Synthèse du SSTIC 2006v2.1

Note : Ceci est la version allégée de mon compte-rendu, prochainement disponible sur http://bruno.kerouanton.net

Cette année encore le Symposium sur la Sécurité des Technologies de l'Information et de la Communication était d'un excellent niveau avec des présentations de qualité, une très bonne ambiance et l'occasion de se (re)mettre à niveau tout en retrouvant les acteurs majeurs de la sécurité des systèmes d'information en France, du moins sur le plan de l'expertise technique. Mais dans un premier temps, laissons place aux très intéressants exposés non techniques.

Le monde dans dix ans...

La conférence d'ouverture concernait le vaste sujet de la "puissance militaire et modernité au XXIème siècle" et nous a été présenté par le Général Bezacier. Sa grande expérience en matière de forces armées et de conflits contemporains lui a permis de dresser un tableau assez sombre de l'évolution de nos sociétés pour la prochaine décennie.

Notons tout d'abord l'augmentation de la valeur des matières premières et ressources naturelles qui ne sont pas inépuisables, et la diminution de la valeur des prestations intellectuelles due à l'augmentation de la population cultivée et faiblement rémunérée, notamment dans les pays émergents. L'attrait représenté par les pays stables et riches ne pourra que susciter les convoitises et les flux migratoires en provenance de pays défavorisés devront désormais être considérés comme une composante normale.

Ces deux éléments seront forcément source de nombreux conflits car entraînant une nouvelle répartition des richesses, qu'elles soient financières ou sociales. La montée en puissance de la criminalité organisée et la difficulté à maîtriser les flux financiers planétaires sont également source d'inquiétude pour les années à venir. Enfin on constate une implication de plus en plus marquée des populations civiles dans les conflits, et une dimension urbaine qui remet en cause nombre de tactiques des forces armées.

La sécurité depuis dix ans...

Cet exposé illustre parfaitement les différents bouleversements et inversions de rapports de force qui ont déjà commencé à se faire sentir, mais force est de constater qu'en matière de sécurité des systèmes d'information il n'en est rien, et que depuis la dernière décennie plus cela change et plus on en est au même point ! Pierre Vandevenne n'a malheureusement pas pu intervenir, mais son article expose les défaillances de la sécurité des systèmes d'information.

Le discours sécuritaire n'évolue que très peu, les sociétés commerciales proposent toujours plus de produits et solutions en tous genres, les dépenses en matière de sécurité sont de plus en plus importantes, et pourtant on a le ressentiment que l'on est aussi vulnérable qu'il y a dix ans, les utilisateurs notent toujours leurs mots de passe sur un papier collé non loin du PC... dans le cas extrême où le mot de passe en question ne se résume pas à un « coucou », une date d'anniversaire

ou bien encore un prénom familier.

Les mêmes failles ressurgissent, et les bonnes vieilles méthodes d'attaque ne sont pas reléguées au placard, faute d'avoir pu convaincre les éditeurs de logiciels de prendre la sécurité un peu au sérieux, et certains professionnels de la sécurité d'avoir crié un peu trop souvent au loup dans l'espoir d'attirer l'attention (et le porte monnaie) sur eux.

Le patrimoine immatériel

Dans le même ordre d'idées, M. Santoni de la société de conseil en gestion des risques Marsh nous a expliqué comment depuis les dix dernières années les assureurs tentaient de définir les risques en vue d'une éventuelle indemnisation en cas de sinistre.

Au début, on indemnisait le matériel qui en effet représentait un investissement conséquent, et dont la valeur était très facilement chiffrable par le biais des différentes factures. Puis peu à peu la prise de conscience collective que cela ne suffisait pas, a entraîné les assureurs à se pencher vers les sauvegardes et la reconstitution des données en cas de problème. Indemnisation rarement effectuée car quand les sauvegardes fonctionnaient il n'y avait pas lieu d'indemniser, et quand la restauration n'était pas possible la police d'assurance ne couvrait pas ce risque !

