Protection des Systèmes d'information

Quoi securisé?

- Securite physique
- Securite logique
- Securite de l'information
- Securite reseau

SECURITE physique

Control d'acces

La sécurité physique doit être renforcée Via

- Une architecture centralisée de contrôle d'accès par badge, surveillance vidéo
- Installation de contacts de porte et détecteurs de présence
- Installation de Barrières infra-rouge,
- Détection d'intrusion

SECURITE physique

- L'authentification est la **vérification de l'identité** d'une entité.
- A chaque utilisateur est associé un **compte**. Celui ci détermine les moyens qui doivent être utilisés pour authentifier cet utilisateur:
  - Limite apportée au droit de connexion (les machines sur lesquelles il peut se connecter,
  - Le nombre maximal de connexions simultanées,
  - Les heures qui lui sont autorisées ou interdites…),
  - Et les droits initiaux qui lui sont accordés lors d'une connexion.

SECURITE physique

L'authentification est la **vérification de l'identité** d'une entité.

- L'authentification devrait être assurée en continu(pas une fois pour toutes à l'ouverture d'un objet (en début de session)

  ☹ Personne :elle peut quitter son poste en le laissant ouvert

  ☺ procédure de déconnexion automatique, procédure d'authentification périodique.

L'authentification des personnes peut se faire par trois méthodes:

- ✓ Ce que connaît l'utilisateur (mot de passe),
- ✓ Ce que détient l'utilisateur (carte…),
- ✓ Ce qu'est l'utilisateur (méthode biométrique)

QUELQUES TECHNIQUES BIOMETRIQUES À L' ETUDE

- L'empreinte digitale

- La vascularisation de la rétine

- La voix

- La géométrie de la main

- Dynamique de la signature

- Dynamique de la frappe clavier

- Empreinte génétique

Sécurité logique

- Mise en place d'une gestion par parc pour les mises à jour (anti-virus, migrations logicielles, changement de version de systèmes d'exploitation…)

Sécurité logique

- Control d'acces
- Seule les personnes habilitées par un administrateur système ont accès au système informatique
- Moyens pour assurer la règle:
  - Système d 'authentification (Login +mot de passe) géré par l 'administrateur
  - Modification périodique des mots de passe par les utilisateurs
  - Protection informatique du contrôle d 'accès aux comptes
  - Audit des tentatives de fraude
  - ….

PROTECTION DE L'INFORMATION

CRYPTOGRAPHIE

Historique et introduction

La stéganographie : écriture couverte

L'information est dissimulée au sein d'une autre information afin de la rendre invisible.

Durant l'antiquité, certains généraux rasaient le crâne de leurs esclaves, leur tatouaient un message et attendaient que les cheveux repoussent pour faire passer des informations importantes.

Définitions

Message clair: Cette expression désigne le message original n'ayant subi aucune modification

Clé: La clé désigne l'information permettant de chiffrer et de déchiffrer un message

Chiffrement:
Processus de transformation d'un message M de telle manière à le rendre incompréhensible :

- Basé sur une fonction de chiffrement E
- On génère ainsi un message chiffré C = E(M)

Définitions

Déchiffrement:

Processus de reconstruction du message clair à partir du message chiffré :

Basé sur une fonction de déchiffrement D
On a donc D(C) = D(E(M)) = M

En pratique : E et D sont généralement paramétrées par des clefs Ke et Kd :
$E_{ke}(M) = C$
$D_{kd}(C)=M$

Définitions

- **La cryptographie** est la science qui utilise les mathématiques pour le cryptage et le décryptage de données.

- **La cryptanalyse** est l'étude des informations cryptées, afin d'en découvrir le secret. C'est donc l'ensemble des procédés *d'attaque* d'un système cryptographique.

- **La cryptologie** englobe la cryptographie et la cryptanalyse

Familles des codes

1. Les codes à répertoire
2. Les codes à clefs secrètes qui se subdivisent en deux familles

   – les codes de transposition ou de permutation. L'ordre des éléments d'une information est modifiée (caractères d'une phrase, pixels d'une image, ...)

   – les codes de substitution, les éléments d'une information sont remplacés par d'autres (remplacer tous les A par B, B par C, etc...)

I Codes à répertoire.

- Ils consistent en un dictionnaire qui permet de remplacer certains mots par des mots différents. Ils sont très anciens et ont été utilisés intensivement
- On peut par exemple créer le dictionnaire suivant:
  - rendez-vous ↔ 175
  - demain ↔ oiseaux
  - midi ↔ à vendre
  - Villetaneuse ↔ au marché
- La phrase en clair:
  - RENDEZ VOUS DEMAIN MIDI VILLETANEUSE
- Elle devient avec ce code
  - 175 OISEAUX A VENDRE AU MARCHE

I Codes à répertoire.

☹

- Ces codes manquent de souplesse ils ne permettent pas de coder des mots nouveaux sans un accord préalable entre l'expéditeur et le destinataire. Pour cela il faut qu'ils échangent des documents ce qui accroit le risque d'interception du code.

☺

- Par contre ils peuvent rendre des services appréciables pour un usage unique.

II Codes à cle secrete

– les codes de transposition ou de permutation.
– les codes de substitution,

II-1-Codes de permutation

- On partage le texte en blocs,
- On garde le même alphabet mais on change la place des lettres à l'intérieur d'un bloc (on les permute).
- L'expéditeur et le destinataire du message se mettent d'accord sur une grille de largeur fixée à l'avance.
- L'expéditeur écrit le message dans la grille en remplaçant les espaces entre les mots par le symbole □.

II-1-Codes de permutation

- Exemple : ici la grille est de 6 cases de large.

Le message

M=RENDEZ VOUS DEMAIN MIDI VILLETANEUSE

R	E	N	D	E	Z
□	V	O	U	S	□
D	E	M	A	I	N
□	M	I	D	I	□
V	I	L	L	E	T
A	N	E	U	S	E

- On lit le texte en colonne et obtient ainsi le message crypté:
  C=R□D□VAEVEMINNOMILEDUADLUESIIESZ □N □TEC

II-1-Codes de permutation

- ☼On peut augmenter la securite du code en rajoutant une clé secrète constituée par l'ordre de lecture des colonnes.
- Exemple :
  - ✓On choisit la clé: CAPTER
  - ✓On numérote les colonnes en fonction du rang des lettres du mot CAPTER dans l'alphabet

    2, 1, 4, 6, 3, 5
  - ✓et on lit les colonnes dans l'ordre indiqué.

  C=EVEMIN R□D□DA DUADLU Z□N□TE NOMILE ESIIES

II-1-Codes de permutation

- C=EVEMINR □D □VADUADLUZ □N □TENOMILEESIIES
- Pour décoder le message précédent on range en colonne sur la grille en suivant l'ordre des colonnes donné par le mot du code.

2	1	4	6	3	5
R	E	N	D	E	Z
□	V	O	U	S	□
D	E	M	A	I	N
□	M	I	D	I	□
V	I	L	L	E	T
A	N	E	U	S	E

II-2-Codes de substitution.

- Dans les codes de substitution par flots ou par blocs l'ordre des lettres est conservé mais on les remplace par des symboles d'un nouvel alphabet suivant un algorithme précis.
- Exemple Code de César:

II-2-Codes de substitution.
Code de César

- Consiste à décaler l'alphabet clair.
- Le décalage est la clé du chiffrement
- Pour coder on remplace chaque lettre par son rang dans l'alphabet.

A=1, B=2, C=3,....,M=13, N=14,...,S=20,...,X=24, Y=25, Z=26

- **Exemple** :
  - On veut chiffrer le mot *CRYPTOGRAPHIE* avec un décalage de 3. Pour cela on écrit les alphabets clair et chiffré comme suit :

    ABCDEFGHIJKLMNOPQRSTUVWXYZ

    DEFGHIJKLMNOPQRSTUVWXYZABC
  - *Et on remplace:*

    CRYPTOGRAPHIE ---> FUBSWRJUDSKLH

II-2-Codes de substitution. Code de César

- Lettre codée=lettre claire+n modulo 26
- Où n est un entier entre 0 et 25 appelé la clef du code.
- Le décodage se fait en utlisant la relation
- Lettre claire=lettre codée -n mod 26

II-2-Codes de substitution.
Chiffrement de César

☹

- Il n'y a que 26 clés possibles !
- Donc étant donnée un message chiffré, il suffit de tester les 26 clés possibles pour retrouver le message clair.
- Cela se fait en quelques minutes !!

