Cet article a été publié dans les actes du Symposium sur la Sécurité des Technologies de l'Information et des Communication 2003.

Les enjeux de la sécurité des systèmes d'information

GDI Jean-Louis Desvignes
École Supérieure et d'Application des Transmissions
Quartier Leschi - BP 18
35998 Rennes Armées

SSTIC 2003

Organisation

SSTIC03 a été organisé par l'École Supérieure d'Électricité, l'École Supérieure et d'Application des Transmissions, le Commissariat à l'Énergie Atomique, la société Cartel Sécurité et le magazine de la sécurité informatique MISC.

Comité d'organisation

Christophe Bidan	Supélec
Philippe Biondi	Cartel Sécurité
Eric Detoisien	
Thiébaut Devergranne	
Eric Filiol	École Sup. et d'Application des Transmissions
Thierry Martineau	École Sup. et d'Application des Transmissions
Laurent Oudot	Commissariat à l'Énergie Atomique
Frédéric Raynal (Président)	MISC Magazine

Comité de programme

Gildas Avoine	EPFL
Christophe Bidan	Supélec
Renaud Bidou	
Philippe Biondi	Cartel Sécurité
Cédric Blancher	Cartel Sécurité
Patrick Chambet	Edelweb
Yves Correc	CELAR
Eric Detoisien	
Thiébaut Devergranne	
Eric Filiol	ESAT
Nicolas Fischbach	Colt Telecom / Securite.org
Sylvain Gombault	ENST Bretagne
Pascal Lointier	CLUSIF
Robert Longeon	CNRS
Thierry Martineau	ESAT
Marc Mouffron	EADS Telecom
Laurent Oudot	CEA/DAM
Frédéric Raynal	MISC magazine
Ludovic Rousseau	Gemplus
Marc Rybowicz	Université de Limoges
Franck Veysset	France Télécom R&D

Les enjeux de la sécurité des systèmes d'information

GDI Jean-Louis Desvignes

École Supérieure
et d'Application des Transmissions
Quartier Leschi - BP 18
35998 Rennes Armées

1 Introduction

C'est pour moi un très grand plaisir d'ouvrir ce cycle de conférences consacré à la SSI : c'est d'abord avec une certaine émotion que je retrouve l'amphi de cette belle école quelques vingt-cinq ans après l'avoir quittée. C'est ici que je me suis réellement initié aux joies des systèmes informatiques et c'est ici d'ailleurs, que j'ai découvert que ces machines étaient foncièrement sournoises : déjà à l'époque, lorsqu'elles avaient enfin accepté d'effectuer une tâche (écrite en FORTRAN ou en COBOL), il n'était pas certain que celle-ci fût réellement et complètement accomplie et il n'était pas exclu en revanche que ces automates évolués n'en eussent pas exécuté une autre qui ne leur était pas demandée.

Aujourd'hui, ce n'est plus une suspicion, c'est une certitude !

C'est ensuite un plaisir de me retrouver dans ce milieu délicieusement paranoïaque du monde de la sécurité. Comme c'est agréable de pouvoir frissonner ensemble en évoquant les dangers qui nous guettent chaque fois que nous nous laissons aller à jouer de notre clavier ou à flirter avec une souris ("*caresser le mulot*" aurait rectifié notre Président) en étant certains d'être compris à demi-mot ! Quel bonheur de pouvoir fustiger l'inconscience de ces responsables qui mettent en péril la vie de leur société, voire des services de l'Etat, par leurs coupables négligences ! Et quels frissons nous parcourent lorsque nous évoquons les mille et une manières que peuvent employer les Big Brothers potentiels de la planète pour épier nos moindres faits et gestes : les coups de fil que nous donnons et tous nos déplacements par l'exploitation des capacités des réseaux cellulaires, les lieux où nous dégainons notre carte bancaire, nos excès de vitesse sur les autoroutes, bientôt, en raison de la trahison des tickets de péage ; et toutes nos petites manies à cause des traces que nous laissons sur le WEB ou des petits cadeaux empoisonnés que nous récoltons au gré de nos promenades sur la toile. Ah ! Quel vertige s'empare de nous quand nous pensons que toutes ces informations, qui constituent des pans entiers de notre vie, sont stockées à notre insu, des semaines, des mois, dans certains cas des années. Alzheimer peut bien frapper, nous sommes protégés, notre mémoire est externalisée !

On peut effectivement prendre les choses avec bonne humeur et se dire qu'après tout, toutes les possibilités qu'offrent les nouvelles technologies consti-

tuent des avancées propres à satisfaire le mieux possible nos besoins de consommateurs paresseux, pressés et exigeants, ou à garantir notre sécurité vis à vis des mauvaises gens. Mais on peut tout aussi bien les aborder avec effroi en constatant que le périmètre de notre vie privée s'est rétréci comme peau de chagrin, davantage encore depuis le 11 septembre 2001, et que ce n'est pas fini ! Certaines annonces relatives aux nouvelles générations de puces ont en effet de quoi nous faire frémir, même s'il n'est pas encore envisagé de nous les greffer sous la peau, ...

