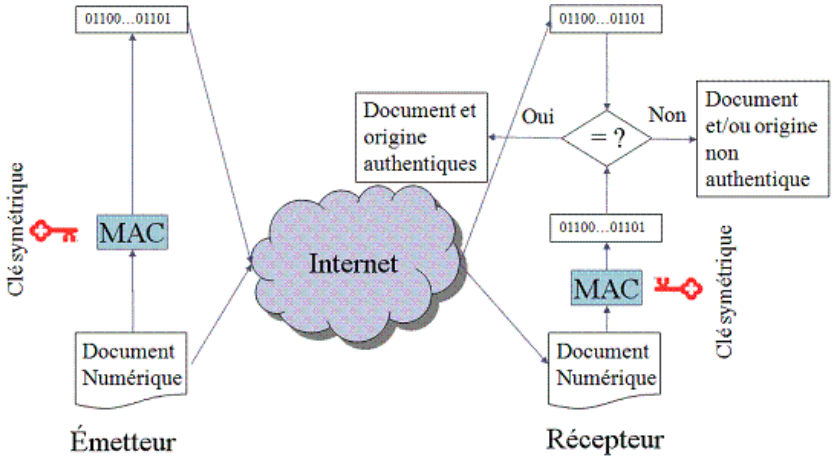
ierie des Protocoles et Logiciels Sécurisés

Introduction à la Sécurité Informatique

Version 1



Yacine Challal

14/01/2015

Table des matières

Introduction à la sécurité des échanges

I

Dans cette partie on présentera les différents défis de la sécurité informatique, les différents types d'attaques et leurs motivations, les services de sécurité, et des statistiques sur les pertes engendrées par des attaques sur les systèmes d'information d'entreprise.

A. Réseaux informatiques : Risques et enjeux

Confiance et Internet

Dans la vie courante la plupart des transactions reposent sur une « confiance » acquise par une relation en face à face ou un contact physique . Dans le cybermonde cette relation de proximité est rompue. Comment établir une relation de confiance indispensable à la réalisation de transactions à distance entre personnes qui ne se connaissent pas ? Ce cours a pour but de répondre à cette question.

Fondamental : Part de responsabilité des usagers

Thucydite dit : « Ce ne sont pas les murs qui protègent la citadelle, mais l'esprit de ses habitants ». Ceci s'applique également aux systèmes d'information où les statistiques indiquent que 40% des attaques sont causées par les usagers du SI eux mêmes.

Rappel : Environnement de l'entreprise

Une vingtaine d'années auparavant, les systèmes d'information d'entreprises étaient plutôt centralisés, basés sur des échange papiers, sans accès distants. Aujourd'hui les SI d'entreprises sont plutôt distribués sur plusieurs sites: on retrouve notamment un siège principales et des succursales, des filiales, des télé-travailleurs, des commerciaux, ... L'accès distants devient alors indispensable pour supporter cette décentralisation et la mondialisation des échanges. Ceci devient plus important avec les nouvelles technologies sans fils (Haut débit sur GSM, UMTS, WiMAX, etc.) et la forte pénétration d'Internet dans nos sociétés ;dans quelques années le nombre d'internautes atteindra les 3.000.000.000 de personnes.

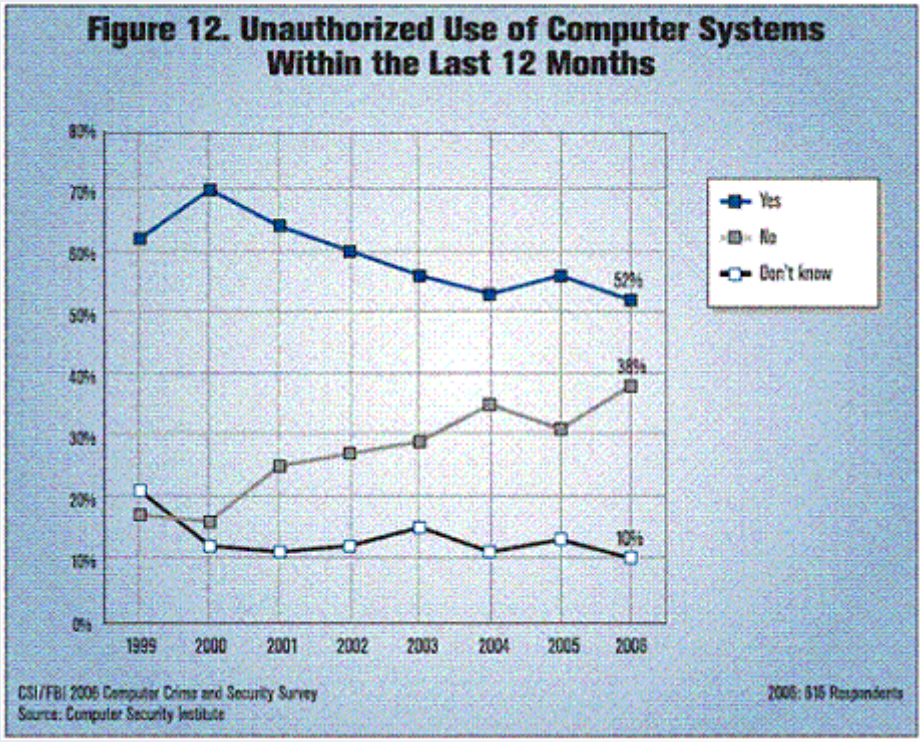
Attention : Risques liés aux réseaux

Malgré les bienfaits des réseaux informatiques, ceux-ci présentent d'énormes

risques. Parmi ceux-là on peut citer :

