

# La sécurité des transactions sur le net: nouvelles solutions

*Les attaques sur le net sont de plus en plus sophistiquées et dangereuses. De nouvelles solutions pour sécuriser les transactions commencent à voir le jour. Elles donnent une deuxième chance aux solutions très répandues dites d'authentification forte.*



JEAN-MARC BOST  
 Head of Security  
 Division, ELCA

**LES SERVICES** sur internet ont le vent en poupe, mais la confiance qu'ils doivent assurer pour attirer les internautes est menacée. D'un côté, consommateurs et citoyens apprécient de plus en plus de ne pas devoir se précipiter à la sortie du travail pour faire leurs courses ou leurs formalités administratives, de l'autre, marchands, banques et administrations peuvent fournir sur internet plus de services, plus rapidement, tout en réduisant leurs coûts.

Mais le développement de la cybercriminalité pose un réel problème tant d'un point de vue financier qu'en termes d'image. Les attaques avérées sont de plus en plus nombreuses et efficaces. Tous les chiffres ne sont pas connus mais, rien qu'en 2004, les banques anglaises ont admis avoir subi des vols à hauteur de 4,5 millions de livres, et des attaques par key logger (programmes espions interceptant les données saisies par un utilisateur) ont été annoncées, respectivement, à hauteur de 1 et 4 millions de dollars de pertes pour les banques françaises et brésiliennes.

Les attaques sont de plus en plus

sophistiquées et dangereuses. Leur évolution sur le web peut être schématiquement découpée en 3 cibles: l'internaute, le réseau internet, le poste de l'internaute. Le phishing (le hacker cherche à leurrer l'internaute en se faisant passer pour un autre) appartient à la première catégorie. Il est omniprésent aujourd'hui. Les intrusions man-in-the-middle (un site intermédiaire intercepte le flux transactionnel entre le navigateur et le service internet) appartiennent à la seconde. Elles étaient annoncées depuis un certain temps mais ne sont effectives que depuis peu. Quant aux dernières, il s'agit d'intrusions par malware entre l'internaute et son navigateur. Les malwares deviennent une réalité envahissante (voir l'encadré ci-contre).

## L'authentification forte ne suffit plus

L'authentification forte par mot de passe unique est très répandue en Suisse et de plus en plus de pays l'imposent pour les transactions financières. Ces solutions apportent un remède efficace contre le phishing. Elles sont cependant de plus en plus

décriées pour leurs coûts sans rapport avec la sécurité réelle qu'elles apportent face aux nouvelles attaques. Par définition, un mot de passe unique n'est protégé qu'après avoir été utilisé. S'il est intercepté avant, par man-in-the-middle ou par malware, il reste exposé (voir l'encadré ci-contre).

Les solutions PKI (infrastructures à clé publique) prévoient la distribution aux utilisateurs de clés de chiffrement et de certificats sous forme logicielle, de clé USB ou de smart card. Elles reposent sur le cryptage systématique des échanges qui permettent d'authentifier les deux parties à chaque bout de la ligne et d'empêcher les hackers de s'immiscer entre elles. Malheureusement, elles sont complexes et coûteuses à mettre en œuvre, et



les spécialistes mettent en garde contre un excès de confiance tant que l'on ne peut être sûr de «qui utilise les clés?». Si un malware peut prendre le contrôle du PC, qu'est-ce qui l'empêcherait d'utiliser les clés de l'internaute? (voir encadré *Attaques*)

