

Zoom

■ La base de données des authentifications – L'authentification des individus est stockée dans une base de données. Cette base de données peut être par exemple le fichier /etc/shadow sur Linux et Solaris, la SAM \$windir\system32\config\sam sous Windows NT ou encore les fichiers .htpasswd du serveur Web Apache.

Les systèmes d'exploitation proposent diverses méthodes pour partager une base de données d'authentification entre machines. On peut utiliser un serveur d'authentification, comme NIS sous Unix, qui centralisera ainsi la base d'authentification.

Les opérateurs Internet utilisent les composants du réseau pour effectuer l'authentification, recourant à des serveurs d'authentification tels que TACACS (*Terminal Access Controller Access Control System*) et surtout RADIUS. Cette méthode est dorénavant connue sous le nom de AAA pour «*Authentication, Authorization and Accounting*», mais le protocole largement déployé est toujours RADIUS, dont le RFC peut être consulté à l'adresse suivante : <http://www.ietf.org/rfc/rfc2865.txt>

La sécurisation des procédures d'authentification

Qui accède au système d'information ? La réponse à cette question constitue l'une des bases de la sécurité. Sécuriser le système d'information est une tâche dont la complexité va croissant, parallèlement à l'augmentation du nombre d'applications et au degré d'ouverture vers l'extérieur qu'elles impliquent. L'authentification des utilisateurs est nécessaire, qu'ils soient internes ou externes à l'entreprise. Elle est importante tant au niveau de la sécurité que de la facilité et de la sûreté d'emploi pour l'utilisateur, donc au final de la performance de l'entreprise.

Définir qui a accès à quoi, où et quand, mais aussi journaliser les actions des individus, voilà ce que doit permettre le contrôle d'accès au système d'information. Il revêt deux aspects. Fondamentalement, il sera réalisé par une identification, suivie d'une authentification, les deux pouvant être liées. Alors que l'identification requiert de l'individu qu'il déclare son identité, l'authentification nécessite que cet individu fournisse la preuve de son identité. Cette preuve peut être constituée soit :

- par une information connue du seul individu, dont l'exemple classique et omniprésent est le mot de passe ;
- par un certificat fourni par l'individu, une technique intégrée dans les PKI (*Public Key Infrastructure*) et donc sur-représentée par le biais du marketing ;
- par un objet que l'individu est le seul à posséder, telle qu'une calculatrice ou une carte à puces ;
- par une caractéristique physique unique de l'individu, telle que définie par les techniques de la biométrie ;
- par une combinaison des éléments précédents, ce qui est généralement le cas dès lors qu'on a recours à un élément autre que le mot de passe. L'authentification par mot de passe est celle uti-

lisée par défaut sur l'ensemble des systèmes d'exploitation. Le choix et la gestion du mot de passe sont du ressort de l'utilisateur, mais le respect de quelques règles doit permettre de maintenir un niveau de sécurité homogène sur ce point. Un « bon » mot de passe doit comporter au minimum 7 caractères, et doit alterner caractères de contrôles, de ponctuation, chiffres, ainsi que majuscules et minuscules. De surcroît, un mot de passe ne doit pas pouvoir être déduit ou deviné en analysant les informations privées ou générales, liées à l'individu, à l'organisation, au système, etc.

La prédominance du password

L'ensemble des cas de vols de mots de passe présente deux caractéristiques communes. D'une part, le mot de passe obtenu sera immédiatement utilisé, aucune attaque, aucune subtilisation de mot de passe n'est sans conséquence. D'autre part, l'opération pourra être réitérée dans plus de 90 % des cas. Il est donc fondamental de responsabiliser les utilisateurs vis-à-vis du choix et de la gestion de leur mot de passe. Parallèlement, les administrateurs doivent protéger la base de données contenant les empreintes, et empêcher que les mots de passe soient transmis en clair sur le réseau, en généralisant l'usage des protocoles applicatifs SSL et SSH.