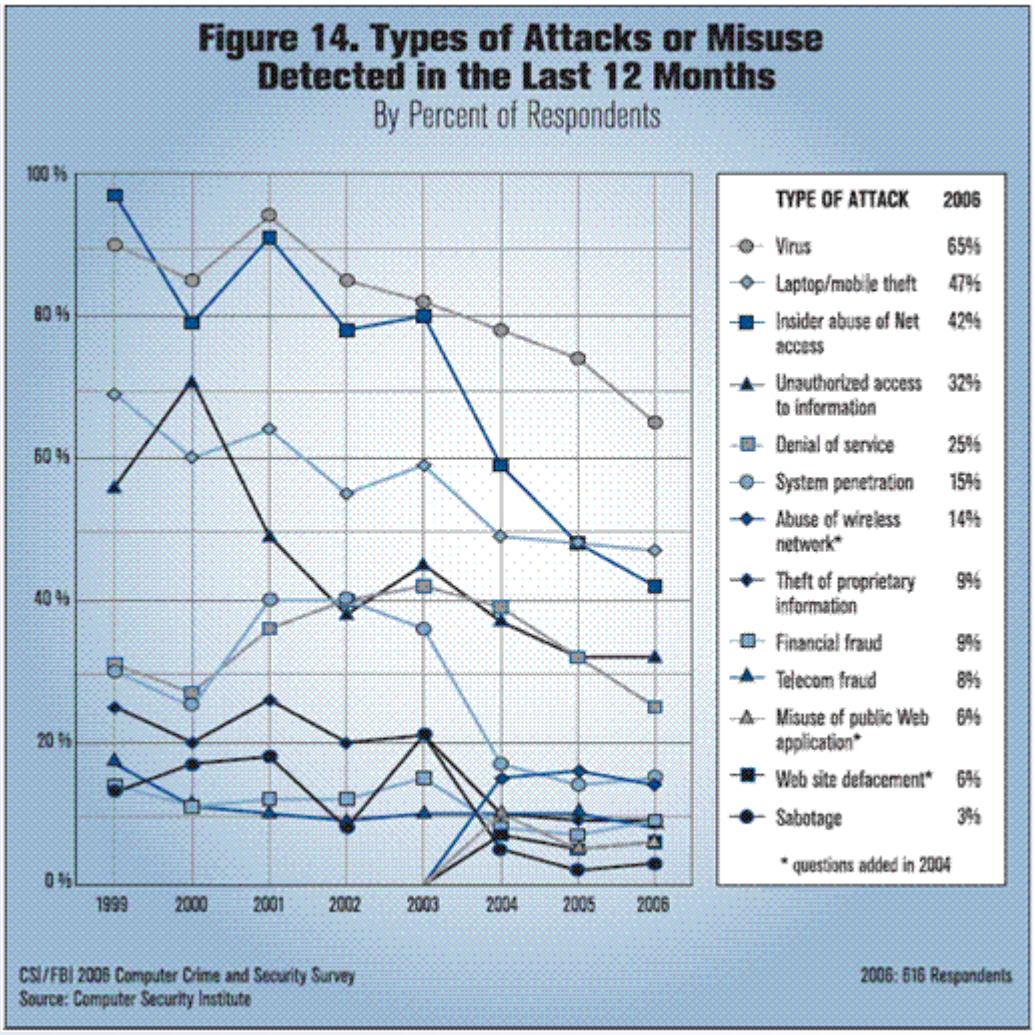
- Interception de messages
  - Prise de connaissance des mots de passe
  - Vol d'information
  - Perte d'intégrité du système et du réseau
- Intrusion des systèmes
  - Vol ou compromission des informations
  - Destruction des informations
  - Virus
  - Détournement de biens
- Perte d'accessibilité au système ou au réseau
- Faux clients, marchands escrocs

Malgré la panoplie de technologies utilisées pour sécuriser les SI des entreprises, les attaques sur les SI existent toujours comme illustré dans la figure suivante tirée d'une enquête du FBI/CSI en 2006.



Accès frauduleux aux SI

La figure suivante illustre les différents types d'attaques notées en 2006 :



Types d'attaques sur les SI en 2006

Motivations d'un attaquant

Un attaquant n'est pas forcément un "hacker" chevronné. Ca peut être n'importe quelle personne avec des motivations aussi banales que les suivantes :

- Le gain financier
  - Récupération de num de cartes bancaires, ...
- Vengeance
  - Site www.aljazeera.net lors de la couverture de la guerre d'irak
- Besoin de reconnaissance
  - Attaque contre le site du cerist avec un message sur les restrictions d'accès à Internet à Cuba.
- Curiosité
  - Attaques d'étudiants du MIT sur le premier ordinateur IBM 704 au MIT en 1959.
- Recherche d'émotions fortes
- Ignorance
  - Envoie de mots de passes par email, ...

Pertes phénoménales !!!

Les pertes financières dues aux attaques informatiques sont phénoménales. D'après une enquête réalisée par le FBI/CSI :

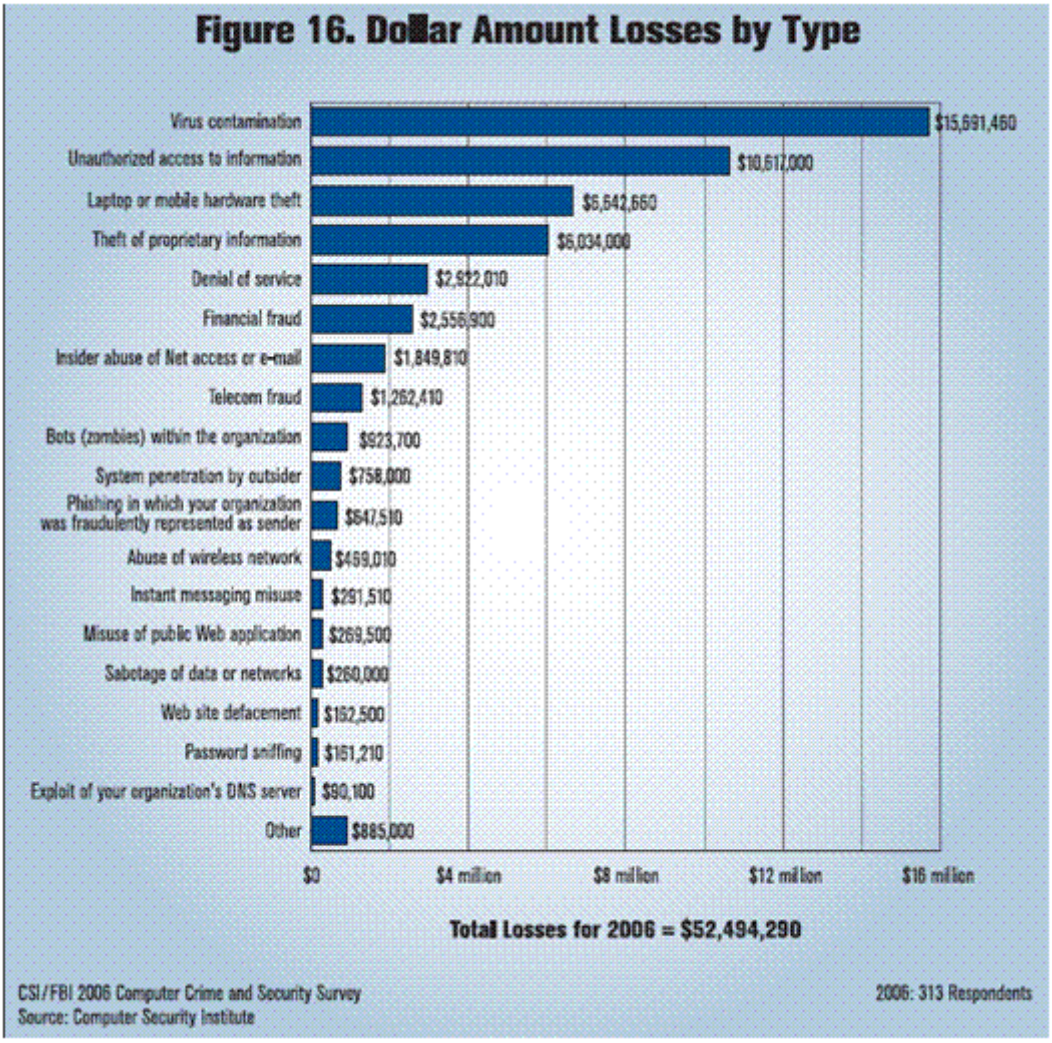
74% des pertes financières des entreprise sujets de l'enquête sont duent aux :

- attaques de virus (plus de 15 millions de dollars de perte)
- accès non autorisés aux systèmes d'information (plus de 10 millions de dollars de perte)
- vols d'équipement mobile (plus de 6 millions de dollars)
- vols de la propriété intellectuelle (plus de 6 millions de dollars)

52% des organisations sondées ont déclaré avoir été attaqué les 12 derniers mois (2006) :

- 24% d'entre elles ont reporté plus de 6 attaques
- 48% ont reporté 1 à 5 attaques

La figure suivante illustre la répartition des pertes sur leurs causes :



