

Sécurité des systèmes d'information

Authentification forte : les nouvelles tendances

INCONTOURNABLE. Pour Sylvain Maret, directeur veille technologique e-Xpert Solutions SA, l'authentification forte s'impose parmi les principes de base d'une protection optimale.

Sylvain Maret, directeur
veille technologique e-Xpert
Solutions SA

La protection des biens est une préoccupation majeure de la société, un souci que partage tout un chacun. Certains s'en inquiètent à titre personnel, pour leurs propres biens. D'autres, pour des raisons militaires ou économiques. A l'ère des nouvelles technologies de l'information, les entreprises se sentent de plus en plus concernées – pour des raisons propres à chacune d'entre elles – par la sécurité de leurs systèmes informatiques. Mettre en place une véritable politique de sécurité devient une obligation. Tout comme appliquer les principes de base d'une protection optimale que sont l'authentification, l'autorisation, l'intégrité, la non-répudiation et la confidentialité.

Parmi ces cinq mécanismes, l'authentification, et plus particulièrement l'authentification forte, est, de mon point de vue, la clé de voûte de la sécurité informatique.

L'authentification

L'authentification est une procédure qui vise à s'assurer de l'identité d'un individu ou d'un système informatique. C'est un préliminaire indispensable à l'activation du mécanisme d'autorisation et, donc, à la gestion des droits d'accès à un système d'information donné.

Les méthodes classiques pour identifier une personne physique sont au nombre de quatre :

1. quelque chose que l'on connaît : un mot de passe ou un PIN code;
2. quelque chose que l'on possède : un «token», une carte à puce, etc.;
3. quelque chose que l'on est : un attribut biométrique, tel qu'une empreinte digitale;
4. quelque chose que l'on fait : une action comme la parole ou une signature manuscrite.

On parle d'authentification forte dès que deux de ces méthodes sont utilisées ensemble. Par exemple une carte à puce avec un PIN code.

Pourquoi cette méthode plutôt qu'une autre?

Le mot de passe est actuellement le système le plus couramment utilisé pour identifier un utilisateur. Malheureusement, il n'offre pas le niveau de sécurité requis pour assurer la protection de biens informatiques sensibles. Sa principale faiblesse réside dans la facilité avec laquelle il peut être trouvé, grâce à différentes techniques d'attaques.

Mis à part l'approche, efficace, de la manipulation psychologique («social engineering»), on recense trois grandes catégories d'attaques informatiques :

1) Attaque de «force brute»

Il s'agit d'une attaque qui vise à deviner un ou plusieurs mots de passe en utilisant des dictionnaires ou en testant toutes les combinaisons possibles. Partant

du principe que la majorité des mots de passe sont «faibles» (combinaisons simples du type année de naissance, prénom de son enfant, etc.), les découvrir rapidement se révèle très facile.

2) Ecoute du réseau

La plupart des applications comme «telnet», «ftp», «http», «ldap», etc., n'ont pas recours au chiffrement («encryption») lors du transport d'un mot de passe sur le réseau. «Ecouter» le trafic et en extraire le mot de passe devient un jeu d'enfant dès lors qu'on dispose d'un logiciel d'écoute appelé «sniffer» (littéralement, renifleur).

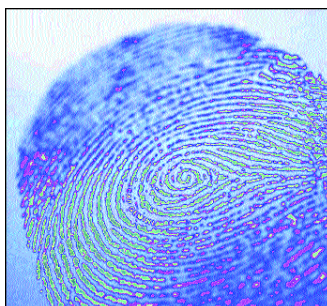
Il existe un grand nombre de «sniffers» dédiés exclusivement à la capture des mots de passe. Un des plus efficaces est «dsniff». Ce type de logiciels est également capable de capturer des mots de passe dans un environnement réseau commuté. La méthode utilisée dans un tel environnement est celle du «ARPPoisoning».

3) Ecoute du clavier

Imaginons que le trafic sur le réseau soit chiffré et que l'utilisateur ait pris soin de choisir un mot de passe extrêmement «solide». Une méthode d'attaque se révèle malgré tout imparable : l'écoute du clavier ou «key logger», qui permet de «capturer» l'ensemble des touches tapées sur un clavier.

Les logiciels utilisés dans ce cas sont généralement installés





De plus en plus pointue La sécurité prend des formes diversifiées comme empreintes ou cartes à puce.

sur le poste de travail, à l'insu de l'utilisateur. La «compromission» du système informatique étant le plus souvent effectuée par le biais d'un virus de type cheval de Troie.

