SÉCURITÉ INFORMATIQUE
numéro 46 octobre 2003
SÉCURITÉ DES SYSTÈMES D'INFORMATION

La sécurité des systèmes d'information : un enjeu réaffirmé

éditorial

Le Premier ministre a tenu à le rappeler dans sa circulaire du 4 avril 2003 : «la sécurité des systèmes d'information de l'État est un enjeu de première importance pour les pouvoirs publics».
Dans le dispositif interministériel en place visant à garantir cette sécurité, le Fonctionnaire de Sécurité de Défense a, pour ce qui est du CNRS, un rôle essentiel à jouer, que Philippe Schreiber a su initier en son temps et qu'Alfred Schwenck a poursuivi avec ténacité.
Alfred Schwenck nous a quittés fin juillet pour d'autres horizons… très proches, puisqu'il continuera à œuvrer pour la sécurité au sein de l'équipe du Haut Fonctionnaire de Défense du ministère de la Jeunesse, de l'Éducation nationale et de la Recherche.
Nommé début septembre Fonctionnaire de Sécurité de Défense du CNRS, je profite de ce premier éditorial pour saluer les lecteurs de *Sécurité Informatique* et leur confirmer toute l'importance que j'attache à la sécurité des systèmes d'information qui est et demeure une composante majeure des missions du FSD.
Dans la continuité du travail antérieur et avec la mobilisation des acteurs du CNRS déjà engagés dans cette aventure, l'effort devra donc être maintenu et conforté.
Faciliter une vision stratégique de la sécurité des systèmes d'information au CNRS, dans le contexte de l'action interministérielle, organiser et resserrer les équipes actuelles autour d'objectifs clairs et partagés, faciliter l'appropriation de la culture SSI par tous, constituent d'ores et déjà des objectifs que l'on peut pressentir comme prioritaires.
Dans un contexte, où la sensibilisation et l'information constituent effectivement une large part du dispositif, *Sécurité Informatique* est un outil d'accompagnement qui se doit d'être pertinent et efficace. C'est en tout cas l'ambition de ce présent numéro largement consacré aux techniques d'authentification, qui, comme on le verra, se distinguent de celles de l'identification. Identifier quelqu'un, c'est lui attribuer une identité, l'authentifier, c'est s'assurer qu'on a bien affaire à la personne à laquelle on pense. L'authentification est donc à la base de toute sécurité.
Mais vous en saurez plus en vous plongeant dès à présent dans les articles passionnants et argumentés qui vous sont proposés : M^me^ Caline A. Villacres nous présente un recensement des principales techniques utilisées, où il apparaît que robustesse de la technique et facilité d'emploi sont bien contradictoires. Pourtant des voies nouvelles sont explorées pour rendre l'authentification à la fois plus sûre et moins contraignante pour les utilisateurs. Parmi elles l'authentification «biométrique» (sous ses diverses formes) semble extrêmement séduisante, et bénéficie d'ailleurs d'un très fort engouement… mais les promesses seront-elles tenues ? Non, nous dit, preuves à l'appui, Philippe Wolf, dans un article qui refroidira sans doute les enthousiasmes.
À vous de juger.

Joseph Illand
Fonctionnaire de Sécurité de Défense

De l'authentification biométrique

La biométrie [1], prise dans sa définition moderne [2], est, aujourd'hui, une technique d'identification en pleine évolution qui génère une activité étatique (police et justice) et industrielle très importante. Il semble dès lors naturel d'introduire la biométrie dans le champ de la sécurisation des systèmes d'information, notamment par son application à l'authentification.

Cet article traite de l'authentification biométrique, sujet à la mode dont il convient de situer les principes et surtout les limites en terme de sécurité. Après un rappel des définitions essentielles de la SSI (Sécurité des Systèmes d'Informations), la fonction d'authentification est décrite en détail à travers ses principes de réalisation et quelques-unes de ses applications les plus courantes.

Définitions générales

En France, les fonctions essentielles à satisfaire en SSI sont les suivantes (triptyque DIC) [3] :
Disponibilité : prévention d'un déni non autorisé d'accès à l'information ou à des ressources. Assurance que l'information, les services, et les ressources du SI sont accessibles aux personnes ou programmes autorisés, dans des conditions définies d'horaires, de délais et de performances et protégés contre les dénis de service.
Intégrité : propriété assurant que des données n'ont pas été modifiées ou détruites de façon non autorisée, que le système ou l'information traitée ne sont modifiés que par une action volontaire et légitime ; lorsque l'information est échangée, l'intégrité s'étend à l'authentification du message, c'est-à-dire à la garantie de son origine et de sa destination.
Confidentialité : propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés. Assurance que l'accès à une information d'un SI est limité aux seules personnes, applications, programmes, équipements admis à la connaître.

