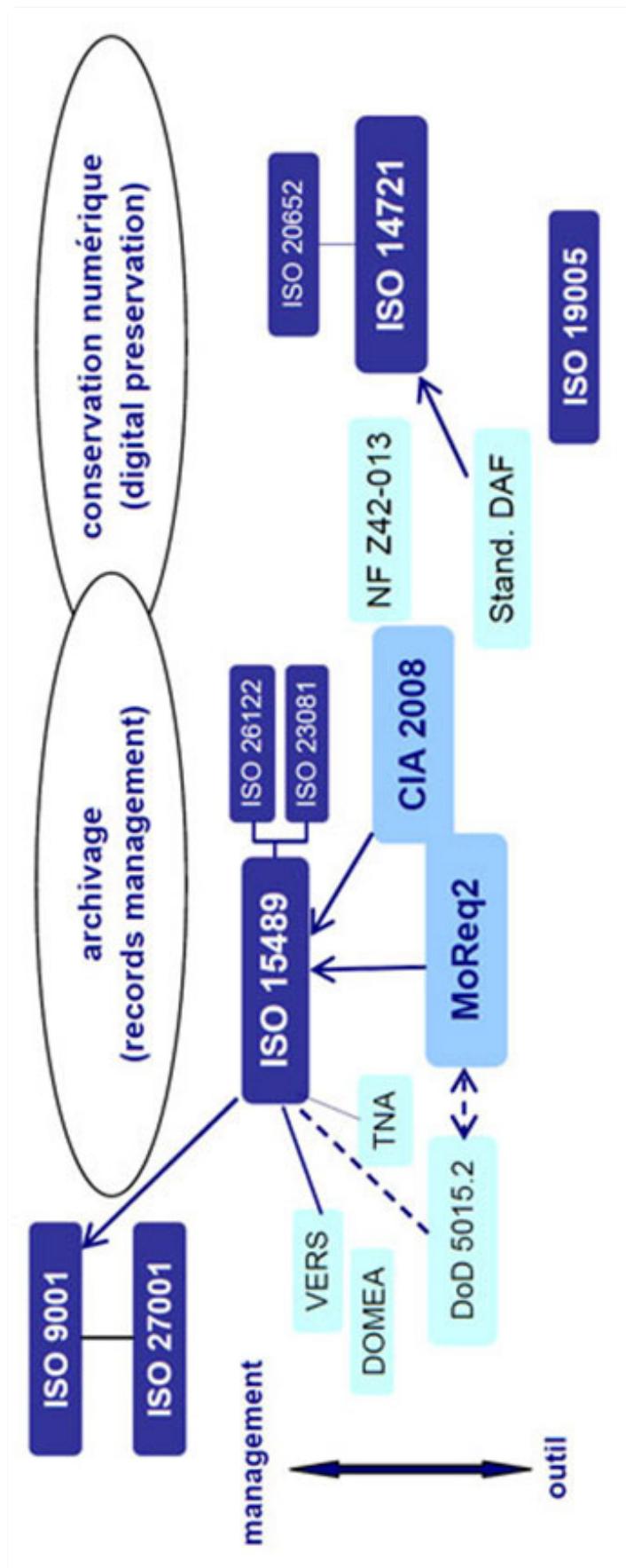
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y

