La sécurité des réseaux et des systèmes

Michel Riguidel

La sécurité des réseaux et des systèmes

Michel Riguidel

Mots-clés : sécurité, sûreté, confiance, confidentialité, intégrité, disponibilité, infrastructure critique, système embarqué, menace, vulnérabilité, piratage, cybercriminalité, cyberterrorisme, traçabilité, cryptographie, chiffrement, signature, authentification, protocole cryptographique, pare-feu, pot de miel, biométrie, stéganographie, tatouage, carte à puce, IGC, PKI, SSL, IPSec, VPN, PGP, IDS, SIM, WEP.

Résumé : La sécurité est un enjeu majeur des technologies numériques modernes. Infrastructures de télécommunication (GSM, GPRS, UMTS), réseaux sans fils (Bluetooth, WiFi, WiMax), Internet, systèmes d'information, routeurs, ordinateurs, téléphones, décodeurs de télévision, assistants numériques, systèmes d'exploitation, applications informatiques, toutes ces entités présentent des vulnérabilités : faille de sécurité, défaut de conception ou de configuration. Ces systèmes tombent en panne, subissent des erreurs d'utilisation et sont attaqués de l'extérieur ou de l'intérieur par des pirates ludiques, des cybercriminels, ou sont la proie d'espionnage industriel. Une approche globale de la sécurité des systèmes est essentielle pour protéger la vie privée, pour défendre le patrimoine d'une entreprise ou pour réduire les vulnérabilités des grands systèmes d'information. Ce chapitre présente d'abord les différents aspects de la sécurité : politique et fonctions de sécurité, menaces et vulnérabilités. Nous introduisons ensuite les principes et les mécanismes de sécurité : cryptographie (chiffrement, signature, protocoles cryptographiques), infrastructure de confiance (IGC ou PKI, certificats). Nous exposons les solutions de sécurité : SSL, IPSec, VPN, sécurité des réseaux cellulaires, de l'Internet et sans fil, pare-feu, système de détection d'intrusion, pot de miel, biométrie, carte à puce, sécurité des systèmes embarqués, des systèmes d'exploitation, des logiciels et tatouage. Nous terminons par un panorama des défis de la recherche en sécurité.

Introduction

Virus informatiques, actes de malveillance interne ou externe, failles de sécurité, espionnage industriel, tous ces dangers constituent la préoccupation majeure des responsables informatiques des entreprises. Cette inquiétude se manifeste aussi chez les utilisateurs et parvient même à troubler la confiance des citoyens dans leur relation avec les technologies numériques : fraude informatique, usurpation de numéro de carte bancaire, vol de carte de téléphonie mobile, irruption de sites sordides sur Internet, invasion de la messagerie non sollicitée, atteinte à la vie privée, filature électronique, vidéosurveillance, inquisition numérique. La sécurité des réseaux et des systèmes est une discipline en pleine évolution, au rythme du déploiement d'une urbanisation digitale autour de l'activité humaine, de l'appropriation concomitante des technologies numériques par un large public, du joug fatal et incontournable à la société numérique et même de l'addiction à Internet ou au téléphone mobile d'une partie de la population. La naissance d'une ubiquité de la communication qui permet de se brancher sur les infrastructures de réseaux, en tout lieu et en tout temps, et l'émergence d'une ubiquité du calcul qui permet de traiter l'information sur ces infrastructures ont provoqué des phénomènes croissants de délinquance informatique. La cybercriminalité, prolongement de la violence du monde réel qui se reflète dans le monde virtuel, emprunte la brèche essentielle des systèmes numériques : la volatilité de l'information. Une donnée numérique peut être divulguée, copiée, plagiée, falsifiée ou détruite. Dans l'univers numérique, véritable village virtuel violent, il n'existe pas une œuvre originale avec des éventuelles copies, il n'existe que des clones identiques que l'on peut reproduire à l'infini. Ce miroir multiplicateur est une vulnérabilité engendrée par l'indépendance consubstantielle à la nature numérique entre le support physique et le contenu intangible de l'information.

Pour accompagner la croissance[1] incoercible des patrimoines numériques des personnes et des entreprises, il est indispensable de contrecarrer les accidents dus à la fatalité aussi bien que les actions malveillantes des pirates par une politique de sécurité qui doit être mise en vigueur, par chaque citoyen et dans chaque institution, grâce à un dispositif, à la fois technique et organisationnel. La gamme des méthodes actuelles et des outils existants permet de parer aux erreurs humaines et aux périls qui risquent de porter atteinte à la confidentialité, à l'intégrité ou à la disponibilité des réseaux et des systèmes.

Par ailleurs, la recherche en sécurité est en plein essor. L'objectif est d'améliorer la maîtrise de la circulation des informations sur les réseaux, de favoriser la dissémination des applications informatiques et d'encourager l'appropriation des technologies numériques par un large public.

Dans ce chapitre sur la sécurité, nous rappellerons les impératifs de sécurité, les menaces et les risques. Nous exposerons ensuite les techniques de sécurité, qui s'appuient essentiellement sur un catalogue de fonctions de sécurité qu'il faut exhiber pour contrer les menaces. Ces fonctions de sécurité mettent en œuvre des techniques cryptographiques pour protéger les informations ou pour sécuriser les interfaces entre les ordinateurs. De plus, des dispositifs particuliers de sécurité existent et sont déployés pour sécuriser des points sensibles des réseaux, comme les points d'accès ou les frontières des systèmes. La gestion de la sécurité est le point délicat de ces techniques car il faut notamment sécuriser ces fonctions de sécurité. Après un tour d'horizon des protocoles cryptographiques, des architectures de sécurité des différents réseaux, des dispositifs de sécurité, de la sécurité des divers systèmes et des contenus, nous esquisserons les verrous technologiques de la recherche en sécurité numérique.

[1] Le volume des données double tous les ans. Il est en relation avec le coût du stockage qui baisse d'un facteur 2 chaque année.

Une urbanisation digitale fragile

Depuis la chute du mur de Berlin, on observe un mouvement général dans le monde, l'effondrement des frontières accordant une libre circulation des marchandises, des individus et des idées. Les systèmes numériques n'échappent pas à cette tendance. Une évolution des services, des infrastructures, des réseaux et des architectures informatiques, s'organise autour d'utilisateurs plus nomades, avec des éléments mobiles ou déplaçables[2], par du matériel informatique modulaire[3], du logiciel mobile et des données fluides[4]. De vastes infrastructures s'échafaudent depuis le succès d'Internet. Une urbanisation hétérogène s'installe au niveau des réseaux d'accès pour quadriller la Terre et créer une ubiquité de la communication. Des initiatives de métacalcul[5] briguent la complexion d'une ubiquité des calculs pour entrer en compétition avec les réseaux d'information actuels. Tous ces mouvements se construisent autour des deux ressorts de la technologie moderne : Internet et les réseaux cellulaires.

- Internet s'est révélé un authentique laboratoire informatique en vraie grandeur, un pur accélérateur d'expérimentation et d'usage et a fédéré grâce à sa capacité d'interconnexion (réseau de réseaux, avec le protocole IP comme point focal) de nouveaux concepts[6] sur des principes efficaces de simplicité et a balayé sur son passage des concepts désormais caducs[7]. Malgré cette réussite, Internet a acquis au fil du temps une mauvaise réputation, en termes de sécurité et d'intimité numérique, forgée sur le caractère anonyme et virtuel de son fonctionnement et accentuée par les conséquences néfastes de l'éthique libertaire prônée par ses précurseurs.
- Les réseaux cellulaires ont réuni les utilisateurs autour du sentiment d'appartenir à une communauté délivrée du carcan des fils et des câbles, branchée sur le monde, et ont ressuscité au niveau du développement logiciel, l'informatique « janséniste » et confinée du temps réel embarqué[8]. Les réseaux sans fil WiFi à la bordure de l'Internet ont connu des failles de sécurité, la nomadicité des usagers et la portabilité des terminaux (téléphone mobile avec carte SIM, agenda électronique) ont suscité des vols et déclenché des fraudes et des abus.

Notre société de l'information est ainsi devenue complexe et fragile. Il s'établit de fréquentes interdépendances entre les différents systèmes d'information et de communication et les nombreux domaines d'activités : administration, banque, énergie, transport, santé et défense. Deux tendances inquiétantes doivent faire l'objet d'un éclairage spécifique :

- Monochromie : la société de l'information converge vers un monde plus interconnecté et uniformisé, suite au nivellement de la technologie par les standards du marché. En informatique et communication, l'étanchéité et l'hétérogénéité des systèmes propriétaires jouent de moins en moins leur rôle protecteur. Ce monde décloisonné et monochrome favorise la vulnérabilité à toutes sortes d'agressions fortuites ou préméditées, parfois propagées en cascade par les infrastructures qui fonctionnent de plus en plus en interdépendance.
- Flux tendus : l'évolution à venir imbriquera changements techniques, comportementaux et organisationnels et même psychologiques comme en témoigne notre addiction grandissante aux technologies des communications. Les entreprises sont dites agiles, avec des cycles de décision à boucle de réaction courte et des cycles d'approvisionnement à flux tendus. Or la sécurité évolue elle-même vers le flux tendu (mise à jour de logiciels, d'antivirus) et son efficacité sera ainsi de plus en plus précaire et confrontée à des menaces croissantes. La sécurité de la reconfigurabilité et de la mise à jour du matériel et du logiciel accueillant les évolutions technologiques, est un défi majeur pour les techniques numériques.

[2] Les constellations de satellites ou les réseaux ad hoc sont des exemples d'infrastructures mobiles.
[3] Les périphériques en *plug & play* se sont généralisés.
[4] Par exemple, technologie *push*, messagerie, flux vidéo, téléchargement de fichiers, applets Java.
[5] Les grilles et l'externalisation de l'informatique sont à la mode mais présentent de réels problèmes de sécurité.
[6] Citons XML, Java, navigateur asynchrone, lecteur synchrone, sites Web, protocoles Internet de l'IETF, architecture en pair à pair.
[7] On observe une réelle crainte envers les structures propriétaires, l'informatique cloîtrée et l'ordinateur personnel hypertrophié. Cependant le marché informatique fonctionne souvent encore avec des innovations propriétaires qui évoluent, ne s'ouvrent et se standardisent que bien plus tard, avec le succès de la technologie en question.
[8] Elle se caractérise par de nouveaux systèmes d'exploitation temps réel, des ateliers de développement logiciel formel, des optimisations de compilation du code en taille ou en temps, de la validation plus sûre.

Le domaine de la sécurité

Les enjeux

La sécurité comporte des enjeux essentiels d'ordre stratégique puisque, dans le monde contemporain, les individus physiques (mais aussi les robots ou les entités logiques) doivent pouvoir communiquer, l'information doit être accessible sur les réseaux, que l'on soit au bureau, en voyage ou à domicile.

Le premier enjeu est de maîtriser le cycle de vie, le transport, le traitement et le stockage des patrimoines numériques. Le patrimoine numérique peut être personnel, industriel, intellectuel ou culturel. Il s'agit d'un enjeu politique de souveraineté pour enrayer la régence des contenus intangibles dans le cadre de la mondialisation. La technique maîtresse est ici la cryptographie, avec son cortège de protocoles cryptographiques utilisés à travers les réseaux.

Le deuxième enjeu est de valoriser les contenus[9] immatériels. Il s'agit d'assurer la libre circulation des contenus en toute confiance et de disséminer les œuvres, de rétribuer les auteurs et d'essaimer le savoir-faire. Il s'agit d'un enjeu économique. Les techniques font ici appel à la cryptographie mais aussi au tatouage électronique ou à la stéganographie, afin de dissimuler des détails secrets dans le corps même des œuvres, décelables exclusivement par leurs auteurs et les ayant-droits et de garantir ainsi leur propriété.

Le troisième enjeu est d'instaurer ou de restaurer la confiance dans l'univers numérique pour intensifier le commerce électronique, les échanges immatériels, l'administration électronique, voire la république[10] numérique. Il s'agit d'un enjeu social pour faciliter l'usage des nouvelles technologies et lutter contre la fracture numérique. Les techniques sont encore la cryptographie, mais aussi la sociologie de la confiance, car les usages, et notamment l'idée que l'on se fait de l'assurance de sécurité, ont ici un impact fort. Les infrastructures de confiance vont consister à administrer le cycle de vie de certificats, véritables cartes d'identité électroniques des interlocuteurs afin d'authentifier leurs échanges.

Le quatrième enjeu est de sécuriser les infosphères, c'est-à-dire la sphère privée immatérielle, ou bien le nuage de données, de programmes et de connexions appartenant à un sujet, selon les trois granularités suivantes :

l'infosphère de l'individu pour protéger sa liberté et préserver son intimité. Parmi la palette des techniques utilisées, la biométrie va permettre d'identifier les individus physiques, responsables des actions informatiques. Les personnes physiques se déplacent désormais avec un attirail électronique qui les assujettit à une traçabilité à leur insu. Le téléphone portable ou la carte bancaire peuvent être utilisés comme des instruments de filature électronique. Les enregistrements de factures détaillées, les agendas électroniques livrent des indications qui peuvent porter atteinte à la vie privée.

l'infosphère des organisations pour prévenir les attaques contre les biens ou l'image de marque de la personne morale, et pour lutter contre l'espionnage, le renseignement informatique. L'ouverture des systèmes d'information vers l'extérieur constitue un défi stratégique pour les entreprises. La sécurité de leur système d'information est donc devenue un élément crucial de la protection des actifs de l'entreprise. C'est ici que toute l'ingénierie des réseaux intervient. Des architectures de sécurité vont être mises en place afin de protéger la confidentialité des informations sensibles, de sécuriser l'intégrité des systèmes d'information (SI) et d'assurer la disponibilité des réseaux. On va installer des produits de sécurité aux endroits stratégiques du SI de l'entreprise : pare-feu à la frontière du SI pour filtrer les accès entrant et sortant, pots de miel dans une zone démilitarisée où est érigé le site Web, chiffreur IP à la lisière d'Internet, pour franchir, en toute confiance, le no man's land que sont les réseaux publics, système de détection d'intrusion au cœur du SI pour vérifier l'état du réseau et pour établir des lignes de défense en profondeur.

l'infosphère de l'État[11] dans l'objectif de réduire les vulnérabilités des infrastructures critiques avec leurs interdépendances (catastrophes à effet domino) et de traquer la cybercriminalité lourde.

Comme il n'existe pas de sécurité à 100% ou de construction à zéro défaut, le dernier enjeu est de gérer rapidement et efficacement les crises quand elles se déroulent, sans s'engouffrer inexorablement dans un engrenage vicieux de surenchères entre l'armure et la cuirasse, mais plutôt en tentant de surmonter le syndrome sécuritaire voire paranoïaque, qui guette souvent dès que l'on veut protéger le monde virtuel. Les techniques font appel aux modèles dynamiques de politique de

[9] Les contenus sont des données ou des programmes, comme les contenus multimédias, les logiciels, les «*Intellectual Properties*» (schémas informatiques de composants matériels) ou les bases de données (encyclopédies, programmes d'éducation à distance).

[10] Vote électronique, carte d'identité biométrique numérique.

[11] Les infrastructures critiques ne sont pas forcément directement dépendantes des États. Mais les opérateurs privés qui gèrent ces infrastructures ont en général des obligations vis-à-vis des États.

sécurité, aux méthodologies de gestion de crises (par escalades et paliers), aux modèles de confiance, aux méthodes d'autocicatrisation et à la théorie des jeux.

La typologie des réseaux et des systèmes

Le monde numérique des réseaux et des systèmes comprend :

- les réseaux informatiques : les réseaux locaux d'entreprises, les réseaux de vidéosurveillance sur IP, Internet, les réseaux sans fil (WiMax, WiFi, Bluetooth), les réseaux passifs d'étiquettes intelligentes (RFId) ;
- les réseaux de télécoms : les réseaux satellites, les réseaux de localisation GPS ou Galiléo, les réseaux téléphoniques, les réseaux d'opérateurs de téléphonie mobile (GSM, GPRS, EDGE, UMTS) ;
- les réseaux de diffusion de télévision (TNT, câble) et de radio mais aussi les réseaux résultant de la numérisation de la totalité du processus de production audiovisuelle, et ceux qui émergeront du déploiement des salles de cinéma numérique ;
- les SI de l'État, des institutions, des entreprises, des banques, des organisations, des réseaux à domicile (réseau domestique), de gestion des infrastructures critiques et du patrimoine numérique naissant des familles et des individus.

Le périmètre et la segmentation

Sécuriser un système impose de maîtriser son cycle de vie et son utilisation à bon escient, de contrôler son fonctionnement, de pérenniser son évolution et consiste à s'assurer que les ressources matérielles et logicielles ainsi que les informations d'une personne ou d'une organisation sont strictement utilisées dans le cadre général qui est prévu. La sécurité est une propriété qui contribue à l'intégrité d'un système dans son acception la plus large. Elle permet d'empêcher la conjoncture d'événements accidentels (perte de données, pannes de serveurs) ou intentionnels (messages parasites, saturations intempestives des ressources) qui le perturberaient. Ces périls d'occurrences aléatoires ou ces menaces issues d'une volonté malveillante, peuvent ou veulent porter atteinte à son domaine privé ou à ses secrets, altérer tout ou partie de ses organes, corrompre son environnement ou bien empêcher ou ralentir son fonctionnement habituel.

