Sécurité des systèmes d'informations

Etat de l'art des medias d'authentification

27 Janvier 2006

Michaud Matthieu	michau_m
Bauvin Germain	bauvin_g
Rofes-Vernis Pierre-Yves	rofes-_p

Sommaire

Introduction

Dans un système d'information sensible, l'authentification par une simple paire d'identifiant et de mot de passe n'est parfois pas satisfaisante. On met en concurrence un identifiant souvent connu du public et un mot de passe seulement connu de l'utilisateur. Un utilisateur est donc authentifié parce qu'il sait son mot de passe et qu'il est le seul.

Le recours à des algorithmes d'encryptions forts, symétriques ou asymétriques, est une première solution pour augmenter le niveau de sécurité de ce type d'authentification. Cela prévient de l'interception du mot de passe pendant son transport. Cependant, un mot de passe peut toujours être volé autre part. A sa saisie, par exemple en espionnant les frappes du clavier, ou sa validation, lors de la comparaison avec sa valeur connu du système d'authentification. N'importe quelle personne en connaissance de cette information est donc considérée comme l'utilisateur. En d'autres termes ce procédé est répudiable.

L'authentification forte consiste à ajouter d'autres facteurs. Pour y parvenir, les solutions proposées font souvent appel à des éléments matériels portatifs. A l'heure actuelle, il en existe à base de calculette, carte à puce et clef USB. L'utilisateur a besoin d'avoir un élément qui lui est propre en sa possession et non plus uniquement son mot de passe.

Des moyens cryptographiques forts protègent le contenu des medias. Ce document présente de manière synthétique l'offre d'authentification forte du marché ainsi que les technologies employées pour assurer le niveau de sécurité promis.

Les calculettes

L'un des éléments phares de l'authentification forte est l'utilisation de mot de passe à usage unique (*One Time Password* ou *OTP*). Plusieurs éléments sont utilisés pour calculer ces mots de passe. Cela peut être l'heure où il a été généré et un élément connu de l'utilisateur seul (mot de passe, PIN). Afin de faciliter la génération de ces jetons éphémères, certaines entreprises du domaine de la sécurité ont développé des systèmes, matériels et logiciels, qui se chargent de cette partie du travail. Nous ne nous intéresserons dans ce dossier qu'aux solutions matérielles.

Se présentant sous la forme d'un petit boîtier, contenant ou non un clavier (selon que l'utilisateur a des informations à renseigner ou non), la calculette dispose d'un écran LCD lui permettant d'indiquer à l'utilisateur le code à taper pour s'authentifier sur la machine ou le serveur désiré. Sur certains modèles, l'OTP est directement envoyer à l'ordinateur via USB.

En ce qui concerne le déploiement, il reste le même quel que soit le produit choisi. En effet, tout les jetons (en anglais *Token*), demandent à être initialisés par une semence (*Seed* dans la langue de Shakespeare), propre au client. Pour cela, seuls sont nécessaires un périphérique d'initialisation et le logiciel approprié. Un seul suffit pour toute une entreprise, permettant de configurer les différents paramètres de chaque jeton en un temps réduit. CryptoCard, par exemple, table sur 15 secondes environ par jeton.

Une fois chaque utilisateur en possession de son générateur, reste la mise en place logicielle. Elle consiste en la mise en place d'un serveur qui se charge de la centralisation des tâches d'authentification et de client pour contrôler l'accès aux machines et aux services de la société.

Vous trouverez un tableau récapitulatif des principales offres du marché à la page suivante. Elle est accompagnée d'une page d'illustrations de la plupart de ces produits.

Constructeur	Nom du produit	Format	Génération	Informations requises	Algorithme de Hachage			Prix
					AES	DES / (3)DES	Autre	
RSA Security	RSA SecurID 700	porte-clefs	toutes les 60sec	temporelle + Semence	X			65,00$
	RSA SecurID 800	clef USB*	toutes les 60sec	temporelle + Semence	X			/
	RSA SecurID 600	porte-clefs	toutes les 60sec	temporelle + Semence	X			/
	RSA SecurID 200	carte	toutes les 60sec	temporelle + Semence	X			/
	RSA SecurID 520	carte avec clavier	sur demande	temporelle + Semence + PIN	X			/
Vasco	DigiPass G01	porte-clefs	sur demande	temporelle + Semence		X		/
	DigiPass G03	porte-clefs	sur demande	temporelle + Semence		X		/
	DigiPass 250**	calculette	sur demande	temporelle + challenge		X		/
	DigiPass 260**	calculette	sur demande	temporelle + challenge		X		/
	DigiPass 300**	calculette	sur demande	temporelle + challenge		X		/
	DigiPass 550**	calculette	sur demande	temporelle + challenge	X	X		/
	DigiPass 560**	calculette	sur demande	temporelle + challenge	X	X		/
	DigiPass 580**	calculette	sur demande	temporelle + challenge	X	X		/
Alladin	eToken NG-OTP	clef USB*	sur demande	temporelle + Semence		X	RSA (1024 bits), SHA1	89,00$
ActivIdentity	ActivIdentity Token	porte-clefs avec touches	sur demande	temporelle + Semence + PIN	X			/
CryptoCard	Key Chain Token	porte-clefs	sur demande	temporelle + Semence	X	X	AES 128, 192, 256	69,00$
	Pin Pad Token	carte avec clavier	sur demande	temporelle + Semence + PIN	X	X	AES 128, 192, 256	69,00$