Dans l'Union Européenne, le concept de cyber-sécurité [4] ajoute la fonction suivante :
Authentification : l'authentification a pour but de vérifier l'identité dont une entité se réclame. Généralement l'authentification est précédée d'une identification qui permet à cette entité de se faire reconnaître du système par un élément dont on l'a dotée. En résumé, s'identifier c'est communiquer son identité, s'authentifier c'est apporter la preuve de son identité.

suite page 2

CNRS CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

suite de la page 1

Enfin, aux USA (concept d'Information Assurance [5]), il convient d'ajouter aux quatre fonctions précédentes :

La non répudiation : la répudiation est le fait de nier avoir participé à des échanges, totalement ou en partie. La non répudiation introduit la notion juridique d'imputabilité.

À ces cinq fonctions, il conviendrait d'ajouter une sixième fonction de protection de la vie privée, qui est essentielle dans les systèmes d'information manipulant les données personnelles protégées par la loi et qui sera centrale dans des systèmes futurs comme le vote électronique.

Ces approches du même problème ne sont pas contradictoires, mais complémentaires. Dans l'approche française, on distingue les propriétés de sécurité («Features») Disponibilité, Intégrité (dont Preuve), et Confidentialité, des fonctions qui y concourent («les supportent») dont l'Identification/Authentification, le Contrôle d'accès, et la Non répudiation qui sert à améliorer l'aspect intégrité de la preuve. La fonction d'authentification, liée dans l'approche française aux questions d'intégrité, est distinguée dans les autres approches, ce qui en marque l'importance centrale. Elle fait l'objet depuis les débuts de l'informatique d'une attention et d'un traitement tout à fait particuliers.

Principes de l'authentification

Précisons quelques éléments de la définition de l'Authentification donnée ci-dessus.

Dans cette définition, l'entité peut être soit une personne désirant utiliser un dispositif de traitement de l'information (carte à puce, ordinateur, équipement électronique quelconque), soit un dispositif électronique : les machines fonctionnent aujourd'hui en réseau et doivent se reconnaître entre elles. Dans le premier cas, l'authentification intervient après une phase d'identification qui consiste à établir l'identité annoncée par l'utilisateur. Elle est indispensable à la mise en œuvre :

- du contrôle d'accès, qui consiste à administrer et à vérifier les droits que la politique de sécurité confère à chaque utilisateur,
- de l'imputabilité, qui consiste à enregistrer l'usage des droits des utilisateurs, les tentatives infructueuses et les accès illicites de leur exercice, afin de pouvoir attribuer les responsabilités ou détecter les anomalies et y remédier dans les meilleurs délais.

On parle souvent de la phase d'identification — authentification ou I/A.

Pour définir l'identité dont une entité (humaine ou machine) se réclame, on distingue quatre familles de conventions qui permettent de concevoir des pièces d'identité :

1. *Un secret que le titulaire partage et peut énoncer, transcrire ou utiliser*

   Exemples : un mot de passe, un code porteur (PIN), une clé de chiffrement.

2. *Un objet que le titulaire possède comme un bien matériel.*

   Exemples : une clef, une carte d'identification (à code à barre, à bande magnétique, à mémoire), une télécommande (infrarouge, radio).

3. *Un caractère de la personne.*

   Exemples : un caractère physique (biométrique) : l'empreinte digitale, palmaire, rétinienne, auriculaire, du profil, de l'ADN, etc.

4. *Un savoir faire de la personne.*

   Exemples : le résultat d'une action spontanée comme la signature manuscrite, un signal de la voix, la reconnaissance de portraits (mimiques) ; les mécanismes exploitant ces objets sont encore du domaine de la recherche.

On considère qu'une authentification forte consiste en l'usage combiné d'objets de la première et de la deuxième famille (code porteur et carte à puce par exemple) ; cette solution conduit à l'enchaînement conditionnel de deux mécanismes.

Exemples d'usage de l'authentification

Exemple 1 : dans le domaine de l'informatique personnelle (au sens de poste de travail personnel dans un usage professionnel ou domestique), l'authentification est réalisée, dans une proportion très importante, par la saisie d'un mot de passe. Le dispositif peut être consolidé par un «token» matériel (clé USB ou carte à puce). La principale difficulté consiste ici à former les utilisateurs au choix d'un mot de passe fort (de longueur suffisante et absent des dictionnaires sophistiqués utilisés dans les techniques intrusives), à les sensibiliser au fait que ce mot de passe est une donnée personnelle qui ne peut être partagée (il s'agit là d'une difficulté psychologique trop souvent négligée), et à imposer, dans un usage professionnel principalement, des changements de mots de passe après une durée d'usage définie dans le cadre de la politique de sécurité du système d'information auquel appartient le poste de travail.

Exemple 2 : Carte de paiement (carte à puce). Elle fait appel à trois mécanismes d'authentification :

- une authentification du porteur humain de la carte par un code pin (de 4 chiffres) ;
- une authentification locale, statique entre la carte et le terminal de paiement du commerçant pour les achats de faible montant utilisant une technique cryptographique dite à clé publique. C'est ce mécanisme qui avait été percé lors de l'affaire de la «Yescard» ;
- une authentification distante et dynamique entre la carte et la banque pour les montants plus élevés utilisant une technique cryptographique à clé secrète.

