Deux mots de passe valent mieux qu'un?

Plus que de développer des systèmes complexes de sécurité, il existe un moyen simple, plein de bon sens, pour se protéger efficacement : employer non plus un mais deux mots clés.

L'utilisateur qui doit accéder à des espaces protégés, un réseau ou un compte bancaire par exemple, reçoit ou créé lui même un mot de passe. Un code unique présente aujourd'hui une véritable faille de sécurité, qui prend en grande partie sa source dans le comportement de son utilisateur. Notation du code, logique du mot de passe, récurrence par l'utilisation d'un unique code, vol, etc. De plus, les pirates informatiques disposent d'outils simples qui leur permettent de tester et de décrypter rapidement, et souvent avec logique, le code de protection de bien des systèmes. L'usage d'un code unique permanent par utilisateur devient donc inefficace, et les sociétés commencent à penser que la solution la plus simple tiendrait dans la présence obligatoire de deux mots de passe. Mais attention, pas deux codes fournis par l'utilisateur, mais bien deux sources, l'utilisateur et la société Une clé, créée par l'utilisateur, ne suffit pas à ouvrir un accès. Une seconde clé est nécessaire, elle est fournie par la société, mais temporairement, c'est-à-dire à usage unique. RSA Security propose dans cette optique une solution électronique originale, qui d'ailleurs a retenu l'attention de Microsoft pour protéger les machines Windows. Le système SecurID Key Fob se présente sous la forme d'un petit boîtier, sur lequel un écran affiche un code à 6 chiffres, qui change toutes les 60 secondes. Pour se connecter à un poste ou à un service, il suffit de saisir son identifiant, son mode de passe, et le code qui s'affiche sur les boîtier. Plusieurs banques suédoises quant à elles ont commencé à expérimenter un autre système. Elles fournissent à leurs clients une carte à gratter. Lorsqu'un client se connecte, il saisit son code personnel, puis il gratte la carte pour découvrir un code, qu'il introduit ensuite. En l'absence de la carte, pas d'accès, un code utilisé est automatiquement annulé, la carte terminée, une nouvelle vient la remplacer. En plus d'assurer un haut niveau de protection par une méthode simple, dont le plus évident porte sur le code à usage unique, l'utilisation de deux mots de passe sous la forme évoquée ci-dessus présente aussi un intérêt rare : le consommateur peut se réserver l'usage d'un mot de passe simple, facile à mémoriser, le vrai plus de protection apporté par cette méthode lui est fourni par le fournisseur du service, en clair?