SÉCURITÉ INFORMATIQUE
numéro 51 décembre 2004
SÉCURITÉ DES SYSTÈMES D'INFORMATION

éditorial

Le nomadisme en question

Ce numéro 51 propose une réflexion sur les dangers de l'informatique nomade. Le thème qu'aborde Marie-Claude Quidoz ne se limite pas à la question de la sécurité du Wi-Fi, sa vue est plus générale : des machines administrées par leurs utilisateurs, donc souvent mal configurées, pouvant se connecter n'importe où, donc sur des réseaux « non sûrs », représentent un risque pour l'informatique interne en l'absence de règles particulières et d'architectures adaptées. Mais n'est-ce pas imposer encore aux utilisateurs des contraintes qui risquent à la longue de devenir insupportables ? Marie-Claude Quidoz nous propose d'explorer quelques pistes.

Ce numéro est le dernier dont j'assume la responsabilité, je change en effet de fonction au début de l'année 2005. Je voudrais profiter de cette occasion pour vous remercier, vous lecteur de *Sécurité informatique*, de votre fidélité – de longue date pour certains d'entre vous – qui s'est manifestée plus particulièrement lors de l'enquête que nous avons organisée au printemps dernier. Vos réponses nous ont permis d'améliorer ce bulletin, vos encouragements, nombreux, de nous rassurer sur son utilité. *Sécurité informatique* a été créé en 1994 par mon prédécesseur, Michel Dreyfus. C'était un bulletin interne, orienté plus particulièrement vers la sécurité des micro-ordinateurs sur lesquels semblaient planer des menaces graves du fait de leur prolifération désordonnée. Dès 1997, avec le soutien de la Direction du CNRS et plus particulièrement du FSD de l'époque, Philippe Schreiber, nous avons décidé d'ouvrir plus largement nos colonnes à des auteurs extérieurs au CNRS et d'offrir une version électronique en téléchargement libre. Aujourd'hui, la diffusion au format PDF dépasse largement les 40 000 exemplaires et touche l'ensemble de l'espace francophone. Tous les grands ministères et de nombreuses entreprises, parmi les plus prestigieuses, sont abonnés au bulletin. Certains des articles ont été cités dans la presse. En définitive, l'ouverture n'a présenté que des avantages. Elle a permis de sensibiliser à la SSI un public plus large que notre organisme et donc de remplir notre mission de diffusion de l'information scientifique et technique. En retour, nous avons beaucoup reçu : l'ouverture nous a permis d'évaluer la pertinence de nos conceptions, de tirer profit des autres expériences, d'accepter la confrontation de points de vue, de ne pas nous laisser enfermer dans une conception purement technique de la SSI (celle qui dérange le moins !).

Sécurité informatique continuera et évoluera encore. Faudrait-il plus de pages ? Peut-être, mais plus long à lire, il ne toucherait plus le « public des décideurs », celui que nous voulons intéresser à la SSI. Faudrait-il plus d'articles de fond ou plutôt plus de brèves ? Notre objectif est avant tout de tracer des pistes de réflexion, de donner des références auxquelles tout le monde peut se reporter. Faudrait-il augmenter la fréquence de parution ou la diminuer ? Cinq numéros par an nous semblent être la périodicité qui permet d'aborder les sujets importants de l'année sans prendre le risque de trop rabâcher. Bref, tout peut être repensé, mais une chose est à préserver absolument, c'est cette ouverture à l'extérieur du CNRS qui a été si profitable pour nous tous.

Robert Longeon
Chargé de mission SSI au CNRS

L'accueil des portables sur nos réseaux informatiques

par Marie-Claude Quidoz
Ingénieur à l'unité réseau du CNRS

Le but de cet article n'est pas de définir une politique d'accueil des portables sur nos réseaux informatiques (faut-il les interdire, les autoriser, limiter leur droit d'accès ?), mais de présenter des pistes de réflexion pour qu'à terme cet accueil soit moins problématique. Il s'appuie sur des recherches bibliographiques, des retours d'expériences et sur l'article* Strategies for Automating Network Policy Enforcement *dans lequel les auteurs citent des scénarios intéressants pour détecter les portables qui ne respectent pas la politique de sécurité définie par l'organisme et pour se protéger des nuisances qu'ils peuvent occasionner.