Pourtant, une discipline, une science, un art, je ne sais trop comment la qualifier, est censé nous apporter la sérénité et nous permettre de redevenir maîtres de ce que nous souhaitons ou divulguer ou au contraire protéger parmi les informations qui nous concernent ou qui nous sont confiées à un titre ou à un autre : c'est **la sécurité des système d'information** ou, pour adopter le langage de ce séminaire, **la sécurité des technologies de l'information et de la communication**.

2 Qu'est-ce que la SSI ?

La première expression, née au milieu des années 80, désigne l'ensemble des techniques propres à garantir les informations traitées ou transmises par un système d'information, au sens large, en termes de **confidentialité, d'authenticité, d'intégrité et de disponibilité** comme tout un chacun le sait dans cette noble assemblée.

Permettez-moi simplement de souligner **l'importance de la disponibilité** des informations qui implique, de facto, celle du système qui les traite lui-même. Dès lors la SSI concerne bien évidemment tout système d'information, quand bien même celui-ci ne traiterait aucune information confidentielle : ce n'est pas parce que le PABX d'une entreprise voit transiter des informations sensibles qu'il doit être protégé (si tel était le cas ses dirigeants seraient coupables de légèreté) mais parce que sans lui, l'entreprise ne peut plus travailler. Par extension, tout système pilotant un processus doit être l'objet d'une protection SSI, qu'il s'agisse des télécommandes d'un lanceur spatial, du système de contrôle d'une centrale nucléaire, du système de gestion des stocks d'une usine automobile, etc,... qui doivent être protégés comme l'ordinateur de la secrétaire de direction, celui de notre médecin traitant ou la puce de notre carte de paiement. "*Vaste programme !*" comme aurait dit le général de Gaulle. Et pourtant, c'est bien de cela qu'il s'agit car les enjeux de la SSI sont énormes.

Si vous le permettez, je commencerai par évoquer ses principales composantes et les évolutions qui sont intervenues sur chacune d'elles avant d'examiner les enjeux.

La SSI, c'est l'art de combiner un ensemble de mesures préventives et curatives, à la fois au plan technique et organisationnel en vue de faire face aux menaces que l'on aura pris soin, au préalable, d'identifier et de hiérarchiser. Ce n'est pas à vous que je vais apprendre que toute entreprise de sécurisation doit débuter par une analyse des risques et

des menaces : que dois-je protéger, contre qui ou quoi ? Pourtant, combien de sociétés ou d'organismes se laissent-ils encore séduire par toutes sortes de solutions techniques coûteuses ne répondant pas à leur véritable besoin de sécurité. Rappelons-nous que, bien souvent, de simples mesures organisationnelles bien appliquées suffisent à contrer la majorité des risques, surtout lorsque ceux-ci peuvent provenir aussi bien de l'intérieur que de l'extérieur de l'entreprise.

Mais je suppose que si vous êtes venus à ce séminaire, vous savez cela très bien, et c'est surtout de technique que vous souhaitez traiter.

Sur ce plan je rappelle que la SSI repose sur trois techniques de base, par ordre d'apparition : la cryptographie, l'anti-compromission électromagnétique et la sécurité informatique. Ces trois techniques de protection sont aujourd'hui étroitement imbriquées, comme le sont d'ailleurs de plus en plus les télécommunications et l'informatique, ce qui implique dorénavant une approche globale de la SSI.

3 Au commencement était la Cryptographie...

Première apparue dans l'histoire de l'humanité, la cryptographie, qui n'avait guère évolué pendant deux millénaires – on en était resté au bon vieux principe des systèmes symétriques de partage d'une convention secrète, ce qui rendait délicate toute utilisation de masse – a connu sa grande révolution avec l'invention, au milieu des années soixante dix, des systèmes asymétriques, dits "*à clefs publiques*. Cette découverte, née à l'occasion de la compétition qui allait être remportée par le fameux DES (Data Encryption Standard), d'ailleurs symétrique, d'IBM, a mis quelque temps à entrer en application, mais a largement dépassé aujourd'hui son objectif initial : comme on le sait, selon que l'on utilise un tel procédé, par exemple le célèbre R.S.A. (du nom de ses inventeurs : Rivest, Shamir et Aldeman), dans un sens ou dans un autre, on obtient soit un système de chiffrement, soit un système de signature assurant l'authentification des correspondants, l'authenticité et l'intégrité des informations. En combinant de surcroît ce procédé asymétrique peu performant en terme de débit d'information avec un procédé symétrique, on dispose de la boîte à outil du parfait cryptologue, prêt à satisfaire le besoin de sécurité exprimé pour toutes les formes de transaction électronique.

Naturellement les choses ne sont pas aussi simples, et l'installation d'un système de sécurité reposant sur l'usage des clefs publiques pour un vaste réseau de correspondants tel que celui du réseau Santé sociale, celui du monde bancaire ou celui de la Défense, se heurte à de nombreuses difficultés, notamment d'organisation des infrastructures de gestion de clefs (IGC). Le seul problème de la désignation d'une **autorité de certification** et de sa reconnaissance par d'autres a déjà alimenté bien des débats.

