Sécurité et réseaux

MIAGe

Ahmed Mehaoua
Professeur

UFR de Mathématiques et Informatique
Université de Paris – René Descartes

Plan

- Introduction: Définitions et motivations
- Typologie des menaces et attaques
- Principes de cryptographie
- Typologie des solutions de sécurité des réseaux
- Protocoles de sécurisation des échanges

Introduction

Pourquoi la sécurité des réseaux ?

- Le développement rapide des technologies de l'information a entraîné une dépendance croissante des organismes envers leurs système d'information (= composante vitale de l'organisation).
- Par ailleurs, le système d'information est aujourd'hui utilisé dans des applications variées

Conséquence :

les moyens de communication doivent être sûrs et fiables (disponibilité, intégrité, confidentialité, etc)

Vulnérabilité des systèmes

- Raisons de la vulnérabilités des systèmes :
  - ✓ La multiplication des serveurs
  - ✓ La désinformation et l'obsolescence
  - ✓ L'accès Internet et les applications extranet
  - ✓ PC utilisant des Dialup-IP contournant la sécurité
  - ✓ L'encapsulation des protocoles
  - ✓ La diffusion de codes mobiles incontrôlables
  - ✓ Utilisation de formats propriétaires mal conçus
  - ✓ Microsoft Word/Excel/... transmission accrue de virus
  - ✓ Systèmes d'exploitation et applications inadaptées à la sécurité (Microsoft)
  - ✓ Modems dangereusement configurés...

Sureté vs Sécurité

- La protection des systèmes informatiques couvre deux domaines:
  - la sureté ou Safety: les méthodes et les moyens mis en oeuvre pour éviter les défaillances “naturelles” :
  - la sécurité ou Security: les méthodes et les moyens mis en oeuvre pour se protéger contre les défaillances résultant d’une action intentionnelle :

Sureté de fonctionnement

- Systèmes à tolérance de pannes par:
  - Renforcement de la fiabilité matérielle
    - Sélection des composants (politique d'achat)
    - Redondance matérielle : doublement des éléments principaux
  - Redondance logicielle :
    - Systèmes RAID (Redundant Array of Independent Disk)
    - Six Niveaux (RAID0,……,RAID5)
    - Deux techniques utilisées pour la redondance des données :
      - Mirroring
      - Duplexing

Les différents niveaux de sécurité

- Sécurité physique
  - Relative à la protection des locaux et des machines
- Sécurité du personnel
  - Relative à la protection physique des employés et à la protection du S.I. de l'entreprise contre ces employés
- Sécurité des communications
  - Relative à la protection du système de communication (réseau)
- Sécurité des opérations
  - Relative à la protection des échanges de données et des systèmes informatiques

La politique de sécurité

- Nécessité de définir une politique de sécurité
  - Ensemble de règles formalisées auxquelles les personnes ayant accès aux ressources technologiques et aux S.I. d'une organisation doivent se soumettre (RFC 2196 Site Security Handbook)
  - Deux philosophies pour la mise en place d'une politique :
    - Prohibitive : tout ce qui n'est pas explicitement autorisé est interdit. EX. institutions financières ou militaires
    - Permissive : tout ce qui n'est pas explicitement interdit est autorisé. Ex. éducation familiale
- Composantes d'une politique de sécurité
  - Politique d'achat
  - Politique de confidentialité
  - Politique d'accès
  - Politique de responsabilité
  - Politique d'authentification
  - Politique d'audit et de reporting

Les services de la sécurité

- Authentification
- Identification
- Intégrité
- Non-répudiation
- Confidentialité
- Non-rejeu

Authentification

- L'authentification est la procédure qui consiste, pour un système informatique, à vérifier l'identité d'une entité afin d'autoriser l'accès de cette entité à des ressources (systèmes, réseaux, applications...).
  - L'authentification permet donc de valider l'authenticité de l'entité en question.
  - Elle protège de l'usurpation d'identité
- Les entités à authentifier peuvent être :
  - une personne
  - un programme qui s'exécute (processus)
  - une machine dans un réseau (serveur ou routeur)

Authentification

- Dans le cas d'un utilisateur, l'authentification consiste, en général, à vérifier que celui-ci possède une preuve de son identité ou de son statut, sous l'une des formes (éventuellement combinées) suivantes :
  - Ce qu'il sait (mot de passe, code PIN).
  - Ce qu'il possède (carte à puce, certificat électronique).
  - Ce qu'il est (caractéristique physique, voir biométrie).
  - Ce qu'il sait faire (geste, signature).
- La phase de vérification fait intervenir un protocole d'authentification. ex. :
  - SSL (Secure Socket Layer) pour le commerce électronique (qui peut également fournir un service de confidentialité par chiffrement)
  - Kerberos, standard utilisé par Windows et Linux pour se connecter sur une machine

Authentification

- une authentification simple est une procédure d'authentification qui requiert un seul élément ou « facteur » d'authentification valide pour permettre l'accès à une ressource.
  - Ex. login/password sur Linux
- une authentification forte est une procédure d'authentification qui requiert au moins deux éléments ou « facteurs » d'authentification valides pour permettre l'accès à une ressource
  - Ex. carte bancaire (1. être en possession de la carte; 2. connaître le PIN)
- Une authentification mutuelle impose une double authentification entre les deux entités
  - GSM vs UMTS

Identification

- L'authentification peut inclure une phase d'identification, au cours de laquelle l'entité indique son identité. Cependant, cela n'est pas obligatoire ; il est en effet possible d'avoir des entités munies de droits d'accès mais restant anonymes.