La sécurité englobe la sécurité des systèmes d'exploitation (OS), des logiciels, des communications interpersonnelles, de la messagerie, des données elles-mêmes, du partage des connaissances et de la propriété intellectuelle. La sécurité de l'informatique et des télécoms conjugue la liberté et la volonté de protéger les valeurs matérielles ou intangibles et leur image de marque, avec la correction des logiciels, la robustesse des architectures, l'immunité des applications, la résilience des systèmes, l'instillation et le maintien de la confiance dans les édifices numériques. L'importance croissante des liens hertziens, particulièrement sensibles, vient renforcer et compliquer cette priorité de sécurité.

La sécurité se décompose en plusieurs volets :

- la sécurité physique (l'innocuité) des lieux, des personnes et des biens, des infrastructures et des ressources matérielles[12], relative à des accidents (dégâts des eaux, sinistres) ou des sabotages ;
- la sécurité logique, la sûreté de fonctionnement, la fiabilité des systèmes embarqués, relative à la bonne marche, à la robustesse ou à la survie d'un système, suite à des dysfonctionnements internes ou externes ou des perturbations accidentelles ou intentionnelles de l'environnement. La sécurité, c'est-à-dire aussi la correction et la conformité des logiciels, des applications et des données rentrent dans ce contexte ;
- la sécurité des infrastructures, des systèmes de télécommunication, des réseaux et des systèmes répartis, utilisant une informatique prépondérante en réseau, relative à la perturbation par des attaques ou des propagations d'erreurs via le réseau ;
- la sécurité des SI de nature personnelle, technique[13], bureautique ou administrative[14], relative à la divulgation d'informations confidentielles ou à la corruption de base de données.

La sécurité moderne se concentre donc sur l'intimité numérique (*privacy*) des personnes, sur la protection du patrimoine et des idées (*Intellectual Property Rights*), sur la distribution des contenus en lignes tout en gérant les droits d'auteurs et de marques déposées (*Digital Rights Management*), sur la sécurité classique des réseaux et des SI et sur la protection des grandes infrastructures.

Il s'agit techniquement de cryptographie, de stéganographie, de biométrie, mais aussi d'ingénierie de sécurité dans les architectures et les protocoles de réseau. En outre, le facteur humain est essentiel en sécurité. La pédagogie vers une

[12] Les ordinateurs centraux, les accès aux salles informatiques ou les endroits de sauvegarde sont particulièrement sensibles.
[13] Applications scientifiques et techniques, gestion de production.
[14] Logistique, gestion des achats, des clients ou du personnel.

responsabilité proportionnée de tous les acteurs de la chaîne de confiance, la formation à l'administration vigilante des systèmes et des applications ainsi que la sensibilisation volontariste de tous les utilisateurs sont les critères primordiaux de la réussite d'une démarche de sécurité dans une structure. Enfin, la sociologie de la confiance, les aspects réglementaires, juridiques et éthiques ne doivent pas être sous-estimés.

Les concepts et la démarche de la sécurité

La démarche traditionnelle de la sécurité consiste à cloisonner les ressources (réseaux et serveurs) et les informations (programmes et données) en fonction de leur sensibilité et de leur domaine d'application, dans le respect de la réglementation.

Les objectifs de la sécurité

La sécurité numérique brigue trois objectifs : la confidentialité, l'intégrité et la disponibilité des ressources et des informations des réseaux et des systèmes :

- la confidentialité, vise à assurer que seuls les sujets (les personnes, les machines ou les logiciels) autorisés aient accès aux ressources et aux informations auxquelles ils ont droit. La confidentialité a pour objectif d'empêcher que des informations secrètes soient divulguées à des sujets non autorisés. L'objectif des attaques sur la confidentialité est d'extorquer des informations ;
- l'intégrité vise à assurer que les ressources et les informations ne soient pas corrompues, altérées ou détruites par des sujets non autorisés. L'objectif des attaques sur l'intégrité est de changer, d'ajouter ou de supprimer des informations ou des ressources ;
- la disponibilité vise à assurer que le système soit bien prêt à l'emploi, que les ressources et les informations soient en quelque sorte consommables, que les ressources ne soient pas saturées, que les informations, les services soient accessibles et que l'accès au système par des sujets non autorisés soit prohibé. L'objectif des attaques sur la disponibilité est de rendre le système inexploitable ou inutilisable.

La cryptologie permet de remplir largement les deux premiers objectifs en confidentialité et en intégrité. Malheureusement, il n'existe pas de modèles pour parvenir entièrement à la finalité de disponibilité[15].

La politique de sécurité

Pour atteindre ces objectifs de sécurité, il est nécessaire de mettre en œuvre une politique de sécurité, applicable à l'ensemble des entités à l'intérieur d'un domaine géographique ou fonctionnel. Cette politique désigne l'ensemble des lois et des consignes aux fins de protéger les ressources et les informations contre tout préjudice à leur confidentialité, leur intégrité et leur disponibilité, lequel serait dû à un usage inapproprié (incorrect, abusif ou frauduleux). La politique exhibe, dans sa rédaction sous forme de règles, des sujets et des objets et précise les activités et opérations autorisées et interdites. Pour ce qui concerne la sécurité logique, il est essentiel de connaître la part de la politique de sécurité, traitée informatiquement et dévolue intrinsèquement au réseau et au système. Le reste de la politique sera pris en charge par des mesures non techniques, organisationnelles ou juridiques.

Les fonctions de sécurité

La politique de sécurité utilise un catalogue de fonctions de sécurité, parmi lesquelles on peut trouver :

- l'identification des sujets, des objets et des opérations effectuées par ces sujets sur ces objets. Il s'agit de donner un nom à une personne, à une carte graphique, à un document, à un paquet IP. Un sujet qui n'a pas de nom est anonyme. Dans ce cas, le sujet ne peut être tenu responsable d'une action fautive. Un sujet peut avoir un pseudonyme (un alias) : il cache alors son vrai nom, mais reste responsable des actions qu'il pourrait exécuter sous son faux nom ;
- l'authentification, c'est-à-dire la preuve de l'identité de ces entités ou de ces opérations. Il s'agit d'un processus incorruptible pour garantir que le sujet est bien celui qu'il prétend être, pour garantir que l'objet est bien celui que l'entité responsable nomme ou bien que l'opération est bien celle qu'elle doit être ;
- l'intimité numérique est une fonction qui consiste à abriter l'identité d'une entité et ses activités, en masquant son observation et en rendant impraticable le croisement d'informations (statut d'un sujet, état d'un objet) sporadiques et disparates. Une manière de satisfaire cette intimité est de rester anonyme, mais un anonymat sévère peut à son tour devenir un danger pour autrui, se traduire par une irresponsabilité des actes et affaiblir la sécurité de l'ensemble du système ;

[15] Les attaques de dénis de services sont par ailleurs simples à mettre en œuvre sur les réseaux. C'est en dernier ressort la législation qui reste un garde-fou contre ces attaques techniquement faciles mais judiciairement périlleuses pour leurs auteurs.

- la traçabilité, c'est-à-dire une fonction qui consiste à repérer l'histoire des entités (ou des fractions d'entités) et leur cinématique dans un monde mobile. La traçabilité peut localiser par intermittence la position d'un sujet ou d'un objet, peut dater des transactions, peut noter des renseignements sur des situations, le tout avec des attributs de sécurité. Cette fonction s'avère irremplaçable pour contrôler un objet, pour pister un suspect ou pour reconstituer un scénario lors d'une enquête ou d'une perquisition informatique ;
- l'audit du système, c'est-à-dire l'observation, l'enregistrement, l'analyse et la compréhension des événements importants ou anormaux qui vont concourir à reconstituer le fil de son histoire, après la constatation d'une panne ou d'une attaque. Dans la pratique, on enregistre, dans les différents dispositifs de sécurité, des journaux infalsifiables qui seront des témoins de confiance chargés d'interpréter la trame des opérations et d'imputer la responsabilité d'une erreur ou d'un acte malveillant à son initiateur. Cette fonction d'audit, témoin de la mémoire du système, est déterminante dans un système. Le cybercriminel s'efforce de dissimuler les traces de son passage en tentant de détériorer ces fichiers d'audit. L'auditabilité est une fonction qui consiste à pouvoir récupérer des preuves numériques incontestables, en cas de perquisition des données ou d'examen ultérieur des activités ;
- l'imputabilité des actions d'un sujet sur des objets, en relation avec sa responsabilité. Par exemple, la non-répudiation est une fonction qui permet de garantir qu'une communication ou une transaction ne peut être niée, ni à l'émission, ni à la destination par ses responsables ;
- l'autorisation des actions par un sujet sur des objets. Les droits spécifiques et les privilèges des sujets sont définis par cette fonction ;
- le contrôle d'accès, c'est-à-dire la restriction d'accès aux ressources et aux informations, aux seuls sujets qui sont autorisés. Il s'agit, par exemple, de filtrer les flux entrant et sortant dans un périmètre selon des règles définies ;
- la protection des contenus, c'est-à-dire ici la confidentialité et l'intégrité des informations des utilisateurs. Il s'agit de cacher la signification des informations aux sujets non autorisés, en utilisant des primitives cryptographiques. La protection des contenus, dans le domaine du multimédia, signifie plutôt la disponibilité et le contrôle d'usage des informations. Il s'agit alors de contrôler et de restreindre l'usage des contenus aux seuls sujets autorisés par tatouage, sans nécessairement cacher ces informations pour des exécutions de logiciels, ou des lectures de documents audiovisuels ;
- la gestion de la sécurité, c'est-à-dire la gestion du cycle de vie de toutes les fonctions précédentes, essentiellement la configuration et la protection de ces fonctions de sécurité. L'objectif de la gestion[16] de la sécurité est d'établir et de maintenir un état de sécurité conforme à la politique en vigueur.

La mise en vigueur de la sécurité

Au commencement, il faut définir un état de sécurité pour les services[17] de sécurité et leur gestion[18]. Celui qui procure la sécurité doit être de confiance[19]. La sécurité exige une permanence des prescriptions : celles-ci ne doivent pas changer sans cesse et les états[20] de confiance doivent se maintenir beaucoup plus longtemps que leurs transitions. Dans les règles de cette politique, il est capital d'octroyer une priorité aux opérations de configuration de la sécurité.

Pour mettre en place la politique de sécurité, il faut déployer toute la panoplie des fonctions de sécurité qui permettront de résister aux menaces potentielles. Les personnes, les entreprises et les États implémentent de nos jours des solutions compétitives relatives à ces fonctions :

- l'identité d'une personne[21], d'une application, d'un document, d'un réseau, d'une entité informatique[22] ; depuis les événements du 11 septembre 2001, une compétition rude est en cours pour gagner les standards de l'identification physique, biométrique de chaque individu[23] ;

[16] La gestion de la sécurité est un ensemble d'opérations, en dehors des instances normales de l'utilisation du système mais indispensables, pour supporter et contrôler la sécurité du système.

[17] Essentiellement les services de confidentialité, d'intégrité, de disponibilité, d'authentification, de contrôle d'accès.

[18] La création des fonctions de sécurité et la modification des paramètres des fonctions de sécurité sont, à cet effet, cruciales.

[19] Clés pour l'authentification, le chiffrement d'un message.

[20] Il existe, du reste, un principe d'urgence : la politique de sécurité doit être installée promptement, les transitions lors des changements d'états doivent être rapides et contrôlées et les ordres de sécurité doivent avoir la priorité. Les considérations de temps sont importantes entre la gestion de la sécurité et les systèmes gérés, par exemple, pour mettre à jour des listes de contrôle d'accès.

[21] Par biométrie, par entité de confiance personnelle comme une carte à puce ou par nom de compte informatique.

[22] Un paquet IP, une connexion, une station relais téléphonique.

[23] Passeport électronique en Europe, initiative américaine pour les passeports et les visas.

- la preuve de l'identité (l'authentification) par l'authenticité d'un titre, d'une étiquette, d'un tatouage par signature numérique ;
- l'audit des faits, l'imputabilité, l'enregistrement de l'histoire du système à partir de capteurs et de sondes, la traçabilité des mouvements des divers sujets et des objets ;
- la preuve d'une communication (non-répudiation), d'un consentement avec des signatures numériques de toutes sortes ;
- la protection du transport, du traitement, du stockage et de l'archivage de documents ou de bases de données, et la sécurité de transactions et d'actes, le tout par chiffrement cryptographique ;
- la gestion des droits et des devoirs des propriétaires, des auteurs, des distributeurs, des abonnés : protection contre le piratage, la modification, le plagiat, la rediffusion ;
- la restriction d'accès, les autorisations en accord avec des politiques de sécurité, variables avec le temps, l'espace et le contexte ;
- l'intégrité d'un document, preuve de sa non-manipulation, par signature numérique ;
- la gestion de la sécurité : administration des outils et dispositifs de sécurité, évaluation globale du niveau d'assurance de sécurité. Afin de simplifier cette administration de la sécurité, les entreprises ont tendance à regrouper au sein d'un centre de gestion centralisée de la sécurité, les fonctions critiques (cellule de crise, système de secours). Cet organe vital devra à son tour être protégé.

Les menaces et les vulnérabilités

Les risques[24] potentiels sur le fonctionnement conforme des réseaux, des systèmes et des infrastructures sont de types variés qui vont de la panne ordinaire à la malveillance technique en passant par la maladresse humaine.

Les menaces

La construction effrénée du cyberespace ne s'élabore pas sans essais et erreurs, sans conséquences néfastes qu'il faut affronter et, pour le moins, restreindre. L'origine des menaces émane avant tout de l'idéologie ambiante « il est interdit d'interdire » de la Toile, qui suscite l'apparition d'effets nuisibles ou pervers, amplifiés par la résonance de la taille du réseau.

Les menaces sont incarnées pêle-mêle par l'irruption de sites qui hébergent des serveurs suspects, par l'encombrement des réseaux sous forme de contenus illicites ou de messages non sollicités, par la pollution des messageries, la propagation de virus, le téléchargement illégal de fichiers audio et vidéo, la circulation de fausses informations et par l'intrusion d'informations cachées ou de logiciels malveillants. Enfin le réseau favorise la création de nids pour des implantations de sectes, de mafias ou bien de refuges pour les réseaux de cybercriminels, voire bientôt de cyberterroristes.

L'impact de ces agressions peut être fatal en termes économiques[25], sociaux[26] ou juridiques[27].

Les entreprises du secteur de l'audiovisuel et du multimédia cumulent la plupart des problématiques de sécurité précitées, dans le contexte spécifique de ce métier et de ses usages : l'inéluctable dématérialisation des contenus impose non seulement de trouver des parades acceptables aux phénomènes de piratage, mais de garantir leur traçabilité et leur intégration sans couture dans les processus de production, ainsi que leur transparence pour les utilisateurs finaux légitimes.

Statistiques[28] sur la sécurité et sur le coût de l'insécurité

Il existe de nos jours 20 000 attaques réussies (sur un ou plusieurs sites) par mois dans le monde. Cependant la cartographie et le volume de la délinquance dans le cyberespace sont mal connus car la plupart des infractions commises ne sont pas portées à la connaissance des autorités. De plus, la métrologie des attaques est un domaine de recherche pour mesurer, en toute intelligibilité, avec une toise irrécusable la dangerosité d'un site, d'un système ou d'un réseau et pour jauger ou annoncer une « météorologie des attaques » sur un réseau.

On comptait environ 70 000 virus en 2004. L'augmentation est d'environ 1000 par mois, mais il n'existe environ que 10 000 virus actifs en permanence. Pendant le pic d'une infection, 10% des mails de l'Internet sont infectés. En 2005, le spam comprend quelque 20 milliards de messages par jour à l'échelle mondiale. Les fraudes sur les cartes bancaires et sur les téléphones sont finalement plus importantes, car elles se caractérisent par des pertes financières directes, alors que les virus et les spams n'engendrent en général qu'indirectement des coûts financiers qui se comptent toutefois par milliards d'euros par an, à l'échelle mondiale. On peut estimer le coût des dommages directs de la cybercriminalité dans les entreprises à 1 milliard d'euros par an, mais le coût global de l'insécurité[29] numérique culmine plutôt vers 50 milliards d'euros par an.

Le marché mondial de la sécurité des systèmes d'information est de l'ordre de 20 milliards d'euros, mais le marché mondial de la sécurité numérique dans le cadre de la convergence avoisine 80 milliards d'euros. Les dépenses en sécurité ne doivent pas être calculées sur des critères classiques de modèles financiers avec un retour sur investissement, car la sécurité ne contribue pas directement au chiffre d'affaire. La cyber-assurance a d'ailleurs du mal à trouver son bien-fondé. En règle générale, les dépenses de sécurité sont de l'ordre de 5 % à 10 % du budget correspondant aux technologies numériques.

La typologie des attaquants

Les pirates du numérique appartiennent à des catégories très hétéroclites. Ce sont :

- des cyberterroristes qui exploiteront bientôt le côté virtuel du réseau pour harceler et atteindre des cibles stratégiques, dans l'intention de déstabiliser les États et terroriser les populations ;

[24] Les CERT (*Computer Emergency Response Teams*) – www.cert.org – sont des organismes qui gèrent les vulnérabilités.
[25] Perte financière, vol d'information, destruction logique de systèmes, perte de la confiance des clients.
[26] Perturbation dans la disponibilité des systèmes, déstabilisation de l'organisation de la société.
[27] Mise en cause de la responsabilité de personnes physique ou morale.
[28] Tous les chiffres de ce paragraphe sont des estimations de l'auteur qui ne sont données qu'à titre indicatif de l'ordre de grandeur.
[29] Pour une entreprise, il faut considérer le coût de l'atteinte à l'image de marque. Par exemple, pour un opérateur, de nos jours, c'est catastrophique de ne plus fournir un service GSM. Si pour une mise à jour ratée de logiciels, le manque à gagner par les clients est de 10 millions d'euros, la perte par l'image de marque est sans doute de l'ordre du quintuple, sinon plus.

