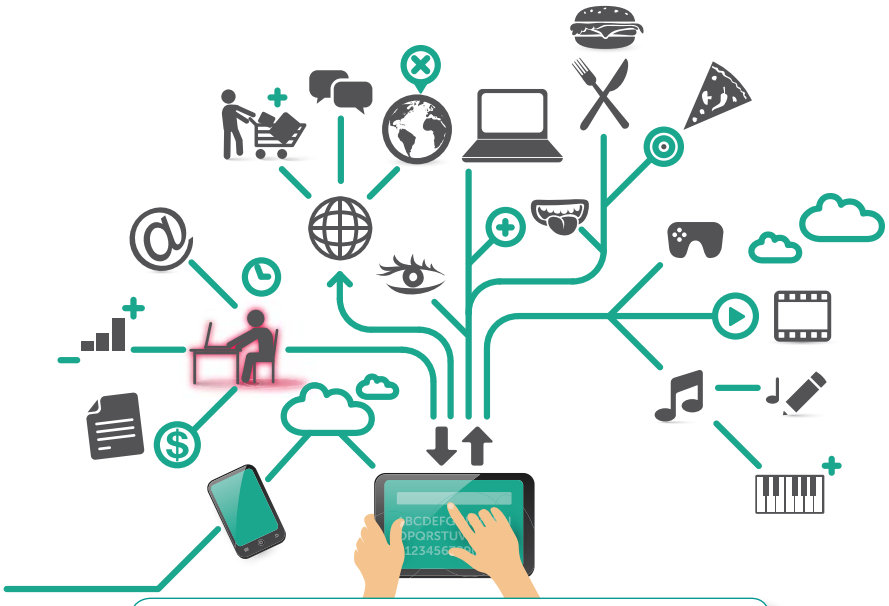
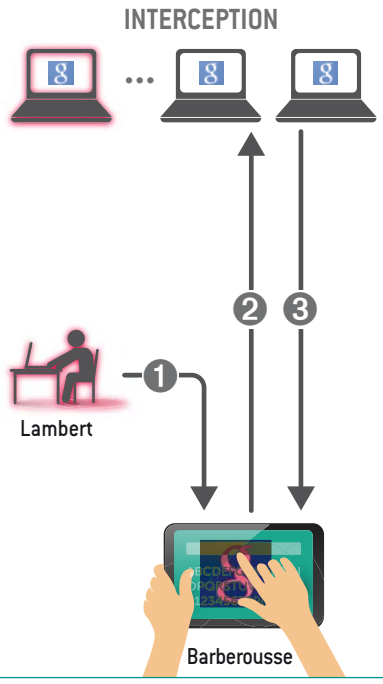
UN EXEMPLE DE VOL DE DONNÉES PERSONNELLES SUR INTERNET

L'usurpation d'identité sur Internet prend de nombreuses formes. Nous avons tous reçu des courriels dans lesquels des escrocs nous demandent des données sur notre identité ou nos moyens de paiement en se faisant passer pour l'administrateur de l'un des sites que nous fréquentons (banque, librairie en ligne, etc.). La ficelle grossière de cette escroquerie a son équivalent en temps réel, qui est décrit ci-dessous.



Transactions bancaires, achats de morceaux de musique, etc. : un individu a aujourd'hui de nombreuses activités en ligne et doit pour cela s'identifier souvent. Cette réalité rend la confidentialité sur Internet cruciale pour le fonctionnement de la société ; elle explique aussi que les escrocs font de nombreuses tentatives pour usurper notre identité ou voler nos mots de passe en temps réel.



Levé de bonne humeur, Lambert se connecte ❶ grâce à son compte *Google* à une nouvelle application affichant en ligne les résultats de l'équipe de France de basket. Mais il ignore que ce service a été créé par Barberousse, un escroc qui lui fait faire bien plus que seulement afficher des résultats sportifs... Barberousse utilise l'identité de Lambert pour demander ❷ une connexion à l'une des applications du compte *Google* de Lam-

LES AUTEURS


Stéphanie DELAUNE, chargée de recherche au CNRS, travaille au LSV (Laboratoire de spécification et vérification), le laboratoire d'informatique de l'École normale supérieure de Cachan.

Rémy CHRÉTIEN est doctorant au LSV et au Laboratoire lorrain de recherche en informatique et ses applications (LORIA).

