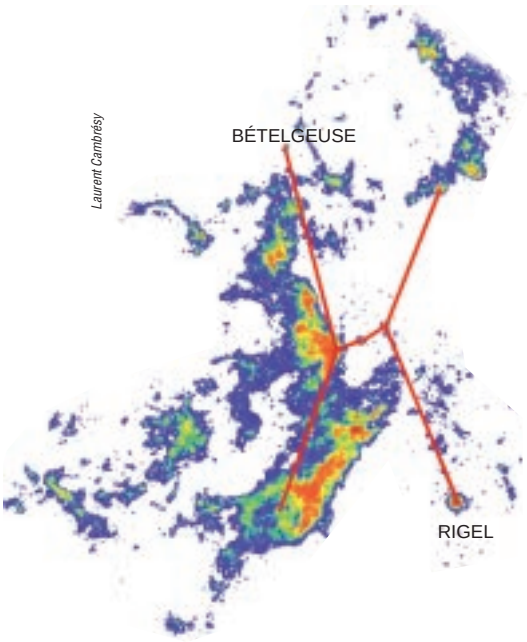


Laurent Cambrésy

Cette carte du nuage moléculaire d'Orion montre l'étendue du nuage par rapport à la constellation d'Orion, aisément identifiable sur le ciel. Les régions rouges sont celles où l'extinction des étoiles situées à l'arrière du nuage est la plus forte et donc où l'absorption de la matière est la plus grande. On estime ainsi la masse du nuage à près de 300 000 fois la masse du Soleil.

fond sont tellement absorbées qu'elles disparaissent. Aussi, complète-t-on ces observations avec des comptages dans l'infrarouge proche (longueurs d'onde de l'ordre du micromètre). Cette gamme de longueur d'onde est bien adaptée à l'observation de ces régions : moins sensible à l'extinction, elle permet de sonder les cœurs les plus denses des nuages.

L'un des objectifs du relevé DENIS est justement de cartographier tout le ciel austral dans l'infrarouge proche. Commencées en 1996, à l'observatoire de la Silla, au Chili, les observations de ce relevé ont déjà permis de cartographier le nuage du Caméléon. On a ainsi distingué une dizaine de cœurs denses, alors que les observations dans le visible n'en faisaient apparaître que quatre. Les données de DENIS sont également un remarquable outil de recherche d'étoiles jeunes, car celles-ci émettent la majeure partie de leur rayonnement dans l'infrarouge. Toujours dans le nuage du Caméléon, on a trouvé une cinquantaine de candidats étoiles jeunes (en plus des 130 connues auparavant dans ce nuage). Leur statut devra être confirmé par des observations spectrales. Les comparaisons des cartes d'extinction avec les observations dans le domaine radio sont également fructueuses. Les différences entre les cartes d'émission du monoxyde de carbone (CO) et les cartes d'extinction révèlent les régions où le monoxyde de carbone est détruit par un fort rayonnement stellaire local. De même, la comparaison entre cartes d'extinction dans le proche infrarouge (ou dans le visible) et l'émission dans l'infrarouge lointain (obtenue par les satellites IRAS et ISO) indique la nature des grains du nuage : les variations du quotient extinction sur émission traduisent probablement des changements dans la composition chimique des grains de poussière.

L'utilisation systématique des comptages d'étoiles est un outil puissant pour cartographier les nuages moléculaires proches. Ces cartes ont déjà révélé de nouveaux nuages, tel un sixième nuage d'une masse d'environ 10 000 masses solaires dans la constellation du Loup. Gageons que les données de DENIS, dont les observations continueront jusqu'en 2000, révéleront d'autres surprises.

Laurent CAMBRÉSY, Obs. de Meudon

Calcul verbal

Notre cerveau traite différemment calcul exact et calcul approché.

Les ordinateurs calculent par des méthodes différentes, et dans des zones différentes des microprocesseurs, avec des entiers ou avec des multiples de puissances de dix positives ou négatives (les nombres «à virgule flottante»). Les informaticiens ignoraient que leurs propres capacités de calcul suivent aussi deux chemins différents : lorsque nous souhaitons donner un résultat exact, nous utilisons des circuits neuronaux associés au langage, tandis que la production d'un résultat approximatif repose sur un «sens des nombres» de type analogique.

Des personnes atteintes de lésions cérébrales ne peuvent répondre à la question simple «neuf est-il plus proche de dix ou de cinq?», bien qu'elles récitent sans problème des tables de multiplication. À l'opposé, des individus incapables d'additionner deux et deux savent toutefois que le résultat est plus proche de trois que de neuf. Par ailleurs, des enfants de six mois, qui ne savent ni compter ni parler, manifestent un sens des quantités : ils sont surpris lorsque trois marionnettes passent derrière un rideau et quand il n'en reste qu'une une fois le rideau levé. Ces quelques indices, parmi d'autres, incitent à penser que nous pouvons manipuler des nombres sans savoir compter, et que cette manipulation sollicite des capacités différentes de celles du calcul exact.

Pour tester ces hypothèses, Stanislas Dehaene et ses collègues du Centre hospitalier Frédéric Joliot d'Orsay et de l'Institut de technologie du Massachusetts ont entraîné des bilingues au calcul mental, dans l'une de leurs deux langues. Ils leur ont appris à choisir, entre deux solutions possibles, le résultat exact ou le plus proche d'une série d'additions en base dix, en base six ou en base huit, ou la valeur approchée du logarithme à base deux ou de la racine cubique de plusieurs nombres.

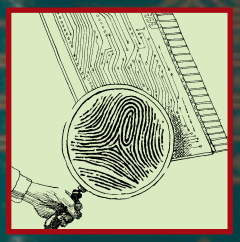
Premier résultat, encourageant pour les écoliers, l'entraînement améliore les performances dans tous les exercices : le temps de réponse diminue. Cette amélioration est-elle transférable dans l'autre langue? Pour le calcul exact, la réponse arrive toujours beaucoup plus vite dans la langue d'entraînement : on retrouve le fait, souvent rapporté, que les bilingues comptent préférentiellement dans la langue où ils ont d'abord appris à le faire. Pour les calculs approchés, en revanche, l'entraînement dans une seule langue réduit le temps moyen de réponse dans les deux langues.

On obtient le même résultat lorsque, plutôt que la langue, on change les nombres sur lesquels portent les opérations : pour les approximations, l'amélioration est conservée, mais pas pour le calcul exact. Le bénéfice de l'entraînement reposerait donc sur la mémorisation des résultats exacts, dans la langue où ils sont appris, tandis que, pour les approximations, le processus de réflexion lui-même semble accéléré.

L'observation, en imagerie par résonance magnétique, des zones du cerveau actives pendant les calculs et le suivi de cette activité en temps réel par électroencéphalographie (on détecte l'activité électrique à la surface du crâne) confirment que nous traitons très différemment les deux types de calculs . Notamment, le calcul exact active fortement, dans le lobe frontal inférieur gauche, une zone stimulée aussi par des exercices linguistiques, telles des associations sémantiques entre des mots. Nous utilisons dans ce cas les tables d'addition et de multiplication que nous avons apprises verbalement, et nous retenons sous la même forme les résultats des opérations : l'entraînement n'est pas facilement transférable à de nouveaux exercices (nous n'avons pas enregistré l'association nécessaire entre le problème et la solution), ni à une autre langue. En revanche, le calcul approché fait appel, dans les deux lobes pariétaux, à des zones actives aussi lorsque nous manipulons mentalement des objets, ou, plus étrangement lorsque nous bougeons les mains : ferions-nous inconsciemment des approximations sur nos doigts?

