Abonnez-vous à POUR LA SCIENCE

Plus de **24%** de réduction

OFFRE DÉCOUVERTE

12 nos par an

4,90€ PAR MOIS SEULEMENT

BULLETIN D'ABONNEMENT

À renvoyer accompagné de votre règlement à : Pour la Science - Service abonnements - 19 rue de l'industrie - BP 90 053 - 67 402 Illkirch cedex

PAS474

❑ **OUI**, je m'abonne à *Pour la Science* **formule Découverte.**
Je règle par prélèvement automatique de 4,90€ par mois et je complète l'autorisation ci-contre. **J'économise 24% par mois.**
(DPV4E90)

MES COORDONNÉES

Nom : _____

Prénom : _____

Adresse : _____

_____

Code postal |_|_|_|_|_|

Ville : _____

Tél. Pour le suivi client (facultatif) : |_|_|_|_|_|_|_|_|_|

E-mail obligatoire : _____

@ _____

J'accepte de recevoir les informations de *Pour la Science* ❑ OUI ❑ NON
et de ses partenaires ❑ OUI ❑ NON

Délai de livraison: dans le mois suivant l'enregistrement de votre règlement. Offre réservée aux nouveaux abonnés, valable jusqu'au 31/07/2017 en France métropolitaine uniquement. Pour un abonnement à l'étranger, merci de consulter notre site www.pourlascience.fr. Conformément à la loi "Informatique et libertés" du 6 janvier 1978, vous disposez d'un droit d'accès et de rectification aux données vous concernant en adressant un courrier à *Pour la Science*. Votre abonnement en prélèvement est reconduit automatiquement et peut être interrompu par simple lettre.

MANDAT DE PRÉLÈVEMENT SEPA En signant ce mandat SEPA, j'autorise Pour la Science à transmettre des instructions à ma banque pour le prélèvement de mon abonnement dès réception de mon bulletin. Je bénéficie d'un droit de rétractation dans la limite de 8 semaines suivant le premier prélèvement. Plus d'informations auprès de mon établissement bancaire.

TYPE DE PAIEMENT : PAIEMENT RÉCURRENT

Titulaire du compte

Nom : _____

Adresse : _____

Code postal |_|_|_|_|_| Ville : _____

Désignation du compte à débiter

BIC (Identification internationale de la banque) |_|_|_|_|_|_|_|_|_|_|_|

IBAN |_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|_|
(Numéro d'identification international du compte bancaire)

Établissement teneur du compte

Nom : _____

Adresse : _____

Code postal |_|_|_|_|_| Ville : _____

Date et signature

Joindre un RIB

Organisme Créancier
Pour la Science - 8 rue Férou - 75006 Paris
N° ICS FR92ZZZ426900
N° de référence unique de mandat (RUM)

Partie réservée au service abonnement. Ne rien inscrire

LOGIQUE & CALCUL

Big Brother à nos portes (dérobées)

Parfois totalement indétectables, les portes dérobées informatiques nuisent gravement à la sécurité. Introduites à des fins d'espionnage ou de malveillance, ces « backdoors » exposent aussi chacun de nous au risque d'intrusion dans sa vie privée.

Jean-Paul DELAHAYE

Je ne veux pas vivre dans un monde où tout ce que je dis, tout ce que je fais, chaque personne à qui je parle, chaque expression de créativité, d'amour ou d'amitié, est enregistré.
Edward Snowden

En informatique et particulièrement dans tout ce qui est lié à la sécurité des systèmes, le terme de *backdoor* (signifiant « porte dérobée » ou « entrée cachée ») désigne un point d'accès secret. Celui-ci, ménagé dans un dispositif informatique, un programme, une machine, un réseau, permet d'en prendre le contrôle, d'en fausser l'usage ou au moins d'être informé de ce qui s'y passe, à l'insu de ceux qui s'en servent.

En cryptographie, ces portes dérobées donnent le pouvoir à celui qui en connaît l'existence de lire les messages chiffrés par un algorithme dont les utilisateurs pensent, de manière illusoire, qu'ils sont impossibles à percer. On a parfois envisagé d'installer des portes dérobées dont la présence serait connue de tous, mais dont l'accès serait réservé aux autorités.