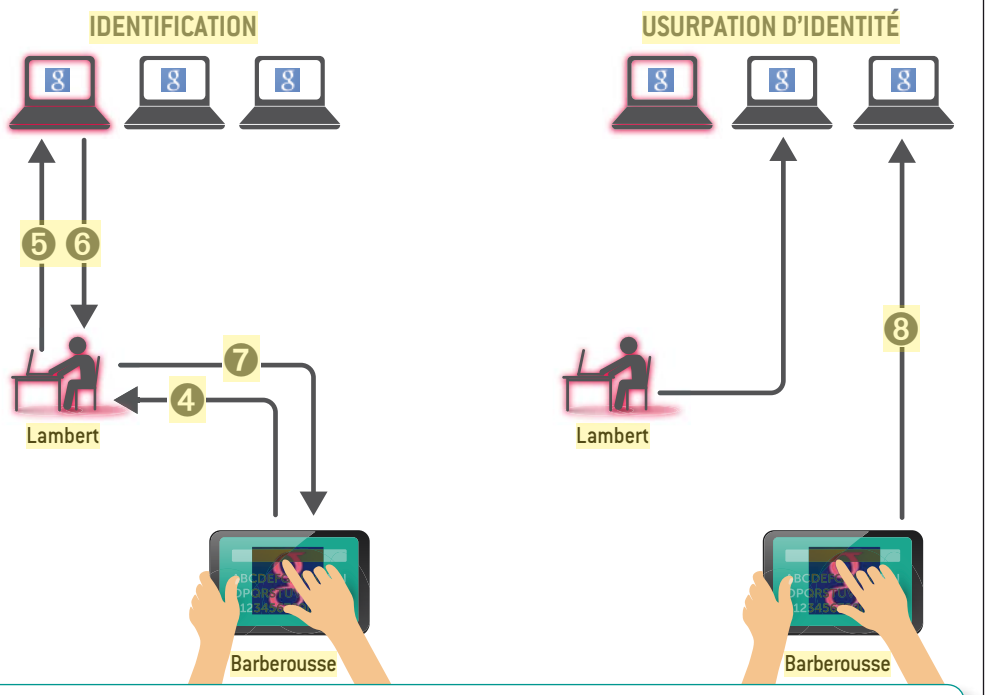
De telles erreurs de conception montrent que, pour éviter ce genre de désastre, d'importants efforts de recherche sont nécessaires avant de déployer un système très utilisé. Il est fréquent que le même algorithme de chiffrement soit employé dans une myriade d'applications différentes, de sorte qu'elles deviennent toutes vulnérables si l'algorithme est attaqué avec succès. Et le nombre énorme de systèmes impliqués ainsi que la complexité inhérente aux primitives cryptographiques rendent impraticables, en général, les corrections à la volée (par exemple par un patch, c'est-à-dire une section de code correctrice).

Une fois le coffre-fort choisi, il importe de maîtriser son expédition, ce qui n'a rien de facile. En effet, une fois effectué le choix des primitives cryptographiques adaptées à la situation, il reste à les mettre en œuvre sans commettre d'erreurs ou de maladresses fatales pour la sécurité des données. La construction d'un cryptosystème s'accompagne en effet de spécifications fixant la façon dont ses composantes échangent des informations, qui sont le plus souvent chiffrées, mais pas toujours. Comme une erreur dans le choix du coffre-fort peut être fatale, un mauvais choix de système de transport (de protocole de communication) annule vite la sécurité apportée par le blindage (par le chiffrement).

Des failles dans la couche logique...

Lorsqu'on traite les problèmes d'organisation et de mise en œuvre d'un système de sécurisation des données, on quitte la couche cryptographique pour entrer dans ce que l'on nomme la couche logique de sécurité. L'emploi d'un algorithme de cryptage dépourvu des faiblesses mentionnées plus haut ne garantit pas l'absence

ET D'ACCÈS AUX APPLICATIONS *GOOGLE*



bert. Celle-ci répond par une demande d'identification ❸, que Barberousse répercute à Lambert ❹. Ce dernier s'identifie ❺ auprès du serveur dédié à l'authentification des utilisateurs de *Google*. Ce serveur renvoie ❻ la preuve de l'identité de Lambert à son ordinateur, lequel, conditionné par l'application malveillante de Barberousse, lui communique ladite preuve ❼. Barberousse se sert de cette preuve pour se connecter ❽ par le compte de Lambert à une application *Google*, par exemple l'agenda ou la messagerie de Lambert ; dès lors qu'il s'est connecté avec l'identifiant et le mot de passe de Lambert, ce dernier est aussi simultanément connecté sur l'application sportive, qu'il consulte alors, toujours de bonne humeur, pendant que Barberousse lit son emploi du temps, vole ses secrets ou envoie des messages depuis son ordinateur...

d'erreurs dans la logique présidant à la conception du système.