- L'identification permet donc de *connaitre* l'identité d'une entité alors que l'authentification permet de *vérifier* cette identité

Intégrité et Non-répudiation

- Un mécanisme de non-répudation permet d'empêcher à une personne de nier le fait qu'elle a effectué une opération (exemple : envoi d'un message, passage d'une commande).
  - Pour assurer la non-répudiation d'un message, on peut, par exemple, utiliser la signature électronique
- L'intégrité des données consiste à vérifier qu'elles n'ont pas été altérées accidentellement ou frauduleusement au cours de leur transmission ou de leur stockage.
  - Ce principe regroupe un ensemble de fonctionnalités mises en oeuvre afin de s'assurer de leur intégrité, comme les fonctions de hachage telles que MAC (Message Authentification Code)..

Confidentialité

- La confidentialité est la propriété qui assure qu'une information ne peut être lue que par des entités habilitées (selon des contraintes précises)
  - le chiffrement (parfois appelé à tort cryptage) est le procédé grâce auquel on peut rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement.
  - On distingue deux familles de systèmes de chiffrement :
    - Chiffrement symétrique ou à clé privé
    - Chiffrement asymétrique ou à clé publique (en réalité utilisant une paire de clés)

Une synthèse

- Bien que le *chiffrement* puisse rendre secret/confidentiel le sens d'un document, d'autres techniques cryptographiques sont nécessaires pour communiquer de façon sûre.
- Pour vérifier l'intégrité ou l'authenticité d'un document, on utilise respectivement un *Message Authentification Code* (MAC) ou une *signature numérique*.
- On peut aussi prendre en considération *l'analyse de trafic* dont la communication peut faire l'objet, puisque les motifs provenant de la présence de communications peuvent faire l'objet d'une reconnaissance de motifs. Pour rendre secrète la présence de communications, on utilise la stéganographie.
- L'utilisation d'un *compteur* associé aux messages échangés permet de s'affranchir du problème du re-jeux

Typologie des attaques

Typologie des attaques

- Les attaques sur les systèmes
  - Le vol des mots de passe
  - L'accès aux fichiers et répertoires sans autorisation
- Les attaques sur l'information
  - L'écoute de données communiquées sur le réseau
  - La modification des données communiquées sur le réseau
- Les attaques sur les applications
  - Attaquer les applications réseaux (émail, DNS, Web, FTP, …)
- Les attaques sur les protocoles de communications
  - Exploiter les failles des protocoles et de leur implémentations (IP, ICMP, TCP, …)

Origines des attaques

- ⇨ Attaques dues à des faiblesses des protocoles réseau
  - ✓ Identification des systèmes réseau (balyages, scanning)
  - ✓ Reniflement des paquets (sniffing)
  - ✓ Déni de service (DoS)
  - ✓ Déni de service distribué (DDoS)
- ⇨ Attaques dues à des faiblesses d'authentification
  - ✓ Attaque ARP spoofing
  - ✓ Attaque IP spoofing
  - ✓ Attaque man-in-the-middle
  - ✓ Crackage de mots de passe
- ⇨ Attaques dues à des faiblesses d'implémentation ou bogues
  - ✓ Attaque TCP SYN
  - ✓ Attaque sur les bogues des piles TCP/IP
  - ✓ Attaques sur les bogues des systèmes d'exploitation
- ⇨ Attaque par virus, chevaux de Troie

Attaque : Ping of Death

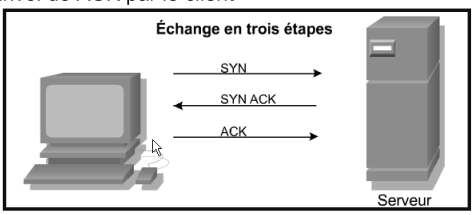
- Description :
  - Ping est basé sur ICMP echo/reply
  - ICMP est encapsulé dans IP
  - Taille maximum d'un paquet IP est de 65536 octets
  - Si taille supérieure, alors fragmentation à la source
  - Attaque consiste à génerer des paquets ICMP de taille 65510 (+8 octets pour header ICMP + 20 octets header IP)
  - Fragmentation à la source
- Effet :
  - le réassemblage provoque le crash du buffer de l'émetteur
- Action :
  - logiciel (patches)

Attaque : Teardrop

- Description :
  - Les valeurs de MTU (Maximum Transmission Unit) différentes implique la fragmentation des paquets IP
  - Initialisation des champs : Identification, flags et fragment offset
  - Attaque par altération du champ « fragment offset »
- Effet :
  - Crash de la machine
- Action :
  - logiciel (patches)