Néanmoins il est devenu nécessaire de trouver une solution à cet épineux problème, et semble t-il qu'une ébauche de solution est désormais utilisée. Puisque la valeur intrinsèque correspond au patrimoine informationnel, il faut d'une part identifier et qualifier ses composantes, d'autre part identifier les flux de ces mêmes données et par corolaire les acteurs concernés, et enfin tenter de garantir l'ininterruptibilité et l'intégrité de ces flux et données par le biais de plans de continuité d'activité soigneusement conçus.

En synthèse, il est intéressant de constater que le patrimoine informationnel est si difficile à quantifier en termes de valeur éventuellement indemnisable en cas de sinistre, que la meilleure solution est de ne pas avoir de sinistre... en investissant sur tout moyen permettant à l'entreprise de garantir la continuité d'activité.

Tous en prison ?

Se pose alors la question de la responsabilité des dirigeants, responsables informatiques et responsables sécurité face à des sinistres ou malveillance. La juriste Marie Barel nous à exposé dans les grandes lignes quelle était la conduite à tenir lorsque l'on est confronté à certains problèmes courants.

Tout d'abord, il faut savoir que la responsabilité pénale qui est susceptible de hanter nos nuits n'est pas toujours applicable. Il faut en effet que la délégation de pouvoir soit effective, et que nous ayons à cet effet des capacités réelles en termes d'autorité hiérarchique, de compétences et de moyens permettant de réaliser la mission. De plus, cette délégation et l'étendue de la mission doivent avoir été préalablement précisées et ne doivent pas avoir un caractère temporaire.

Ces éléments acquis, nous pouvons nous aventurer dans les différents méandres du droit civil et pénal en prenant quelques exemples : En cas de défaut de sécurisation des données à caractère personnelles le cadre réglementaire est clair, le responsable sera coupable ! Le cas du spam est intéressant car il est souvent effectué par l'utilisation de machines attaquées et servant de relais (attaques par rebond). Dans ce cas précis, nous sommes en mesure de nous interroger quant à

responsabilité d'une personne ayant laissé sa machine devenir un relais.

Bien que la loi Godfrain sanctionne toute intrusion dans un système, et que le désormais connu article 323-3-1 du code pénal sanctionne toute détention d'outils ou données permettant de commettre de telles infractions, force est de constater qu'il sera bien difficile au législateur d'incriminer toute victime de spam dont la machine aurait ensuite servi de relais d'attaque. Néanmoins il semble que le législateur soit moins clément envers les responsables dont le comportement en matière de sécurité semble laxiste, et il conviendra par conséquent au responsable de faire preuve de rigueur afin de maintenir la sécurité de ses systèmes d'information à niveau.

De même, le responsable devra rester vigilant face aux actions de ses salariés, notamment lors de l'absence d'une charte informatique précise, car il est responsable civilement et pénalement de leurs agissements par exemple en cas de création d'un blog à caractère diffamatoire réalisé dans l'entreprise avec les moyens de l'entreprise.

On en vient alors tout naturellement à la cyber surveillance et au contrôle de la messagerie électronique... un flou encore présent tant dans les esprits que dans la législation, puisqu'au final seul le juge sera à même d'apprécier de manière souveraine la légalité ou non des actions mises en œuvre par les administrateurs de la messagerie ou des réseaux. Prudence donc...

Ces trois jours étant comme d'habitude fort denses en enseignements, et comme je ne souhaite pas vous égarer dans les nombreuses méandres techniques dont faisaient état la plupart des présentations, je vous livrerai donc ici un condensé de ces exposé en les groupant un peu et en tirant de grandes tendances, le lecteur intéressé pourra de toute manière se référer au compte-rendu détaillé, voire mieux encore aux actes de conférence du symposium.