Si d'autres technologies (la biométrie, les cartes à puces, les certificats et les PKI) sont envisageables, le mot de passe demeure la base de l'authentification même s'il montre clairement ses limites. À cet égard, l'utilisation de *tokens*, à l'instar des solutions Safe Data, semble un bon compromis. L'utilisation de serveurs d'authentification centralisés au travers des protocoles RADIUS (*Remote Authentication Dial-in User Service*) et LDAP (*Lightweight Directory Access Protocol*) constitue également une solution fiable dans laquelle investir. ■

Du bon usage du mot de passe

Les deux méthodes suivantes garantissent une sécurité minimale dans l'usage des mots de passe :

- combiner 2 mots existants, avec l'introduction de chiffres et/ou de caractères de ponctuation ;
- utiliser des mots écrits en phonétique, tel que «*13abilE*», ou les premières lettres de vers, phrases, expressions, adresses, etc.

Les mots référencés par les dictionnaires français, anglais et autres, seront systématiquement découverts. Toutefois même un mot de passe choisi avec le plus grand soin reste cependant vulnérable à un certain nombre d'attaques, de dangers :

- l'utilisateur peut taper son mot de passe alors qu'une tierce personne regarde son clavier ;
- l'utilisateur peut communiquer, souvent sans

intention de nuire, son mot de passe au voisin ;

- il n'est pas rare qu'un utilisateur note son mot de passe sous son clavier, sur un carnet, etc. ;
- un pirate peut «*écouter*» le mot de passe passant en clair sur le réseau dans un protocole comme HTTP, POP3, IMAP, Telnet, FTP, SQLnet, etc. ;
- le système d'exploitation peut être victime d'un cheval de Troie, qui utilise la phase d'authentification pour voler le mot de passe, par exemple une écoute de l'écran sous X11 ou un serveur SSH modifié par le pirate ;
- la base de données des mots de passe peut être volée, et soumise à plusieurs logiciels de craquage de mot de passe.

Un exposé sur le craquage et le durcissement des mots de passe est consultable à l'adresse suivante : <http://www.hsc.fr/ressources/presentations/mdp2/>

L'authentification dans Windows 2000

Windows 2000 (W2K) se caractérise par des fonctions de sécurité variées et complexes. Active Directory est la base de données spécifique de W2K dans laquelle les informations liées à la sécurité sont stockées. Elle remplace la SAM (Security Accounts Manager) de NT4.

L'imbrication des bases centralisées et décentralisées de W2K impose souvent la création d'un compte local pour un utilisateur d'ores et déjà déclaré dans un domaine. W2K supporte quatre systèmes d'authentification :

- MS-Kerberos qui est celui utilisé par défaut ;
- les cartes à puces ;
- un *mapping* de certificats stockés dans son répertoire Active Directory ;
- NTLM (*NT LAN Manager*) pour la compatibilité avec Windows NT, les comptes locaux et les groupes de travail.

L'authentification W2K par défaut est celle préférable pour la sécurité, mais elle ne sera utilisable qu'en environnement exclusivement W2K, sans PC sous Windows 95, 98 ou NT. W2K distingue quatre types de connexions sur le système : la connexion interactive classique à la console, la connexion secondaire pour se connecter sous une autre identité sans être obligé de se déconnecter, la connexion *batch* et enfin une connexion pour les objets et des accès confinés à des applications.

Les limites de MS-Kerberos

L'authentification MS-Kerberos n'est pas universelle et elle n'est pas utilisée par de nombreux systèmes de connexion à la machine. Les serveurs FTP et Telnet fournis dans W2K ne connaissent pas MS-Kerberos, tout comme les services Macintosh fournis en standard. Il n'existe pas de support de MS-Kerberos dans le *middleware* comme la messagerie MS-Exchange. Il n'y a pas de SSH (*Secure Shell*) fourni en standard, ni de SSH disponible supportant MS-Kerberos, ce qui constitue un frein important compte tenu de l'importance de SSH. De plus, il ne faut pas oublier que les clients habituels Windows 95 et 98 n'ont bien sûr pas de support pour MS-Kerberos. Tout cela limite donc très fortement la portée à court terme de MS-Kerberos.

