La sécurité sur les réseaux

1- Définitions et généralités
2- Le chiffrement et ses usages
3- Les fire-walls

version CNAM 1999-2000

1ère partie: Définitions et généralités

- Les réseaux sont très exposés aux risques:
  - plusieurs points de défaillances: nœuds, liaisons, etc…
  - le caractère « réparti » augmente les risques mais aussi peut les diminuer !
- Nature des risques:
  - risques passifs: ils n 'influent pas sur la structure du système:
    - confidentialité des personnes
    - vols de données, etc...
  - risques actifs:
    - brouillage d 'une émission
    - modification de données
    - la mascarade (se faire passer pour un utilisateur autorisé)
    - et tous les risques « classiques »: imprudence, incendies, dégâts des eaux, etc...

Besoins de sécurité

- Les mesures de sécurité propres aux réseaux ne se préoccupent que des actions malveillantes et des erreurs
- On distingue 4 types de besoins de sécurité:
  - la continuité du service: il s 'agit de maintenir le canal de transmission en fonctionnement, éventuellement en mode dégradé,
  - la confidentialité des informations, pour qu'elles ne tombent pas aux mains d 'un tiers non-autorisé,
  - l 'intégrité, c 'est-à-dire la certitude que l 'information n 'a pas été altérée pendant son transport,
  - l 'authentification, pour être sûr qu'émetteur et destinataire sont bien les personnes qu'elles prétendent être

R. CHALON La sécurité sur les réseaux 3

La sécurité selon l 'ISO (1/2)

- L 'ISO distingue **sept services**:
  - l 'authentification de l 'entité homologue
  - le contrôle d 'accès
  - la confidentialité des données
  - le secret des flux
  - l 'intégrité des données
  - l 'authentification de l 'origine
  - la non-répudiation, qui fait qu'un récepteur ne peut nier avoir reçu le message
- A ces services correspondent diverses combinaisons parmi **sept mécanismes** de sécurité:
  - **le chiffrement**: basé sur un codage à l 'aide de clés. Il permet la réalisation de plusieurs services: la confidentialité, l 'intégrité, et l authentification

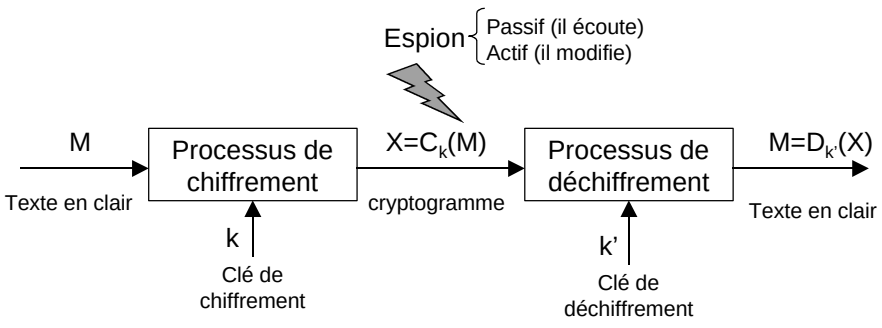
R. CHALON La sécurité sur les réseaux 4

La sécurité selon l ’ISO (2/2)

- **l ’échange d ’authentification**: si les moyens de communication sont considérés comme sûrs; l ’identification de l ’identité homologue peut être obtenue par un système de mot de passe simple ou double.
- **la signature**: permet d ’authentifier lorsque les entités ne font ni confiance à leurs homologues, ni aux moyens de communication.
- **le contrôle d ’accès**: il utilise l ’identité authentifiée des entités pour déterminer le droit d ’accès à une ressource.
- **l ’intégrité**: obtenue par des codes de détection d ’erreur, des codes de contrôle cryptographique et l ’horodatage des PDU
- **le bourrage**: Pour dissimuler les variations de trafic (qui peuvent être significatives pour un tiers) on effectue un bourrage de voie.
- **le contrôle de routage**: utilisation de routes différentes, soit après détection d ’une attaque, soit en fonction de l ’importance du trafic.