Tableau de Vigénère

Annexe 2



Machine ENIGMA



Panorama des normes en matière de stockage de l'information

Annexe 4

Function	Roles			
	User Roles		Administrative Roles	
	End User	Reviewer	Local Administrator	Central Administrator
Add new classes	No	No	Yes	Yes
Create new files	Yes	No	Yes	Yes
Change file metadata	No	Yes	Yes	Yes
Maintain classification scheme and files	No	No	Yes	Yes
Delete files	No	No	Yes	Yes
Capture records	Yes	No	Yes	Yes
Relocate a record to a different file	Yes	No	Yes	Yes
Search for and read records	Yes	Yes	Yes	Yes
Change content of records	No	No	No	No
Change record metadata	No	Yes	Yes	Yes
Delete records	No	No	Yes	Yes
Place and remove disposal holds	No	Yes	Yes	Yes
Retention and disposition schedule and disposition transactions	No	Yes	Yes	Yes
Export and import files and records	No	Yes	Yes	Yes
View audit trails	No	Yes	Yes	Yes
Configure and manage audit trail	No	No	No	Yes
Change audit trail data	No	No	No	No
Move audit trail data to off-line storage media	No	No	Yes	Yes
Perform all transactions related to users and their access privileges	No	No	Yes	Yes
Allocate access permissions to local administrators	No	No	No	Yes
Allocate own access permissions also to other users	Yes	Yes	Yes	Yes
Set up and manage case management roles	No	No	No	Yes
Maintain database and storage	No	No	Yes	Yes
Maintain other system parameters	No	No	No	Yes
Define and view other system reports	No	Yes	Yes	Yes

Annexe 5

Introduction :

A furious war of the future of our society is underway for most, this war is invisible. On the one side, a network of governments and corporations spy on everything we do, on the other the cypherpunks virtuosos geeks activists who make code and shake public policy. This is the movement which borned wikileaks. I am joined by three cypherpunks friends, from Germany Andy Müller-Maguhn, from France Jérémie Zimmermann and from the United States Jacob Appelbaum, I want to ask them is the future of the world the future of the Internet.

[...]

Julian Assange :

I want to take a look of the three basic freedoms. When I interviewed the head of Hesbollah Hassan Nasrallah.

Jacob Appelbaum :

What's that up there ?

[...]

Julian Assange :

I want to go back to this three fundamental freedoms, freedom of communication, freedom of movement, and freedom of economic interaction. So if you look at the transition of our global society onto the internet when me made that transition the

freedom of personal movement is unchanged essentially. The freedom of communication is unhand tremendously in some way in that we now can communicate with many more people and in the other hand is also tremendously degraded because there is no privacy anymore and so our communication can be spied on, are spied on and stored and as a result can be used against us. So this is a sort of militarization of these interactions and our economic interactions have suffered precisely the same consequences.

Andy Müller-Maguhn :

Julian it's not wrong what you have being saying but I'm not sure you can really distinguish between point 2 and 3, because the internet that we have today is an infrastructure for our social, our economic, our cultural, our political and other things. So however the communication architecture is, the money is just bits, this is just a use of the internet.

[...]

Andy Müller-Maguhn :

If you compare the military budget to the cost of surveillance and the cost of cyber warriors. Normal weapon system cost a lot of money. If you compare cyber warriors and mass surveillance, that is very cheap, super cheap compare to just one aircraft.

Jérémie Zimmermann :

There are 2 questions there. We also have this example of EAGLE the system sold by the French company Amesys that was sold to Kaddafi's regime in Libya and on the commercial document it was written nationwide interception mechanism. That a big box that you put somewhere and you just listen to all your people communication so we can discuss about the technology, I'm interested very much by that.

Julian Assange :

Ten years ago this was saying to be a fantasy. It was saying to be something only paranoid people believed in but the cost of doing it have now decreased at the point where even countries like Libya with relatively few resources was doing it with French technology.

Jérémie Zimmermann :

So now that's a fact, technology enables total surveillance of every communications. Then, there is the other side of that coin, what do we do with it. We could admit for what you call the tactical one there is indeed some legitimate use. Investigators investigating on bad guys, network of bad guys and so on they need, under the supervision of the judicial authority, to be able to use such

tools. But the question is where to draw this judicial supervision, where to draw the control that the citizens can have over the use of these technologies and this is a policy issue, and when we get to this policy issue you have politicians that are asked to just sign something and don't understand the underlying technology.

[...]

Julian Assange :

Now we take our personal life and we put it all on facebook we communicate using internet we communicate using mobile phones which is now meshed to the internet and the military or the intelligence agencies have control of that data or are studying that data so this is some kind of militarization of civilian life.

[...]