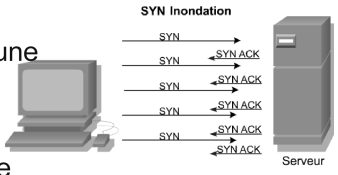
Attaque DoS: TCP SYN

- La technique d'inondation SYN s'appuie sur une demande de connexion qui n'aboutit pas, c-à-d ne termine pas les étapes nécessaires à l'établissement de cette connexion
- En effet, une négociation en 3 temps est nécessaire pour établir une connexion TCP
  1. Envoi de SYN par le client
  2. Envoi de SYN/ACK par le serveur
  3. Envoi de ACK par le client



Attaque DoS: TCP SYN (2)

- Le pirate initie une connexion mais n'envoie jamais d'ACK. Il en résulte une saturation de la pile TCP/IP de la machine cible



- Les pirates inondent l'hôte attaqué de fausses requêtes SYN, l'obligeant à utiliser ses ressources de connexion, ce qui l'empêche de répondre aux requêtes de connexion légitimes.
- **Comment se protéger contre ces attaques ??**

  l'administrateur système peut diminuer le délai d'attente de connexion et augmenter la taille de la file d'attente de connexion.

  Il existe également des logiciels capables de détecter ce type d'attaque et de mettre en place des mesures de protection.

Attaque: Email bombing/spamming

- Description :
  - Bombing : envoi d'un message répété à une même adresse
  - Spamming: variante du bombing, le message est envoyé à des milliers d'adresses émails
  - Falsification de l'adresse d'origine
- Effet :
  - Saturation des ressources systèmes et des ressources réseaux
  - Congestion du réseau
  - Crash du serveur de messagerie
  - Indisponibilité du serveur
- Action :
  - supervision
  - Filtrage,
  - proxy

Attaque: Smurf

- Description :
  - Envoi de ping (ICMP echo) vers une adresse de diffusion avec l'adresse source, celle de la victime
  - Réponses (ICMP reply) arrivent en grand nombre vers la victime
- Effet :
  - Saturation des ressources systèmes et des ressources réseaux
  - Congestion du réseau
  - Indisponibilité du système client
- Action :
  - Filtrage au niveau des routeurs
  - Patch logiciel de l'OS pour ne pas répondre à des adresses broadcast

Attaque: Spoofing

- Description :
  - Détournement et interceptions (eavesdropping) des comm.
  - Écoute indiscrète du trafic sur le réseau (sniffing)
  - Se faire passer pour l'interlocuteur légitime aux niveaux :
    - Liaison des données (ARP spoofing)
    - Réseau (IP spoofing, TCP hijacking)
    - Application (email/DNS/web spoofing)
  - Attaque passive, les informations recueillis peuvent servir pour une attaque active future
- Effet :
  - Perte de confidentialité (mot de passe, …)
- Action :
  - Chiffrement
  - Architecture avancée de réseau (switch/routeur à la place de hub, LAN virtuel, …

Attaque: ARP Spoofing

- Description :
  - Répondre à une trame ARP « who is ? » par une trame ARP reply avec une adresse MAC qui ne correspond pas à l'adresse IP de la requête.
  - ARP est sans état, l'attaquant peu anticipé les requêtes ARP
  - Mise à jour erronée de la table ARP de la machine cible
- Effet :
  - Redirection du trafic
- Action :
  - VLAN, patch routeur

Attaque: mot de passe

- les agresseurs essayent de
  - ✓ récupérer les fichiers de mots de passe (dans certains systèmes Unix /etc/passwd)
  - ✓ observer le réseau
  - ✓ utiliser des dictionnaires de clefs communs
- **Comment se prémunir contre ce genre d'attaque ?**
  - ✓ ne pas stocker les mots de passe en clair dans lesystème, par contre fournir au système le moyen de distinguer un mot de passe correct d'un mot de passe incorrect
  - ✓ empêcher l'utilisation de mot de passe que l'on peut trouver dans un dictionnaire.
  - ✓ Malheureusement les mots de passe impossible à deviner sont impossibles à mémoriser !!

Attaque: mots de passe

- les agresseurs essayent de
  - ✓ récupérer les fichiers de mots de passe (dans certains systèmes Unix /etc/passwd)
  - ✓ observer le réseau
  - ✓ utiliser des dictionnaires de clefs communs
- **Comment se prémunir contre ce genre d'attaque ?**
  - ✓ ne pas stocker les mots de passe en clair dans lesystème, par contre fournir au système le moyen de distinguer un mot de passe correct d'un mot de passe incorrect
  - ✓ empêcher l'utilisation de mot de passe que l'on peut trouver dans un dictionnaire.
  - ✓ Malheureusement les mots de passe impossible à deviner sont impossibles à mémoriser !!