La première erreur logique possible consiste à envoyer la clef sans la cacher, en d'autres termes à transmettre la clef en clair, ou d'une façon qui permet de la voler. Le vol d'identité résultant d'informations de connexion d'un utilisateur à un service en ligne (une banque en ligne, par exemple) non chiffrées sur Internet fournit un exemple trivial d'une telle erreur logique. Dans ce cas simple, un attaquant n'a qu'à intercepter la communication entre l'usager et son fournisseur de service pour dérober les informations confidentielles permettant de se connecter à la place de l'usager. De telles failles se sont révélées récemment sur des services bien connus du grand public. On peut citer une version ancienne du protocole de connexion des particuliers aux services de *Google* (dit *Google Single Sign-on*), qui a la particularité d'étendre à toutes les applications de *Google* la connexion d'un utilisateur à une seule application.

Ce genre d'attaque permet, par exemple, d'accéder à l'agenda d'une personne après qu'elle a entré son nom d'utilisateur et son mot de passe. Elle repose sur la ruse consistant à pousser l'utilisateur à se connecter à une application malveillante conçue pour l'intéresser, mais secrètement contrôlée par l'attaquant. Il pourra s'agir, par exemple, d'une application affichant les derniers résultats sportifs. L'attaquant intercepte le message envoyé par l'utilisateur pour accéder à cette application. Cette interception est intéressante pour l'attaquant, car ce message a le défaut de ne pas être spécifique à une application donnée, de sorte que l'attaquant peut réutiliser les informations de connexion pour se connecter à d'autres applications depuis le compte *Google* de l'utilisateur, par exemple à sa messagerie, à l'agenda, au service cartographique, à ses archives personnelles, etc. *(voir l'encadré ci-contre)*.

Ce cas illustre qu'en matière de sécurité informatique aussi, le diable est dans les détails, dans des détails de conception infimes, parfois presque invisibles, mais qui peuvent avoir d'importantes répercussions sur la sécurité. Ces failles dans la conception d'un système de protection des données sont d'autant plus graves que la faiblesse qu'elles engendrent affecte des services déjà déployés, et que le déploiement d'un patch ne suffit pas à les réparer. Dans le cas du protocole de connexion aux services de *Google*, changer un message de connexion utilisé par toutes les applications n'est guère réaliste, car cela a des effets à la fois sur la pratique de l'utilisateur et sur l'accessibilité des autres applications. Il est en effet souvent important de maintenir la compatibilité entre les divers protocoles donnant accès à un faisceau d'applications, même si l'un d'eux est défectueux. Une révision complète du système de connexion des services de *Google* a donc été nécessaire pour supprimer la faille.

Que faire pour éviter ce genre de difficulté ? Pour l'essentiel, il s'agit de tester de façon complète, avant de déployer le système de protection, la sûreté des procédures utilisées pour faire circuler les coffres-forts (les informations cryptées) qui protègent les données. Différents modèles théoriques de mise en œuvre existent. Dans le modèle dit symbolique, on procède en supposant d'abord que les primitives cryptographiques choisies sont incassables, puis en représentant par des symboles toutes les opérations effectuées par le système de sécurité. Sur la base d'une définition rigoureuse de la sécurité à obtenir, une technique mathématique rigoureuse permet ensuite de s'assurer que le protocole résiste à toutes les formes d'attaques décrites au sein du modèle utilisé. Une fois cette étape franchie, on peut passer à la mise en œuvre du système de sécurité.

... ou dans l'implémentation

Nous avons maintenant soigneusement choisi des coffres-forts adéquats (des algorithmes de cryptage), organisé scrupuleusement leur transport en nous méfiant de toutes les trahisons volontaires ou involontaires du transporteur (des procédures de communication) et des ruses imaginables