2ème partie: Le chiffrement et ses usages

- Cryptographie: conception des méthodes de chiffrement
  - Chiffrer/déchiffrer: activités de codage et décodage associées
- Cryptologie: chercher à casser les messages chiffrés
  - décrypter: décoder un message dont on a pas la clé
- Principe général du chiffrement:



Algorithme et clés

- Le chiffrement (et le déchiffrement) c 'est l 'application d 'un fonction mathématique (un algorithme) au message M paramétrée par la clé k
- L 'algorithme de chiffrement E lui-même n 'est pas secret (ce serait illusoire de penser pouvoir le garder secret!)
- La clé k, par contre, doit être changée le plus souvent possible et bien sûr être gardée secrète
- Les clés de chiffrement k et k' peuvent être identiques (algo à clés secrètes) ou différentes (algo à clés publiques)
- La complexité de décryptage d 'un message pour un espion varie avec l '**exponentielle** de la longueur de la clé

R. CHALON La sécurité sur les réseaux 7

Chiffrement par substitution

- Dans la méthode par substitution, chaque lettre (ou chaque groupe de lettres) est remplacée par une autre lettre (ou un autre groupe de lettres)
- La plus ancienne est le Jules César: *a* devient *d*, *b* devient *e*, *c* devient *f*, etc…
  - exemple: ***attaque*** devient ***dwwdtxh***
- Amélioration: au lieu de décaler de 3 lettres (ou même de n lettres) on substitue chaque lettre par une lettre quelconque
  - la clé est donc de 26 lettres et il y a donc 26! = 4.10^{26} combinaisons possibles
  - ce pendant il est facile de casser ce code en cherchant la fréquence d'apparition des lettres (e la plus fréquente, etc…) ou de groupes de 2 lettres (ch, qu, etc…) ou de 3 lettres (ion, eau, etc…)

R. CHALON La sécurité sur les réseaux 8

Chiffrement par transposition

- Dans ces méthodes c 'est l 'ordre des lettres qui est modifié (les lettres elles-mêmes n 'étant pas modifiées)
- Principe:
  - on se donne une clé
  - on range en lignes le texte en clair
  - on lit en colonnes dans l'ordre alphabétique des lettres de la clé pour obtenir le texte chiffré
- Exemple:
  - clé: BIDULE
  - **Texte en clair:**
    - `ACHETER_DEUX_MILLE_ACTIONS_DE_LA_SOCIETE_PEUGEOT`
  - **Texte chiffré:**
    - `AR__NLIEHDIC__TGEXEO_CPTC_MASAEUTULIEO_OEELTDSEE`

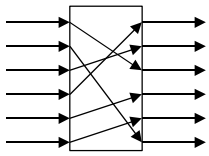
```
142653
BIDULE
ACHETE
R_DEUX
_MILLE
_ACTIO
NS_DE_
LA_SOC
IETE_P
EUGEOT
```


Chiffrement par bloc jetables

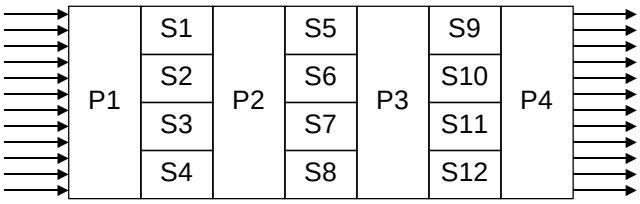
- Principe:
  - choisir une suite aléatoire de bits de longueur égale au message à coder, pour constituer la clé
  - coder le message en faisant un OU EXCLUSIF entre le message et la clé
- Avantage:
  - ce code est théoriquement incassable
- Inconvénient:
  - la clé ne peut être apprise, elle est donc écrite ce qui augmente les risques
  - la clé doit être au moins aussi longue que la totalité de tous les messages à transmettre!
  - Ce codage est très sensible à la perte de caractère qui peut produire une désynchronisation entre l'émetteur et le récepteur

Algorithmes à clés secrètes

- Principe généraux:
  - les algorithmes modernes utilisent des combinaisons des méthodes de substitution et de transposition
  - Boites-P: assurent la permutation de x bits en entrée,
  - Boites-S: assurent la substitution de mots à x bits par d 'autres
- Utilisation de successions de boîtes-P et de boîtes-S pour obtenir des algorithmes complexes:

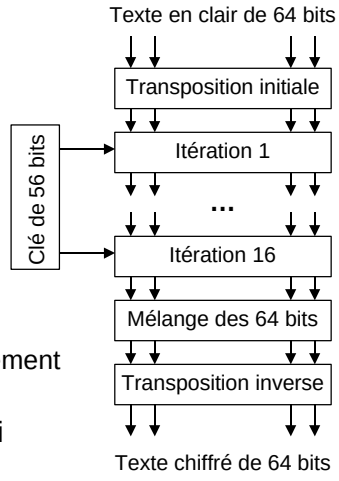


P-box



DES

- DES [Data Encryption Standard] a été inventé par IBM en 1977
- Principe:
  - le texte en clair est découpé en blocs de 64 bits
  - la clé est de 56 bits
  - 19 étapes distinctes
  - pour le déchiffrement il suffit de renverser l 'algorithme
- Problème:
  - DES est cassable car la clé est trop courte
  - amélioration avec un triple chiffrement et l 'usage de 2 clés
- DES est le plus utilisé aujourd'hui