Attaque: mots de passe (2)

- Rien n'empêche d'utiliser des outils pour tester ses mots de passe (CRACK) et de générer des mots de passe robustes comme le font les crackers.
  - ⇨ Un bon mot de passe doit toutefois être facile à se souvenir mais difficile à cracker.
  - ⇨ Penser à insérer des chiffres et des signes de ponctuation dans le mot de passe.
  - ⇨ **Conseils pour bien choisir son mot de passe**
    - ✓ Longueur
    - ✓ Choix : éviter des mots de passe se trouvant dans un dictionnaire, éviter d'utiliser le même code pour le login et mot de passe

upt&tp1?

Collecte d'information: les services

- Une attaque est généralement précédée par une étape de collecte d'information sur le système ou entité cible :
  - Précaution : désactivation de certains services réseaux :
    - ✓ **systat** : processus en cours d'exécution (équivalent d'un ps)
    - ✓ **netstat** : sockets ouvertes sur le système
    - ✓ **finger** : utilisateurs ayant une session ouverte sur le système (équivalent de who).
    - ✓ "**telnet victime.net systat**" ou "**telnet victime.net netstat**" suffit pour récupérer des informations sur ce système.
    - ✓ "**finger @victime.net**" affichera la liste des utilisateurs (noms de login) connectés

Collecte d'information: les scanners

- Les pirates utilisant des scanners pour obtenir des informations sur les systèmes cibles
  - Exemples d'outils de tests de vulnérabilité par balayage de systèmes :
  - Le plus célèbre : SATAN (Security Administrator's Tool for Analysing Networks) et ses dérivés (SARA : www-arc.com/sara/)
  - Le plus récent et performant : NESSUS sous Linux (www.nessus.org)
  - WebTrends Security Analyzer (www.webtrends.com)
- Effet :
  - founit le nom et la nature ainsi que le niveau de risque et la manière de remédier au problème
- Action :
  - Rien n'empêche un administrateur de tester tous ses systèmes à l'aide de ces outils

Principe de Cryptographie

Cryptographie : Définitions

- chiffrement : transformation à l'aide d'une clé de chiffrement d'un message en clair en un message incompréhensible si on ne dispose pas d'une clé de déchiffrement (en anglais encryption) ;
- chiffre : anciennement code secret, par extension l'algorithme utilisé pour le chiffrement ;
- cryptogramme : message chiffré ;
- décrypter : retrouver le message clair correspondant à un message chiffré sans posséder la clé de déchiffrement (terme que ne possèdent pas les anglophones, qui eux « cassent » des codes secrets);
- cryptographie : étymologiquement « écriture secrète », devenue par extension l'étude de cet art (donc aujourd'hui la science visant à créer des cryptogrammes, c'est-à-dire à chiffrer) ;
- cryptanalyse : science analysant les cryptogrammes en vue de les décrypter ;
- cryptologie : science regroupant la cryptographie et la cryptanalyse.

Cryptographie : Synonymes

- Message en clair = message originale = plaintext
- chiffrer = crypter = cryptographier = encypher = encrypt
- déchiffrer = décrypter = decypher = decrypt
- chiffre = algorithme de chiffrement = cypher
- cryptogramme = message chiffré = cyphertext
- Clé = secret = key
- Cryptanalyse = codebreaking

Cryptographie: principes

- Assuré par un système de clé (algorithme) appliqué sur le message. Ce dernier est décryptable par une clé unique correspondant au cryptage.

  Deux grands principes de cryptage :

  - ✓ le cryptage symétrique basé sur l'utilisation d'une clé secrète partagée - cryptographie à clé secrète -
  - ✓ le cryptage asymétrique repose sur un codage à deux clés, une privée et l'autre publique - cryptographie à clé publique -

- La sécurité d'un système de chiffrement doit reposer sur le secret de la clé de chiffrement et non sur celui de l'algorithme. Le *principe de Kerkhoff* suppose en effet que l'ennemi (ou la personne qui veut connaître le message chiffré) connaît l'algorithme utilisé.

Cryptographie et services de sécurité

- Le but de la cryptographie traditionnelle est d'élaborer des méthodes permettant de transmettre des données de manière confidentielle par chiffrement;
- Le but de la cryptographie moderne est de traiter plus généralement des problèmes de sécurité des communications et de fournir un certain nombre de services de sécurité :
  - Confidentialité
  - Authentification de l'origine des données
  - Intégrité
  - Non-répudiation
  - Non-rejeux
  - etc …
  - Authenticité = Authentification + Intégrité
- Les moyens mis en œuvre pour offrir ces services sont appelés mécanismes de sécurité.

Mécanismes et outils

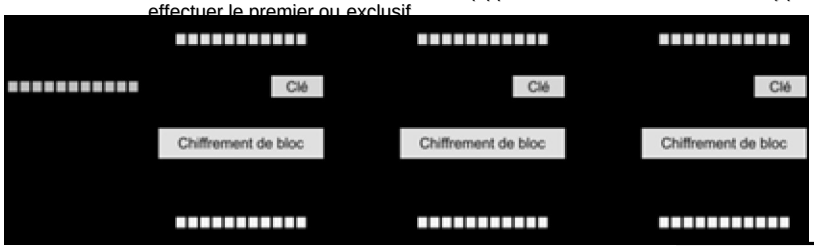
- Les mécanismes de sécurité sont basés sur un ensemble d'outils cryptographiques :
  - Fonctions de hachage
  - Algorithmes de chiffrement
  - Générateur aléatoire
  - Protocoles, …
- Ces outils peuvent être utilisés seuls ou combinés pour réaliser des opérations de :
  - Chiffrement
  - Scellement et signature
  - Échange de clés
  - Authentification mutuelle
  - ….