Pertes financères

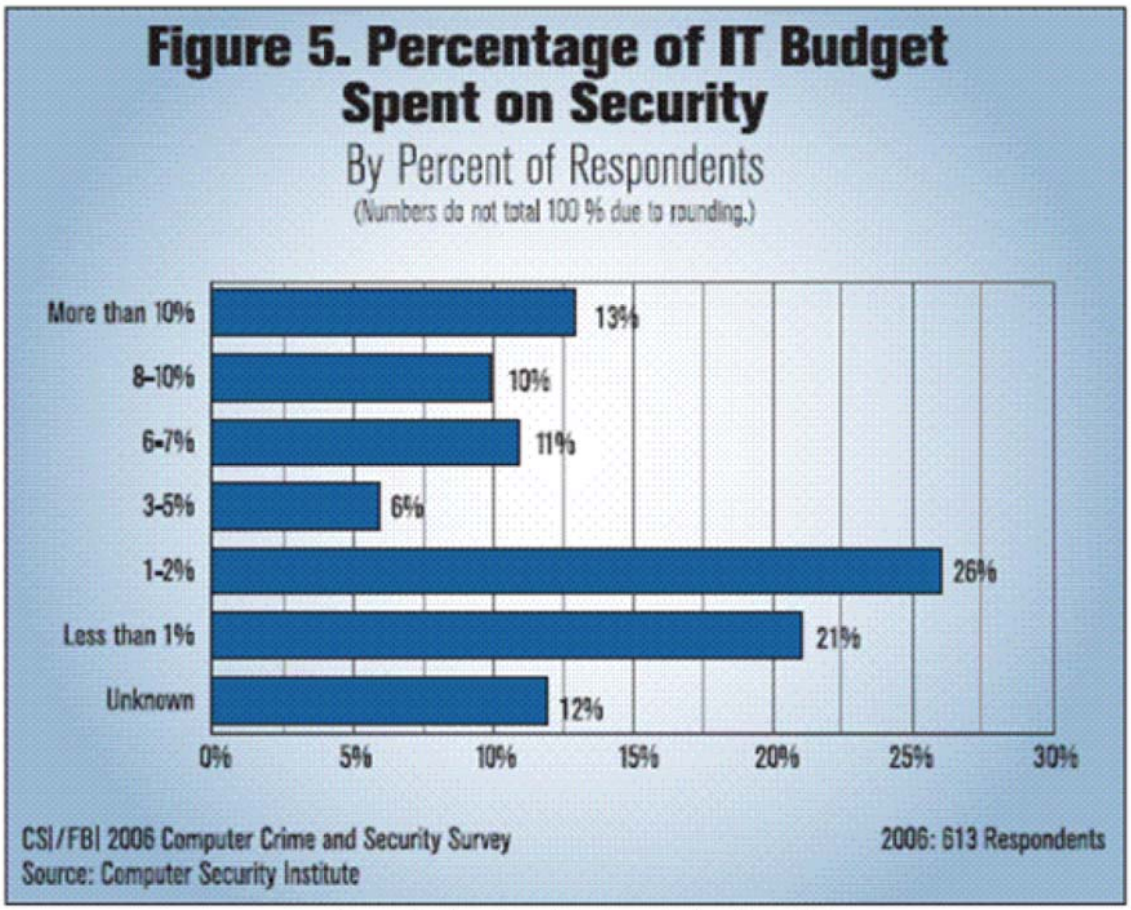
Complément : Rehaussement des budgets réservés à la sécurité des SI

La conséquence immédiate de ces pertes qui sont majoritairement liées à la sécurité des SI, est l'augmentation importante des budgets alloués à sécuriser les SI et à former le personnel sur la sécurisation des SI et des échanges d'information. Selon la même enquête :

- 34% des organisations allouent pas moins de 5% du budget informatique à la sécurité informatique

  - En 2006, les compagnies de revenues inférieurs à 10 millions de dollars ont dépensé en moyenne 1349 dollars par employé pour la sécurité informatique- un rehaussement de 210% par rapport à l'année 2005
- plus de 80% des institutions conduisent un audit de sécurité informatique
- la majorité des institutions jugent la formation en sécurité informatique comme importante et stratégique
  - 61% de ces organisations refusent de sous-traiter leurs fonctions de sécurité informatique

La figure suivante illustre le pourcentage du budget IT alloué à la sécurité :



Part de la sécurité dans le budget IT

Remarque : Rapport du FBI/CSI

Le FBI/CSI (Computer Security Institute) publie chaque année un rapport sur la sécurité informatique. Voici le rapport du FBI/CSI pour 2007 :

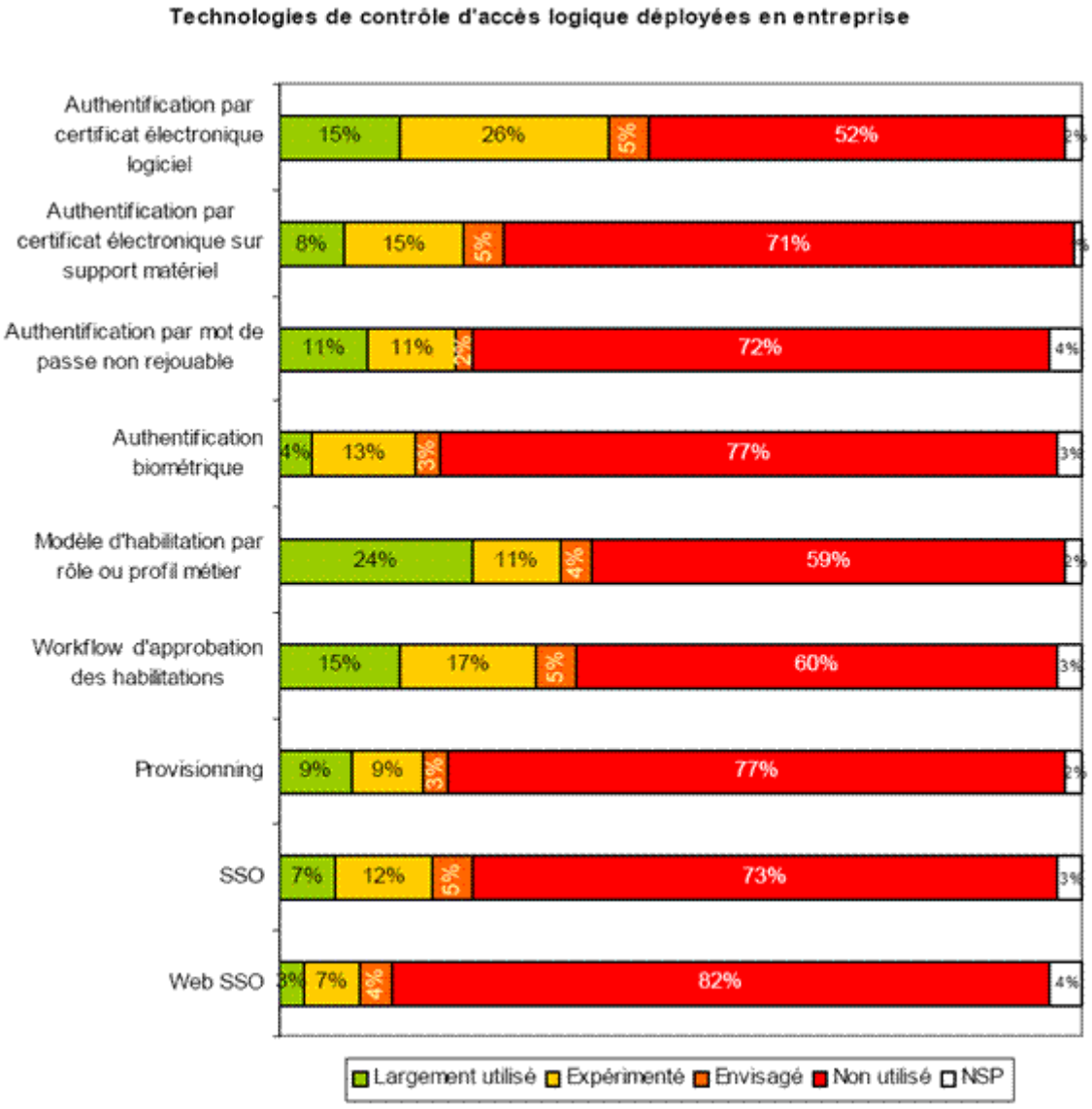
Exemple : Menaces Informatiques et Pratiques de Sécurité en France