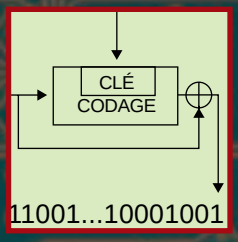
Dossier

La sécurité sur l'Internet



Pirates sur l'Internet

par Carolyn Meinel

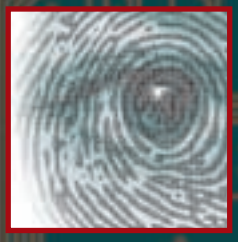


Cryptographie et réseau

par Philip Zimmermann

Le paiement sur l'Internet

par Octavian Ureche et Réjean Plamondon



Pour la libéralisation de la cryptographie

par Ronald Rivest

En février 1998, des pirates informatiques s'introduisent, par le réseau Internet, dans plusieurs réseaux d'ordinateurs de l'armée et de la marine américaines. Ces intrusions semblent avoir été faites par deux adolescents de Californie qui cherchaient à accéder à des informations confidentielles sur les équipages, le personnel et les soldes des militaires (pendant un temps, le Pentagone a cru que ces attaques étaient commanditées par Saddam Hussein). Ces agressions électroniques ne sont pas rares : au cours de l'année 1998, deux tiers des entreprises surveillées par les services américains de contre-espionnage ont été victimes de violations informatiques.

Dans ce dossier, des experts décrivent les techniques mises en œuvre pour déjouer les manœuvres des indésirables, des cambrioleurs et des indiscrets. Des systèmes nommés «pare-feu informatiques» détectent et arrêtent les intrus ; si ces défenses cédaient, des techniques de cryptographie assureraient néanmoins le secret des données.

Ces techniques de cryptographie permettent aussi l'émission de messages secrets sur le réseau Internet ainsi que le paiement sécurisé. La sécurité informatique est un atout pour la préservation des richesses accessibles par le réseau Internet.

Pirates sur l'Internet

CAROLYN MEINEL

Les pirates informatiques emploient un arsenal varié pour commettre leurs méfaits. Pourtant, aucun d'eux n'est invincible.

La fiction qui suit présente des techniques et des logiciels réels. Certains des événements relatés ici sont issus de mes propres expériences. Je remercie le fournisseur d'accès Rt66 Internet *qui a testé la plupart des logiciels décrits dans cet article.*

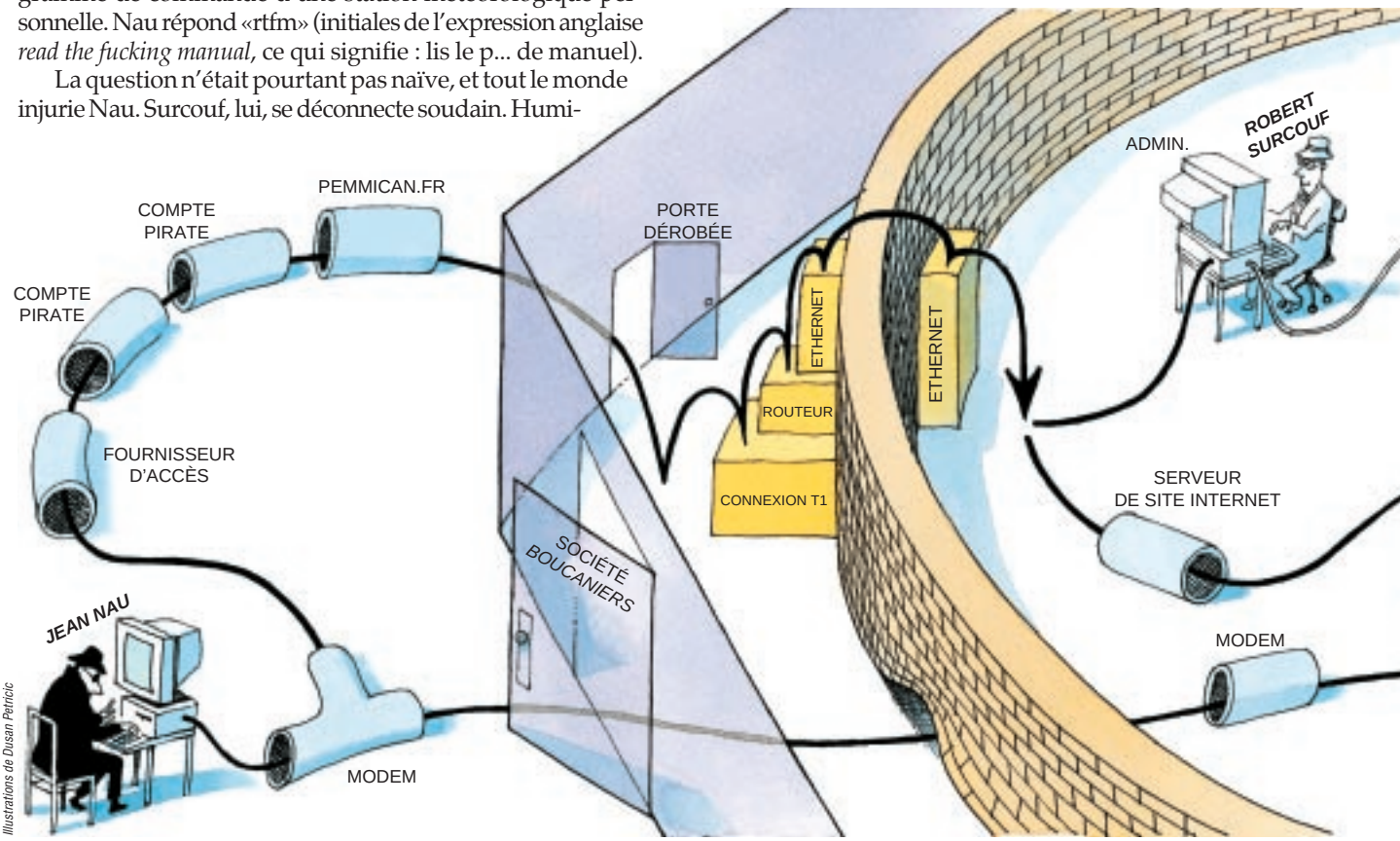
La nuit est tombée depuis longtemps quand, face à son ordinateur, Jean Nau se connecte sur le réseau Internet à un «système de causette» où chaque utilisateur introduit des remarques et lit celles des autres en temps réel. Dans la zone de dialogue consacrée au puissant système d'exploitation *Unix*, il observe les habitués : leurs contacts, leurs alliances, leurs échanges de connaissances. Ces échanges ressemblent à ceux qui avaient sans doute lieu dans les tavernes de l'île de la Tortue après un abordage réussi.

Imbu de ses compétences informatiques, Nau attend l'occasion – par exemple, une question naïve – de provoquer une bagarre verbale. Il saisit sa chance lorsqu'un certain Robert Surcouf demande si quelqu'un sait comment écrire un programme de commande d'une station météorologique personnelle. Nau répond «rtfm» (initiales de l'expression anglaise *read the fucking manual*, ce qui signifie : lis le p... de manuel).

La question n'était pourtant pas naïve, et tout le monde injurie Nau. Surcouf, lui, se déconnecte soudain. Humilié, Nau veut sa revanche. Il obtient rapidement l'adresse électronique surcouf@boucanier.fr, puis apprend que Surcouf est l'administrateur du réseau informatique boucanier.fr.

Grâce au logiciel *Strobe*, Nau essaie de se connecter à chacun des milliers de ports virtuels, c'est-à-dire des canaux de connexion, de boucanier.fr. Sur certains ports, un programme nommé *Démon* répond automatiquement. Découvrira-t-il une faille dans l'un d'eux ?

Tentative après tentative, le logiciel *Strobe* rencontre un mur, le «pare-feu» de Surcouf ; ce logiciel puissant lit l'entête de chaque message, par exemple une tentative du logiciel *Strobe*, et identifie sa destination. Le pare-feu rejette ou accepte les messages en fonction de règles d'accès définies. Face à *Strobe*, il réagit en envoyant des données dépourvues de sens, jusqu'à saturer l'ordinateur personnel de Nau. Parallèlement, un courrier électronique est envoyé au fournisseur d'accès Internet de Nau : quelques minutes plus tard, Nau, soupçonné d'infraction informatique, est privé d'accès au réseau.