- des cybercriminels qui cultivent la dimension de communication du réseau pour gagner de l'argent (vol, extorsion) de manière frauduleuse et pour fertiliser leur propre réseau de diffusion : délinquance, mafia, casinos, blanchiment d'argent, narcotique, contrefaçon, proxénétisme, pédophilie, racisme, sectes en tout genre ;
- des *hackers*, des *cyberpunks* : sur un mode ludique, ces amateurs (souvent informaticiens adolescents) se lancent des défis, publient les découvertes de failles de sécurité sur les OS et les protocoles, jouent sur le réseau à déverrouiller des accès, transgressant la législation à leurs risques et périls ;
- des organisations privées ou gouvernementales qui commanditent des interventions[30] peu recommandables ou délictueuses : intelligence économique sur Internet, surveillance, écoutes, interceptions, infractions envers des concurrents ;
- des utilisateurs standard qui ont des pratiques illégales comme le téléchargement de fichiers musicaux ou l'utilisation illégale de logiciels.

Sur le plan juridique, la délinquance et la cybercriminalité englobent les infractions[31] liées aux technologies numériques et celles[32] dont la commission est facilitée ou liée à l'utilisation de ces technologies.

Les attaques traditionnelles

Toute stratégie d'intrusion est construite autour de l'exploitation des vulnérabilités de l'application concrète de la politique de sécurité d'un système par ses utilisateurs. La méthode pour organiser des attaques informatiques est donc d'exploiter systématiquement la mise en échec de la politique de sécurité en vigueur (expression prise ici au sens très large du terme), c'est-à-dire d'exploiter les failles dans l'état de confiance et dans la gestion de la sécurité.

En matière d'attaque, il existe deux phases capitales :

- l'accès au système ou au réseau de communication (par le renseignement, par des essais et erreurs) qui peut demander beaucoup de temps et de ressources, l'apparition des réseaux radio facilitant cette phase ;
- une fois la pénétration réalisée, il convient de naviguer discrètement (ou pas) dans le système pour toucher les zones[33] sensibles du système.

Les moyens mis en œuvre vont dépendre :

- de la connaissance a priori de la cible attaquée, allant d'une connaissance nulle exigeant des attaques aveugles jusqu'à une connaissance idéale soulageant les prospections, suite à une compromission de l'ingénieur responsable du système, en passant par une connaissance moyenne, suite à une phase de renseignement informatique ;
- de la volonté de la détectabilité de l'attaque : volonté d'être indécelable dans le cas de l'espionnage ou, au contraire, intention de médiatisation de l'agression comme faisant partie de sa réussite dans le cas d'attaques symboliques ;
- du degré de compromission que l'attaquant souhaite avoir avec cette cible : attaque directe par pénétration physique ou compromission avec le personnel de l'entreprise attaquée ou, au contraire, attaque indirecte via la mise à contribution de serveurs informatiques externes, compromis au préalable. Internet, devenu un refuge et un support d'attaques, a acquis cette mauvaise réputation de sécurité en éloignant les attaquants de leur cible, hors des frontières nationales.

Un système possède un cycle de vie : conception et développement avant la mise en service, installation, déploiement, exploitation et maintenance pendant son utilisation, puis obsolescence et destruction. L'attaque d'un système peut se préparer pendant la phase de conception et développement, lorsqu'on est fournisseur d'éléments du système, par l'insertion de chevaux de Troie dans l'architecture, de portes dérobées dans les applications. On peut aussi profiter des défaillances dans la chaîne de distribution des matériels et logiciels en interceptant et en corrompant ces produits. Dans la phase exploitation, c'est au cours des phases de maintenance (matérielle, logicielle, mise à niveau d'un logiciel en flux tendus) que les politiques de sécurité sont mises en péril. En phase de maintenance, des personnes étrangères au système sont amenées à fréquenter des

[30] On désigne parfois ces activités sous l'expression de guerre de l'information, la *soft war* par le *software* !

[31] Atteinte aux SI, diffusion de logiciels permettant de commettre ces atteintes, infraction aux lois sur la protection des données personnelles, infractions aux cartes de paiements, et infractions à la législation sur la cryptologie.

[32] Diffusion de contenus illicites, escroquerie par utilisation frauduleuse de numéro de carte bancaire lors de transactions numériques, escroquerie de commerce électronique, contrefaçons de logiciels ou d'œuvres audiovisuelles. Pour les infractions d'ordre sexuel, l'utilisation d'Internet est une circonstance aggravante.

[33] Le cœur du système, l'annuaire des abonnés, le centre de gestion des clés cryptographiques, un nœud du réseau important pour les flux.

zones sensibles du système[34]. C'est cette vulnérabilité qui peut être exploitée à fond pour avoir accès à un système ou pénétrer un réseau, en provoquant ultérieurement des pannes ou en obligeant le système à être exploité en mode dégradé.

Les attaques modernes

Les attaques ont évolué, ces dernières années, tant en volume qu'en nature. Autrefois, les attaques ciblaient toujours un gain tangible. Il faut de nos jours considérer l'éventail des motivations hétéroclites des attaquants : récupérer la connaissance d'une donnée, modifier ou détruire un fichier, ternir l'image de marque d'une entreprise, offenser la notoriété d'une personne, déstabiliser une institution ou un pays. Les attaques devraient encore s'intensifier dans l'avenir.

- les systèmes numériques peuvent être exploités pour perpétrer à distance des attentats à l'aide de télécommande informatique. Ces agressions vont se sophistiquer ;
- le cœur des réseaux est encore épargné[35] par les attaques. Avec la fragmentation du marché et le partage des infrastructures de communication, les modules racines des réseaux seront bientôt vulnérables à des assauts redoutables ;
- les communications cellulaires sont protégées par leur structure centralisée sous forme d'une gestion par un opérateur de télécoms et par la notion de circuit virtuel encore présente dans le GSM. L'évolution vers des télécoms « informatiques » (voix sur IP, GPRS, UMTS) devrait briser la confiance dans ce secteur : écoutes et dérivations téléphoniques, dénis de services, virus dans les téléphones. Comme Internet, le GSM est victime de son succès qui le rend vulnérable par l'ampleur de son déploiement et de son utilisation, par la multiplication des opérateurs de télécoms qui interviennent dans le trafic international, lesquels se doivent une confiance réciproque, et par l'addiction des usagers pour qui le téléphone mobile est devenu un compagnon inséparable de la vie quotidienne ;
- l'évolution vers la diffusion interactive et numérique d'émissions de télévision devrait aussi venir à bout de la confiance en une télévision passive, en direct du producteur (les grandes chaînes de télévision) au consommateur passif. Les émissions incontrôlées de télévision sont apparues avec la diffusion par satellite et pourraient se généraliser avec la convergence audiovisuelle. De plus, la vidéosurveillance risque de se banaliser pour enregistrer et contrôler l'activité urbaine. Elle peut, à son tour, devenir la proie d'attaques insidieuses.

Le cyberterrorisme à venir

La mondialisation a modifié les enjeux et de nouvelles formes d'offensives apparaissent. Avec les attentats du 11 septembre 2001, le monde a pris conscience qu'une nouvelle ère dans les formes d'agression pouvait survenir. Les causes profondes des conflits ne prendraient plus racine dans des enjeux territoriaux, ni même dans la convoitise économique, mais l'origine des conflits futurs serait plutôt dans la contestation des systèmes de valeurs. Les guerres « symboliques » utilisant les technologies numériques, conduites par des petits groupes motivés, dotés de peu de ressources, prendraient une dimension inédite[36].

Le cyberterrorisme n'existe pas encore dans ces premières années 2000. Il apparaîtra sans doute vers la fin de la décennie, quand la convergence numérique sera établie[37] et quand l'informatique répartie sera effective[38] sur les réseaux.

Les atteintes à la liberté individuelle : la filature électronique

Dans le monde numérique, il existe des menaces réelles contre la sphère privée de la personne, physique et morale, créées par les traces numériques laissées par chacun d'entre nous, suite à une navigation dans le monde virtuel. Des filatures électroniques sont fatalement réalisables, suite au repérage continu par GPS, suite à la localisation permanente enregistrée par un téléphone portable chez l'opérateur de télécoms, suite aux dépenses inscrites sur la carte bancaire dans les divers magasins, suite aux multiples photographies mémorisées par les caméras citadines. Les recoupements avec les sites Web visités, les numéros de téléphones joints, les citations détectées sur les moteurs de recherche, tout concourt à confectionner une glu

[34] Accès au mot de passe de l'ingénieur système, remplacement de modules en salle informatique, substitution de disque de photocopieurs en maintenance préventive.

[35] Bien qu'il y ait déjà eu des attaques des DNS racines sur Internet.

[36] Les moyens pour mettre en œuvre ces guerres de symboles pourront être numériques, car le cyberterrorisme est une menace dont le rapport coût/efficacité est très favorable. Il pourra infliger un préjudice aveugle de grande ampleur et propager un message avec vigueur. En outre, il est coûteux d'anticiper et de combattre de tels risques.

[37] La convergence, synonyme de compatibilité générale, aura pour conséquence la monochromie, l'uniformisation, l'interopérabilité, l'interfonctionnement des infrastructures informatiques, téléphoniques et audiovisuelles.

[38] L'incarnation de cette informatique répartie, amplifiée par le haut débit, fragilisée par le flux tendu, se présentera sous forme de grilles étendues avec des calculs illicites potentiels et de prolifération d'objets communicants qui occasionneront des risques dans la vie quotidienne lors de dysfonctionnements aléatoires ou provoqués.

numérique qui emprisonne chaque individu dans sa vie quotidienne. De nos jours, tout citoyen est enregistré sur environ cinq cents fichiers, tout individu circulant dans les grandes villes est filmé une dizaine, voire une centaine de fois par jour par des entités publiques ou privées et tous les utilisateurs[39] d'un téléphone portable sont pistés dans d'immenses fichiers. Ces enregistrements d'itinéraires électroniques ont des utilisations indirectes justifiées pour repérer efficacement des terroristes ou des criminels, mais pourraient être détournées pour connaître les activités intimes des personnes : dates et heures du téléphone portable allumé et éteint, position dans les cellules des réseaux, circulation à travers les cellules[40].

Les menaces d'inquisition numérique doivent être réduites par un encadrement strict de l'utilisation des fichiers nominaux ainsi que des registres de traçabilité des personnes ou des biens[41] (objets communicants, voitures) qui les accompagnent.

Les vulnérabilités des systèmes

Les vulnérabilités d'un système dépendent de nombreux facteurs. Les critères primordiaux sont la complexité du système, sa répartition, sa sensibilité et sa mobilité. La complexité dépend elle-même de multiples éléments :

- les ontologies (c'est-à-dire les entités informatiques en tant que telle) qui composent le système et leur structuration ;
- l'hétérogénéité du système. Le pluralisme des technologies présentes, la diversité des acteurs, des entités et des actions sur le système sont des facteurs de complication qui créent des erreurs de conformité, mais aussi des facteurs de cloisonnement qui jouent un rôle d'étanchéité dans la propagation des attaques ;
- la taille du système, c'est-à-dire le cardinal des diverses ontologies qui composent ce système ;
- les architectures, c'est-à-dire les composants et les liens entre ces composants, avec leurs articulations aux différentes échelles de temps, d'espace et de géométrie de ce système ;
- la virtualité des abstractions qui sont mises en jeu. La complexité des systèmes augmente avec le degré d'abstraction des paradigmes[42] qui sont utilisés pour concevoir le système.

D'une manière schématique, les attaques sur les réseaux filaires vont se situer plutôt dans les couches hautes du modèle OSI de référence, alors que les attaques sur les réseaux sans fil vont se situer plutôt dans les couches basses. En effet, les vulnérabilités[43] des réseaux filaires (Internet sur fibre optique ou sur cuivre, réseaux locaux sur fibre ou sur câble) sont plus dans les protocoles de couches hautes, les intergiciels, les applications et les contenus. Au contraire, les vulnérabilités des réseaux sans fil vont plutôt résider dans la couche physique et provoquer des attaques par des brouillages possibles de la transmission et dans la couche de liaison de données, par des tentatives intempestives à l'accès de la communication.

Les défaillances dans la conception et la fabrication des systèmes

La fragilité du monde numérique provient intrinsèquement de l'insuffisante maîtrise des infrastructures informatiques par les concepteurs (fabricants, distributeurs, équipementiers et systémiers) et par leur absence de transparence pour les usagers (utilisateurs des entreprises et utilisateurs personnels, managers et ingénieurs). Les raisons sont théoriques[44], pratiques[45], économiques[46] et sociologiques[47]. Une surenchère dans l'accélération des techniques ne favorise pas un déploiement mature des solutions.

L'ingénieur concepteur de système et de service est devenu un architecte qui ne maîtrise plus ses composants ; dès lors la sécurité des infrastructures est édifiée sur des sables mouvants. L'intégration des composants s'opère plus avec des

[39] 70 % de la population française et 1,4 milliards d'individus dans le monde, en 2005.

[40] On peut induire, à partir de ces enregistrements, des situations ou des comportements : un changement de cellules GSM à 300 km/h suggère que le propriétaire du téléphone portable est dans un TGV, les propriétaires d'un téléphone portable proche du lieu d'un attentat au moment du déroulement, sont ou bien des victimes éventuelles ou bien des terroristes potentiels. Ceux qui éteignent leur téléphone portable au début de la messe le dimanche et qui l'allument à la fin de la messe près d'une église sont probablement des catholiques pratiquants.

[41] Les bracelets électroniques apparaissent pour le suivi de personnes considérées comme dangereuses pour la société (prisonniers) ou pour elles-mêmes (enfants, personnes atteintes de la maladie d'Alzheimer). Les animaux domestiques auront bientôt un tatouage interne constitué d'une puce informatique incrustée sous la peau.

[42] Il est de plus en plus difficile d'identifier des ontologies virtuelles distribuées sur tout le réseau. Il est d'ailleurs remarquable d'observer cette similitude partagée à la fois par les attaques sophistiquées, les mécanismes de sécurité et l'informatique moderne. Ces trois éléments progressent en consacrant ce paradigme d'ontologie virtuelle répartie, comme si les attaquants, les défenseurs et les informaticiens prenaient le même sillage pour innover et employaient les mêmes armes.

[43] Dans la couche application avec des contenus ou services illicites, dans la couche réseau avec des attaques par déni de services.

[44] Sémantique des langages de programmation procéduraux.

[45] Absence d'environnement correct et efficace de développement logiciel, lacunes dans les méthodologies de conception et de développement de systèmes à logiciels prépondérants.

[46] Modèles économiques des logiciels vendus et distribués sous forme de versions révisées, suite aux réactions des usagers.

[47] Appropriation du numérique par une faible partie de la population.

obligations de délai et des objectifs de coût, que des enjeux de sécurité pour l'exploitant et l'utilisateur. Les préoccupations sont plus dans le respect de l'interopérabilité et l'interfonctionnement que dans la sécurité et la sûreté de fonctionnement[48].

L'informatique est une industrie où la latitude envers les écarts de conformité aux spécifications et aux services attendus a toujours été surprenante :

- tolérance aux bugs : les utilisateurs acceptent d'acheter des logiciels avec des erreurs sans protester. Ils admettent d'acheter plusieurs fois les nouvelles versions des programmes. La notion de « copyrights » vient d'ailleurs de cette incapacité à produire des logiciels sans erreurs. Pour éviter les poursuites judiciaires, on a décrété que le logiciel était une œuvre d'art[49] plutôt qu'une marchandise qui rendait un service spécifié ;
- tolérance aux spams (courriers électroniques non sollicités), aux virus : les Internautes consentent à équiper leurs ordinateurs de logiciels antivirus, lesquels vampirisent les ressources de calcul. Les logiciels d'antivirus sont en tête des ventes de logiciels. On peut s'en réjouir car ce palmarès montre la sensibilisation des utilisateurs. On peut aussi s'en désoler quand on considère le problème dans sa globalité. La gouvernance numérique de la communauté internationale devra tôt ou tard prendre en compte sérieusement cette question de l'économie de la sécurité numérique au niveau de la planète.

Le maillon faible : l'intervention humaine

Les réseaux et les SI sont sous la responsabilité d'entités physiques ou morales. Ils sont toujours actionnés par un individu. Cet individu est pleinement responsable de ses actes et de ses conséquences. Il constitue toujours le maillon faible dans les systèmes numériques.

Il va se tromper de manière involontaire, provoquer des effacements de fichiers, des dérèglements dans le fonctionnement normal d'un système.

Il peut agir de manière intentionnelle et tenter de pénétrer dans un réseau, dans un ordinateur, dans un SI, pour percer les secrets d'une institution, d'une organisation, pour modifier la configuration du parc de machines, de logiciels ou des données, pour utiliser les ressources illégalement, ou pour empêcher les personnes autorisées à les utiliser.

[48] D'ailleurs, la sûreté de fonctionnement des grands systèmes déployés dans les années 1990 a fortement baissé par rapport à celle des anciennes infrastructures : Internet et le GSM ont des sûretés de fonctionnement plus faibles que le téléphone fixe et les systèmes de distribution d'énergie conçus naguère.

[49] Désignation inconvenante quand on considère les sources de certains logiciels !