Dans le cas d'un serveur reliant des machines ou constituant les nœuds principaux dans un réseau informatique, il s'agira de procédures permettant de contrôler les machines. Il s'agira aussi de dispositifs matériels mis en place dès la conception des machines, ou à l'insu de leurs fabricants après la sortie d'usine, et qui dupliquent toutes les informations qui y passent et en envoient la copie à un destinataire complice, sans que le vendeur du matériel ou ses acheteurs ne le sachent.

Parfois, une porte dérobée est une fonction utilisée normalement lors de la mise au point des dispositifs logiciels ou matériels qui permet de les observer afin de comprendre ce qui s'y passe et corriger des erreurs éventuelles ; mais il arrive qu'on oublie de la supprimer ou de la désactiver avant la commercialisation, donnant ainsi la possibilité aux concepteurs des programmes d'y accéder subrepticement. La plus fameuse histoire de ce type concerne le poker en ligne.

Poker en ligne frauduleux

Cette porte dérobée fit gagner des millions de dollars à une équipe de tricheurs qui ne fut jamais parfaitement identifiée. Le principe de la tricherie était élémentaire : les développeurs d'un logiciel de jeu de poker en ligne avaient prévu une combinaison de touches qui leur donnait accès aux cartes cachées des adversaires, y compris quand ils n'étaient liés au système que comme simples joueurs et non comme administrateurs. Une fois le logiciel vendu et installé sur une plateforme qui n'était pas informée du trucage, ils s'inscrivaient comme simples clients et, lorsque les enjeux leur semblaient en valoir la peine, ils activaient la fonction qui leur montrait toutes les cartes, ce qui augmentait considérablement leurs chances de gagner !

L'escroquerie a duré des années, aux dépens d'une multitude de clients américains des sites *Ultimate bet* et *Absolute Poker* qui utilisaient, sans le savoir, le programme truqué. Russ Hamilton et plusieurs de ses complices ont ainsi gagné des sommes considérables entre 2003 et 2007. Ils se présentaient sous des identités différentes pour jouer, mais des experts attentifs qui étudiaient les taux de réussite des joueurs ont observé que certains comptes réussissaient souvent des coups qu'ils n'auraient dû gagner que rarement. Nionio, le premier joueur repéré, obtenait un taux de réussite 20 fois supérieur, pour certaines positions de jeu, à celui des meilleurs joueurs de poker.

Les sites de jeux, obligés de reconnaître les anomalies et donc la tricherie, ont dû rembourser partiellement les joueurs roulés. Ce qui a d'ailleurs mis en péril leur équilibre financier. Dans cette histoire, les escrocs et leurs complices ont gardé l'essentiel des sommes acquises. Des études détaillées des parties jouées au cours de la période concernée indiquent que plus de 110 noms de joueurs fictifs avaient tiré des gains anormaux du jeu. Le montant des sommes volées grâce à la porte dérobée a été évalué à plus de 22 millions de dollars.

Lors du développement d'un logiciel, il est nécessaire de disposer de fonctions d'observation qui donnent des droits supérieurs à ceux des utilisateurs normaux. Cela facilite la maintenance, le repérage des

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

Edward Snowden et les portes dérobées

Grâce aux révélations d'Edward Snowden, on a su que la NSA tentait et réussissait parfois à introduire des portes dérobées dans certains programmes de cryptographie (comme celui d'un générateur pseudoaléatoire du NIST), se donnant ainsi la possibilité de déchiffrer facilement les communications de ceux qui les utilisaient : la NSA espionnait ainsi des citoyens américains, ce que les lois des États-Unis interdisent pourtant.

Le film *Snowden* du réalisateur Oliver Stone est sorti en 2016. Il retrace les péripéties de ce lanceur d'alerte toujours recherché par la police des États-Unis et aujourd'hui réfugié en Russie.