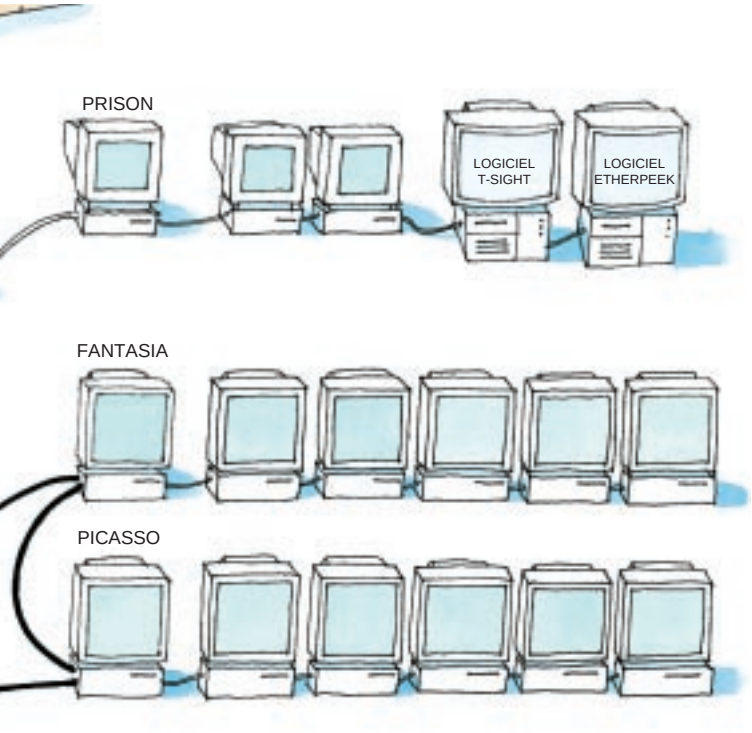


Illustrations de Dusan Petricic

Malgré la rapidité des représailles, Nau n'est pas neutralisé : ce n'est que l'un de ses nombreux comptes piratés qui est clôturé. La fermeture de ce compte l'élimine de la causette, où il apparaît comme un cuistre ou un lâche. Il est temps d'utiliser une autre arme : un scanner de ports furtif.

Ce programme est plus subtil que *Strobe*, car il manipule les informations échangées lors des communications entre les ordinateurs. Lorsqu'un ordinateur souhaite transmettre un message, il envoie tout d'abord un signal nommé SYN, destiné à la synchronisation des deux ordinateurs. Le programme qui le reçoit répond par un double signal (un d'accord, ACK, et un de synchronisation, SYN), et par une valeur de temporisation qui sera utilisée pour régler la transmission des données *(voir la figure 4)* et, en outre, ralentir le temps de réaction de l'ordinateur émetteur. Ce dernier envoie enfin un signal d'accord, ACK ; puis les salutations achevées, il transmet son message, qui se termine par un signal FIN. Le destinataire retourne alors un signal d'accord, pour indiquer qu'il a bien reçu le message.

Un scanner de ports furtif ne respecte pas ce protocole *(voir la figure 2)* : il envoie un signal FIN prématuré à plusieurs canaux de connexion de l'ordinateur récepteur. De ce fait, le programme récepteur n'envoie aucune réponse, mais il transmet sur chaque canal un signal RST pour demander de recommencer la procédure. Ce signal RST, contrairement aux signaux ACK et SYN est caractéristique de l'ordinateur qui l'envoie : il fournit des informations importantes au pirate, telles le type d'ordinateur et les démons en service. Cependant, sans les triples salutations, il n'identifie aucune connexion et n'enregistre pas la transmission dans ses comptes rendus d'opérations. Le scanner de port furtif sonde un ordinateur en toute discrétion.



1. MALGRÉ LES PUISSANTS LOGICIELS DE DÉFENSE, par exemple les pare-feu qui stoppent les intrus non autorisés, les systèmes informatiques connectés au réseau Internet ont presque toujours plusieurs points faibles que les pirates exploitent.

Sur un site du réseau Internet, Nau trouve un scanner de port furtif performant écrit en langage C. Nau doit le compiler, c'est-à-dire le traduire dans le langage de son ordinateur. Cependant, chaque version d'*Unix* est unique, et Nau n'a jamais étudié la programmation. Il n'en a jamais eu besoin, car tous les logiciels qu'un pirate désire sont en libre-service gratuit sur le réseau Internet. Reste à savoir les traduire.

Le jeune Surcouf a suivi un parcours différent. Un ami technicien lui a appris comment gérer un système informatique. Puis il s'est perfectionné en affrontant son ami dans des jeux d'attaque et de défense de systèmes informatiques. Ils ont ensuite aidé le fournisseur d'accès Internet à renforcer sa propre sécurité. Surcouf a alors été embauché à temps partiel, en parallèle avec des études d'informatique.

Nau le pirate a donc commis sa première erreur : attaquer Surcouf, corsaire confirmé.

Le repérage des lieux

Au petit matin, Nau a traduit le programme. En quelques minutes, le scanner de ports furtifs lui fournit la liste des services proposés par boucanier.fr à des personnes dûment répertoriées. Un programme assurant la sécurité de l'interpréteur des commandes – pour qu'elles soient exécutables – grâce à des connexions codées et un serveur de site Internet retiennent son attention. Le cœur de Nau s'accélère. Un canal de connexion s'est entrouvert au moment de son examen. Un autre intrus l'a-t-il précédé? A-t-il maintenu une porte dérobée pour pénétrer dans le système?

La sonnerie d'un messager de poche réveille Surcouf. Un programme de détection nommé *Etherpeek*, installé sur le réseau d'ordinateurs boucanier.fr, a décelé l'examen des canaux de connexion par Nau. Surcouf se précipite au bureau et, assis devant sa station de travail (un ordinateur performant), il fait le guet. Installés uniquement sur son propre ordinateur, ses meilleurs programmes de défense ne fonctionnent que lorsqu'il est aux commandes, afin d'éviter tout assaut de l'extérieur. Cependant, Surcouf n'observe aucune manœuvre : malgré la tentation, Nau, guidé par son intuition de pirate, a abandonné l'assaut.

Tout de même intrigué, Surcouf analyse les comptes rendus d'opérations de son ordinateur et retrouve l'adresse du message pirate. Par courrier électronique, il informe le fournisseur d'accès de Nau de la tentative d'effraction et lui demande des informations sur le compte du pirate. La clause de confidentialité des clients empêche la requête d'aboutir.

Toutefois, trois soirs plus tard, Nau découvre que son mot de passe n'est plus valable : son fournisseur d'accès lui apprend que son compte a été supprimé parce qu'il a utilisé un scanner de ports furtif.

Plus déterminé que jamais, Nau revient quelques minutes plus tard sur le réseau Internet grâce à un téléphone et à une carte bancaire. Il doit être prudent. De ce nouveau compte, il se connecte sur un de ses comptes piratés chez un autre fournisseur d'accès, et il apprend que le site informatique boucanier.fr appartient à la Société *Boucaniers*, qui produit de la viande fumée.

Nau tente alors de se connecter au réseau boucanier.fr par le canal inhabituel repéré trois nuits plus tôt. La réponse

est cinglante : «Espèce de marin d'eau douce ! Pensais-tu vraiment trouver un passage secret ?» Puis le programme associé au canal transmet des données incohérentes et envoie un courrier électronique au système administrateur du fournisseur d'accès dénonçant la tentative de piratage. Quelques minutes plus tard, la connexion de Nau est supprimée.

Mieux vaut contourner le pare-feu sur la pointe des pieds plutôt que de le passer en force. D'un autre compte, également piraté, Nau tente, par une simple commande saisie sur le clavier, de dresser la liste des ordinateurs du réseau boucanier.fr.