☺ Solution au problème de clés :

Utiliser un alphabet chiffré aléatoirement

Cryptanalyse des codes de substitution.

- Décodage par analyse de fréquence, cette méthode a été mise au point au moyen âge par des lettrés arabes.

Cryptanalyse des codes de substitution.

Dans la langue française, par exemple, on sait que la fréquence d'apparition de chaque lettre est à peu près stable. Il suffit donc de:

- Mesurer la fréquence d'apparition de chaque lettre d'un texte chiffré
- Comparer avec la table des fréquences des lettres françaises
- Déduire l'alphabet chiffré

Cryptanalyse des codes de substitution.

Analyse de fréquence

Lettre	% français	Lettre	% français
A	9,4	N	7,2
B	1,0	O	5.1
C	2,6	P	2,9
D	3,4	Q	1,1
E	15,9	R	6,5
F	1	S	7,9
G	1	T	7,3
H	0,8	U	6,2
I	8,4	V	2,1
J	0,9	W	0
K	0	X	0,3
L	5,3	Y	0,2
M	3,2	Z	0,3

Cryptanalyse des codes de substitution.

«uftu ef gsfrvfodft» à déchiffrer

Cryptanalyse des codes de substitution.

Réponse «uftu ef gsfrvfodft»

`f -> e` (lettre la plus fréquente 5, donc e)

`u -> t` (lettre fréquente 2, donc t, r, n, o, i, a, s)

`t -> s` (lettre fréquente 2, donc r, n, o, i, a, s)

«test ee gserveodes»

`e -> d` «test des gserveodes»

on essaie avec n, r, o, i, a …

II-2-Codes de substitution. Le code de Vigénère

- La faiblesse des codes de César et des systèmes analogues est que la fréquence des lettres est conservée ce qui permet une cryptanalyse aisée par analyse de fréquences.
- Pour améliorer la sécurité on peut faire un code de César par blocs où on change de substitution pour chaque lettre d'un bloc.
- On obtient ainsi le code de Vigénère.

II-2-Codes de substitution. Le code de Vigénère

- On se fixe une longueur de bloc m.
- On découpe le message en blocs de m-lettres.
- On chiffre par blocs de m lettres. On décide par exemple que la première lettre d'un bloc de m est codée avec un code de César de clef n_1, la deuxième avec un code de César de clef n_2 et la m-ième par un code de César de clef n_m.

II-2-Codes de substitution. Le code de Vigénère

- Exemple
  - m = 5, n1 = 3, n2 = 14, n3 = 7, n4 = 22, n5 = 19,
  - Le message en clair est:

  M=Ce système de codage n'est pas sur, mais plus que le code de César si la clé est longue
  - on partage en blocs de taille 5 en partant de la gauche

  CESYS TEMED ECODA GENES TPASS URMAI SPLUS QUELE CODED ECESA RSILA CLEES TLONG UEXXX
  - Les XXX ont été ajoutés pour compléter le dernier bloc.
  - Dans chaque bloc on code la première lettre avec le code de César de clef $n_1 = 3$,..., la cinquième lettre du bloc avec le code de César de clef $n_5 = 19$.

- E(M)= FSZUL WSTAW HQVZT JSUAL WDHOL XFTWB VDSQLTILHX FCKAW HQLOT UGPHT FZLAL WZVJZ XSETQ

Cryptographie moderne

Cryptographie symétrique

- Ou cryptographie à clé privée

- On utilise la même clé pour chiffrer et déchiffrer un message (ke = kd = k).

- Les deux communicants doivent être en possession de cette clé.

- La norme de cryptage de données (**DES**) est un exemple de ce type de système largement utilisé par le gouvernement fédéral des Etats-Unis.
- Exemple : césar et vegenere

Cryptographie symétrique
Avantages et inconvenants

Avantage:

- Il est très rapide

Inconvénient:

- La distribution des clés reste le problème majeur du cryptage conventionnel surtout lorsque le nombre de communicants devient grand.

Autrement dit, comment faire parvenir la clé à son destinataire sans qu'aucune personne ne l'intercepte ? De là va apparaître la cryptographie asymetrique (à clé publique).

Cryptographie asymétrique

- Chaque entité possède une paire de clés :
Une clé publique, connue par toutes les autres entités et utilisée pour chiffrer un message donné,

Une clé privée qui ne doit être connue que par l'entité qui possède la paire en question, et qui est utilisée pour déchiffrer un message

- Un message chiffré avec une clé publique ne peut être déchiffré qu'avec la clé privée correspondante.

Cryptographie asymétrique

Principe:

- Bob laisse ses cadenas en libre accès à la poste
- Alice peut à tout moment venir à la poste prendre un cadenas et envoyer un message à Bob
- Bob peut facilement ouvrir son cadenas avec sa clé et récupérer le message.

Cryptographie asymétrique
RSA

-Le système RSA est nommé à partir des noms de ses inventeurs: Rivest, Shamir, Adleman

-Principe:

- On choisit deux grands nombres premiers p et q et calcule :

$$n = p.\ q \text{ et}$$

$$\varphi(n) = (p-1)(q-1).$$

$\varphi(n)$ est la fonction indicatrice d'Euler

Cryptographie asymétrique
RSA

- On choisit un entier **e** qui n'a pas de facteur commun avec φ(n) (premiers entre eux).
- e est superieur à 3
- e n'est pas necessairement premier mais Pgcd (e, φ(n))=1

- On calcule **d** tel que (e. d-1) est exactement divisible par φ(n).
- **On déduit :**

Clé publique = (n,e)

et

clé privée =(n,d)

Cryptographie asymétrique
RSA

- Grâce à sa clé public, on peut chiffrer un message avec la formule RSA. Mais on ne peut plus le déchiffrer, car RSA est impossible à inverser, à moins de connaître p et q.

chiffrement : $\mathbf{c = m^e \bmod n}$

Alice reçoit le message c et calcule :

déchiffrement : $\mathbf{m = c^d \bmod n = (m^e \bmod n)^d \bmod n}$

Cryptographie asymétrique
RSA

- **Exemple**:

p=5, q=7, m=12

e?

d?

c?

Exemple :

p=5, q=7, donc n=p.q=35

φ(n)=(p-1)(q-1)=24

on choisit e=5 tel que e est premier avec φ(n)

et on déduit d=29 tel que (d.e)mod φ(n)=1

Cryptographie asymétrique
RSA

- **Exemple**:

p=5, q=7, m=12

Cle publique (n, e)=(35,5)
Cle privee (n,d)= (35,29)
Pour le message m= 12
$c = m^e \bmod n$ =248832mod n
c= 17
Essayons de retrouver le message en clair m depuis le message chifree c
$m = c^d \bmod n = 12$

Signature numérique

- L'un des principaux avantages de la cryptographie à clé publique est qu'elle offre une méthode d'utilisation des signatures numériques.

- La signature est une chaîne de données qui associe un message (dans sa forme numérique) à l'entité dont il est originaire.

- Il devient difficile de déchiffrer un document chiffré quand on n'en est pas le destinataire légitime.

Signature

- La signature électronique doit être difficile à falsifier
- Il doit être difficile de se procurer les dispositifs qui peuvent fabriquer la signature, pour fabriquer par exemple un faux ;
- L'authenticité d'une signature doit en revanche être facile à vérifier;
- Sauf le destinataire légitime peut déchiffrer le code.
- Pour que la signature soit valide pour un chiffrement RSA elle doit vérifier cette condition

$$c = s^e \bmod n.$$

- Pour signer un message m :
- On calcule $s = m^d \bmod n$.

Sécurité des BDD

- Protéger la BDD contre l'accès, la modification ou la destruction non autorisé
- Protéger les informations sensibles
  - Comptes bancaires
  - Info personnelles des cartes de crédit
  - Notes et moyennes des étudiants

principales menaces de sécurité des bases de données

- Abus de privilège
- Injection SQL
- Déni de service
- Vulnérabilités des protocoles de communication des bases de données
- Copies non autorisées de données sensibles
- Exposition de données de sauvegarde

Abus de privilège

- Lorsque les utilisateurs (ou les applications) ont des privilèges d'accès à une base de données excédant les exigences de leur fonction professionnelle, ils peuvent abuser de ces privilèges à des fins malveillantes. Par exemple, un directeur d'université dont la fonction n'exige que la capacité à modifier les coordonnées des étudiants peut profiter de privilèges de mise à jour de bases de données excessifs pour modifier les notes.