Selon un le rapport 2008 du CLUSIF (Club de la Sécurité de l'Information Français) :

- Plus de 70% des entreprises françaises ont une forte dépendance à l'informatique
- Le budget moyen alloué pour la sécurité du SI dépasse 114K€ dans 21% des cas.
- 28% des entreprises du secteur des services, banques et assurances ont augmenté leur budget sécurité du SI de plus de 10% en 2008

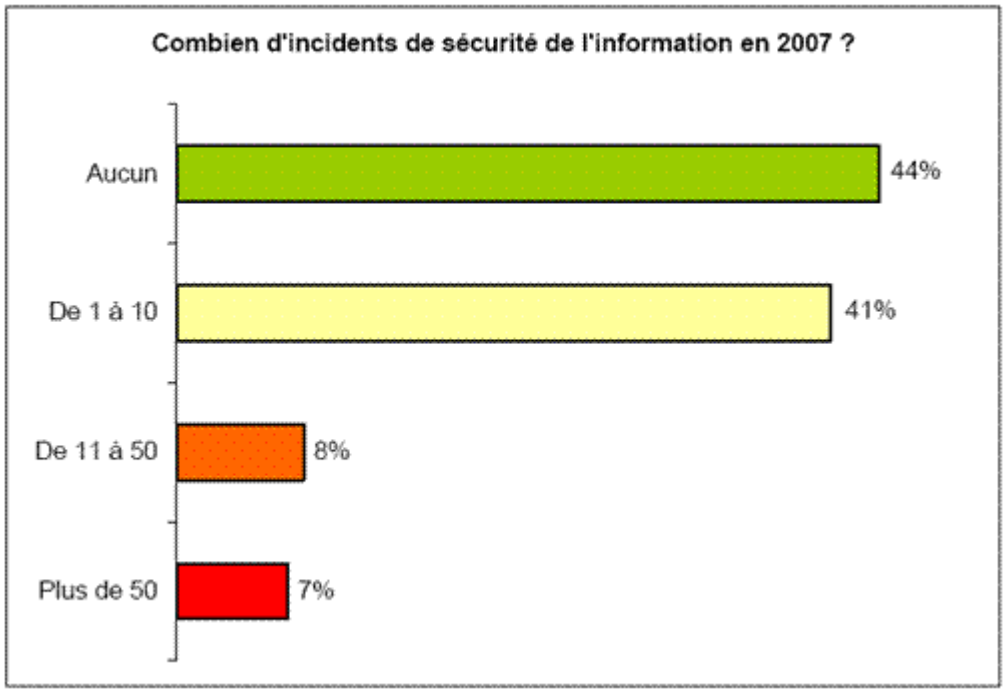
- 53% des Responsables de Sécurité du SI (RSSI) dénoncent le manque de personnel qualifié comme frein majeur à la conduite de leur mission.
- Plus de 30% des entreprises n'ont pas une Politique de Sécurité de l'Information (PSI), et 45% de celles qui en ont ne respectent pas une norme de sécurité.
- Le rattachement de la RSSI à la DG passe de 39% en 2006 à 45% des cas en 2008.

Selon le même rapport du CLUSIF, beaucoup de technologies de contrôle d'accès sont méconnues et/ou non utilisées en entreprises françaises comme illustré dans la figure suivante :



Technologies de contrôle d'accès non utilisées en France

Le rapport note aussi que 56% des RSSI ont noté au moins un incident de sécurité



Incidents de sécurité informatique en France

Le rapport du CLUSIF 2008 est très riche et mérite une lecture. Le voici :

B. Définitions des Services de Sécurité

Voici quelques définitions informelles à retenir concernant les services de sécurité les plus importants

Définition : Authentification

Permet de vérifier l'identité revendiquée par une entité, ou l'origine d'un message, ou d'une donnée .

Définition : Confidentialité

Permet de se protéger contre la consultation abusive des données par des entités tierces indésirables

Définition : Contrôle d'intégrité

Permet de vérifier qu'une données n'a pas été modifiée par une entité tierce (accidentellement ou intentionnellement)

Définition : Contrôle d'accès

Permet de vérifier que toute entité n'accède qu'aux services et informations pour lesquelles elle est autorisée

Définition : Non répudiation

Permet de se protéger contre la contestation d'envoi et de réception de données lors d'une communication

Introduction à la cryptographie

II

Cette partie du cours introduira les mécanismes de base de la cryptographie moderne qui permettent de réaliser quatre services de sécurité fondamentaux :

1. La confidentialité
2. L'intégrité des données
3. L'authentification de l'origine de données
4. La non-répudiation de l'origine

Pour chacun de ces services nous rappellerons la définition puis nous introduirons le mécanisme cryptographique permettant de le réaliser.

A. La cryptographie

Définition : La cryptographie

Le mot « Cryptographie » est composé des mots grecques :

- CRYPTO = caché
- GRAPHY = écrire

C'est donc l'art de l'écriture secrète.

C'est une science permettant de préserver la confidentialité des échanges.

Définition : Cryptanalyse

La cryptanalyse est l'art de décrypter des messages chiffrés.

Objectifs

Parmi les objectifs de la cryptographie :

- Garantir la confidentialité
- Vérifier l'intégrité des données
- Gérer l'authentification

- Assurer la non-répudiation

B. La confidentialité

1. Confidentialité et chiffrement

Définition : Confidentialité

La confidentialité est la propriété qui assure que l'information est rendu inintelligible aux individus, entités, et processus non autorisés.

Définition : Chiffrement / déchiffrement

Le chiffrement est une transformation cryptographique qui transforme un message clair en un message inintelligible (dit message chiffré), afin de cacher la signification du message original aux tierces entités non autorisées à l'utiliser ou le lire. Le déchiffrement est l'opération qui permet de restaurer le message original à partir du message chiffré.