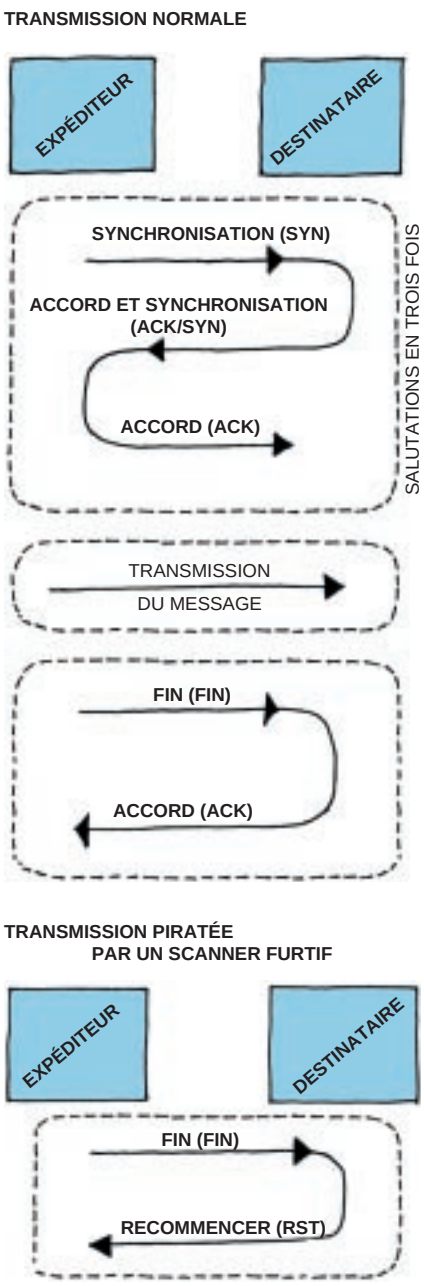
La commande ne fournit aucun résultat utilisable : Surcouf a probablement configuré le réseau de sorte que les données adressées à n'importe quel ordinateur transitent d'abord par un programme central, qui les redistribue ensuite. Cette méthode empêche les intrus d'accéder à l'intérieur du pare-feu.

Après avoir converti l'adresse informatique boucanier.fr en un nombre, Nau utilise un scanner d'adresses informatiques, puis il teste les 50 adresses numériques immédiatement inférieures et supérieures. Peut-être appartiennent-elles à des ordinateurs du réseau boucanier.fr, car les adresses numériques des ordinateurs d'un réseau sont souvent proches ? Hélas, non.

Avec une autre commande, il découvre alors un second réseau appartenant à la Société *Boucaniers* : boucanum.fr, dont l'adresse numérique est éloignée de celle de boucanier.fr. Le scanner d'adresses découvre alors cinq ordinateurs dont l'adresse est numériquement proche de celle du réseau boucanum.fr.

Par précaution, Nau se connecte de son compte piraté à un autre compte piraté et, de là, vers un autre compte, d'où il exécute d'autres scanners de ports furtifs. Ces étapes supplémentaires engorgeront toute procédure judiciaire, puisque celle-ci nécessiterait trois mandats de perquisition. Échaudé, il utilise également un programme nommé *Root kit*, grâce auquel il effacera toute trace de son activité dans les comptes rendus utilisés pour détecter les activités douteuses et les modifications des fichiers de configuration de cet ordinateur.

De son galion, Nau examine les ordinateurs de boucanier.fr et de boucanum.fr connectés au réseau Internet. Le scanner de ports furtif se glisse au



2. LES TRANSMISSIONS DE MESSAGES obéissent à un protocole rigide. L'expéditeur envoie un signal de synchronisation (SYN) des communications à venir *(en haut)*. Le destinataire retourne alors un double signal (ACK/SYN) d'accord et de synchronisation pour accepter la demande. Enfin, l'expéditeur envoie à son tour un signal d'accord (ACK). Le message lui-même est alors transmis. Un signal de fin (FIN) le suit de peu. Le destinataire répond par un autre signal d'accord qui clôt définitivement la correspondance. Un pirate corrompt cet échange *(en bas)* en envoyant immédiatement un signal FIN auquel le destinataire est obligé de répondre par un signal pour recommencer (RST). La réponse – ou l'absence de réponse – fournit des informations sur le destinataire. Cependant, l'absence des triples salutations empêche la transmission d'être enregistrée dans les comptes rendus du destinataire. Le pirate sonde ainsi un ordinateur avec une certaine discrétion.

travers du pare-feu vers chacun d'eux. Cependant la manœuvre a été détectée par le programme *Etherpeek*, qui prévient à nouveau Surcouf.

Celui-ci déboule dans son bureau ; il identifie rapidement l'origine du scanner et alerte l'administratrice du système du troisième compte de Nau. Cependant, le programme *Root kit* dissimule Nau, qui continue avec impudence, grâce au scanner furtif et au logiciel *Strobe*, de chercher une adresse informatique non protégée par le pare-feu. Celui-ci ne fait que lui transmettre un flot de données incohérentes.

Cet afflux soudain convainc l'administratrice du compte de Nau qu'un agresseur est à l'œuvre. Elle déconnecte alors tout le système du réseau : la connexion de Nau s'arrête dans un sifflement.

À la recherche d'horaires décalés

Nau suppose alors que de nombreuses stations de travail non connectées au réseau boucanier.fr sont utilisées par des employés de la Société *Boucaniers* pour travailler chez eux. Ces ordinateurs, reliés directement, ne sont pas protégés par le pare-feu. La probabilité est grande : avec un modem, n'importe qui peut relier un ordinateur personnel à une ligne téléphonique.

Grâce à un logiciel de numérotation téléphonique automatique nommé *Shokdial*, Nau appelle chacune des lignes téléphoniques de la Société *Boucaniers*. Au siège de la société, les gardiens de nuit entendront sonner successivement les postes sans comprendre de quoi il retourne.

À 2 heures 57, un modem répond au programme *Shokdial* : Nau est alors face à une station de travail de la marque *Silicon Graphics* : «Boucaniers SA. Département mercatique. Irix 6.3» (*Irix* est une forme d'*Unix*). Nau a enfin trouvé une porte d'accès au fief de Surcouf.

Assez d'élégance ; Nau décide d'utiliser la force. Il exécute un programme qui se connecte autant de fois que nécessaire pour découvrir le mot de passe d'un compte administrateur, c'est-à-dire un accès sans restrictions dans ses possibilités d'action, duquel il pourra agir en toute liberté. Le possesseur de cet ordinateur *Irix* aura peut-être autorisé la connexion à distance sur le compte administrateur.

La recherche de mot de passe commence avec les mots et les noms courants,

puis le programme teste des groupes de signes moins naturels ; l'exploration peut durer des mois, voire des années. Cependant Nau est chanceux. Vers 5 heures, le prénom «Nancy» est identifié : le compte administrateur est accessible!

Nau est ravi. Il crée une fenêtre de dialogue entre lui et le système d'exploitation de l'ordinateur, d'où il dispose des mêmes pouvoirs que l'administrateur. Puis il renforce sa position en transférant un programme *Root kit* pour la discrétion et un programme *Sniffer* sur l'ordinateur de sa nouvelle victime : toute saisie et toute connexion seront enregistrées par le programme *Sniffer* dans un fichier dissimulé. Le programme *Root kit* permet également de créer un chemin d'accès supplémentaire que Nau baptise «revanche» ; mot de passe «MoRtSurCf».