Pour le développeur d'applications, Microsoft ne fournit pas les API (*Application Program Interface*) Kerberos, mais des API propriétaires spécifiques : SSPI (*Security Support Provider Interface*). Une application « cerberisée » (supportant Kerberos) ne peut pas être recompilée sur W2K. Les SSPI sont proches des GSS-API mais restent différentes et n'existent que sur W2K. À noter que les noms des royaumes MS-Kerberos sont obligatoirement les noms du DNS, seule la casse changeant. Un client W2K trouve le serveur Kerberos (KDC) auquel il doit s'adresser par le DNS qui

repose sur la bonne configuration du client.

En outre, il n'y a pas véritablement de compatibilité entre MS-Kerberos et Kerberos V diffusé avec DCE⁽¹⁾ (Solaris, Aix, HP-UX, OSF-1) mais reconnaissons qu'il n'y a quasiment pas d'utilisateurs de Kerberos dans DCE, ce n'est donc pas un inconvénient majeur. La sécurité dans MS-Kerberos repose sur le champ propriétaire SID dont le fonctionnement est tenu secret par Microsoft⁽²⁾. Enfin il ne faut pas oublier qu'une authentification centralisée de type MS-Kerberos peut être handicapante pour les utilisateurs en *dialup* car il est impossible de sortir d'un verrouillage écran si le réseau est coupé.

Une autre difficulté est de savoir quand l'authentification MS-Kerberos est utilisée. La seule solution est d'avoir un serveur Kerberos MIT et de le tester avec un compte déclaré uniquement dans ce serveur. Si cela fonctionne, c'était une authentification Windows NT, sinon, il s'agissait de l'authentification centralisée Kerberos. Enfin, le SP1 (service pack) de W2K propose aussi NTML v2, mais cela n'est pas documenté. Les attaques sont toujours possibles malgré l'authentification MS-Kerberos :

- la connexion anonyme (null session) permet par défaut la lecture de tous les objets ;
- la connexion anonyme par MSRPC permet d'avoir la liste des utilisateurs ;
- W2K a des comptes par défaut : Administrator, Guest, IUSR-systemname, etc. ;
- il est possible d'extraire les *hashes* de la SAM locale ou d'Active Directory, et les techniques de crackages seront alors utilisables⁽³⁾.

(1) Distributed Computing Environment

(2) L'article de Bruce Schneier explique ce problème : <http://www.counterpane.com/crypto-gram-0003.html#KerberosandWindows2000>

(3) voir les présentations de Patrick Chambet : <http://www.ossir.org/ftp/supports/2000/SecuW2K.zip> et Denis Ducamp : <http://www.hsc.fr/ressources/presentations/mdp2/mdp.htm>

L'authentification MS-Kerberos est utilisée pour :

- l'authentification initiale des utilisateurs à la console ;
- l'authentification auprès d'Active Directory ;
- l'accès à des fichiers distants par CIFS/SMB ;
- la gestion et la mise en place de permissions (referrals) sur des systèmes de gestion de fichiers distants ;
- le système d'impression ;
- les MS-RPCs et DCOM ;
- les mises à jour dynamiques du DNS ;
- IPsec ;
- la réservation de bande passante (QoS) ;
- l'authentification entre MS-Explorer et MS-IIS ;
- la demande de certificat auprès de MS-Certificate Server ;
- WinCE.