Exemple 3 : Achat en ligne. Dans une procédure d'achat en ligne (sur Internet), le client authentifie le serveur du cyber-commerçant en vérifiant, grâce à un certificat numérique dont il dispose sur sa machine, la signature du site auquel il accède. Il utilise pour cela le protocole SSL (Secure Socket Layer marqué par un cadenas fermé sur les navigateurs usuels) dans un mode particulier. Dans la majorité des cas, le serveur commerçant n'authentifie pas son client, mais l'identifie à partir des donnée fourniess (numéro de carte de paiement, données personnelles du client et date de validité par exemple).

Exemple 4 : Téléprocédure «impôts en ligne» ou «télé-tva». Le fonctionnement de ces téléprocédures sécurisées ajoute à l'authentification du site du Ministère des finances (mécanisme identique à l'exemple 3) une authentification du contribuable à partir soit d'un bi-clé généré sur sa machine pour le citoyen lors d'une première phase ou d'un bi-clé acheté par l'entreprise auprès d'un opérateur de certification. Les protocoles utilisés offrent ici une authentification mutuelle.

Mise en œuvre de l'authentification biométrique

Le principe de réalisation de l'authentification biométrique se présente en cinq phases :

- Phase 1 : présentation de la donnée biométrique par la personne à authentifier [6] ;
- Phase 2 : acquisition de cette donnée par un lecteur biométrique ;
- Phase 3 : traitement de cette donnée par un dispositif électronique qui la transforme en une information numérique, sous forme d'un fichier ; ce codage peut faire appel à des techniques cryptographiques ;
- Phase 4 : comparaison de ce fichier caractérisant la personne à authentifier avec une donnée de référence (quand la personne s'est identifiée au préalable) ou des données pré-stockées de

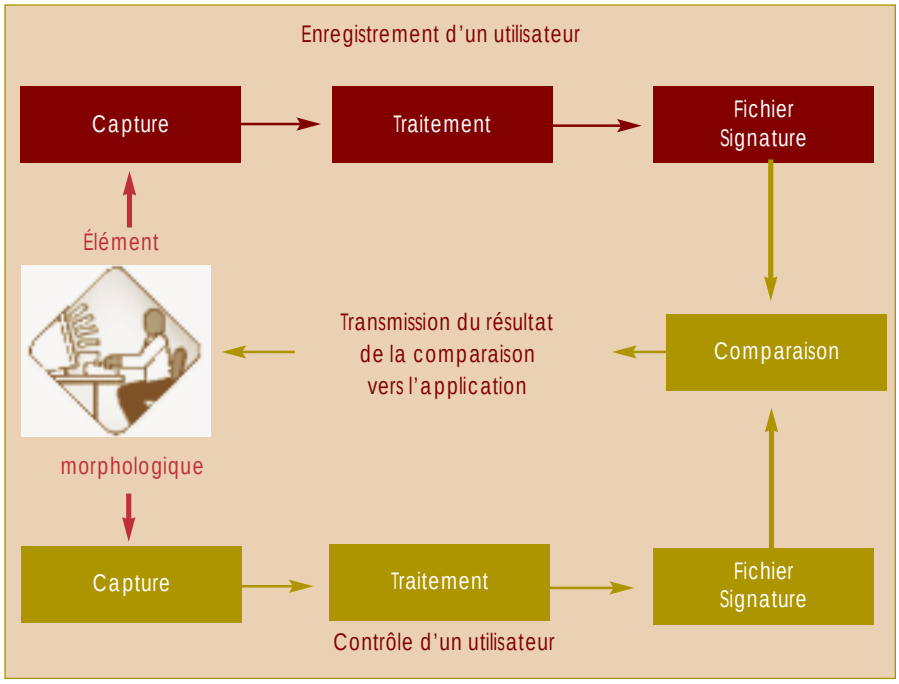
suite page 3

suite de la page 2

références (représentant l'ensemble des personnes que l'on souhaite authentifier) ;

- Phase 5 : décision, à partir de la comparaison effectuée en phase 4, d'authentifier ou non la personne grâce à une fonction mathématique ou statistique (on retrouve la définition initiale de la biométrie). Ici, la décision binaire (réponse par oui ou non) est propagée (de manière sûre de préférence) au dispositif informatique demandant l'authentification.

En voici un schéma simplifié [7] :



Donnons quelques exemples de dispositifs d'authentification biométriques :

- La souris à reconnaissance digitale (limitée aux phases 1 et 2 et/ou 3, les phases 4 et 5 sont souvent réalisées par l'ordinateur) [8]
- Dispositifs combinant reconnaissance d'empreinte digitale et carte à puce [9]
- Un dispositif à reconnaissance de fond d'œil [10]
- Un dispositif de stockage de masse (clé USB) [11]

Beaucoup d'assistants personnels (PDAs) sont aujourd'hui équipés d'un dispositif d'authentification biométrique [12]. Le marché de l'authentification biométrique est en plein essor, marqué principalement par les techniques de reconnaissances d'empreintes digitales.