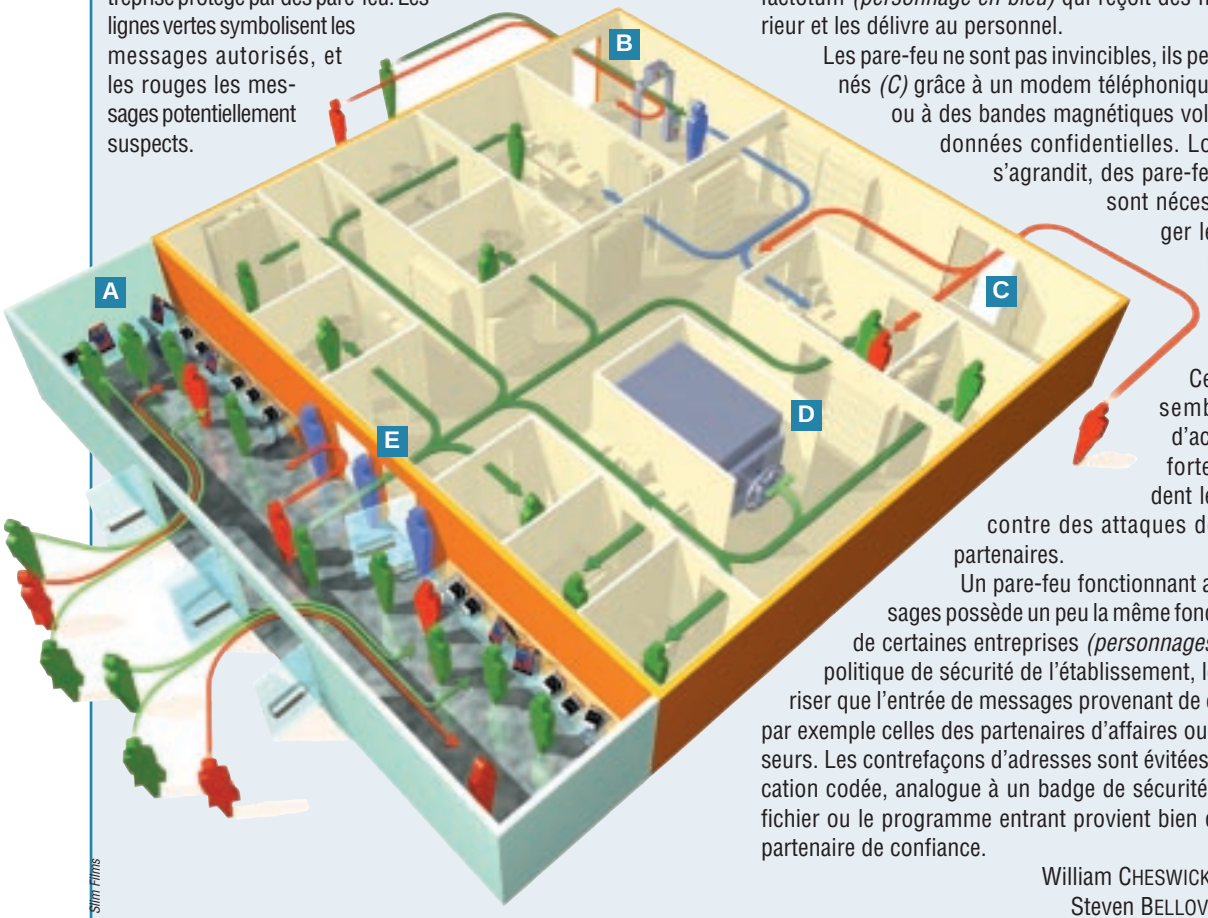
Nau termine sa nuit en déterminant que le compte administrateur auquel il a accédé est connecté sur l'ordinateur picasso du réseau boucanum.fr. Grâce au programme *Root kit*, l'utilisateur normal de l'ordinateur picasso ne remarquera pas que son ordinateur est maintenant commandé par quelqu'un d'autre. Surcouf ne détecte qu'une tentative d'intrusion dans boucanum.fr à partir du réseau Internet. Ce nouvel incident l'inquiète, mais, faute d'informations suffisantes, il ne peut rien faire.

Deux nuits plus tard, Nau se connecte sur l'ordinateur picasso et examine les comptes rendus du programme *Sniffer*. Toutes les informations concernant le trafic interne du réseau sont codées, mais le programme *Sniffer* a enregistré la connexion de quelqu'un, de l'ordinateur picasso sur un autre ordinateur du nom de fantasia.

Les pare-feu

Aucun réseau informatique relié au réseau Internet n'est invulnérable, mais des protections peuvent être installées. La première ligne de défense est le pare-feu, dont les deux types le plus fréquemment utilisés agissent soit au niveau des messages transmis, soit au niveau des logiciels. Le premier fonctionne sur une machine nommée routeur. Il examine dans chaque message entrant ou sortant les adresses de la source et de la destination, qu'il compare à des règles d'accès. Les messages autorisés sont transmis, les autres sont bloqués. Le second examine les adresses et le contenu des messages. Plus lent qu'un filtre de messages, il permet toutefois une politique de sécurité plus raffinée.

L'illustration représente un réseau informatique d'entreprise protégé par des pare-feu. Les lignes vertes symbolisent les messages autorisés, et les rouges les messages potentiellement suspects.



Slim Films

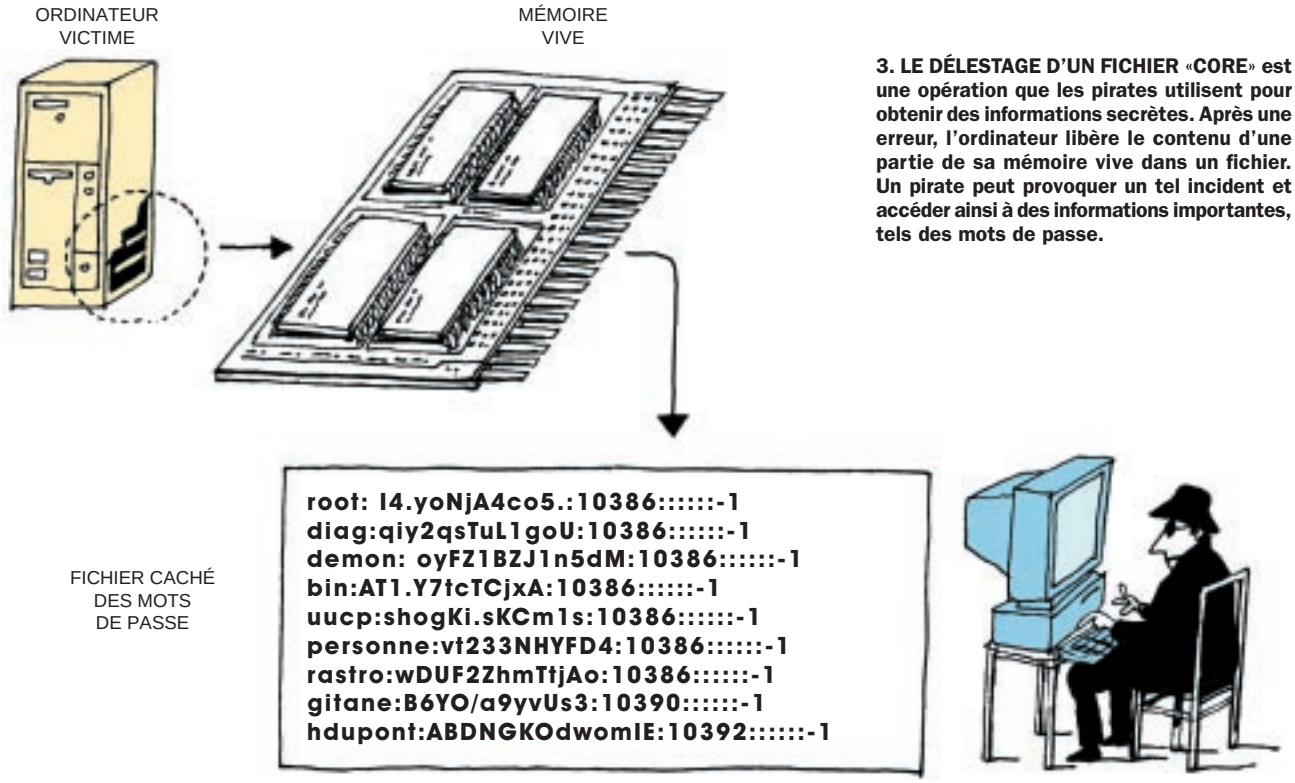
À l'extérieur du pare-feu *(en orange)*, l'entreprise possède un réseau accessible au public, qui permet aux clients d'envoyer des courriers électroniques vers l'entreprise ou de naviguer sur ses différents sites informatiques. Cette zone *(A)* est analogue à l'espace d'accueil réservé au public que l'on trouve à l'entrée de certains établissements : aucune information confidentielle n'y est présente.

Un pare-feu fonctionnant au niveau des logiciels ressemble aux salles de police des aéroports *(B)* : les courriers électroniques sont inspectés. Les programmes reçus par le réseau Internet, qui peuvent contenir des instructions néfastes, sont envoyés sur un serveur mandataire, puis à un programme mandataire qui fonctionne en toute sécurité sur le réseau. Un programme mandataire est l'analogue du factotum *(personnage en bleu)* qui reçoit des messages de l'extérieur et les délivre au personnel.

