SÉCURITÉ INFORMATIQUE

numéro 23 février 1999

SÉCURITÉ DES SYSTÈMES D'INFORMATION

L'étrange beauté et le charme de la sécurité au sommet…

éditorial

À quoi bon chercher ce que d'autres ont déjà trouvé… et… le malheur des uns peut faire le bonheur des autres. Si l'on applique ces vieux adages à la sécurité des systèmes d'information, il apparaît qu'il y a toujours à apprendre lorsqu'un voisin vous invite à regarder dans son assiette où les succulentes lentilles du Puy cohabitent parfois avec des cailloux.

Les responsables de la sécurité informatique d'organismes prestigieux comme l'INRA, l'INSERM, l'IPG de Paris, l'ORSTOM et l'IDRIS sont ainsi venus exposer, dans les colonnes de précédents numéros de *Sécurité Informatique*, leur conception de la sécurité, les moyens et les astuces qu'ils mettent en œuvre, les attaques qu'ils ont subies et comment ils y ont fait face.

Dans ce premier numéro de l'année, c'est l'Institut national de physique nucléaire et de physique des particules qui apporte sa contribution à cette somme d'expériences variées. Né il y a 27 ans, au moment où l'informatique commençait timidement à s'installer dans les laboratoires, l'IN2P3 en est rapidement devenu un très gros utilisateur, au point de créer son propre centre de calcul scientifique et son propre réseau d'interconnexion.

Ce que vous allez découvrir sous la plume de Bernard Perrot est le fruit d'une longue pratique et d'une réflexion féconde ; il nous apprend que rien n'est jamais gagné d'avance et qu'il faut sans relâche analyser les risques, traquer les faiblesses et instruire les utilisateurs.

* * *

Le mois de janvier 1999 a apporté du nouveau sur le programme d'action gouvernemental pour la société de l'information, et notamment sur la libéralisation de l'usage de la cryptologie. Nous en reparlerons dans le prochain numéro.

Philippe Schreiber
Fonctionnaire de Défense

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

Cela n'arrive pas qu'aux autres !

Ce petit récit d'un acte malveillant survenu dans une de nos unités est authentique, les noms propres ont bien entendu été dissimulés

Ce matin-là, début juillet, une mauvaise surprise attend Patricio, chercheur visiteur au laboratoire : il se connecte sur son compte au CERN, plus rien… tous ses fichiers ont disparu. Sauf un : le fichier historique de la dernière session (il s'agit d'un serveur Unix) qui contient les dernières commandes exécutées, la dernière étant «rm –rf *». C'est certain, cela ne pardonne pas. Mais Patricio est bien certain de ne pas avoir fait cela lui-même. La commande a été exécutée vers 6 heures ce matin, et Patricio avait quitté normalement son bureau hier soir. Par chance, une sauvegarde automatique de son compte a eu lieu en milieu de nuit : il sera possible de restaurer son environnement (sauf quelques résultats de calcul de la nuit, mais le préjudice reste heureusement faible). Patricio m'avertit du piratage probable de son compte ; pour lui qui va récupérer très rapidement ses fichiers, l'incident est clos. Pour moi, il commence : que s'est-il passé cette nuit sur son compte ?

À part le «rm» fatal, l'historique révèle quelques «telnet» sur des machines distantes inconnues, et un curieux «set DISPLAY» (déport de l'affichage Xwindow) vers un «terminal X» situé dans une salle d'enseignement du laboratoire, équipée d'une dizaine de ces terminaux. Le forfait a donc eu lieu dans nos murs. Les commandes de l'historique sont datées, cela s'est déroulé dans la nuit. Il est désormais plus de 10 heures du matin, je vais quand même voir dans cette salle d'enseignement. Plusieurs étudiants y sont présents, ce qui est tout à fait normal *a priori*. L'un d'eux, que je n'ai jamais vu, est en train de travailler sur celui mis en cause dans les logs. Je lui demande ce qu'il fait ici puisque je ne le connais pas : il me répond qu'il est étudiant sur le campus, que les salles informatiques des étudiants du

…… *suite page 4* ……►

La sécurité informatique à l'IN2P3

Voilà près de quinze ans qu'il existe une expérience et une pratique de la sécurité informatique à l'IN2P3. En fait, cette pratique a, par la force des choses, été rendue nécessaire à partir du moment où il y a une connexion et accessibilité de nos laboratoires *via* des réseaux publics.

Nous avons été, moi et des collègues, confrontés à nos premiers pirates dès le début des années 80: déjà quelques soirées et nuits à confondre des adeptes, conscients ou non, du déjà célèbre Chaos Computer Club de Hambourg (dont les «dirigeants» agissaient en fait pour le compte de la Stasi et du KGB...) qui pirataient *via* Transpac.

