Sécurité Informatique

Yves Deswarte
deswarte@laas.fr

LAAS-CNRS
Toulouse (France)
(*en séjour sabbatique à Microsoft Research, Cambridge, UK*)

Sommaire

- Définitions - principes - propriétés de sécurité
- Attaques
  - Qui sont les intrus ?
  - Classification des attaques
- Défenses
  - Politiques de sécurité
  - Cryptographie
  - Authentification
  - Protection
  - autres

Sécurité-Confidentialité

- Sécurité-confidentialité =

  Confidentialité
  « non-occurrence de divulgations non autorisées de l 'information »

  + Intégrité
    « non-occurrence d 'altérations inappropriées de l 'information »

  + Disponibilité
    « être prêt à l 'utilisation »

Confidentialité

1) Empêcher les utilisateurs de lire une information confidentielle (sauf s 'ils y sont autorisés)

2) Empêcher les utilisateurs autorisés à lire une information confidentielle de la divulguer à des utilisateurs non autorisés à la lire

Intégrité

1) Empêcher une modification (*création, mise à jour ou destruction*) indue de l 'information (ou du système) :
   - Modification par des utilisateurs non-autorisés
   - Modification incorrecte par des utilisateurs autorisés (ou faute accidentelle)

2) Faire en sorte qu 'aucun utilisateur (ou faute accidentelle) ne puisse empêcher la modification légitime de l 'information (ou du système)

Disponibilité

1) Fournir l 'accès à l 'information pour que les utilisateurs autorisés puissent la lire ou la modifier

2) Faire en sorte qu 'aucun utilisateur (ou faute accidentelle) ne puisse empêcher l es utilisateurs autorisés d 'accéder à l 'information

Autres propriétés de sécurité (1)

- Intimité (privacy) : respect des libertés individuelles, protection de la vie privée : *confidentialité*
- Authenticité / non-répudiation : *intégrité* de l'information + *intégrité* de l'origine (+ de la réception)
- Responsabilité (accountability) : pouvoir prouver quel utilisateur a réalisé une opération : *intégrité*
- Pérennité : *disponibilité* de l'information (à long terme, plutôt qu'accessibilité immédiate)

Autres propriétés de sécurité (2)

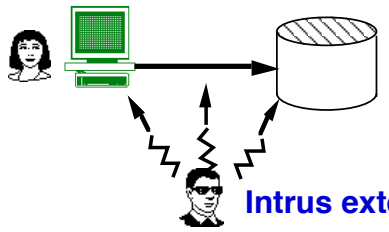
- Exclusivité : ne fournir l'accès qu'aux utilisateurs autorisés : *intégrité, confidentialité* du service
- Protection de la propriété intellectuelle (ex. contre la copie illicite de logiciels, d'œuvres musicales, …) :

  confidentialité (ne pas permettre les accès en lecture, seulement les accès en exécution)

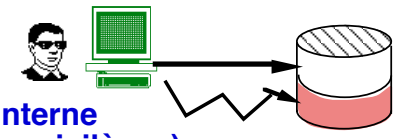
  \+ *intégrité* (empêcher la création de la copie)

Qui sont les intrus ?

1)

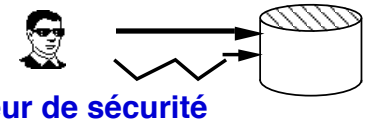


2)



Intrus interne
(extension de privilèges)

3)



Administrateur de sécurité
(abus de pouvoir)

Classification des attaques (1)

- Écoute passive : lire les informations entrées, affichées, transmises, stockées ou traitées (*confidentialité*)
  - Exemple : sniffers
  - Écrans, claviers, imprimantes, lignes de communications, UC, …
    - -> *matériel TEMPEST*
- Interception : modifier des informations transmises (*intégrité*) :
  - Destruction de messages (*éblouissement*)
  - Modification de messages
  - Insertion de messages (*rejeu*)

Classification des attaques (2)

- Répudiation : refuser de reconnaître une opération qu 'on a effectuée (*intégrité*)
  - L 'émetteur d 'un message refuse de reconnaître qu 'il l 'a émis
  - Le récepteur d 'un message refuse de reconnaître qu 'il l 'a reçu
- Cryptanalyse : obtenir des informations secrètes à partir des informations publiques (*confidentialité*)
  - Message en clair
  - Clés
  - Algorithme de chiffrement