Algorithmes à clé publique

- Le problème posé par les algorithmes à clé secrète réside dans la distribution des clés et le risque de vol de ces clés
- La solution consiste à utiliser deux clés différentes:
  - l 'une pour le chiffrement, C
  - l 'autre pour le déchiffrement, D
- Pour que ce soit efficace il faut que:
  - il soit très difficile de déduire l 'une des clés par rapport à l 'autre
  - la clé de chiffrement ne puisse être cassée par une technique de « texte en clair choisi » (essais de codage avec ses propres textes)
- Dans ces conditions, la clé de chiffrement peut très bien être rendue **publique** l 'autre clé étant tenue secrète et est appelée, **clé privée**
- Exemple: B envoie un message à A en utilisant la clé publique de A. A la réception, seul A est capable de déchiffrer le message avec sa clé privée

RSA

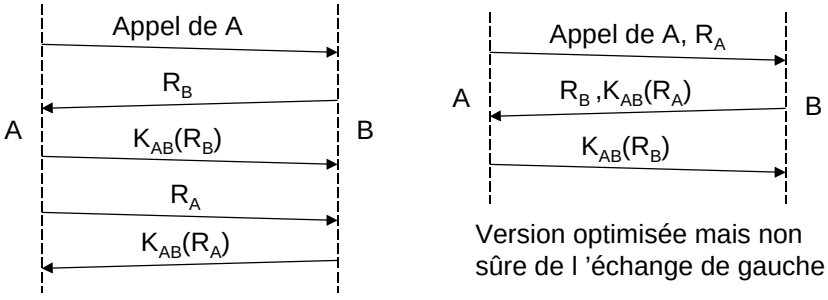
- RSA (initiales de Rivest, Shamir et Adelman, les inventeurs) a été créé en 1978 au MIT
- Calcul des clés:
  - on prend 2 nombres premiers, *p* et *q* plus grands que 10^{100}
  - on calcule n=p.q et z=(p-1).(q-1)
  - on choisit un nombre d premier avec z
  - on cherche e tel que e.d=1 (mod z)
- Chiffrement d 'un message:
  - on regroupe le texte en blocs de k bits tels que $2^k<n$, chaque bloc constituant un nombre M compris entre 0 et n
  - on chiffre chaque bloc M en calculant $X=M^e$ (mod n)
- Déchiffrement:
  - le déchiffrement s 'obtient en calculant $M=X^d$ (mod n)
- La clé publique est le couple (e,n) et la clé privée (d,n)
- RSA est trop lent. Il est très utilisé pour distribuer les clés DES!

Protocoles d ’authentification

- L ’authentification permet de s ’assurer que l ’entité distante est bien celle qu’elle prétend être et non un intrus
- les deux parties A et B qui cherchent à s ’authentifier s ’échangent des messages qui mêmes s ’il sont espionnés doivent leur permettre de s ’assurer de l ’identité de chacune
- Un tiers de confiance peut également être utilisé dans cet échange
- les deux parties peuvent également s ’entendre sur une clé de session secrète qui sera utilisée par la suite

Authentification par clé secrète partagée

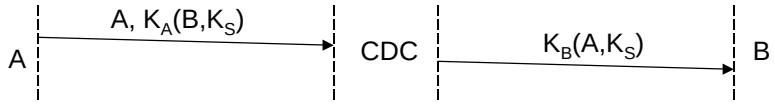
- Les deux parties A et B partagent une clé K_{AB} qu’ils se sont échangés au préalable par une méthode sûre
- Protocole question-réponse [challenge-response]:
  - un nombre assez grand est tiré au hasard par une partie et est proposé en question à l ’autre (le challenge)
  - l ’autre partie code avec KAB la question et la renvoie (response) qui peut vérifier aisément qu’il s ’agit bien de son correspondant