À cette époque, l'informatique était encore très peu développée au niveau du «grand public», surtout en moyen de connexions: les faits «graves» étaient peu fréquents (moins d'un par an en moyenne).

Le développement fulgurant d'Internet, d'un réseau thématique ne concernant que quelques centaines de sites académiques ou de recherche à l'instrument domestique qu'il est en train de devenir, modifie radicalement les données du problème: le réseau de communication que nous utilisions de façon naturellement conviviale avec une approche «réseau local» – même si l'infrastructure était planétaire – s'est transformé en un réseau public dans lequel notre activité tient une place marginale. Les problèmes de sécurité informatique se sont multipliés (le nombre d'incident grave – c'est-à-dire nécessitant une intervention d'autorité de police ou de justice – est passé de moins d'un seul tous les trois ans, en moyenne, à plusieurs par an). Cette généralisation de l'utilisation de l'Internet a représenté, pour nous une dégradation de l'outil de travail: l'introduction de mesures de sécurité (inévitablement contraignantes mais devenues indispensables) est vécue comme une perte de confort et d'ergonomie, et provoque une perte de productivité.

La migration du réseau PHYNET d'une infrastructure «privée» (lignes louées dont nous contrôlions l'architecture en totalité) vers une infrastructure utilisant désormais les réseaux campus et Renater n'a fait qu'accroître pour nous les risques et les incidents: nous ne pouvons plus considérer PHYNET comme un «réseau local» avec les avantages que cela constitue pour gérer la sécurité et contrôler l'activité.

L'activité de l'IN2P3 nécessite un fort soutien technique en général, et informatique en particulier. Tous les laboratoires possèdent des services informatiques. Dès la fin des années 80, il a été décidé de fédérer la prise en compte de la sécurité informatique afin de ne pas disperser les efforts en constituant une structure tout à fait classique de «correspondants sécurité» dans les laboratoires (si possible et en général assistés d'au moins un suppléant en cas d'indisponibilité), et d'un responsable au niveau national (moi-même), assurant également le rôle d'interface vis-à-vis des autres organismes et autorités agissant dans le domaine (Certs, etc.). Cette structure, efficace, se heurte cependant chez nous comme partout ailleurs au problème de disponibilité des personnes: la sécurité (dont la prévention) prend beaucoup de temps, et les correspondants n'en disposent pas d'assez pour traiter le sujet de façon entièrement satisfaisante. On travaille malheureusement beaucoup plus dans l'urgence que dans la sérénité: sur ce point, nous ne sommes pas très différents tous nos collègues au CNRS.

Le travail «quotidien» avec les correspondants se fait essentiellement par voie électronique (et téléphonique), *via* deux listes de diffusion (bien vieille technique qui se révèle en fait une des plus efficace) et un serveur Web spécialisé (http://www.in2p3.fr/securite/). Afin de traiter des sujets de fond et partager de l'expérience, les correspondants sont réunis en moyenne une fois par an. Dans les semaines qui viennent, un programme de formation interne spécialisé sur la mise en œuvre et l'utilisation d'outils de sécurité va également être mis en place à leur attention.

Afin d'être en conformité avec la législation concernant les traitements d'informations nominatives (législation *Informatique et liberté*), l'IN2P3 a effectué, avant tout le monde, les démarches nécessaires auprès de la CNIL (demande d'autorisation préalable) pour développer ses annuaires *via* les serveurs Web des laboratoires: tous nos annuaires sont déclarés et autorisés.

L'IN2P3

Créé en 1971, l'IN2P3 (Institut National de Physique Nucléaire et de Physique des Particules) est un institut du CNRS dont la mission est de promouvoir et de fédérer les activités de recherche dans ces domaines de la physique.

Les laboratoires de l'IN2P3 en chiffres

L'IN2P3, ce sont 17 laboratoires en France, totalisant plus de 800 enseignants et chercheurs, plus de 1600 ITA, et environ 250 doctorants. ■

Les missions de l'IN2P3

Recherche fondamentale et instrumentation

Au cœur du programme scientifique de l'Institut, les expériences visent à identifier les constituants fondamentaux de la matière, à étudier leurs interactions, et à comprendre les édifices qu'ils forment, c'est-à-dire les différents niveaux de structure de la matière nucléaire. Pour réaliser ces expériences, les laboratoires de l'IN2P3 mettent au point des détecteurs et des accélérateurs, outils de base indispensables aux progrès de la discipline. La création de ces outils nécessite le développement de techniques de pointe qui peuvent trouver des applications bien au-delà du champ de la physique nucléaire et de la physique des particules.

