La signature électronique et les réseaux de confiance

Marc.Schaefer@he-arc.ch

HE-Arc Ingénierie

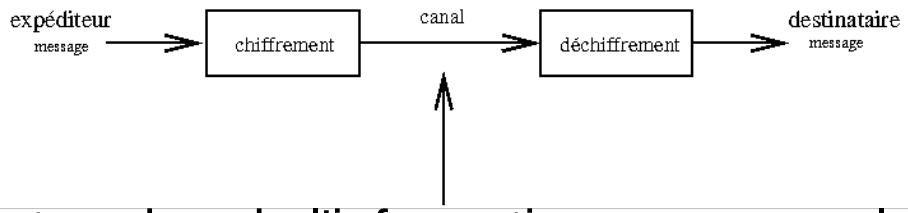
Institut des systèmes d'information et de communication (ISIC)
Laboratoire de téléinformatique (TINF)

Plan

- la cryptographie en bref et sur Internet, avec un exemple mathématique
- les principes de la signature électronique et des réseaux de confiance, avec mise en pratique (jeu)
- les risques et dangers
- le projet SuisseID

La cryptographie

- cacher l'information: la stéganographie
- la rendre incompréhensible : le **chiffrement**
- les bases mathématiques sont connues, les algorithmes aussi, les implémentations aussi : avantage pour la **confiance**
- le secret réside dans le paramètre de l'algorithme : la **clé** (ou une des clés)



- on peut cacher de l'information, par exemple :
  - dans une image (de l'information, ou une étiquette p.ex. avec le watermarking utilisé dans la propriété intellectuelle)
  - dans un texte (la fameuse lettre de George Sand à Alfred de Musset)

- le chiffrement consiste à modifier l'information de manière à la rendre inintelligible, par exemple :
  - code de César (permutations dans l'alphabet)
  - fonction OU exclusif avec une clé
  - propriété du modulo des nombres entiers (RSA)
  - propriété du logarithme discret (El Gamal)
  - algorithme mélangeur par blocs, puis chiffrement
  - compression initiale pour supprimer la structure des données (redondance)

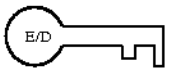
- la confiance dans une technologie de chiffrement provient du **contrôle par les pairs**, rendu possible par l'ouverture des implémentations

Types de cryptosystèmes

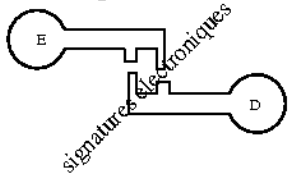
- systèmes à clé secrète ou dits **symétriques**
  - une clé unique (un mot de passe) connue des participants
  - on chiffre et on déchiffre avec cette clé

- systèmes à clé publique ou dits **asymétriques**
  - un couple de clé (clé publique, clé privée) par participant
  - on chiffre avec la clé publique du destinataire (connue, publiée, évt. **Certifiée**)
  - le destinataire déchiffre avec sa clé privée
  - permet la **signature électronique** !

chiffrement symétrique



asymétrique (PK)



- la sécurité de tout cryptosystème se juge surtout sur le **générateur aléatoire** ayant créé la clé, la sécurité des échanges de clés initiaux, et la résistance de l'algorithme de chiffrement à des attaques statistiques

- On combine souvent un cryptosystème asymétrique (pour ses propriétés intéressantes que l'on verra plus tard) avec un cryptosystème symétrique (pour son efficacité – par exemple pour les clés de session)

Cryptosystèmes symétriques

- algorithmes efficaces et sûrs même avec des tailles de clés faibles (p.ex. 128 bits)
  - AES, 3-DES, IDEA, ...
- une seule clé chiffre et déchiffre
- comment distribuer ces clés ?
  - avec N participants communiquant entre eux, il y en a :

$$N\frac{N-1}{2}$$

complexité

- s'il y a N participants qui veulent discuter en paires entre eux, il y a donc N * (N-1) liens ; en considérant que l'on peut utiliser la même clé secrète pour chacune des communications bidirectionnelles, on divise encore par 2
- évidemment, une complexité proportionnelle au **carré des participants** n'est pas intéressante !
- on n'a pas non plus réglé le problème de comment **distribuer** les clés de manière sûre.

Cryptosystèmes asymétriques

- couple de clé (publique, privée)
  - générées ensemble
  - dépendance mathématique entre elles
  - difficulté de passer d'une clé à l'autre
- principe : fonctions difficilement inversibles en temps « payable »
- on chiffre avec l'une, on déchiffre avec l'autre
  - exemple : Alice envoie un message à Bob en le chiffrant avec la clé publique de Bob

- par exemple : RSA (modulos entiers) ou El-Gamal (logarithmes entiers), codes elliptiques, etc.