Classification des attaques (3)

- Déduction par inférence, furetage : recouper des informations auxquelles on a légitimement accès pour obtenir des informations confidentielles (*confidentialité*)

  Exemple : dossiers médicaux
- Déguisement (masquerade) : se faire passer pour un autre utilisateur (*intégrité*)

  Tromper les mécanismes d 'authentification

Classification des attaques (4)

- Porte dérobée (trap-door) : mécanisme de contournement des contrôles d 'accès (installé délibérément ou faille)
- Utilisation de canaux cachés (covert channels) : transmettre des informations confidentielles à un utilisateur non autorisé (*confidentialité*...)
  -> contournement des contrôles d'accès
  - Canaux de mémoire directs (réutilisation de buffers, fichiers temporaires, secteurs disques, ...) ou indirects
  - Canaux temporels : modulation de l'utilisation de ressources communes (UC, disques, réseaux, périphériques, ...)

Classification des attaques (5)

- Bombe logique : fonction dévastatrice déclenchée à retardement ou par des conditions particulières (ex. présence de certains utilisateurs, logiciels, matériels) ou après un certain nombre d 'activations
  - Destruction d'informations stockées (ex. formatage de disque) : données, programmes, infos de sécurité
  - Diffusion de fausses information de diagnostic
  - Dégâts matériels : usure anormale de périphériques mécaniques (disquettes, disques durs, imprimantes, ...), destruction d'écrans, flash-BIOS, ...

Classification des attaques (6)

- Cheval de Troie : programme exécutant une fonction illicite tout en ayant l'apparence d'exécuter une fonction légitime
  - Confidentialité : divulgation d'informations confidentielles
  - Intégrité et disponibilité : fausses informations, bombe logique

Classification des attaques (7)

- Virus : segment de programme qui, lorsqu'il s'exécute, se reproduit en s'attachant à un programme (système ou d 'application) qui devient ainsi un cheval de Troie)
  - Propagation d'une machine à une autre par échange de support de fichiers (disquettes), téléchargement, partage (réseau) ou attaché à un courrier
  - Éventuellement porteur d'une bombe logique
  - Tout programme peut être contaminé (sauf protection physique) :
    - Boot
    - OS
    - Application
    - Macros dans un document (Word, Excel, …)

Classification des attaques (8)

- Ver (worm) : programme autonome qui, lorsqu'il s'exécute, se reproduit pour s 'exécuter sur une autre machine
  - Éventuellement porteur d 'une bombe logique
  - Propagation par exécution à distance ou par mél

  Exemple : le ver d 'Internet (2 novembre 1988)

Classification des attaques (9)

- Bourrage de boîte aux lettres (spamming)
- Altération de pages web : directe ou par indirection
- Déni de service sur les protocoles réseaux (ex. : SYN) ou sur des services automatiques, ou par des utilisateurs non-privilégiés (ex. : crashme)
- ...

Classification des attaques (Fin)

- Fautes de conception délibérément nuisibles
  - Bombe logique, porte dérobée, cheval de Troie, virus, ver
- Fautes de conception sans volonté de nuire (accidentelles ou délibérées)
  - Porte dérobée, canaux cachés, insuffisance des protection
- Fautes d 'interaction délibérément nuisibles
  - Intrusions, virus, ver, implantation de cheval de Troie

Défenses (1) : Politiques de sécurité

- Politique de sécurité =
  Objectifs de sécurité (propriétés vérifiables)
  + Règles pour faire évoluer l 'état de sécurité
- Problème de la cohérence (safety problem) :
  La politique est «cohérente» si, partant d 'un état sûr (où les propriétés sont vérifiées), il n 'est pas possible d 'atteindre un état non sûr en appliquant les règles
- Modèle de sécurité = représentation formelle de la politique

Politiques de sécurité (suite)

- Politiques «discrétionnaires» : le gestionnaire d 'une information (généralement le propriétaire) décide librement des droits d 'accès à cette information

  - Généralement incohérentes (ne permettent pas de vérifier des propriétés de confidentialité ou d 'intégrité fortes)
    ex. : empêcher la divulgation par un utilisateur autorisé à lire