La colonne ‘Format’ correspond à la forme que prend le jeton
La colonne ‘Génération’ correspond à quand un nouvelle OTP est généré : à intervalle régulier ou bien lorsque l’utilisateur appuie sur un bouton ou entre son code PIN.
Enfin la colonne’ Information requises’ indique les information utilisées par le jeton pour générer l’OTP à un instant donné.

*: Ces jetons sont des hybrides, intégrant une interface USB en plus de l’écran LCD. Elle permet la mémorisation de couple identifiant/mots de passe pour des authentifications par medias USB.
**: Ces produits très complets proposent également d’autres fonctions, notamment la signature électronique.

RSA Security

RSA SecurID 700

RSA SecurID 800

RSA SecurID 600

RSA SecurID 200

RSA SecurID 520

Vasco

Alladin:

NG-OPT

ActivIdentity:

ActivIdentity Tokens

CryptoCard:

RB-1 PIN Pad

KT-1 Key Chain

Clef USB

Avec la forte démocratisation de l'USB, l'idée qui semble désormais évidente d'utiliser des clefs USB cryptographiquement protégées est apparue. On y stocke des informations confidentielles. Le contenu est irréversiblement encrypté, l'utilisateur peut y accéder s'il valide l'étape d'authentification (code PIN, emprunte digitale, …). En pratique, des clefs privées peuvent y être stockées et non plus rester sur un disque dur en attente d'être dérobé. Quitter le travail avec ses données sensibles apporte la tranquillité d'esprit.

Parmi les fonctionnalités supplémentaires il existe :

- Fournisseur de certificats

  Certains produits supportent le standard SSLv3 avec des certificats X.509. Cela permet de profiter des points forts de cette technologie largement utilisée. Dans un réseau comportant une autorité de certification, on bénéficie aussi d'une tierce partie et de la révocation.

- Echange de clefs Internet

  Pour sécuriser un flux IP, il est possible d'encapsuler des paquets encryptés dans des paquets en clair, c'est l'IPSEC en mode transport ou encore un VPN. Pour accomplir l'encryptage, les passerelles échangent des clefs pré-partagées puis des publiques. Certaines clefs USB cryptographiques prennent en charge le protocole d'échange de clefs Internet (IKE) pour établir des connexions réseaux sécurisé au niveau du protocole et non au niveau applicatif.

Voici une présentation des produits de référence sur le marché.

Constructeur	Nom du produit	Capacités cryptographiques	Administration / Deploiement	Coût
RSA Security	USB Authenticator	- Génération de clefs : DES, 3DES, RSA - Signature : RSA - Encryptage : DES, 3-DES, SHA-1	- Lecteur inclus sur la clef : pas d'interface si ce n'est le port USB - Avec RSA SecurID, authentification Windows et réseau - JavaCard Framework - Global Plateform - ISO 7816 compliant	58.50 $
CryptoGram	iKey	- Encryptage : 3DES	- Compatible avec CryptoGram SecureLogin et CryptoGram Folder - Compatible avec RSA PKCS #11 Cryptoki - Authentification Windows (possiblement plusieurs comptes) - Administration centralisé - Code PIN	159 $
Aladdin	eToken Pro USB	- Encryptage : RSA (jusqu'à 2048), DES, 3-DES, SHA-1	- Facilement integrable dans une PKI - Certifie ITSEC LE4 - Standards : ISO 7816, PKCS#11 v2.01, CAPI (Microsoft Crypto API), APDU (Siemens/Infineon), PC/SC, X.509 v3, SSL v3, IPSec/IKE	90 €
Xelios	Secure Bio Drive Key	- Encryptage : AES-256	- La clef a deux segments : un prive et un publique. Un lecteur d'emprunte digitale contrôle l'accès a la zone prive. - Console d'administration pour redimensionner les deux partitions. - FAR (taux de fausse acceptance) < 0.05 - FRR (taux de faux rejet) < 0.1 - Stocke jusqu'à 10 empruntes	107 $ (64M) 285 $ (1G)
CRYPTOCard	UB-1 USB Token	- Encryptage : DES, 3DES, AES 128, 192, 256		