Les nouvelles tendances

Il existe aujourd'hui un grand nombre de solutions d'authentification forte basées sur des «tokens» physiques, comme, par exemple, SecurID, Vasco, ActiveCard, etc. Ces technologies procurent un haut degré de sécurité et ont l'avantage d'être très «mobiles». Elles sont toutefois dédiées uniquement à l'authentification. Elles sont en effet conçues sur le principe du secret partagé et ne sont dès lors pas en mesure d'offrir la non-répudiation.

Une des solutions pour combiner authentification forte et non-répudiation consiste à utiliser des certificats digitaux (norme X509). Basés sur les algorithmes à clés publiques (RSA, DSA, etc.), ils sont un excellent moyen d'authentifier des individus. Ils ouvrent surtout la voie à d'autres services de sécurité, comme la signature de transactions, le chiffrement de données, la gestion de privilèges ou encore le Single Sign On. Reste que pour garantir un haut niveau de sécurité, il est primordial de se poser la question du stockage du certificat et, surtout, de sa clé privée.

Sécurisation de la clé privée

L'utilisateur qui souhaite sécuriser la partie privée d'un certi-

ficat dispose de plusieurs possibilités. Une des plus connues est le recours à des cartes à puce (format carte de crédit ou «tokens» USB). Ces supports permettent le stockage aussi bien des clés que du certificat numérique.

Il existe deux grandes familles de supports : les cartes mémoire et les cartes à processeur cryptographique. En termes de sécurité, la deuxième famille est à recommander, dans la mesure où la clé privée est intégrée au support et n'en sort jamais. Les calculs cryptographiques sont en effet réalisés à l'intérieur de la carte par le processeur.

Cette méthode garantit une protection optimale contre les attaques qui visent à obtenir la clé privée. De plus, la carte à puce peut être protégée par un PIN code.

L'avènement de la biométrie

La biométrie – par exemple un lecteur d'empreintes digitales en lieu et place du PIN code des cartes à puce – ouvre, elle aussi, des perspectives intéressantes. L'idée est de coupler un lecteur biométrique et un lecteur de cartes à puce. L'utilisateur s'identifie alors par le biais de sa carte, ainsi que par un attribut biométrique.

Ces technologies sont actuellement disponibles sur le marché et méritent d'être évaluées. Elles permettent en effet de stocker une signature biométrique sur une carte à puce – c'est ce qu'on appelle le MOC (*Match*

On Card). Elles offrent par ailleurs un niveau de sécurité très élevé pour les environnements sensibles tels que la finance, l'industrie, etc.

Utiliser des certificats digitaux sur un support physique est donc une excellente solution pour sécuriser un système d'information. Cette méthode présente toutefois un certain nombre de limitations auxquelles il convient d'être attentif. La principale est la mobilité du support. A l'heure actuelle, il est très difficile d'utiliser une carte à puce dans un cybercafé ou dans un hôtel. Ces supports offrent par contre un bon retour sur investissement lorsqu'ils sont utilisés dans un environnement maîtrisé.

A quand les cartes à puce dans l'entreprise?

Un des principaux freins à l'utilisation des cartes à puce dans l'entreprise est le manque d'applications susceptibles de les supporter de manière native. De nombreuses solutions sont certes disponibles sur le marché, mais elles demandent généralement l'ajout de composants logiciels. Comme, par exemple, le remplacement de la mire d'authentification (GINA) Microsoft.

La «démocratisation» des cartes à puce viendra, à mon

sens, de Microsoft. L'architecture Win2k (avec Kerberos et PKINIT) supporte en effet, de manière native, les certificats stockés sur les cartes à puce. On peut ainsi imaginer un grand nombre d'applications gravitant autour de cette architecture: des solutions de «Single Sign On», la sécurisation d'accès au bâtiment, l'accès à des portails «web based», etc.

En conclusion, il ne fait plus de doute que l'authentification forte devient incontournable dès lors qu'il s'agit de sécuriser un système informatique. Quant au choix de la technologie (cartes à puce ou «tokens» classiques), il dépend beaucoup de l'environnement et des contraintes propres à chaque entreprise. ●

Sylvain Maret

Contact : e-Xpert Solutions SA
Route de Pré-Marais 29
1233 Bernex-Genève
Tél : +41 22 727 05 55
info@e-xpertsolutions.com

e-Xpert Solutions SA

Au bénéfice d'une longue expérience dans les secteurs financiers et industriels, e-Xpert Solutions SA propose à sa clientèle des solutions «clés en main» dans le domaine de la sécurité informatique des réseaux et des applications. Des solutions qui vont de la sécurité d'architecture – tel le firewall, VPN, IDS, le contrôle de contenu, l'antivirus – aux solutions plus avant-gardistes comme l'authentification forte, la biométrie, le Single Sign On, les architectures PKI ou encore la sécurisation des OS.

