dysfonctionnements et leur correction. Il est tentant de laisser actives ces fonctions en conditionnant leur accès à la connaissance d'une clé ou d'une manœuvre particulière telle que l'appui simultané sur trois touches éloignées du clavier.

Le programmeur peut aussi se garder la possibilité de désactiver complètement le système informatique si celui auquel on l'a vendu ne paye pas son abonnement, ou s'il est devenu un ennemi, ou tout simplement si on veut l'inciter à acheter une nouvelle version du logiciel ou de la machine.

On peut également installer la porte dérobée après coup, sans que les développeurs en aient connaissance : la version modifiée du logiciel pourra par exemple mémoriser les codes des cartes bancaires utilisées et les envoyer à une adresse aux mains de pirates. La porte dérobée pourrait aussi donner le contrôle complet de l'ordinateur et, par exemple, en faire un esclave pour envoyer massivement des messages publicitaires. La prise de contrôle d'un ordinateur permet aussi de l'enrôler dans ce qu'on nomme des botnets (des armées d'ordinateurs sous contrôle), puis de les faire participer, à l'insu bien sûr de leurs propriétaires, à l'attaque massive d'un site internet, attaque qui rendrait celui-ci momentanément inopérant (attaque par déni de service).

Le réseau mis en danger

Parmi les affaires récentes les plus graves de porte dérobée, il y a celle concernant les équipements réseau commercialisés par la firme américaine F5-Network, un concurrent de Cisco qui emploie plus de 4 000 salariés et dont le chiffre d'affaires avoisine 2 milliards de dollars.

Le Français Florent Daignière découvrit le 12 février 2012 une grave faille de sécurité concernant une partie importante des machines vendues par F5-Network. Après en avoir averti les responsables de la firme, la faille fut rendue publique en juin 2012 : une porte dérobée donnait accès aux niveaux de contrôle les plus élevés des machines. En langage technique, elle permettait de devenir administrateur de la machine, laquelle aurait pu mener une attaque sur tout le réseau auquel elle participait. On corrigea la faille,

Portes dérobées et tricheries au jeu

Les portes dérobées autorisent celui qui les a placées à opérer des actions dont les utilisateurs n'ont pas connaissance : lecture d'informations privées, copie et envoi de données à des tiers, prise de contrôle partiel ou complet du système informatique, voire destruction de ce dernier.

© De Pra/Shutterstock.com

La plus célèbre affaire de tricherie au poker en ligne, qui a rapporté au moins 20 millions de dollars à ses protagonistes, était fondée sur une porte dérobée présente à l'insu des sites qui proposaient innocemment des jeux de Poker en ligne. La porte dérobée avait été installée par certains des ingénieurs qui avaient développé le programme : elle leur permettait de connaître les cartes cachées des autres joueurs.

Les portes dérobées sont susceptibles de concerner tous les types de systèmes ou de machines électroniques et obligent les autorités de surveillance des jeux de casino à Las Vegas à des mesures particulières, telles que le contrôle par un second technicien de toute modification opérée par un premier technicien. Ce soin méticuleux a été mis en place à la suite d'une affaire de porte dérobée installée dans les circuits des bandits manchots de casinos du Nevada.

Ron Harris, qui était technicien dans une entreprise de machines de casino, avait échangé les circuits de plusieurs machines (des EPROM) par des circuits qu'il avait programmés lui-même, pour qu'elles fassent gagner tout joueur effectuant une certaine séquence de jeu du type : insérer 3 pièces, puis 2 pièces, puis 2, puis 1, puis 3, puis 5. Il n'allait pas jouer lui-même ces séquences, car cela aurait été suspect, mais il faisait jouer des complices. Il fut arrêté non pas à cause des 24 jackpots qu'il gagna grâce à ces bandits manchots truqués, mais à cause d'une autre manipulation qui avait permis à l'un de ses complices de gagner au *Keno* un lot de 100 000 dollars qui attira l'attention des autorités et les conduisit à lui.

Il fut condamné à sept ans de prison (voir http://www.americancasinoguide.com/slot-machines/the-worlds-greatest-slot-cheat.html).

mais les raisons de sa présence dans les machines ne furent pas éclaircies.
Dans les logiciels *open source,* c'est-à-dire dont le programme de base est public et compréhensible, il est presque impossible de cacher des portes dérobées.

Les logiciels ouverts sont aussi concernés

Lors de la conception d'un logiciel, on utilise des langages dits de haut niveau tels que Java, Python, Fortran, C, Pascal, Prolog, etc. Comme les programmes écrits dans ces langages sont incompréhensibles par les machines, ils sont traduits, par des programmes nommés compilateurs, en langage de « bas niveau », ce qui permet aux machines de les exécuter. Les instructions en langage de haut niveau sont compréhensibles par un humain qui peut les contrôler, les modifier et les reprendre pour les perfectionner. Compilé en langage de bas niveau, un programme est illisible et il est difficile de savoir ce qu'il va faire et pourquoi, et donc de le modifier ou de le corriger. Il y a une opposition entre « exécutable par une machine » et « déchiffrable par un humain ».

