

Enjeux et défis de la sécurité des systèmes d'information

Franck Leprévost

Université du Luxembourg
Laboratoire d'Algorithmique, Cryptologie et Sécurité
<http://lacs.uni.lu>

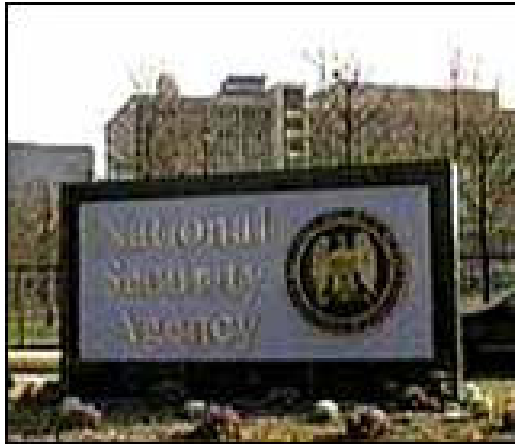


22 mars 2007

Outlines

- 1 Surveillance électronique
- 2 CAIN
- 3 Cryptologie
- 4 Infrastructures à clef publique : PKI
- 5 Quelques perspectives
- 6 Pour en savoir plus

Surveillance électronique



Source : <http://www.echelon-online.fr.st>

Surveillance électronique : un peu d'histoire

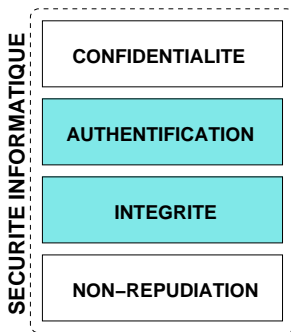
- BRUSA puis UKUSA
- COCOM puis Wassenaar Arrangement
- Les rapports du Parlement Européen

La base de Menwith Hill



Source : <http://www.echelon-online.fr.st>

CAIN



Cryptologie

- Cryptologie = Cryptographie + Cryptanalyse
- Cryptographie = Construire des
 - Cryptosystèmes à clef secrète
 - Cryptosystèmes à clef publique
- Cryptanalyse = Trouver les failles, les attaques
- Alice, Bob et Oscar

Cryptologie à clef secrète :



- Le principe de base : une unique clef pour chiffrer et déchiffrer
- Deux catégories :
 - Stream ciphers
 - Block ciphers

Cryptologie à clef secrète

- Chiffrement affine linéaire
- Chiffrement de Vigenère (XVI ème siècle), de Hill (1929), à permutation
- One-Time Pad (Gilbert Vernam 1917, preuve de sécurité Shannon 1949)
- DES : Data Encryption Standard (FIPS 46-3 du NIST)
- AES : Advanced Encryption Standard (FIPS 197 du NIST)
- FSE 2007 (26-28 mars 2007, LACS, UL)

Les limites de la cryptologie symétrique

- Problème de la création des clefs
- Problème du stockage des clefs
- Problème de l'échange des clefs
- Problème de la gestion des clefs dans un réseau
- Problème de l'authentification : signatures électroniques

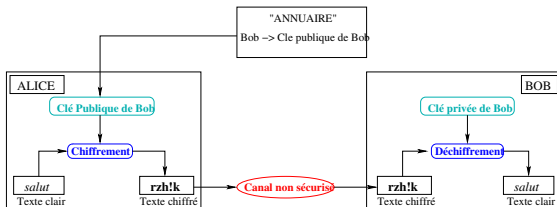
Les cryptosystèmes à clef publique

- Le principe de base : deux clefs :
 - l'une publique (pour chiffrer et vérifier les signatures)
 - l'autre secrète (pour déchiffrer et signer)
- Fonctionnalités : chiffrement, signature électronique, échange de clefs
- Sécurité basée sur des problèmes mathématiques
- Un long processus de standardisation : IEEE P1363, P1363A, ANSI X9.42, X9.62, X9.63

Chiffrement

- Alice et Bob disposent chacun d'une paire de clefs (x_A, y_A) et (x_B, y_B)
- Bob peut crypter, avec la clef publique y_A de Alice, un message à son intention
- Seule Alice peut, avec sa clef secrète x_A , décrypter le message envoyé par Bob

Chiffrement



- Eq. fondamentale : ici : $K_e \neq K_d$,
 - K_e publique (connue de tous)
 - K_d secrète (connue de Bob)
- **Analogie : Boite aux lettres**
 - toute personne peut envoyer du courrier à Bob ;
 - seul Bob peut lire le courrier déposé dans sa boîte.

Signature électronique

- Bob peut signer un message à l'aide de x_B
- La signature dépend du message à signer
- Chacun (y compris un juge) peut vérifier la validité de la signature

Signature électronique

But des signatures manuscrites :

- prouver l'identité de leur auteur **et/ou**
- l'accord du signataire avec le contenu du document

La signature électronique dépend du signataire **et** du document !