Jacob Appelbaum :

There is no question that this kind of technology is a weapon in places like Syria or in places like Libya, where they specifically use this surveillance equipment to target people politically, they targeted people in the United Kingdoms using French equipment that would be illegal to run in France.

[...]

Julian Assange :

This line between government and corporation, if you look at the expansion in the military contractive sector in the west over the past 10 years, the National Security Agency, which is the biggest wide agency in the world, had 10 primary contractors on their books who they worked with. Now, two years ago, they've got one thousand contracts so there is a spreading out a smearing out of the border between governments and companies.

[...]

Jacob Appelbaum :

In our twitter case so far which unfortunately I can't talk about because I don't actually live in a free country [...] For the twitter case it's public that we lost the stay where we said that disclosing this data to the government would do a irreparable harm because they will not forget this data once they receive it and the government said your stay is denied and twitter must disclose this data.

[...]

Julian Assange :

This is a political radicalization of the internet youth over the past 2 years especially. You've been all over the world, talking to people who want anonymity want privacy in relation to their own government. You must

have seen in many different countries this phenomena, is it something significant ?

Jacob Appelbaum :

Sure, it's absolutely significant, I want to Tunisia after Ben Ali's regime fell and you see that there is a sort of awakening about that. But I think you're wrong to say that it just happen the last couple of years
[...]

Julian Assange :

We all speak about the privacy of communication and the right to publish and that something that is quite easy to understand because it has a long history and in fact journalist love to talk about this because they're protecting their own interests. But if we compare that value to the value of the privacy and freedom of economic interaction [...] isn't actually the freedom or privacy of economic interaction more important than the freedom of speech?

Andy Müller-Maguhn :

That's a very though one

Julian Assange :

If you just look from a simple intelligence

perspective you got a 10 million dollar intelligence project you can spy on peoples email interaction or you could have total surveillance of economic interactions which one would you prefer ?

[...]

Andy Müller-Maguhn :

Where it is a very interesting thing from the cables leaks. It is the Russian government trying to negotiate a way that Visa Mastercard payment from Russian citizens within Russia would have to be processed in Russia and Visa Mastercard actually refused it. [...] Meaning that even payments from Russian citizens in Russia to Russian shop would be processed to American datacenters so United States would have a restrictional control. And that of course is very unsatisfying situation independent of the fact that I like US or not it's just a very central dangerous thing to have a central place where all payments are stored because it invites de facto to all kind of usage of that data.

[...]

Jacob Appelbaum :

[...] What cypherpunks wanted to do was to create systems where they can compensate each other in a truly free way where it is not possible to interfere, and with financial issues it is the most dangerous thing to be

working on. I mean they're is a reason that the persons that created bitcoin did it so anonymously.

[...]

Julian Assange :

Are you sure it's a problem Jérémi maybe in fact it's a good tribute that those industries that are productive, they produce wealth for the all society they have the money in order to make sure that they continue to be productive and random legislation that comes out of a political mythmaking isn't constraining their productivity and the best way to do that is to buy congressman to take the labor of your productive industry and use it to modify the law and keep the productive nature of your industry.

[...]

Jérémie Zimmermann :

When you say let the dominant actors decide what the policy will be I can answer you from the perspective of what was the internet in the last fifteen years where innovation was so called bottom up where new practices emerged out of nothing where a couple of guys in a garage invented a technology that spread.

Julian Assange :

For nearly everything for Apple for Google

for Youtube...

[...]

Jérémie Zimmermann :

My point here is that policy have to adapt to society and not the other way around. We have the impression with the copyright war that legislators try to make the whole society to change to adapt to a framework that is defined by Hollywood. [...]

What we are discussing since the beginning are all global issues whether we're talking of the financial system whether we're talking of corruption whether we're talking of geopolitics or energy or environment all of these are global problems that mankind

is facing today and we still have one global tool between our hands that enables better communication, better sharing of knowledge better participation in political and democratic process. What I feel is that a global universal internet is the only tool we still have to resolve those global issues.

[...]

Julian Assange :

There is this notion from cypherpunks that code is law on the internet what you can do is defined by what programs run and therefore code is law.