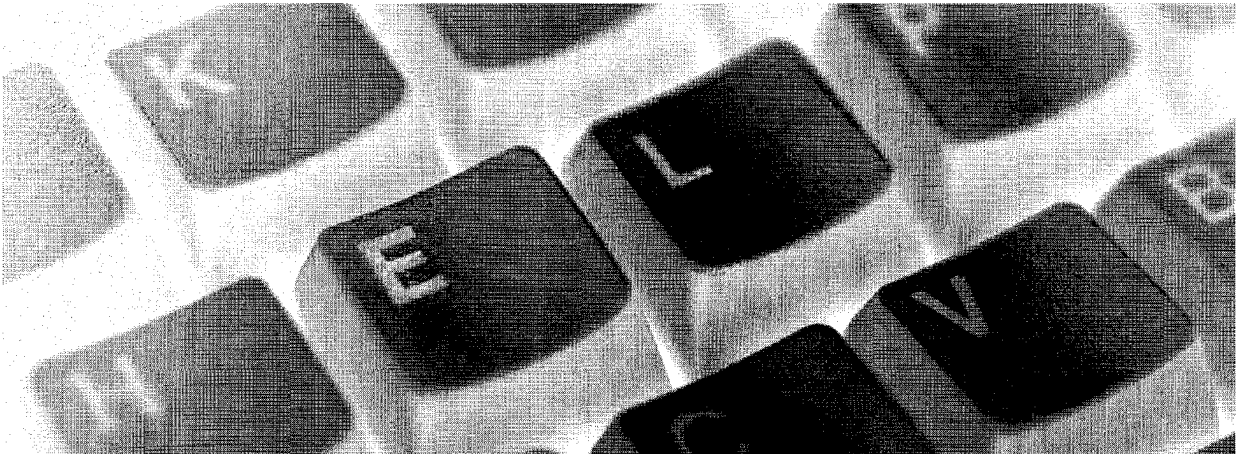
L'enjeu peut-être résumé ainsi: comment éviter qu'un mot de passe unique ou qu'une clé de chiffrement soit utilisé abusivement par un malware? Distribuer aux internautes du logiciel sécurisé pour accéder aux clés complique le déploiement sans réellement éliminer la menace. D'autres solutions commencent à voir le jour et redonnent une deuxième chance aux solutions d'authentification forte. L'idée est de permettre à l'internaute de lier ses mots de passe uniques aux transactions qu'il effectue pour que ceux-ci ne soient plus utilisables ailleurs.

### Des transactions sécurisées, et même irréfutables

Les solutions proposées pour renforcer l'authentification lors de la validation de transaction sont de deux types. Les premières se présentent sous la forme de calechettes indépendantes permettant d'obtenir un mot de passe unique indissociable des données de la transaction. L'internaute rentre les données de la transaction dans sa calechette, obtient un mot de passe, et rentre à nouveau ces informations dans le navigateur. Pour simplifier, on peut lui proposer de ne rentrer qu'une synthèse de la transaction dans sa calechette, mais au prix d'une sécurité amoindrie.

Les autres solutions affichent à l'internaute un reçu sécurisé, typiquement un SMS, avec les données de la transaction et un

mot de passe unique indissociable. Le canal SMS ne présentant pas forcément toutes les garanties de disponibilité et de confidentialité recherchées par les banques, Elca propose une alternative ne nécessitant qu'un navigateur récent et une solution d'authentification forte (voir l'encadré *de gauche*) et qui, de plus, peut être contresigné par l'internaute pour fournir une preuve de la transaction. Moins exigeantes que les calechettes, ces solutions sont plus dépendantes de la vigilance de l'internaute. Comme toujours, le choix de la bonne solution est affaire de compromis entre sécurité, satisfaction des besoins et des contraintes de la banque, confort d'utilisation et coûts. Une chose semble acquise: il faut protéger les transactions sur internet et l'authentification forte est déjà là. ■



## Des attaques malicieuses

Depuis 2003, les banques subissent des attaques par des programmes malicieux (malwares), capables d'intercepter et modifier les données saisies et affichées dans les navigateurs. Tout récemment, 10000 postes australiens ont été contaminés par un malware capable de récupérer toutes les données personnelles échangées avec une application. Lors d'une étude récente, Microsoft a constaté avec son anti-spyware qu'environ 62% des postes audités étaient infectés et SANS estime que 9,9 millions de machines sont infectées par des key-loggers aux USA. CitiBank aux USA est la première victime avérée d'une attaque man-in-the-middle. L'attaque a mis à mal les coûteux «time-tokens» (générateurs de mots de passe uniques dans le temps) qui avaient pourtant été introduits pour lutter contre le phishing. Chez Elca, nous avons démontré la faisabilité d'une attaque de masse, visant les transactions effectuées dans un navigateur web, que le site cible soit ou non protégé par authentification réciproque et cryptage des échanges. Cette attaque est à la portée d'un développeur débutant.

## Une solution pratique et sûre

Elcard utilise des cartes à grille plastifiées faciles à produire et peu coûteuses à distribuer aux internautes. Lorsque l'internaute s'authentifie fortement, il reçoit un défi dans son navigateur sous la forme des coordonnées d'une cellule de sa grille. Il répond par le contenu des cellules parcourues en suivant un chemin secret connu de lui seul. Principe de ELCARDeST: l'internaute soumet une transaction dans son navigateur; celle-ci est enregistrée par la banque qui présente ensuite un reçu sécurisé intégrant un défi; l'internaute valide visuellement le reçu, puis répond au défi pour approuver la transaction; sa réponse au défi est utilisée pour accéder à sa clé de chiffrement et contre-signer le reçu; la banque conserve le reçu signé électroniquement par les deux parties, et l'internaute sa copie; le reçu archivé fournit la preuve de la transaction.