- SOLUTION
  - Prévention des abus de privilège
  - Elimination des droits excessifs (les droits qui ne sont pas nécessaires à l'utilisateur pour remplir sa fonction)
  - Le contrôle d'accès des requêtes permet de restreindre les privilèges d'accès aux bases de données à un minimum requis d'opérations SQL (SELECTIONNER, METTRE A JOUR).

Droits d'accès et Privilèges

- À la création d'un objet (table, relation,….etc) son propriétaire a tous les droits, y compris celui d'accorder ou de révoquer des privilèges à d'autres utilisateurs.
- Un privilège est composé des éléments suivants
  - Utilisateur qui accorde le privilège
  - Utilisateur qui reçoit le privilège
  - Objet
  - Action permise
  - Transmission possible du privilège

Droits d'accès et Privilèges

- Exemple
  - si Alice est propriétaire de la relation R, elle peut accorder le privilège de la consulter (SELECT) à Bob
  - si elle indique que ce privilège est transmissible, Bob pourra à son tour accorder ce privilège à un autre utilisateur
  - si Alice révoque le privilège à Bob, alors Bob et tous ceux qui ont reçu ce privilège de Bob perdent l'accès à la relation R

Droits d’accès et Privilèges

- Les contrôles d'accès vérifient l'identité des usagers qui se présentent et en conséquence leur assignent des droits d'accès sur tel ou tel ensemble de données.

  Autorisation (GRANT en SQL)

  Tout usager qui a le droit de transmettre des privilèges sur un objet peut utiliser la commande GRANT pour transmettre ce privilège :

Droits d'accès et Privilèges

- Syntaxe

```
GRANT <privileges>|ALL
 ON <object>
 TO <users>
[WITH GRANT OPTION]
```

Valeur de **<users>** peut etre une liste de **noms d'utilisateurs** ou **PUBLIC**

<object> est le noms d'une table ou d'une vue

- Les privilèges peuvent être :

- lire (SELECT),
- insérer de nouveaux n-uplets (INSERT),
- modifier des valeurs (UPDATE),
- supprimer la totalité d'une relation (DROP),
- créer de nouvelles relations (CREATE).
- ALL : tous les privilèges que le donneur peut accorder

- L'option facultative WITH GRANT OPTION permet au donneur d'autoriser le receveur à transmettre à d'autres les privilèges qu'il reçoit.
- Un usager peut recevoir un privilège de plusieurs sources différentes.

Droits d'accès et Privilèges

- Exemple : attribution de privilèges sur des objets sql

```
GRANT ALL ON Employee
TO Manager
WITH GRANT OPTION
```

L'utilisateur 'Manager' peut effectuer n'importe qu'elle peration sur la table Employee et il peut accorder les memes privileges aux autres utilisateurs (**`WITH GRANT OPTION`**)

Droits d'accès et Privilèges

- Révocation (REVOKE en SQL)
  - Tout usager ayant donné un privilège peut à tout moment retirer ce privilège grâce à la commande REVOKE :

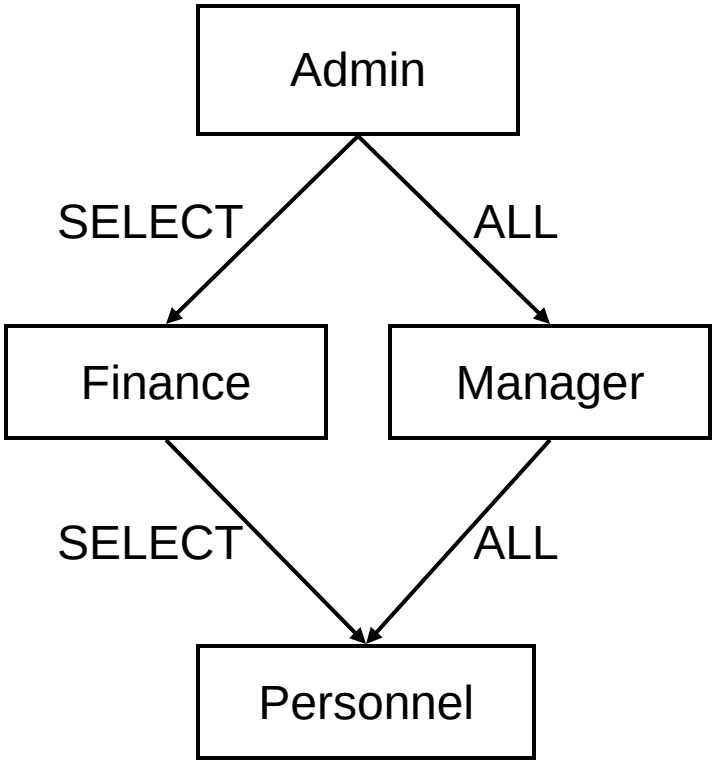
  syntaxe

```
REVOKE <privileges>
ON <object>
FROM <users>
```

  - Les privilèges sur l'objet mentionné sont retirés au receveur à moins que ce dernier ne les ait reçus d'une autre source, indépendante.
  - Cette procédure de révocation complique le mécanisme d'autorisation car il faut appliquer récursivement les procédures de révocation puisqu'un usager auquel on retire un privilège a pu le transmettre à d'autres.

Droits d'accès et Privilèges

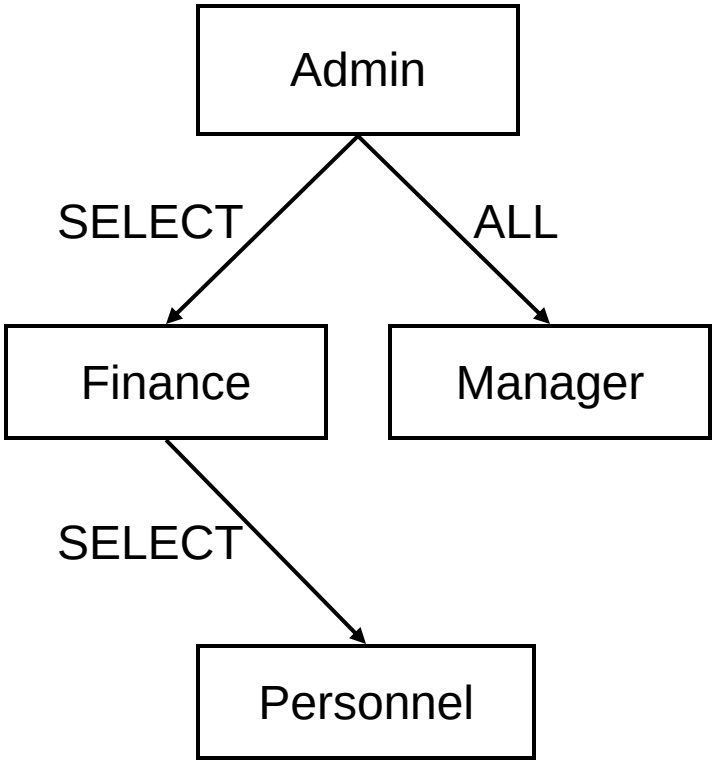
- Exemple
  - 'Admin' attribut tout les privileges à 'Manager' (ALL), et SELECT à 'Finance' avec **grant option**
  - 'Manager' attribut tout les privileges (ALL) à Personnel
  - 'Finance' attribut SELECT à Personnel



Droits d'accès et Privilèges

Exemple

- Manager' revoke tout les privileges (ALL) de 'Personnel'
  - 'Personnel' a encore le privilege SELECT aquis depuis 'Finance'
- 'Admin' revokes SELECT depuis 'Finance'
  - Personnel perd le privilege de selectionner SELECT pareillement



Injection SQL

- Dans une attaque par injection SQL, l'auteur insère généralement (ou « injecte ») des informations de bases de données non autorisées dans une chaîne de données SQL vulnérable.
- Ces informations injectées sont ensuite envoyées vers la base de données où elles sont exécutées. En utilisant l'injection SQL, les auteurs d'attaques peuvent obtenir l'accès illimité à l'ensemble d'une base de données.
  - SOLUTION
- La technologie IPS peut identifier les procédures enregistrées vulnérables ou les chaînes d'injection SQL. Cependant, la technologie IPS seule n'est pas fiable puisque les chaînes d'injection SQL sont sujettes à des faux positifs.
- Le contrôle d'accès des requêtes permet de restreindre les privilèges d'accès aux bases de données à un minimum requis d'opérations SQL (SELECTIONNER, METTRE A JOUR).