- la clé publique de Bob devrait être idéalement publiée le plus largement possible

- Bob déchiffrera le message avec sa clé privée, qu'il ne communique à personne.

Exemple mathématique : RSA

- clé publique : (e, n)
- clé privée : (d, n) gardée secrète
- les autres valeurs sont jetées
- propriétés
  - difficile de trouver d sans connaître phi
  - difficile de factoriser n en p et q
  - chiffrement de m : $c = m^e \bmod n$
  - déchiffrement de c : $m = c^d \bmod n$

- on choisit 2 entiers premiers p et q
  - par exemple p=11, q=7
  - on peut calculer
    - n = p*q = 77
    - phi = (n-1)(q-1) = 60
  - on choisit e < n et n'étant pas facteur des facteurs premiers de phi
    - phi se décompose comme 2, 3, 5
    - p.ex. e = 17
  - d est à trouver tel que
    - e * d mod phi = 1
    - par exemple :
      - 17 * d mod phi = 1
      - D=53
- message m=42
  - chiffrement : 42^17 mod 77 = 70
  - déchiffrement : 70^53 mod 77 = 42
- en réalité, les nombres choisis sont très grands (p.ex. 2048 bits, soit de l'ordre de 600 chiffres)

La cryptographie sur Internet

- chiffrement des sites Web (HTTPS) – très courant
- chiffrement/signature électronique des e-mails – parfois
- connexion à des services par authentification à clés asymétriques – encore rare
- certificats X.509
- couche logicielle: SSL/TLS
- pour l'e-mail : souvent avec GPG/PGP

- les certificats sont une donnée informatique qui garantit le lien entre clé publique et identité du monde réel, en faisant usage de la **signature électronique**

L'attaque de l'intermédiaire

- Alice veut envoyer un message chiffré à Bob
- Charles veut pouvoir lire ce message
- Charles persuade Alice que la clé publique de Bob est en fait la sienne
- Alice utilise la clé publique de Charles (au lieu de celle de Bob) pour chiffrer
- Charles déchiffre avec sa clé privée, puis ré-enchiffre avec la clé publique réelle de Bob
- Bob reçoit le message, le déchiffre, sans se douter que Charles sait tout !
- que faire ?

- Cette attaque a pour nom « man in the middle » attack en anglais
- La seule façon de l'empêcher estde faire en sorte qu'Alice soit sûre que la clé publique qu'elle utilise pour chiffrer son message soit celle de Bob

- on utilise pour cela notamment la **signature électronique** et les **réseaux de confiance** *(prochaines pages!)*

- le problème de la diffusion des clés vue en cryptosystème symétrique n'en est plus un
  - les clés publiques sont largement **diffusées**
  - une infrastructure à clé publique (PKI) règle tous les problèmes
  - les réseaux de confiance assurent qu'une clé provient bien d'une **identité** donnée

La signature électronique

- buts
  - prouver qu'un message provient bien d'un expéditeur donné
  - basé sur la cryptographie asymétrique
- avez-vous une idée de comment faire pour que Bob puisse vérifier que c'est bien Alice qui lui a envoyé un message ?

- soit le message m envoyé par Alice à Bob
- soient les clés publiques P_A et P_B connues de tous
- soient les clés privées S_A et S_B connues respectivement uniquement d'Alice et uniquement de Bob
- si le but est d'assurer l'authenticité d'un message :
  - Alice envoie un hâchage de son message chiffré m avec .....
  - Bob vérifie que c'est bien Alice qui a envoyé le message en ...
- en pratique, on signe des hâchages (résumés cryptographiquement sûrs ou HMAC) plutôt que les messages complets : p.ex. avec SHA-256 – si on signait le message cela entrerait en conflit avec la confidentialité éventuelle de celui-ci
- on met un **estampillage** (horodatage) pour éviter des attaques de type « rejeu »

Le certificat

- garantit le lien entre une identité et une clé publique
- contient
  - une identité, par exemple :
    - *.alphanet.ch
    - Marc SCHAEFER, habitant à 2053 Cernier
  - la clé publique de cette identité
  - des critères de vérifications de cette identité
  - un estampillage (horodatage), une durée de validité, ...
  - une signature électronique de ce qui précéde, par la clé privée de l'autorité de certification (CA)
- un certificat valide fait partie d'une chaîne de confiance menant à un CA connu

- exemples d'autorités de certification
  - Verisign
  - CAcert
  - ...
- certaines se retrouvent dans votre navigateur !
- vous pouvez en installer manuellement (mais ...)
- votre navigateur réagit différemment lorsqu'il reçoit un certificat X.509 signé par une autorité connue ou non ainsi qu'en fonction des caractéristiques de vérification.