Les pare-feu ne sont pas invincibles, ils peuvent être contournés *(C)* grâce à un modem téléphonique, à des disquettes ou à des bandes magnétiques volées, contenant des données confidentielles. Lorsque l'entreprise s'agrandit, des pare-feu supplémentaires sont nécessaires pour protéger les systèmes informatiques de services importants, tel celui de la comptabilité. Ces protections ressemblent à la porte d'acier d'une chambre forte *(D)* ; elles défendent les systèmes vitaux contre des attaques de l'intérieur ou de partenaires.

Un pare-feu fonctionnant au niveau des messages possède un peu la même fonction que les gardes de certaines entreprises *(personnages en bleu)*. Selon la politique de sécurité de l'établissement, le filtre peut n'autoriser que l'entrée de messages provenant de certaines adresses, par exemple celles des partenaires d'affaires ou celles des fournisseurs. Les contrefaçons d'adresses sont évitées par une authentification codée, analogue à un badge de sécurité, qui assure que le fichier ou le programme entrant provient bien d'une adresse d'un partenaire de confiance.

William CHESWICK, Laboratoires *Bell*
Steven BELLOVIN, *AT&T Research*

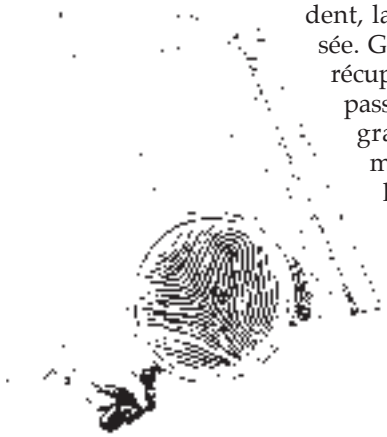


3. LE DÉLESTAGE D'UN FICHIER «CORE» est une opération que les pirates utilisent pour obtenir des informations secrètes. Après une erreur, l'ordinateur libère le contenu d'une partie de sa mémoire vive dans un fichier. Un pirate peut provoquer un tel incident et accéder ainsi à des informations importantes, tels des mots de passe.

Nau passe maintenant à l'abordage d'une nouvelle zone du réseau.

Cet ordinateur fantasia est une station de travail de type SPARC, utilisée pour la création d'animations en images de synthèse, peut-être des génériques pour la télévision. C'est certainement un serveur auquel accèdent de nombreux autres ordinateurs. Nau cherche un fichier de mots de passe. Peut-être en trouvera-t-il certains valables sur d'autres ordinateurs à l'intérieur du réseau de la société.

Il localise ce fichier, mais n'y trouve que des «x» : l'information est probablement dissimulée ailleurs. Peu importe : utilisant le protocole de transfert de fichiers, Nau provoque une erreur qui oblige fantasia à transférer une partie de sa mémoire vive dans le compte que Nau s'est créé. Cette procédure est un «délestage de fichier core» *(voir la figure 3)*, qui permet normalement aux programmeurs de découvrir des indices lors d'une panne de programme. Des mots de passe codés sont parfois stockés dans la mémoire vive. Lors d'une connexion, l'ordinateur code le mot de passe saisi par l'utilisateur et le compare aux mots de passe déjà codés du fichier caché. Lorsque les deux coïncident, la connexion est autorisée. Grâce au délestage, Nau récupère le fichier de mots de passe codés. Il lance son programme de recherche de mots de passe : il va falloir patienter...



Impatient, Nau élabore déjà sa prochaine manœuvre. Avec un système d'exploitation *Unix*, lorsqu'un programme fournit trop de données à un espace de mémoire temporaire, nommé tampon, les informations en excès dépassent la capacité du tampon et s'écoulent dans d'autres zones de la mémoire de l'ordinateur. Nau utilise ces dépassements de capacité *(voir la figure 5)* pour introduire dans la station de travail SPARC un programme grâce auquel il peut exécuter d'autres commandes et d'autres programmes. Ravi de son dernier forfait, Nau installe un autre programme *Sniffer* et un autre *Root kit*. Ce dernier ne masquera son œuvre qu'une fois activé ; le forban efface donc les traces de ses premières activités.

Une dernière chose à faire encore. Quelqu'un est-il autorisé à se connecter sur fantasia à partir du réseau Internet? D'une simple commande qui affiche l'enregistrement de toutes les connexions sur fantasia, Nau constate que des utilisateurs prénommés nancy et vangogh sont récemment entrés sur fantasia par le réseau à partir du site pemmican.fr, qui se situe en dehors du pare-feu de la Société *Boucaniers*. Au matin, Nau s'effondre, terrassé par le sommeil, mais satisfait : bientôt, il vaincra la Société *Boucaniers*.

La mise à mort

Le lendemain soir, Nau se présente sous une fausse adresse informatique chez pemmican.fr. Puis, en testant des signaux de synchronisation sur pemmican.fr, il détermine la valeur de temporisation qu'utilise pemmican.fr et falsifie sa propre origine. Il installe alors un programme *Sniffer* sur pemmican.fr et un interpréteur sécurisé pour se connecter en toute sécurité sur fantasia. Une commande lui fournit la liste des connexions actives à l'intérieur du réseau de la Société *Boucaniers*, où il découvre un nouvel ordinateur : «admin.boucanier.fr». L'ordinateur de Surcouf?

Parallèlement, Nau essaie chaque nouveau mot de passe et le nom d'utilisateur associé, découverts par son programme de recherche sur les ordinateurs du site boucanier.fr. Hélas, aucun ne fonctionne ailleurs que sur fantasia, qu'il a déjà conquis.

Cependant, cette déconvenue est largement compensée par fantasia, qui lui fournit l'enregistrement de ce qu'a tapé l'utilisateur vangogh lorsqu'il a mis à jour la page Internet de la société. Nau y trouve le mot de passe nécessaire au piratage de la page Internet de la Société *Boucaniers*. Par ailleurs, son programme *Sniffer* installé sur l'ordinateur picasso lui indique qu'une certaine Nancy a utilisé cet ordinateur pour se connecter par une porte dérobée sur le compte administrateur d'admin.boucanier.fr, dissimulée derrière un programme *Root kit*.

Il se glisse juste derrière elle et essaie de se connecter sur tous les ordinateurs de boucanier.fr. Hélas, Surcouf a été prudent : sur le réseau boucanier.fr, même les pouvoirs d'administrateur n'autorisent pas l'accès à d'autres ordinateurs sans nouveaux mots de passe. Nau est bloqué. Il retourne à l'assaut du site Internet. De son propre ordinateur, il installe une nouvelle version du site spécialement préparée.