Interaction et concertation caractérisent l'activité de recherche des laboratoires de l'IN2P3: la mise en œuvre de grands programmes implique un partage des tâches et des échanges constants au sein de collaborations nationales (entre les laboratoires de l'Institut et le CEA) et internationales

Interdisciplinarité

Des liens privilégiés sont noués entre les chercheurs de l'IN2P3 et d'autres secteurs: l'astrophysique et la cosmologie; la chimie (dans les programmes de chimie nucléaire et de radiochimie) ; la physique du solide et la physique des matériaux; la biologie au travers de l'imagerie médicale.

L'IN2P3 dans la société

Institut de recherche fondamentale, l'IN2P3 se doit aussi d'apporter sa pierre à la solution de problèmes de société. Il est notamment concerné par la question du devenir des déchets radioactifs.

Institut à la pointe de la technologie, il se doit également de diffuser vers l'industrie les ressources technologiques qu'il a su développer dans de multiples domaines lors de la construction des grands instruments, et de faire bénéficier de son expertise le monde de l'entreprise.

Composé dans sa quasi-totalité de laboratoires étroitement associés aux universités, l'IN2P3 est un lieu de formation de haut niveau à la physique fondamentale et à la haute technologie. Les étudiants préparant une thèse acquièrent dans ses laboratoires une compétence reconnue tant au niveau de la recherche que de l'industrie. ■

La sécurité informatique à l'IN2P3

Plus récemment (*voir article concernant SSF*), des démarches auprès du SCSSI ont été menées avec succès afin d'obtenir la possibilité d'utiliser de façon libre un produit de chiffrement adapté pour les besoins de l'Institut.

En concertation avec les correspondants sécurité, il a été élaboré un modèle de Charte de «bon usage des ressources informatiques» adaptée de celle mise en place à l'Université Louis Pasteur de Strasbourg: cette charte est en cours de déploiement dans les laboratoires (voir http://www.u-strasbg.fr/Documents/Securite/charte_osiris.html et http://www.in2p3.fr/chartes pour détails).

La politique préventive de sécurité actuelle se veut très pragmatique: malgré la présence de personnels informaticiens dans tous les laboratoires, le temps manque cruellement pour sécuriser et surtout surveiller des milliers de machines (et l'évolution constante vers la dispersion des matériels et les postes personnels).

Les laboratoires sont responsables de la politique locale de sécurité informatique, mais en concordance minimum avec une politique nationale (élaborée en concertation et sous la responsabilité de la Direction nationale et du Chargé de mission à la sécurité informatique). Cette politique est bien entendu en accord avec la Charte Renater et les directives du CNRS.

Dernièrement, il a été décidé de filtrer les principaux protocoles en entrée des routeurs de connexion du réseau du laboratoire au réseau extérieur. Ce filtrage est total dans certains cas. Dans d'autre, on accepte le protocole, mais on sécurise avec un chiffrement de type SSF (*cf.* l'article qui lui est consacré). Pour certains services (ftp, web, courrier...), seules les machines dédiées sont accessibles. Ces mesures sont actuellement en cours de déploiement. Ainsi, une machine banalisée du laboratoire ne devrait pas être accessible directement à partir de machines extérieures. L'éventualité de l'usage de «firewalls» plus complets se heurte au besoin de bande passante importante de la part de la discipline, incompatible avec de firewalls en coupure totale (le firewall qui ne dégrade pas une connexion ATM n'a pas encore été inventé...). Ces mesures viendront compléter celles déjà mises en place au niveau national de plus longue date: filtrage sélectif du protocole ICMP, filtrage de NFS en dehors des réseaux locaux, filtrage du protocole IRC: il est surprenant que IRC fasse l'objet d'une véritable assistance et «promotion» au niveau d'infrastructures de campus, d'écoles, etc., alors que c'est actuellement un véhicule très important de la malveillance informatique et que son utilité professionnelle est nulle. Il y a parfois une certaine incohérence entre les chartes et le fait que certaines autorités qui les ont signées ou élaborées ne les appliquent pas...