Le graal de la connectivité permanente

Le SSTIC étant pour partie à connotation universitaire/recherche, de nombreux sujets en cours d'étude ont été présentés, tels que l'utilisation de réseaux neuronaux pour rendre plus fiable les prises d'empreintes de machines (également désigné sous le terme anglo-saxon « OS fingerprinting »), un aperçu des méthodes de sécurisation des consoles de jeu et des mécanismes de contournement associés, la description des mécanismes sous-jacents permettant de sécuriser un réseau de systèmes mobiles (« roaming ») basés sur le protocole Ipv6, la détection d'intrusions dans les réseaux 802.11, l'application de la théorie des jeux et de l'évolution dans le cadre d'observabilité imparfaite pour la coopération dans les réseaux ad hoc (!), ou bien encore l'étude de la sécurité des flux multimédia sur réseaux hétérogènes, notamment à destination des téléphones mobiles et ordinateurs de poche.

Outre l'intérêt suscité par le côté technique et novateur de ces travaux de recherche, il est important de constater que l'on tend progressivement vers une utilisation de systèmes mobiles (téléphonie, ordinateurs de poche ou reliés par radio), connectés en permanence au réseau Internet, ayant une capacité à s'auto-gérer vis-à-vis des différentes contraintes extérieures (adaptation du terminal en fonction de la nature du réseau et des autres terminaux présents), et possédant une connectivité lui offrant une capacité de transfert haut débit. Clairement, on voit que la recherche tente de trouver les mécanismes et solutions permettant à un individu de rester connecter en permanence, de manière fiable et sécurisée.

Cette symbiose et les risques inhérents sont mis en exergue de manière remarquable dans l'exposé de Gildas Avoine, qui nous fait part de ses inquiétudes face à l'introduction presque incontrôlée des technologies d'identification radio (RFID) dans une bonne partie de notre quotidien. Après un bref rappel de ces différentes technologies et champs d'application, il nous présente certaines attaques possibles avant de nous faire partager quelques extraits vidéos montrant comment utiliser de telles failles pour faire démarrer des véhicules sans posséder la clef, voire pour faire le plein d'essence sans débourser un sou... le tout grâce aux RFID. Plus inquiétant encore, Gildas Avoine nous présente quelques scénarios dignes de Georges Orwell, dans le cas où nous aurions des dizaines de puces électroniques activables à distance sur nous, ce qui risque d'arriver plus vite qu'on n'oserait l'imaginer.

De même, la généralisation des boîtiers ADSL dans les foyers semble anodine, mais cela pourrait entraîner certaines dérives, surtout si des personnes malveillantes en prenaient le contrôle, comme l'explique très concrètement Nicolas Ruff qui a réalisé durant deux années une étude aux conclusions peu réjouissantes sur cet aspect.

Téléphonie gratuite, téléphonie magique ?

Et comme ces boîtiers intègrent de plus en plus des fonctions de téléphonie, il est temps de parler du très répandu logiciel de téléphonie (presque) gratuite utilisant le réseau Internet. Comme certains le savent déjà peut-être, un petit groupe de chercheurs d'élite travaillant au sein du centre de recherches d'EADS a mené une étude approfondie du logiciel Skype, et notamment des nombreux mécanismes mis en œuvre par les concepteurs.

Le premier constat est que ceux-ci ont particulièrement soigné les contremesures permettant d'éloigner les curieux, ce qui a valu à notre vaillante équipe un travail acharné plusieurs mois durant afin de disséquer la bête. Outre l'utilisation massive de techniques sophistiquées anti-désassemblage et anti-déboguage afin de décourager la rétroconception et dignes d'être retrouvées dans les plus sophistiqués des virus et chevaux de Troie, le logiciel est également muni d'un ensemble de protocoles réseaux lui permettant de camoufler l'ensemble des données échangées avec ses pairs, tout en utilisant des techniques sophistiquées de contournement des pare-feux et de dissimulation du trafic téléphonique au sein du trafic légitime de l'entreprise.