Déni de service(DOS - Denial Of Service)

- Techniques communes de dos:

- Se profiter de la vulnérabilité d'une plate-forme de bases de données pour faire tomber un serveur.
- L'engorgement du réseau, et la surcharge en ressources du serveur (mémoire, unité centrale, etc.).
- Solution
  - Les contrôles de connexion empêchent la surcharge en ressources du serveur en limitant les taux de connexion, les taux de requêtes, et autres variables pour chaque utilisateur des bases de données.

Déni de service(DOS - Denial Of Service)

- Solution (suite)
  - Le contrôle d'accès des requêtes, pour détecter toutes requêtes non autorisées pouvant créer un déni de service.
  - Le contrôle du temps de réponse -response timing– les attaques de déni de service des bases de données visant à surcharger le serveur en ressources provoquent des réponses de bases de données différées.
  - Détecter les délais de réponse pour une requête individuelle ainsi que pour l'ensemble du système.

Vulnérabilités des protocoles de communication des bases de données

- Exemple: Le ver informatique SQL Slammer2, a profité d'une faille sur le protocole du serveur Microsoft SQL pour forcer un déni de service
- Solution
  - La technologie de validation de protocole décompose (désassemble) essentiellement le trafic des bases de données et le compare aux prévisions de trafic. Dans le cas où le trafic réel ne correspond pas aux prévisions, des alertes ou des actions de blocage peuvent être mises en place.

Copies non autorisées de données sensibles

- Si les contrôles nécessaires ne sont pas appliqués on risque de créer de nouvelles BDD « cachées » et les données sensibles –(les détails des transactions, ainsi que les coordonnées des clients et des employés) peuvent être copiées dans ces bases de données.
- Que ce soit de manière intentionnelle ou non, les employés ou les pirates informatiques peuvent alors accéder illégalement aux données sensibles.
- Solution
  - Prévention des copies non autorisées de données sensibles
    - Identifier toutes les bases de données sur le réseau qui contiennent des données sensibles.
    - Ensuite trouver quels sont les types de données sensibles dans les objets des bases de données.

Exposition de données de sauvegarde

- Les dispositifs de sauvegarde de bases de données auxiliaires ne sont généralement pas protégés contre d'éventuelles attaques.
- Par conséquent, plusieurs violations de sécurité importantes ont vu le jour, y compris le vol de disques durs et de bandes de sauvegarde de bases de données.
- SOLUTION
  - Prévention de l'exposition de données auxiliaires
    - Toutes les sauvegardes de bases de données devraient être cryptées. (cryptage de toute les BDD y compris les fichiers, les relations, et les tables ou cryptage des colonnes seulement)
    - mais les performances et les inconvénients liés à la gestion des clés cryptographiques rend souvent cette solution peu pratique.

Protection du réseau

Introduction

- Circulation des mots de passe en clair.
- Authentification faible basée sur le numéro IP (Cas du protocole rlogin)
- Commandes à distance non sécurisées.
- Transferts de fichiers non sécurisés.

Solution: l'utilisation des protocoles de communication sécurisés

Virtual Private Network (VPN)

- Principe:
  - Permet d'établir des communications sécurisées en s'appuyant sur un réseau existant non sécurisé.
  - Utilisation de protocoles sécurisés pour la création d'un canal de communication sécurisé à usage privé, au travers d'un réseau public non sécurisé.
  - Souvent mis en œuvre par une organisation pour assurer la sécurité des échanges notamment pour l'interconnexion de ses différents sites géographiques via Internet ou bien pour autoriser des utilisateurs nomades.
  - Utilisation de protocoles réseaux sécurisés de tunneling (e.g. L2TP, IPsec, SSL/TLS)

Virtual Private Network (VPN)

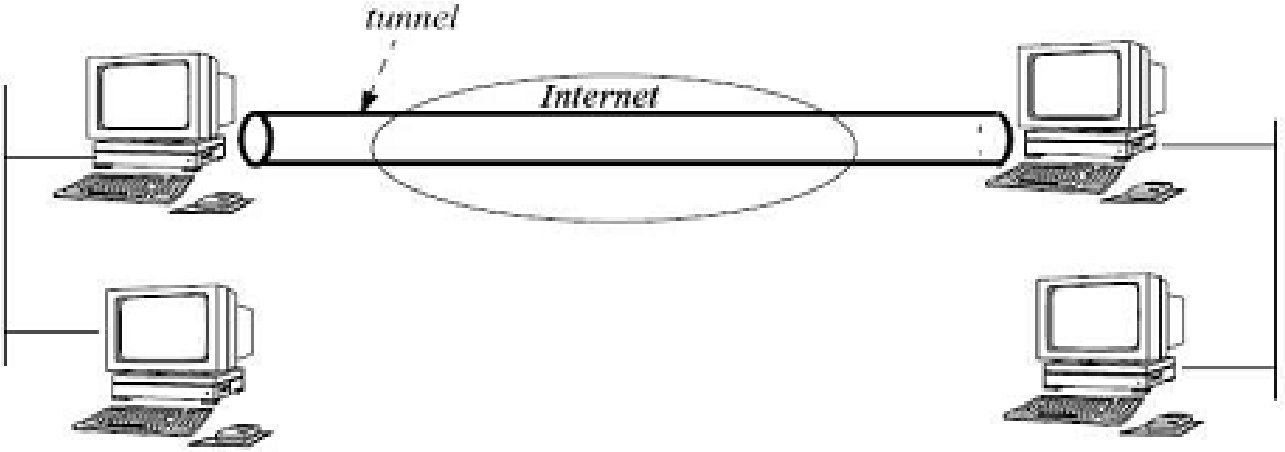
- Protocole de Tunneling : protocole réseau qui encapsule un autre protocole.
- BUT("protocole de tunneling")

  – Faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre du tunnel.

  –Les utilisateur ont l'impression de se connecter directement sur le réseau de leur entreprise.

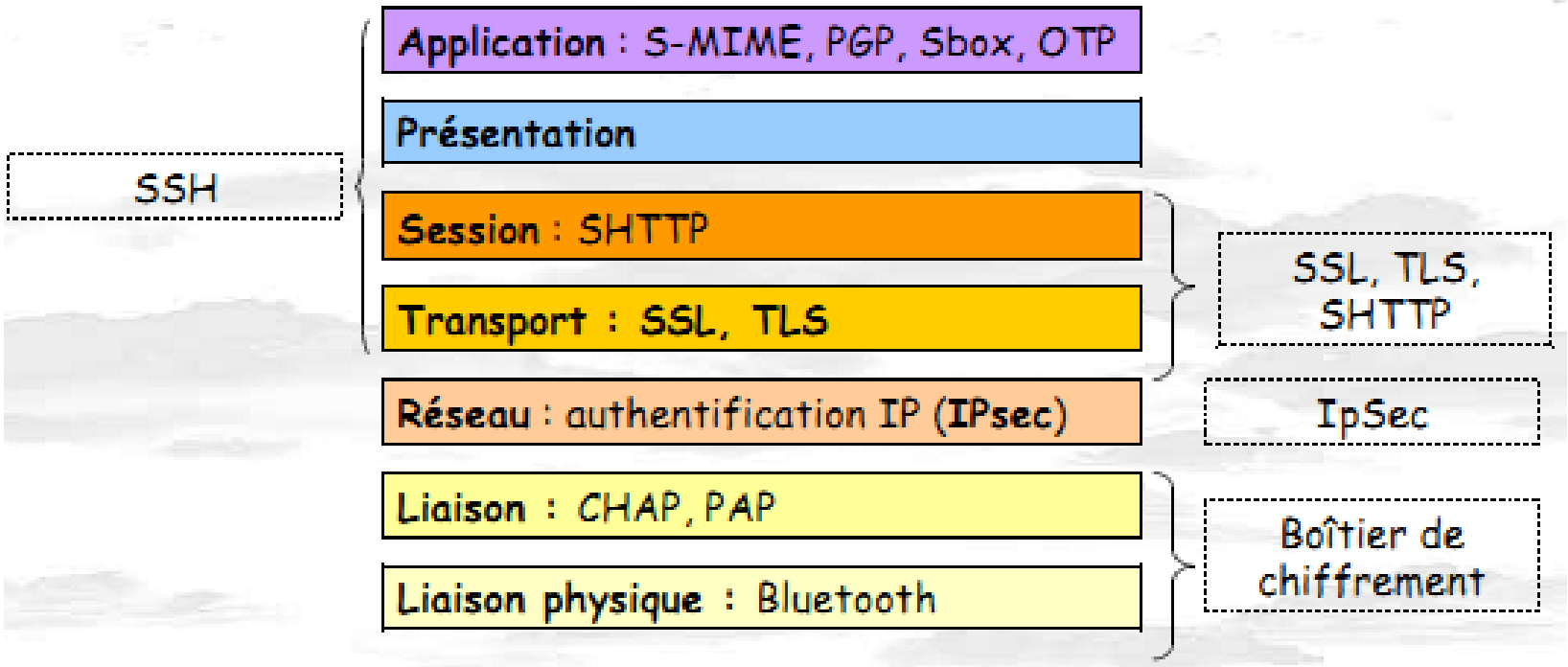
Virtual Private Network (VPN)

- Consiste à construire un chemin virtuel après avoir identifié l'émetteur/destinataire la source chiffre les données et les achemine en empruntant ce chemin virtuel.
- Le tunneling est l'ensemble de processus d'encapsulation, transmission et désencapsulation.



