L'école nationale supérieure d'informatique

Authentification Par biométrie

Goutal Soumeya 07

Messai Noussaiba 05

Sommaire

Problématique

Vue la sensibilité de certaines zones, leurs protection devient de plus en plus difficile et nécessite des techniques plus élaborées

Actuellement, la majorité des utilisateurs externes se connectent aux ressources de l'entreprise via Internet en utilisant une passerelle VPN sécurisée, une combinaison username/password et une authentification forte (SecurID, Mobile Token, SMS, Carte matricielle, Certificat, etc).

Il en est tout autrement au bureau, où en règle générale, c'est uniquement le binôme «username/password» qui permet l'accès aux données que celles-ci soient sensibles ou non

Par analogie, pour retirer de l'argent à un Bancomat dans la rue (utilisateur externe), on saisit son PIN code (quelque chose que l'on sait) et on insère sa carte bancaire (quelque chose que l'on possède) afin d'obtenir l'accès à son argent (ses données). Il ne serait pas imaginable, si vous vouliez retirez de l'argent à un Bancomat d'étage (en interne) de taper uniquement votre code PIN sans insérer votre carte

Il existe de nombreux cas d'usurpation d'identité en interne au moyen de keylogger logiciel ou plus simplement matériel (inclus des keylogger de type wifi) pouvant être facilement inséré par du personnel interne, consultant externe, ou toute autre personne ayant accès aux locaux.

Les entreprises en sont conscientes, et les nouvelles technologies d'authentification interne vont démocratiser l'authentification forte en entreprise, ce que certaine d'entres elles ont déjà fait.

Authentification par biométrie

Définitions

Biométrie

Analyse statistique des données biologiques d'un Individu.

Authentification

Procédure qui consiste, pour un système informatique, à vérifier
l'identité d'une personne ou
d'un ordinateur afin d'autoriser l'accès de cette entité à des ressources

Authentification par biométrie

Consiste à utiliser un système de reconnaissance basé sur les caractéristiques physiques ou comportementales d'un individu pour vérifier son identité.

Analyse morphologique

Identification par l'empreinte digitale réduite

La donnée de base est le dessin représenté par les crêtes et sillons de l'épiderme (jonctions, terminaisons aveugles, croisements...).
Une empreinte est caractérisée par une centaine de points particuliers (appelés minuties : un point qui se situe sur le changement de continuité des Lignes papillaires), dont seuls une douzaine suffisent pour une identification.
Certains modules de reconnaissance d'empreintes vérifient la température du doigt, sa conductivité, les battements de cœur, ainsi que d'autres paramètres biologiques - pour éviter de confondre un vrai doigt avec une fausse empreinte en gélatine.

Identification par la morphologie de la main

Ou « empreinte palmaire »
90 caractéristiques de la main sont analysées, dont la forme générale, les longueurs et largeurs des doigts, les formes des articulations...
Le taux d'erreurs peut être élevé entre personnes ayant le patrimoine génétique

Identification par l'iris

Cette technique peut être exploitable très tôt dans la vie d'une personne car la structure de l'iris est définitive dès la 8ième semaine de maternité !
Elle est très fiable du fait qu'il est possible de définir plus de 240 points caractéristiques.
Certains systèmes d'identification évolués permettent de contrôler que l'iris change bien de taille avec l'intensité de la lumière.

Identification par la rétine

Les schémas des vaisseaux sanguins de la rétine sont uniques pour chaque individu. Jusqu'à 400 points caractéristiques permettent de les différencier. La contrainte majeure de ce procédé est la proximité de l'œil par rapport au capteur

Reconnaissance faciale

Elle se base sur une photographie du visage décomposée en plusieurs images faites de nuances de gris, chacune mettant en évidence une caractéristique particulière non sujette à une modification (haut des joues, coins de la bouche,...).
Elle est très variable selon l'éclairage, l'expression...
Cette technique peut être utilisée sans obtenir le consentement de la personne identifiée.

Identification par thermographie

Une caméra infrarouge établit une cartographie des températures des différentes régions du visage - une caractéristique biologique qui est propre à chaque individu.
On peut aller même plus loin, en établissant une cartographie du système veineux

Analyse comportementale

L'analyse comportementale est dynamique, et est plus difficile à reproduire.

Authentification par une signature biométrique

Elle est basée sur l'analyse et le calcul de la dynamique d'une signature.
Ce système est basé sur des critères précis comme la pression, l'accélération, la souplesse, les courbes et plusieurs dizaines d'autres paramètres.