SSI et authentification biométrique

La force (en tant que résistance à des attaques) du schéma décrit ci-dessus réside dans son maillon le plus faible. Nous examinerons successivement les deux maillons les plus faibles.

Faiblesse n° 1 : usurpation de la donnée biométrique (phase 1)

Pour leurrer un dispositif d'authentification biométrique, la première idée venant à l'esprit consiste à se doter de la caractéristique biométrique de la personne dont on souhaite usurper l'identité et donc les droits.

Un travail récent [13], montre la simplicité de fabrication d'un faux doigt. Deux procédés de fabrication (de l'achat des matières premières en magasin pour une somme dérisoire à la fabrication et au leurrage de systèmes commerciaux) y sont décrits en détail :

— comment leurrer le dispositif avec une prothèse de son propre doigt ;

— comment leurrer le dispositif avec une prothèse du doigt d'une tierce personne dont on aura prélevé l'empreinte (lors d'un cocktail par exemple).

La presse a relaté cette expérience sous la forme suivante : «*Un mathématicien japonais, Tsutomo Matsumoto, a démontré en direct, lors de la Conférence de l'Union des Télécommunications internationales sur la sécurité, qui s'est déroulée à Séoul à la mi-mai, le peu de fiabilité qu'il fallait accorder aux lecteurs biométriques d'empreintes digitales supposés inviolables et passant pour être le système de sécurité le plus fiable. Avec de la gélatine pour confiseries, il a fabriqué, avec l'aide d'un moule, une maquette de doigt utilisant une empreinte qu'il avait relevée sur un verre avec la technique simple du scotch-adhésif. Il l'a ensuite photographié numériquement puis rehaussé au niveau des contrastes dans un logiciel de retouche courant avant de l'imprimer sur un papier transparent qu'il a ensuite rendu photosensible avec une technique tout aussi simple. Sur les quinze principaux lecteurs biométriques disponibles sur le marché, onze ont été piégés.*»

Ces prothèses mises sur son propre doigt permettent de tromper les dispositifs anti-doigt mort (circulation sanguine et chaleur) usuels. Des dispositifs plus sophistiqués (détection sous l'épiderme) existent et compliquent la tâche du faussaire mais ne semblent pas l'interdire complètement [14]. L'usage de films plastiques (alimentaires ou autres) permet, encore plus facilement, de leurrer certains systèmes d'authentification à empreinte digitale. Sur le même sujet on consultera une étude [15] qui décrit la fabrication en trois heures d'un faux doigt par des procédés accessibles.

Pour les autres marquants biométriques (forme de la main, lobe de l'oreille, portrait, ADN, etc.), il n'est pas difficile d'imaginer des méthodes d'usurpation [16].

Faiblesse n° 2 : divulgation de la donnée biométrique (phase 3)

Ce qui fait l'intérêt d'une donnée biométrique dans l'identification, à savoir le lien quasi unique entre cette donnée et son propriétaire [17], devient dans le cadre de l'authentification une vulnérabilité majeure. Contrairement à un mot de passe ou à une clé, il est difficile de changer la donnée biométrique d'un individu. Le récent film de science-fiction *Minority Report* aborde d'un point de vue futuriste le problème de l'authentification par fond de l'œil ce qui oblige le héros à subir une opération de transplantation des yeux très spectaculaire. *La donnée biométrique ne peut pas être modifiée* à la suite d'une *compromission* qui devient de ce fait définitive. On peut changer un mot de passe, une clé de chiffrement, un certificat numérique, mais on ne peut malheureusement pas changer une donnée biométrique.

Le deuxième maillon faible consiste donc dans la *divulgation* d'une donnée biométrique d'une personne, invalidant de ce fait l'usage ultérieur par cette personne de tout dispositif d'authentification biométrique. Par exemple, la publication sur Internet ou dans des cercles plus restreints d'une photographie du ou des doigts d'une personne, ou pire encore d'un fichier normalisé des points caractéristiques de cette empreinte biométrique, permet d'usurper, à peu de frais, l'identité de cette personne. Pour les caractéristiques biométriques de l'œil d'une personne, le recueil pourra se faire lors suite page 4

suite de la page 3

de l'usage détourné d'un dispositif adéquat. La protection de la base de données biométriques devient cruciale.

De nombreuses bases de données de caractéristiques biométriques existent aujourd'hui pour des besoins d'identification. Plus d'un milliard d'empreintes ont été traitées à ce jour par le système vendu par la société Sagem [18]. La plupart des pays sont dotés d'un système d'identification par empreinte digitale. Des projets de recueil, plus massif, de données biométriques ont démarré. Citons, par exemple :

— le projet de base de donnée «Total Information Awareness» [19] qui privilégie la donnée biométrique ;
— le recueil d'informations biométriques aux frontières. La décision est prise aux États-Unis. Cela concerne à la fois l'empreinte digitale, le fond de l'œil et le portrait. «Les ministres de l'intérieur et de la justice du G8, qui se sont réunis à Paris, lundi 5 mai 2003, se sont d'ailleurs engagés à recourir à la biométrie comme méthode d'identification de leurs citoyens. Les États-Unis ont déjà fixé, en effet, à octobre 2004 la date à partir de laquelle les contrôles recourant à la biométrie des titres de transport et d'identité seront nécessaires pour l'entrée sur le territoire américain.» [20] ;
— des systèmes d'identification à distance [21].