Protocoles de communications sécurisés

- Pour sécuriser les échanges ayant lieu sur un réseau TCP/IP, il existe plusieurs protocoles:



Internet Protocol Security (IPSec)

- IPsec veut dire IP Security Protocols : ensemble de mécanismes de sécurité commun à IPv4 et IPv6
- IPsec vise à sécuriser les échanges de données au niveau de **la couche réseau (IP).**
- Un des méthodes permettant de créer des VPN.

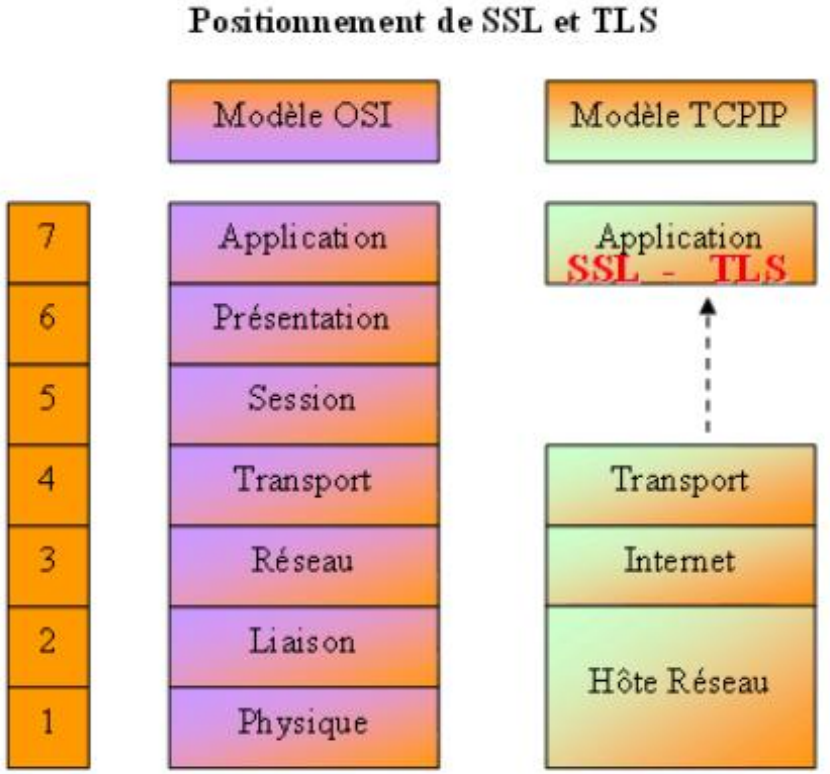
Internet Protocol Security (IPSec)

- Deux modes d'échange
  - Mode Transport : un en-tête (header) IPSec s'intercale entre l'en-tête IP et les données sans modifier l' en-tête IP d'origine. Protège juste les données.

  - Mode tunnel : encapsule l'intégralité du paquet IP original dans un paquet IPSec auquel on ajoute un nouvel en-tête IP. Protège l'en- tête IP +données

Secure Socket Layer/Transport Layer Security (SSL/TLS)

- Conçu et développé par Netscape
- Standardisé par l'IETF sous le nom de TLS
- Couche fine entre la couche application (HTTP) et la couche TCP (transport)



Secure Socket Layer/Transport Layer Security (SSL/TLS)

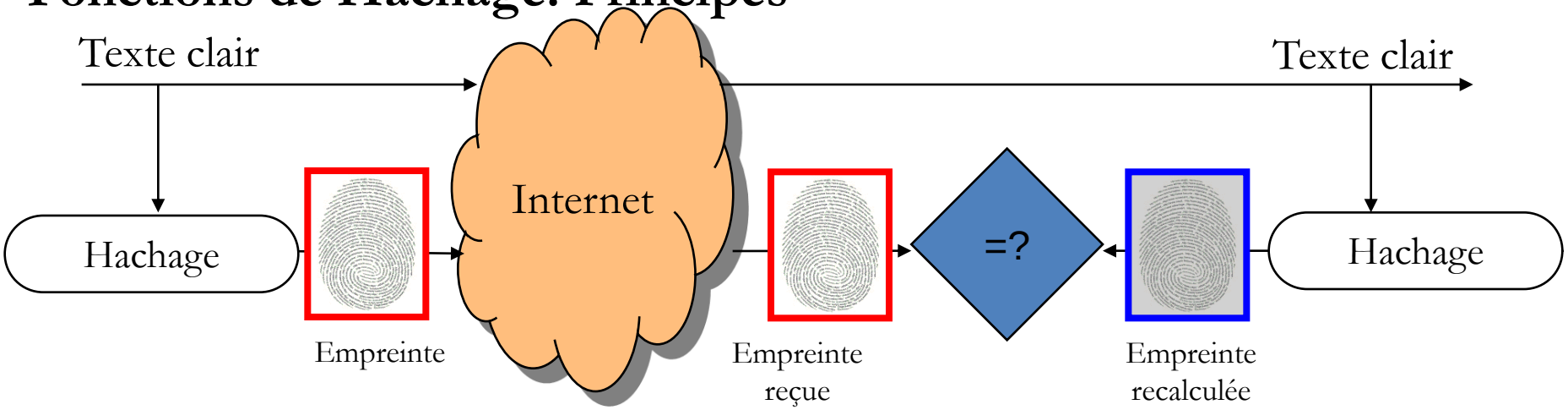
- SSL/TLS sont largement utilisés sur les navigateurs web et les serveurs pour assurer l'e-commerce securisé et pour la sécurisation des sites www **(https)**.
- SSL est composé de:
    - Générateurs de clés
    - Fonctions de hachage
    - Algorithmes de chiffrement
    - Protocoles de négociation et de gestion de session
    - Certificats

Secure Socket Layer/Transport Layer Security (SSL/TLS)

- Fonction de hachage
- Entrée: message M avec contenu et taille arbitraire.
- Sortie: message de taille fixe h=H(M).
- La fonction de hachage permet d'extraire une empreinte qui caractérise les données.
  - Une empreinte a toujours une taille fixe indépendamment de la taille des données.
- Irréversible:
  - Etant donnée h, il est difficile de trouver x tel que: h = H(x)
  - Complexité de l'ordre de 2^n, n est le nombre de bits du *digest*.
- Calcul facile et rapide (plus rapide que le cryptage symétrique).

Secure Socket Layer/Transport Layer Security (SSL/TLS)

Fonctions de Hachage: Principes



1)  =

Empreinte reçue — Empreinte recalculée

Le texte reçu est intègre

2)  ≠ 

Empreinte reçue — Empreinte recalculée

Le texte reçu est altéré

SSL/TLS
Certificats numériques

- Les certificats numériques simplifient la tâche qui consiste à déterminer si une clé publique appartient réellement à son détenteur supposé.

- Un certificat correspond à une référence. Il peut s'agir par exemple de votre **permis de conduire,** de votre **carte de sécurité sociale** ou de votre **certificat de naissance**.

- Chacun de ces éléments contient des informations vous identifiant et **déclarant qu'une autre personne a confirmé votre identité**.

SSL/TLS

Certificats numériques

Un certificat numérique contient des données similaires à celles d'un certificat physique.