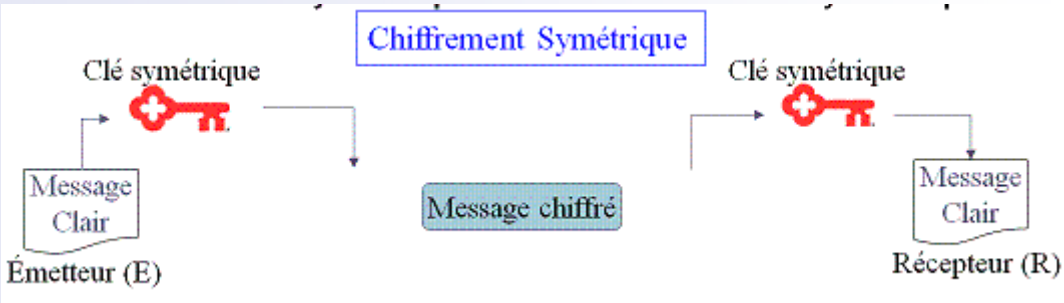
Clé de chiffrement

Dans la cryptographie moderne, l'habilité de maintenir un message chiffré secret, repose non pas sur l'algorithme de chiffrement (qui est largement connu), mais sur une information secrète dite CLE qui doit être utilisée avec l'algorithme pour produire le message chiffré.

Selon que la clé utilisée pour le chiffrement et le déchiffrement est la même ou pas, on parle de système cryptographique symétrique ou asymétrique.

Fondamental : Chiffrement symétrique

Dans le chiffrement symétrique, une même clé est partagée entre l'émetteur et le récepteur. Cette clé dite symétrique est utilisée par l'émetteur pour chiffrer le message te par le récepteur pour le déchiffrer en utilisant un algorithme de chiffrement symétrique.



Chiffrement Symétrique

Exemple : Algorithmes de chiffrement symétriques

Il existe deux types d'algorithmes de chiffrement symétrique :

1. Chiffrement par bloc : division du texte clair en blocs fixe, puis chiffrement bloc par bloc
   - DES: IBM, Standard NIST 1976
   - 3DES: W. Diffie, M. Hellman, W. Tuchmann 1978.
   - IDEA: Xuejia Lai et James Massey en 1992

- Blowfish: Bruce Schneier en 1993
- AES (Rijndael): Joan Daemen et Vincent Rijmen 2000

2. Chiffrement par flux : le bloc a une dimension unitaire (1 bit, 1 octet, ...), ou une taille relativement petite
   - RC4: Ron Rivest 1987
   - SEAL: Don Coppersmith et Phillip Rogaway pour IBM 1993.

Fondamental : Chiffrement asymétrique

Dans un système asymétrique, le récepteur génère une paire de clés asymétrique : une clé publique qui est diffusée à tout le monde et une clé privée maintenue secrète chez le récepteur. La particularité de cette paire de clé est que tout message chiffrée avec la clé publique ne peut être déchiffré qu'avec la clé privée correspondante. D'où la confidentialité des messages chiffré avec la clé publique d'un récepteur. Bien évidemment la clé privée correspondante ne peut être calculée à partir de la clé publique correspondante.

Chiffrement Asymétrique

Exemple : Algorithmes de chiffrement asymétrique

RSA: Rivest, Shamir et Adleman 1978

Diffie et Hellman 1976

2. Les modes d'opération du chiffrement symétrique

Dans le chiffrement symétrique l'algorithme opère sur un bloc. Pour chiffrer un ensemble de blocs constituants le message à chiffrer il est nécessaire de définir une stratégie d'opération sur la succession des blocs à chiffrer.

Il existe quatre modes définis dans FIPS 81 (1980)

- Electronic Code Book (ECB),
- Cipher Block Chaining (CBC),
- Cipher FeedBack (CFB) et
- Output FeedBack (OFB).

Syntaxe : Notation

Nous adoptons la notation suivante dans la description des quatre modes d'opération :

- T[n]: n-ième bloc du texte clair
- C[n]: n-ième bloc du texte chiffré
- E(m): fonction de chiffrement
- D(m): fonction de déchiffrement
- IV : Initialization Vector

- ^ : XOR

Electronic Code Book (ECB)

Chiffrement :C[n] = E(T[n])
Déchiffrement :T[n] = D(C[n])
Le même texte clair et clé de chiffrement donnent le même texte chiffré.

CBC : Cipher Block Chaining

Chiffrement :

- C[0] = E(T[0] ^ IV)
- C[n] = E(T[n] ^ C[n-1]) , si (n > 0)

Déchiffrement :

- T[0] = D(C[n]) ^ IV
- T[n] = D(C[n]) ^ C[n-1] , si (n > 0)

IV est envoyé en clair avec le message chiffré

CFB : Cipher Feedback

I[n]: bloc temporaire
Chiffrement :

- I[0] = VI
- I[n] = C[n-1] , si (n > 0)
- C[n] = T[n] ^ E(I[n])

Déchiffrement :

- I[0] = VI
- I[n] = C[n-1], si (n > 0)
- T[n] = C[n] ^ E(I[n])

Offre une sécurité plus élevée

OFB : Output Feedback

I[n]=nième bloc temporaire
R[n]=nième bloc temporaire second
Chiffrement :

- I[0] = VI
- I[n] = R[n-1] , si (n > 0)
- R[n] = E(I[n])
- C[n] = T[n] ^ R[n]

Déchiffrement :

- I[0] = VI
- I[n] = R[n-1] , si (n > 0)
- R[n] = E(I[n])
- T[n] = C[n] ^ R[n]

C. Intégrité de données

Définition : Intégrité de donnée

C'est la propriété qui permet de vérifier qu'une données n'a pas été modifiée par

une entité tierce (accidentellement ou intentionnellement).

Une fonction de hachage est typiquement utilisée pour vérifier l'intégrité de données.

Définition : Fonction de hashage cryptographique

Une fonction de hashage associe à une chaîne binaire (de longueur variable) une chaîne de longueur fixe [Menezes et al.]

Une fonction de hashage cryptographique a les propriétés suivantes :

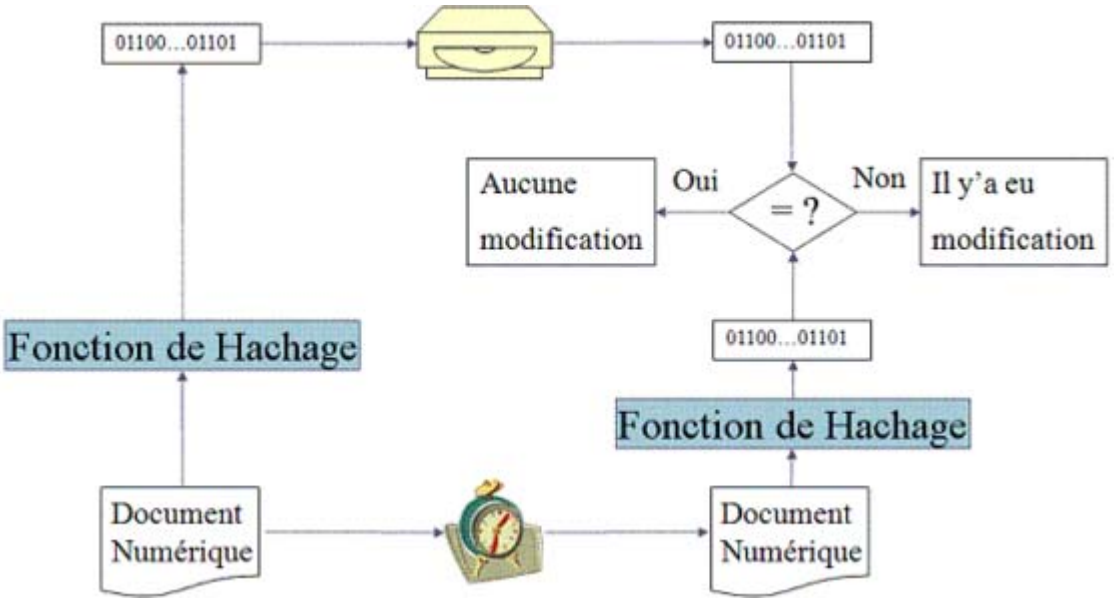
- Étant donné m, il est facile de calculer h(m)
- Étant donné h, il est difficile de calculer m tel que h(m)=h
- Étant donné m, il est difficile de trouver un autre message, m', tel que h(m)=h(m').

