Les techniques de pare-feux (5)

- Les garde-barrières filtrants
  - observent tout trafic entrant/sortant
  - utilisent des tables pour déterminer ce qui est autorisé et ce qui ne l'est pas
- Avantages :
  - transparence aux utilisateurs
  - possibilité d'associer des techniques comme la traduction d'adresse (NAT - Network Address Translation)
  - connaissance fine des protocoles (FTP, par exemple)

Sécuriser les échanges de données

Echanger des données en confiance :

- **authentification** : les techniques doivent garantir l'identité de l'émetteur
- **confidentialité** : même sur des supports non sûrs (écoute), les données ne dôivent pouvoir être lues que par le destinataire
- **intégrité** : les données ne doivent pas être altérées (ajouts, suppressions, modification) pendant leur transfert
- **autres souhaits** : non répudiation : preuve d'émission, preuve de réception

Rappels sur les techniques (1)

- codage à clé secrète (exemple : DES)
  - chiffrement = algorithme dépendant d'un clé prenant en entrée un message en clair et produisant en sortie un message codé
  - déchiffrement = algorithme symétrique du premier utilisant la même clé pour transformer le message codé dans le message original
- propriétés
  - chiffrement / déchiffrement rapides
  - difficulté de reconstituer la clé même en connaissant des exemples de messages en clair et leur résultat chiffré

Rappels sur les techniques (2)

- codage à clé publique (exemple : RSA)
  - utilise deux clés, l'une, privée, pour chiffrer, l'autre, publique, pour déchiffrer
- propriétés
  - chiffrement / déchiffrement rapides
  - difficulté de reconstituer la clé privée, même en connaissant la clé publique et des exemples de messages en clair ou codés
  - particularite de RSA : commutativité. Message codé avec la clé publique ne peut être décodé qu'avec la clé privée.

Rappels sur les techniques (3)

- fonction de hashage à sens unique (exemple : MD4, MD5)
  - chiffrement = l'algorithme n'utilise pas de clé et transforme tout texte en une chaîne de longueur fixe.en sortie un message codé. Pas d'opération de déchiffrement
- propriétés
  - chiffrement rapide
  - incidence très importante de la moindre modification du texte
  - MD4 et 5 : transforment le texte en une signature de 128 bits, i.e. 8 mots de 16 bits, représentés par 32 chiffres hexadécimaux

L'utilisation de ces techniques (2)

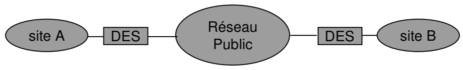
- sécuriser des connexions
  - utilisation de fonction de hashage à sens unique pour des mots de passe à usage unique (OTP = *One Time Passwords*)
  - exemple : S/Key (Bellcore)
    - utilise MD4
    - serveur : propose un défi au client
    - client : encode le défi et une clé secrète pour générer une succession desix mots anglais => c'est l'OTP
    - les mots sont pris dans un dictionnaire public de 2048 mots (2^{66} possibilités)
    - avantage : simplicité, robustesse ; inconvénients : le défi n'est pas aléatoire (défi n° *n+1* peut se déduire du défi n° *n* => mascarade possible)

L'utilisation de ces techniques (3)

- authentification, intégrité
  - utilisation d'algorithme à clé publiques ou privées + hashage à sens unique
  - exemple : RSA pour authentifier A vis à vis de B, MD5 pour la signature du message (*Message Digest*)
    - A calcule (MD5) la signature du message , puis chiffre(RSA) cette signature avec sa clé privée
    - A envoie à B le message et la signature chiffrée
    - B déchiffre (RSA) la signature avec la clé publique de A et la compare avec le calcul sur le message (MD5)
    - si égalité : le message provient de A et n'a pas été altéré

L'utilisation de ces techniques (4)

- confidentialité, authentification
  - utilisation d'algorithme à clé publiques ou privées ou bien à clé secrète
  - exemple
    - boîtiers de chiffrement DES (56 bits) ou triple-DES (= 112 bits, par codage avec clé1, décodage avec clé2, codage avec clé1):



L'utilisation de ces techniques (5)

- non répudiation => utilisation d'un tiers (notaire électronique) pour journaliser les transactions
  - A envoie au notaire le message + l'id. du destinataire (B)
  - le notaire renvoie à A le message chiffré par une clé à usage unique et un id. de transaction
  - A envoie ce message + l'id. de transaction à B
  - B envoie l'id. de transaction au notaire et reçoit la clé
  - B déchiffre le message et envoie un accusé de réception au notaire.

NB: chaque transmission est chiffrée par la clé privée de l'émetteur