La prévention seule ne suffit pas: il faut y adjoindre des moyens de détection et de traitement des incidents de sécurité. Lorsque ceux-ci surviennent – qu'ils soient graves ou non –, il faut procéder à une enquête, essayer d'en comprendre les causes et les conséquences et en tirer les enseignements quant à la politique de sécurité à mener. Il faut également alerter les services appropriés de l'État qui mèneront une enquête, laquelle pourra, éventuellement, déboucher sur une action judiciaire. Pour cela, ayant constaté qu'il n'est pas rare que les traces soient absentes des machines piratées lorsqu'un incident est découvert, nous utilisons un outil à la fois simple et très efficace: nous conservons les journaux

PHYNET

La pratique du réseau à l'IN2P3 date des années 1970 et a suivi constamment l'évolution des techniques d'interconnexion et des protocoles (Earn/Bitnet, DECnet/HEPnet/SPAN, IP/Internet). «PHYNET», c'est le nom donné au réseau d'interconnexion des laboratoires de l'Institut développé dès 1986 par le centre de Calcul, à une époque ou Renater n'existait pas. Depuis quelques années, l'infrastructure «privée» d'interconnexion (lignes louées) a été remplacée par une topologie utilisant Renater (sauf quelques cas pour cause d'infrastructure régionale) (*voir schéma*). L'administration de la partie «privative» nationale du réseau PHYNET est confiée au Centre de calcul de l'IN2P3 (CC.IN2P3) situé à Villeurbanne. Celle-ci est sous astreinte, afin d'assurer une disponibilité maximale du réseau et l'accès à Internet. Malheureusement, le fait de transiter désormais par des infrastructures (campus, Renater, etc.) moins disponibles la nuit et les week-ends limite son efficacité.

L'IN2P3 est présent sur le Web depuis son origine: http://www.in2p3.fr/ ■

La sécurité informatique à l'IN2P3

(«logs») des routeurs d'interconnexion entre les laboratoires et l'extérieur. Ces logs sont prélevés avec une périodicité de vingt minutes, et centralisés pour archivage. L'archivage est fait à la fois sur cartouches magnétiques (pour le long terme), et sur cédérom (pour faciliter l'analyse en ligne). Ces logs sont extrêmement riches d'informations, par exemple pour déterminer le volume de données échangées lors d'une intrusion, pour y détecter la présence (l'adresse) de machines suspectes, pour détecter le piratage de machines par rebonds. Un projet est actuellement en cours pour compléter ces logs par d'autres prélèvements, plus complets, effectués par une machine connectée en «sniffer» juste derrière les routeurs afin de journaliser l'activité entrante et sortante avec plus de précision (informations sur les protocoles utilisés, les sessions, etc.).

La gestion de la sécurité informatique nécessite du temps et des personnes pour faire le travail: il n'y a pas pléthore d'informaticiens à l'IN2P3, mais nous avons cependant la chance d'être moins démunis que beaucoup d'unités du CNRS. Sans doute est-ce là une des raisons qui font que l'IN2P3 n'est pas trop mal loti en traitement de la sécurité informatique, qu'il a réussi à acquérir une certaine expérience (malheureusement par la pratique et la force des choses), et obtenu quelques succès. Il n'est pas possible de gérer correctement la sécurité informatique sans prise de conscience et motivation de la hiérarchie et des informaticiens eux-mêmes: la Direction et les informaticiens de l'IN2P3 ne font pas défaut sur ce point. Il reste cependant un gros travail à effectuer pour sensibiliser les utilisateurs.

Bernard Perrot
Chargé de mission
pour la sécurité informatique à l'In2p3
perrot@lal.in2p3.fr

Routeurs ou «gardes-barrières» ?

Seul un «coupe feu» permet de filtrer le trafic réseau? NON! Hervé Schauer (Herve.Schauer@hsc.fr) remet une fois encore les points sur les «i» : «La majorité des routeurs du marché savent analyser les trames au niveau applicatif (NSC, 3COM, CISCO, etc.). Ils savent même avec des options faire du filtrage de session (*stateful inspection*) qui fait plus de contrôle dans la continuité de la session que des produits dits "firewall"… Donc, s'il n'y a pas besoin d'authentification et d'analyse de contenu de type recherche d'anti-virus, par exemple, un routeur filtrant fait désormais aussi bien – si ce n'est pas mieux – qu'un produit appelé "firewall" par du marketing.» ■

R. L.

suite de la page 1

bâtiment 123 sont fermées depuis le début de la semaine (pour cause de vacances), et qu'il lui a été dit d'aller à la salle restée ouverte du bâtiment 250. Je lui réponds qu'il s'est trompé, le bâtiment 250 est celui de l'autre côté de la rue, il est ici au 240. Je le prie donc de ne pas rester ici. Comme il s'apprête à fermer les fenêtres ouvertes sur le terminal, je l'en empêche, un doute soudain… Comme il prend mal la chose, je lui demande alors de me montrer sa carte d'étudiant, qu'il n'a pas. Il me présente un récépissé de perte de papier d'identité, que je photocopie et le prie de quitter enfin les locaux. Je reviens sur le terminal, trouve des sessions ouvertes vers une école parisienne et une activité manifestement inamicale dévoilée par les historiques: je comprends que je viens de laisser partir l'auteur du piratage du compte de Patricio.

