Sécurité Réseau

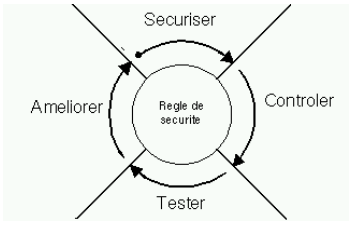
Alain AINA

AFNOG 2010

Sécurité Réseau

Sécurité Réseau

La sécurité n'est pas un produit
C'est un processus toujours actif:
Analyse -> Planification -> Implémentation -> Analyse ...



Sécurité = à 90% une bonne administration
La sécurité par l'obscurité = danger
(votre sécurité, et celles de logiciels propriétaires dont vous disposez)

Sécurité Réseau
Plan

- **Services de sécurité**
- **Filtrage**

TCP/IP, Anti-spoofing, ACLs Cisco

- **Mots de passes**

Simples, s/key ou OTP, clés, tokens physiques

- **Chiffrement**

Chiffrement à clé privée, clé publique, signature numérique et hash

- **Sécurité des machines**

Désactivation des services inutiles

- **SSH**

Utilisation et configuration

Sécurité Réseau
Elements de sécurité

- **Confidentialité**
- **Authenticité**
- **Intégrité**
- **Non-repudiation**
- **Controle d'accès**
- **Disponibilité**

- **Six services fournis par plusieurs mécanismes de sécurité utilisant pour la plupart des techniques de cryptage.**

Sécurité Réseau
Filtrage

- **Filtrage TCP**

TCP: ACK, SYN: le minimum
Aussi Window, numéro de séquence, MSS, ...

- **Systèmes de filtrages**

IPFIREWALL (IPFW), IPFilter, PF: *BSD (FreeBSD, ...)
Netfilter, IP Chains: Linux

- **Produits commerciaux**

Cisco PIX, Checkpoint FW-1

Sécurité Réseau

- **ACL cisco**

http://www.networkcomputing.com/907/907ws1.html

Configuration du filtrage: ACL

- Interface Serial0 configuration

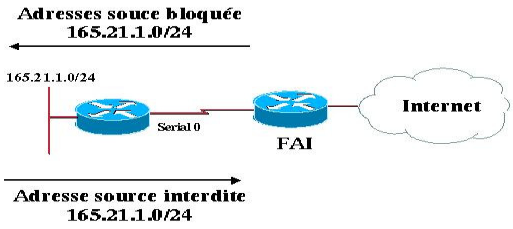
```
interface serial0
ip access-group 150 in
ip access-group 160 out

access-list 150 deny   ip 165.21.1.0 0.0.0.255 any
access-list 150 permit ip any any
access-list 160 permit ip 165.21.1.0 0.0.0.255 any
access-list 160 deny   ip any any
```

Sécurité Réseau

- **Anti-spoofing**

Filtrage: anti-spoofing



Sécurité Réseau

- **Protection contre les dénis de service**

no ip directed-broadcast

Sécurité Réseau

- **Limitation de débit**

Exemple de limitation du trafic

- Limitation du trafic ICMP à 256 kbps

```
! Trafic à limiter
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any echo-reply
! Configuration de l'interface au bord
interface Serial0
rate-limit input access-group 102 256000 8000
8000 conform-action transmit exceed-action drop
```

Sécurité Réseau
Mots de passe

- **Mots de passe**

Mots de clés simples

Danger avec Telnet, HTTP, ...

- **s/key ou OTP**

Génération à partir d'un numéro de séquence (seed) et d'une clé secrète -- pas de danger de compromission

- **clés**

RSA (SSH), X.509, ... -- la clé réside sur un portable ou une disquette, elle est chiffrée. Avantage: aucun mot de passe n'est transmis.

- **Tokens physiques**

SecureID (propriétaire, non documenté), Secure Net Key

Sécurité Réseau
Chiffrement

- **Chiffrement symétrique**

DES, Triple DES, AES

- **Chiffrement à clé publique / clé privée**

RSA

Sécurité Réseau

- **Principes du chiffrement**

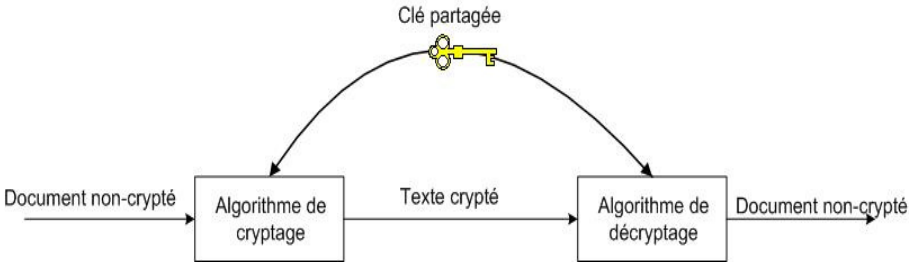
- **Chiffrement symétrique**

Un clé sert à chiffrer et à déchiffrer
Problème: comment transmettre la clé de manière sûre ?