Algorithmes de chiffrement

- Les algorithmes de chiffrement peuvent être classés selon 2 critères:
  - Symétrique / Asymétrique (type de clés)
  - En continu / par bloc (format des données traitées)
- Les algorithmes de chiffrement en continu (stream cipher)
  - Agissent sur un bit à la fois
  - Rapides et robustes aux erreurs de communications
    - Le plus courant : RC4 (longueur de clé variable, 128 bits)
- Les algorithmes de chiffrement par blocs (block cipher)
  - Opérent sur le texte en claire par blocs (généralement de 64 bits)
  - 4 modes opératoires: ECB, CBC, CFB, OFB
  - Plus lents et requièrent plus de ressource
  - Plus robustes aux attaques
    - DES (clés de 56 bits codée sur 64)
    - 3DES (3 clés distinctes de 112 ou 168 bits)
    - IDEA (128 bits)
    - Blowfish (longueur de clé variable, 128 bits jusqu'à 448 bits)
    - AES (longueur de clé variable: 128, 192, 256 bits)

Mode opératoire: Cipher Block Chaining

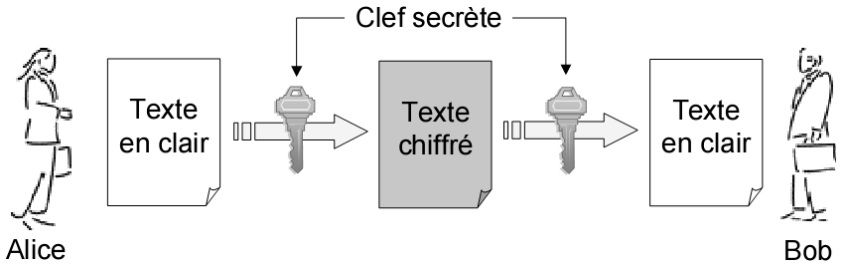
- Cipher Block Chaining: Le message est découpé en blocs de taille fixe.
- Chaque bloc est chiffré de manière corrélée avec le bloc précédent en utilisant l'opération XOR (⊕) entre le bloc de message i (M_i) et le résultat du chiffrement du bloc de Message M_{i-1}
  - à l'étape i,
    - Calcule: $M_i \oplus C_{i-1}$
    - Puis on chiffre le résultat: $C_{i-1} = E(M_i \oplus C_{i-1})$
    - Et on transmet C_i
  - pour l'étape 1 :
    - On introduit une valeur d'initialisation (appelé seed ou initialisation Vector) pour effectuer le premier ou exclusif



chiffrement symétrique

- Les algorithmes de chiffrement symétrique se fondent sur une clé unique pour chiffrer et déchiffrer un message.
- Basée sur 2 approches :
  - Substitution
  - Permutation
- Avantages :
  - Les algorithmes symétriques sont beaucoup plus rapides que les algorithmes asymétriques
  - Longueur réduite des clés (128 – 256 bits)
- Inconvénients :
  - la distribution de la clé doit être confidentielle (Problème dans Internet !).
  - Si un grand nombre de personnes désirent communiquer ensemble, le nombre de clés augmente de façon importante (une pour chaque couple de communicants).
  - pour *n* partenaires, il faut *(n*(n-1))/2* clés
  - Service de non répudiation non assuré
- Exemples :
  - DES (Data Encryption Standard), 3DES, AES, RC4, RC5, Kerberos, Blowfish, IDEA

Chiffrement symétrique (2)



Chiffrement symétrique (3)

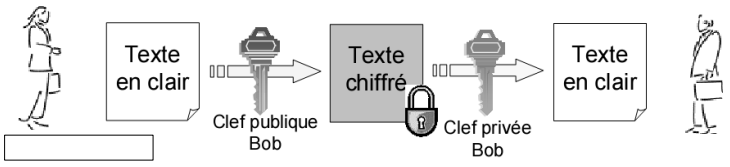
- Cependant toute utilisation de clé de chiffrement symétrique nécessite que les deux correspondants se partagent cette clé, c'est-à-dire la connaissent avant l'échange. Ceci peut être un problème si la communication de cette clé s'effectue par l'intermédiaire d'un medium non sécurisé, « en clair ».
- Afin de pallier cet inconvénient, on :
  - utilise un mécanisme d'échange de clés privées (Diffie-Hellman) basée sur un mécanisme de chiffrement asymétrique pour la seule phase d'échange de la clé privée de session, et l'on utilise cette dernière pour tout le reste de l'échange (RSA).