Un outil va se révéler une fois de plus très utile: à l'IN2P3, nous prélevons les fichiers journaux (les «logs») de nos routeurs avec une périodicité de 30 minutes, et ils sont tous archivés sur une machine de service pour le court terme, et sur bande et cédérom pour le long terme. Ces logs contiennent les paires d'adresses IP des machines communicantes durant la période de temps, ainsi que le volume de paquets et octets échangés. Une analyse de ces logs permet de connaître les adresses des machines avec qui des connexions ont été établies depuis le terminal utilisé par notre visiteur dans la nuit. Ensuite, je recherche s'il y a eu une activité avec les machines découvertes les jours précédents: il apparaît effectivement qu'une activité similaire à celle de la nuit avait lieu depuis déjà quatre jours, et depuis plusieurs terminaux X du laboratoire. Il apparaîtra que l'intrus se faisait enfermer dans les locaux le soir, cherchait des terminaux avec des sessions non fermées (fenêtres «telnet» sur des terminaux X), et les récupérait pour pirater les machines sur lesquelles les sessions étaient ouvertes! Pas besoin de connaître les mots de passe, les sessions étaient déjà ouvertes… grave «négligence» de la part des utilisateurs de ces terminaux. Il est possible de constater que l'intrus «possède» des accès sur de nombreuses machines, dont une récurrente, très au nord du continent européen.

Contact est pris avec les autorités de police spécialisées: il apparaît alors que l'individu est déjà «connu» (les papiers qu'il m'a présentés étaient authentiques, il ne manquait pas d'assurance ni d'audace!). Une plainte est déposée.

Craignant un retour du pirate, je contrôle les semaines suivantes les logs des routeurs pour y détecter une éventuelle activité similaire à la sienne (il se connectait beaucoup sur des serveurs Web pornographiques, des serveurs IRC, et certaines machines récurrentes) : nulle trace. Affaire bouclée.

Il sera interpellé quelques mois plus tard. Où l'on découvrira alors qu'il est revenu dans nos locaux régulièrement pendant plus de trois semaines après le dépôt de plainte sans être remarqué: la nuit, il passait par les toits ou le week-end par la fenêtre pour entrer dans le bureau fermé d'un collaborateur en congé. Qu'il avait déjà «visité» ce bureau lors de sa première incursion, et avait alors (toujours en récupérant des sessions non fermées sur un terminal) obtenu l'accès sur des ordinateurs d'un grand centre de recherche avec lequel l'occupant habituel du bureau avait un contrat. Que cette nouvelle série de visites était exclusivement ciblée sur le piratage discret de ce centre à l'exclusion de toute autre connexion (ce qui explique que je n'ai pas pu détecter son activité dans le trafic réseau). Qu'au retour de congé du locataire du bureau, il a continué plusieurs semaines à pirater ce centre de recherche depuis d'autres sites franciliens (universitaires, écoles). Que sa première visite était prospective. Qu'il était manipulé. Que la machine sur laquelle il se connectait, celle très au nord, il ne l'avait pas piratée, celle-là… c'était celle de ses commanditaires, qui lui avaient passé une commande (pénétrer des ordinateurs du centre de recherche en question). Qu'il était en fait très bien renseigné. Que ça n'arrive pas qu'aux autres, ni que dans les romans…

Bernard Perrot

À l'heure où nous mettons sous presse, un important changement de la législation française en matière de cryptologie vient d'être annoncé le 19 janvier par le Premier Ministre lors d'une allocution. Un prochain numéro fera le point précis. Cette déclaration annonce qu'il va être déposé un projet de loi libéralisant totalement l'usage de la cryptologie en France. En attendant le changement de législation, de nouveaux décrets devraient être publiés dans les prochaines semaines, modifiant ceux du printemps 1998 sur les points suivants : le seuil entre régime déclaratif et le régime d'autorisation préalable sera situé pour une taille d'espace de clés de 2¨128 (contre 2¨40 actuellement), et la notion de test d'arrêt simple devrait être supprimée. SSF devrait donc rester d'actualité au moins jusqu'au vote de la nouvelle législation et parution de ces décrets d'application (afin d'en légaliser la fourniture). Cependant, l'entropie des clés sera immédiatement adaptée au nouveau régime «128 bits» dès qu'il sera instauré.