Quant à la protection réellement assurée par les procédés cryptologiques, celle-ci est naturellement au cœur des enjeux. Depuis la nuit des temps le combat entre l'épée et la cuirasse était resté équilibré : décrypter la scytale ou Jules César est à la portée d'un enfant sachant lire et écrire. Casser le chiffre allemand

pendant la Première guerre mondiale, le capitaine Painvin l'a fait ; venir à bout de l'ENIGMA était un sacré défi, mais les Anglais de Bletchey Park, bien aidés par les services polonais et français, y sont parvenus et c'est sans doute grâce à cela que la bataille de l'Atlantique, véritable tournant de la seconde guerre mondiale, a été remportée. Pourtant, à un certain moment, face à des algorithmes solides, soumis à la sagacité de la communauté internationale des cryptologues, on a vraiment cru que la cuirasse l'avait définitivement emporté. Qu'une nouvelle puissance de calcul se profile à l'horizon pour mener à bien l'exploration exhaustive de toutes les combinaisons d'une clef, (un nouveau supercalculateur, des machines massivement parallèles ou des milliers d'ordinateurs personnels connectés à travers l'Internet) il semblait suffisant d'augmenter de quelques bits la longueur de la clé, en théorie, pour se remettre à l'abri pour plusieurs années (de 40 bits on passait à 56, de 56 à 64, etc...)[1]

4 Des clefs longues certes, mais ....

Mais la longueur des clefs n'est pas tout dans un système de sécurité. Vous le savez bien. Cependant, dans le débat sur la libéralisation de la cryptologie qui faisait rage il y a quelques années, on a, pour simplifier les dossiers à l'intention des politiques, quelque peu caricaturé la problématique et finalement tout le monde s'est polarisé sur ces fichues longueurs de clefs alors que les vrais problèmes étaient ailleurs. Il y a parmi vous des spécialistes qui savent que concevoir un bon système de chiffrement n'est déjà pas si aisé, mais que le réaliser et le mettre en œuvre pour qu'il soit suffisamment ergonomique et utilisable par un quidam en toute sécurité est un autre challenge ! A quoi bon s'encombrer d'une clef de 128 bits, si seulement 8 bits sont effectivement utilisés, si votre clef se promène quelque part sur votre ordinateur ou si elle est transmise à votre insu avec vos messages ?

Or, et c'est là l'un des effets néfastes de la libéralisation de la cryptologie tellement applaudie en 1999 lorsqu'elle a été annoncée : ce que certains politiques ont pris pour un remède miracle contre les actes de piratage de toutes sortes contre lesquels ils voulaient nous protéger (rappelez-vous ECHELON !) s'est en fait traduit par **un envahissement de produits de sécurité aussi efficaces qu'un placebo**. La plupart des logiciels de cryptographie grand public affichant pourtant des clefs de belle taille ne résistent pas aux investigations d'un stagiaire de l'un des prestigieux cours du CFSSI, du mastère spécialisé de SUPELEC ou de l'ENST. La preuve avait été établie, bien avant le 11 septembre, que les modules

[1] Pour les systèmes asymétriques, la problématique est différente : s'il s'agit de factoriser des nombres premiers (c'est-à-dire de retrouver les deux nombres premiers à partir de leur produit quand ce sont des nombres de plus d'une centaine de chiffres, 1024, 2048 bits, etc..) certes, on peut compter sur la puissance de calcul mais aussi sur la découverte d'un meilleur algorithme de factorisation, une astuce mathématique en somme, qui pourrait subitement décrédibiliser les systèmes les plus répandus. Pour certains, casser le RSA est leur raison de vivre, pour ceux qui l'utilisent massivement, comme les banquiers, la perspective d'une telle percée est un véritable cauchemar !

cryptographiques d'un grand éditeur de logiciel étaient "*plombés*" à la demande de son gouvernement, on imagine ce qu'il peut en être aujourd'hui ...

Mais, quand bien même le module cryptographique serait de bonne facture, celui-ci peut dans bien des cas être comparé à une porte blindée que l'on fixerait sur des cloisons en placoplâtre. A quoi bon, faut-il encore le souligner, s'embêter à chiffrer ses fichiers avant de les envoyer si ceux-ci sont accessibles lorsqu'ils sont encore en clair, à partir de l'Internet, en utilisant l'une des multiples failles du système d'exploitation devenu le standard mondial dont on ne veut pas nous donner les sources. J'y reviendrai tout à l'heure.

5 Le débat sur la cryptographie : un écran de fumée ?

Vous aurez compris, à travers mes propos, que je considère que le problème de la cryptologie, s'il est loin d'être secondaire, n'en a pas moins servi à occulter celui, plus délicat, de **la sécurité informatique**. Pendant que l'on guerroyait entre spécialistes de fraîche date sur la longueur des clefs, d'autres imaginaient comment rester maîtres des systèmes informatiques, quand toutes les informations de la planète seraient chiffrées. On perçoit bien l'importance relative des deux domaines à l'aulne des mesures de restriction au commerce des systèmes informatiques sécurisés. Alors qu'ils libéralisaient les produits cryptologiques apparemment forts, les E.U. maintenaient l'embargo sur les systèmes évalués au plus haut niveau de sécurité selon les critères de l'*ORANGE BOOK*.