Rendre public le code source d'un programme, c'est risquer que quelqu'un se l'approprie, le modifie, et en tire profit sous forme compilée. C'est pourquoi les programmes vendus le sont le plus souvent sous forme compilée, donc illisible. Malheureusement, cette pratique met les utilisateurs en danger puisque de tels programmes peuvent comporter des portes dérobées indétectables. Plus généralement, ils peuvent exécuter à l'insu de l'utilisateur toutes sortes de fonctions. Ce conflit d'intérêts entre utilisateurs et vendeurs de logiciels est à l'origine des logiciels libres.

L'assurance qu'un programme ne fait pas autre chose que ce que vous voulez impose de connaître le programme source en langage de haut niveau. D'ailleurs, l'utilisateur pourra, s'il est très méfiant, compiler lui-même le programme source pour être certain que l'exécutable qu'il utilise est vraiment celui issu du programme source. Il faut cependant un peu plus pour que l'on soit assuré d'un fonctionnement conforme à une description : des experts indépendants doivent examiner le programme source, ligne par ligne, et contrôler qu'il ne fait rien de plus que ce qui est annoncé.

Le système d'exploitation Linux est un programme ouvert et pourtant, il a été victime d'une tentative d'introduction de porte dérobée. Le 4 novembre 2003, David Miller, un développeur du noyau, ajoute deux lignes apparemment innocentes au programme. Ces lignes pouvaient être comprises comme n'ayant qu'un effet de prise en compte d'un cas particulier improbable pour éviter qu'il engendre une erreur. En fait, les lignes ajoutées avaient pour effet de rendre administrateur l'opérateur qui entrerait une séquence particulière de caractères. L'astuce était fondée sur une confusion possible entre plusieurs langages de programmation utilisant différents signes d'égalité, le signe = dans certains langages, le signe == dans d'autres.

Les deux lignes ajoutées avaient donc de bonnes chances de passer inaperçues et de créer une porte dérobée dans un programme pourtant ouvert. Les autres développeurs du programme identifièrent l'astuce et retirèrent la porte dérobée, prouvant ainsi l'intérêt des logiciels libres et ouverts. Retenons qu'une astuce, assimilable à un jeu de mots, permet de cacher dans un programme ouvert des fonctions particulières quasi invisibles, voire de graves lacunes de sécurité.

Un conflit ancien entre utilisateurs et États

Depuis longtemps, les experts en sécurité informatique défendent le principe que les meilleures méthodes cryptographiques doivent être disponibles pour tous, ce qui est le cas en France depuis 1998. L'idée inverse a pourtant été soutenue, et même traduite dans certaines lois à l'étranger : selon cette idée, seules des méthodes faibles de cryptographie devraient être autorisées, ou pire, toutes les méthodes cryptographiques autorisées devraient comporter des portes dérobées dont l'accès serait réservé aux autorités.

Dans un article de *Pour la Science (n° 290, juin 1999, pp. 50-51),* Ronald Rivest (le R de l'algorithme de chiffrement RSA) s'opposait clairement à ce désir de brider les méthodes de cryptographie autorisées ou de les munir d'une porte dérobée. Il faisait une intéressante comparaison : « La cryptographie protège les données ; les gants protègent les mains. La cryptographie protège contre les intrus et les espions industriels ; les gants protègent contre les coupures, la chaleur, le froid et les infections. La cryptographie peut gêner la police, qui ne pourra plus pratiquer d'écoutes téléphoniques ; les gants peuvent gêner la police qui trouve difficilement des empreintes digitales. La cryptographie est devenue bon marché et d'emploi facile ; les gants le sont depuis longtemps. » Puisqu'on n'interdit pas la vente et l'usage des gants et qu'on ne limite pas la qualité des gants vendus, pourquoi interdire l'usage de la cryptographie ou tenter de supprimer la sécurité qu'elle offre par des portes dérobées ?

L'une des méthodes, un temps défendue par l'administration américaine, était qu'à chaque fois qu'on envoie un message chiffré, on y joigne la clé de déchiffrement… en la chiffrant avec une autre clé dont seules les autorités connaîtraient la clé de déchiffrement associée. Tant que cette super-clé des autorités reste secrète et inutilisée, tout se passe comme si elle n'existait pas, et l'on peut mettre en œuvre les meilleures méthodes de cryptographie pour donner aux utilisateurs une sécurité aussi forte qu'ils le souhaitent. En revanche, en cas de besoin, pour une enquête ou pour établir une preuve, l'utilisation de la super-clé permet aux autorités de lire tout ce qu'elles veulent des échanges chiffrés entre utilisateurs.

Cette méthode de super-clé revient à associer volontairement une porte dérobée à toute méthode de chiffrement, porte dérobée réservée aux autorités. Le danger est que la super-clé de déchiffrement soit rendue publique à la suite d'un vol. Dans un tel cas, tous les messages respectant la procédure deviennent lisibles de tous, même les plus anciens. Pour reprendre l'analogie avec les gants, la méthode de la super-clé revient à munir les gants d'un dispositif électrochimique commandé par radio tel qu'un signal particulier déclenche