SSF (Shell Sécurisé Francisé)

Les «sniffeurs» sont des logiciels malveillants qui lisent les trames Ethernet et capturent les identifications des connexions qui circulent «en clair» sur les réseaux. C'est bien entendu là, un danger majeur, dans la mesure où toute la sécurité des systèmes standards UNIX repose sur ce mécanisme d'authentification des utilisateurs. Les mésaventures de ce type arrivent surtout à l'occasion de connexions depuis l'extérieur du laboratoire. Le danger est alors d'autant plus grand que le trafic transite par des réseaux universitaires ou de prestataires de service grand public. Or, en raison de la nature même de notre discipline, les collaborations internationales sont d'une absolue nécessité. Il s'ensuit qu'un utilisateur veut, a priori, pouvoir se connecter de n'importe où, n'importe quand, en toute sécurité.

Un outil populaire sur Internet depuis quatre ans s'appelle SSH (pour *Secure Shell*). SSH est en fait un protocole, et une collection de logiciels implémentant ce protocole. En première approche, on peut dire que SSH est un remplacement sécurisé pour «telnet», «rlogin, rsh» et «rcp». Plus précisément, SSH crée et utilise un «tunnel» chiffré de bout en bout pour sécuriser la connexion (en particulier, les mots de passe circulant se trouvent donc protégés contre toutes écoutes). Plus en détail, SSH permet de faire passer dans ce «tunnel» chiffré toutes applications TCP, et les sécuriser également. Il permet également, grâce aux techniques de «clés publiques», une authentification accrue des machines source et destination des connexions (protection contre le «spoofing»). SSH utilisant du chiffrement (cryptage) «dur», son usage en France nécessite l'obtention d'une autorisation préalable, en raison de la législation sur la cryptologie. À noter que l'architecture du protocole ne nécessite pas de mettre en place une politique et une organisation de gestion des clés ; il n'y a pas à échanger ou communiquer des clés dans SSH ; les clés de sessions sont aléatoires, dynamiquement volatiles et renouvelées à chaque connexion.

Non seulement SSF apporte une réponse séduisante au risque de violation des mots de passe, mais il offre désormais une alternative légale à SSH. Cette mise en œuvre était d'autant plus urgente que plusieurs laboratoires partenaires à l'étranger nous ont informés de leur intention de rendre bientôt l'usage du protocole SSH obligatoire pour se connecter à leur site.

Ce besoin apparaît au moment de la parution des nouveaux décrets du printemps 1998 instituant un nouveau régime d'usage libre pour une

suite page 6

SSF est-il sûr puisque limité à 40 bits ?

Un espace de clé limité à 2^{40} offrira une moindre résistance à un craquage par *force brute* que si les clés étaient plus grandes, c'est un fait.

Il est à noter d'abord qu'il n'est cependant pas si «facile» de casser un chiffre de cette entropie : contrairement à ce que certains prétendent, il ne faut pas «cinq minutes sur une machine grand public standard» pour décrypter un tel code. Dans le cas présent – communication en temps réel avec protocole paquet, chiffrement en mode rebouclé (CBC) –, il faudrait au moins deux semaines de calcul intensif et exclusif sur du matériel haut de gamme pour un «amateur», qui devra de plus avoir les moyens de capturer («sniffer») la session à décrypter (et chaque session a des clés différentes). Par contre, il est réel que les moyens d'une «agence gouvernementale» permettent de casser une telle session : SSF n'est pas adapté à de tels besoins de confidentialité et ce n'est pas son objectif.

De plus, il est important de savoir que la force des algorithmes de chiffrement d'un produit n'est pas le seul garant de la robustesse et de la confiance totale du produit. En ce qui concerne le paquetage SSH Unix sur lequel a été bâti SSF, il faut savoir, par exemple, qu'à l'occasion de cette adaptation :

– j'ai trouvé un bogue d'implémentation dans le traitement des paquets de type SSH_MSG_IGNORE. Cela démontre au moins que ce paquetage (de référence, et dont la base est la même que le produit commercial correspondant) n'a jamais été validé pour vérifier qu'il implémente correctement le «RFC». Ce bogue a été corrigé depuis la version 1.2.23, suite a mon intervention.