Il est vrai que sur le plan de la sécurité informatique, il y a fort à faire si l'on veut pouvoir se mettre un jour au volant de son ordinateur et prendre les autoroutes de l'information, pour utiliser une expression désuète, en toute sécurité. Vous connaissez certainement cette boutade émanant d'un grand constructeur d'automobiles : "si on avait construit les voitures comme on a construit l'informatique, on roulerait encore en trottinette" ! C'est un jugement un peu sévère, mais il est vrai qu'il y a peu de temps, lorsqu'un bogue était découvert dans un logiciel, on nous demandait d'être patient, et d'attendre la version suivante pour le voir corrigé. Aujourd'hui, grand progrès : on a la possibilité de souscrire un contrat nous donnant le droit d'accéder à des "*patchs*" correctifs. Pauvres constructeurs automobiles qui sont encore obligés de rappeler à grands frais des milliers d'autos pour modifier un boulon ! La facilité de réparation n'est cependant pas un gage de qualité de service au bout du compte. On s'habitue à ce genre de rustines et à cette accumulation de couches de logiciels qui encombrent nos machines et nous obligent à en acheter sans cesse de plus puissantes pour des tâches qui, dans bien des cas, n'ont pas fondamentalement évolué.

6 Des livres de différentes couleurs

Les travaux américains sur la sécurité informatique, le COMPUSEC comme ils disent, furent concrétisés au début des années 80 par la publication de l'*ORANGE BOOK* qui établissait les critères permettant de classer les systèmes informatiques selon le niveau de confiance que l'on pouvait leur accorder.

Très vite quatre pays européens ont compris que ces critères pourraient fausser la compétition économique et se sont efforcés de définir leurs propres critères : il y eut bientôt un livre de couleur différente par pays avant que les quatre ne se décident à harmoniser ces critères qui devinrent les "*ITSEC*". Ceux-ci, heureusement, ne différaient pas des critères américains uniquement par la couleur mais par leur pertinence.

Mon premier travail en arrivant au SCSSI fut, d'ailleurs, de mettre en place le schéma national de certification des produits de sécurité évalués selon ces critères. Cela consistait, en particulier, à faire accréditer par le COFRAC les laboratoires d'évaluation selon la norme ISO/IEC 17025 et à les agréer selon des critères gouvernementaux. Mais, en parallèle nous avions déjà engagé des travaux pour aboutir à la convergence américano-européenne. Les "*critères communs*" furent publiés en 1999 et un accord de reconnaissance mutuelle fut alors signé entre six pays : ces critères allaient ensuite être adoptés comme une norme ISO (ISO/IEC 15408).

Un grand pas avait été franchi en matière d'instauration de la confiance réciproque. Je dois dire que j'étais particulièrement fier de l'action des équipes françaises dans cette entreprise. A côté du SCSSI, les laboratoires du CNET repris par le LETI, du CELAR et d'autres laboratoires privés avaient acquis une solide expérience en évaluation. Dans un domaine particulier, celui des cartes à puce sécurisées, nous étions, et j'espère que nous le sommes encore, leaders mondiaux.

7 La carte à puce : meilleur rapport coût/efficacité en matière de sécurité

Il est inutile, je crois, de signaler l'importance de ce domaine pour tout ce qui touche à la sécurité et les enjeux colossaux de ce marché. La carte à puce est en effet l'élément qui a le meilleur rapport cout/efficacité pour améliorer de manière significative le niveau de sécurité d'un système Or, les Américains, pour diverses raisons en particulier juridiques et commerciales, n'ont pas cru immédiatement à cette technologie. Je me souviens que la première fois où l'ordre du jour d'une réunion avec la NSA a comporté l'item "*smart cards*", ce devait être en 1986, nos collègues américains ont déposé sur la table une calculette genre convertisseur d'euros pour personnes âgées, tandis que nous exhibions la première CP8 de BULL. Inutile de vous dire qu'ils ne nous ont pas pris au sérieux avec notre bout de plastique.

Aussi, quel plaisir ai-je ressenti, lorsque fin 99, le patron de la branche INFOSEC de la NSA, m'a demandé s'il pourrait bénéficier de notre aide parce que le Département de la Défense avait décidé de doter tout son personnel de carte à puce. En lui répondant que nous, petits français, étions prêts à apporter notre assistance à la colossale NSA, je pensais à l'histoire de cette souris se promenant dans la savane à côté de son copain l'éléphant et qui, se retournant, s'exclamait : "*tu as vu toute la poussière que nous faisons ?*".

8 Des tentatives de déstabilisation

Pourrons-nous préserver cette avance ? La lutte est féroce. Il y a eu des tentatives de déstabilisation et de discrédit de notre technologie par des laboratoires commandités par de grands éditeurs de cartes ; il y a eu la publication sur le NET de la liste de toutes les vulnérabilités des cartes. Si le pirate Serge Humpich avait eu cette liste, il ne lui aurait pas fallu quatre années de labeur pour fabriquer ses fausses cartes (les "*YES CARDS*").