  - Plus de 99% des systèmes commerciaux

Politiques de sécurité (fin)

- Politiques «obligatoires» (mandatory) : en plus des contrôles discrétionnaires, il y a des règles incontournables

  Exemple : Bell-LaPadula :
  Tout élément a un niveau de sécurité (classification+compartiment)
  sujet (utilisateur, processus) : habilitation $h(s)$
  objet : niveau de classification $c(o)$
  Règle simple : s peut lire $o \Rightarrow h(s) \geq c(o)$
  Règle étoile : s peut lire o_1 et écrire $o_2 \Rightarrow c(o_1) \geq c(o_2)$

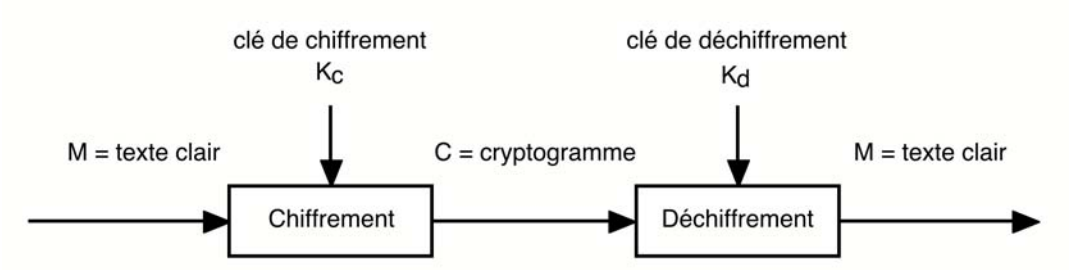
- Pour la confidentialité ou l 'intégrité

Défenses (2) : Cryptographie

- **Cryptographie** = concevoir des *chiffres* transformant des *clairs* en *cryptogrammes* (*chiffrement*) et réciproquement (*déchiffrement*) à l 'aide de *clés*
- **Cryptanalyse** = casser les chiffres
- **Cryptologie** = cryptographie + cryptanalyse

Chiffrement / déchiffrement

- Principe : confidentialité



Chiffrement : $M \rightarrow C = [M]_{Kc}$

Déhiffrement : $C \rightarrow M = [M]_{Kd}$

La confidentialité repose sur [algo] et sur Kd

Chiffres symétriques

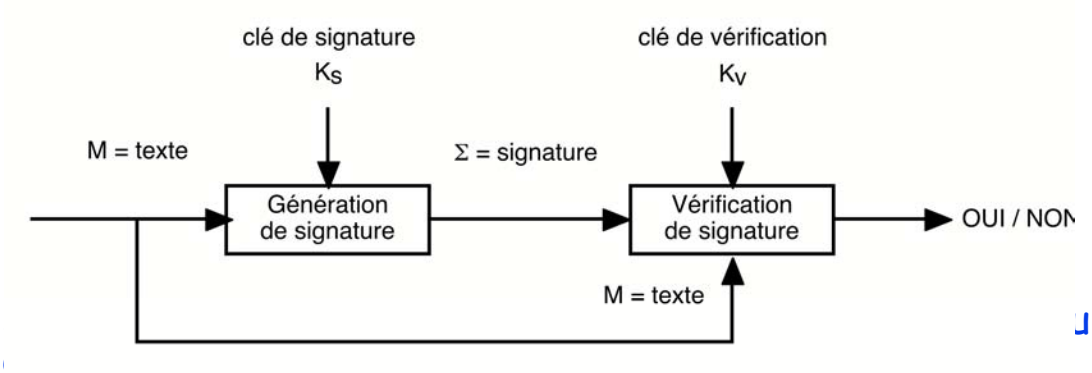
- Seuls chiffres connus jusqu 'en 1976
- Kc = Kd, [ ] = { }$^{-1}$
- Exemples : DES, IDEA, AES, …
- Rapides (Gbit/s), clés ~80 ou 128 bits
- Confiance mutuelle entre émetteur et récepteur (clé partagée)

Chiffres à clés publiques

- (officiellement) apparus qu 'en 1976 (Diffie-Helmann)
- Kc ≠ Kd : Kc est public, Kd secret : tout le monde peut chiffrer, seul celui qui connaît Kd peut déchiffrer
- Exemple : RSA (Rivest-Shamir-Adleman) : MIT 1978
  N est les produit de 2 grands nombres premiers (P et Q)
  Kc fixe (exemple : 65), N et Kc publics, Kd = 1/Kc mod ((P-1).(Q-1))
  (sans connaître P et Q, il est «impossible» de calculer Kc)
  $C = M^{Kc} \bmod(N)$ et $M = C^{Kd} \bmod(N) = M^{Kc.Kd} \bmod(N)$
- Lents (qqs Mbits/s), clés ~1024 ou 2048 bits, mais pas de confiance mutuelle entre émetteur et récepteur.