– J'ai trouvé un bogue gravissime de sécurité, qui affectait la qualité du générateur de nombres aléatoires, et rendait SSH bien moins sûr que ce que l'on pouvait croire (sans entrer ici dans les détails, disons simplement que les aléas étaient prévisibles… !). Cela prouve une nouvelle fois que ce paquetage n'a pas été correctement testé et n'a pas été validé. Accessoirement, cela démontre que, contrairement à une légende tenace, les sources d'un produit (de sécurité ou autre) sont disponibles et peuvent être examinées par toute la communauté, mais qu'en fait, personne n'en fait rien… La correction de ce bogue prenait une seule ligne de code, et il était détectable par quiconque examinait le flux de données émis par SSH. Il était présent dès l'origine, c'est-à-dire plus de trois ans. Dans le cadre d'un examen (de principe) paranoïaque des failles de sécurité sur un produit revendiquant une très haute sécurité, il n'est pas possible d'écarter l'hypothèse que ce bogue fût en fait une *backdoor* (une faille introduite intentionnellement afin de pervertir le produit à l'usage des auteurs de cette faille). Ce bogue a été corrigé depuis la version 1.2.25 suite à mon rapport aux auteurs, mais, curieusement, celui-ci ne fait l'objet d'aucune mention dans la liste des corrections de cette version, contrairement à l'usage habituel.

– J'ai constaté qu'il y a un canal subliminal dans le *padding* : ceci est un problème grave du protocole SSH, pas de l'implémentation. Sans entrer ici trop dans la technique, résumons en disant que ce dispositif permet de pervertir le protocole d'une façon totalement indétectable par une des parties communicantes, ou les deux, (d'où l'origine du terme «subliminal»), pour (par exemple) permettre le déchiffrement et l'écoute de la communication par un tiers. Les auteurs (commerciaux) du protocole ont été très peu réceptifs à ma demande de correction de cette faille (y compris pour la traiter dans la définition de la nouvelle version 2 de ce protocole en cours de standardisation). Mais des mauvaises langues vous diront que la présence d'un canal subliminal est une «*obligation*» pour un produit «*autorisé*» à l'export outre océan…

– La conséquence de ce dernier problème est que, si vous redoutez (et avez de bonnes raisons de redouter) qu'un adversaire ait la volonté, le temps et les moyens de casser vos sessions SSF avec des clés de 40 bits, vous devez alors vous demander si ce même adversaire n'aurait pas les moyens d'utiliser ce canal subliminal. Si la réponse est positive, peut-être ne faut-il pas utiliser le protocole SSH.

En conclusion, faut-il ne pas utiliser SSF ? Bien sûr que non, tout dépend de l'objectif : SSF, comme tous les produits de sécurité en général, et ceux utilisant des techniques cryptographiques en particulier, n'est pas un jouet : son utilisation doit correspondre à un objectif précis dans le cadre d'une politique de sécurité dans laquelle les risques ont été évalués, et les outils choisis en fonction de ces risques. Cela est de l'appréciation et la responsabilité de chacun. ■

suite de la page 5

catégorie de produits de cryptologie de robustesse «moyenne» (entropie des clés inférieure à 2^{40}, voir encart) : il a donc été choisi de tenter une stratégie consistant à adapter SSH afin de le rendre conforme à ce régime, ce qui présentait l'énorme avantage d'en obtenir un usage libre de démarche à partir du moment où l'adaptation serait conforme à la législation.

C'est ainsi qu'est né SSF. SSF est donc une adaptation de SSH, entièrement compatible au niveau protocole avec les clients et/ou serveurs SSH standards ayant fait l'objet d'une déclaration conforme auprès du SCSSI, et donc désormais d'usage libre sur le territoire français.

L'entropie des clés de session a été limitée à 2^{40} dans SSF, mais sans nuire à l'interopérabilité avec les produits SSH standards.

Le paquetage SSF (client, serveur et outils) pour système Unix est disponible depuis septembre 1998 *via* le serveur Web de l'IN2P3 ; une version incluant le support complémentaire de l'identification par S/Key est en cours de test. Un client Windows 95/98/NT est disponible depuis janvier 1999 (il tient sur une disquette, et permet donc de sécuriser facilement une connexion depuis une machine d'accueil en exécutant le logiciel depuis celle-ci). Un client Java est en cours de portage, qui devrait permettre l'utilisation sur des systèmes plus exotiques.

Tout cela est disponible (le produit est gratuit, mais reste la propriété de l'IN2P3) *via* http://www.in2p3.fr/securite/ssf/, qui vous fournira également les informations techniques complémentaires. Depuis le début 1999, une liste de diffusion (<ssf-l@in2p3.fr>) a été mise en service, liste qui permet l'information et le partage d'expériences entre les utilisateurs de SSF qui le souhaitent : cette liste n'est pas réservée aux collaborateurs de l'IN2P3, et bien que SSF ait été écrit pour les besoins propres de l'Institut, il est déjà très utilisé en dehors, comme en témoignent les nombreux téléchargements et abonnements à cette liste.