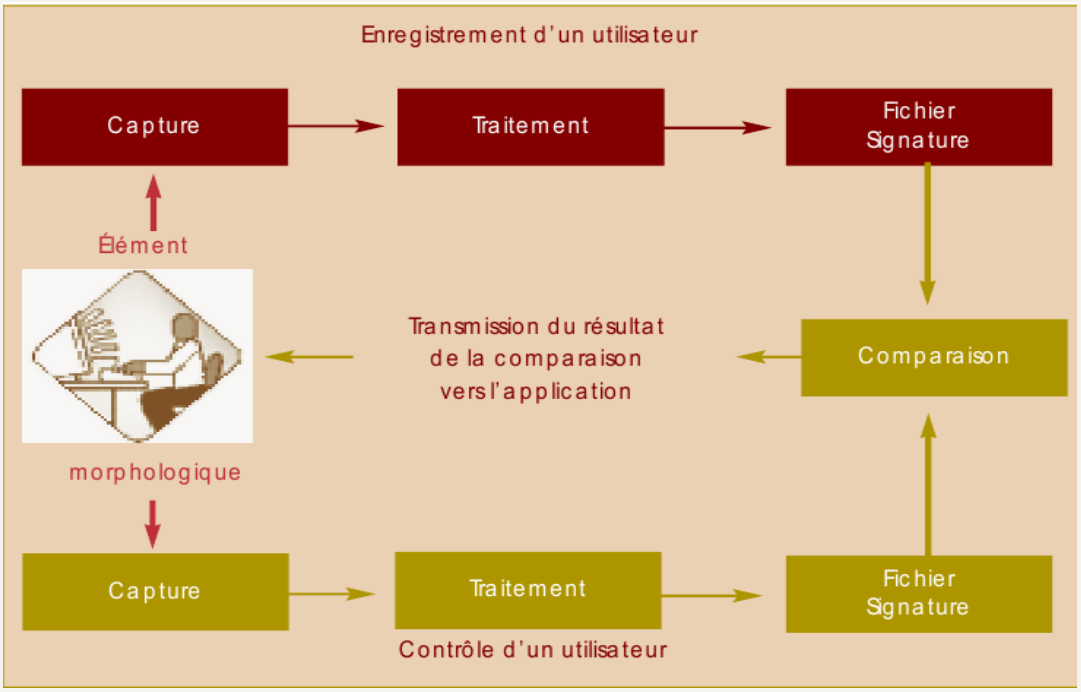
Identification par la voix

Elle est basée essentiellement sur la tonalité, la fréquence vocale et la distance entre la formation des lettres, et dépend grandement de la qualité d'enregistrement et de la méthode utilisée : on distingue les systèmes à texte prédéterminé où l'utilisateur doit répéter un texte qu'il ne choisit pas, et les systèmes où la personne peut parler librement.
De plus, on doit tenir compte de la variabilité de la voix du locuteur dans le temps comme dans le cas de maladie (rhume,...), et des états émotionnels. Cette technique peut être utilisée sans obtenir le consentement de la personne identifiée.

Mise en œuvre de l'authentification biométrique

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

- Phase 1 : présentation de la donnée biométrique par la personne à authentifier
- 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 sécurité informatique références (représentant l'ensemble des personnes que l'on souhaite authentifier)
- Phase 5 : décision, à partir de la comparaison effectuée en phase4, d'authentifier ou non la personne grâce à une fonction mathématique ou statistique.



Faiblesses de l'authentification par Un système biométrique

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.

La presse a relaté une expérience sous la forme suivante : «Un mathématicien japonais, Tutamoe Matsumoto, a démontré en direct, lors de la Conférence de l'Union des Télécommunications internationales sur la sécurité, le peu de fiabilité qu'il fallait accorder aux lecteurs biométriques d'empreintes digitales supposés inviolables.

Avec de la gélatine pour sa confiserie, il a fabriqué, avec l'aide d'un moule, une maquette de doigt utilisant une empreinte qu'il avait relevée sur un verre, 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

Sur les quinze principaux lecteurs biométriques disponibles sur le marché, onze ont été piégés.»

2 Divulgation de la donnée biométrique (Phase 3)

Contrairement à un mot de passe ou à une clé, il est difficile de changer la donnée biométrique d'un individu.

Par exemple, la publication sur Internet ou dans des cercles plus restreints d'une photographie des doigts d'une personne, ou encore d'un fichier normalisé des points caractéristiques de cette empreinte biométrique, permet d'usurper. Pour les caractéristiques biométriques de l'œil d'une personne, le recueil pourra se faire lors de l'usage détourné d'un dispositif adéquat donc 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.

Par exemple, les systèmes d'identification à distance 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.

3 Autres Problèmes

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

La plupart des dispositifs actuels utilisent le port USB d'une machine, grâce à une attaque par le port USB des chercheurs ont reproduit l'image d'une empreinte digitale qui peut être interceptée en clair sur un bus USB.

Biométrie révocable

L'expression « biométrie révocable » est définie pour la première fois dans les articles. Ce concept repose sur une transformation des données biométriques brutes, de telle sorte que les données transformées soient sûres et respectueuses de la vie privée, en accord avec les propriétés détaillées par Maltoni :

- Non-inversibilité : il ne doit pas être possible de retrouver des informations sur la donnée biométrique originale.
- Performance : l'efficacité du système de vérification ne doit pas être détérioré par la transformation.
- Diversité : on doit pouvoir générer plusieurs données protégées à partir d'une seule donnée brute. Le recoupement de différentes données protégées ne doit pas affecter la protection de la vie privée.
- Révocabilité : on doit pouvoir facilement révoquer les données en cas de compromission.