Contexte

Depuis quelques années, un élément « perturbateur » a été introduit dans nos réseaux informatiques : le portable (principal équipement nomade pour nous). Cet équipement ne soulève pas de nouveaux problèmes mais remet à l'ordre du jour des problèmes anciens, comme le fait que l'utilisateur dispose du droit d'administrer sa machine, ce droit pouvant être utilisé à bon ou à mauvais escient. Cette situation n'est pas nouvelle en soi (de nombreux utilisateurs administrent déjà leur poste de travail), mais à la différence des postes fixes qui sont en permanence à l'intérieur du périmètre de sécurité défini par l'administrateur système et réseau du laboratoire, ces portables sont amenés à se connecter un jour ou l'autre dans un environnement hostile et si des précautions minutieuses ne sont pas prises, ces portables peuvent se retrouver infectés et ainsi devenir vecteur d'infection. La situation peut devenir problématique le jour où la machine vient se connecter au réseau du laboratoire, que la connexion soit locale (accès filaire ou accès sans fil) ou à distance.

Par conséquent c'est le fait de naviguer entre deux environnements (l'un supposé « sain » et *suite page 2*

CNRS CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

suite de la page 1

l'autre supposé «hostile») qui est devenu la principale cause des problèmes posés par les portables. Problèmes que l'on rencontre, de façon plus générale, dans l'accueil des machines extérieures (que ce soit un portable ou un poste fixe situé hors du périmètre de sécurité) qui ont besoin d'accéder à la totalité de leur environnement de travail. À noter que dans cet article, nous restreindrons volontairement notre discours au portable afin d'en simplifier la lecture.

Des règles de sécurité existent

Des conseils sont régulièrement diffusés par les CERTs ou par les équipes en charge de la sécurité du CNRS en direction des correspondants sécurité de chaque laboratoire, à charge pour eux de les relayer vers les utilisateurs finaux. Ces conseils génériques qui à terme seront partie intégrante de la politique de sécurité du système d'information (PSSI) du laboratoire et de ses règles d'application sont de plusieurs types : éducation de l'utilisateur (ne pas cliquer sur des éléments inconnus…), sensibilisation au danger (ne pas transformer son portable en un serveur…), incitation forte à la mise à jour du système d'exploitation et des logiciels, installation de produits de protection (garde-barrière personnel, antivirus…).

Mais…

Il est utopique de penser que tous ces conseils seront suivis à la lettre tant le nombre de vulnérabilités annoncées chaque jour augmente. Il devient de plus en plus difficile de maintenir sa machine à jour, surtout si on est un nomade qui ne se connecte que ponctuellement au réseau Internet. En dehors du réseau d'accueil habituel de la machine, il est parfois difficile, faute de temps ou à cause de contraintes imposées par la politique de sécurité du site d'accueil de mettre à jour sa machine et cela même si on dispose d'un accès de bonne qualité au réseau Internet. Force est donc de constater qu'un jour ou l'autre, notre portable sera infecté.
Ce constat conduit l'administrateur système et réseau à ne pas laisser les portables se connecter n'importe où (il faut définir une architecture réseau) et l'incite à vouloir vérifier leur état avant (ou lors de) leur connexion :

Architecture sécurisée

Depuis la multiplication des portables dans notre environnement, nous avons essayé de classifier leur utilisation pour tenter ensuite de les intégrer au mieux à l'architecture sécurisée mise en place au sein du laboratoire. La démarche a consisté à définir deux façons d'utiliser un portable : soit occasionnellement en cas de déplacement, soit quotidiennement en remplacement d'un poste fixe. Ensuite, et presque indépendamment de cette classification, une réponse unique a été apportée : la mise en place d'un sous-réseau «visiteur» qui, grâce à des filtres définis avec minutie, permet un accès au réseau Internet mais pas au réseau local (éventuellement à une imprimante locale). Si nécessaire, on peut également autoriser l'utilisateur à rapatrier ses fichiers depuis le réseau interne (et inversement).

Qualité du poste

En imposant ainsi un sous-réseau «visiteur» à un utilisateur dont le portable est l'outil de travail quotidien, nous faisons plus ou moins implicitement l'hypothèse que cet équipement est hostile. Cette hypothèse a été traduite par certains en «le poste ne respecte pas la politique de sécurité définie», ce qui sous-entend que le respect de la politique de sécurité définie pour un poste client est suffisant pour éviter toute infection, ce qui sous-entend aussi qu'une politique de sécurité doit être traduite par un ensemble de règles applicables et à appliquer.
Même si ces affirmations semblent un peu excessives, cette façon d'envisager le problème nous donne des éléments de réflexion pour définir les vérifications à faire avant de laisser un ordinateur se connecter au réseau du laboratoire. Parmi ces vérifications, nous pouvons citer la vérification des correctifs installés, la présence suite page 3

■ Que peut-on trouver dans une PSSI «Politique de Sécurité des Systèmes d'Information» concernant «l'accueil des portables sur nos réseaux informatiques» ?