Chiffrement asymétrique

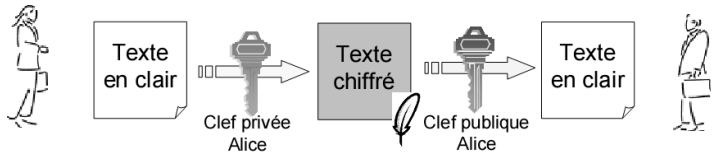
- Un algorithme de chiffrement asymétrique est une fonction cryptographique de codage à clé secrète dont la clé de chiffrement est différente de la clé de déchiffrement (cette dernière pouvant être difficilement calculée à partir de la clé de chiffrement).
  - On a une paire de clé (privé et publique) appelé aussi bi-clé
- La clé publique servant au chiffrement des messages peut être distribuée. Seul le détenteur de la clé de déchiffrement (clé privée) peut alors déchiffrer un message chiffré avec la clé publique correspondante.
  - *Confidentialité des échanges*
- Cependant les algorithmes asymétriques sont plus lents que les algorithmes symétriques et sont donc utilisés en général pour chiffrer des données de taille réduite telles que des signatures numériques ou d'autres clés (les clés de session).
  - *Authentification*
  - *Intégrité*
  - *Partage d'un secret à travers un canal non sécurisé (Internet)*
- Exemples d'algorithmes de chiffrement asymétrique très utilisés:
  - RSA (Riverst-Shamir-Adleman)
  - DSA (Digital Signature Algorithm)
  - ElGamal,

Chiffrement asymétrique (2)

- Confidentialité (Chiffrement)



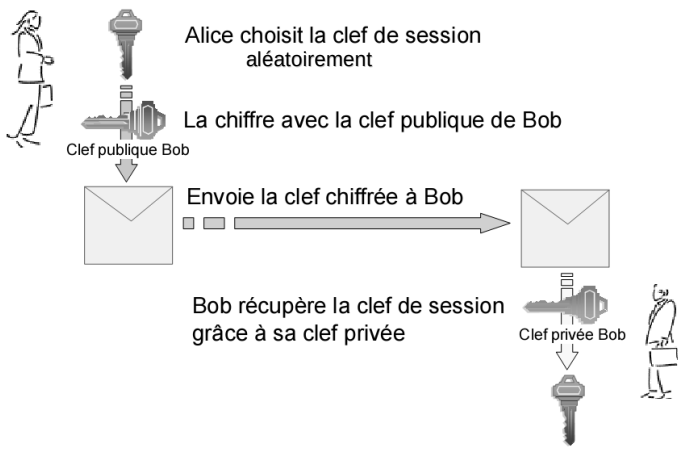
- Authentification (Signature)



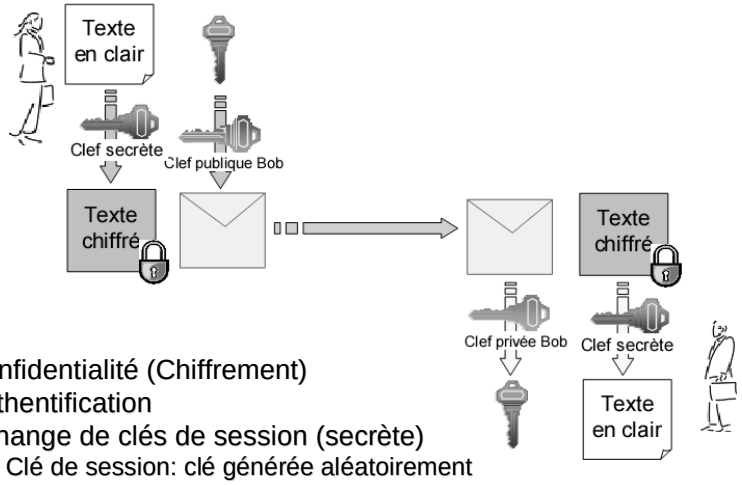
Protocole d'échange de clés

- Tout comme les protocoles de communication, les protocoles cryptographiques sont une série d'étape prédéfinies, basées sur un langage commun (spécifications des structures de données et de messages valides), qui permet à deux entités d'accomplir des taches d'authentification mutuelle et d'échange de clés.
- Il existe 2 types de protocoles d'échange de clés:
  - Les protocoles qui supposent la connaissance de la clé publique d'une des 2 entités (ex. RSA utilisé par SSL)
  - Les protocoles qui supposent aucune connaissance préalable d'informations entre les 2 entités (ex. Diffie-Hellman)

Protocole d'échange de clés: ex. DSA



Chiffrement hybride

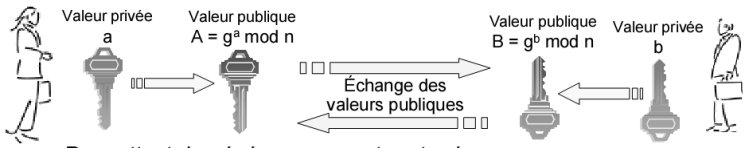


- Confidentialité (Chiffrement)
- Authentification
- Echange de clés de session (secrète)
  - Clé de session: clé générée aléatoirement
  - compromis entre le chiffrement symétrique et asymétrique.