Les données biométriques d'un individu ont donc une très forte probabilité d'être recueillies et stockées dans de multiples bases de données.

Cela contredit le principe de sécurité suivant : un élément authentifiant doit être localisé uniquement dans le périmètre de sécurité du système d'information qu'il est censé protéger.

La donnée biométrique doit donc être considérée comme une donnée publique ce qui suffit à déconseiller l'usage de la biométrie pour l'authentification.

D'autres problèmes qui touchent, plus généralement, les dispositifs d'authentification peuvent encore être évoqués rapidement.

Autres problèmes

En phase 2, le dispositif d'acquisition doit mettre en œuvre des stratégies qui peuvent révéler des faiblesses. Une étude récente [16] en détaille quelques-unes :

- désactivation (déni de service) du dispositif d'authentification biométrique ;
- activation (usurpation d'identité) de la reconnaissance, après qu'une personne licite se soit authentifiée.

L'analyse de risque de l'usage de ces dispositifs, en particulier pour le nomadisme, doit envisager ces attaques.

En phase 4, il est bien sûr fortement recommandé de protéger les données biométriques de référence en les chiffrant et/ou en utilisant une enceinte de sécurité inviolable.

En phase 5, le programme informatique réalisant la décision doit être protégé en intégrité.

Pour contourner ces protections, il peut être envisagé pour un attaquant de récupérer les données biométriques avant traitement. Cela peut être l'objet d'un cheval de Troie comme dans l'exemple qui suit. La plupart des dispositifs actuels utilisent le port USB d'une machine. Grâce à une attaque par le port USB (utilisant un logiciel de type usbsnoop [22]), des chercheurs [16] ont reproduit l'image d'une empreinte digitale qui peut être interceptée (en clair) sur un bus USB. Les attaques correspondantes consisteront généralement à remplacer le dispositif externe de mesure par un «yes-token». La connaissance «théorique» de la valeur de la donnée biométrique attendue n'est pas forcément nécessaire. Dans les cas où elle l'est, il ne sera pas utile de tenter de la reproduire sous une forme «biométrique» (rejouer l'image d'une empreinte sur un bus USB ne nécessite pas de mettre cette empreinte sur un doigt).

On peut également remarquer, par analogie avec un VPN (réseau privé virtuel consistant à établir un tuyau de communication chiffré entre deux entités informatiques), que «l'authentification biométrique» (comme souvent l'authentification usuelle par mot de passe d'ailleurs) est ponctuelle : elle intervient en début de session, mais ne fournit pas de garantie en soi que les commandes exécutées en cours de session proviennent bien de la personne qui s'est connectée.

Quand on examine un dispositif d'authentification, quel qu'il soit, il faut se poser ces bonnes questions et développer des architectures de confiance adaptées.

Causes possibles de la fascination actuelle

La première cause de cette fascination est liée à la confusion entre identification et authentification décrite dans l'article. Cette confusion est entretenue par les usages actuels en identification qui se développent comme le contrôle d'accès physique.

Une deuxième cause est liée à la commodité d'emploi de l'authentification biométrique, vantée par ses promoteurs. Il s'agit cependant de nuancer cela : les faux rejets entraînent une frustration évidente d'une personne autorisée. Enfin certains dispositifs provoquent des résistances tout à fait naturelles. Il est très difficile aujourd'hui pour quiconque de mettre ses yeux devant un dispositif de reconnaissance de l'iris.

Une anecdote, rapportée par un informaticien, vaut d'être racontée : «Mon patron m'a appelé à trois heures du matin du Japon pour me demander le mot de passe de son portable qui lui était absolument indispensable pour sa réunion de travail. À son retour, je l'ai doté d'une souris à reconnaissance d'empreinte digitale pour son portable. Depuis je n'ai plus d'ennuis.» Où est le souci de sécurité dans cette histoire, malheureusement réelle ?

Une troisième cause est liée à l'imagerie diffusée par les médias de ces dispositifs (films d'espionnage, films policiers) qui fascinent par leurs technologies encore considérées comme futuristes.

Une quatrième cause est liée à l'absence d'analyse des failles des dispositifs d'authentification biométrique par les articles de vulgarisation qui vont parfois jusqu'à les présenter comme totalement inviolables. L'évaluation «sécurité» indépendante s'impose ici comme ailleurs en SSI. Il est à noter que la compréhension de la biométrie est plus immédiate que celle des techniques mathématiques cryptographiques d'où une confiance accordée plus naturellement, à tort. ■

Faux problèmes

Pour en revenir à l'authentification biométrique, les taux suivants ont été définis :

- T.F.R. - Taux de faux rejets : pourcentage de personnes rejetées par erreur.
- T.F.A. - Taux de fausses acceptations : pourcentage d'acceptations qui n'auraient pas dû être retenues.