Il s'agit par conséquent d'un logiciel très sophistiqué mais dont les concepteurs ont souhaité obscurcir un certain nombre de fonctions… pour y insérer des portes dérobées, me direz-vous ? A priori il est difficile d'établir des conclusions à ce sujet car tous les mystères du logiciel n'ont pas encore été mis à jour, mais il est certain que sur le plan stratégique, tout le « business-model » de l'entreprise Skype repose sur la capacité à maintenir un contrôle total de son logiciel et des flux de communications associées, ce qui peut expliquer cet acharnement à décourager les curieux. La gratuité de l'utilisation du système n'est que toute relative, puisqu'elle ne concerne que les appels entre utilisateurs de Skype, et les effets provoqués par un second réseau Skype incontrôlé seraient désastreux, tant par les risques de détournement des communications, que par le manque à gagner de la société qui verrait une solution concurrente éventuellement gratuite et ouverte s'interfaçer à son propre réseau.

Car si la téléphonie sur IP semble gratuite, il faut bien que les investissements et les frais de fonctionnement soient rentabilisés… et si l'on y réfléchit un peu c'est parce que Skype, en utilisant la technologie du peer-to-peer et donc le partage forcé de nos ressources informatiques, permet la gratuité… Du coup, la prochaine fois que vous démarrerez un tel logiciel sur votre ordinateur sans vous en servir, je vous invite à surveiller l'activité de celui-ci… vous serez surpris !

Chassez le naturel, il revient au galop

Parmi les inquiétudes revenant régulièrement dans les esprits non initiés, on note souvent les virus et le spam. Mais ce qui nous a marqués en tant que professionnels de la sécurité, c'est que de nombreux exposés faisaient état d'anciennes techniques d'attaque, du moins dans les grands principes même si techniquement les solutions semblaient plus novatrices. Ainsi, et ce plus de deux années après la grande vague des virus Sasser et Blaster qui ont défrayé la chronique, le protocole RPC a fait parler de lui lors de deux exposés, le premier par Renaud Bidou qui expliquait comment s'en servir pour traverser différentes marques de pare-feux et d'outils de détection d'intrusion sans inquiétude, et le second par Nicolas Pouvesle qui, tout en expliquant les grands principes de ce protocole complexe, tirait à boulets rouges sur la plupart des éditeurs de solutions informatiques qui n'ont toujours pas corrigé leurs applications malgré ces fameuses vagues de virus...

De même, lors des Rump-sessions, qui sont de petites présentations, de nombreux thèmes récurrents ont été exposés : la résurgence des macro-virus sous OpenOffice, certains problèmes liés aux réseaux Wi-Fi, le vol (automatisé !) de données présentes sur les clefs USB, les différents problèmes liés à la crédulité des utilisateurs et à l'ingénierie sociale, les problèmes de corruption des postes utilisateur, et même un débat relatif à la grande quantité de réseaux sécurisés chiffrés IPSEC qui sont mal implémentés ou configurés par des concepteurs et des administrateurs trop confiants ou perdus par la complexité de la chose, rendant du coup ces réseaux vulnérables malgré les budgets et les efforts consentis.

Hacker vaillant rien d'impossible

Un certain nombre d'exposés très techniques nous ont démontré qu'à attaquant motivé les chances de réussir une attaque bien ciblée et préparée à l'avance étaient assez importantes. Ainsi, une équipe de la DCSSI a exposé deux méthodes permettant à un attaquant d'accroître ses privilèges sur une machine, en détournant judicieusement certaines des fonctionnalités matérielles présentes en standard sur les processeurs et circuits présents sur les cartes mères. Samuel Dralet et François Gaspard ont mis au point des techniques permettant d'attaquer un système en n'utilisant que sa mémoire vive, garantissant ainsi que le disque dur ne sera pas affecté et qu'il n'y aura par conséquent aucune trace de l'attaque laissée à disposition d'un éventuel enquêteur. De même Nicolas Bareil utilisera certaines fonctions méconnues du système d'exploitation pour effectuer des attaques.