Les principes de la sécurité numérique

La sécurité numérique, c'est l'art de partager un secret. Ce secret est dissimulé dans un coffre-fort (mémoire d'un individu ou de carte à puce, tiers de confiance). Quand ces secrets sont numériques (clés transitant sur un réseau), ils sont chiffrés, ce qui nécessite encore un autre secret, et ainsi de suite. Si tout était numérique, il ne subsisterait que des secrets de polichinelle. Les entités de confiance sur un réseau sont là pour amorcer la pompe de la confiance, en se prolongeant par capillarité dans les méandres des réseaux et des systèmes, via des protocoles cryptographiques implantant ces secrets, spatialement et temporellement.

Les modèles opérationnels

Un système en état de sécurité est un système « tranquille » qui peut fonctionner et vaquer à son occupation réelle, sans se soucier de sa mise en danger dans son propre cycle de vie. Pour sécuriser un système :

- on peut le plonger dans un bain de totale confiance, auquel cas des dispositifs de protection sont superflus. C'est l'organisation qui prend alors en charge les effractions potentielles et les fautes des utilisateurs légitimes ;
- on peut le protéger, avec des dispositifs de défense, mais ce n'est pas le seul modèle de sécurité ;
- on peut, ne pas le protéger, mais dissuader[50] les assaillants potentiels ;
- on peut désinformer ou leurrer les adversaires. Pour éviter le piratage des œuvres sur Internet, le propriétaire des œuvres peut mettre en place un serveur de distribution pirate pour repérer les gens qui viennent s'abreuver à sa source. Pour ralentir les éventuelles écoutes indiscrètes sur un réseau, on engendre de faux messages correspondant à de nombreux leurres, ce qui a pour effet de camoufler dans la pluralité le vrai message. Les pots de miel, décrits ci-dessous, sont aussi des exemples de leurres.

Quand on sécurise un système, il faut apprécier la situation dans laquelle on se place : contexte hostile où les attaques sont régulières, contexte défavorable où il faut être vigilant, contexte neutre où il convient d'être prudent, contexte clément où la confiance est de mise, où il est inutile de se protéger des attaques et où il faut simplement se prémunir d'erreurs humaines toujours possibles.

Quand on sécurise[51] un système, il est rentable de se servir de son architecture[52] informatique. Mais il est aussi intéressant de s'appuyer sur sa composition[53]. Les solutions techniques de sécurité doivent se répartir de manière harmonieuse et efficace dans le contenu des données, dans le cœur des réseaux, dans les serveurs des opérateurs, des fournisseurs d'accès et de services, et dans les entités[54] informatiques des utilisateurs.

La dualité de l'intimité numérique et de la sécurité collective : la dignité numérique

En sécurité, il existe toujours deux angles de vue : le point de vue de l'utilisateur qui veut se protéger du réseau (c'est la perspective de l'intimité numérique avec une exigence de préservation de la liberté individuelle) et le point de vue du réseau ou de la société qui veut se prémunir de l'utilisateur malveillant ou imprudent (c'est la perspective de la sécurité ambiante avec une exigence de défense de la collectivité).

Pour protéger ses objets intangibles, un propriétaire va les dupliquer et stocker une copie dans un endroit sûr. Pour les transporter et protéger leur contenu sémantique et esthétique, il va brouiller, selon un code secret, le contenu de l'information et/ou son formatage.

Pour protéger l'intégrité de son infosphère :

- il va encapsuler le contenu dans une enveloppe intangible sécurisée ;

[50] Le tatouage électronique des documents est une technique qui rejoint cette stratégie.

[51] De manière schématique, on peut dire qu'il est plus aisé de sécuriser un huis clos qu'un campus ! Il est ainsi facile de sécuriser un territoire de faible volume, convexe, avec une frontière nette, peuplé de peu d'entités, celles-ci étant simples, confinées, statiques et dotées d'une identité. Il est plus difficile de protéger un vaste domaine, non connexe, composé de petites enclaves, éventuellement sans frontières précises, peuplé d'une multitude d'entités distinctes, lesquelles sont abstraites, anonymes, ou identifiées avec des noms versatiles, et se déplacent en entrant et en sortant du domaine.

[52] En effet, il est facile de s'introduire dans un système avec une architecture en bus (c'est-à-dire, une structure où toutes les entités peuvent communiquer et où les informations sont publiques). Mais il est plus difficile de pénétrer dans un système dont l'architecture se présente avec des liaisons ramifiées en point à point, à l'image des réseaux terroristes.

[53] L'hétérogénéité et la diversité des instanciations sont un rempart à la propagation des attaques et des erreurs : un monde uniforme avec des ordinateurs dotés d'un OS identique est très vulnérable.

[54] Ordinateur personnel, téléphone portable, agenda électronique.

- il va souder et coupler le message formaté avec une signature électronique, laquelle dépend secrètement du texte intégral formaté, signature que pourra vérifier un partenaire ;
- il va tagguer le message ou estampiller ses transactions avec horodatage pour en authentifier l'heure et la date ;
- il va incruster de façon secrète et répartir de manière continue dans tout le message, une marque invisible, indélébile et éventuellement indécelable pour marquer de sa griffe, qu'il est bien l'auteur ou le propriétaire de ce message.

Pour se protéger en tant que sujet, un être informatique (un programme informatique ou un dispositif) doit être discret, surveiller son territoire (les ressources qu'il utilise) ; il doit filtrer les accès aux frontières, guetter ses voisins, en les discernant ou au moins en les traçant.

Pour se protéger des objets des autres, le propriétaire va filtrer les objets (suivant leur nom, leur contenu, leur syntaxe) et inspecter les actions des sujets qui les commandent. Il va contrôler les mouvements à la frontière et dans son environnement pour repérer les événements anormaux.

On conçoit ainsi la compétition subtile et assidue qui se joue entre, d'une part les méthodes qui préservent l'intimité d'un sujet et les procédures légales pour observer ce sujet, et d'autre part les pratiques qui immunisent le reste du monde des exactions et bévues potentielles de ce sujet, et les recours indispensables du sujet afin d'accéder à la connaissance des moyens mis en œuvre pour le contrôler. L'instauration d'un climat de respect et de confiance n'entrave pas la mise en place de procédures croisées de défenses réciproques. Une dialectique transparente doit permettre de négocier les règles et de souscrire à des politiques de sécurité, claires et harmonieuses. La valeur démocratique de notre civilisation est au prix de cette dignité numérique[55].

La confiance en la sécurité offerte : la souveraineté numérique

Il est essentiel que l'utilisateur final, conservant son libre arbitre, ne puisse être l'otage de solutions obligatoires secrètes de sécurité dont il n'aurait ni l'information sur la présence, ni le contrôle sur la marche et l'arrêt. Il faut offrir à l'utilisateur une sécurité concrète, vérifiable ou vérifiée et certifiée par une entité garante, digne de confiance (comme l'État) de façon qu'il garde confiance dans l'arsenal des outils de sécurité proposés. Il faut donc insister sur la garantie, la certification ou la qualification effectuée par une entité de confiance disposant d'experts. Il ne faut pas confondre la véritable sécurité informatique et l'illusion de sécurité. Pour éviter cette méprise, il suffit de donner, à l'utilisateur final, la possibilité de connaître les défenses et les protections mises en place. Si la sécurité, dite dans l'obscurité, s'abrite sous l'égide d'une boîte noire, il est non seulement impossible d'analyser les faiblesses et les vulnérabilités résiduelles, et donc de faire confiance au dispositif, mais il est impossible d'intervenir en cas d'attaques. Les spécifications de sécurité mises en place ne peuvent être donc un secret absolu de fabrication. Le fournisseur de solutions de sécurité, à l'ambition parfois hégémonique, ne doit pas établir un rapport de force intolérable entre lui et l'utilisateur en sorte que ce dernier devienne esclave, lui abandonnant ainsi toute sa confiance. Au bas mot, un tiers de confiance, habilité par les deux protagonistes, devrait être capable d'apprécier les mesures techniques et de valider la réelle sécurité mise en vigueur. Mais les techniques, opérationnelles pour la sécurité des biens et des personnes dans les secteurs du transport ou de la santé ne sont pas du tout ébauchées ni transposées pour la sécurité logique dans le secteur de l'informatique.

Les méthodologies d'évaluation

Les critères communs (CC) sont une méthodologie pour l'évaluation des propriétés de sécurité des produits et systèmes numériques. Les CC permettent un étalonnage des résultats d'évaluations de sécurité menées indépendamment les unes des autres. Cette comparaison est rendue possible grâce à un ensemble d'exigences pour les fonctions de sécurité des produits et systèmes et pour les mesures d'assurance qui leur sont appliquées. Le processus d'évaluation établit un niveau de confiance, s'échelonnant de 1 à 7, par le fait que les fonctions de sécurité de tels produits et systèmes et les mesures d'assurance qui leur sont appliquées satisfont à ces exigences.

La norme ISO 17799 constitue un guide de bonnes pratiques pour la gestion de la sécurité, avec une centaine de recommandations d'ordre organisationnel et technique.

[55] On comprend le rôle primordial des fonctions d'identification et d'authentification d'une entité parée de ses attributs de sécurité (droits, devoirs, accès, autorisations, privilèges, traçabilité). Les fonctions de sécurité (protection des données) relatives aux échanges entre ces entités interviennent dans un second temps, les fonctions relatives à la gestion de l'état de sécurité opèrent en dernier lieu.

Les outils cryptographiques de sécurité

(Pour une approche plus complète et plus théorique, se reporter au Cours de cryptographie de G Zémor)

Les outils cryptographiques fondamentaux

La cryptographie demeure la technique indispensable pour, d'une part, protéger la confidentialité des informations transmises sur les réseaux ou stockées dans les serveurs de données et pour, d'autre part, assurer l'intégrité d'un document ou pour prouver l'authenticité d'une opération ou d'une transaction. Elle applique des concepts mathématiques et met en place des paradigmes informatiques afin de résister aux attaques potentielles d'assaillants ou de prouver, de manière quasi sûre, qu'une procédure est incorruptible.

La fonction première de la cryptographie est de proposer des algorithmes de chiffrement et de signature électronique. En principe, l'algorithme est normalisé et connu de tous. Le secret ne réside que dans la clé secrète. Ces algorithmes sont installés dans les entités de confiance personnelles (cartes à puces), ou dans des coffres-forts logiciels des serveurs informatiques.

Les deux familles d'algorithmes de chiffrement

Il existe deux familles d'algorithmes :

- La cryptographie symétrique, avec les algorithmes DES, 3DES, AES, n'emploie qu'une unique clé pour chiffrer et déchiffrer un message. Il est donc nécessaire de distribuer cette même clé aux deux protagonistes de la communication. Si une personne s'adresse séparément à plusieurs personnes distinctes, elle aura besoin d'autant de clés[56] distinctes. Cette famille d'algorithmes sert à chiffrer en temps réel ou en différé, des documents, des flots d'information, car ces algorithmes sont puissants et nécessitent assez peu de ressources. La taille des clés est faible, par exemple 128 bits.

- La cryptographie asymétrique emploie deux clés différentes : si l'on chiffre avec une clé, il faut déchiffrer avec l'autre. Il existe ainsi deux possibilités d'applications qui servent des objectifs distincts. Dans le cas du système RSA, le système asymétrique le plus utilisé, la taille des clés les plus courantes est 1024 bits. Notons que les clés sont beaucoup plus longues que dans le cas du chiffrement symétrique. Ceci est dû à la nature arithmétique du système RSA dont la sécurité repose sur la difficulté de factoriser des grands entiers. Or les progrès mathématiques et informatiques dans le domaine de la factorisation imposent maintenant cette taille de clé. Ces algorithmes sont beaucoup plus lents (dans un ordre de 10 à 100) que les algorithmes symétriques. On les réserve donc au chiffrement et déchiffrement des messages courts.

Un message court peut justement être une clé d'un algorithme symétrique. Cryptographie asymétrique et cryptographie symétrique sont donc exploitées de manière complémentaire et successive dans les protocoles cryptographiques pour authentifier l'émetteur, le récepteur, énoncer la non-répudiation des interlocuteurs, et déployer les systèmes de secrets qui vont permettre de communiquer de manière sécurisée.

Les fonctions de hachage

Une fonction de hachage permet de calculer un résumé (une empreinte, un condensé) de taille réduite et fixe (160 bits, par exemple) d'un document volumineux, écrit au niveau atomique à l'aide de 0 et de 1. Ces fonctions[57] ne sont absolument pas continues, si bien que si le document est un tant soit peu modifié, le résumé sera radicalement transformé. C'est en particulier cette propriété que l'on utilise pour valider l'intégrité d'un transfert de documents ou pour vérifier qu'un fichier n'a pas été corrompu sur un disque d'ordinateur.

L'application classique des outils cryptographiques

Le chiffrement des communications et des fichiers

Pour que deux personnes échangent des documents de manière sécurisée, il suffit que ces deux personnes partagent au préalable un secret (une clé de longueur 128 bits, par exemple) qui va permettre à l'émetteur de broyer le message intelligible en une farine numérique indistincte grâce à un algorithme de cryptographie symétrique. Cette même clé va servir ensuite au récepteur, à déchiffrer le message avec ce même algorithme réversible et cette même clé.

Pour stocker de l'information sur un support physique, la personne qui archive procède de la même façon. Elle chiffre l'information avec une clé et stocke cette information chiffrée. Pour la relire, elle utilise la même clé secrète afin de déchiffrer l'information.

[56] Pour un ensemble de n personnes souhaitant communiquer deux à deux, il faudra donc n(n-1)/2 clés.
[57] Les algorithmes les plus courants sont MD4, MD5 (empreinte de 128 bits). SHA1 fournit des condensés de 160 bits.

Si ces algorithmes sont performants, leur défaut majeur est la gestion lourde des clés dont le nombre croît avec le carré du nombre de partenaires dans le réseau, et ce d'autant plus qu'il convient de changer fréquemment les clés pour empêcher leur compromission.

La double utilisation de la cryptographie asymétrique

La cryptographie asymétrique résout le problème de la distribution initiale des clés secrètes qui doivent être partagées par les interlocuteurs d'une communication, dans le cas de la cryptographie symétrique. Elle attribue à chaque personne un couple d'éléments associés, une clé privée qui doit rester connue de son seul propriétaire, et une autre clé associée, publique qui, au contraire, doit être connue de tous. Munie de ce couple de clés qui sont reliées entre elles par une solidarité mathématique difficile à briser, chaque personne peut ainsi communiquer de manière sécurisée de deux façons. L'ensemble des partenaires connaissant la clé publique de cette personne ne peut pas découvrir la clé privée car il faudrait, pour percer ce secret, des ressources incommensurables de calcul.

Les messages peuvent être chiffrés avec une clé et déchiffrés avec l'autre qui est différente. On peut ainsi grâce à ce stratagème, communiquer de manière sécurisée, sans partager de secret initial. En chiffrant un message avec sa clé privée, l'émetteur assure aux récepteurs, sa propre authentification. En chiffrant un message avec la clé publique d'un destinataire, l'émetteur permet, à ce seul récepteur, d'être capable de déchiffrer ce message avec sa clé privée (celle du destinataire), et donc d'assurer la confidentialité du message.

Dans la pratique, un émetteur peut ainsi choisir une clé symétrique qui va servir de clé de session pour une communication avec un destinataire, la chiffrer avec sa clé privée asymétrique, rechiffrer le résultat avec la clé publique du récepteur. En envoyant ce message doublement codé, au récepteur, ce dernier pourra seul le déchiffrer avec sa clé privée, puis redéchiffrer avec la clé publique de l'émetteur et recevra ainsi la clé symétrique pour communiquer avec ce destinataire. Des travaux récents portent sur des algorithmes associant une seule clé de chiffrement à plusieurs clés de déchiffrement distinctes, notamment dans le cas de la télévision cryptée. La clé de chiffrement du diffuseur de la télévision peut être une fonction mathématique de l'ensemble des clés de déchiffrement conservées dans les décodeurs des abonnés de la télévision cryptée. Ainsi, pour désactiver un récepteur, il suffit d'éliminer son secret de la fonction calculant la clé de chiffrement de l'abonné sans pour autant affecter les autres récepteurs[58]. Pour admettre un nouvel élément dans le groupe, il suffit d'ajouter sa clé de chiffrement dans la fonction précitée.

La signature numérique

Une signature numérique est une empreinte (d'un document) chiffrée par la clé privée de l'auteur, cette empreinte chiffrée étant jointe au document originel. La signature[59] permet ainsi de vérifier l'intégrité du document et l'identité de l'expéditeur. On signe un document via des fonctions de hachage.

Les infrastructures de confiance

La difficulté de la cryptographie asymétrique provient de l'authenticité non établie de la clé publique d'un interlocuteur. N'importe qui peut, à présent, engendrer un couple de clés privée-publique en récupérant un algorithme sur Internet. Aussi, lorsqu'une personne publie son nom et sa clé publique associée, un pirate peut se glisser sous cet affichage et usurper la clé, en proposant sa propre clé publique. De cette façon, le pirate pourra décoder avec sa propre clé privée les messages à destination de l'interlocuteur véridique, quitte à restituer les messages chiffrés à l'interlocuteur de départ avec la clé publique originelle. C'est ce qu'on appelle une attaque par l'homme au milieu.

Les autorités de confiance

Pour éviter cette méprise, la solution consiste à s'en remettre à un tiers, en faisant signer la clé publique par une autorité digne de confiance, qui va ainsi garantir que la clé publique appartient bien au bon interlocuteur. On va donc signer numériquement le couple composé du nom du propriétaire de la clé publique et de la clé publique. La clé privée de l'autorité va donc signer ce couple de manière que la clé publique de cette autorité puisse permettre de vérifier cette signature.