La PSSI, qui décrit les éléments stratégiques (enjeux, référentiel, principaux besoins de sécurité et menaces) et les règles de sécurité applicables à la protection du système d'information d'un organisme, précise entre autres les principes et les règles concernant la **Connexion des postes nomades et PDA**
Principes :
Une attention particulière doit être portée aux équipements nomades et PDA pour éviter, notamment, de servir de passerelle vis-à-vis de l'extérieur, de contaminer l'intérieur par des logiciels malveillants. D'une manière générale, leur connexion au SI ne doit pas modifier ou remettre en cause la sécurité du SI.
Règles :
Pour mesurer au mieux l'impact de l'intégration des postes nomades dans le SI, il est nécessaire de prendre en compte toutes les informations, les conseils et les recommandations fournis sur les sites :
http://www.urec.cnrs.fr/sans-fil/index.html
http://www.cru.fr/wl/
http://www.cru.fr/nomadisme-sans-fil/
La recommandation relative à la question «Vos utilisateurs possèdent-ils des portables ?» du chapitre II de la liste de contrôles accessible à la rubrique Liste_de_contrôles de l'URL :
https://www.urec.cnrs.fr/securite/corres-secu doit être mise en œuvre.
Au sein de la PSSI, on retrouve également cette intégration mentionnée dans les principes et les règles définis pour l'**Architecture sécurisée**.
Principes :
Les accès modems, les accès distants, les réseaux privés virtuels et les réseaux sans fil sont à intégrer. Pour le réseau sans fil, il faut veiller à son intégration : choix d'un protocole comme ceux décrits dans 802.11i ou accès par VPN,
Règles :
Se reporter aux informations données à :
http://www.urec.cnrs.fr/sans-fil/index.html

Informations fournies par le groupe de travail CAPSEC

suite de la page 2

d'un antivirus et la vérification de sa base de signature, la présence d'un garde-barrière, la liste des ports ouverts… À noter que cette référence à la politique de sécurité définie au sein de l'organisme et/ou du laboratoire et à son respect, a aussi l'avantage, en rendant plus concrète son application, de sensibiliser l'utilisateur à la notion même de politique de sécurité.

Autorisation d'accès et charte

En pratique, la majorité des vérifications à faire sur le portable qui se connecte au réseau du laboratoire nécessitent de disposer d'un droit d'accès sur le portable ; par exemple pour rechercher la présence de tel ou tel fichier (pour vérifier l'installation d'un antivirus ou l'absence de virus/ver/trojan), pour connaître le numéro de version de la base de signature de l'antivirus, pour diagnostiquer la présence de programmes en mémoire (pour savoir si l'antivirus est lancé)… À terme, c'est la totalité des vérifications qui risquent de nécessiter un droit d'accès ; en effet, si actuellement nous pouvons encore imaginer vérifier *via* le réseau les services offerts (donc les ports ouverts) sur un poste de travail pour rechercher des indices nous permettant d'établir un indicateur de l'état de santé de la machine, cela ne sera sans doute plus possible quand, sur tous les postes de travail, nous aurons activé des gardes-barrières individuels.

Ce problème de droit d'accès est ancien mais il n'a jamais été véritablement résolu. Les arguments sont connus (portable personnel versus portable professionnel, protection de la vie privée…) et recevables, mais sont-ils acceptables pour autant à partir du moment où l'utilisateur souhaite connecter son portable directement sur le sous-réseau interne et non sur le sous-réseau « visiteurs » ? Une analogie est souvent faite avec la voiture où il y a un code de la route à respecter, des normes de pollution à ne pas dépasser… et si on ne les respecte pas, le droit d'utiliser la route nous est retiré. La charte peut permettre de répondre à cette question de façon claire. Dans la charte du CNRS publiée en 1999, rien n'est indiqué à ce sujet, mais tout laisse à penser que, dans la prochaine version, des instructions plus précises seront données.