Version optimisée mais non sûre de l ’échange de gauche

Authentif. avec un centre de distribution de clés

- Si l 'on doit partager des clés secrètes avec tous ses interlocuteurs cela peut devenir très lourd à gérer
- Solution: utiliser un CDC (Centre de distribution de clés) en lequel on a confiance et qui gère les clés
- Principe (protocole de la grenouille à bouche béante):
  - A choisit un clé de session K_S et indique au CDC qu'il veut communiquer avec B en utilisant K_S; ce message est codé en utilisant K_A clé secrète partagée entre A et le CDC
  - le CDC code un nouveau message avec l 'identité de A et la clé K_S et code le tout avec K_B, clé secrète partagée entre le CDC et B



- Problème:
  - sensible à l 'attaque par rejeu

R. CHALON La sécurité sur les réseaux 17

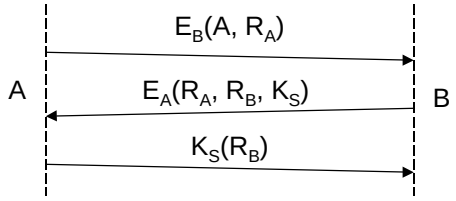
Authentification avec Kerberos

- Kerberos (Cerbère) a été développé au MIT pour permettre l 'authentification sûre de stations de travail sur un réseau
- Utilise un protocole basé sur un serveur de clé
- Utilisation d 'un horodatage des clés pour éviter tout rejeu par un intrus
- Pour se connecter une station A utilise trois serveurs:
  - SA, serveur d 'authentification
  - ST, serveur qui donne des tickets de « preuve d 'identité »
  - B, le serveur avec lequel il veut dialoguer
- Principe:
  - le SA permet d 'établir le login de l 'utilisateur sur A et d 'obtenir un ticket pour contacter ST
  - le ST permet d 'obtenir des clés de sessions K_{AB} pour se connecter au serveur B

R. CHALON La sécurité sur les réseaux 18

Authentification par chiffrement à clé publique

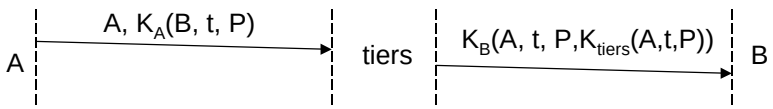
- Principe:
  - A chiffre son identité et un nombre aléatoire R_A en utilisant la clé publique de B, E_B
  - B déchiffre ce message avec sa clé privée et répond avec un message contenant R_A, un nombre aléatoire R_B qu'il génère, et une clé de session K_S, le tout chiffré avec la clé publique de A, E_A
  - A déchiffre ce message avec sa clé privée et répond en renvoyant R_B chiffré avec K_S



R. CHALON La sécurité sur les réseaux 19

Signatures numériques

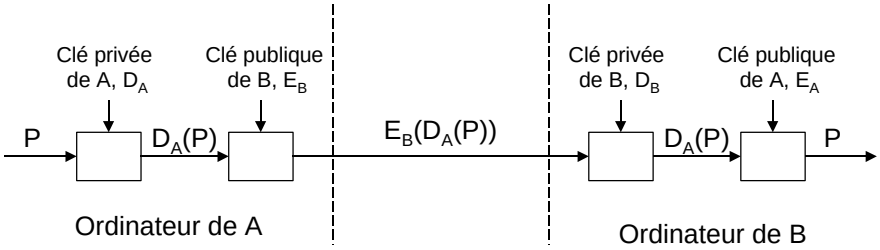
- La signature électronique d 'un document cherche à ce qu'une partie puisse envoyer un document à une autre partie de telle sorte que:
  - Le récepteur puisse vérifier l 'identité affichée par l 'émetteur
  - L 'émetteur ne puisse pas renier ensuite le contenu du message
  - Le récepteur ne puisse avoir fabriqué lui-même le message
- Signature à l 'aide de clés secrètes:
  - utilisation d 'un tiers de confiance avec qui connaît les clés secrètes de A et de B: K_A et K_B
  - Le tiers de confiance utilise sa clé privée K_{tiers} pour générer un signature $K_{tiers}(A,t,P)$



R. CHALON La sécurité sur les réseaux 20

Signatures à l ’aide de clés publiques

- Principe:
  - A utilise sa clé privée pour chiffrer le message. Puis il utilise la clé publique de B pour chiffrer le tout avant de le transmettre
  - à la réception B utilise sa clé privée pour déchiffrer le message puis la clé publique de A pour obtenir le texte en clair, ce qui prouve bien qu’il vient de A.