Aujourd'hui, d'un côté, il y a des tentatives américaines pour mettre la main sur ce secteur notamment par les prises de participation dans Gemplus (et probablement des transferts de brevets), de l'autre, l'initiative conjointe INTEL /MICROSOFT sur la puce FRITZ et le logiciel PALADIUM, pourrait bien assécher, comme le craint Ross Anderson, le marché de la carte à puce, si les fonctions que celle-ci assure peuvent être reprises par celle-là. L'horizon est donc loin d'être clair.

Quittons les cartes pour revenir aux systèmes d'exploitation les plus répandus et dont on ne veut pas nous donner les sources.

9 Et les logiciels libres ?

Ce refus est peut-être, tous comptes faits, pure charité, car je ne connais pas grand monde aujourd'hui, à part les Chinois, en mesure de se lancer dans l'investigation des quelques dizaines de millions d'octets que comportent les différentes strates des packs de M.S ! Certes on peut y découvrir quelques bogues accidentels ou non, mais on n'aura jamais l'assurance qu'il n'en subsiste pas. Ah ! Que notre bon vieux MINITEL était rassurant sur ce point ! Pas d'intelligence, pas de malice ! Comme les fantassins !

Pour faire face à ce double problème de monopole et de défiance, une voie existait pourtant. Celle-ci n'a pas suffisamment été explorée quand il était encore temps de ne pas se livrer corps et âme à ce cher, très cher Bill ! Celle des logiciels libres. Certains Etats ont pourtant manifesté des velléités de le faire, comme l'Allemagne, j'ai même appris que la Tunisie s'était attelée à ce challenge. En France, est-ce à cause de l'échec du tristement célèbre Plan Calcul que le gouvernement, qui a lancé le PAGSI, et l'Administration, qui s'informatise pourtant à marche forcée, se sont montrés si frileux et sans ambition sur ce dossier ? Toujours est-il que même un département ministériel tel que celui de la Défense, généralement soucieux de préserver l'indépendance et la sécurité de notre outil militaire, ne s'est pas engagé avec conviction dans la voie des logiciels libres. Je connais une armée qui a même choisi, pour des raisons certes louables d'uniformisation et de simplicité de mise en œuvre, d'utiliser Windows pour ses serveurs quand la grande majorité du marché plébiscite LINUX !

Cela dit, il ne faut sans doute pas attendre des miracles ni des économies aussi substantielles que celles que certains prétendent faire en recourant aux logiciels libres. D'abord l'investissement intellectuel pour les organismes qui les utilisent n'est pas à négliger. Ensuite, la faveur dont ils sont l'objet depuis quelques temps

a eu tôt fait d'estomper leur caractère libre. Nombre d'offres reposent désormais sur des solutions, certes à base de logiciels libres, mais exigeant pour être intégrées et maintenues, des prestations grassement rémunérées et débouchant sur des produits propriétaires. C'est normal.

10 Une ambition européenne ?

Pourtant, je persiste à penser qu'un recours aux logiciels libres est possible et serait hautement bénéfique, tant en termes de coût qu'en termes de confiance. J'ajoute que c'est à l'Administration de donner l'exemple : elle regorge de gens compétents qui trouveraient un intérêt immense à se lancer dans cette aventure. Naturellement, ce que je dis pour notre pays prendrait encore plus de sens si une telle action était réellement soutenue à l'échelle de l'Union européenne. Nous avons réussi dans les domaines de l'énergie nucléaire, de l'aéronautique et de l'espace, à gagner notre indépendance, nous allons lancer GALILEO, le concurrent du GPS, pourquoi ne tenterions-nous pas de conquérir notre autonomie dans les technologies de l'information si, comme on nous l'assène depuis des années, l'information est devenue la matière première la plus précieuse ?

Une première étape a été franchie il y a peu de temps : une agence européenne de la sécurité des systèmes d'information va voir le jour. Il y a quelques années, je l'appelais de mes vœux, tant j'étais ulcéré de voir nos systèmes de protection les plus évolués traverser l'Atlantique pour se faire évaluer dans une agence de l'OTAN située en fait au sein de la NSA. Certains pays étaient même prêts à s'en remettre à celle-ci pour choisir des équipements de chiffrement destinés à un usage purement européen ! Je précise qu'il ne s'agissait pas de la Grande Bretagne, ...J'avais, à l'époque, préconisé d'utiliser les compétences des trois ou quatre pays ayant une compétence en cryptologie, en créant dans un premier temps une sorte d'agence virtuelle s'appuyant sur les accords de reconnaissance mutuelle des certificats de sécurité qui venaient d'être signés ... Je vois avec satisfaction que nous avons franchi un grand pas et j'espère que le représentant de la DCSSI pourra nous dire quel rôle la France entend jouer dans cette nouvelle agence.

11 BIG BROTHER n'est pas loin !

Car la vigilance s'impose plus que jamais : il y a quelque temps déjà, dans le but de lutter contre le piratage de logiciels, de grandes firmes américaines avaient imaginé de graver dans le silicium des microprocesseurs un numéro d'identité qui aurait pu servir à vérifier, au moment d'une connexion volontaire ou indirecte avec le site de Microsoft, que vous aviez bien acquitté les droits de vos licences en ouvrant toute grande la porte de votre disque dur à votre éditeur préféré. A l'époque, je me souviens qu'un slogan publicitaire avait été détourné : "*la NSA et ... MICROSOFTen avaient rêvé, INTEL l'a fait*".