Des solutions commencent à voir le jour

Suite aux nombreux incidents provoqués par les virus depuis plus d'un an et presque indépendamment de la problématique des portables, des travaux ont vu le jour pour essayer d'automatiser d'une part la détection des postes qui ne respectent pas la politique de sécurité et d'autre part la réponse à donner. Une bonne synthèse des problèmes soulevés est disponible dans l'article Strategies for Automating Network Policy Enforcement ; article dans lequel les auteurs décrivent quatre étapes à réaliser lors de la connexion au réseau interne :
- Authentification ;
- Détection ;
- Isolation ;
- Mise en conformité.

À noter que les auteurs n'imposent pas vraiment d'ordre (même si l'article est construit sur cette trame) ; le but étant qu'à la fin du cycle, la machine soit « saine ».
Cette démarche en quatre phases doit être adaptée pour nos nomades. D'une part, il est peu envisageable que les contraintes à faire respecter aux visiteurs (voulant seulement consulter leur messagerie par exemple) soient les mêmes que celles imposées à un personnel permanent qui souhaite utiliser son portable comme si c'était son poste de travail quotidien. D'autre part, il faut envisager le cas où l'utilisateur ne peut pas mettre à jour son portable (à titre d'exemple, vous pouvez vous référer aux nombreux articles parus lors de la sortie du Service Pack 2 pour Windows XP !).
Pour toutes ces raisons, suite page 4

■ Une solution pour maintenir un parc informatique Windows à jour

Si vous avez un environnement tout Windows, si vos utilisateurs se connectent de façon régulière sur votre réseau et s'ils vous donnent l'autorisation de mettre à jour automatiquement leur portable, une bonne solution est de déployer une architecture à base de serveur SUS (Software Update Services) pour le déploiement des mises à jour du système d'exploitation, de serveur EPO (EPolicy Orchestrator) pour le déploiement des stratégies de sécurité (antivirus, garde-barrière) et de domaine Active Directory. Vos portables seront ainsi mis à jour régulièrement et les intrus éventuels seront facilement détectés. ■

■ Détection de machines vulnérables sans faire appel à un agent et en s'appuyant sur des logiciels libres

Deux méthodes : une active et une passive.

Méthode active :
Cette méthode permet de détecter un problème sur une machine en scannant ses ports ; le scan pouvant être fait lors de sa connexion ou de façon périodique (en scannant régulièrement le réseau d'accueil des nomades par exemple). Le but est de faire un état des lieux de la machine pour connaître le système d'exploitation installé et les ports ouverts. Ces derniers nous permettront de détecter une éventuelle trappe (backdoor) et ainsi de déterminer si la machine est saine ou non. La limite de cette méthode intervient lorsqu'un garde-barrière personnel est installé sur la machine car ce dernier nous enlève, dans la plupart des cas, toute visibilité sur les informations demandées.
Les outils testés à l'UREC pour cette méthode sont Nessus et Nmap.

Méthode passive :
Cette méthode permet de détecter une machine compromise en écoutant, en temps réel, le trafic réseau à la recherche d'un trafic caractéristique (nombreux scans dans un court laps de temps, trafic de déni de service, exploit…). Suite à cette détection, une réponse, manuelle ou automatique, peut être mise en place. Mais attention au risque important de déni de service en cas de faux positifs. À noter que cette méthode peut être complétée par une analyse de fichiers de trace et/ou par la mise en place d'outil de métrologie.
L'outil testé à l'UREC pour cette méthode est Snort. ■

suite de la page 3

la logique suivante nous semble devoir être privilégiée :
1. Obliger le portable à se connecter à un sous-réseau étanche et clos
2. Authentifier l'utilisateur et/ou le portable
3. Tester la conformité du portable par rapport au profil déterminé
4. Basculer le portable dans le bon sous-réseau.

À noter que la mise en place de la phase d'isolation d'une machine va dépendre de l'architecture réseau existante (concentrateur VPN/IPSec et/ou VPN/SSL, 802.1x, portail captif…).

Conclusion

De nombreux points restent à approfondir dans ce domaine en pleine évolution. Actuellement, des développements sont en cours aussi bien dans le monde des logiciels libres que dans celui des logiciels commerciaux ; cette confrontation des deux mondes ne pouvant être que bénéfique pour nous.

Des solutions commencent à voir le jour pour faciliter l'intégration des portables dans nos réseaux informatiques ; il est nécessaire de démarrer l'étude de leur mise en œuvre. Cependant il faut prendre conscience que pour résoudre les problèmes de l'accueil des portables sur nos réseaux informatiques, les réponses techniques ne sont (et ne seront) d'aucune aide si en parallèle les problèmes politiques ne sont pas résolus ; une attention toute particulière doit être apportée à la mise en œuvre d'une politique de sécurité du système d'information et à la formation/sensibilisation de l'utilisateur, maillon important de la sécurité.

marie-claude.quidoz@urec.cnrs.fr

■ Utiliser un réseau sans fil introduit-il des contraintes supplémentaires ?