Zoom

■ Les principaux fournisseurs de *tokens* –

• Activcard propose ses *tokens* sur le principe du challenge/response, avec soit un serveur d'authentification propriétaire, soit un serveur LDAP Novell, ou une intégration directe dans les systèmes d'exploitation ou les applications. Activcard propose également des cartes à puce.

www.activcard.com/activ/products/

• SafeData propose une gamme complète de *tokens*. Outre les OS et les *firewalls*, Safe Data s'intègre avec les serveurs Web Microsoft IIS et Netscape, et des logiciels de tunnels chiffrés comme VPN-1. Différents types de Tokens sont utilisables : calculatrice challenge/response, carte à puces, clé USB, etc. Le serveur d'authentification (sous NT) peut utiliser un annuaire LDAP. SafeData permet également une authentification mutuelle : le client peut authentifier son serveur d'authentification.

www.safedata.com

• Le principe du *token* SecureID de RSA sans clavier est le mot de passe dynamique en fonction du temps. Ce *token* ne permettant pas de changement de pile. Lorsque celle-ci est épuisée il faut racheter un nouveau *token*. Depuis, RSA offre une gamme plus complète de *tokens* y compris des cartes à puces.

www.rsasecurity.com

• CryptoCard propose des *tokens* de type challenge/Response ou SecurID, ainsi que l'utilisation d'un Palm-Pilot comme *token*.

www.cryptocard.com/products/products.htm

• Secure Computing propose SafeWord qui marche sur le principe du Challenge/Response. Il permet une intégration avec Microsoft IIS et Netscape.

www.securecomputing.com/index.cfm?skey=21

• Vasco propose les *tokens* Digipass, sur le principe du challenge/response, avec un serveur Radius.

www.vasco.com/static/productsauth.html

Zoom

■ Architectures de SSO – Ces différents produits représentent des conceptions différentes d'architectures de Single-Sign-On, permettant un mot de passe unique aux utilisateurs.

• Architecture proposée par Axent : Client -> Authentification habituelle
Authentification habituelle <- Serveur SSO

• Architecture proposée par Evidian : Client -> Serveur SSO -> Authentification habituelle

• Architecture proposée par Computer Associates : Client -> Authentification habituelle -> Serveur SSO

• Architecture proposée par IBM-Tivoli : Client -> Serveur SSO

• L'architecture de CA, Client -> Authentification habituelle -> Serveur d'authentification, est classique. C'est celle retenue lorsque l'on utilise un serveur LDAP avec l'intégration de LDAP dans les clients, comme PAM sous Unix, les serveurs Web, ou des relais HTTP. Les architectures d'IBM et Evidian imposent un déploiement du logiciel client sur tous les postes utilisateurs, les autres ne l'imposent que pour les intégrations aux applications où le SSO se substitue à l'utilisateur au niveau de l'interface graphique. Cependant, seule l'architecture d'authentification Client -> Serveur SSO permet un véritable SSO.

■ Sites web des éditeurs SSO –
www.axent.com
www.evidian.com
www.evidian.com/accessmaster/webssso/
www.cai.com
www.tivoli.com

Le Single-Sign-On ou signature unique

Dans de nombreux systèmes d'information, la multiplication des mots de passe devient un problème aux conséquences concrètes. Chaque système a ses propres règles de construction et de gestion dans le temps des mots de passe, rendant plus complexe leur gestion quotidienne. Le Single-Sign-On (SSO) apporte à cette problématique une solution intéressante et sécurisée.

L'objectif du SSO est de centraliser l'authentification et de permettre ainsi l'utilisation d'un mot de passe unique. Si cette solution peut être mise en œuvre par le biais d'architectures diverses, une caractéristique constante est l'usage d'un serveur d'authentification centralisé pour toutes les authentifications. Les serveurs et la base d'authentification peuvent être répartis et dupliqués, mais la base du SSO est la centralisation de l'authentification. Elle n'est en effet plus disséminée sur des applications, des serveurs Windows NT, des serveurs Unix, un *mainframe* MVS, etc. Fort logiquement, le SSO permet également une centralisation et une consolidation des alarmes et de la journalisation. Sans être exhaustive, voici une sélection des différents produits disponibles.