Protocole d'échange de clés: ex. DH

- Qu'est ce que Diffie-Hellman (DH) ?
  - Inventé en 1976. Protocole cryptographique qui permet à deux entités de générer un secret partagé sans informations préalables l'un sur l'autre.
- Principe : basée sur la difficulté de calculer des logarithmes discrets sur un corps fini.
  - Le secret généré peut ensuite être utilisé pour dériver une ou plusieurs clés (clé de session, clé de chiffrement de clés, …)

◆ Échange de valeurs publiques



◆ Permettant de générer un secret partagé

Diffie Hellman

- Une fonction de hachage doit être :

Fonction de hachage

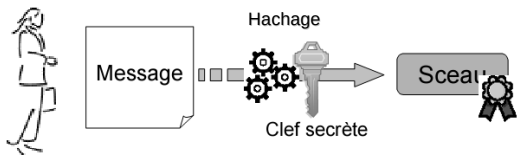
- Aussi appelée fonction de condensation
- Permet à partir d'un texte de longueur quelconque, de calculer une chaîne de taille inférieure et fixe appelé condensé ou empreinte (*message digest* ou *hash* en anglais)
- Utilisée seule, elle permet de vérifier *l'intégrité* d'un message.
- Associé à une clé privé, elle permet le calcul d'un sceau ou MAC (Message Authentification Code), pour assurer :
  - *Intégrité* des données
  - *Authentification* de la source
- Associé à un chiffrement asymétrique, elle permet le calcul de signatures, pour assurer :
  - *Intégrité* des données
  - *Authentification* de la source
  - *Non-répudiation* de la source
- Une fonction de hachage doit être :
  - à *sens unique*, c'est à dire qu'il doit être impossible étant donné une empreinte de retrouver le message original.
  - *sans collisions*, impossibilité de trouver deux messages distincts ayant la même valeur de condensé. La moindre modification du message entraîne la modification de l'empreinte.
- Exemples :
  - MD5 (Message Digest 5 - Rivest1991-RFC 1321) : calcul une empreinte de 128 bits
  - SHA-1 (Secure Hash Algorithm 1 - NIST1994) : plus sûr que MD5 - empreinte de 160 bits

Scellement

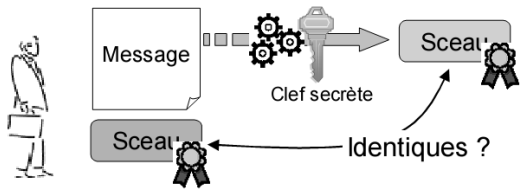
- Mécanisme qui consiste à calculer (ou sceller) une empreinte à partir d'un message et d'une clé privée pour:
  - Authentifier l'origine des données
  - Vérifier l'intégrité des données
- La scellement d'une empreinte génère:
  - un *sceau* ou *code d'authentification de message (MAC)*
- Il peut être réalisé de 2 manières possibles :
  - Fonction de hachage avec une clé privée:
    - Keyed-MAC (Keyed-MD-5, Keyed-SHA-1)
    - H(message, secret), H(secret, message), H(secret, message, secret)
  - Le dernier bloc du cryptogramme obtenu avec un algo. De chiffrement symétrique en mode CBC:
    - HMAC (HMAC-MD5, HMAC-SHA-1)
    - H(K+M)

Scellement (2)

- Scellement



- Vérification

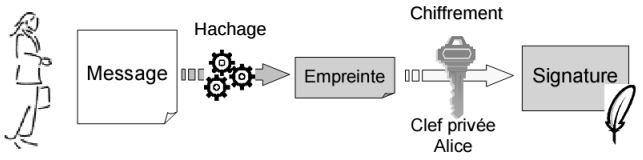


Signature numérique

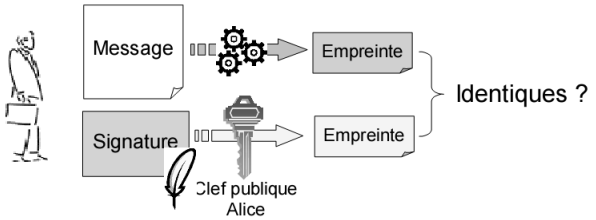
- La norme ISO 7498-2 définit la signature numérique comme des « données ajoutées à un message, ou transformation cryptographique d'un message, permettant à un destinataire de :
  - authentifier l'auteur d'un document électronique
  - garantir son intégrité
  - Protéger contre la contrefaçon (seule l'expéditeur doit être capable de générer la signature) -> non-répudiation.
- La signature électronique est basée sur l'utilisation conjointe d'une fonction de hachage et de la cryptographie asymétrique
- Depuis mars 2000, la signature numérique d'un document a en France la même valeur légale qu'une signature sur papier

Signature numérique (2)

- Signature



- Vérification



Certificat électronique

- Les certificats électroniques sont des données publiques.
  - Ex. lors de l'accès à un serveur web sécurisé, le client télécharge automatiquement le certificat.
- A chaque certificat électronique correspond une clef privée, qui est soigneusement protégée par le propriétaire du certificat, et une clé publique qui est incluse dans le certificat et qui doit être signée par une tierce organisation (l'autorité de certification).
  - Ainsi, sur Internet, le certificat permet à un client de vérifier que la clé publique et l'URL d'un site marchand appartiennent bien à leur auteur (Ex. www.laposte.fr, www.fnac.fr, ...).