Quand le ver est dans le fruit...

On voit par ces exposés que le problème majeur est dû à l'historique de nos systèmes, qui de version en évolution doivent pouvoir assurer une certaine compatibilité avec nos vielles applications, et par conséquent conservent également un certain nombre de failles. Charge aux concepteurs de ces systèmes d'exploitation de trouver des parades pour concilier compatibilité et sécurité, ce que Microsoft a fait, compte-tenu de leur souci constant d'amélioration de leur mauvaise image en matière de sécurité.

Ainsi, la prochaine version du système d'exploitation de Microsoft, Vista, comporte un certain nombre d'améliorations. Le mécanisme ASLR est par exemple destiné à empêcher les attaques par injection de code, puisque les programmes se trouveront désormais chargés en mémoire à des

adresses déterminées aléatoirement. Malheureusement Nicolas Pouvesle nous explique que malgré l'originalité de ce concept, il risque d'y avoir des attaques malgré tout, car l'implémentation est insuffisante.

Mais Microsoft a d'autres tours dans son sac car un mécanisme de contrôle de tout ce qui est fait sur le PC est prévu (dans les versions haut de gamme) de Vista. Le mécanisme BitLocker est un dérivé revu et corrigé du très controversé Tcpa/Palladium, qui permet à la fois le chiffrement de l'ensemble du disque dur et le contrôle de toute la chaîne de démarrage en allant du BIOS jusqu'à Windows, et en y incluant si besoin est les applications lancées par la suite. Le tout reposant sur un composant réputé inviolable soudé sur la carte mère de l'ordinateur. L'avenir nous dira si cette solution est ou non efficace.

Conclusion : Plus cela change…

En conclusion, je me permets de paraphraser Pierre Vandevenne car ses remarques sont fort justes. J'en discutais il y a une semaine lors de la rencontre annuelle Netfocus ou les Responsables sécurité de grands groupes se rencontrent à leur tour pour exposer leur vision organisationnelle de la sécurité… et piteusement nous étions en train d'avouer que depuis quelques années déjà les mêmes thèmes revenaient, comme si il n'y avait pas eu d'idées géniales depuis les années précédentes, ou comme si ne rien changeait dans notre petit monde de la sécurité.

A croire qu'il n'existe aucune solution efficace, ou plus précisément qu'il n'y a pas eu de rupture technologique depuis un certain temps, dans le domaine. Et force est de constater que finalement, Linux et les autres Unix datent de plusieurs dizaines d'années, idem pour les réseaux informatiques, idem pour les langages de programmation couramment utilisés, et que la seule véritable évolution majeure de la part de Microsoft remonte à Windows NT4. Ce qui explique pourquoi d'une année sur l'autre, on nous repasse une couche supplémentaire de correctifs bien ressemblant à ceux déjà appliqués, pour corriger les « nouvelles » failles qui en fait n'en sont pas, et qu'on nous vend des produits qui ne sont rien de plus que des évolutions sans prétention de concepts imaginés il y a une bonne quinzaine d'années…

Ces propos certainement agaçants pour certains étant désormais écrits, je reviens au SSTIC, et comme chaque année je peux peut affirmer haut et fort qu'il s'agit de la meilleure conférence française en sécurité informatique, car on y apprend beaucoup sans avoir à se déplacer à Las Vegas, à Toronto ou à Amsterdam, tout en y rencontrant des experts réputés et sympathiques, dans une ambiance cordiale (voire festive une fois le soir venu). Vivement l'année prochaine…

Références et liens intéressants :

Le site officiel du SSTIC : http//www.sstic.org

Quelques impressions à chaud livrées par des habitué(e)s du SSTIC :

http://teh-win.blogspot.com/2006/06/sstic-06-ca-dnonce.html

http://nonop.blogspot.com/2006/06/sstic-compte-rendu-22.html

http://sid.rstack.org/blog/index.php/2006/06/04/91-sstic-2006-compte-rendu-et-impressions