Récemment encore, une vieille idée pourtant combattue par tous les spécialistes de sécurité informatique a resurgi. Deux sénateurs américains, Richard Burr et Dianne Feinstein, ont déposé un projet de loi qui forcerait tous les acteurs des technologies de l'information à truffer de portes dérobées leurs matériels et logiciels. Le projet voulait accorder aux tribunaux américains le pouvoir d'exiger des entreprises telles que Microsoft, Apple, Google, Facebook, etc. qu'elles donnent accès à toutes les données des appareils qu'elles vendent et des services qu'elles offrent.

Comme c'est le cas depuis longtemps maintenant, un grand nombre d'experts se sont élevés contre cette idée qui, si elle était adoptée, reviendrait à affaiblir gravement tous les systèmes de sécurité pourtant de plus en plus nécessaires qui protègent les informations des particuliers et des entreprises. Comme l'écrivaient Pauline Glikman et Nicolas Glady de l'Essec (École supérieure des sciences économiques et commerciales) le 27 mai 2016 dans une tribune sur www.silicon.fr : « Si ce projet de loi américain était voté, les entreprises européennes se verraient donc dans l'obligation d'abandonner l'usage des appareils et services informatiques des fournisseurs américains. Ce serait un coup majeur porté à la compétitivité des États-Unis, qui verraient leurs clients se tourner vers les services chiffrés offerts par des entreprises non soumises à ces contraintes... »

Même aux États-Unis, où l'on sait que les révélations d'Edward Snowden ont déjà affaibli la confiance dans les entreprises et produits nationaux, le projet de loi fait l'objet de très vives critiques. Reste qu'il n'y a aujourd'hui aucun doute que les systèmes d'écoute et d'espionnage massifs mis en place par la NSA au niveau mondial sont un problème pour la souveraineté de tous les États, en même temps qu'un danger économique majeur... et que ces systèmes n'ont pas été désactivés.

la destruction simultanée de tous les gants. Certes, les autorités ne devraient utiliser ce message radio secret que dans des enceintes fermées ne laissant pas échapper le signal destructeur, et uniquement dans le but de s'attaquer à des gants mêlés à des affaires de banditisme ou de terrorisme, mais comment ne pas craindre un accident ou un détournement ?

Le FBI contre Apple

Ces questions ont récemment défrayé la chronique à propos des téléphones d'Apple. En février 2016, le FBI (*Federal Bureau of Investigation*, la police judiciaire américaine) demanda à Apple de l'aider à rendre accessibles les données du téléphone d'un des auteurs de la tuerie de décembre 2015 à San Bernardino, où 14 personnes périrent. Le problème n'était pas directement celui d'une porte dérobée, mais il se fondait sur l'idée très proche que le système de protection des téléphones d'Apple pouvait être contourné avec l'aide des ingénieurs d'Apple. En clair, le FBI ne doutait pas qu'une sorte de porte dérobée existait et demandait à Apple de la faire fonctionner pour lui livrer le contenu du téléphone.

Apple répondit qu'il ne voulait pas collaborer, non pas que cela fût pour lui impossible, mais parce que cela aurait été contraire à l'intérêt de ses clients. Plus précisément, le FBI demandait à Apple de lui donner un moyen d'éviter que ne fonctionne le système d'effacement automatique qui s'enclenche en cas de tentatives répétées d'accès aux données de l'appareil.

Tim Cook, le président d'Apple, a expliqué : « Le gouvernement des États-Unis a exigé qu'Apple prenne une mesure sans précédent qui menace la sécurité de nos clients. Nous ne voulons pas nous soumettre à sa demande, car cela aurait des conséquences bien au-delà du cas particulier concerné. La situation exige un débat public ; nous voulons que nos clients et tous les gens à travers le pays comprennent ce qui est en jeu. »

Quelques jours plus tard, l'affaire trouva un épilogue décevant et inquiétant pour les clients d'Apple : le FBI, avec une aide dont l'identité est restée cachée, réussit à accéder aux données du téléphone. Ce dénouement signifie tout simplement que les protections prétendues inviolables des téléphones d'Apple ne le sont pas, soit parce qu'un tiers sait les contourner, soit parce