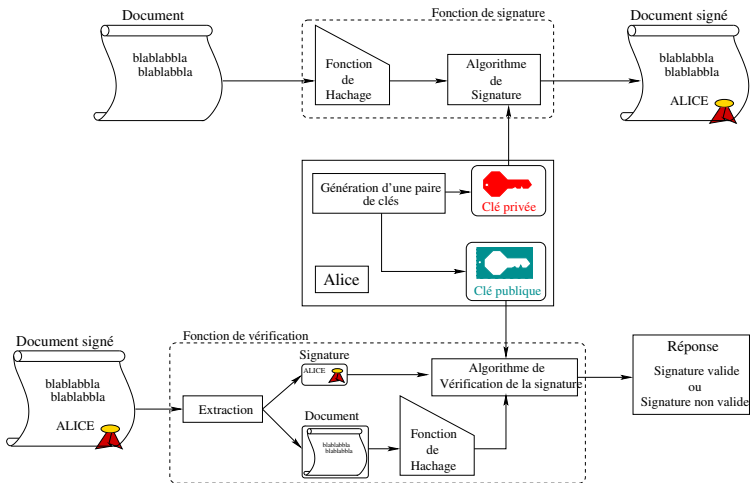
Objectifs d'une signature électronique

- Une signature est authentique.
- Une signature ne peut être falsifiée (imitée).
- Une signature n'est pas réutilisable sur un autre document.
- Un document signé est inaltérable.
- Une signature ne peut pas être reniée.

Signature électronique

- Protocole de signature électronique sûr : Impossible de falsifier la signature $s(M)$ d'un document M
 - sans connaître la clef secrète K (resp. K_d)
 - même en disposant de signatures d'autres documents.
 - Attention : impossibilité *pratique*
- Il existe d'autres conditions nécessaires de sécurité ! Elles relèvent davantage des architectures de sécurité des cryptosystèmes à clef publiques (PKI) ou du secret entourant la clé secrète.

Signature électronique



Authentification (d'un utilisateur)

- Les mots de passe
- Les mots de passe jetables
- Les challenges questions-réponses
 - A l'aide de la cryptographie à clef secrète
 - A l'aide de la cryptographie à clef publique
 - A l'aide de procédures sans diffusion de secret (Zero-Knowledge)

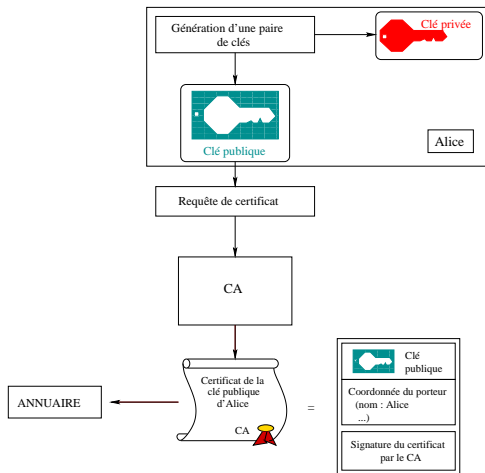
Échange de clefs

- Principe : une clef de session (pour un protocole à clef secrète) est transmise chiffrée (avec un protocole à clef publique)
- Motivation : un cryptosystème à clef publique est en pratique 100 à 1000 fois plus lent qu'un cryptosystème à clef secrète
- Utilisation combinée de cryptosystèmes à clef publique et à clef secrète

Infrastructures à clef publique : PKI

- Permettent de résoudre ces problèmes
- S'appuient sur la cryptologie à clef publique
- PKI et DRM
- Les architectures :
 - Les certificats X.509 (utilisés par SSL et TLS)
 - PGP
 - PKIX
 - D'autres encore

Infrastructures à clef publique : PKI



Quelques perspectives

Quelques constats

- La sécurité du know-how des entreprises européennes est un facteur de prospérité et de stabilité sociale.
- Il y a des solutions ...

Quelques défis technologiques

- De nouveaux standards
- Sécurité des infrastructures distribuées
- Anonymat
- Protection de la sphère privée dans le domaine de la vidéo-surveillance numérique

Quelques ouvrages



Enjeux
de la sécurité
multimédia

Jean-Louis
François
Bernard



Ebrahimi T., Leprévost F., Warusfel B. Ed, *Cryptographie et Sécurité des Systèmes et Réseaux*,
Hermès Lavoisier, 2006.



Cryptographie et sécurité
des systèmes et réseaux

Jean-Louis
François
Bernard



Ebrahimi T., Leprévost F., Warusfel B. Ed, *Enjeux de la Sécurité Multimédia*,
Hermès Lavoisier, 2006.