- un certificat de CA qui ne figure pas dans votre navigateur mais qui est signé avec une propriété de CA par un CA reconnu est considéré valide (chaîne de confiance)

Partie pratique

- vous avez reçu (mauvais !) une carte avec une clé publique et sa clé privée correspondante
- la 1ère étape est d'essayer de chiffrer un message pour votre voisin, qu'il déchiffrera
- la 2e étape est de faire imprimer un certificat par une autorité de certification
- la 3e étape est de vous connecter sur un système grâce à votre clé privée, un « challenge » et à votre certificat (obtenu sous 2)

Les problèmes des cryptotechniques

- on ne comprend pas toujours ce qu'on fait
- on ne signe pas toujours le message que l'on croit
  - en particulier si la clé privée est stockée sur un ordinateur ou un terminal sans affichage
- les générateurs aléatoires ne sont pas toujours bons
- les logiciels ont des bugs
- les clés doivent être assez longues
- les algorithmes ont des problèmes
- les bases mathématiques peuvent avoir des faiblesses

Les problèmes des cryptosystèmes dans l'ordre de leur importance décroissante :

- **formation**
- interfaces et **confinement**
- **maintenance** des logiciels
- générateurs aléatoires
- problèmes à la conception des logiciels
- augmentation de la puissance de calcul
- problèmes de la théorie mathématique impliquée

Le « plus » sûr :

- la clé privée est stockée sur une carte à puce et n'est jamais copiée sur l'ordinateur et est de préférence stockée protégée par un PIN
- le terminal qui effectue le chiffrement vous explique sur une interface séparée de l'ordinateur ce que vous faites et dispose d'une touche OK et d'une touche NON
- le terminal communique avec l'ordinateur par une interface « simple » (port série émulé p.ex.)
- le terminal est mis à jour de manière sûre

La confiance

- la société est basée sur la confiance
  - confiance en la monnaie papier alors qu'il n'y a plus de garantie or depuis longtemps
- la confiance est souvent basée sur des critères subjectifs
  - p.ex. si une compagnie aérienne a un accident d'avion, faut-il l'éviter (faut-il avoir plus ou moins confiance dans sa gestion des prochains vols?)
- utiliser des logiciels de cryptographie ou sa carte bancaire c'est faire confiance tout d'abord à des logiciels qui **agissent** en votre nom !

La confiance appliquée aux logiciels

- en général, plus de bugs sont trouvés, moins on a confiance
- **on a tort** : dans un logiciel, c'est surtout le fait de ne pas (pouvoir?) trouver de bugs qui est un problème !
- tout logiciel a des bugs, l'important est de les trouver, de les corriger, et de diffuser les corrections rapidement !

Réseau de confiance

- la chaîne qui mène d'un certificat présenté par un site Web vers une validation par un certificat reconnu par (stocké dans le) navigateur est une **chaîne de confiance (tout ou rien) –** système hiérarchique
- d'autres systèmes sont basés sur la notion de **réseau de confiance** (p.ex. PGP/PGP)
  - le nombre de certificats qui vous font confiance donne une estimation de la confiance qu'ont vos partenaires en vous (échelle) – système communautaire
- rôle des l**istes de révocations**

- le problème des chaînes de confiance est qu'il suffit qu'une autorité de certification soit compromise pour que le système s'effondre (sauf listes de révocations)
- le réseau de confiance est un système basé sur la reconnaissance des partenaires (communautaire)

- les deux technologies peuvent bénéficier de listes de révocations
  - liste en temps réel, accessible sur Internet, des révocations de certificats compromis
  - attaque de disponibilité (DoS) ?

SuisseID

- initiative de la confédération et de partenaires privés, compatible avec la loi fédérale
- but : délivrer des clés et certificats officiels pour l'usage généralisé de la cryptographie en suisse
- en pratique
  - commander par Internet (p.ex. La Poste) (79.- min.)
  - valider auprès d'une commune ou d'un office postal (25.-)
  - installer ce que La Poste livre
- les clés sont générés par le matériel et devraient donc être sûres
- la sécurité de l'utilisation dépend du traitement (p.ex. qui signe, où la clé privée est stockée, etc)

- une initiative précédente (en 1998) avait raté
  - UBS et les chambres de commerce
  - SwissKey SA a fait faillite

Références

Merci de votre attention !

Documents et informations

- http://ateliers.wiki.alphanet.ch/TecDays2012