Les certificats numériques

Un certificat numérique est un message signé par la clé privée d'une autorité de confiance. Cette autorité de confiance est un tiers qui est reconnu digne de confiance par les deux parties d'une transaction. Un certificat X.509 version 3 est un standard qui contient notamment les renseignements suivants :

[58] Plusieurs travaux ont développé des schémas de ce genre. Citons Yi M., Varadharajan V., *Robust and Secure Broadcasting*.

[59] La signature numérique a une propriété de non-répudiation, car seule la personne digne de confiance doit être capable d'exécuter cette signature valide. Le processus de signature doit être accompli par le signataire et la vérification doit pouvoir être exécutée par n'importe qui, d'où cette utilisation de la propriété de dissymétrie propre à la cryptographie asymétrique.

- l'identité du porteur du certificat ;
- l'identité de l'autorité de certification ;
- les coordonnées de l'émetteur du certificat ;
- la clé publique, objet du certificat ;
- les paramètres de sécurité utilisés ;
- la période de validité du certificat ;
- la signature numérique de l'autorité émettrice pour valider le certificat.

Avant tout échange, il convient donc de se procurer un certificat auprès d'une autorité de certification. Le partenaire doit fournir son identité.

- on y adjoint sa clé publique ;
- l'autorité ajoute ses propres informations dont sa propre clé publique ;
- l'autorité calcule l'empreinte du tout et chiffre avec sa clé privée ;
- l'autorité signe un certificat pour le partenaire à l'aide de cette empreinte.

Le récepteur peut récupérer ce certificat, recalculer l'empreinte correspondante pour vérifier l'intégrité du certificat, déchiffrer la signature du certificat avec la clé publique de l'autorité et vérifier que les deux empreintes sont identiques. On peut donc faire la preuve de son identité, produire sa clé publique avec le certificat associé qui est une assurance de sécurité entre un nom de personne et sa clé publique associée. Quiconque peut ainsi vérifier la validité de la relation entre la clé publique et le nom associé.

Les infrastructures de gestion de clés (IGC)

Le mécanisme de gestion de ces certificats est mis en place dans les infrastructures de gestion de clés qui sont des infrastructures de confiance sur les réseaux pour vérifier l'identité des partenaires dans une communication ou une transaction.

Les IGC (*Public Key Infrastructure*, PKI) sont des infrastructures matérielles et logicielles dont le déploiement et les procédures sont en définitive assez lourdes.

Une IGC comprend donc :

- une autorité d'enregistrement : cette autorité recueille en différé les demandes de certificats et prépare les certificats à valider ;
- une autorité de certification : cette autorité signe les certificats à l'aide de sa clé privée ;
- une autorité de dépôt et de séquestre : cette autorité permet de conserver et éventuellement de régénérer un certificat délivré à un utilisateur pour déchiffrer des messages quand le certificat n'est plus valable ou s'il a été perdu.

Les protocoles cryptographiques

PGP, S/MIME

PGP, acronyme de *Pretty Good Privacy*, été créé en 1991 par un militant, Philip Zimmermann, objecteur de la vision cryptologique autocratique des organisations gouvernementales américaines. PGP a été conçu pour offrir aux citoyens une solution de sécurité, librement téléchargeable sur le Web, pour se protéger de l'État en particulier. Au départ, il s'agissait de protéger un fichier informatique. PGP est à présent utilisé pour protéger la messagerie personnelle ou l'échange d'information entre deux partenaires. Il garantit l'origine des messages et leur confidentialité.

S/MIME (*Secure/Multipurpose Internet Mail Extension*) est une extension de sécurité du protocole de messagerie MIME, définie dans les RFC 3850 et RFC 3851 de l'IETF. C'est un format de message qui inclut les paramètres de sécurité comme, par exemple, la signature du message, le certificat du signataire et le corps du message éventuellement chiffré.

Il faut souligner que les formats PGP et S/MIME sont distincts et qu'il n'existe pas d'interopérabilité entre les deux protocoles.

SSL

Le protocole SSL[60] (*Secure Socket Layer*) est un protocole cryptographique, défini en 1994 par Netscape, appliqué à la communication sécurisée point à point entre deux entités d'un réseau. C'est un protocole de sécurisation des échanges électroniques, qui est intégré dans tous les butineurs (les navigateurs) des terminaux connectables à Internet. C'est le protocole de sécurité, le plus déployé, pour sécuriser le canal de transmission d'informations entre deux ordinateurs. Son application la plus répandue est la connexion sécurisée sur un serveur pour éviter les abus et les fraudes, pendant une transaction de commerce électronique.

SSL, au niveau 5 de la couche session du modèle de référence, sécurise toutes les applications qui fonctionnent nativement sur le protocole TCP[61]. Il utilise les fonctionnalités du protocole TCP/IP pour permettre aux applications d'accéder à un mode sécurisé pour la transmission sécurisée de documents ou l'exécution de transactions sécurisées. SSL n'implique aucune modification au niveau des applications pourvu qu'il soit incorporé dans le navigateur, ce qui a concouru à faciliter son déploiement.

SSL permet donc d'assurer la confidentialité et l'intégrité des données échangées comme un numéro de carte bancaire au cours de la communication. Toutes les données sont chiffrées afin d'empêcher leur lecture par des tiers, si bien que rien ne transite en clair. Le chiffrement de ces données mobilise d'importantes ressources de processeurs, ce qui ralentit les échanges et réduit les performances globales des systèmes.

SSL permet d'assurer l'authentification[62] du serveur et, optionnellement, l'ordinateur du client. En d'autres termes, le client peut être sûr de s'adresser au bon serveur sur Internet lors d'une transaction sécurisée pour acheter sur Internet ou pour déclarer ses impôts. SSL nécessite pour cette authentification l'entremise d'un certificat X509 valide afin de garantir l'identité du serveur (en fait l'organisme qui exploite ce serveur) et le cas échéant l'ordinateur du client[63] (en fait l'identité de l'utilisateur) pendant la session.

SSL offre enfin le service de sécurité de non-rejeu.

SSL, qui fonctionne sous un mode client/serveur, est en fait composé de quatre protocoles : *Handshake, Record, Alert* et *Change Cipher Spec*. Il fonctionne en deux étapes : la première phase est assurée par le protocole *Handshake,* durant laquelle les deux protagonistes négocient les algorithmes de chiffrement, la création et le partage des secrets, ainsi que l'authentification des parties. Dans la deuxième phase, le protocole *Change Cipher Spec* active les paramètres négociés entre les parties, le protocole *Record* assure les services de sécurité du protocole SSL, décrits plus haut. Enfin, le protocole *Alert* gère les erreurs et les dysfonctionnements.

IPSec

IPSec (*Internet Protocol Security*) est une collection de protocoles cryptographiques de sécurisation des réseaux IP. C'est un protocole de niveau 3 du modèle de référence. IPSec est indépendant des applications et du transport fiable TCP ou du transport UDP. Il peut se déployer sur les réseaux, indépendamment des utilisateurs, car il est transparent aux applications.

Il est défini dans le RFC 2401 de l'IETF. Son élaboration fut laborieuse de 1992 à 1998 dans le cadre de la nouvelle version v6 du protocole IP, qui tarde toujours à être déployée à grande échelle. IPSec est désormais un module indépendant qui fonctionne sur IPv6, mais aussi sur la version la plus courante IPv4. Il est disponible sur tous les OS des stations de travail et des serveurs.

IPSec peut être installé en natif dans la pile protocolaire de l'OS de l'ordinateur, du serveur, du routeur ou de la passerelle. Mais il est plus simple de l'insérer comme un module autonome entre la couche 3 et la couche 2, au-dessus de la couche de liaison des entités du réseau.

IPSec peut être aussi déporté dans un boîtier dédié, indépendant des machines, module géré par le responsable réseau, de manière analogue à la gestion d'un routeur ou d'un pare-feu.

IPSec est composé de deux protocoles, AH (*Authentication Header*) défini dans le RFC 2406 et ESP (*Encapsulating Security Payload*) défini dans le RFC 2402. ESP offre les services d'authentification, d'intégrité et de confidentialité des

[60] TLS est le standard IETF qui doit remplacer SSL.

[61] Un port de TCP est dédié à chacune des applications. Le port 80 est réservé à HTTP pour l'affichage des pages Web, le port 25 à SMTP pour la messagerie, le port 21 à FTP pour le transfert de fichiers, le port 23 à Telnet pour émuler un accès par terminal à une machine distante.

[62] Deux versions de SSL sont supportées par les applications. La version 3 de SSL, la plus usuelle, exige l'authentification pour le serveur. L'authentification est basée sur les certificats X.509v3.

[63] En général, le client n'a pas de certificat, ce qui signifie que le serveur ne peut pas s'assurer de l'identité de ce client. Ce dernier pourra donc potentiellement répudier une commande réalisée sur son ordinateur via SSL.

données utiles associées au paquet IP. AH, moins utilisé qu'ESP, offre les services d'authentification et d'intégrité de la totalité du paquet IP.

IPSec fonctionne sous deux modes. Dans le mode tunnel, le paquet IP initial est totalement encapsulé dans un nouveau paquet IP. C'est avec ce mode que le service VPN est mis en œuvre. Dans le mode transport, on conserve le paquet initial. Dans les deux modes, les champs spécifiques des protocoles AH et ESP sont ajoutés à la suite des rubriques classiques du format IP et les données du paquet sont signées ou chiffrées selon la politique en vigueur.

Comme pour SSL, une phase initiale est nécessaire pour la négociation des algorithmes de chiffrement, la génération des clés et de l'authentification des parties. Cette phase est assurée par le protocole IKE (*Internet Key Exchange*) défini dans le RFC 2409.

PPTP

PPTP (*Point-to-Point Tunneling Protocol*) est une extension du protocole PPP (*Point-to-Point Protocol*), soumise à l'IETF en 1996. PPTP est un protocole de tunnel de la couche 2, qui permet aux données passant d'une extrémité à l'autre du tunnel d'être sécurisées par des algorithmes de cryptographie. PPTP encapsule des trames PPP dans des datagrammes IP pour une transmission sur un réseau IP, tel qu'Internet. C'est un protocole utilisé dans la mise en place des VPN.

Les réseaux virtuels privés (VPN)

Les entreprises et les organisations possèdent en général plusieurs sites[64] géographiques qui travaillent conjointement en permanence. Dans chaque site géographique, les utilisateurs sont connectés ensemble grâce à un réseau local. Ces réseaux locaux sont souvent connectés via Internet. En outre, certains utilisateurs peuvent vouloir se connecter aux réseaux de l'entreprise en étant à l'extérieur chez un client ou en déplacement.

Il existait autrefois des liaisons physiques spécialisées, qui sont maintenant abandonnées au profit de liaisons logiques.

Un réseau virtuel privé (*Virtual Private Network*, VPN) consiste en la fabrication d'un tunnel logique qui sera contracté par les communications de l'entreprise, lesquelles seront véhiculées dans cette tranchée numérique construite sur un réseau fréquenté par d'autres usagers. Dans la pratique, il s'agit d'un artifice, car les données vont utiliser un chemin ordinaire, emprunté par tout le monde, mais ces données chiffrées et tagguées seront sécurisées, à l'image du transport de containers plombés sur une route. Le caractère privé du réseau est donc complètement virtuel puisqu'il ne s'agit pas de liaison physique spécialisée. Le caractère privé est créé par un protocole cryptographique (IPSec ou PPTP). Un VPN est donc une communication sécurisée entre deux points d'un réseau public, d'où l'expression de tunnel.

[64] Siège social, site de production, agences.

La sécurité des réseaux

En sécurité, on distingue deux styles d'architecture de réseaux : les réseaux gérés par une autorité, comme les réseaux d'entreprise ou les réseaux d'opérateurs de télécoms et les réseaux comme Internet qui ne sont pas administrés pour les fonctions de sécurité de manière centralisée par une tutelle.

Pour les réseaux gérés par une autorité, l'architecture est centralisée et les utilisateurs du réseau sont comme des abonnés appartenant à un club fermé. Chaque membre de ce club possède un secret (une carte à puce, un jeton, un mot de passe) et doit d'abord s'identifier, puis s'authentifier auprès de l'autorité de sécurité. Il peut alors, selon son profil dans l'institution ou selon les privilèges de son contrat d'abonné, solliciter les services du réseau auxquels il a droit.

Pour les réseaux non protégés par un office administrateur, les utilisateurs doivent se débrouiller seuls en installant des outils de sécurité sur leur propre machine ou se procurer des solutions de sécurité en faisant appel à des fournisseurs qui sont en intermédiation sur le réseau. Dans ces réseaux, la sécurité globale ne règne donc pas et l'anarchie prévaut puisqu'il existe toujours une machine non protégée qu'une personne imprudente ou malveillante va utiliser à l'origine d'une attaque.

La sécurité des réseaux cellulaires

La sécurité des réseaux cellulaires nécessite de prendre en compte d'une part, les spécificités du fragment radio du circuit emprunté par les communications et d'autre part, la mobilité de l'utilisateur qui est repéré dans ses déplacements par une segmentation radio de l'espace géographique en cellules disjointes. Une cellule est un domaine radio au centre duquel se situe une station relais qui raccorde le téléphone portable à une infrastructure filaire.

La sécurité des réseaux cellulaires doit donc protéger notamment le canal de l'interface air des transmissions pour inhiber des interceptions et restreindre les brouillages. On doit donc spécifier le protocole d'identification et d'authentification du téléphone mobile de l'abonné. On doit aussi définir la protection du canal radio, en général, par le chiffrement des trames qui transitent entre le terminal et la station de base. Les brouillages sont plutôt traités par des algorithmes de traitement de signal de diversité, des sauts de fréquence ou un étalement du spectre.

La disponibilité du réseau est critique pour les réseaux cellulaires comme pour tout type de réseaux sans fil, à cause de la rareté des ressources radio. Les réseaux cellulaires sont donc vulnérables à différentes attaques de type déni de service.

De plus, il faut aussi protéger le terminal miniature nomade devenu la proie des pickpockets et le profil de l'utilisateur stocké dans la carte à puce susceptible d'être déplombée puis triturée par des fraudeurs.

Du point de vue de l'abonné, la sécurité du GSM est une sécurité centralisée, fondée sur un secret partagé entre l'opérateur de télécoms et l'utilisateur. Ce secret est stocké dans une carte à puce SIM (*Subscriber Identification Module*) encastrée dans le téléphone portable. Il s'agit en fait d'une clé connue de l'opérateur et exploitée par les protocoles, et d'un identifiant unique IMSI (*International Mobile Subscriber Identity*) permettant notamment l'itinérance, c'est-à-dire d'être reconnu des autres opérateurs de télécoms et de pouvoir ainsi téléphoner à partir d'un autre pays ou d'un autre réseau d'opérateur que le sien. Cet identifiant est remplacé par un numéro temporaire, renégocié régulièrement, pour assurer un certain anonymat. Le protocole vérifie également le numéro du téléphone, un code unique composé de quinze chiffres, identifiant le terminal, le code IMEI (*International Mobile Equipment Identity*) pour limiter les vols.

Du point de vue de l'infrastructure mondiale, la sécurité du GSM repose sur la confiance mutuelle entre tous les opérateurs de télécoms. Ceux-ci sont garants du trafic international, administré sous la tutelle de cette sécurité fédérée.

La sécurité des réseaux GSM se manifeste donc par les éléments suivants :

- l'authentification de l'utilisateur repose sur le principe défi-réponse, en utilisant l'algorithme d'authentification A3 ;
- la confidentialité des données de l'utilisateur est assurée sur le segment radio par un chiffrement symétrique ; l'algorithme A8 est utilisé pour la génération de clés de chiffrement, l'algorithme A5[65] pour le chiffrement des données. Cet algorithme A5, relativement faible, fut cassé plusieurs fois par des cryptanalystes et dut supporter des améliorations ;

[65] L'algorithme A5 existe en différentes versions avec des niveaux de chiffrement variés : A5/0, sans chiffrement, A5/1, niveau élevé, utilisé en Europe, A5/2, niveau faible, utilisé aux Etats-Unis.

- la confidentialité de l'identité de l'utilisateur est assurée par la génération d'une identité temporaire pour l'utilisateur appelée TMSI (*Temporary Mobile Subscriber Identity*).

Les vulnérabilités du GSM proviennent surtout de la dissymétrie de traitement entre le terminal et la station relais. Des attaques de type homme au milieu sont possibles en se plaçant en coupure entre une station relais et un téléphone portable, dans le but d'intercepter les numéros ou les champs des protocoles et de capter finalement les communications.

Les réseaux GSM sont vulnérables à plusieurs attaques de type déni de service. Divers scénarios[66] existent, analogues aux attaques par inondation sur Internet.

La sécurité du GPRS ou de l'UMTS est similaire à celle du GSM dans son esprit et son architecture. L'UMTS protège les nouveaux services et apporte des améliorations significatives pour prendre en compte le retour sur expérience du GSM. En particulier, on a rééquilibré la symétrie de sécurité entre le téléphone et la station relais qui s'authentifient mutuellement.

La sécurité des accès sur Internet

La structure Internet est telle que les menaces ne sont jamais interceptées par le réseau, pour le moment. On peut les bloquer à une extrémité du réseau, mais le réseau lui-même est incapable de reconnaître ce qui devrait ou non circuler librement. Les fournisseurs d'accès relient les utilisateurs à Internet et ont par conséquent une situation clef pour contrôler les menaces entrantes et sortantes envers les ordinateurs de leurs clients. Ils pourraient éliminer un certain nombre de ces menaces avant même leur apparition sur les ordinateurs personnels et commencent à proposer des dispositifs de sécurité tels que des filtrages dans la messagerie, mais cette démarche n'est pas facile, surtout si on demande une obligation de résultats.