Signature

- Principe : intégrité



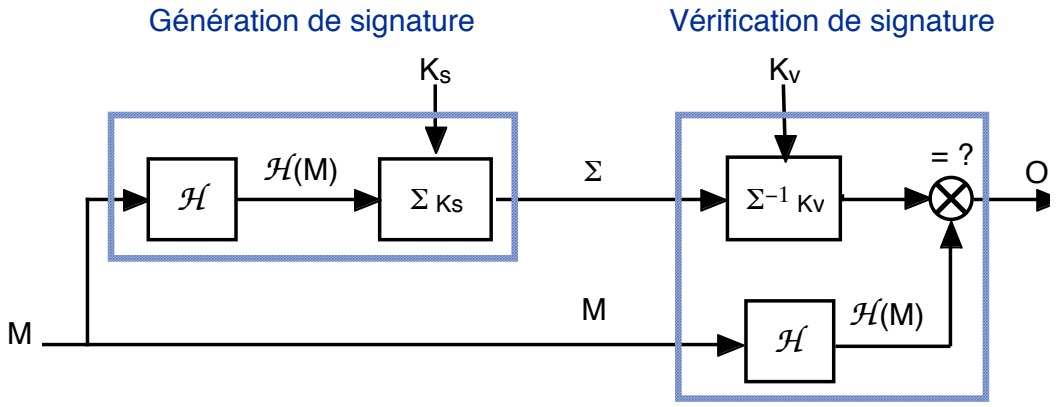
- ur

Si Ks ≠ Kv et Kv est public, seul celui qui connaît Ks peut avoir généré la signature.

Fonction de hachage (one-way hash function)

- Obtenir une «empreinte» $\mathcal{H}(M)$ de longueur fixe n pour un message M de longueur quelconque
  exemple : n = 128 bits
- Connaissant M, il est facile de calculer $\mathcal{H}(M)$, mais il doit être «impossible» de trouver $M' \neq M$ tel que $\mathcal{H}(M') = \mathcal{H}(M)$
- Application : accélérer les signatures à clés publiques, scellement de messages, de logiciels, …
- Exemples : MD5, SHA

Scellement



Exemple : RSA, El-Gamal, DSA

Génération de clé commune

Alice veut échanger une clé secrète avec Bob, sans qu 'Ève (à l 'écoute sur le réseau) ne puisse l 'obtenir

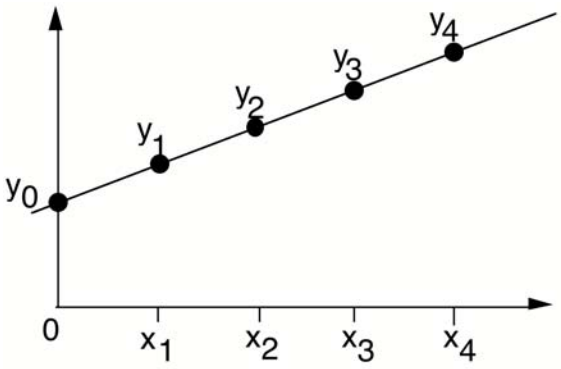
Exemple : Diffie-Helmann

- A génère un nombre aléatoire Ska, un grand nombre premier N et un générateur G de N. A calcule Pka = G^{Ska} mod N
  et envoie à B : (N,G, Pka)
- B génère un nombre aléatoire Skb, calcule Pkb = G^{Skb}mod N
  et l 'envoie à A
- A calcule Ks = $Pkb^{Ska.}$ mod N = $G^{Skb.Ska}$ mod N
  B calcule Ks = Pka^{Skb} mod N = $G^{Ska.Skb}$ mod N