Certificat électronique (2)

- C'est une carte d'identité électronique dont l'objet est principalement d'authentifier un utilisateur ou un équipement informatique (comme une passerelle d'accès ou un serveur d'application sécurisé, Ex. web marchand).
- Le certificat numérique est un bloc de données contenant, dans un format spécifié, les parties suivantes :
  - la clé publique d'une paire de clés asymétriques,
  - des informations identifiant le porteur de cette paire de clés (qui peut être une personne ou un équipement), telles que son nom, son adresse IP, son adresse de messagerie électronique, son URL, son titre, son numéro de téléphone, etc...
  - l'identité de l'entité ou de la personne qui a délivré ce certificat (autorité de certification), Ex. Verisign,
  - et enfin la signature numérique des données ci-dessus par la personne ou l'entité prenant en charge la création ou l'authentification de ce certificat et servant d'autorité de certification.

Certificat électronique (3)

- Usuellement, on distingue deux familles de certificats numériques :
  - les certificats de signature, utilisés pour signer des e-mails ou s'authentifier sur un site web, et
  - les certificat de chiffrement : les gens qui vous envoient des e-mails utilisent la partie publique de votre certificat pour chiffrer le contenu que vous serez seul à pouvoir déchiffrer
- Il existe deux façons distinctes de créer des certificats électroniques :
  - le mode décentralisé (le plus courant) qui consiste à faire créer, par l'utilisateur (ou, plus exactement par son logiciel ou carte à puce) le biclef cryptographique et de remettre la partie publique à l'AC qui va y adjoindre les informations de l'utilisateur et signer l'ensemble (information + clé publique)
  - le mode centralisé qui consiste en la création du biclef par l'AC, qui génère le certificat et le remet avec la clé privée à son utilisateur.

Certificat électronique (4)

- Les certificats électroniques respectent des standards spécifiant leur contenu de façon rigoureuse. On trouve parmi les plus connus et les plus utilisés :
  - la norme X.509 en version 1, 2, et 3, sur lequel se fondent certaines infrastructures à clés publiques.
  - OpenPGP, format standard (normalisé dans le RFC 2440) de logiciels comme GnuPG.
- Un Certificat électronique est géré tout au long de son cycle de vie (création, renouvellemnt et révocation) par l'autorité de Certification (CA) au moyen d'une infrastructure à clés publiques, ou PKI pour Public Key Infrastructure en anglais.

Autorité de certification

- Une Autorité de Certification appelée aussi AC ou CA (Certificate Authority) est chargée d'émettre et de gérer des certificats numériques.
- Elle est responsable de l'ensemble du processus de certification et de la validité des certificats émis.
- Une Autorité de Certification doit définir une Politique de certification qui va établir l'ensemble des règles de vérification, de stockage et de confidentialité des données appartenant à un certificat ainsi que la sécurité de stockage de sa propre clef privée nécessaire à la signature des certificats.
- Ex. Verisign, EnTrust.net, CyberTrust, CertPlus, …

Public Key Infrastructure

- Une PKI (Public Key Infrastructure), aussi communément appelée IGC (Infrastructure de Gestion de Clefs) ou ICP (Infrastructure à Clefs Publiques), est un ensemble de composants physiques (des ordinateurs, des équipements cryptographiques, des cartes à puces), de procédures humaines (vérifications, validation) et de logiciels (système et application) en vue de gérer le cycle de vie des certificats numériques ou certificats électroniques.
- Une PKI permet la délivrance des certificats numériques. Ces certificats permettent d'effectuer des opérations cryptographiques, comme le chiffrement et la signature numérique.

Public Key Infrastructure (2)

- Une infrastructure à clés publiques délivre un ensemble de services pour le compte de ses utilisateurs :
  - Enregistrement des utilisateurs (ou équipement informatique),
  - Génération de certificats,
  - Renouvellement de certificats,
  - Révocation de certificats,
  - Publication des certificats,
  - Publication des listes des certificats révoqués,
  - Identification et authentification des utilisateurs (administrateurs ou utilisateurs qui accèdent à l'IGC),
  - Archivage ou séquestre des certificats (option).

Typologie des solutions

Technologies de sécurité des communications

Communication layers	Security protocols
Application layer	ssh, S/MIME, PGP
Transport layer	SSL, TLS, WTLS
Network layer	IPsec
Data Link layer	PPTP, L2TP
Physical layer	Scrambling, Hopping, Quantum Communications

MPLS

Sécurisation des échanges

- Pour sécuriser les échanges ayant lieu sur le réseau Internet, il existe plusieurs approches :
  - niveau applicatif (PGP)
  - niveau transport (SSL/TLS)
  - niveau réseau (protocole IPsec)
  - niveau physique (boîtiers chiffrant).
- Application typique : sécurisation du Web