Si nous faisons l'hypothèse que les deux vulnérabilités principales du sans fil (l'écoute et les connexions illicites) sont résolues, utiliser un réseau sans fil pour se connecter sur nos réseaux informatiques n'introduit pas de contraintes supplémentaires ; la mise en œuvre des solutions présentées pourrait même s'avérer plus facile à réaliser.
D'une part, comme il s'agit de réseaux à l'état de projet et/ou de construction, l'ajout d'un sous-réseau étanche et clos dans l'architecture peut être envisagé dès le début du projet. Étant donné aussi que les utilisateurs n'ont pas encore acquis trop d'habitudes, changer la méthode de connexion posera peu voire pas de problème. Et, dernier élément positif, les besoins des utilisateurs du sans fil sont, encore à ce jour, identiques à ceux décrits pour les accès distants ; le sans fil ne remplaçant pas encore le filaire.
D'autre part, des solutions techniques intéressantes pour isoler, détecter, protéger les postes clients… voient le jour ; citons le cas des commutateurs Wifi qui permettent une administration centralisée du réseau sans fil, mais qui intègrent aussi des mécanismes pour interdire la communication entre clients du réseau, des systèmes de détection d'intrusion, des mécanismes de filtrage… Ce type de solution est à considérer dans le cadre d'un projet de taille importante. ■

■ Principe de fonctionnement avec agent (exemple de CleanMachines) (http://www.perfigo.com/products/index.html)

Ce schéma, extrait des informations disponibles sur le site Web, est une bonne illustration de la logique de fonctionnement de ce type de produit (isolation, prise en compte de plusieurs profils de population…) sachant que la vérification de la bonne santé du poste est basée, dans le cas de ce produit, sur un agent installé sur chaque poste.
1. L'utilisateur connecte sa machine au réseau.
2. CleanMachines essaie d'authentifier l'utilisateur. S'il est connu, il détermine son rôle et la politique de sécurité à lui appliquer.
3. La machine est alors analysée pour déterminer sa conformité avec la politique de sécurité à lui appliquer.
4. Si des vulnérabilités sont trouvées, la machine est isolée du réseau (quarantaine) avec un accès uniquement aux fichiers de mises à jour/correctifs et outils nécessaires à sa mise en conformité.
5. La machine est nettoyée puis réanalysée.
6. Une fois sa machine rendue conforme à la politique de sécurité définie, l'utilisateur a accès au réseau. ■

■ Bibliographie/Références

- Epolicy Orchestrator (McAfee) : antivirus retenu par le groupe logiciel dans le cadre de l'opération nationale https://www.services.cnrs.fr/Logiciels/breves.html
- Software Update Services – Microsoft – produit gratuit permettant de faire du déploiement centralisé de correctif
  http://www.crhea.cnrs.fr/crhea/cours/Software%20Update%20Services.pdf
  http://www.crhea.cnrs.fr/crhea/cours/Maj%20Windows%20par%20GPO.pdf
- Nessus 2.2.0RC1 : http://www.nessus.org/
- Clean Machine (Perfigo) : http://www.perfigo.com/products/index.html
- Network Admission Control (Cisco) :
  http://www.cisco.com/en/US/netsol/ns466/networking_solutions_white_paper0900aecd800fdd66.shtml
- Network Access Protection (Microsoft) : http://www.microsoft.com/windowsserver2003/technologies/networking/nap/default.mspx
- Jedi (Juniper) : http://www.nwfusion.com/newsletters/vpn/2004/0830vpn2.html
- Strategies for Automating Network Policy Enforcement (DRAFT 02), Eric Gauthier et Phil Rodrigues, août 2004, Internet2 (http://security.internet2.edu/netauth/docs/draft-internet2-salsa-netauth-summary-02.html)
- Exemples de solutions d'administration d'un réseau sans fil, Sylvie Dupuy et Catherine Grenet, octobre 2004, http://www.cru.fr/nomadisme-sans-fil/J1310/cg-sd.pdf
- Recommandations d'architecture de réseau avec filtrages pour améliorer la sécurité, Jean-Luc Archimbaud, 2000, http://www.urec.cnrs.fr/securite/articles/archi.reseau.html
- Recommandations de sécurité destinées aux administrateurs systèmes et réseaux du CNRS pour l'installation de réseaux locaux sans fil (« WiFi »), Jean-Luc Archimbaud, Catherine Grenet, Marie-Claude Quidoz, novembre 2004,
  http://www.urec.cnrs.fr/securite/articles/RecomWIFI.html
- Charte utilisateur pour l'usage de ressources informatiques et de services Internet :
  http://www.cnrs.fr/Infosecu/Charte.html
- Groupe de travail « le nomadisme et les réseaux sans fil », http://www.cru.fr/nomadisme-sans-fil/
- Groupe de travail « Comment Adapter une Politique de Sécurité pour les Entités du CNRS (CAPSEC) » https://www.urec.cnrs.fr/securite/corres-secu/CAPSEC.html ■