Partage de secret

- Schéma à seuil : stocker K sous forme d 'images telles qu 'en réunissant au moins S images on puisse regénérer K mais qu 'avec S-1 images on n 'ai aucune information sur K

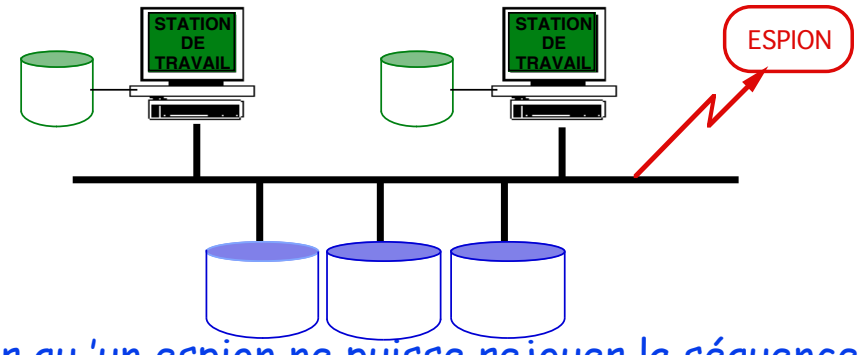
- Exemple : S=2
  y = ax + b



Défenses (3) : Authentification

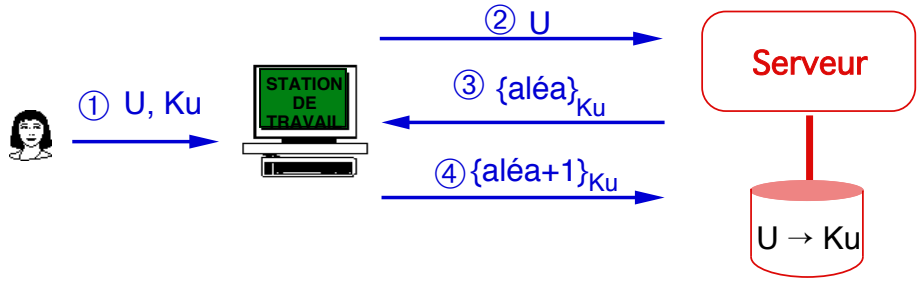
- Identification = présentation de l 'identité : information non secrète, différente pour chaque utilisateur (nom, numéro, …) connue au moins de l 'utilisateur et de la machine
- Vérification de l 'identité : l 'utilisateur présente qq chose :
  - Qu'il connaît : mot-de-passe, infos personnelles, …
  - Qu'il possède : badge, carte à puce, …
  - Qui lui est propre : empreinte digitale, iris, voix, signature manuelle
- Taux d 'acceptation à tort, taux de rejet à tort
- Vérification par secret partagé, secret caractéristique de l 'utilisateur, ou sans apport de connaissance

Authentification à distance



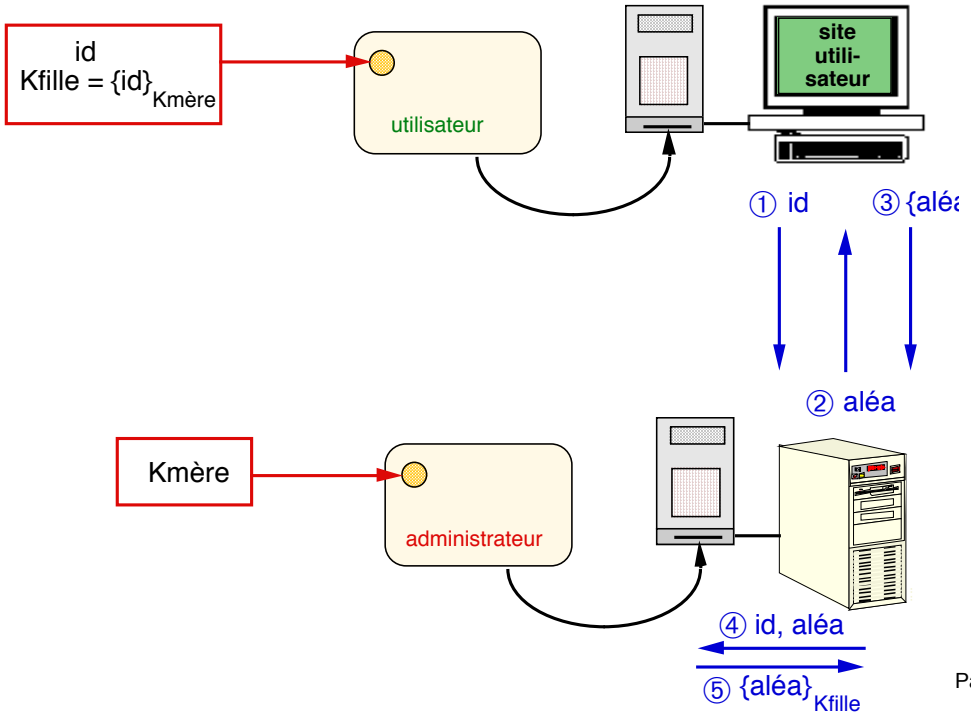
- Éviter qu 'un espion ne puisse rejouer la séquence
- Vérification locale : pages-jaunes
- Protocoles à défi-réponse : one-time password, S-Key, cartes à puces, ...