Les techniques de biométrie révocable permettent de ne jamais stocker les données originales : seules les données transformées sont conservées pour la vérification. La propriété de révocabilité est ainsi garantie : si une donnée transformée est compromise, il suffit de changer les paramètres de la fonction de transformation. La propriété de diversité est également assurée par le choix de fonctions différentes pour des applications distinctes. En outre, le système de vérification doit être sensible aux variations interclasse (pouvoir distinguer deux utilisateurs différents) et en même temps robuste aux variations intra classe (la donnée biométrique d'un utilisateur varie inévitablement, à cause de conditions de capture différentes, du vieillissement. . .).

Pour cela, les transformations de données biométriques utilisent une donnée ou clé secrète en plus de la donnée biométrique originale. L'enrôlement consiste à calculer la transformée de la donnée de référence à l'aide de la clé, puis à stocker cette donnée transformée. La vérification nécessite le calcul de la transformée de

la donnée présentée avec la clé de l'utilisateur, et la comparaison est effectuée entre les données transformées uniquement.

De nouvelles contraintes spécifiques à la biométrie révocable apparaissent. Le risque de compromission pèse sur la donnée biométrique transformée, mais aussi sur le secret. Par conséquent ces deux données ne doivent pas être stockées ensemble. Par ailleurs, la compromission de l'une de ces deux données ne doit pas permettre une usurpation d'identité. De la même façon, l'interception de données transformées (avec différents secrets) correspondant à des applications différentes ne doit pas permettre de remonter au secret, ni à la donnée originale.

Il y a deux types de transformations utilisées pour la biométrie révocable.

- Le premier type de transformation s'applique directement sur l'image de la donnée biométrique et utilise des représentations à base de texture, comme l'iris ou pour les empreintes digitales.

La donnée biométrique brute est ainsi modélisée par un vecteur de réels. Les descripteurs à base de texture (Gabor, LBP. . .) permettent de générer des vecteurs de taille fixe, contrairement aux minuties dans le cas des empreintes digitales.

- Le second type de transformation prend en entrée un vecteur binaire ou réel, extrait à partir de la donnée biométrique. Le respect des propriétés de robustesse intra-classe et de sensibilité interclasse, ainsi que la nature du vecteur de données originales vont avoir un impact sur le choix de la transformation

Les transformations de données biométriques les plus simples sont celles qui sont appliquées aux données binaires, comme l'iriscode(vecteur binaire de taille 2048 bits dérivé de l'image d'un iris

La sécurité de la biométrie basée une donnée secrète pour diversifier et masquer l'iriscode [23, 32]. Si cette donnée est compromise, il est possible soit de retrouver l'iriscode original, soit de construire facilement un autre iriscode dont l'image serait identique à la donnée transformée. La transformation binaire révocable la plus sécurisée est connue sous le nom d'engagement flou, basée sur les codes correcteurs. Néanmoins, cette technique ne peut être

appliquée qu'à des données binaires de taille similaire à un iriscode et ne peut donc pas être utilisée efficacement sur n'importe quelle modalité biométrique. La section suivante fait l'objet d'une transformation appliquée sur une telle donnée.

Conclusion

La biométrie est une technologie récente qui propose de nouveaux facteurs d'authentification pour des applications variées. Les schémas actuels sont basés sur de multiples modalités allant de la reconnaissance faciale et les empreintes digitales jusqu'à la biométrie comportementale comme la dynamique de frappe sur un clavier ou sur l'écran tactile d'un mobile. Le développement important des systèmes biométriques s'accompagne toutefois de nouvelles menaces, spécifiques à cette technologie, car les données biométriques sont des données personnelles, non-révocables et donc particulièrement sensibles. Les attaques et les vulnérabilités sur les systèmes biométriques incluent notamment l'usurpation d'identité, les attaques par substitution et par rejeu, la possibilité de créer une fausse donnée biométrique, l'utilisation secondaire non autorisée de la donnée suite à un vol, ou encore l'injection de virus informatiques dans le système lui-même.

Le modèle de sécurité traditionnel sur les systèmes biométriques, décrit par Ratha comprend notamment les vulnérabilités suivantes :

- la possibilité de présenter une fausse donnée biométrique au capteur (usurpation d'identité)
- la compromission de la base de données de référence ; la récupération des données biométriques (ou secrètes) qui transitent dans le système ou durant le procédé de comparaison
- la présentation par un attaquant de sa propre donnée

La mise en place de schémas assurant la protection des données biométriques est indispensable et fait l'objet d'une recherche spécifique depuis une dizaine d'années