Le taux de faux rejets est un paramètre essentiel d'acceptabilité de ces techniques : rien de plus frustrant pour un utilisateur légitime que de se faire rejeter, sans même parler de déni de dispositif.

Une fausse acceptation, elle, introduit le loup dans la bergerie. Une authentification biométrique est par nature non prédictible.

suite page 6

Un point sur l'authentification

Des contraintes de mise en pages nous ont obligés à abréger cet article.
Vous pouvez retrouver la version intégrale à l'URL http://www.cnrs.fr/Infosecu/Revue.html

*L'**authentification** est la vérification d'informations relatives à une personne ou à un processus informatique. L'authentification complète le processus d'identification dans le sens où l'authentification permet de prouver une identité déclarée. Dans un serveur, un processus de contrôle valide l'identité et après authentification, donne l'accès aux données, applications, bases de données, fichiers ou sites Internet. Dans le cas contraire, l'accès est refusé.*

Méthodes courantes d'authentification

1 - Mots de passe

Les mots de passe pris dans leur ensemble sont le moyen d'authentification le plus répandu à ce jour. On distingue deux catégories : les mots de passe statiques et les mots de passe dynamiques.

Les mots de passe statiques sont ceux qui restent identiques pour plusieurs connexions sur un même compte. Ce type de mot de passe est couramment rencontré sous Windows NT ou Unix. Cette technique d'authentification est la plus utilisée mais aussi la moins robuste.

Les mots de passe dynamiques quant à eux sont modifiés à chaque session. Parmi ces mots de passe à usage unique — One Time Password (OTP) en anglais —, on trouve notamment le programme SKEY dont la sécurité repose sur une fonction à sens unique. En version logicielle, les générateurs de mots de passe dynamiques utilisent certains composants du PC, comme le microprocesseur, le CPU ou l'horloge interne (on parle alors de méthode d'authentification en mode synchrone dépendant du temps). Que le mot de passe à usage unique soit obtenu à partir d'un générateur matériel ou logiciel, l'utilisateur est authentifié de manière forte grâce à la vérification du mot de passe dynamique par un serveur appelé serveur d'authentification.

Le Single Sign On (SSO) est une technique qui, en donnant un point d'entrée unique pour tous les systèmes, permet d'éviter aux utilisateurs de retenir de trop nombreux mots de passe : c'est essentiellement une mesure pratique qui ne renforce en aucun cas la robustesse du processus de contrôle d'accès au SI. Le problème est la capacité de ce point d'entrée à résister à une malveillance, un dysfonctionnement ou une attaque venant d'Internet.

Par ailleurs, l'authentification peut aussi reposer sur un protocole d'authentification réseau, le protocole Kerberos, qui permet de sécuriser les mots de passe statiques lorsqu'ils sont transmis sur le réseau. Ce protocole, créé par le Massachusetts Institute of Technology (MIT), utilise la cryptographie à clés publiques.

2 - Certificats de clés publiques

La cryptographie à clé publique peut être utilisée pour chiffrer des mots de passe. En outre, elle peut également être employée pour signer des données, qu'il s'agisse d'un contrat afin que les parties qui l'ont signé ne puissent pas en répudier le contenu a posteriori, ou qu'il s'agisse d'une valeur aléatoire pour assurer l'authentification. Les certificats de clés publiques sont l'une des techniques d'authentification les plus usitées à ce jour, certes loin derrière les mots de passe, mais ce moyen d'authentification devient de plus en plus populaire. Pour un usage personnel, les certificats des utilisateurs ainsi que de leur autorité de certification (AC) — éventuellement, hiérarchie de certification jusqu'à l'AC racine — sont souvent stockés dans les navigateurs (Microsoft Internet Explorer et Netscape Communicator). Ceux-ci comportent déjà par défaut un certain nombre de certificats d'AC racines (*cf.* Outils/Options internet/Contenu/Certificats). Notons pour information, qu'une mesure de sécurité est d'effacer (Remove) ces certificats lors de l'installation et de ne rajouter que ceux que vous autorisez.

3 - Biométrie

Nous renvoyons le lecteur à l'article de P. Wolf dans ce numéro.

Protocoles d'authentification couramment utilisés

1 - Protocole RADIUS

Le protocole RADIUS (Remote Authentication Dial-In User Service) développé par Livingston Enterprise et standardisé par l'IETF (*cf.* RFC 2865 et 2866) s'appuie sur une architecture client/serveur et permet de fournir des services d'authentification, d'autorisation et de gestion des comptes lors d'accès à distance.