À l'IN2P3, nous avons décidé la mise en place d'une politique de sécurité basée sur le filtrage, dans les routeurs, de certains protocoles tels que telnet, rlogin, ftp... pour les remplacer par des connexions sécurisées utilisant SSF. Conscient de la difficulté (l'impossibilité ?) de sécuriser et de surveiller des milliers de machines dans nos laboratoires, il nous semble plus prudent d'exclure *a priori* le routage des protocoles essentiels, nécessaires aux «pirates» pour mener à bien les intrusions dans les systèmes. SSF est un outil indispensable pour mener une telle politique, sans toutefois dégrader de façon sensible l'ergonomie d'utilisation des machines, ni les fonctionnalités réseau. C'est également une solution très adaptée aux connexions itinérantes, très vulnérables au piratage des mots de passe et sessions (la connexion à domicile via un prestataire d'accès à Internet fait partie de cette catégorie : savez-vous par exemple que, *via* le «cybercable», vous pouvez «écouter» les communications Internet de vos voisins sans problème ?).

Bernard Perrot

Le Décret n° 98-207 du 23 mars 1998 définit les catégories de moyens et de prestations de cryptologie pour lesquelles la procédure de déclaration préalable est substituée à celle d'autorisation (extrait) :

La procédure de déclaration préalable est substituée à celle d'autorisation pour la fourniture des *«équipements dont le déchiffrement d'un message ou d'un fichier au moyen du parcours systématique de toutes les clés possibles ne requiert pas plus de 2^{40} essais sur un test d'arrêt simple»*.

L'utilisation et l'importation des équipements répondant à cette définition sont déterminées dans le Décret n° 98-206 du 23 mars 1998 définissant les catégories de moyens et de prestations de cryptologie qui les dispensent de formalités préalables.

En conséquence, l'usage d'un tel équipement est donc libre de formalités à partir du moment où il a été déclaré auprès du SCSSI qui dispose d'un délai d'un mois pour examiner si l'équipement déclaré correspond bien au régime déclaratif revendiqué (le régime étant déclaratif, s'il n'y a pas rejet explicite, il y a acceptation par défaut de réponse dans le délai légal).

Pour informations complémentaires, voir : http://www.telecom.gouv.fr/francais/activ/techno/technweb1g.htm et http://www.in2p3.fr/securite/legal/legi-crypto.html ■

Comment se protéger contre les macro-virus ?

Les macro-virus, cela commence maintenant à être connu, sont des virus qui se transmettent (en particulier) par des fichiers Word. Pour bien s'en protéger, il faut d'abord un anti-virus à jour, correctement installé sur son poste de travail. Mais que se passe-t-il quand apparaît un nouveau macro-virus, non répertorié par les éditeurs de logiciel de protection ? Tant que ceux-ci n'ont pas proposé une nouvelle mise à jour du «fichier signatures», votre système est vulnérable. C'est le cas actuellement avec un macro-virus tout neuf, de la souche W97M, qu'aucun anti-virus ne reconnaît encore. Il faut donc mettre en place des protections supplémentaires. Parmi celles-ci, les deux qu'il faut connaître en Word 97 sont :

- La protection par un mot de passe du fichier Normal.dot
  1. Démarrez Word
  2. Dans le menu «Outils», rubrique «Macro», choisissez «Visual Basic Editor»
  3. Dans la fenêtre projet de l'éditeur de visual Basic, sélectionnez «Normal»
  4. Dans le menu «Outils», sélectionnez «Propriétés de normal»
  5. Dans la boîte qui apparaît, sélectionnez l'onglet «Protections»
  6. Cochez la case «Verrouiller le projet pour l'affichage» et inscrivez votre mot de passe dans les champs indiqués.
  7. Fermez la boîte de dialogue, sortez de l'éditeur VB et quittez Word en confirmant l'enregistrement de votre nouvel environnement.

Votre fichier Normal.dot est maintenant protégé.

- Activez la protection macro de Word
  1. Démarrez Word
  2. Dans le menu «Outils», choisissez la rubrique «Options…»
  3. Dans la boîte qui apparaît, sélectionnez l'onglet «Général»
  4. Cochez «Protection contre les virus, contenu dans les macros»
  5. Fermez la boîte de commande.

Avec cette protection, à chaque fois que vous ouvrirez un document contenant des macros commandes, vous serez prévenu par une boîte de dialogue qui vous demandera si vous voulez activer, ou non, les macros contenues dans le document. ■ R. L.

SÉCURITÉ INFORMATIQUE
numéro 23 février 1999
SÉCURITÉ DES SYSTÈMES D'INFORMATION

Sujets traités : tout ce qui concerne la sécurité informatique. Gratuit.
Périodicité : 5 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

Conseil et coordination : CNRS - DIST - Jacqueline Leclère • Conception et réalisation : La Souris 01 45 21 09 61