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*