2 - Protocole SSL

Le protocole SSL (Secure Socket Layer) développé par Netscape Communications Corp. avec RSA Data Security Inc. permet théoriquement de sécuriser tout protocole applicatif s'appuyant sur TCP/IP i.e. HTTP, FTP, LDAP, SNMP, Telnet, etc. mais en pratique ses implémentations les plus répandues sont LDAPS et HTTPS. Le protocole SSL permet non seulement de fournir les services d'authentification du serveur, d'authentification du client (par certificat à partir de SSL version 3), mais également les services de confidentialité et d'intégrité.

Afin d'éviter des attaques, il est recommandé d'utiliser la double authentification, c'est-à-dire non seulement l'authentification du serveur mais également celle du client, bien que l'authentification du client avec SSL soit facultative.

Le protocole TLS version 1.0 (Transport Security Layer) est la version normalisée de SSL version 3.0 (*cf.* RFC 2246 de l'IETF). Les versions de TLS sont amenées à évoluer, au moins au fur et à mesure que de nouvelles attaques apparaissent. En février dernier, une faiblesse majeure a été identifiée dans le protocole SSL : des chercheurs de l'École Polytechnique de Lausanne ont montré qu'il est possible en moins d'une heure de trouver le mot de passe d'un internaute connecté à un service d'eCommerce. Que l'URL (Uniform Resource Locator) soit «sûre» ou pas, c'est-à-dire qu'une société dont la réputation n'est plus à faire héberge ce site Internet ou bien qu'il s'agisse d'une compagnie dont la sécurité des transactions n'est pas une priorité, la faille de sécurité basée sur une usurpation d'identité était bien présente pour les plates-formes Linux, Unix, Solaris et dérivés. L'information a été rapidement transmise à l'organisation OpenSSL afin de mettre à jour le protocole et développer une nouvelle version de SSL qui résiste à cette attaque (*cf.* le site www.openssl.org pour les différentes mises à jour).

3 - Protocole WTLS

Le protocole WTLS (Wireless Transport Layer Security) est la transposition du protocole TLS dans le monde des réseaux sans fil. Cependant, les négociations entre le client et le serveur ont été adaptées afin de répondre aux contraintes du réseau «wireless». Ainsi le nombre d'en-têtes du protocole WTLS est réduit par rapport au protocole SSL et le taux de compression est supérieur pour le protocole WTLS puisque la bande passante est plus faible.

La passerelle WAP étant le cœur des échanges, il est essentiel d'en garantir la sécurité non seulement sur le plan logiciel mais également physique.

4 - Protocole 802.1X-EAP

Le protocole 802.1X-EAP crée une structure standardisée pour l'authentification mutuelle entre un poste client et un élément du réseau tel qu'un commutateur suite page 6

suite de la page 4

Conclusion sur la valeur SSI de l'authentification biométrique

L'utilisation de la biométrie comme moyen d'authentification dans le cadre d'une politique de sécurisation d'un système d'information est à déconseiller.
Les deux raisons fondamentales sont les suivantes :

- l'usurpation d'une donnée biométrique est réalisable par des techniques diffusées et accessibles ;
- une donnée biométrique ne se révoque pas quand elle est compromise ; or la donnée biométrique sera de plus en plus une donnée publique (au sens de la SSI).

En revanche, les capteurs biométriques sont utilisables pour faciliter l'opération d'identification préalable à une authentification, par exemple en remplaçant un login par une reconnaissance d'empreinte. Ce qui importe, c'est d'éviter de confondre ces deux opérations ; dans le cas précédent, le mot de passe nécessaire à l'authentification devra de toute façon être saisi après l'identification biométrique.

Philippe Wolf
Responsable du CFSSI à la DCSSI
cfssi@sgdn.pm.gouv.fr

(1) Définition du *Petit Robert* : science qui étudie, à l'aide des mathématiques (statistiques, probabilités), les variations biologiques à l'intérieur d'un groupe déterminé.

(2) Définition du site *Le Jargon Français* : Mesure du corps humain. En général à des fins d'authentification ou d'identification (empreintes digitales, rétiniennes...). Il est possible de numériser des empreintes digitales. Il est bien utilisé dans ce sens en France (traduction de «Biometric» en anglais) mais le vrai terme français devrait être anthropométrie... (http://www.tout-savoir.net/lexique.php)

(3) Voir site http://www.ssi.gouv.fr/fr/glossaire/index.html

(4) Voir site http://europa.eu.int/information_society/eeurope/news_library/pdf_files/netsec_fr.pdf

(5) Voir site http://niap.nist.gov/

(6) Notons que dans cette phase, les aspects psychologiques rentrent en ligne de compte : ainsi, la présentation de son œil est souvent mal reçue.