Annexe 6

Nassim Ben Ghmiss :

Plus un système cryptographique est libre d'accès pour une analyse, plus il est considérable comme sûr

on s'est rendu compte 10 ans après à l'aide de la cryptanalyse différentielle que l'algorithme était vulnérable. Sauf dans le cas de l'utilisation de ces tables fournies par la NSA. Ils avaient donc 10 ans d'avance au niveau de la cryptanalyse.

Emmanuel Fleury :

Depuis les années 1980 le principe de Kerckhoff est appliqué dans l'analyse d'un algorithme cryptographique. Ce principe consiste à partir de l'hypothèse que l'attaquant a accès au code de l'algorithme et donc que l'accès est total. L'algorithme ne doit donc pas donné de détails par rapport au secret protégé. Bien sûr cela concerne les algorithmes cryptographiques et non les protocoles cryptographiques

Nassim Ben Ghmiss :

Présentez vous en quelques mots

Emmanuel Fleury :

Je m'appelle Emmanuel Fleury, je suis maître de conférence à l'Université de Bordeaux 1 dans deux branches différentes, au sein du Master Ingénierie des Systèmes Critiques comme enseignant en Vérification Logicielle et au sein du Master Cryptologie et Sécurité où je donne des cours sur la Sécurité Logicielle. Je suis également chercheur au LabRi de Bordeaux. Je suis donc à cheval sur deux domaines d'expertises, le génie logiciel pour l'aspect algorithmique et les mathématiques.

Nassim Ben Ghmiss :

Plus une information est accessible, plus elle est vérifiable

Emmanuel Fleury :

Ceci n'est pas totalement vrai. En effet, pour vérifier un algorithme, peu importe le nombre de personnes qui peuvent y accéder. Dans la majorité des cas la découverte de failles dans un algorithme est fait par des experts qui sont payés pour analyser un algorithme. Comme dans le cas du DES qui est un chiffrement par bloc où des tables statiques sont nécessaires. La NSA a fourni très tôt les tables statiques à utiliser puis

Nassim Ben Ghmiss :

Qu'est ce qu'une information sensible ?

Emmanuel Fleury :

C'est une information dont on ne souhaite pas qu'elle soit divulguée. Pour cela on met en général en place un système de niveaux d'accès. Pour le domaine militaire

par exemple avec la classification militaire, secret, secret défense, très secret défense...

Nassim Ben Ghmiss :

Qu'est ce que la cryptologie ? La stéganographie ?

Emmanuel Fleury :

La stéganographie consiste à cacher un média donné dans un autre média tout en gardant le média d'origine intact. C'est une branche de la cryptologie. Un exemple de stéganographie simple étant de donné une signification aux espaces dans un texte et d'y cacher un message.

La cryptologie est différent de la cryptographie. La cryptologie est la science des procédés cryptographiques. Elle est composée de la cryptographie et de la cryptanalyse. La cryptanalyse est l'analyse des procédés cryptographiques. La cryptographie consiste à rendre un message intelligible seulement par la personne possédant la clé de cryptage.

Nassim Ben Ghmiss :

Un algorithme cryptographique est-il libre d'accès à tous ?

Emmanuel Fleury :

Pas forcément mais lors de l'analyse par des experts, on part du principe que l'algorithme

est libre d'accès. Les algorithmes qui ne sont pas libres sont analysés pour passer certaines certifications et c'est lors de cette analyse que l'on part de ce postulat.

Nassim Ben Ghmiss :

Quels sont selon vous les algorithmes les plus utilisés ?

Emmanuel Fleury :

En matière de cryptage symétrique, on peut citer le cryptage par bloc AES qui est très utilisé. Il existe le cryptage par flot RC4 mais il a été prouvé qu'il montre quelques faiblesses. En cryptage asymétrique il existe le cryptage RSA qui est assez utilisé et dont le principe fondateur est basé sur la factorisation de nombres premiers. Mais comme les ordinateurs sont de plus en plus performant, une nouvelle méthode basée sur les courbes elliptiques a vu le jour et donc l'algorithme ElGamal est devenu de plus en plus répandu.