• **Axent** propose **PassGo**, un serveur indépendant qui permet de synchroniser les mots de passe des utilisateurs sur l'ensemble des systèmes qui authentifient l'utilisateur, comme Unix, WNT, MVS RACF, Lotus Domino, etc. Cette technique facilite le déploiement d'un SSO au travers d'un mot de passe identique d'un système d'authentification à un autre. Le niveau de sécurité de l'entreprise est ainsi celui du système d'authentification le plus faible de la société.

• **Evidian** (anciennement BullSoft) avec **AccessMaster** est un leader du SSO. Il propose une première authentification vis-à-vis du serveur AccessMaster, qui va ensuite authentifier l'utilisateur sur chaque système d'authentification existant avec un mot de passe différent. AccessMaster supporte le *token* SSPI de W2K ou les certificats, et préfère l'usage de la carte à puces avec un système d'administration complet. Evidian a ajouté un relais HTTP, sans doute d'origine Netscape, appelé WebSSO. Ce relais permet d'utiliser AccessMaster comme système d'authentification sur des serveurs WWW.

• **Computer Associates** avait un système de SSO, **TNG**. Ce produit semble avoir été totalement abandonné par CA, même s'il n'y a pas eu d'annonce officielle. Désormais, CA commercialise Etrust SSO, anciennement Proxima SSO de la société israélienne MEMCO, qui avait été racheté par Platinum, elle-même rachetée par Computer Associates. Etrust SSO propose un serveur d'authentification qui est interrogé par l'authentification propre à NT, Netware ou un serveur

WWW. Etrust permet aussi une intégration aux PKI Entrust et ID2.

• **Tivoli** propose **GlobalSignOn**, ancien produit IBM passé chez Tivoli. GSO est basé sur OSF/DCE et Kerberos et s'interface au travers de PAM.

Les difficultés du SSO

La caractéristique commune aux produits de SSO est la difficulté à les déployer dans une grande organisation. Les principales difficultés sont :

- le support des authentifications existantes dans les systèmes d'exploitation et les applications ;
- le déploiement : la migration de l'existant vers le SSO ;

- l'administration et la mise à jour ;
- l'intégration faible dans les technologies Internet, avec les serveurs WWW, les annuaires ;
- le coût, en notant toutefois qu'il reste généralement inférieur à celui du déploiement d'une infrastructure de clés avec des certificats.

Si les logiciels de SSO ne présentent pas le caractère de nouveauté d'autres technologies, il s'agit cependant d'une technologie d'avenir, de par son rôle dans la gestion globale des profils des utilisateurs. L'évolution des SSO doit à présent se porter vers une intégration plus aisée dans le système d'information, avec des serveurs d'authentification et des clients utilisant des protocoles standards. L'intense présence marketing des fournisseurs de PKI devrait également favoriser la migration vers l'usage des certificats. ■

Dossier réalisé par Hervé Schauer
www.hsc.fr

La gestion des profils des utilisateurs

La gestion des utilisateurs constitue un complément indispensable à la signature unique. Les logiciels de SSO prennent en charge cette fonction, mais il existe également des logiciels spécialisés dans ce domaine, qui ne sont pas perçus comme SSO. Pour exemples :

• BMC Software

BMC propose Control-SA un ancien produit de Boole and Babbage, qui permet une administration globale des utilisateurs sur des plates-formes hétérogènes, ainsi qu'une synchronisation des mots de passe.
www.bmc.com

• Access360

EnRole est à l'origine une solution de SSO, mais s'est orientée vers la gestion des utilisateurs, typiquement pour les portails Internet utilisant une notion de souscription et d'authentification des utilisateurs.
www.access360.com/products6.html

• Oblix

Secure User Management Solution se place au-dessus d'un annuaire LDAP (Microsoft, Iplanet, Novell, etc) et permet des facilités de gestion et de configuration des profils utilisateurs.
www.oblix.com/solutions/solu_secureuser.html