EN BREF...

●●● Une fiche de l'université de Limoges sur les Spywares, en français «espiogiciels», fait le point. Attention, certains sont très invasifs!
http://www.unilim.fr/sci/fiches/Spyware.pdf

●●● Présentation de la réflexion et des résultats des expériences effectués par François MORRIS sur l'authentification 802.1X (à la fois en filaire et en sans fil) à l'URL:
http://www.lmcp.jussieu.fr/~morris/802.1X/mobile.pdf

●●● Comment utiliser le MUA mutt (http://www.mutt.org/) avec les certificats smime pour signer et chiffrer les messages électronique par Maurice Libes de (UMS2196) et Albert Shih (UMR7586) du CNRS.
http://www.com.univ-mrs.fr/ssc/info/cours/mutt-smime.pdf

●●● Les supports des présentations de l'observatoire de la Sécurité des Systèmes d'Information et des Réseaux sont à: http://www.ossir.org/sur/supports/liste.shtml

●●● Exemple d'un Cahier des Clauses Techniques et Particulières pour un chantier de câblage rédigé par l'Université Joseph Fourier:
http://listes.ujf-grenoble.fr/wws/d_read/cablage/CCTP-CABLAGE.pdf

et de préconisations sur le nomadisme et déploiement de réseaux sans fil: http://listes.ujf-grenoble.fr/wws/d_read/wifi/

●●● La Commission européenne, DG INFSO, unité ETEN publie un appel à candidatures en vue de la sélection d'experts indépendants dans le cadre du programme eTEN
http://europa.eu.int/information_society/activities/eten/index_en.htm

●●● Trois questions à Philippe Rosé (Journaliste, spécialiste des questions de sécurité) sur le web de crise:
http://www.asti.asso.fr/pages/Hebdo/sh37/sh37.htm

●●● La Mission de contrôle à l'exportation des biens et technologies à double usage de la DiGITIP publie une brochure intitulée: «Le contrôle de l'exportation des biens et technologies à double usage».
http://www.industrie.gouv.fr/biblioth/docu/dossiers/sect/bienettechnologie.pdf

●●● Ces dernières années, la sécurité est devenue une priorité pour les pouvoirs publics et les entreprises. Crime organisé, terrorisme, interruption des chaînes d'approvisionnement mondiales, virus informatiques – autant de menaces avec lesquelles il faut compter dans le monde d'aujourd'hui, d'où l'émergence d'un marché des équipements et des services de sécurité de 100 milliards de dollars.
On trouvera une étude de la question, publiée par l'OCDE, sur:
http://www1.oecd.org/publications/e-book/0304032E.PDF
Elle jette un jour nouveau sur ces enjeux cruciaux ainsi que sur bien d'autres questions posées par l'économie de la sécurité du XXIe siècle.