Méthode : Comment utiliser une fonction de hashage pour contrôler l'intégrité de données.

La figure ci-contre illustre comment utiliser une fonction de hashage pour vérifier l'intégrité d'un document numérique.

Initialement le code de hashage du document numérique est calculé et stocké dans un endroit sûre. Ultérieurement ce code est recalculé et comparé à celui qui a été stocké.

Si les deux valeurs sont égales alors le document n'a pas été modifié. Sinon, le document a subit une modification.



Intégrité de données

Exemple

Il existe plusieurs fonctions de hashages ; En voici quelques unes :

- MD2 (Message Digest 2) : Opère sur des bloques de 16 octets, manipule des mots de 8 bits Output 128 bits.
- MD4 (Message Digest 4) : Manipule des mots de 32 bits, plus performant sur des processeurs 32 bits.
- MD5 (Message Digest 5) : Une passe de plus / MD4, plus sûre
- SHA-1 (Secure Hash Algorithm) : Proposé par le NIST Input message 2^{64}

octets (au max), output 160 bits.

D. Authentification de l'origine de données

Définition : Authentification de l'origine

C'est la propriété qui permet de vérifier que la source de données est bien l'identité prétendue.

Définition : Message Authentication Code (MAC)

C'est est un mécanisme cryptographique qui permet de vérifier l'authenticité de l'origine des données et leur intégrité en même temps.

Un MAC est une famille de fonctions h_k paramétrée par une clé secrète k avec les propriétés suivantes :

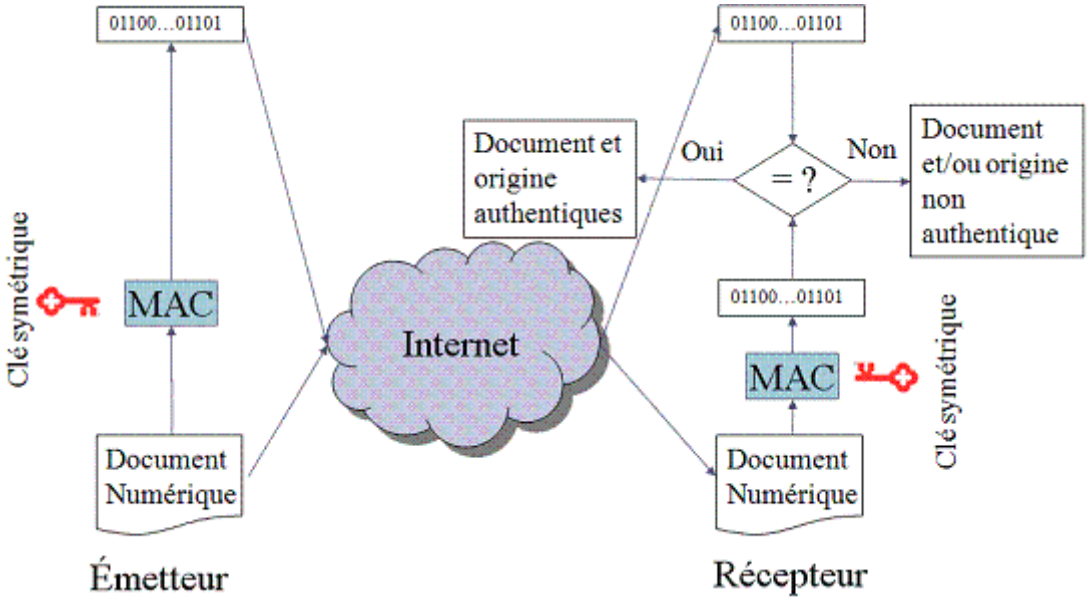
- Étant donné une clé k et un message m, $h_k(m)$ est facile à calculer,
- Étant donné zéro ou plusieurs paires $(m_j,h_k(m_j))$, il est rès difficile de calculer n'importe quelle paire $(m,h_k(m))$ pour n'importe quel message m.

Méthode : Comment utiliser un MAC pour garantir l'authentification d el'origine

Pour garantir d'authenticité de l'origine, l'émetteur et le récepteur doivent partager une clé symétrique.

Cette clé sera utilisé par l'émetteur pour calculer un MAC sur le message à envoyer. Ce MAC (code de hashage) est la preuve d'authenticité qui accompagnera le message.

Le récepteur utilisera la même clé secrète pour calculer le MAC de nouveau sur le message reçus. Le MAC nouvellement calculé sera comparé au MAC accompagnant le message. Si les deux valeurs sont égales alors le message et l'origine sont authentiques. Sinon, soit le message ou l'origine n'est pas authentique.



Authentification de l'origine

Exemple : Exemple de MAC

HMAC : Mihir Bellare, Ran Canetti, et Hugo Krawczyk 1996 FIPS PUB 198, RFC 2104

- HMAC-MD5
- HMAC-SHA-1

$$HMAC_K(m) = h\Big((K \oplus opad) \parallel h\big((K \oplus ipad) \parallel m\big)\Big)$$

opad= 0x5c5c5c...5c5c

Ipad= 0x363636...3636

Exemple de MAC : HMAC

E. Non-répudiation de l'origine

Définition : Non-répudiation de l'origine

La non répudiation de l'origine assure que l'émetteur du message ne pourra pas nier avoir émis le message dans le futur.

La signature digitale

La signature digitale est un mécanisme cryptographique qui permet d'assurer la non répudiation de l'origine.

Ce mécanisme repose sur un système cryptographique asymétrique

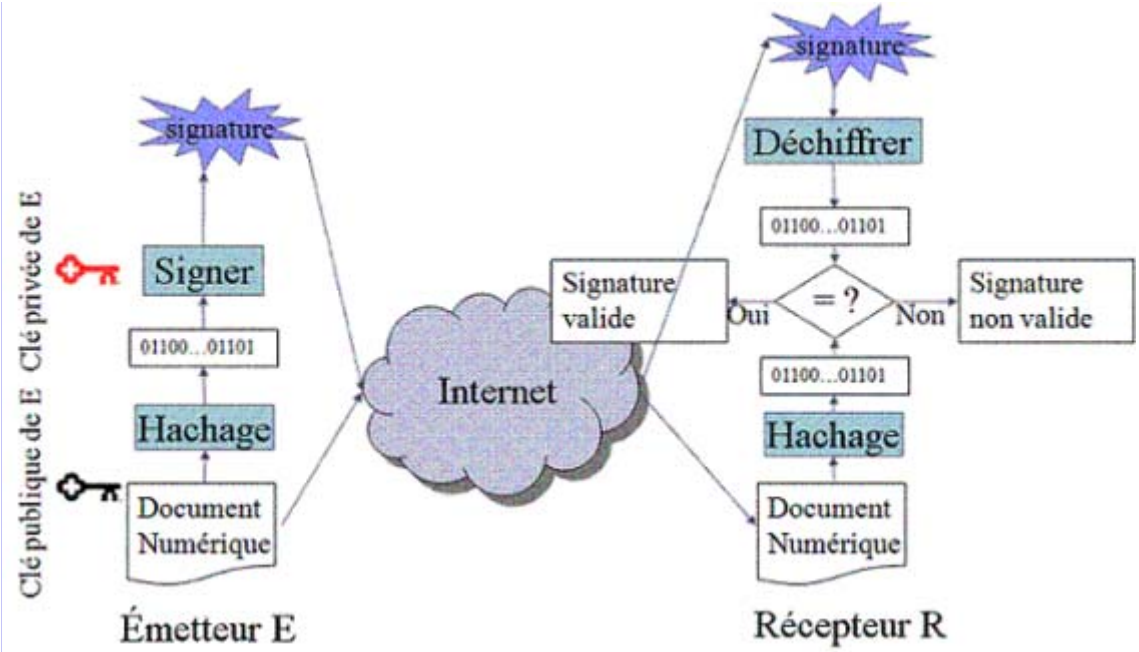
La signature est calculée en utilisant la clé privé de l'émetteur