La quarantaine de Java

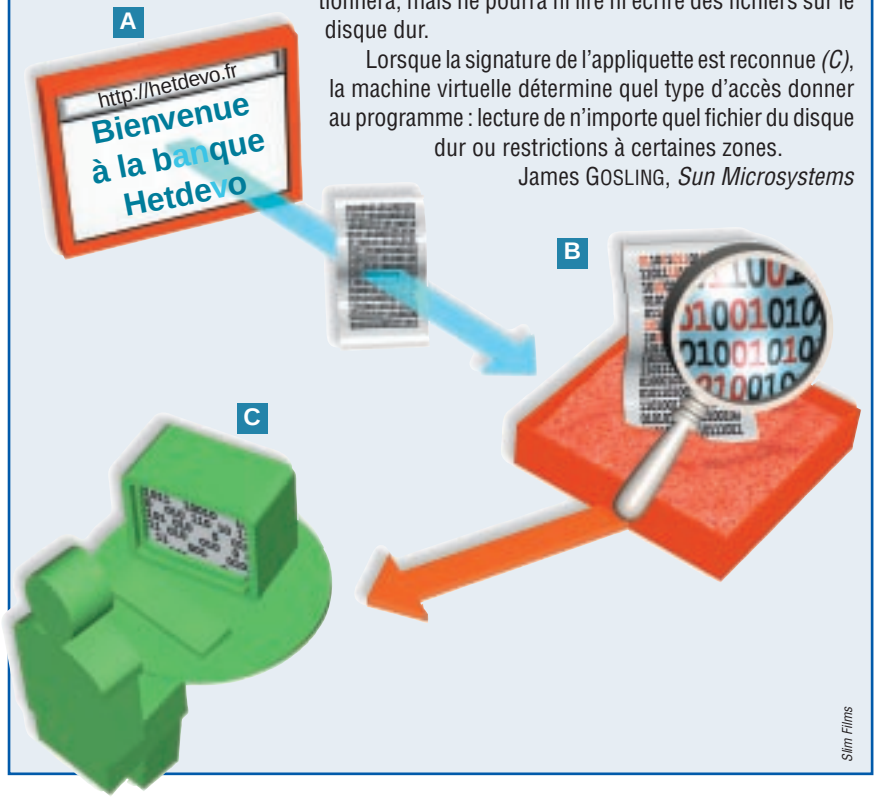
Le langage Java est utilisé par les programmeurs pour écrire de petits programmes, ou appliquettes, qui peuvent être récupérés sur le réseau Internet ou sur d'autres réseaux d'ordinateurs. Un individu peut toutefois créer une appliquette malveillante qui efface des fichiers, vole des données ou injecte un virus. Cependant, le langage Java a prévu une sécurité : il s'agit d'un ensemble de logiciels, nommé machine virtuelle Java, indispensable à l'exécution de n'importe quelle appliquette.

Lorsqu'un utilisateur récupère une appliquette *(A)*, par exemple un programme de gestion bancaire, la machine virtuelle empêche l'accès au disque dur, au réseau et à d'autres ressources vitales. L'appliquette se trouve alors en une sorte de quarantaine, d'où elle ne peut provoquer aucun dommage. L'appliquette n'est libérée que lorsque la machine virtuelle a vérifié qu'elle provenait d'une source de confiance.

En premier lieu, un vérificateur de code détermine si l'appliquette est écrite dans une syntaxe Java correcte *(B)*. Quand ce n'est pas le cas, le programme ne pourra pas être utilisé. Ensuite, la machine virtuelle recherche une signature numérique, associée à l'appliquette qui identifie la personne ou l'organisme créateur et révèle toute altération. En cas de signature invérifiable, l'appliquette restera en quarantaine. Le programme fonctionnera, mais ne pourra ni lire ni écrire des fichiers sur le disque dur.

Lorsque la signature de l'appliquette est reconnue *(C)*, la machine virtuelle détermine quel type d'accès donner au programme : lecture de n'importe quel fichier du disque dur ou restrictions à certaines zones.

James GOSLING, *Sun Microsystems*



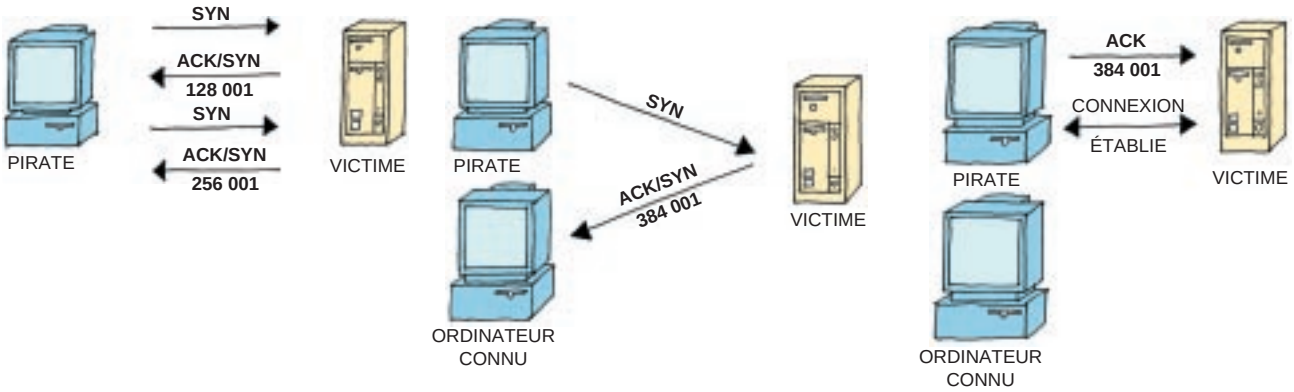
Aujourd'hui, Surcouf travaille tard, il étudie les comptes rendus où apparaît un nombre inhabituel de connexions par le système commercial. Que s'est-il passé? L'aide de l'administratrice du système de pemmican.fr, une collègue qui lui est redevable, l'aidera sûrement.

La sonnerie du téléphone retient Surcouf au moment de partir. Un client se plaint de la séquence pornographique affichée sur le site Internet de la Société *Boucaniers*. Après vérification, Surcouf débranche rapidement le câble Ethernet, le cordon ombilical qui relie la société au réseau Internet.

Nau enrage de voir son chef-d'œuvre d'obscénité détruit aussi vite. Il s'inquiète également d'avoir laissé autant de traces derrière lui : il se connecte par modem sur l'ordinateur picasso – un accès qu'ignore Surcouf – et reformate complètement le disque dur de l'ordinateur d'administration du système. Le système de la société est hors service. Surcouf ne rassemblera aucun indice. Surcouf redémarre rapidement l'ordinateur d'administration, mais c'est trop tard : il devra complètement réinstaller les logiciels. Cependant, Nau ignore qu'un programme de détection *Etherpeek*, installé sur un des ordinateurs du réseau, a enregistré ses activités...

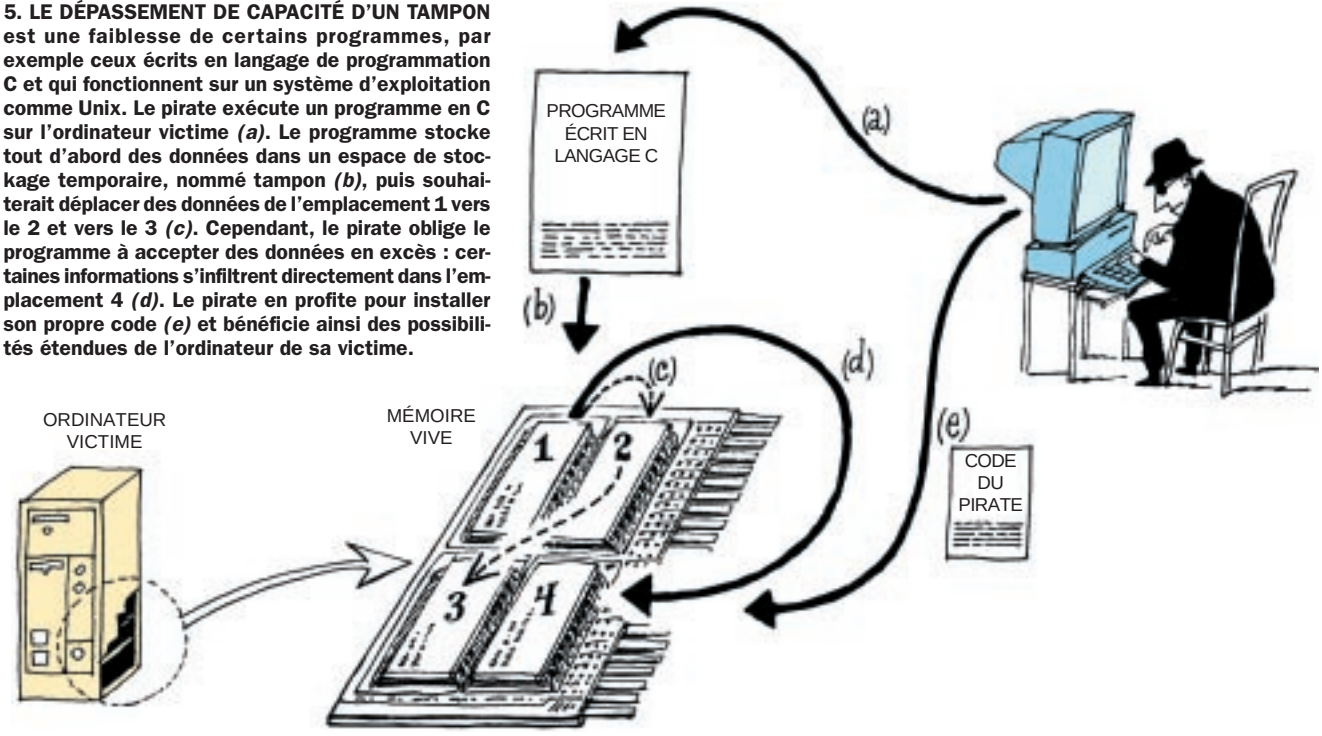
Nau est irrité : il noie boucanier.fr sous un flot de données. Peu après, Surcouf reçoit la plainte d'une représentante de la société qui n'arrive pas à se connecter sur le serveur de courrier électronique.