Résumés de message

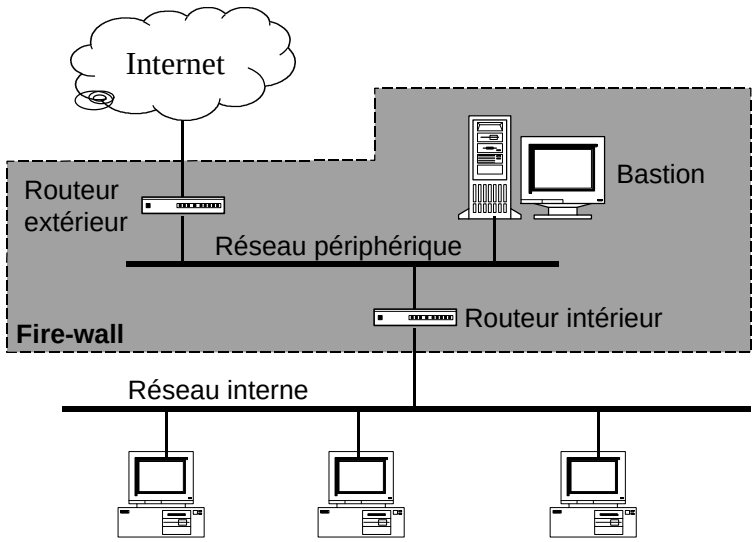
- Dans les méthodes précédentes, c ’est la totalité du message qui est chiffrée, ce qui peut être lourd si l ’on a pas besoin de confidentialité
- On peut donc calculer un résumé du message à l’aide d’une fonction de hachage bien choisie pour qu’il soit impossible de fabriquer un autre message qui ait le même résumé
- On se contente de chiffrer le résumé par une méthode à clé secrète ou à clé publique ce qui permet de gagner en performance (surtout pour de grands messages)
- Deux algorithmes sont utilisés:
  - MD5, conçu par Rivest, est surtout utilisé sur l ’Internet
  - SHA [Secure Hash Algorithm] développé par le NSA, plus sûr (mais plus lent), utilisé par les entreprises américaines

3ème partie: les fire-walls

- Les fire-walls [pare-feu] s 'intercalent entre l 'Internet et le réseau privé de l 'entreprise
- Son but est de protéger le réseau interne contre:
  - les intrusions sur les serveurs de l 'entreprise: l 'intrus va chercher à se connecter en se faisant passer pour un utilisateur autorisé
  - le refus de service: l 'intrus cherchera à vous empêcher de vous servir de vos ressources; par exemple il peut chercher à vous submerger sous un flot de messages électroniques
  - vol d 'informations: l 'intrus cherche à récupérer des informations confidentielles en général par l 'écoute passive des réseaux
- Le fire-wall est une sécurité au niveau du réseau qui doit venir **en complément** de la sécurité au niveau des hôtes (authentification des accès)

R. CHALON La sécurité sur les réseaux 23

Architecture d 'un fire-wall



R. CHALON La sécurité sur les réseaux 24

Définitions

- **Réseau périphérique** ou DMZ [De-Militarized Zone]: réseau intermédiaire entre l 'Internet et le réseau interne et sur lequel sont placé les ordinateurs accessibles depuis l 'Internet
- **Bastion**: ordinateur hautement sécurisé car il est exposé à l 'Internet et à des attaques potentielles.
- **Serveur mandataire** [proxy server]: serveur intermédiaire relayant les demandes des clients internes vers les serveurs Internet. Ainsi les clients ne sont pas directement exposés à l 'Internet. Il faut un proxy par application (FTP, Web, etc…)
- **Filtrage de paquets**: les routeurs (extérieur et intérieur) filtrent le trafic de manière à ce que le réseau périphérique communique avec l 'Internet et le réseau interne mais que la communication directe (Internet-réseau interne) soit impossible (ou seulement limitée selon le degré de sécurité souhaité)

R. CHALON La sécurité sur les réseaux 25

Filtrage de Paquets

- Le filtrage de paquet permet de vérifier d 'où proviennent les paquets et de les autoriser ou non à franchir le routeur
- Le filtrage peut agir:
  - au niveau Ethernet:
    - filtrage sur l 'adresse MAC (source et destination)
    - filtrage sur le type de paquet: IP, IPX, AppleTalk, etc...
  - au niveau IP:
    - filtrage sur l 'adresse IP source et destination
    - filtrage sur le type de protocole, TCP, UDP, ICMP
    - filtrage sur les options IP
  - au niveau TCP:
    - filtrage sur le port TCP ou UDP source et destination (et donc l 'application utilisée, Web, FTP, etc…)
    - filtrage sur les options TCP

R. CHALON La sécurité sur les réseaux 26