La signature est vérifiée en utilisant la clé publique de l'émetteur

Méthode : Comment utiliser la signature digitale pour assurer la non-répudiation de l'origine ?

L'émetteur du message génère sa paire de clés (publique, privée). Il diffuse sa clé publique te maintient sa clé privée secrète. Pour signer un document l'émetteur commence par calculer le code hashage du document puis signe ce code de hashage avec sa clé privée. Le résultat de cette dernière opération (chiffrement avec clé privée dans le cas de RSA) est la signature digitale qui accompagnera le document. Quand le récepteur reçoit le message et la signature digitale, il recalcule le code de hashage, déchiffre la signature avec la clé publique de l'émetteur et compare les deux codes de hshages. Si les deux codes sont similaires alors la signature est valide.

L'émetteur ne pourra pas nier dans le futur avoir émis le message puisque y a que lui qui peut générer la signature digitale avec sa clé privée secrète.



Signature digitale et non-répudiation

F. Historiques

Quelques fais marquants de l'histoire de la cryptographie

- 50 av. JC. : Julius Cesar utilise une simple substitution de l'alphabet pour les communications gouvernementales
- 1918 : Gilbert Vernam, mathématicien américain, inventa le one-time pad, l'algorithme de chiffrement le plus sûr jusqu'à aujoud'hui, mais impratiquable
- 1923 : Dr. Albert Scherbius, hollondais résidant en Allemagne, met au point la machine Enigma qui sert à encoder des messages. Le prix très cher en fait un échec.
- 1925 : La marine de guerre allemande reprend le projet Enigma en le confiant au Chiffrierstelle, le service de chiffrement
- 1937 : Enigma M3 est adoptée par le Wehrmacht, l'armée allemande
- 1939 : début de la seconde guerre mondiale, où des milliers de scientifiques britanniques, polonais et français travaillaient pour solutionner Enigma, et les milliers de messages chiffrés. L'équipe de Alan Turing trouva la solution
- 1976 : IBM publie un algorithme de chiffrement basé sur Lucifer. Il devient le DES (Data Encryption Standard)
- 1976 : Whitfield Diffie et Martin Hellman introduisent l'idée d'un système à clé publique
- 1978 : l'algorithme de chiffrement à clé publique RSA est publié par Rivest, Shamir et Adleman
- 1978 : Le RC4 est développé par Ronald Rivest pour la RSA Security et sera gardé secret jusqu'en
- 1994, où l'algorithme est rendu public anonymement dans une liste de distribution de Cypherpunks
- 1991 : Phil Zimmermann rend disponible sa première versio de PGP
- 1992 : IDEA est inventé en Suisse par Xuejia Lai et James Massey

- 1992 : MD5 est développé par Ronald L. Rivest
- 1994 : Ron Rivest, déjà auteur de RC2 et RC4, publie RC5
- 2000 : Rijndael devient l'AES, le standard du chiffrement avancé

G. La libraire OpenSSL

Le projet OpenSSL

OpenSSL (http://www.openssl.org) est une libraire qui compte 60.000 lignes de code (langage C). Elle est utilisées par de nombreuses applications; openssh, apache+mod_ssl,... Elle est fondé sur la bibliothèque cryptographique SSLeay d'Eric Toung et Tim Hudson. L'objectif initial de cette librairie était la mise en œuvre des protocoles SSL et servir comme bibliothèque cryptographique.

La bibliothèque OpenSSL

La librairie OpenSSL en décline en deux formes :

1. Interface de programmation en C
   - Bibliothèque SSL/TLS (libssl.a)
     - Mise en œuvre des protocoles SSLv2, SSLv3, TLSv1
   - Bibliothèque cryptographique
     - Cryptographie clé publique et certificats X509: RSA, DSA, DH
     - Chiffrement: DES, 3DES, Blowfish, RC2, IDEA, RC4, + modes ECB, CBC,CFB,OFb pour les algorithmes par blocs
     - Hachage: MD2, MD4, MD5, SHA1, MDC2, RIPEMD160
2. Suite d'applications en ligne de commande openssl(1)
   - Un ensemble de commandes permettant de réaliser les différentes opérations cryptographiques

Testez vos connaissances

III

A. Chiffrement symétrique

Le chiffrement symétrique

- ☐ Garantie la confidentialité du message chiffré
- ☐ Utilise une paire de clés publique/privée
- ☐ Assure la non répudiation
- ☐ Repose sur la confidentialité de la clé utilisée
- ☐ Repose sur la confidentialité de l'algorithme de chiffrement utilisé

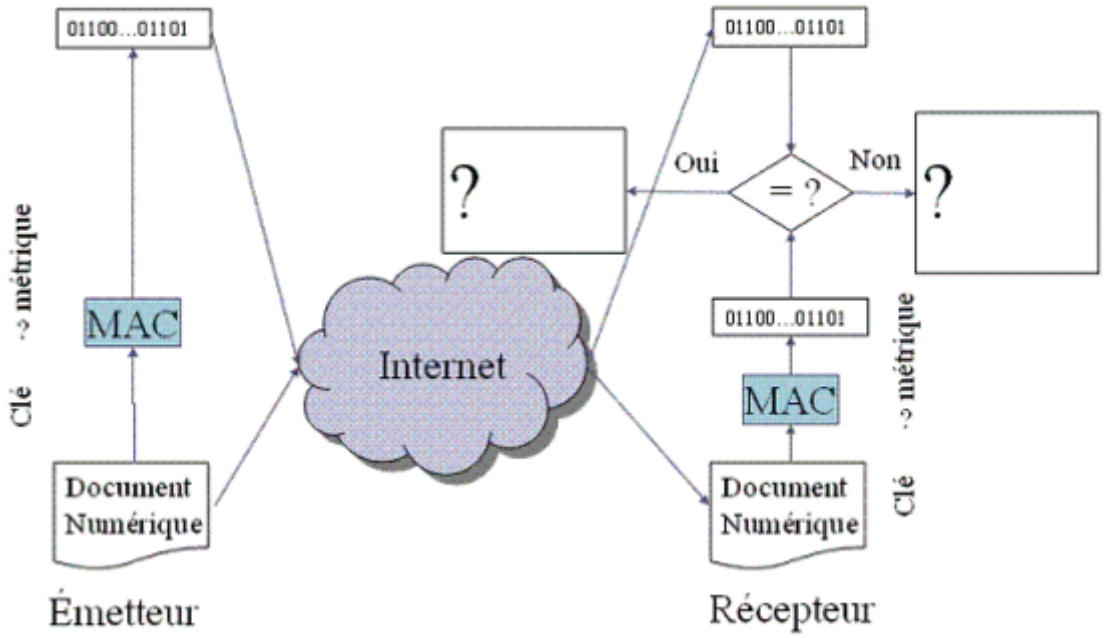
B. RSA

RSA

- ☐ Est un système cryptographique asymétrique
- ☐ Repose sur la difficulté de factoriser un grand nombre en ses facteurs premiers
- ☐ Repose sur la difficulté du logarithme discret
- ☐ Permet de faire une signature digitale
- ☐ Ne peut pas être utilisé pour assurer la confidentialité