Exemple de défi-réponse : mot-de-passe



1. L 'utilisateur tape son nom (U) et son mot-de-passe (Ku)
2. la station transmet U au serveur
3. le serveur recherche localement Ku et chiffre un aléa
4. La station déchiffre avec le Ku local et répond au défi

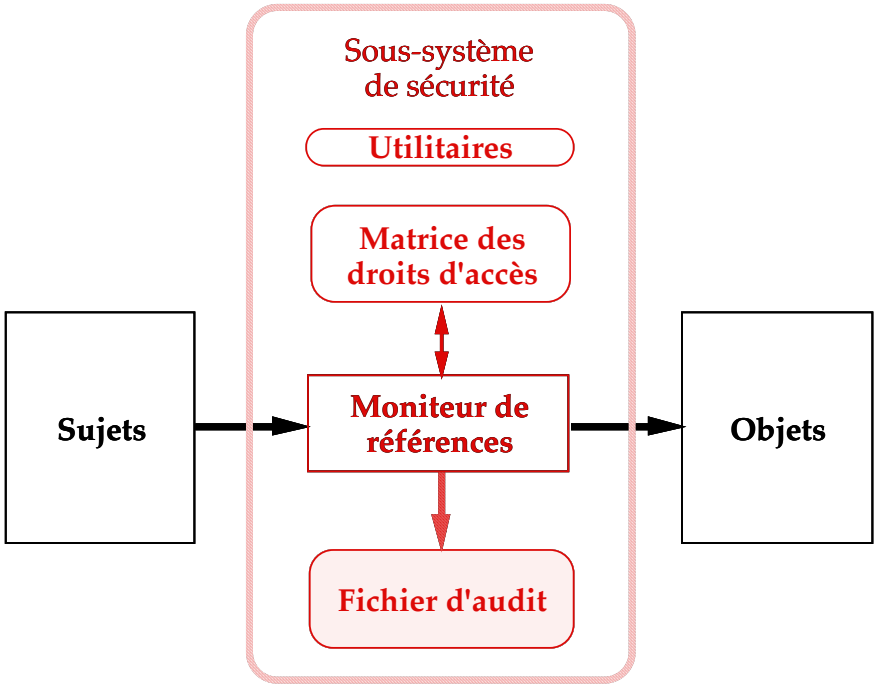
Exemple de défi-réponse : carte à puce



Défenses (4) : protection

- Un sujet a un *droit d'accès* sur un objet s'il est autorisé à exécuter la fonction d'accès correspondante sur l'objet
  - Sujet = processus s'exécutant pour le compte d'un utilisateur
  - Utilisateur = individu (ou service, ex. d'impression) enregistré et authentifié
  - Objet = n'importe quoi dont on peut vérifier les accès
- Vérification des droits par un moniteur de références *incontournable, infalsifiable, totalement vérifié*

Trusted Computing Base (TCB)



Autres défenses

- Cloisonnement : isoler tout ce qui peut l 'être, filtrer toutes les communications : firewall
- Journalisation (audit) : enregistrer toutes les opérations susceptibles de mettre en cause la sécurité
- Détection d 'intrusions
- Systèmes de secours
- Évaluation