Pour concevoir une sécurité des accès sur Internet, il faut mettre en œuvre des mécanismes très généraux pour intégrer tous les nouveaux services. La première préoccupation est la gestion sécurisée des accès à ces services. Aussi, les mécanismes ont été regroupés par l'IETF, autour de trois fonctions principales, sous le sigle AAA, l'authentification, l'autorisation et l'imputation (*accounting*). L'objectif originel d'AAA était d'offrir aux abonnés en déplacement la possibilité de se connecter à Internet depuis un modem téléphonique.

Le protocole AAA[67] utilise une architecture client-serveur classique. Il identifie et authentifie l'utilisateur par l'intermédiaire d'un secret partagé par l'utilisateur et le serveur d'authentification, détermine les droits de cet utilisateur et impute l'utilisation des ressources à des fins de facturation. Les serveurs AAA sont sur des serveurs d'accès au réseau, gérés par des opérateurs offrant des services de télécommunication.

RADIUS (*Remote Access Dial-In User Service*) est un standard de l'IETF (RFC 2138-2139) pour les utilisateurs qui se connectent à Internet par modem. C'est le protocole AAA le plus répandu chez les fournisseurs d'accès à Internet, mais il comporte des limitations. DIAMETER (RFC 3588) améliore les fonctionnalités de RADIUS, pour notamment la gestion des inter-domaines et le passage à l'échelle. TACACS+ (*Terminal Access Controller Access Control System*) est une solution propriétaire reprise par Cisco, qui utilise TCP et gère séparément les trois fonctions AAA.

La sécurité des réseaux sans fil

L'utilisation accrue de réseaux radio pour accéder à d'autres réseaux adjacents et aux réseaux d'entreprise aggrave les préoccupations d'ensemble de sécurité.

Les réseaux de faible portée comme Bluetooth se banalisent pour des connexions en point à point, par exemple, entre le clavier ou la souris et son ordinateur, ou bien entre le téléphone portable et un assistant numérique. Les vulnérabilités sont des interceptions (capture du mot de passe) ou des intrusions (diffusion de virus). Le protocole de sécurité de Bluetooth met en œuvre des mécanismes particuliers mais performants qui ne sont hélas pas souvent activés.

Les réseaux WiFi se déploient à la périphérie des réseaux filaires, dans les sites privés comme les entreprises, les institutions ou à la maison pour partager une connexion Internet et dans les sites publics ouverts (aéroport, campus) avec des portées radio de l'ordre de la centaine de mètres. Les vulnérabilités sont nombreuses : connexions pirates, usurpations, écoutes intempestives… La mauvaise conception initiale de la sécurité des réseaux sans fil IEEE 802.11 paralysa son déploiement. La première génération de réseau sans fil IEEE 802.11, normalisée en 1997, comporte un protocole de sécurité, WEP (*Wired Equivalent Privacy*), qui délivre les services d'authentification par une méthode de défi, de confidentialité en chiffrant les trames et d'intégrité en signant les trames par le chiffrement de leur empreinte. Le protocole WEP comporte d'importantes faiblesses : l'authentification n'est pas fiable car elle peut être corrompue par rejeu, la signature n'est pas efficace, enfin la saisie d'environ un million de trames chiffrées permet de déduire la valeur du secret partagé. Face à ces

[66] Par exemple, un terminal envoie plusieurs requêtes d'allocation sans compléter les échanges nécessaires. La limitation des canaux de signalisation va causer la congestion locale du réseau et les requêtes légitimes seront rejetées par manque de canaux disponibles.

[67] Le concept AAA apparu au début des années 1990 s'inspire du protocole d'authentification Kerberos, développé en 1978 au MIT.

insuffisances, diverses méthodes, en particulier le protocole TKIP (*Temporal Key Integrity Protocol*), sont venues se greffer pour résoudre ces lacunes. La norme IEEE 802.1X, dédiée initialement au contrôle d'accès des réseaux utilisant des commutateurs de paquets, réalise l'authentification des utilisateurs et le filtrage des trames qu'ils échangent. Toutefois, la norme ne définit pas expressément le procédé de distribution des clés entre le point d'accès et le client. En outre, l'application de l'architecture IEEE 802.1X aux réseaux sans fil 802.11 peut introduire des problèmes de sécurité comme les attaques de l'homme au milieu ou l'usurpation de session, notamment quand il n'y a pas d'authentification mutuelle.

Consciente des failles de sécurité, l'IEEE a proposé en juillet 2004, comme extension du protocole de base, la norme IEEE 802.11i qui introduit des protocoles de sécurité renforcés au niveau de la couche MAC de liaison de données ; elle décrit également le protocole d'échange de clés entre le point d'accès et le terminal sans fil. Elle supporte le protocole WEP, ainsi que les protocoles TKIP et CCMP (*Counter Mode/CBC-MAC*) qui améliorent les mécanismes de chiffrement des standards précédents.

Le WPA (*WiFi Protected Access*) est une norme destinée à accélérer la diffusion des réseaux sans fil. C'est un sous-ensemble de la norme IEEE 802.11i, basé sur le protocole TKIP. WPA définit des éléments d'informations spécifiques et des machines d'états de gestion de clés partiellement compatibles avec 802.11i. Le déploiement de cette norme implique donc la disponibilité de points d'accès, de cartes réseaux et de logiciels clients spécifiques.

Le WPA2 est conforme au standard IEEE 802.11i et inclut le chiffrement AES (*Advanced Encryption Standard*) plus robuste. Le WPA2 est compatible avec les produits supportant le WPA, mais la compatibilité avec les produits utilisant le protocole WEP n'est pas assurée.

Les dispositifs de sécurité

Les pare-feu

Un pare-feu (*firewall*) est un dispositif matériel et/ou logiciel qui implémente la fonction de sécurité de contrôle d'accès. Un pare-feu est donc un dispositif pour filtrer les accès, les paquets IP, les flux entrant et sortant d'un système[68]. Un pare-feu est installé en coupure sur un réseau lorsqu'il sert de passerelle filtrante pour un domaine à la frontière d'un périmètre fermé. Dans le cas d'un pare-feu personnel, sur une machine cliente, il est installé en son cœur pour y contrôler et filtrer les accès au réseau.

Un pare-feu met en vigueur une politique de sécurité qui laisse passer, ou arrête les trames ou les paquets d'information selon cette politique. Il peut donc autoriser ou empêcher des communications selon leur origine, leur destination ou leur contenu. Dans la pratique, un pare-feu lit et analyse chacun des paquets qui arrivent. Après analyse, il décide du passage ou de l'arrêt selon l'adresse IP de l'émetteur, du récepteur, selon le type de transport (TCP ou UDP) et le numéro de port, en relation avec le type d'application réseau.

Quand la politique de sécurité ne concerne que les couches basses, la seule analyse du paquet permet d'autoriser, de rejeter ou d'ignorer le paquet.

Quand la politique décrit des règles de sécurité qui mettent en jeu le transport fiable (TCP), les sessions ou les applications, le pare-feu doit connaître l'état momentané de la connexion et doit garder en mémoire de nombreux paquets pendant un certain temps de façon qu'il puisse décider de l'autorisation ou du rejet des paquets.

Les pare-feu ont des limitations : ils doivent être très puissants en termes de ressources pour ne pas ralentir le trafic dans un sens ou dans un autre, puisqu'ils sont en coupure sur le réseau. Ils ne doivent pas être court-circuités par d'autres passerelles ou des modems connectés directement à l'extérieur. Ils sont des « bastions », c'est-à-dire des cibles pour les attaquants qui peuvent les assaillir pour saturer leur ressource.

Un pare-feu doit posséder un système de journalisation (.log) sophistiqué de manière à analyser a posteriori tous les faits importants qui jalonnent la vie de cette passerelle filtrante : tentatives d'intrusion, événements anormaux, attaques par saturation, par balayage.

Un pare-feu est en général architecturé de telle manière que l'on puisse distinguer physiquement les communications avec l'extérieur, celles avec le réseau à protéger et enfin celles qui sont déviées vers une zone tampon de parking, souvent appelée zone démilitarisée (*demilitarized zone*, DMZ). C'est dans cette zone qu'on place le site Web, ouvert sur Internet, à l'abri d'un pare-feu, mais nettement séparé du réseau interne à protéger.

Les systèmes de détection et de prévention d'intrusion

Un système de détection d'intrusion (*Intrusion Detection System*, IDS) est un dispositif[69] matériel et/ou logiciel de surveillance qui permet de détecter en temps réel et de façon continue des tentatives d'intrusion dans un réseau, dans un SI ou dans un ordinateur seul, de présenter des alertes à l'administrateur, voire pour certains IDS plus sophistiqué, de neutraliser ces pénétrations éventuelles et de prendre en compte ces intrusions afin de sécuriser davantage le système agressé.

Un IDS réagit en cas d'anomalies, à condition que le système puisse bien identifier les intrus externes ou internes qui ont un comportement anormal, en déclenchant un avertissement, une alerte, en analysant éventuellement cette intrusion pour empêcher qu'elle ne se reproduise, ou en paralysant même l'intrusion.

Un IDS est donc un capteur informatique qui écoute de manière furtive le trafic sur un système, vérifie, filtre et repère les activités anormales ou suspectes, ce qui permet ultérieurement de décider d'actions de prévention. Sur un réseau, l'IDS est souvent réparti dans tous les emplacements stratégiques du réseau.

Les techniques sont différentes selon que l'IDS inspecte un réseau ou que l'IDS contrôle l'activité d'une machine (hôte, serveur) :

- sur un réseau, il existe en général plusieurs sondes qui analysent de concert, les attaques en amont d'un pare-feu ou d'un serveur ;

[68] Un réseau local d'entreprise connecté à Internet ou un ordinateur connecté à ADSL sur Internet.
[69] Dans ce paragraphe, on a réuni sous le même vocable IDS, les IDS et les IPS (*Intrusion Prevention System*).

- sur un système hôte, les IDS sont incarnés par des démons ou des applications standards furtives qui analysent des fichiers de journalisation et examinent certains paquets issus du réseau.

La détection d'intrusion est un problème[70] difficile que des chercheurs ont appréhendé, il y a maintenant plus de trente ans. Le problème était assez simple à exprimer lorsque ces systèmes étaient des systèmes fermés, à l'intérieur d'un périmètre défini, avec des utilisateurs connus. Le problème s'est compliqué notablement depuis que les systèmes sont sans fil et ouverts (le périmètre est presque impossible à cerner), que les utilisateurs sont nomades (avec des entrants, des sortants et parfois des anonymes), que les services[71] sont mobiles et que ces systèmes s'étendent par interconnexion sur de grands espaces géographiques (infrastructure de télécommunications). Pour vaincre les tentatives d'intrusion, il faut définir un schéma d'identification, d'authentification et d'autorisation destiné à des utilisateurs légitimes et aux matériels et logiciels qui se situent à l'intérieur du système. On soulage fortement l'IDS en filtrant au préalable le trafic forcément régulier et légitime. On définit alors une sonde intelligente qui observe, enregistre et analyse le comportement des sujets, des objets et des événements. À partir d'un modèle de normalité et conformément à certains seuils, on décrète que le comportement du système et des personnes est normal ou suspect. On en déduit des actions à mettre en œuvre, immédiatement ou non.

Ces dispositifs ont des défauts majeurs (fausse alerte et carence de détection), bien décrits dans la littérature.

Les pots de miel

Les pots de miel (*honey pots*) sont des dispositifs de leurre, à la frontière des SI, destinés à piéger les attaques des pirates. Les attaques par balayage, en particulier, ont tendance à tomber dans le panneau de ces attrape-nigauds.

Un pot de miel est un mécanisme qui permet d'augmenter la sécurité d'un réseau ou d'un système, pourvu qu'on soit capable d'analyser les profils des attaques tombées dans l'embuscade. Un pot de miel peut venir en complément d'un pare-feu. Mais les mises en œuvre concrètes sont plutôt rares.

Les pots de miel sont répertoriés selon deux catégories, à faible ou à forte interaction. L'interaction représente l'intensité de l'activité que peut avoir un attaquant avec le pot de miel.

Les pots de miel à faible interaction consistent à émuler des OS et des services. L'émulation présente l'avantage de circonscrire les possibilités de l'attaquant incapable de prendre le contrôle du véritable OS pour endommager d'autres systèmes. L'activité est réduite au degré d'émulation offerte. Ainsi, ces pots de miel offrent peu de prérogatives à l'intrus qui aura un champ d'action limité, car ils ne font que proposer des services factices et ne renvoient jamais de réponse. L'avantage des pots de miel à faible interaction est leur simplicité. Ils sont faciles à implémenter, à gérer et présentent peu de danger avec des attaquants très cantonnés. En pratique, on installe un logiciel, on sélectionne les OS et les services qu'on veut émuler et on surveille l'activité en laissant le pot de miel fonctionner. Les inconvénients sont que ces pots de miel examinent une information limitée et ne peuvent épier que des activités connues. Enfin ces pots de miel à faible interaction sont aisément détectables par un attaquant.

Les pots de miel à forte interaction n'émulent rien mais engagent des OS véritables et des applications réelles. L'avantage de cette solution est qu'il est possible de recueillir des informations nombreuses. Comme les attaquants ont accès à de vrais systèmes, on peut observer l'intégralité de leur comportement et on peut analyser ainsi les méthodes et les outils qu'ils utilisent. Ce type de pots de miel ne fait pas de suppositions sur le comportement probable de l'attaquant et capture tout ce qu'il peut. Ces pots de miels permettent donc de révéler des modes d'attaques encore insoupçonnées. Néanmoins, leur utilisation comprend des risques élevés puisque la machine, désignée comme pot de miel, est destinée à être compromise. Il existe donc un risque que l'attaquant puisse utiliser les vrais services du pot de miel comme rebond pour affronter d'autres systèmes voisins. Enfin, ces pots de miel sont plus compliqués à mettre en place et à gérer.

[70] La formalisation des systèmes de détection d'intrusion est classique. Dans un système, on spécifie des sujets, des objets et des opérations licites et on essaie d'appréhender des situations et des ontologies avec leur comportement normal ou anomalique.

[71] Services reconfigurables dynamiquement, caches, applications téléchargeables, intergiciels de distribution.

Les solutions d'identification et d'authentification

La biométrie : une présence numérique liant l'homme au système

La biométrie est une technique ancienne qui connaît un engouement récent dans son application électronique. Elle a pour but d'identifier les personnes physiques par des caractéristiques physiologiques[72] ou comportementales[73]. La mesure d'une grandeur de l'apparence du vivant et le calcul du représentant biométrique pour assurer l'identification doivent être discriminants, fidèles, automatiques et rapides. La biométrie identifie[74] donc un individu par ce qu'il est et qui est unique et caractéristique de la personne. On peut ensuite l'authentifier par le respect d'un procédé sûr de validation biométrique ou bien par la vérification de ce qu'il sait, comme un mot de passe dont il se souvient.

Pour déployer un système biométrique, il est nécessaire de recueillir tout d'abord un échantillon de référence et d'extraire ensuite une représentation[75] numérique réduite, opérations qui doivent être réalisées par une institution de confiance. Les échantillons sont alors stockés globalement dans une base de données sous la responsabilité d'une organisation de confiance ou localement, dans une carte à puce par exemple, sous la responsabilité du propriétaire. Lorsque cette infrastructure biométrique est déployée, une personne physique peut alors être identifiée, après capture en temps réel d'un nouvel échantillon, calcul de la représentation numérique caractéristique de la personne, et comparaison avec le gabarit.

Les inconvénients des méthodes biométriques sont connus : l'enregistrement et le déploiement sont lourds, le coût d'exploitation est élevé, l'interopérabilité des infrastructures biométriques est faible, la durée de vie des informations de référence est limitée, mais surtout le contrôle, c'est-à-dire la comparaison entre un étalon et un échantillon prélevé en temps réel est statistique, sans garantie totale de succès. Les procédés possèdent donc des performances qui varient avec la source biométrique. Pour chaque mode d'identification, il faut estimer statistiquement le taux de mauvais rejets (on a refusé des personnes légitimes) et le taux d'acceptations incorrectes (on a admis des personnes illégitimes). La conjonction de plusieurs modes[76] biométriques est indispensable pour atténuer le risque d'erreur. Ensuite, plutôt que d'attaquer en amont la chaîne de traitement de biométrie, les attaquants préfèrent mettre en défaut l'algorithme final de comparaison des deux échantillons et faire en sorte que sa réponse[77] soit constamment positive, ce qui annihile alors tout le dispositif de biométrie. Par ailleurs, l'introduction de la biométrie soulève des questions délicates de protection de la vie privée et des difficultés culturelles et sociologiques qui ne manqueront pas de tempérer l'enthousiasme envers cette technique.

La carte à puce : un écrin de confiance pour amorcer la sécurité

Une carte à puce (*smart card*) est une enceinte hermétique portable de sécurité, une entité de confiance attachée à un individu par l'intermédiaire d'un code secret. C'est un authentique micro-ordinateur doté d'un coffre fort qui renferme des secrets, assisté par un processeur spécifique étanche capable d'exécuter des primitives cryptographiques.

La carte à puce offre principalement une authentification robuste, mais fournit également des fonctions d'identification comme une carte d'identité électronique. Elle est en outre un moteur miniature de sécurité, une machine de chiffrement de messages courts et de calcul de signatures.