C. Devinette ?

Ce schéma



Q3

- [ ] Assure l'authentification de l'origine
- [ ] Utilise une clé asymétrique
- [ ] Permet d'assurer l'intégrité du Document Numérique échangé
- [ ] Utilise un MAC qui est une fonction de hashage paramétrée par une clé
- [ ] Permet de signer le document pour assurer la non répudiation

D. Non-répudiation de l'origine

Pour garantir la non-répudiation de l'origine, on peut utiliser

- [ ] Un chiffrement RSA avec la clé privée de l'émetteur
- [ ] Un MAC
- [ ] Une signature digitale
- [ ] Un chiffrement RSA avec la clé publique de l'émetteur
- [ ] Un échange de clé Diffie-Hellman

Série d'exercices I: Services de sécurité et mécanismes cryptographiques

IV

A. Chiffrement Symétrique et Asymétrique

[Avoine et al. 2010]

Un groupe de n personnes souhaite utiliser un système cryptographique pour s'échanger deux à deux des informations confidentielles. Les informations échangées entre deux membres du groupe ne devront pas pouvoir être lues par un autre membre.

Le groupe décide d'utiliser un système de chiffrement symétrique

Question 1

Quel est le nombre minimal de clés symétriques nécessaires ?

Le groupe décide ensuite de remplacer ce système par un système asymétrique

Question 2

Quel est le nombre minimal de couples de clés asymétriques nécessaires pour que chaque membre puisse envoyer et recevoir des informations chiffrées et/ou signées ?

Question 3

Bob souhaite envoyer des informations chiffrées et signées à Alice. Quelles clés Bob doit-il utiliser ?

Le groupe décide finalement d'utiliser un système hybride pour le chiffrement.

Question 4

Donner les raisons qui ont poussé ce groupe à utiliser un tel système.

B. Perte d'une clé privée

[Avoine et al. 2010]

Bob qui utilise souvent la messagerie sécurisée de son entreprise, vient de perdre sa clés privée, mais dispose encore de la clé publique correspondante.

Question 1

Peut-il encore envoyer des courriers électroniques chiffrés ? En recevoir ?

Question 2

Peut-il encore signer les courriers électroniques qu'il envoie ? Vérifier les signatures des courriers électroniques qu'il reçoit ?

Question 3

Que doit-il faire pour être de nouveau capable d'effectuer toutes les opérations mentionnées ci-dessus ?

C. Conception d'un protocole d'échange sécurisé

On souhaite concevoir un protocole d'échange sécurisé. Ce protocole doit garantir les services de sécurité suivants :

- Confidentialité de l'échange
- Intégrité des données échangées
- Non-répudiation de l'émetteur

Question

On suppose que la confidentialité est assurée grâce à un chiffrement symétrique. Initialement, les deux parties communicantes ne partagent aucun secret.

Ecrire une spécification de ce protocole en utilisant la notation suivante :

- S ==> D : M (S envoie M à D)
- $\{M\}_K$: M chiffré/déchiffré avec K
- SK_X : Clé privée de X
- PK_X : Clé publique de X
- K_{AB} : Clé symétrique partagée entre A et B
- . (point) : Concaténation entre deux messages

D. Implémentation d'un protocole d'échange sécurisé avec OpenSSL

Dans cet exercice, vous allez implémenter le protocole que vous avez conçu dans l'exercice précédent en utilisant OpenSSL.

Cet atelier nécessite un jeu de rôles. Une partie (élève ou binôme) jouera le rôle de l'émetteur (source), et une autre partie jouera le rôle du récepteur (destinataire).

Pensez à inverser les rôles et refaire l'exercice.

La Source souhaite transmettre un message stocké dans un fichier message.txt à une Destination tout en assurant sa confidentialité, intégrité et non-répudiation.

Cet atelier pratique sera réalisé avec OpenSSL. Vous pouvez utiliser l'outil déjà installé dans les distribution Linux. Sous Windows, vous pouvez installer xampp qui

fournira cet outil. Dans ce cas, pensez à rajouter dans la variable d'environnement PATH le chemin vers le répertoire qui contient openssl.exe : ....xampp\apache\bin

Question

Voici ci-après des commandes openssl qui permettent de mettre en oeuvre les différentes étapes du protocole.

Pensez à analyser chaque commande avant son utilisation

La liste n'est pas exhaustive. Néanmoins, vous pouvez changer certains paramètres pour répondre aux besoins nécessaires pour mettre en œuvre votre protocole

Indice :

- *Générer la clé privée RSA de la source:* **openssl genrsa -out src_rsa.pem -passout pass:srcpasswd -des 512**

  src_rsa.pem va contenir la clé privée de la source protégée par le mot de passe srcpasswd
- *Extraction de la clé publique à partir de la clé privée vers "src_rsa_pub.pem" :* **openssl rsa -in src_rsa.pem -passin pass:srcpasswd -out src_rsa_pub.pem -pubout**

  Ici l'option -pubout permet d'extraire la clé publique (par defaut c'est la clé privée qui est extraite)

  L'option passin et passout c'est pour ptoteger les fichiers, pass:xxxx permet de faire une protection par mots de passe.
- *Chiffrer un secret avec la clé publique du destinataire :* **openssl rsautl -in secret.txt -out secret.crypt -inkey dest_rsa_pub.pem -pubin -encrypt**
- *Chiffrement d'un message avec un secret (clé symétrique) en utilisant l'algorithme DES-CBC:* **openssl enc -des-cbc -in message.txt -out message.crypt -pass file:secret.txt**
- *Calcul de condensat (code de hashage) avec MD5 :* **openssl dgst -md5 -binary -out message.crypt.dgst message.crypt**
- *Chiffrement du condensat (code de hashage) avec la clé privée de la source "src_rsa.pem" :* **openssl rsautl -in message.crypt.dgst -out message.crypt.dgst.sign -sign -inkey src_rsa.pem**
- *Déchiffrement de l'empreinte (code de hashage) du message vers dgst1 :* **openssl rsautl -in message.crypt.dgst.sign -out dgst1 -pubin -inkey src_rsa_pub.pem**
- *Déchiffrement d'un secret avec la clé privée du destinataire :* **openssl rsautl -decrypt -in secret.crypt -out secret.txt -inkey dest_rsa.pem**
- *Déchiffrement du "message.crypt" à l'aide de secret qui se trouve dans "secret.txt" :* **openssl enc -in message.crypt -out message.txt -pass file:secret.txt -d -des-cbc**