Il existe aussi les algorithmes de hashage, dont le MD5 et le SHA sont les plus utilisés.

Nassim Ben Ghmiss :

Quelles sont les normes en vigueur en matière de cryptographie au niveau national ? Sont-elles suffisantes ?

Les normes actuelles sont EBIOS, l'ensemble

ISO 27000 et la norme MEHARI. Ces normes ne sont que des recommandations à suivre pour améliorer la sécurité mais pour la mise en place sur une infrastructure, il est indispensable de contracter un expert en la matière qui a les connaissances et le savoir faire sinon les recommandations seront inutiles.

Nassim Ben Ghmiss :

Que pensez-vous du système d'authentification par certificat mis en place actuellement ?

Emmanuel Fleury :

Et bien on en revient au problème du tiers de confiance c'est à dire qu'il faut qu'il y ait une confiance mutuelle entre l'émetteur et le récepteur de l'autorité de certification.

En effet, il est tout à fait possible de se faire passer pour l'autorité de certification et d'exploiter cette confiance mutuelle. C'est pour cela qu'il existe un niveau hiérarchique d'autorité de certification permettant d'assurer une meilleure sécurité dans les niveaux de confiances. De plus avec le protocole https par exemple il est possible de se faire passer pour une autorité de certification d'où la création de liste de confiance pour savoir si une autorité est oui ou non légitime. Mais là on parle de protocole de cryptographie.

Nassim Ben Ghmiss :

Au niveau législatif, pensez-vous que les lois Françaises sont adaptées à la protection des données personnelles ?

Emmanuel Fleury :

La loi Française offre depuis les années 2000 la possibilité de choisir la taille de la clé de cryptage. Ce qui permet d'avoir un cryptage sûr des informations. Avant il fallait se déclarer auprès d'organismes spécialisés et de l'armée si l'on utilisait une clé de taille supérieur à 256 bits.

Nassim Ben Ghmiss :

La cryptographie limite-t-elle l'accès à l'information dans sa globalité ?

Emmanuel Fleury :

Et bien, c'est le principe de la cryptographie de limiter l'accès à une information. Je m'intéresse plus à comment fonctionne les algorithmes cryptographiques qu'à l'usage qu'on en fait. Ceci relève plus au domaine du protocole cryptographique et des réseaux sécurisés. En ce qui concerne les informations publiques, ce n'est pas de notre ressort de nous intéresser aux usages de la cryptographie mais plus de s'intéresser à son fonctionnement intrinsèque.

Nassim Ben Ghmiss :

Oui mais cela peut-il être une astreinte à la liberté de s'informer ou d'apprendre par exemple ?

Emmanuel Fleury :

Il est vrai que dans les nouveaux périphériques on utilise de plus en plus de procédés cryptographiques limitant l'utilisation de ceux-ci. On peut parler des téléphones portables par exemple où l'utilisation est limitée par des cryptages. Personnellement, il m'est arrivé d'être limité par des cryptages lors de travaux.

Nassim Ben Ghmiss :

Est-il vrai que la technique de chiffrement par courbe elliptique présente des faiblesses?

Emmanuel Fleury :

Non le chiffrement par courbe elliptique n'est pas en soi sensible à une faiblesse. En effet, il a été vérifié et déclarer conforme. Par contre il est vrai qu'étant donné l'utilisation de logarithme discret dans son fonctionnement, seuls certains domaines de courbes sont jugé totalement sûrs.

Nassim Ben Ghmiss :

Cette faiblesse du domaine de courbe n'a pas été publiée par la NSA lors de la présentation de l'algorithme par courbes

elliptiques, pourquoi ?

Emmanuel Fleury :

En effet, lors de sa création, le chiffrement par courbe elliptique était considéré comme sûr peu importe le domaine de courbes. Mais il s'est avéré plus tard que des cryptanalystes indépendants ont découvert cette faiblesse.