Un certificat numérique se compose de:

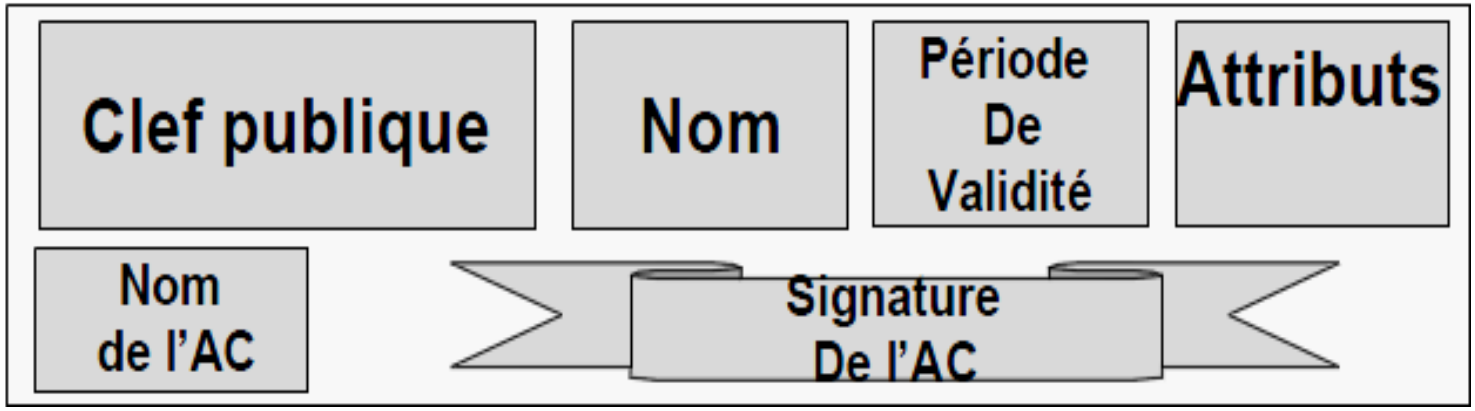
- Une clé publique.
- Des informations sur le certificat. (Informations sur l'« identité » de l'utilisateur:nom, ID utilisateur, etc.)
- Une ou plusieurs signatures numériques.

- La signature numérique d'un certificat permet de déclarer que ses informations ont été attestées par une autre personne ou entité.