La carte à puce déployée en Europe, a connu son essor depuis trente ans grâce à la carte bancaire, aux télécartes de téléphonie, puis grâce à la carte SIM du GSM. La carte à puce peut stocker des certificats X.509[78] pour l'identification et des caractéristiques biométriques. Elle connaît une puissance croissante de calcul, améliorant ainsi les performances[79] de résistance aux attaques par essais et erreurs, et une ouverture plus grande grâce à l'émergence d'applications en langage Java, au sein même de la carte. Le crypto-processeur permet de calculer en toute confidentialité les opérations de sécurité : la clé privée reste secrète à l'intérieur de la carte à puce.

[72] Empreinte digitale, morphométrie de la main ou du visage, iris, rétine, voix. L'ADN n'intervient pas ici car le code génétique ne peut pas être révélé en temps réel.

[73] Manière de saisir au clavier ou de signer manuellement.

[74] La biométrie n'authentifie pas le sujet, comme on le croit souvent, car la caractéristique biométrique d'un sujet n'est pas secrète. La confusion provient du fait que la biométrie est utilisée de deux façons : d'une part, on cherche une donnée parmi *n* dans une base de données – et on parle d'identification, d'autre part, on met en correspondance une donnée avec une donnée de référence – et par abus de langage, on parle d'authentification.

[75] Les minuties des empreintes digitales n'occupent que 300 octets.

[76] Par exemple, l'empreinte digitale et la morphométrie du visage.

[77] Un seul bit, 0 ou 1, est à falsifier.

[78] La taille d'un certificat est de l'ordre de 1 à 2 kilo-octets et les cartes à puces actuelles ont une capacité mémoire d'environ 128 kilo-octets, voire plus.

[79] Un calcul RSA s'effectue en une demi-seconde avec une clé de longueur 1024.

Avec la commercialisation massive des cartes à puces et leur rôle dans les transactions de paiement, les pirates redoublent d'imagination pour élaborer de nouvelles attaques[80] physiques ou par canaux cachés sur le matériel afin de contourner la sécurité toujours plus ferme de ces micro-ordinateurs de confiance.

La carte à puce demeure un dispositif de sécurité très fiable grâce aux contre-mesures des fabricants. Elle évite la multiplication des mots de passe souvent peu protégés par les utilisateurs négligents. Elle obéit à des normes de sécurité (FIPS I40) et se généralise dans les applications des réseaux et des SI pour la sécurité de bout en bout entre deux protagonistes, le client, l'abonné ou l'utilisateur d'une part et le vendeur, l'opérateur ou le serveur informatique, d'autre part.

[80] Attaques en observant finement la consommation électrique ou bien le temps d'exécution des opérations, attaques par champs électromagnétiques, attaques par injection de fautes en perturbant le fonctionnement.

La sécurité des systèmes confinés

La sécurité des systèmes embarqués

Les systèmes embarqués ou les logiciels enfouis (*embedded systems or software*), sont des entités autonomes qui remplissent une mission indépendante, parfois critique, sans intervention humaine, en général en interaction directe avec l'environnement extérieur que celui-ci soit physique ou informatique. Ces systèmes[81] autonomes miniaturisés peuvent être isolés mais ils sont la plupart du temps reliés et communiquent à travers un réseau. Ces systèmes sont soumis à des contraintes fonctionnelles qui mettent en jeu leur définition, leur robustesse, leur conception, leur capacité à accomplir une tâche avec des ressources déterminées souvent liées aux astreintes temporelles ou à la consommation énergétique.

Le comportement de ces systèmes doit être blindé, voire garanti avec un haut niveau de sécurité et de sûreté[82], pendant tout leur cycle de vie. Ces systèmes doivent être protégés, mais ils doivent avant tout fonctionner correctement tant dans leurs fonctions purement intestines que dans leurs interactions avec le monde extérieur, d'autant plus que ces systèmes embarqués sont plongés de nos jours dans une « intelligence ambiante », de sorte que les interlocuteurs et les voisins du système peuvent être eux-mêmes des ordinateurs.

Avec la diffusion massive des capteurs et des actuateurs électroniques, les systèmes complexes bénéficient d'une instrumentation importante. Les échanges d'information avec l'extérieur et la faculté d'adaptation de ces systèmes à l'environnement nécessitent des contrôles sévères sur la bonne marche de ces systèmes avec des modules flexibles, autochargeables, autoconfigurables. Les systèmes embarqués ou les logiciels enfouis doivent donc posséder des propriétés de sécurité et de sûreté de fonctionnement, localement, puisque ces systèmes autonomes doivent résister seuls à des sollicitations imprévisibles de leur entourage. Ils doivent donc être pourvus algorithmiquement d'une sorte de conscience de sécurité et d'une espèce d'instinct de survie, le tout étant conçu et calculé à partir des données et des traitements in situ, disponibles. Sur la base des informations fournies par l'instrumentation en place et des connaissances disponibles par des modèles mathématiques, physiques et de sécurité, il s'agit d'implanter localement une carapace de sécurité et de sûreté, voire de résilience pour d'abord percevoir (observer, détecter, localiser, diagnostiquer), analyser (selon la politique en vigueur) la situation *hic et nunc* en fonction des événements imprévus, des occurrences aléatoires, des dangers et réagir (corriger, se cicatriser, tolérer, se maintenir, s'adapter, se dégrader, survivre en autarcie, voire s'anéantir) en fonction des évolutions et des déviations par rapport à un état ou un comportement de référence normal, souhaitable ou nominal.

La sécurité et la sûreté des systèmes et logiciels embarqués se construisent donc en plusieurs phases :

- pendant la spécification du système : maîtrise de sa complexité, de son architecture et claire séparation entre le module autonome et son infrastructure en considérant l'énergie consommée et les flux de communication : application traditionnelle des méthodologies pour la spécification de sécurité et de sûreté[83];
- pendant la conception du système : utilisation de techniques de modélisation, d'abstraction et de techniques du comportement dynamique des systèmes, temps réel strict ou adaptatif, méthodes mathématiques et ingénierie système ;
- pendant l'implantation : épargne rigoureuse des ressources spatiotemporelles, parcimonie dans les communications avec les périphériques, économie temporelle intransigeante dans les réseaux, calcul d'horloge, ordonnancement des messages, compilation optimisée des algorithmes en travaillant à l'aide d'ateliers de développements informatiques spécifiques ;
- pendant la validation : vérification formelle, simulation et test, évaluation de l'assurance de sécurité et de sûreté.

La conception du système doit prendre en compte les aspects mathématiques, informatiques, électroniques et architecturaux, les aspects de normalisation et de standardisations (interopérabilité) et les impératifs[84] économiques. La difficulté porte en général sur l'assemblage hétérogène de composants et de modules.

[81] Ce sont des terminaux communicants (téléphones portables, cartes à puce), des capteurs intelligents (robots, instruments de contrôle dans l'avionique ou les ouvrages de génie civil), des actuateurs critiques (composants dans les centrales nucléaire ou les missiles balistiques) ou des appareils électroniques dans le domaine de la santé (stimulateur cardiaque, instrument de chirurgie), de l'automobile (modules de contrôle-commande du moteur ou du conducteur) ou du grand public (électroménager, appareils de photos, jouets).

[82] Freins d'automobile, capteurs dans les engins spatiaux, équipements dans une chaîne de fabrication, organes de répartiteur téléphonique.

[83] Définition notamment de l'autonomie, de la réactivité, de la criticité et définition de la politique de prévention des risques, de tolérance, de défense et de gestion des crises, des conflits.

[84] Complexité, consommation d'énergie, longévité, mise à jour.

La correction de la spécification[85] ainsi que la conformité de l'implantation réelle par rapport à la spécification[86] sont des étapes importantes qui ne doivent pas être confondues. Dans sa spécification, il faut scrupuleusement définir les menaces et l'intelligence locale de sécurité et de sûreté du système. Il faut le rendre tolérant aux fautes, aux incertitudes de l'environnement et des situations. Il faut l'immuniser contre des agressions potentielles. La sécurité d'un système, c'est-à-dire d'une part la non-agressivité du monde extérieur face aux vulnérabilités résiduelles du système embarqué et d'autre part son caractère inoffensif vis-à-vis de l'entourage reste en définitive une question complexe à cause de l'incomplétude de sa caractérisation.

La sécurité des terminaux

Alors que SSL résout la sécurité des communications de point à point sur un réseau et que la carte à puce est le lien sécurisé entre l'utilisateur final et le SI, il convient aussi de préserver le terminal lui-même d'une utilisation dangereuse ou frauduleuse, soit que son utilisateur laisse ouvertes des brèches ou bien outrepasse ses droits (utilisation irrégulière de licence logicielle), soit que les éditeurs de logiciels abusent de leur position dominante, en interdisant l'installation de logiciels concurrents.

Pour sécuriser un terminal, il est nécessaire de cacher un bouquet de secrets dans ce terminal. Ces éléments secrets peuvent être partagés et exploités par le fournisseur de matériel, les éditeurs de logiciels, les applications et l'utilisateur. Définir une politique de sécurité fédérative pour l'exploitation du poste de travail, est une question qui relève de la quadrature du cercle, puisque le terminal devient un espace où maintes politiques aux intérêts paradoxaux s'affrontent. Pour son implémentation, l'articulation sécurisée entre le matériel et le logiciel demeure toujours un point dur à résoudre. Les secrets peuvent être insérés en dur dans le cœur du matériel ou bien être enfouis en périphérie dans une carte modulaire de chiffrement.

L'architecture de sécurité d'un poste de travail se décompose en trois parties :

- une ressource matérielle avec un processeur sécurisé qui offre des fonctions cryptographiques, qui exécute les tâches sensibles et une mémoire qui stocke les éléments secrets et les informations sensibles ;
- un noyau minimum digne de confiance, qui assure les fonctions de base de l'OS ;
- une interface logicielle sécurisée avec les applications.

La sécurité des applications prend alors racine dans cette infrastructure native de base. Les applications peuvent puiser dans cette plate-forme, les ressources de sécurité dont elles ont besoin. Les outils de sécurité d'un poste de travail permettent :

- de vérifier l'intégrité du poste : à l'amorce, la ressource matérielle vérifie l'identification et la configuration des composants matériels et la certification des composants logiciels ;
- de développer la sécurité des applications grâce à une bibliothèque sécurisée de primitives de sécurité : chiffrement, signature, authentification, gestion de confiance des clés.

TPM (*Trusted Platform Module*) est le résultat des recommandations précisées par TCPA. C'est un composant informatique installé sur la carte mère ou intégré au processeur. TPM est capable de chiffrer les données et les stocker dans des espaces sécurisés.

Indépendamment de ces tentatives de normalisation, il existe sur le marché maintes solutions propriétaires, sous forme de cartes modulaires, utilisées dans les grandes entreprises et gérées par le responsable de sécurité.

[85] C'est-à-dire le système est bien défini.
[86] C'est-à-dire le système réalisé correspond bien à sa définition.

La sécurité des systèmes et des logiciels

La sécurité des systèmes d'exploitation : la faille essentielle

Les systèmes d'exploitation (*Operating System*, OS) sont le talon d'Achille des SI. Les attaquants externes d'un système doivent toujours, à un moment donné, emprunter leur chemin et utiliser leurs services.

Les OS (UNIX, Linux, Windows) et les moniteurs en temps réel (Symbian, Linux embarqué) proposent un ensemble de fonctions mises à la disposition des processus d'applications. Ils possèdent des interfaces qui contiennent habituellement des appels pour ouvrir, fermer, lire, écrire des fichiers et des appels pour communiquer (transferts de messages, appels de procédures). Mais ces OS ne sont, en général, pas sécurisés[87]. Sous UNIX, la politique de sécurité est discrétionnaire, c'est-à-dire que les propriétaires des fichiers décident eux-mêmes des attributs de sécurité de leurs fichiers. Avec la structure actuelle des SI, l'OS est un élément prépondérant. S'il est acheté sur étagère avec la machine, c'est un progiciel hermétique avec toutes les répercussions fâcheuses que cette méconnaissance implique. La gravité des conséquences d'une intrusion dans un SI par la prise de contrôle de l'OS est très élevée. La faiblesse des SI provient souvent de la non-maîtrise de l'élément primordial de ces systèmes : l'OS des serveurs ou des stations terminales. La faiblesse des réseaux découle aussi de l'opacité des OS des routeurs ou des passerelles. Le risque encouru est similaire à la remise d'une clé secrète à un utilisateur non autorisé.

La sécurité minimum d'un OS comprend deux types de fonctions de sécurité : les fonctions intrinsèques[88] et les services supplémentaires offerts aux applications[89]. Avec cet arsenal de fonctions, on peut ainsi sécuriser les principales fonctionnalités vulnérables d'un OS[90].

La sécurité des logiciels : les réponses providentielles, propriétaires ou publiques

La sécurité des applications ou des logiciels est un thème difficile car un logiciel seul n'a pas de propriété réflexive pour déclarer la confiance qu'on peut lui accorder ou décréter la confiance qu'il peut avoir envers telle autre entité. Il est donc nécessaire d'ancrer la sécurité des applications à l'infrastructure générale de sécurité. En pratique, on arrime l'application à un crochet sécurisé qui est relié aux parties sécurisées du terminal ou aux protocoles d'authentification et d'autorisation du réseau ou du système. La sécurité des logiciels se scinde de nos jours en deux volets contradictoires :

- d'une part, les éditeurs désirent enrayer le vol de logiciels et l'usage abusif de licences, distribuer leurs contenus intangibles en les valorisant (DRM) et conserver la confidentialité du texte (IPR) de leur logiciel. S'ils ne sont pas eux-mêmes dignes de confiance, ils peuvent à leur tour abuser les utilisateurs en adjoignant des sondes secrètes pour espionner à leur insu les utilisateurs, ce qui constitue une sécurité dans l'obscurité ;
- d'autre part, la communauté des utilisateurs redoute les positions économiques dominantes des éditeurs qui fort de leur avantage veulent en profiter de manière déloyale. Cette tendance de pensée informatique de type altermondialiste préconise de dépouiller l'informatique de son caractère opaque et libéral, en distribuant[91] des logiciels nus, c'est-à-dire transparents, lisibles par quiconque souhaite inspecter les textes de l'application informatique.

Face à la montée de la menace du piratage de logiciels et de l'hégémonie des logiciels propriétaires, certaines réponses sont inappropriées :

- des éditeurs de logiciels et les industriels de l'électronique se regroupent avec des initiatives propriétaires et conservatrices qui sont plus d'ordre géostratégique, avec des intérêts plus égoïstes que sécuritaires ;

Et d'autres ne sont pas encore arrivées à maturité :

[87] Quand ils le sont, cette sécurité n'est pas toujours évaluée, ni même pas évaluable à un niveau convenable. Par exemple, le niveau EAL4 des CC ne semble pas toujours suffisant pour un serveur de sécurité sous UNIX, compte tenu des menaces. La sécurisation de ce noyau monolithique et imposant, à un niveau d'assurance EAL5 des CC est une entreprise téméraire voire insurmontable.

[88] Blanchiment des zones de mémoire, authentification des objets pour le cloisonnement, l'invocation et le contrôle d'accès, journalisation des événements liés à la sécurité.

[89] Gestion des clés, génération et gestion des aléas, chiffrement des données dès que les objets communiquent à travers un réseau.

[90] L'accès au réseau par protocole TCP/IP, le stockage structuré sur disque par l'intermédiaire d'un système de gestion de fichiers, et la connexion à des périphériques.

[91] La distribution n'est ni forcément gratuite, ni forcément libre. La traduction de l'expression *free software* en logiciel libre ne facilite pas la compréhension.

- la montée en puissance des standards ouverts et des logiciels libres, notamment sur les serveurs, prouve l'existence d'un modèle économique original. Néanmoins et malgré le soutien d'acteurs majeurs, les logiciels libres ne constituent pas aujourd'hui une alternative complète, mature et sûre aux éditeurs de logiciels habituels. Les logiciels libres sont encore des produits d'informaticiens pour des clients informaticiens, et ne sont pas manipulables et configurables par des utilisateurs non spécialistes. Par ailleurs, ces logiciels ne sont exempts ni de bugs, ni de portes dérobées, ni de virus. Si la communauté du logiciel libre arbore un côté Robin des bois sympathique, elle masque, voire ignore elle-même, son versant négatif d'auberge espagnole, en ayant laissé les pirates l'infiltrer largement.

Afin de protéger les applications sur les postes de travail connectés à des réseaux, deux approches très différentes sont apparues dans la dernière décennie :

- en 1995, la sécurité par le langage Java et sa machine virtuelle sécurisée a connu un succès éclatant et a même contribué à la réussite d'Internet. C'est une sécurité partielle qui a permis la diffusion des logiciels Java sur le Web ;
- en 1999, la sécurité par le matériel et son prolongement logiciel, sous le sigle de TCPA[92] est réapparue. C'est une approche classique dans l'informatique de défense, qui suscite depuis son introduction une polémique qui concerne les arrière pensées protectionnistes supposées des concepteurs, pour juguler la progression du logiciel libre et entraver la concurrence apportées par les cartes à puce.

La sécurité des logiciels Java fut conçue au départ pour protéger le poste de travail récepteur des logiciels téléchargés à partir d'Internet. La machine virtuelle Java fait office de réceptacle de sécurité. Le modèle de sécurité de Java est un modèle appelé *sandbox* en anglais, c'est-à-dire bac à sable, à l'image du terrain de jeu pour les enfants où ils peuvent s'amuser sans crainte. Les applications Java s'exécutent alors sûrement dans cette machine virtuelle puisqu'à l'intérieur de cette zone tous les appels à des fonctions abrogatives du système sont proscrits.