Une levée de boucliers des mouvements libertaires s'en était suivie et l'on avait fait mine de faire machine arrière. Depuis il y a eu le 11 septembre, un

deal dans un grand procès américain est intervenu, et le gendarme du monde ne s'embarrasse plus de scrupules pour assurer sa sécurité. C'est dans ce contexte que se profile l'arrivée de nouvelles puces qui pourraient bien, si l'on n'y prend garde, perfectionner le dispositif précédent. Je sais que les puces "*FRITZ*" que j'ai déjà évoquées, suscitent des débats et je suis certain que ce thème sera abordé ici même.

Pour résumer à l'intention de ceux qui n'auraient pas encore entendu parler de ces nouvelles plates-formes de INTEL et du logiciel PALLADIUM qui lui serait associé, il s'agit de faire rentrer dans une puce appelée TCPA qui signifie *Trusted Computing Platform Alliance* une partie du logiciel PALLADIUM également nommé NGSCB (*Next Génération Secure Computing Base*) incorporé dans les futures versions de WINDOWS (et déjà intégré dans XP) de manière à rendre impossibles les opérations de piratage de toute nature. Ceci, en procédant à des contrôles systématiques locaux et **en ligne** de votre configuration matérielle et logicielle. Ce contrôle pourrait aller jusqu'à l'effacement des programmes illicites et même des données obtenues par un traitement illicite !

Toutes sortes de dérives de ce système censé lutter contre le piratage sont imaginables et je ne saurais trop vous conseiller de lire les articles et la foire aux questions de Ross Anderson sur le sujet. Les conséquences de cette innovation peuvent êtres extrêmement lourdes, autant en terme économique qu'en termes de souveraineté des Etats (quid des systèmes de la Défense utilisant WINDOWS ?) ou de libertés individuelles. Les mouvements libertaires qui s'étaient mobilisés contre les projets précédents (CLIPPER et numéro unique) seront-ils capables de résister une nouvelles fois dans le nouveau contexte sécuritaire ? Rien n'est moins sûr. Aux Etats-Unis comme partout, l'heure n'est pas propice aux états d'âme face aux atteintes à la liberté. Mais je suis sûr que le représentant de MICROSOFT qui nous fait l'honneur de participer à ce séminaire se fera un plaisir de nous rassurer.

Cela dit, si en matière de SSI il faut parfois se méfier de ses amis un peu envahissants, il ne faut pas perdre de vue que nous avons tous un ennemi commun, les gens malveillants qui utilisent les TIC à des fins délictueuses ou criminelles. Je salue au passage la création de l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, dont la responsable est venue faire une conférence il y a quelques mois lors de la rentrée de l'ESAT.

12 Des "cyber-vigies et des cyber-pompiers"

Quels que soient, en effet, les progrès que nous réaliserons en matière de sécurité informatique en amont, c'est-à-dire dans la conception, la réalisation et l'évaluation des systèmes de protection, je pense que la cuirasse comportera toujours quelques faiblesses que des pirates, qu'ils soient en culotte courte, en blouse blanche ou en tenue bariolée, tenteront d'exploiter à des fins ludiques, malveillantes, frauduleuses, cupides ou stratégiques.

C'est pourquoi l'autre volet de la SSI, celui du secours aux victimes, c'est-à-dire celui des "cyberpompiers" ou "cybervigies", doit également se développer.

Nous avions pris quelque retard en France sur ce plan. Pendant longtemps, seul le CERT RENATER veillait à la sécurité du réseau et des centres informatiques du ministère de l'Education Nationale et de la Recherche. Puis vint ensuite un centre privé, le CERT IST mis en place par le CNES et quelques grandes sociétés.

En 1999, profitant honteusement de la crainte du bogue de l'an 2000 que certains s'acharnaient à élever au rang de cataclysme mondial programmé, je réussis à faire passer l'idée de la création d'un CERT qui travaillerait au profit de l'Administration dans son ensemble : je fis miroiter que celui-ci pourrait porter assistance aux sinistrés du jour de l'an. Certes, il ne fut d'aucune utilité ce jour-là mais on n'a pas souvent une telle occasion, dans l'Administration, de pouvoir faire débloquer des fonds pour un projet utile dans un laps de temps aussi court !

Aujourd'hui, le CERTA existe et, si j'en crois le rapport du député Bernard Carayon, il rend d'éminents services. A présent, des sociétés se développent autour de prestations du même type au profit des entreprises, je ferai intentionnellement de la publicité à notre voisine, la société AQL, parce que nous sommes partenaires, avec SUPELEC et l'ENSTB, dans le montage du mastère SSI qui se déroule ici et qui connaît un grand succès. Je compte aussi sur le représentant de la DCSSI pour nous faire un point de situation sur la montée en puissance du réseau de confiance qui doit exister au sein de l'Administration.