Gestion et licéité des traces

par Robert Longeon

La constitution de journaux d'activité est consubstantielle à l'informatique. Au tout début, lorsque les architectures étaient fortement centralisées, les coûts d'exploitation étaient alors très élevés, les traces servaient à assurer la fonction comptable permettant de gérer une pénurie de moyens bien réelle. Puis, progressivement, d'autres exigences sont apparues: celle de réguler l'utilisation des ressources, celle de détecter des anomalies afin d'assurer un bon niveau de qualité de service, ou encore celle de faire évoluer les équipements. Parallèlement, la conscience de l'importance de la SSI s'est un peu plus affirmée. Ces nouvelles exigences ont rendu nécessaires des traces toujours plus nombreuses et plus spécifiques jusqu'au point où leur exploitation manuelle était devenue pratiquement impossible. La décentralisation des moyens de calcul qui s'est opérée par la suite, en augmentant considérablement le nombre et la diversité des systèmes, a accentué encore cet embrouillamini. On n'a plus su alors exploiter correctement ces traces, et rares étaient ceux qui avaient conscience des exigences de sécurité dont elles devaient faire l'objet ou des risques que pouvait présenter un hypothétique «détournement de finalités».
Aujourd'hui, avec la nouvelle loi qui refonde la CNIL, il n'est plus possible d'ignorer que ces traces sont «des données à caractère personnel» et qu'en tant que telles, elles doivent être déclarées ainsi que les finalités des traitements dont elles font l'objet. Mais, même sans cette loi, il nous aurait été impossible de continuer ainsi sans savoir ce que nous faisons et pourquoi nous le faisons, c'est-à-dire sans une «politique de gestion des traces».
C'est ce qu'à fait le CNRS. Le texte, disponible sur le nouvel intranet du FSD (http://www.sg.cnrs.fr/fsd/), a été déclaré à la CNIL et est publié au Bulletin Officiel du CNRS du mois de décembre. Il offre aux ARS (Administrateur Réseau et Système) et aux «coordinateurs sécurité» un cadre réglementaire, normatif et organisationnel dont ils ont besoin pour effectuer leur mission sans s'exposer à un risque juridique, pourvu que:
- la collecte des traces s'accompagne d'une bonne information des personnes (elle doit être individuelle, par exemple par affichage du type de traces générées sur les systèmes utilisés),
- la structure représentative, par exemple le conseil de laboratoire, ait donné son accord,
- les traitements ne fassent pas l'objet de détournements de finalité et que les informations ne soient pas conservées au-delà de la durée prévue,
- les résultats de ces traitements et les données collectées fassent l'objet d'une sécurité optimale.

Le cadre réglementaire rappelle les principes d'information préalable, du droit à consultation, du non-détournement de finalité, du droit à l'oubli. Le cadre normatif explicite les traces qu'il est licite de conserver, leur durée maximale de conservation et les finalités de traitement auxquels elles donnent lieu. Le cadre organisationnel permet de distinguer entre structures fonctionnelles et structures hiérarchiques afin de rendre compatibles pour les ARS travail d'équipe et obligation du «secret professionnel». Nous invitons le lecteur à se reporter à ce texte s'il désire entrer plus avant dans les détails.
Vous n'êtes évidemment pas obligé de vous en tenir à ce document, certaines contraintes particulières ne peuvent être prises en compte dans le cadre d'une politique générale; dans ce cas il faudra déclarer vous-même à la CNIL votre propre politique, mais vous n'êtes plus seul, vous pourrez vous aider, si vous le jugez utile, du texte existant.

Une dernière recommandation, pour conclure: que vous vous conformiez à la politique générale telle qu'elle a été définie et publiée au *Bulletin officiel* ou que vous désiriez élaborer votre propre politique, vous ne pouvez plus ignorer que les «traces», ou autrement dit «les logs», sont des données à caractère personnel et que les ARS ont pour ce type de données la double obligation de sécurité et de «secret professionnel». «Secret professionnel», y compris à l'égard de leur hiérarchie... Ce qui n'est évidemment pas sans poser parfois quelques problèmes!

Robert.Longeon@cnrs-dir.fr

Éclairage sur...

par Kostya Kortchinsky Responsable du CERT-Renater

L'analyse de binaires

MALGRÉ la naissance de multiples langages de haut niveau, leur maturation, et leur implantation solide dans le paysage de la conception et du développement, la connaissance du langage assembleur dans le domaine de sécurité des systèmes d'information reste une valeur sûre. Certes, il est nettement plus confortable d'avoir à étudier un code source dans un langage évolué, et si possible bien commenté, mais il est très rare que nous l'ayons à disposition lorsque nous devons analyser des binaires compilés recouvrés sur une machine compromise. Confrontés à ce type de situation, la solution du désassemblage s'offre à nous.

La décompilation – de mon point de vue la possibilité d'obtenir des sources en langage de haut niveau – ne donne dans la réalité des résultats satisfaisants que dans un nombre limité de cas (JAVA ?), contrairement au désassemblage qui nous permettra dans la totalité des cas d'obtenir un listing assembleur relativement lisible – sauf chiffrement ou compression du binaire par exemple. La compréhension des tenants et des aboutissants du programme ainsi décortiqué passera alors nécessairement par l'examen de trames d'instructions assembleur, en «live» (débogage), ou non (désassemblage).