Le lendemain, Surcouf, exténué, demande au directeur technique de la Société *Boucaniers* l'autorisation de nettoyer complètement tous les ordinateurs du réseau et de changer les mots de passe. Cependant, une telle mesure, bien que prudente, nécessiterait l'arrêt du système pour plusieurs jours. Le directeur refuse.



4. UNE ESCROQUERIE INTERNET permet au pirate de falsifier son identité. Il teste d'abord sa victime en lui envoyant de multiples signaux de synchronisation (SYN) pour obtenir, en réponse, un double signal d'accord et de synchronisation (ACK/SYN), et une valeur de temporisation *(à gauche)* caractéristique d'un système d'exploitation. Cette valeur augmente ici de 128 000 à chaque échange. Le pirate envoie ensuite de nombreux signaux de synchronisation dont un est identique à celui d'un ordinateur connu de la victime, qui transmet alors un double signal d'accord et de synchronisation à cet ordinateur autorisé *(au centre)*. Le pirate ne reçoit pas cette réponse, mais poursuit la correspondance. Il délivre un signal d'accord avec la valeur de temporisation correcte : la communication entre son ordinateur et sa victime est établie *(à droite)*. Le piratage commence

5. LE DÉPASSEMENT DE CAPACITÉ D'UN TAMPON est une faiblesse de certains programmes, par exemple ceux écrits en langage de programmation C et qui fonctionnent sur un système d'exploitation comme Unix. Le pirate exécute un programme en C sur l'ordinateur victime *(a)*. Le programme stocke tout d'abord des données dans un espace de stockage temporaire, nommé tampon *(b)*, puis souhaiterait déplacer des données de l'emplacement 1 vers le 2 et vers le 3 *(c)*. Cependant, le pirate oblige le programme à accepter des données en excès : certaines informations s'infiltrent directement dans l'emplacement 4 *(d)*. Le pirate en profite pour installer son propre code *(e)* et bénéficie ainsi des possibilités étendues de l'ordinateur de sa victime.



Nau a franchi depuis longtemps la frontière légale du piratage. Néanmoins, la Direction de la surveillance du territoire, occupée par plusieurs affaires de piratage de réseaux d'ordinateurs des facultés et des grandes écoles ne peut aider Surcouf. Il doit rassembler seul les preuves.

Puisque le forban est resté connecté alors que le système n'était plus relié physiquement au réseau de l'Internet, Surcouf soupçonne l'existence d'un modem piraté dans les bureaux. Son propre numéroteur téléphonique automatique découvre bientôt la brèche utilisée par Nau.

Il réinstalle alors sur son ordinateur d'administration un système propre, puis met en place un logiciel antipirates, nommé *T-Sight*, qui contrôle tous les ordinateurs du réseau de la société. Surcouf prépare également un piège : le logiciel *T-Sight* guettera la prochaine connexion sur admin.boucanier.fr et dirigera l'intrus sur un ordinateur «prison» où le coupable sera maîtrisé et identifié. Surcouf, avec une équipe de programmeurs, camoufle sa prison en un système multi-utilisateurs et y place des données financières factices en guise d'appât.

Le comble de l'orgueil

Deux jours plus tard, à 20 heures 17, quelqu'un s'introduit dans l'ordinateur admin.boucanier.fr. C'est Nau! Pourquoi est-il revenu si tôt? Nau a beaucoup apprécié – il en a même ri aux larmes – que les pirates de l'informatique et les chaînes de télévision parlent de ses talents. Il se sent invincible. Erreur...

Trop pressé, il se connecte sans les précautions habituelles sur pemmican.fr, puis sur l'ordinateur fantasia. Appâté par le leurre, il se dirige rapidement vers la prison. Au comble de l'excitation, il examine ce qu'il croit être des données financières importantes.

De son côté, Surcouf analyse rapidement les informations fournies par le programme *T-Sight* et obtient le mot de passe que Nau utilise pour pirater fantasia. Il suit ainsi l'intrus jusqu'à pemmican.fr. L'administratrice de ce réseau, prévenue au restaurant par son téléphone portable, contacte Surcouf.

Pendant que Nau recopie un énorme fichier contenant des numéros de cartes bancaires factices, Surcouf installe un programme *Sniffer* sur pemmican.fr. et consulte le compte de Nau dans cet ordinateur, car il a négligemment utilisé le même mot de passe pour tous ses comptes. Quelques minutes avant que Nau ait fini de recopier le fichier et se déconnecte, Surcouf retrouve le fichier de cartes bancaires volé sur le compte souscrit par Nau.

Les informations obtenues suffisent à la Direction de la surveillance du territoire, qui contacte le fournisseur et obtient l'identité de Nau. Munie de ces preuves, dont les comptes rendus détaillés fournis par le programme *Etherpeek*, le bureau du juge d'instruction délivre un mandat d'arrêt.

L'appartement de Nau est perquisitionné, et son ordinateur confisqué. Le disque dur de l'ordinateur révélera tout, même ce qui a été effacé. Un laboratoire identifie ses violations passées, notamment celle d'une grande institution bancaire parisienne.

Nau est mis en examen pour piratage informatique. Au procès, face à une juge intransigeante, Nau tente de négocier un compromis, malgré les dizaines de milliers de francs de dégâts occasionnés. Peine perdue, Jean Nau, dit l'Olonnais, purge aujourd'hui une peine de deux ans d'emprisonnement.

Carolyn MEINEL est écrivain scientifique spécialiste du piratage informatique.

Philippe BLANCHARD, *Pirates de l'informatique : enquête sur les hackers français*, Vuibert, 1995.

Æleen FRISCH, *Les bases de l'administration système*, deuxième édition, O'Reilly, 1996.

Jean GUISNEL, *Guerres dans le cyberespace*, Découverte, 1997.

Craig HUNT, *TCP/IP, Administration de réseau*, deuxième édition, O'Reilly, 1998.

Cryptographie et réseau

PHILIP ZIMMERMANN

Les courriers électroniques et les diverses informations numériques envoyées sur le réseau Internet sont comme des cartes postales numériques : leur contenu n'est pas protégé. Des systèmes de cryptographie assurent le secret des transmissions électroniques.

L'acheminement des lettres par la poste prend parfois des jours, mais les enveloppes cachent le contenu des messages. À l'inverse, le courrier électronique arrive en un clin d'œil, mais il peut être lu par des indiscrets. Des systèmes de chiffrement peuvent toutefois assurer la confidentialité de telles transmissions : on mélange l'information de manière tellement complexe qu'elle devient inintelligible, excepté pour le destinataire légitime, qui connaît les règles du mélange.

Depuis les années 1980, les ordinateurs personnels sont si puissants qu'ils peuvent utiliser des systèmes cryptographiques naguère réservés aux militaires. Ces systèmes, très efficaces, résistent à toute tentative de «cassage».

Sortir de l'ombre

Avant le milieu des années 1970, l'Agence de sécurité américaine (NSA pour *National Security Agency*) avait le quasi-monopole de la cryptographie américaine ; les méthodes étaient confidentielles, connues seulement de quelques «hommes du chiffre». En 1976, un article intitulé *De nouvelles voies pour la cryptographie*, a ouvert la cryptographie