J'ai parlé de cryptologie et de sécurité informatique et je n'ai encore rien dit de l'**anti-compromission électromagnétique**. Les spécialistes savent qu'il s'agit de la lutte contre le phénomène des signaux parasites émis par nos machines, ordinateurs, imprimantes, téléphones, fax, etc ... et qui peuvent, dans certaines circonstances, se révéler porteurs d'une information confidentielle. Je dirai que cette menace, dans un monde de connexion et de rayonnement volontaire à outrance –le règne du sans fil aussi bien en téléphonie qu'en microinformatique, le WIFI, etc...) apparaît bien secondaire dans les priorités. Il y a tant d'autres méthodes d'attaque plus facile à mettre en œuvre qu'il paraît possible de faire l'impasse sur cette vulnérabilité. Cependant, lorsque toutes les autres portes ont été verrouillées, et si l'enjeu en vaut la peine, ce mode d'action ne doit pas être négligé. On voit des pirates qui se donnent beaucoup de mal pour récupérer le code secret des cartes bancaires par exemple en dissimulant des micro caméras avec des émetteurs dans les distributeurs automatiques de billets. Pourquoi ne chercheraient-ils pas à récupérer ces codes en détectant les parasites émis par le clavier de ceux-ci ? D'ailleurs certaines méthodes d'attaque des cartes utilisant l'analyse de leur consommation électrique peuvent être classées dans ce que, au sein de l'OTAN, on nomme la menace "TEMPEST".

En fait, toutes les méthodes d'attaque physiques et logiques peuvent se combiner et c'est bien pour cela qu'il faut considérer un système dans sa globalité quand on veut le protéger. Je me souviens que M. MORENO, l'un des inventeurs de la carte à puce, était venu me voir début 2000, après avoir lancé de manière médiatique son défi concernant l'invulnérabilité de sa carte. Il offrait un million de francs à celui qui réussirait à percer son secret mais à condition de ne pas utiliser des moyens d'investigation autres que logiques et mathématiques. Comme si un cambrioleur se fixait des règles déontologiques et s'interdisait l'usage du

chalumeau pour ouvrir un coffre ! Or, en moins de cinq minutes, une équipe spécialisée était capable de lire son code ...

Je pense avoir fait un rapide tour du domaine que vous allez continuer à approfondir tout au long de ces trois jours.

Pour ce qui est des enjeux, ce sera plus rapide. Je distinguerai les enjeux pour l'Etat, pour les entreprises et pour les citoyens.

13 Les enjeux pour l'ETAT

Pour un Etat, la maîtrise de l'information conditionne sa liberté d'appréciation des situations et donc sa liberté d'action. Par conséquent, son système d'information, au sens large, ne doit souffrir aucune perturbation, aucune pollution et naturellement aucune intrusion. A contrario, l'Etat doit posséder les moyens de "compléter" son information en empruntant aux autres, en toute discrétion, voire en contrariant, le cas échéant, le système d'information de ses adversaires. C'est donc un devoir pour lui de se mettre en posture d'assurer son **indépendance** et, si possible, sa supériorité dans ce domaine.

Or, aujourd'hui, sommes-nous capables d'assurer notre indépendance en informatique, domaine qui conditionne quasiment tous les autres ? Certes, nous exhibons de superbes engins dans le domaine aéronautique et spatial mais de nombreux composants sensibles intervenant dans leurs systèmes d'identification, de positionnement et de communication, systèmes sans lesquels un aéronef ne peut voler, ne sont-ils pas d'origine étrangère ? Ce besoin d'indépendance technologique doit impérativement être pris en compte si l'on veut parler d'Europe de la Défense.

En outre, le rôle d'un Etat n'est-il pas aussi d'assurer la protection et le bon fonctionnement des infrastructures du pays ? Le bogue de l'an 2000 a été l'occasion de recenser l'ensemble des systèmes critiques. Ce que le bogue n'a pas affecté fort heureusement, ne pourrait-il pas l'être par une bande de hackers résolus. Le Pearl Harbour informatique évoqué aux Etats-Unis bien avant le 11 septembre est toujours d'actualité : pourquoi serions-nous à l'abri d'un "Cyber Waterloo" ou d'un "digital Trafalgar" ?

Enfin et je m'arrêterai là, le rôle de l'Etat n'est-il pas d'assurer la sécurité publique en prévenant ou en permettant de châtier les crimes et délits commis contre ou en utilisant les technologies de l'information ? Après la période d'euphorie qui avait vu les apôtres de la nouvelle économie l'emporter sur les sécuritaires, le balancier s'est un peu inversé. Dans le débat sur la libéralisation de la cryptologie, après avoir été près de tout lâcher, les gouvernements semblent s'être ravisés et tentent de renforcer leur contrôle mais, sauf pour les Etats-Unis, dans de moins bonnes conditions qu'auparavant.

Je ne terminerai pas ce chapitre consacré aux enjeux pour l'Etat, sans rappeler cette citation du général de Gaulle : "*la défense est la raison d'être de l'Etat. Il ne saurait s'y soustraire sans risquer de se détruire lui-même*". Cette défense, qui doit prendre en compte les nouvelles menaces, impose aujourd'hui un effort considérable en faveur de la sécurité des systèmes d'information.