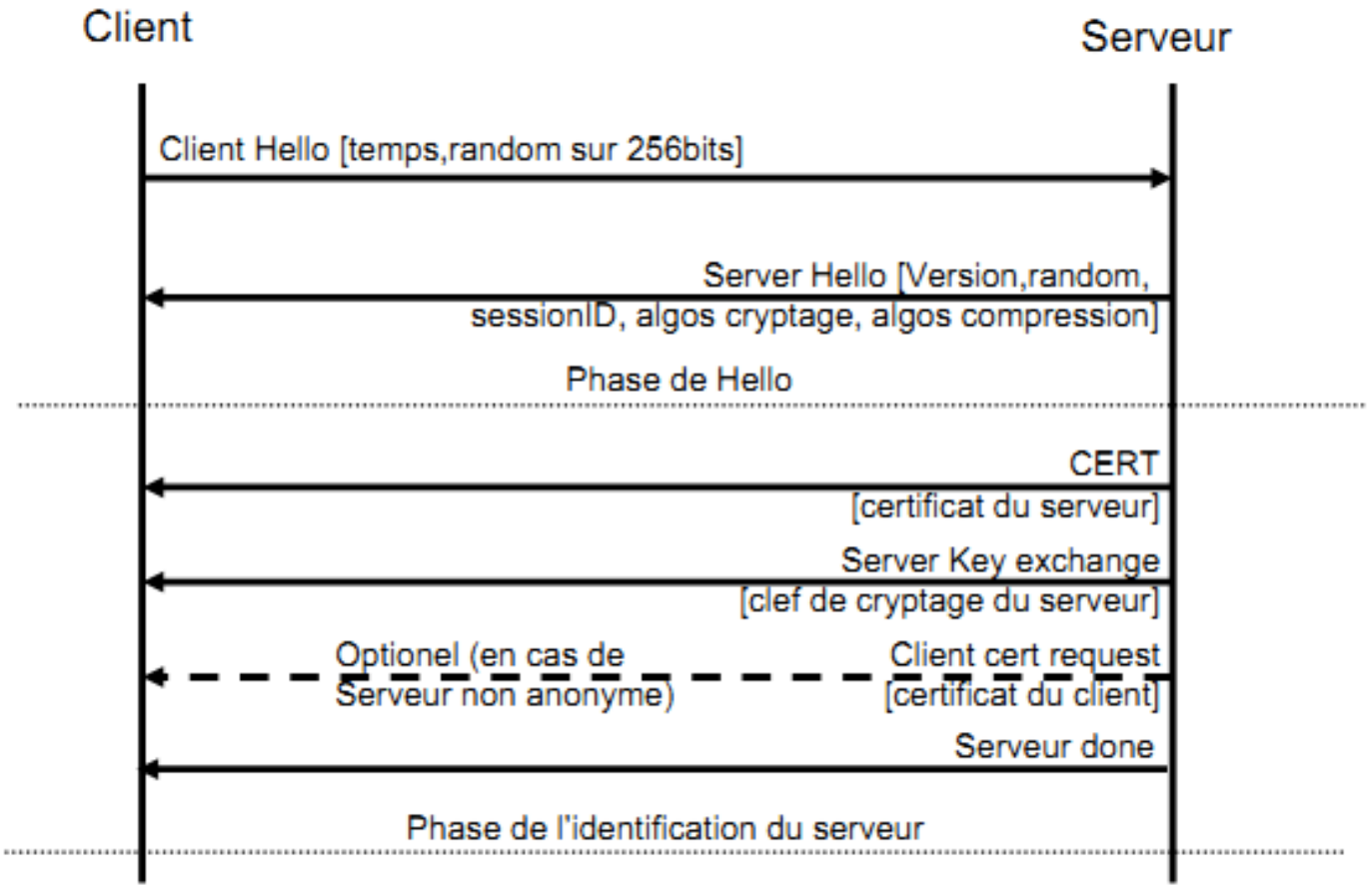
SSL/TLS

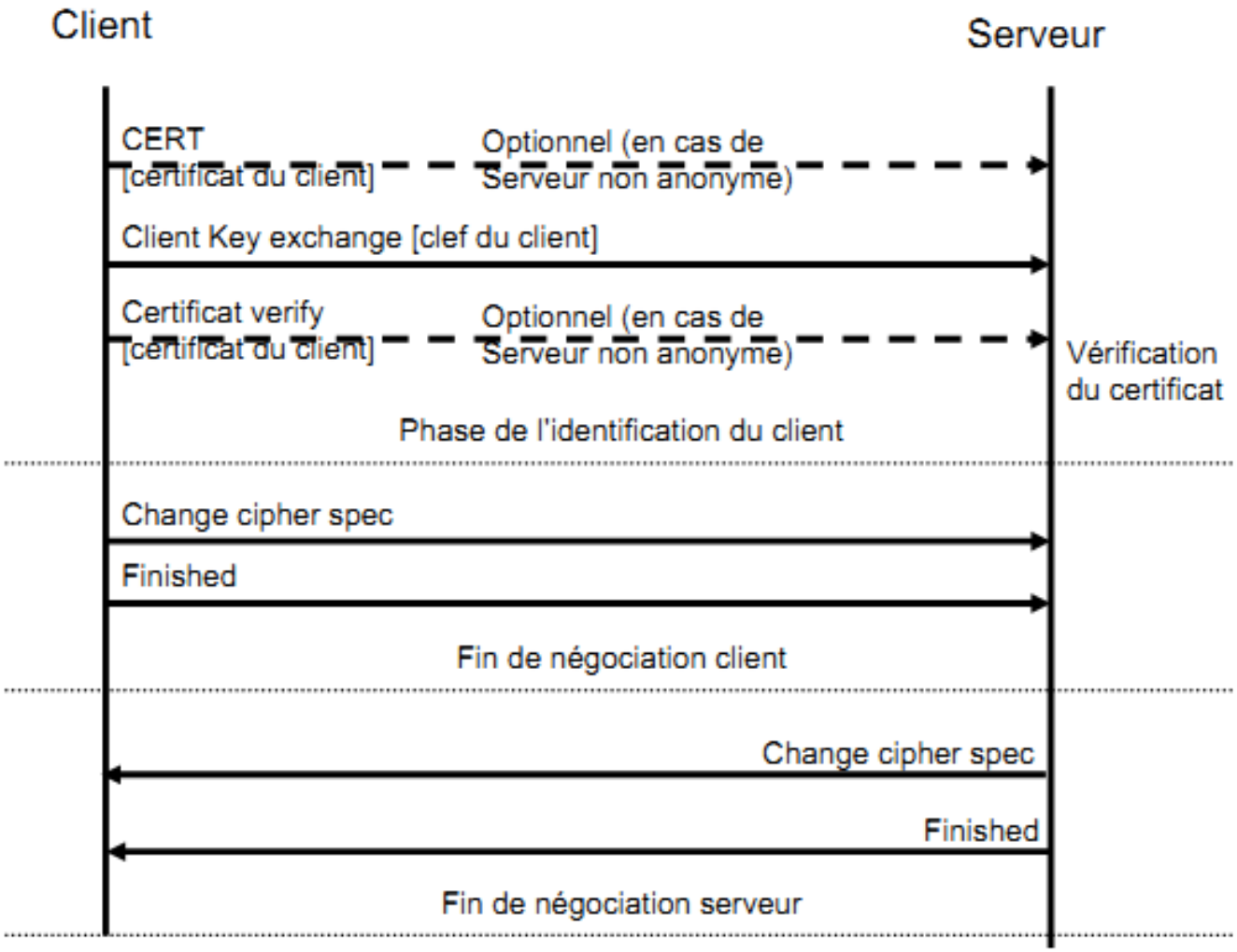
Certificats numériques

Les certificats sont émis par une autorité de certification (Certificate Authority – CA)



La négociation de session SSL




Client
Serveur
CERT
[certificat du client]
Optionnel (en cas de
Serveur non anonyme)
Client Key exchange [clef du client]
Certificat verify
[certificat du client]
Optionnel (en cas de
Serveur non anonyme)
Vérification
du certificat
Phase de l'identification du client
Change cipher spec
Finished
Fin de négociation client
Change cipher spec
Finished
Fin de négociation serveur

La négociation de session TLS (Handshake)

Message	Type de message	Sens de transmission	Signification
HelloRequest	optionnel	serveur → client	Ce message demande au client d'entamer le Handshake.
ClientHello	obligatoire	client → serveur	Ce message contient : le numéro de version du protocole SSL ; le nombre aléatoire : client_random ; l'identificateur de session : session_ID ; la liste des suites de chiffrement choisies par le client ; la liste des méthodes de compression choisies par le client.
ServerHello	obligatoire	serveur → client	Ce message contient : le numéro de version du protocole SSL ; un nombre aléatoire : serveur_random ; l'identificateur de session : session_ID ; une suite de chiffrement ; une méthode de compression.

La négociation de session TLS (Handshake)

Certificate	Optionnel	serveur → client client → serveur	Ce message contient le certificat du serveur ou celui du client si le serveur le lui réclame et que le client en possède un.
ServerKeyExchange	Optionnel	serveur → client	Ce message est envoyé par le serveur que s'il ne possède aucun certificat, ou seulement un certificat de signature.
CertificateRequest	Optionnel	serveur → client	Par ce message, le serveur réclame un certificat au client.
ServerHelloDone	Obligatoire	serveur → client	Ce message signale la fin de l'envoi des messages ServerHello et subséquents.
ClientKeyExchange	Obligatoire	client → serveur	Ce message contient le PreMasterSecret crypté à l'aide de la clé publique du serveur.
CertificateVerify	Optionnel	client → serveur	Ce message permet une vérification explicite du certificat du client.
Finished	obligatoire	serveur → client client → serveur	Ce message signale la fin du protocole Handshake et le début de l'émission des données protégées avec les nouveaux paramètres négociés.

Faille du protocole SSL:

- SSL v2:Forcer une faible taille de clef
- SSL v3: Accepte Finished avant ChangeCipherSpec
- SSLv3:Envoi de données chiffrées avant la réponse serveur au Finished.

Protocole Secure SHell (SSH)

- Permet d'obtenir un interprète de commande (Shell) distant sécurisé avec un système cible donné;
- La commande ssh est une version sécurisée de rsh (remote shell) et rlogin;
- SSH est un client de connexion à distance chiffrée, (couche 7), permet de créer un tunnel réseau.
- SSH utilise la cryptographie asymétrique (RSA) et symétrique;

Protocole Secure SHell (SSH)

Principe

- Un serveur SSH dispose d'un couple de clefs stocké dans le répertoire /etc/ssh et généré lors du lancement du serveur;

- Lorsqu'un client SSH se connecte au serveur, ce dernier envoie sa clé publique au client;

- Le client génère une clé secrète (chiffrement symétrique), et l'envoie au serveur, en cryptant l'échange avec la clé publique du serveur.

- Le serveur déchiffre la clé secrète avec sa clé privée.

Protocole Secure SHell (SSH)

Principe

- Pour prouver au client qu'il est bien le bon serveur (authentification du serveur), il crypte un message standard avec la clé secrète et l'envoie au client.

- Si le client retrouve le message standard en utilisant la clé secrète, il a la preuve que le serveur est le vrai.

- Une fois la clé secrète échangée, le client et le serveur peuvent alors établir un canal sécurisé (grâce à la clé secrète partagée).

Faille du protocole SSH

- Attaque à base de la méthode Man In The Middle: L'attaquant se place entre le client et le serveur afin d'intercepter les clés de l'encryptage.
- Incompatibilités entre différentes versions de ssh
- Accès par SSH à une machine interne donne aussi accès par tunnel SSH à toutes les autres machines internes.
- Avenir incertain face à IPSec, qui peut chiffrer et authentifier des protocoles IP/TCP/UDP et partie intégrante d'IPv6

Le protocole PGP

- Pretty Good Privacy (PGP) : Niveau applicatif
- PGP est une combinaison des fonctionnalités de la cryptographie de clé publique et de la cryptographie de clé secrète : **C'est un système hybride**

- PGP utilise la compression des données afin de renforcer la sécurité des informations, de réduire le temps de transmission et d'économiser l'espace disque.

Le protocole PGP

PGP crée une clé de session à usage unique. Cette clé correspond à un nombre aléatoire, généré par les déplacements aléatoires de la souris et les séquences de frappes de touche.

Pour crypter un texte clair, la clé de session utilise un algorithme de chiffrement symétrique conventionnel (DES, AES,...).

Une fois les données codées, la clé de session est chiffrée à l'aide de la clé publique du destinataire (à l'aide d'une méthode de chiffrement asymétrique).

Le protocole PGP

La clé de session chiffrée ainsi que le texte chiffré est transmis au destinataire.

Le processus de décryptage est l'inverse : le destinataire utilise sa clé privée pour récupérer la clé de session temporaire qui permettra ensuite de déchiffrer le texte chiffré.

DÉTECTION D'INTRUSION

Définitions

Faux-positif : détection en absence d'attaque. Une alarme générée par un IDS pour un évènement légal (Détection erronée).

- Faux-négatif : absence de détection en présence d'attaque. Le Non génération d'alarme par un IDS pour un évènement illégal (Non détection d'un paquet malicieux)
- Log : ligne d'un fichier d'un logiciel qui enregistre les données transitant sur un système pour le surveiller ou faire des statistiques.
- Fichier log : contient les évènements s'étant produits sur un système.

IDS (système de détection d'intrusion)

- On appelle IDS (Intrusion Detection System) un mécanisme écoutant le trafic réseau de manière furtive afin de repérer des activités anormales ou suspectes et permettant ainsi d'avoir une action de détection des risques d'intrusion.
- Intrusion: accès illicite

Classification des IDS

- Il existe deux grandes familles distinctes d'IDS

  ➢ Les N-IDS (Network Based Intrusion Detection System): ils assurent la sécurité au niveau du réseau.

  ➢ Les H-IDS (Host Based Intrusion Detection System) : ils assurent la sécurité au niveau des hôtes (terminaux).