(7) Voir site http://biometrie.online.fr/

(8) Voir site http://www.sagem.fr

(9) Voir site http://www.oberthurcs.com/pages/productsandsolutions/banking_solutions_3.asp

(10) Voir site http://www.oki.com/en/otr/html/nf/otr-182-10-4.html

(11) Voir site http://www.bioslimdisk.com/index.htm

(12) Voir, par exemple, le site http://h40108.www4.hp.com/Produits/content/Fiche.asp?id=14143&p=5922&g=2277

(13) Voir sites http://www.itu.int/itudoc/itu-t/workshop/security/present/s5p4.pdf et http://cryptome.org/gummy.htm

(14) Voir http://www.keuning.com/biometry/Biometrical_Fingerprint_Recognition.pdf

(15) Voir http://www.keuning.com/biometry/Biometrical_Fingerprint_Recognition.pdf. Voir aussi la présentation synthétique http://www.keuning.com/biometry/Biometrics_2001.pdf

(16) Voir site http://www.heise.de/ct/english/02/11/114/

(17) Les partisans de l'empreinte numérique soulignent que, si deux jumeaux ont le même ADN, ils n'ont pas les mêmes empreintes digitales.

(18) Source : journées sur l'authentification organisée par le CELAR le 14 et 15 décembre 2000.

(19) Voir sites http://www.epic.org/privacy/profiling/tia/ et http://www.epic.org/privacy/profiling/tia/tiasystemdescription.pdf. Le projet du DARPA TIA devient Terrorist Information Awareness suite à des pressions au Congrès et ailleurs.

(20) Voir article «Pourquoi la signature électronique reste lettre morte» *Le Monde* du 23 mai 2003

(21) Voir site http://www.darpa.mil/iao/HID.htm

(22) Voir site http://sourceforge.net/projects/usbsnoop/

suite de la page 5

réseau (hub), un point d'accès sans fil, etc. en s'appuyant sur un serveur d'authentification (souvent de type RADIUS) et l'un des protocoles EAP (Extensible Authentication Protocols, RFC 2284 et 2716) possibles. Après mutuelle authentification entre le client et le serveur, une clé est dérivée pour le chiffrement de la communication. Comme une nouvelle clé est dérivée par 802.1X pour chaque nouvelle session entre le client et le serveur, cela s'apparente à une gestion dynamique des clés.

Conclusion

Les systèmes d'authentification à base de certificats X.509 semblent moins facilement attaquables et donc plus robustes que les systèmes basés sur les mots de passe. Mais un système jugé sûr aujourd'hui peut révéler des failles ou faiblesses demain. Nous nous souvenons de la chronique qui a fait la une de nombreux journaux en février 2000 racontant comment un informaticien a fabriqué une fausse carte à puce, appelée «yes card», capable de tromper un automate distribuant des tickets de métro et mettant ainsi en exergue une vulnérabilité dans le système d'authentification du porteur de carte bancaire. Il est donc primordial de garder à l'esprit qu'une méthode d'authentification avec zéro défaut n'existe malheureusement pas. La sécurité absolue est une utopie. Il est possible de réduire à un degré tolérable le risque d'usurpation de droit sur un système d'information en mettant en place des solutions d'authentification forte, mais la sécurité ne doit pas uniquement reposer sur cette procédure, quelle qu'en soit la robustesse supposée. La sécurité est un tout et d'autres mesures de sécurité doivent la compléter, comme la mise en place de séances de sensibilisation à la sécurité informatique, la diffusion aux utilisateurs de la politique de sécurité du laboratoire ou de l'entreprise, le cloisonnement de certains réseaux, etc. (De nombreux exemples sont présentés dans l'article sur les tableaux de bord de la sécurité du système d'information du numéro 45 de la revue.)

Caline Villacres
Ernst & Young LLP - Security & Technology Services
caline.villacres@ey.com

Références

- *Authentication : From Passwords to Public Keys*, par Richard Smith (éditeur : Addison Wesley).
- *Sécuriser ses échanges électroniques avec une PKI — Solutions techniques et aspects juridiques*, par Thierry Autret, Marie-Laure Oble Laffaire et Laurent Bellefin (éditeur : Eyrolles).
- les sites Internet suivants :
  http://www.ietf.org/rfc
  http://www.openssl.org
  http://web.mit.edu/kerberos/www/
- l'article de Caline A. Villacres dans Secure Computing Magazine du mois de Septembre, intitulé «Smart card *vs.* password» qu'on peut retrouver sur le site : http://www.scmagazine.com/scmagazine/2003_09/feature_1

SÉCURITÉ INFORMATIQUE
numéro 46 octobre 2003
SÉCURITÉ DES SYSTÈMES D'INFORMATION

Sujets traités : tout ce qui concerne la sécurité informatique. Gratuit.
Périodicité : 5 numéros par an.
Lectorat : toutes les formations CNRS.

Responsable de la publication :
ROBERT LONGEON
Centre national de la recherche scientifique
Service du Fonctionnaire de Défense
c/o IDRIS - BP 167. 91403 Orsay Cedex
Tél. 01 69 35 84 87
Courriel : robert.longeon@cnrs-dir.fr
http://www.cnrs.fr/Infosecu

ISSN 1257-8819
Commission paritaire n° 3105 ADEP

Conseil et coordination : CNRS - DIST - Jacqueline Leclère • Conception et réalisation : La Souris 01 45210961