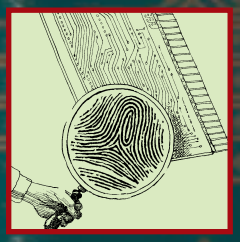
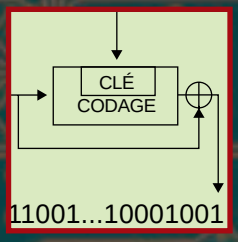
Dossier

La sécurité sur l'Internet



Pirates sur l'Internet

par Carolyn Meinel

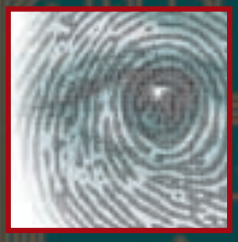


Cryptographie et réseau

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.*

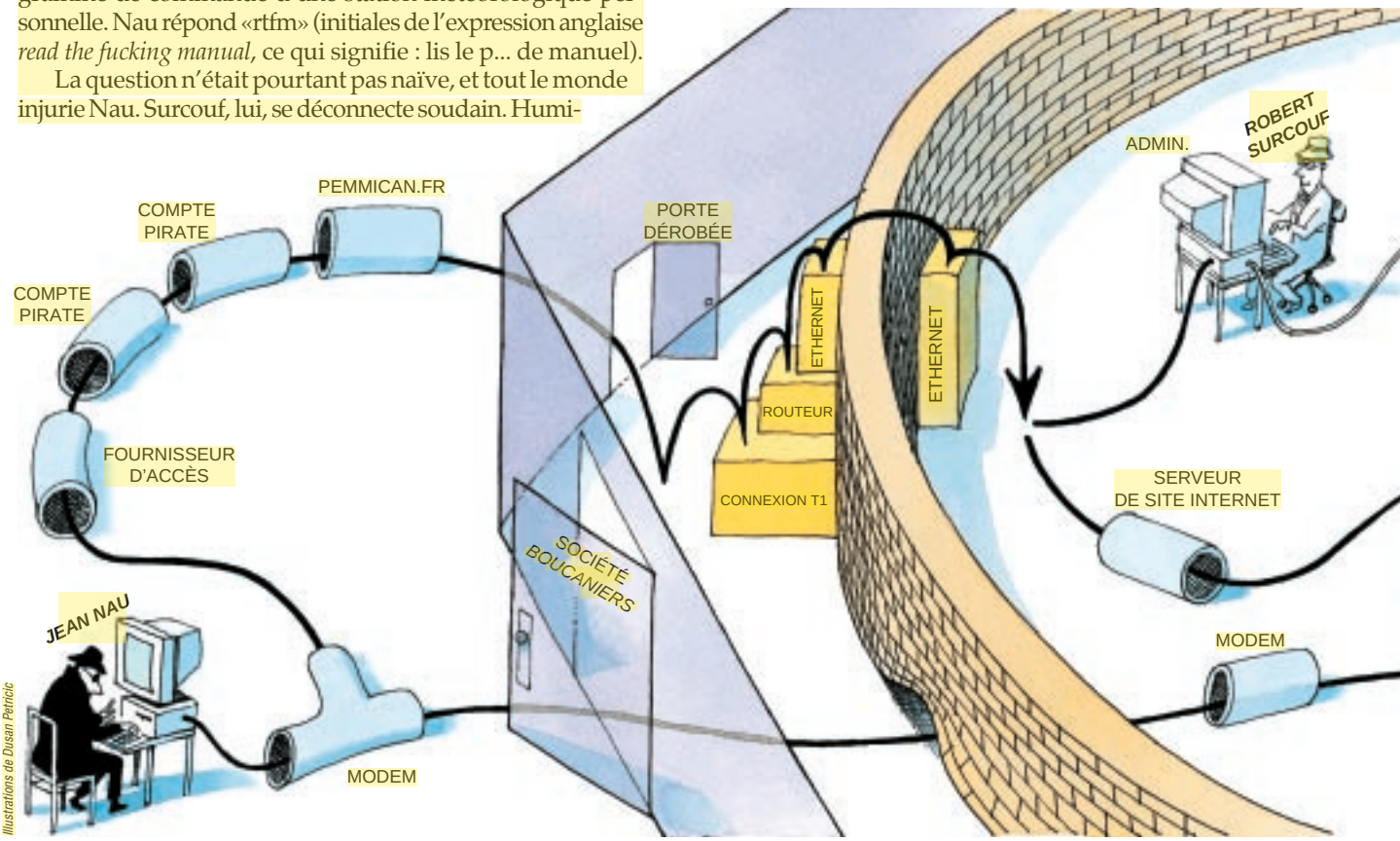
La nuit est tombée depuis longtemps quand, face à son ordinateur, Jean Nau se connecte sur le réseau Internet à un «système de causette» où chaque utilisateur introduit des remarques et lit celles des autres en temps réel. Dans la zone de dialogue consacrée au puissant système d'exploitation *Unix*, 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.

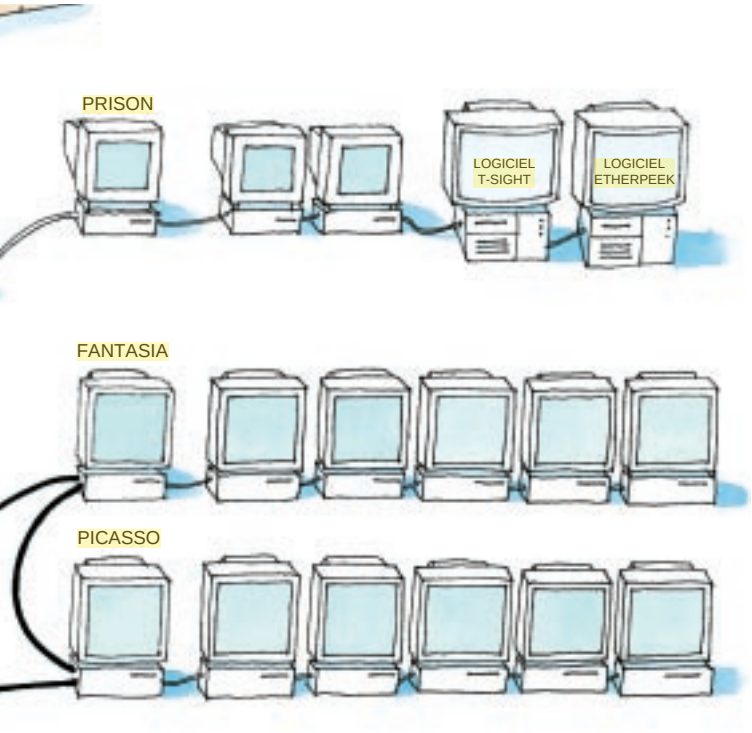


Illustrations de Dusan Petricic

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