Les cartes à puce

Depuis son invention par Roland Moreno en 1974, la carte à puce s'est largement développée et son usage s'est diversifié. Au départ il s'agissait d'un dispositif passif aux capacités limitées, mais des évolutions importantes ont été rendues possibles grâce aux progrès rapides de l'électronique. Ainsi les modèles les plus récents intègrent désormais un microprocesseur et jusqu'a plusieurs mégaoctets de mémoire vive pour les modèles haut de gamme. Grâce à ces nouveaux modèles, il est maintenant possible de régler une consultation médicale (carte Vitale), de prouver son identité dans des pays ayant adopte la carte d'identité électronique, comme par exemple la Belgique, ou encore de déverrouiller l'accès à son ordinateur, la plupart du temps dans un contexte professionnel.

Ces usages nécessitent donc un niveau de sécurité élevé, afin de rendre la falsification ou la contrefaçon les plus difficiles possible, sachant qu'aucun système n'est parfait. Une des protections réside dans le fait que le microprocesseur et la mémoire sont contenus sur la même puce, et donc pour pouvoir accéder a la mémoire il faut obligatoirement passer par l'interface du microprocesseur.

Pour pouvoir s'authentifier, la carte est le plus souvent protégée par un code PIN.

Les standards utilisés ne sont malheureusement pas disponibles librement, mais pour interagir avec la carte il existe les PKCS(Public key Encryption System) développé par les laboratoires RSA, notamment le 11 qui définit une API fournissant des fonctions cryptographiques permettant de communiquer avec la carte indépendamment de la technologie, et le 15 qui définit le format des métadonnées présentes dans la mémoire de la carte afin d'assurer l'interopérabilité et la portabilité entre les différents matériels.

Le déploiement nécessite dans tous les cas des lecteurs adaptés. Dans le cas des cartes bancaires, les frais seront a la charge des commerçants souhaitant s'équiper, de même que les médecins pour la carte Vitale.

Les inclassables

Au gré de nos pérégrinations sur le web, nous sommes tombés sur un fournisseur proposant des périphériques d'authentification atypique. En effet, ces jetons servent de capteurs biométriques, permettant ainsi une identification de l'individu relativement efficace.

L'authentification par biométrie peut s'effectuer par le biais de l'analyse de différentes parties de l'anatomie humaine, allant de l'empreint digitale au tracer de la paume, de l'analyse morphologique du visage au tracé des réseaux veineux de la rétine.

Jusqu'à très récemment, ces procédés nécessitaient la mise en place d'infrastructures lourdes et l'achat de matériel onéreux. Mais quelques fournisseurs se lancent désormais dans ce domaine.

Constructeur	Nom du produit	Format	Plus...	Prix
Microsoft	Fingerprint Reader	lecteur filaire OU souris OU clavier	Intégré directement dans le matériel	39 €
Xelios	MorphoSmart MSO300 & MSO350	lecteur filaire	Lecteur de carte a puce intégré dans le MSO350	/
	MorphoSmart MSO1300x	lecteur filaire	Contrôle d'intégrité via signature numérique ou Chiffrements des transferts	/
	BioSIMKey G4	lecteur filaire portable	stockage des données sur carte SIM	/
	TouchChip G4	lecteur filaire	aucun	/

Ces lecteurs doivent être utilisés en complément de la solution logicielle appropriée l'une d'elle est *CryptoGram Secure Login* qui permet l'utilisation de toute sortes de jetons et de capteurs biométriques pour s'identifier et authentifier.

Microsoft

Le login Windows simplifié par Microsoft

Xelios

MSO300 & 350

MSO1330x

BioSIMKey G4

TouchChip G4

Conclusion

Nous avons vu qu'il existe de nombreuse solutions différentes pour améliorer la sécurité dans une entreprise grâce à l'authentification forte. Au milieu de tant de possibilité, l'aspect financier se révèle souvent décisif.

Les mêmes entreprises se retrouvant dans la plupart des constructeurs, se référer à leur expertise et faire jouer la concurrence entre eux pourrait être une bonne approche pour mettre en place la solution la plus pertinente.