Nassim Ben Ghmiss :

Pensez vous que la NSA a caché cette faiblesse étant donné son avance technique dans le domaine ?

Emmanuel Fleury :

Non je ne pense pas. En effet, les différences d'avancement en matière de cryptographie militaire et civile ont tendances à se réduire. Je pense que cela est principalement dû au fait qu'aujourd'hui il y a de plus en plus de sociétés privées qui se spécialisent dans le secteur et qui font leurs propres audits avec des experts civils. C'est certainement dû au fait que de plus en plus la cryptographie est utilisée dans des dispositifs comme les cartes à puces, la téléphonies et autres...

Annexe 7

```
/* ****
 * Copyright 1998 VMware, Inc. All rights reserved. -- VMware Confidential
 * **** */

/*
 * vmkemit.h --
 *
 * Code emission macros for base x86 architecture used by vmkernel.
 *
 * All macros increment the memptr variable, which must be defined either
 * as a local or global variable, and point to some buffer.
 */

#ifndef _VMK_EMIT_H_
#define _VMK_EMIT_H_

#define INCLUDE_ALLOW_VMKERNEL
#include «includeCheck.h»

#include «x86.h»

/*
 * Emit location pointer
 */
typedef uint8 *EmitPtr;

/*
*-----
* MNEP -- opcode mnemonics
*-----
*/
#define NO_SEGMENT_OVERRIDE -1
#define MNEP_PREFIX_CS 0x2e
#define MNEP_PREFIX_SS 0x36
#define MNEP_PREFIX_DS 0x3e
#define MNEP_PREFIX_ES 0x26
#define MNEP_PREFIX_FS 0x64
#define MNEP_PREFIX_GS 0x65

#define MNEP_PREFIX_OPSIZE 0x66
#define MNEP_PREFIX_ASIZE 0x67
#define MNEP_PREFIX_LOCK 0xF0
#define MNEP_PREFIX_REPN 0xf2
#define MNEP_PREFIX REP 0xf3

#define MNEP_TEST_IMM8 0xf6
#define MNEP_TEST_IMMV 0xf7
```

```

#define MNEM_OPCODE_ESC      0x0f /* Two byte instruction escape (<>prefix>). */
#define MNEM_ADC             0x13
#define MNEM_ADD             0x03
#define MNEM_CMP             0x3b
#define MNEM_CMP_EAX         0x3d
#define MNEM_SUB             0x2b
#define MNEM_NOT8            0xf6
#define MNEM_NOT              0xf7

#define MNEM_PUSH_EAX        0x50
#define MNEM_PUSH_ECX        0x51
#define MNEM_PUSH_EDX        0x52
#define MNEM_PUSH_EBX        0x53
#define MNEM_PUSH_ESP        0x54
#define MNEM_PUSH_EBP        0x55
#define MNEM_PUSH_ESI        0x56
#define MNEM_PUSH_EDI        0x57

#define MNEM_POP_EAX          0x58
#define MNEM_POP_ECX          0x59
#define MNEM_POP_EDX          0x5A
#define MNEM_POP_EBX          0x5B
#define MNEM_POP_ESP          0x5C
#define MNEM_POP_EBP          0x5D
#define MNEM_POP_ESI          0x5E
#define MNEM_POP_EDI          0x5F
#define MNEM_POP_MEM          0x8F

#define MNEM_NOP              0x90
#define MNEM_MOVE_REG_RM      0x89
#define MNEM_MOVE_RM_REG      0x8b

#define MNEM_PUSH              0x68
#define MNEM_PUSHF             0x9c
#define MNEM_POPF              0x9d
#define MNEM_PUSHA             0x60
#define MNEM_POPA              0x61

/*
*-----
* 
* EMIT -- emission macros (memptr implicit)
*
* We try to adopt the following naming convention: For the macros
* that are named EMITxx_yyy, the value <>xxx>> represents the current
* codesize. All operands are assumed to have the same size as the
* codesize, unless otherwise specified. The macros named EMIT_yyy
* should work for any codesize.
*
*-----
*/