14 Les enjeux pour les entreprises

Pour les entreprises, les enjeux dépendent de leur taille, de leur activité, de leur marché et, bien sûr, de l'âpreté de la concurrence. Lorsqu'un concurrent est capable, pour s'emparer d'un secret de fabrication, de prendre le risque d'une agression physique de grande ampleur avec camion bélier et commando nocturne, il est facile d'imaginer qu'il possède les moyens de se livrer au jeu des intrusions informatiques. Je fais là allusion à un cas réel qui a touché une grande entreprise dont la culture sécuritaire est bien établie. Que penser alors des entreprises qui, soumises à une concurrence comparable, ne subissent pas de telles attaques physiques ? Sont-elles véritablement hermétiques aux attaques informatiques ?

Quoiqu'il en soit, le risque pour une entreprise est évident : il va de la perte d'image, pas forcément agréable en cas de tagage du site Internet de la société, à la perte de marchés, jusqu'à à sa disparition pure et simple. Notons que sans être victime de malveillance, certaines sociétés mettent la clef sous la porte à la suite d'un sinistre informatique. Il y a quelques années, j'avais rédigé un article à la demande du rédacteur en chef de la revue "*Risques*", un magazine des assureurs, dans lequel je préconisais d'instaurer un bonus pour les entreprises utilisant des systèmes d'information sécurisés. J'ai eu le plaisir de voir que cette idée faisait son chemin, mais pas forcément en France.

Pour les entreprises qui travaillent dans les TIC, la sécurité des systèmes d'information est de plus en plus déterminante. La demande est de plus en plus forte et les clients de plus en plus exigeants. Les opérateurs de télécommunication comme les services postaux développent leur offre. La culture sécuritaire commence à se répandre même s'il faut parfois ramener à la raison certains paranos ou rectifier le besoin de sécurité affiché.

Pour les sociétés dont l'activité est la sécurité, parmi lesquelles je place les grands de l'électronique, toute l'industrie de la carte à puce et les sociétés de service ou de conseil, il semble que le marché ait commencé à décoller malgré une conjoncture sinistre pour les TIC. Pour ces sociétés, on peut prévoir encore de belles années compte tenu de la permanence des attaques mais surtout des infections virales qui font de gros dégâts et grèvent lourdement la productivité des systèmes et services informatiques des entreprises. Cependant, il se pourrait que l'activité des petites sociétés traitant de SSI soient progressivement ralenties, si d'aventure, les solutions sécuritaires élaborées par les grands groupes monopolistiques se révélaient finalement efficaces et acceptées par le public.

15 Les enjeux pour le citoyen

Pour le citoyen, l'enjeu est d'abord de pouvoir se servir de son ordinateur sans se soucier perpétuellement de la mise à jour de ses "*patchs*" de sécurité, de ses antivirus, et sans être obligé de faire le tri des messages non sollicités qu'il reçoit. Ensuite, il veut avoir confiance dans les outils de protection que l'on met à sa disposition soit pour envoyer du courrier confidentiel, soit pour sécuriser ses transactions. Enfin, il souhaite protéger un minimum sa vie privée. Or, sur

ce plan, la situation, comme je le disais en introduction, ne s'est pas beaucoup améliorée. Il est vrai que dans le contexte actuel, il est prêt à se laisser violer un peu si, en contre partie, cela lui procure davantage de sécurité pour lui et sa famille.

C'est pour cela que ceux dont la tâche est de veiller au respect de nos libertés individuelles et à la protection des données personnelles doivent se montrer doublement vigilants pour éviter les dérives et les abus. La commission informatique et liberté, la célèbre CNIL, souvent décriée pour les contraintes qu'elle impose à tous les concepteurs de systèmes informatisés, est notre rempart contre ces abus et ces dérives. Son action paraît excessive parfois parce que nous sommes dans une démocratie bien établie. J'ai personnellement toujours la crainte de changement pouvant survenir à la suite d'une grave crise et qui nous replacerait dans une situation telle que celle qu'ont connue nos pères. Je préfère qu'on ne facilite pas trop la tâche à ceux qui n'auraient pas la même conception que nous de la démocratie.

16 Conclusion

En introduction, je vous ai dit mon plaisir de me retrouver parmi vous, les spécialistes de la sécurité des systèmes d'information, dont, malgré mon changement de fonctions, je me sens toujours très proche. A présent je voudrais vous dire ma satisfaction de constater que nous avons cessé de prêcher dans le désert. Certes, une foule de responsables n'a pas encore pris la juste mesure des enjeux de ce domaine en pleine évolution pour ne pas dire en pleine révolution. Et de nombreux problèmes n'ont pas encore reçu de solution. Néanmoins, je perçois comme un frémissement, pour plagier l'un de nos anciens ministres. Certains dirigeants ont saisi que, sans SSI maîtrisée par nous-mêmes, il n'y avait pas de véritable indépendance ni de véritable liberté. Souhaitons qu'ils agissent avant qu'il ne soit trop tard. A vous, chacun à votre niveau et là où vous exercez vos talents, de les convaincre de le faire !