TCPA[93] (*Trusted Computing Platform Alliance*), Alliance pour une informatique de confiance, fut un projet lancé par Intel en 1999, très controversé dans le monde de la sécurité. TCPA a évolué, suite à ce tollé, s'est étendu, a modifié certaines ambitions mais la motivation géostratégique monopolistique est restée. L'objectif affiché de TCPA est de protéger les droits des éditeurs de logiciels. TCPA propose les spécifications d'un module de sécurité, de surveillance et d'alerte grâce à une puce ou à un périphérique soudé à la carte mère. C'est l'équivalent d'une carte à puce associée non pas à l'utilisateur mais au poste de travail.

[92] TCPA (www.trustedcomputing.org) a changé de nom, à la suite de sa mauvaise réputation. Il a maintenant pour nom TCG (*Trusted Computing Group*) - https://www.trustedcomputinggroup.org .

[93] L'alliance TCPA inclut Intel, IBM, HP, Microsoft.

La sécurité des contenus

La sécurité dans un monde en clair

Pour protéger les objets nomades intangibles, les techniques cryptographiques permettent d'assurer leur sécurité, de leur faire franchir les régions hostiles sans dommage tout au long de leur pérégrination par le chiffrement des objets et par des protocoles cryptographiques pour leurs déplacements. Mais tôt ou tard, ces objets doivent être vus, entendus, lus ou exécutés en clair. Ils sont alors à la merci de leur utilisateur (copie pirate, falsification, détournement). Une solution pour réduire les vulnérabilités des objets mobiles est de leur laisser transporter eux-mêmes leur sécurité, par exemple en les marquant.

Si cette marque est perceptible (étiquette, code barre, logo), il est relativement aisé d'ôter cette étiquette et de la substituer pour usurper l'identification de cet objet, même si cette étiquette est signée électroniquement.

Si cette marque est indécelable et intimement fondue dans le corps de l'objet, il est plus difficile de l'arracher ou de l'effacer. C'est le but des techniques de tatouage qui consistent à incruster un message clandestin dans le contenu (syntaxique ou sémantique) même de l'objet numérique. Cette greffe doit posséder de bonnes propriétés de robustesse et résister à différentes menaces de lessivage.

Une infrastructure minimale est indispensable pour instiller la confiance dans ces univers numériques mobiles. Des entités (notaire numérique, tierce partie de confiance) vont établir une cartographie de la confiance qui permettra de faire appliquer une politique de sécurité. En effet, le code mobile ou les peuples d'agents mobiles intelligents circulant dans Internet pour le compte d'un usager ne sont pas protégés s'ils ne rendent pas compte à des entités de confiance, situées à des endroits stratégiques.

Le tatouage : une marque pour attester sa propriété

Le mot stéganographie[94] signifie « écriture cachée ». La stéganographie est l'art de dissimuler intimement un message clandestin dans le corps d'un autre message, en général de caractère anodin, de sorte que la présence même du message secret en soit cachée.

Le mot tatouage[95] (*watermarking*), désigne une technique stéganographique, qui incruste électroniquement dans une œuvre, un message clandestin. Ce court message subliminal est inséré de manière robuste (souvent par redondance), indécelable par les organes des sens humains[96] ou par une machine automatique[97] et indélébile, dans toute l'étendue du document. Il sert à étiqueter la propriété de l'auteur ou il peut être exploité à des fins de lecture[98] sous-jacente parallèle par une machine annexe de façon que cette empreinte invisible ne gêne pas une lecture standard.

Les mécanismes de tatouage reposent sur des approches multiples selon le type[99] de support et selon les contraintes[100] imposées pour remplir l'objectif de sécurité souhaité[101]. Une méthode de tatouage englobe des composantes de communication numérique, de traitement du signal, de cryptographie et de capacités physiologiques. Le tatouage est une technique de dissuasion : si la politique de sécurité consiste à prévenir les attaquants potentiels que les images sont tatouées, le pirate peut être découragé de tenter de dérober les œuvres. Encore faut-il, quand on dissuade, que la riposte soit crédible, c'est-à-dire que l'on puisse effectivement détecter et tracer[102] les œuvres tatouées.

Les applications du marquage et du traçage sont nombreuses : contrôle de l'origine (IPR), du contenu, de la destination (DRM) pour la propriété intellectuelle, pour le filtrage, pour l'indexation de contenu, pour la mesure objective (facturation, surveillance). La supervision d'objets répartis mobiles peut être aussi envisagée à travers ces marques, dans un contexte de

[94] La stéganographie qui consiste à élaborer des canaux cachés dans une communication, est une discipline ancienne, qui remonte aux Grecs du V^{ème} siècle avant J.C.

[95] Ce terme français fut proposé par l'auteur de ce chapitre en 1992.

[96] Les yeux pour les images, les oreilles pour les sons et la voix.

[97] Un algorithme de traitement de signal pour un contenu multimédia, un analyseur sémantique pour un logiciel.

[98] Marque d'annotation pour un film ou signe d'indexation pour une base de données d'images.

[99] Photographie, image animée, son musical, voix humaine, flux audio-vidéo, logiciel.

[100] Les stigmates indécelables doivent être résistant à un passage de l'image à l'analogique, à un passage à l'écran de télévision pour des images MPEG2, à une compilation optimisée pour un logiciel.

[101] Contrôle de l'origine, de la destination ou du contenu du document, c'est-à-dire authentification du propriétaire ou du destinataire et intégrité du document.

[102] Lecture automatique d'images ou de bibliothèques de logiciels sur des sites Web, balayage de réseau pour scanner les flux MPEG2.

réseaux hétérogènes. Le tatouage n'est pas encore parvenu à un stade de déploiement industriel. L'absence de standards et la multiplicité des procédés ne facilitent pas sa dissémination.

La stéganographie ne protège pas a priori les objets numériques, elle assure seulement leur sécurité dans l'obscurité. Néanmoins, la stéganographie risque de prendre de l'importance dans l'avenir, car les objets qui navigueront, seront de plus en plus exploités par de multiples utilisateurs qui manipuleront ces objets en clair.

Les perspectives de recherche

L'informatique a atteint une dimension planétaire et touche un large public amené à véhiculer et traiter un très grand nombre d'informations vulnérables. Il est donc indispensable de concevoir de nos jours la sécurité comme un état de vigilance à mettre en œuvre de manière proportionnée, une anticipation permanente à diffuser dans les infrastructures numériques, plutôt que de subir des attaques comme une fatalité moderne et de cicatriser en bout de chaîne les dommages déclenchés par les violences et les incivilités immatérielles. C'est le défi à relever pour gagner la confiance auprès des citoyens et des entreprises afin qu'ils utilisent fructueusement ces technologies.

À brève échéance, les thèmes de recherche portent essentiellement sur :

- la cryptographie : proposer des mécanismes cryptographiques moins gourmands en ressources notamment en environnement contraint, proposer des mécanismes cryptographiques pour la gestion des droits (DRM) garantissant leur traçabilité et proposer des méthodes de chiffrement par flot aussi sûres que les méthodes actuelles de chiffrement par blocs mais plus rapides ;
- les modélisations et mises en œuvre de politiques de sécurité : introduire l'espace, le temps, le contexte, la mobilité, gérer les conflits de politiques de sécurité, modéliser les grandes infrastructures et modéliser les politiques de sécurité pour le dossier médical ;
- la gestion des crises amplifiées par effet domino : protéger les infrastructures critiques et les rendre résilientes ;
- l'identification et authentification des acteurs, des contenus et la gestion des droits ;
- la biométrie : banque de données pour étalonner des algorithmes de reconnaissance, signature avec biométrie, reconnaissance du comportement par suivi de silhouette et analyse des gestes ;
- le tatouage d'images, de sons, de flux vidéos et de logiciels : protection des ayant-droits, contrôle des copies, authentification, intégrité ;
- la stéganalyse : détection d'informations cachées par procédés de stéganographie ;
- la sécurité des SI : techniques de détection d'intrusion, de protection de la vie privée, sécurité des grilles, architectures de système de leurres ;
- la sécurité des réseaux fixes et sans fil, mobiles, actifs, auto-configurables, ad hoc ;
- l'évaluation réaliste des vulnérabilités sur le plan opérationnel, arrêt des virus, filtrage du spam en amont du terminal de l'utilisateur final ;
- la sécurité de l'urbanisation digitale et la sécurité du virtuel : nouveaux paradigmes de sécurité répondant aux besoins des applications ubiquitaires, établissement de confiance sans se baser sur une infrastructure existante ou une organisation a priori, structures avec faible connectivité ou connectivité intermittente, niveau de garanties intermédiaires par rapport à la recherche habituelle d'une assurance absolue ;
- la certification, l'assurance de sécurité : introduction de méthodologies d'évaluation de la sécurité, incrémentales, plus rapides et moins coûteuses.

À plus long terme, la sécurité numérique devrait affronter le mur de la loi de Moore et s'immiscer dans les fissures entre le matériel invisible des transistors binaires en prolifération presque cancériforme et le logiciel éparpillé, grouillant du marché massif des ordinateurs en poussière intelligente (*smart dust*) et franchir le Rubicon du numérique, c'est-à-dire parvenir à l'âge quantique, aborder la sécurité des nanotechnologies et de la bioinformatique, et se saisir des questions suivantes :

- la cryptographie quantique : recherche en amont pour la distribution des attributs de sécurité, en utilisant une confiance inédite fondée sur l'incertitude d'Heisenberg, et bâtir des réseaux quantiques hautement sécurisés à partir de transmissions en clair de photons uniques et/ou de gerbes de photons, résistants à une lecture indiscrète grâce à des protocoles sécurisés fondés sur le constat révélé par la mécanique quantique, à savoir l'impossibilité physique d'observer subrepticement un grain de lumière sans le perturber et finalement prévenir les deux instigateurs de la communication quantique ;
- la sécurité des nanotechnologies : recherche en amont sur le marquage à une échelle invisible du monde physique et sur des infrastructures de confiance pour la traçabilité des nanotechnologies ;
- la sécurité numérique du monde vivant : recherche en amont, avec des principes éthiques, sur le marquage et la traçabilité du règne animal et végétal, avec des prothèses numériques ou une intrication du numérique dans le cœur des cellules vivantes ;

- la sécurité de la poussière intelligente, c'est-à-dire des nano-ordinateurs massifs et passifs, la future génération des ordinateurs en essaim, presque invisibles qui vont jalonner bientôt notre espace ambiant, étiqueter nos vêtements et escorter nos objets familiers ;
- la sécurité de la prochaine convergence à l'horizon, celle du numérique, du quantique avec les bio-nanotechnologies, c'est-à-dire amorcer une synthèse humaniste du traitement de la connaissance du monde artificiel créé ex nihilo, afin de contrôler l'écosystème artificiel que l'Homme vient d'engendrer depuis plus d'un demi-siècle, d'apprivoiser les créatures ultérieures, d'explorer sereinement les nouveaux territoires et d'appréhender les ruptures technologiques à venir.

Conclusion

Avec l'explosion des contenus, l'architecture des cybersphères (données et programmes associés) est rhizomorphe. Ce sont des bulbes de données et de programmes qui (grâce à la convergence informatique et télécoms) sont en train de s'installer durablement et parfois d'échapper à leur propriétaire. Il existe une réelle inquiétude face à l'urbanisation numérique en cours : perplexité des utilisateurs, mais aussi difficulté des développeurs et des exploitants. L'utilisateur va disposer bientôt d'un nouvel écosystème, d'une immense machine de communication où l'on pourra relier les êtres humains nomades et leurs appareils électroniques usuels interconnectés. On assiste à la naissance d'un règne numérique composé d'entités autonomes qui vivent leur propre cycle. La perspective de cette communication généralisée, en réseau, sans hiérarchie, en utilisant ce nouveau règne, soulève des questions de sécurité, listées ci-dessous, qui n'ont pas trouvé de réponses à ce jour :

a) la disparition des cloisons étanches séparant les vies privée, professionnelle et publique. Tout individu construit, sur cette unique infrastructure commune, en prolongement de son corps, un réseau virtuel privé avec ses propres données. Ce réseau commence dans les prochaines prothèses numériques du corps biologique et finit par se dissoudre aux confins de la planète dans la masse chaotique de la pâte numérique indifférenciée de l'information fongible de la Toile. Ce réseau propre à chaque individu est perméable, vulnérable et finalement lui échappe. L'individu laisse aussi des empreintes, des traces numériques indélébiles que d'autres humains peuvent retrouver après enquête, pour reconstituer une biographie à son insu ;

b) la construction complexe au-dessus du monde physique, de plusieurs étages de mondes logiques virtuels, toujours plus symboliques et abstraits. La sécurité numérique consiste justement à amarrer, coûte que coûte dans ces entrelacs virtuels, ces divers étages à des instances physiques réelles, afin de se raccrocher au monde réel. Les concepteurs de ces édifices sont prisonniers de ces paradigmes qui s'accumulent au fil du temps de l'évolution technologique et qui finissent par paralyser l'essor des techniques numériques ;

c) l'édification d'une masse de données (pépites d'information enfouies dans un chaos de déchets informationnels) qui gonfle à vue d'œil et que les moteurs de recherche généralistes ont du mal à vaincre : information fongible, tout venant, qu'il est nécessaire de rechercher, de saisir, de trier, de sélectionner, de vérifier, créant ainsi une entropie envahissante ;

d) l'effacement des frontières des espèces :
   - espèces géographiques comme les États (Internet ignore les contours des pays et transgresse les barrières nationales), les systèmes d'information des entreprises (l'informatique est de plus en plus externalisée), les huis clos (les ondes hertziennes débordent les murs de nos constructions physiques) ;
   - espèces temporelles comme les réunions en chair et en os, les discussions en direct ; la messagerie, les forums permettent le foisonnement de rencontres et de conversations en dehors du temps ;
   - espèces informatiques qui se fondent dans un syncrétisme indescriptible avec des ontologies distinctes mais entremêlées, comme les constructions d'entités protocolaires encapsulées, interopérables qui s'enchevêtrent et deviennent interdépendantes ;

e) la relative disgrâce de la notion d'identité, avec la prévalence de l'anonymat, si essentiel dans la philosophie de l'Internet, et le recul concomitant de la notion d'auteur dans la masse de documents disponibles sur le Web.

Cette vision suscite des interrogations sur les effets regrettables de l'univers numérique, auxquels on n'a pas encore découvert de parades. Le système globalement n'est pas maîtrisé en temps réel. La généralisation des virus n'avait pas été prévue avec l'arrivée du haut débit, la congestion des réseaux par les spams n'a pas été non plus annoncée[103].

La sécurité du XXI^{ème} siècle devra élaborer une confiance renouvelée, dans une clarté numérique assumée par tous les acteurs[104], guidée par une éthique persévérante, dans un esprit civique, entre les deux mondes biologique et numérique, à l'échelle d'une gouvernance numérique planétaire.

[103] Il existe toutefois des satisfactions, c'est la déviance heureuse de certains services, c'est l'imprédictible succès de certains usages : les messages courts (SMS) du téléphone portable n'ont pas été conçus pour les conversations entre utilisateurs, les utilisations légales des architectures P2P ont eu un succès fulgurant au-delà des prédictions de ses précurseurs. Toutes ces réussites n'avaient été pas prévues par les concepteurs de ces systèmes. En sécurité, le pouvoir d'imagination et la capacité de détournement sont plutôt dans le camp des attaquants.

[104] Chercheurs, concepteurs, éditeurs de logiciels et de contenus, distributeurs, exploitants, équipementiers, systémiers, opérateurs, fournisseurs d'accès, de contenus et de services, dirigeants d'entreprise, utilisateurs, services de lutte contre la cybercriminalité, associations.

Bibliographie

Lagrange X., GodlewskiP., Sami Tabbane S. (2000), *Réseaux GSM-DCS*, 5e édition revue et augmentée, éditions Hermès Sciences Publications.

Lagrange X. et al (2005), *Principes et évolutions de l'UMTS*, éditions Hermès Sciences Publications.

Natkin S. (2001), *Les protocoles de sécurité*, Paris, éditions Dunod.

Péliks G. (2005), *La sécurité à l'usage des décideurs*, éditions etna france, Coll. Ténor. www.etnafrance.org .

Riguidel M. (2000), "Pour l'émergence d'une nouvelle sécurité dans les réseaux de communications et les systèmes d'information futurs", OFTA, *Arago Vol. 23*, Paris.

Riguidel M. (2003), "Les infrastructures critiques et leurs interdépendances", Paris, *Revue de l'Électricité et de l'Électronique*, Septembre 2003.

Riguidel M. (2004), *La sécurité à l'ère numérique*, Paris, éditions Hermès Lavoisier, Coll. « Les Cahiers du Numérique »

Riguidel M. (2004) et al, "Intimité et sécurité, les clefs de la confiance dans l'économie numérique", *Rapport du club.sénat.fr, Sénat*, http://www.club.senat.fr .

Riguidel M. (2004), *Le téléphone de demain*, Paris, éditions Le Pommier.

Schneier B. (1996), Cryptographie appliquée, algorithmes, protocoles et codes source en C, 2ème édition, Vuibert, France.

Yi M., Varadharajan V. (2001), "Robust and Secure Broadcasting". *In proc. of International Conference on Cryptology* in India (INDOCRYPT'01). Chennai, India. December 2001.

Zémor G. (2000), *Cours de cryptographie*, Paris, éditions Cassini.

Index, sigles et abréviations

Table des matières