```

Annexe 8

		NAT Truck Remission / Reroute / Cancellation Request					
		257th Joint Movement Control Battalion 4th Joint Sustainment Command (Expeditionary) Bagram Air Field, Afghanistan					
TMR NUMBER	ABC5650	CARRIER	WZG	MCB NEW TMR NUMBER			
LMR NUMBER	BAFMCT5987T12FEB	MCB MAKES NEW LMR #		MCB NEW LMR NUMBER			
SUBMIT DATE	17-Mar-12	SUBMIT TIME	12:32:57 PM	RETURN TIME			
SITUATION (MARK WITH AN "X")							
<input checked="" type="checkbox"/>	TRUCK HAS ARRIVED AT ITS ORIGIN AND NEEDS TO BE SENT TO A DIFFERENT DESTINATION REMISSION						
<input type="checkbox"/>	TRUCK HAS ARRIVED AT ITS ORIGIN AND NEEDS TO BE SENT TO A NEW ORIGIN AND DESTINATION CANCELLATION AND NEW MISSION						
<input type="checkbox"/>	TRUCK HAS ARRIVED AT ITS DESTINATION AND NEEDS TO BE SENT TO A NEW DESTINATION MISSION COMPLETE AND NEW MISSION						
<input type="checkbox"/>	TRUCK HAS ARRIVED AT ITS DESTINATION AND NEEDS TO BE SENT TO A NEW ORIGIN AND DESTINATION MISSION COMPLETE AND NEW MISSION						
<input type="checkbox"/>	CANCEL THIS TMR CANCELLATION						
REQUESTOR INFORMATION							
REQUESTOR UNIT	486TH MCT		SIPR EMAIL	N/A			
REQUESTOR POC	SFC PRITCHETT, COLIN		SVOIP	775-3216			
REQUESTOR DSN	775-3205						
REQUESTOR NIPR EMAIL	COLIN.PRITCHETT@AFGHAN.SWA.ARMY.MIL						
REASON FOR REMISSION	CARGO NEEDED AT NEW LOCATION						
ORIGIN POC INFORMATION							
ORIGIN UNIT	578th EN BN		SIPR EMAIL	N/A			
ORIGIN POC & NIPR PHONE	1LT BULAONG, JESSE / 775-3203		SVOIP	775-3203			
ORIGIN NIPR EMAIL	jesse.bulaong@afghan.swa.army.mil		ORIGIN	ARYAN			
			ORIGIN PROVINCE	GAZNI			
DESTINATION POC INFORMATION							
DESTINATION UNIT	842nd EN CO		SIPR EMAIL	N/A			
DESTINATION POC & NIPR PHONE	1LT GLEASON, CLINTON / 552-1363		SVOIP	552-1363			
DESTINATION NIPR EMAIL	clinton.gleason@afghan.swa.army.mil		DESTINATION	AB BAND			
CUSTOMER PASSPHRASE -->	AB BAND BUILD		<-- ANY WORD OR PHRASE UP TO 20 CHARACTERS				
CARGO INFORMATION							
TRUCK TYPE	40' LOWBOY	CARGO DESCRIPTION	20' CONEX (EMPTY) & HESCO BARRIERS				
WEIGHT (LBS)	30000	ADDITIONAL REMARKS	18 EN BN MATERIALS TO AB BAND				
CANCELLATIONS							
REASON FOR CANCELLATION							
MCT / MCB USE ONLY							
MCT APPROVED BY			MCB APPROVED BY				
TRACKER UPDATED BY (SIGN)			CARRIER APPROVED BY				
SEQUENCE #	5650	EXPECTED ARRIVAL DATE		GDMS NUMBER			
HV / MIL ESC	HV / MIL ESC	SUPPLY CLASS	CL VII				
<i>217 Willie Murray</i>							
Received at AB Band by , <i>J.L.</i>				Version 03-1.7			
EMAIL THIS FORM TO YOUR LOCAL MCT <i>3-21-2012</i>							

Document militaire ayant fuité du CEIEC