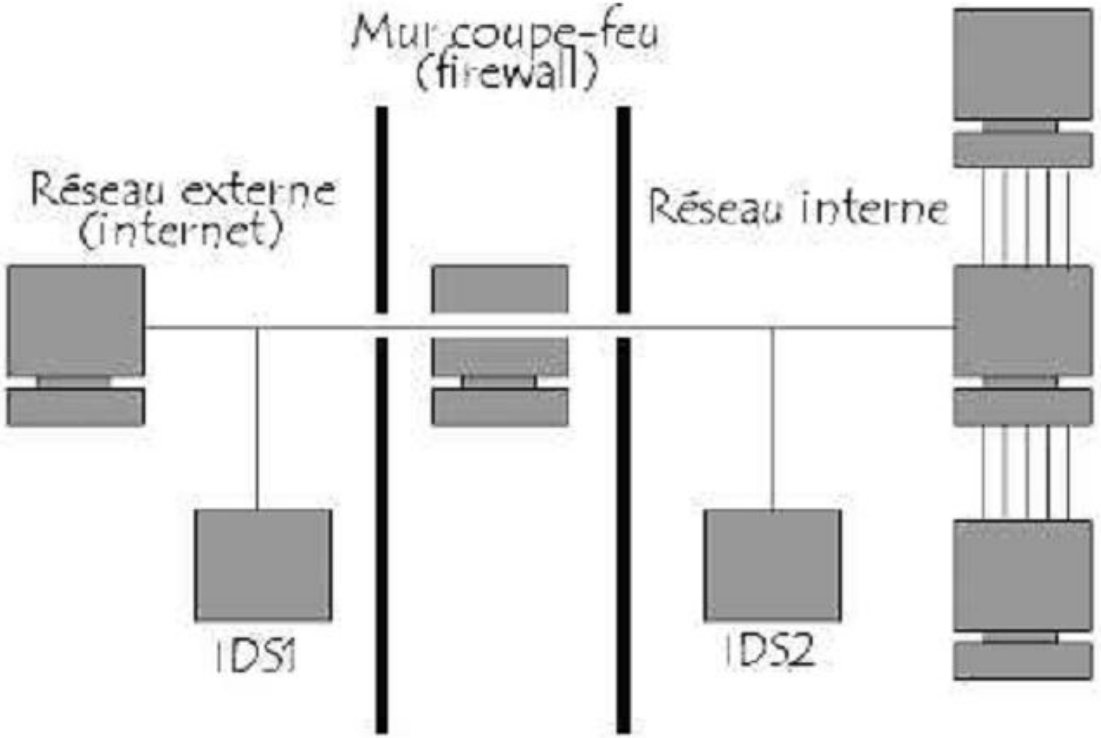
  ➢ IDS Hybrides: ils assurent la surveillance du réseau et de terminaux (NIDS + HIDS)

N-IDS

- Un N-IDS nécessite un matériel dédié et constitue un système capable de contrôler les paquets circulant sur un ou plusieurs liens réseau dans le but de découvrir si un acte malveillant ou anormal a lieu.
- Le N-IDS place une ou plusieurs cartes d'interface réseau du système dédié en mode promiscuité (promiscuous mode), elles sont alors en mode « furtif » afin qu'elles n'aient pas d'adresse IP .
- Doit recevoir tout le trafic du réseau (dorsale)

Positionnement d'un IDS

- Il est fréquent de trouver plusieurs IDS sur les différentes parties du réseau et en particulier de placer une sonde à l'extérieur du réseau afin d'étudier les tentatives d'attaques ainsi qu'une sonde en interne pour analyser les requêtes ayant traversé le pare-feu ou bien menées depuis l'intérieur.



H-IDS

- Le H-IDS réside sur un hôte particulier;
- Le H-IDS analyse des informations particulières dans les journaux de logs et aussi capture les paquets réseaux entrant/sortant de l'hôte pour y déceler des signaux d'intrusions (déni de services, backdoors, chevaux de Troie, tentatives d'accès non autorisés, etc.).

Techniques de détection d'intrusion

- Un N-IDS est capable de capturer les paquets lorsqu'ils circulent sur les liaisons physiques sur lesquelles il est connecté.
- Il peut appliquer les techniques suivantes pour reconnaître les intrusions :
  - 1-Vérification de la pile protocolaire
  - 2- Vérification des protocoles applicatifs
  - 3-Reconnaissance des attaques par pattern matching

Techniques de détection d'intrusion
1-Vérification de la pile protocolaire

- Un nombre d'intrusions, tels que par exemple ping of death ont recours à des violations des protocoles IP, TCP, UDP, et ICMP pour attaquer une machine. Une simple vérification protocolaire peut mettre en évidence les paquets invalides et les signaler .

Techniques de détection d'intrusion
2- Vérification des protocoles applicatifs

- Un nombre d'intrusions utilisent des comportements protocolaires invalides, comme par exemple WinNuke, qui utilise des données NetBIOS invalides.
- Pour détecter efficacement ce type d'intrusions, un N-IDS doit implémenter une grande variété de protocoles applicatifs tels que NetBIOS, TCP/IP…

Techniques de détection d'intrusion
3-Reconnaissance des attaques par pattern matching

- Technique de reconnaissance d'intrusions la plus ancienne et elle est encore très courante.
- Il s'agit de l'identification d'une intrusion par le seul examen d'un paquet et la reconnaissance dans une suite d'octets du paquet d'une séquence caractéristique d'une signature précise.
- Cette technique est répandue chez les N-IDS de type « Network Grep » basé sur la capture des paquets bruts sur le lien surveillé, et comparaison via un analyseur sémantique de type « expressions régulières » qui va tenter de faire correspondre les séquences de la base de signatures octet par octet avec le contenu du paquet capturé.
  - Avantage : sa facilité de mise à jour et évidemment dans la quantité importante de signatures contenues dans la base du N-IDS.
  - Inconvénient : elle entraîne néanmoins inévitablement un nombre important de fausses alertes ou faux positifs.

IPS (système de Prévention d'intrusion)

- L'IPS est un système de prévention/protection contre les intrusions et non plus seulement de reconnaissance et de signalisation des intrusions.
- Un IPS est constitué en natif d'une technique de filtrage de paquets et de moyens de blocages (drop connection, drop offending packets, …).

IPS VS IDS

- Le positionnement en coupure sur le réseau de l'IPS et non plus seulement en écoute sur le réseau pour l'IDS (traditionnellement positionné comme un sniffer sur le réseau).
- La possibilité de bloquer immédiatement les intrusions quel que soit le type de protocole de transport utilisé et sans reconfiguration d'un équipement tierce.

Principe de fonctionnement IDS

- Informations collectées par des sondes
- Traitement des informations
- Comparaison avec des données de référence qui correspondent:
  - À des opérations interdites ou autorisées
- Si anomalie : déclenchement d'une alarme et éventuellement activation d'une réponse active;

Approches de détection

- Approche comportementale
- Approche par scénarios

Approche comportementale

- Détection d'anomalies constatées sur le Système d'Information

1. phase d'apprentissage du comportement normal du système: établir des profils correspondant aux comportements normaux
   - Par respect de la politique de sécurité
   - Par fonctionnement naturel des applications
   - Par habitude des utilisateurs

2. Phase de détection de toute déviation par rapport au comportement normal

Approche comportementale

- IDS probabiliste: Apprentissage des probabilités liées à chaque séquence d'évènements
- IDS statistique: Attribution de valeurs statistiques aux différentes variables utilisées telle que:
  - Taux d'occupation mémoire
  - L'utilisation des processeurs
  - La durée et l'heure des connexions,
  - Sites les plus visités etc.

Approche comportementale …suite

- IDS à réseaux de neurones: surveillance directe du comportement des utilisateurs. Chaque utilisateur peut être identifié par son comportement
  - Ses habitudes de travail
  - Ses activités
  - Ses outils de travail,
  - Construction du profil : réseau de neurones qui reconnait une suite d'opérations effectuées par l'utilisateur
  - But : prédire l'action suivante de l'utilisateur. En cas d´´echec une alerte est levée

Approche comportementale

- Avantages
  - Capacités de détecter de nouvelles attaques
  - Besoin de peu de maintenance
- Inconvénients
  - Risque d'attaque lors de la construction des profils
  - Pas adapté au changement d'entité modélisée
  - Évolution des profils au cours du temps peut être vu comme une faille

Approche par scénarios

- IDS par scénarios: modélisation des comportements interdits
  - L'IDS émet l'hypothèse d'un scénario d'attaque s'il s'agit d'un scénario connu dans la bibliothèque de signatures alors une alarme est déclenchée
- IDS à recherche de motifs: recherche d'une séquence d'informations particulières dans un évènement d'audit;

Approche par scénarios …suite

- IDS à détection par inférences: basé sur le principe d'inférence de Bayes;

- IDS par model checking: basé sur la logique temporelle du premier ordre;

Approche par scénarios

- Avantages
  - Fiabilité pour les attaques connues
- Inconvénients
  - Maintenance active, mise à jour régulière