Les possibilités offertes par de tels procédés sont multiples puisqu'elles couvriront aussi bien l'analyse de binaires suspects (le terme anglophone «malware» est souvent utilisé pour les désigner), que la recherche de failles dans des logiciels ou systèmes d'exploitation aux sources non accessibles (ceux de l'éditeur Microsoft me viennent en tête). Il est cependant regrettable de voir que ce type de compétences est bien souvent délaissé par les professionnels du milieu de la sécurité des systèmes d'information car exigeant un investissement personnel très important. Bien souvent, seuls les éditeurs de solutions antivirales peuvent tirer parti d'un bon niveau en la matière.

Il émerge cependant une volonté de sensibilisation à cette problématique hautement technique particulière, comme le montrent par exemple les deux derniers challenges «Scan of the Month» du projet Honeynet ayant pour objectif la rétroconception de deux programmes suspects[1][2], ou bien le numéro 14 de la revue MISC dont le dossier parcourait le sujet de façon approfondie aussi bien sous systèmes UNIX que Windows[3]. Je ne saurais que trop vous recommander d'aller jeter un œil rapidement sur les solutions proposées aux challenges qui devraient vous permettre d'appréhender une partie des potentialités de cet art. Afin de prendre un exemple concret, l'analyse du ver Witty, diffusé le 19 mars 2004 et d'une taille réduite, n'a pris que quelques dizaines de minutes après la capture du paquet incriminé[4], et a permis de juger de sa dangerosité et de prendre les mesures qui s'imposaient. Les codes malveillants sont loin d'être le seul champ d'application puisque ces mêmes techniques sont à l'origine de la découverte de différentes vulnérabilités dans des éléments aux sources fermées : débordement de tampons, débordements d'entiers, bogues de format, etc., autant de problèmes pouvant être mis au jour par le reverse-engineering des binaires impliqués, ou de façon détournée en étudiant les correctifs diffusés[5] ! Je pourrais aussi citer la validation de la conformité d'un algorithme implémenté avec son modèle théorique (ou même simplement avec ce qui est dit être implémenté) : une présentation sur les applications à la cryptographie a été faite à SSTIC 2004[6].

1. SotM 32, http://www.honeynet.org/scans/scan32/
2. SotM 33, http://www.honeynet.org/scans/scan33/
3. MISC 14, http://www.miscmag.com/sommaire.php
4. Black Ice Worm Disassembly, http://www.caida.org/analysis/security/witty/BlackIceWorm.html
5. Diff, Navigate, Audit, http://www.blackhat.com/presentations/bh-usa-04/bh-us-04-flake.pdf
6. SSTIC, http://www.sstic.org/

La trousse à outils

Bien évidemment, aucun outil ne prendra en charge la tâche de rétroconception d'un programme en totalité, néanmoins certains outils vous faciliteront grandement le travail :

- The IDA Pro Disassembler and Debugger : http://www.datarescue.com/idabase/ Sans nul doute le meilleur outil de désassemblage disponible sur le marché, il vous permettra d'obtenir rapidement un code clair et fiable, et ce pour un grand nombre de processeurs. Il est payant, et sa dernière version est disponible pour Linux.
- OllyDbg : http://home.t-online.de/home/Ollydbg/ Un débogueur 32 bits pour systèmes Windows, gratuit, il est très complet et suffit amplement pour toute activité se cantonnant au Ring 3.
- Programmer's Tools : http://www.programmerstools.org/ Un site regroupant une collection d'outils ayant un rapport avec le développement sous Windows, ciblant entre autres l'analyse de binaires, le reverse-engineering, la décompression d'exécutables. De bonnes idées peuvent y être trouvées.

kostya.kortchinsky@renater.fr

SÉCURITÉ INFORMATIQUE
numéro 51 décembre 2004
SÉCURITÉ DES SYSTÈMES D'INFORMATION

Sujets traités : tout ce qui concerne la sécurité informatique. Gratuit.
Périodicité : 4 numéros par an.
Lectorat : toutes les formations CNRS.

Responsable de la publication :
ROBERT LONGEON
Centre national de la recherche scientifique
Service du Fonctionnaire de Défense
c/o IDRIS - BP 167. 91403 Orsay Cedex
Tél. 01 69 35 84 87
Courriel : robert.longeon@cnrs-dir.fr
http://www.cnrs.fr/Infosecu

ISSN 1257-8819
Commission paritaire n° 3105 ADEP

Conception et réalisation : La Souris 0145210961