- **Chiffrement à clé publique**

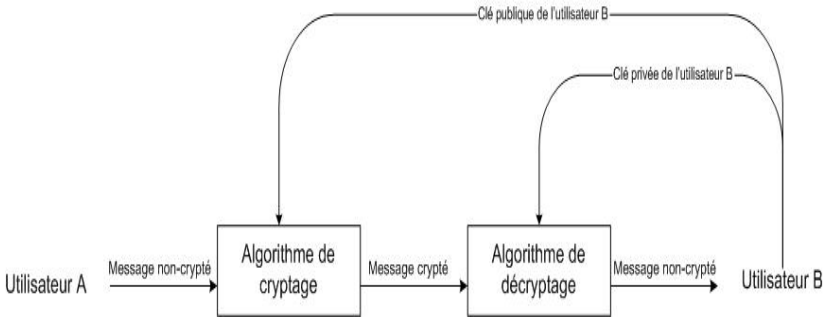
Clé composé d'une partie publique et une privée
Utilisation des propriétés des nombres premiers
On chiffre avec la clé publique, on déchiffre avec la clé privée

Sécurité Réseau



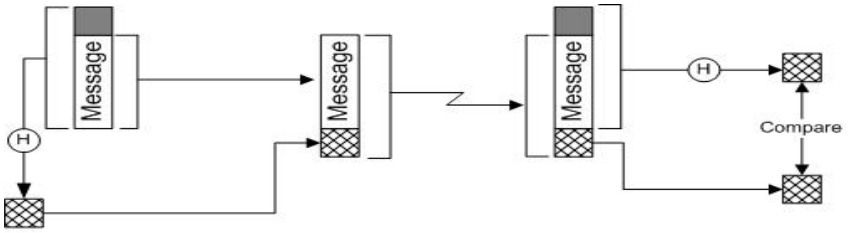
Cryptage conventionnelle

Sécurité Réseau



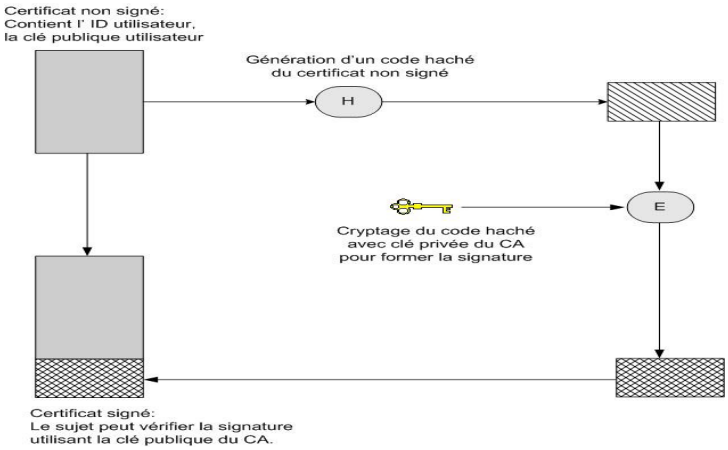
Cryptage asymetrique

Sécurité Réseau



Authentification de message avec du MD5, SHA ou RIPEMD-160 et valeur secrète

Sécurité Réseau



Identité numérique

Sécurité Réseau
Sécurité des machines

Durcissement (hardening)

- **Supprimer les services inutiles**
  - netstat -an | egrep '(tcp|udp)'
  - FreeBSD: sockstat
- **Filtrer si nécessaire**
- **Mise à jour des logiciels qui parlent au réseau**
  Sendmail, pop, imap, ...

Sécurité Réseau
SSH (serveurs et Cisco

- **SSH (serveurs et Cisco)**

http://www.institut.math.jussieu.fr/~jma/cours/cours.ssh.txt
Serveur: sshd
Client: ssh, scp

Utilisation:

- **ssh [utilisateur@]machine**
- **scp [utilisateur@]machine:/chemin/ficher /chemin/local**
- **scp /chemin/local [utilisateur@]machine:/chemin/ficher**

Sécurité Réseau
SSH (serveurs et Cisco)

- Fournit un bon cryptage,authentification des machines et des utilisateurs et l'int**é**grit**é** des données
  - Mot de passe !!!!!
  - Par cl**é** publique (RSA,DSA...)
  - KERBEROS etc.....
- La méthode d'**échange** des clés, l'algorithme a cl**é** publique,l'algorithme de cryptage conventionnelle, l'algorithme de MAC sont tous négociés.
- Disponible sur plusieurs OS.

Filtres de paquets en entrée sur les routeurs de frontière ISP

```
access-list 100 deny ip 221.19.0.0 0.0.31.255 any**
access-list 100 deny ip 0.0.0.0 255.255.255.255 any
access-list 100 deny ip 10.0.0.0 0.255.255.255 any
access-list 100 deny ip 127.0.0.0 0.255.255.255 any
access-list 100 deny ip 169.254.0.0 0.0.255.255 any
access-list 100 deny ip 172.16.0.0 0.0.255.255 any
access-list 100 deny ip 192.0.2.0 0.0.0.255 any
access-list 100 deny ip 192.168.0.0 0.0.255.255 any
access-list 100 permit ip any any
```

** l'ISP a le bloc d'adresse 221.19.0.0/19

Filtres de paquets en sortie sur les routeurs de frontière ISP

```
access-list 110 deny ip 0.0.0.0 255.255.255.255 any
access-list 110 deny ip 10.0.0.0 0.255.255.255 any
access-list 110 deny ip 127.0.0.0 0.255.255.255 any
access-list 110 deny ip 169.254.0.0 0.0.255.255 any
access-list 110 deny ip 172.16.0.0 0.0.255.255 any
access-list 110 deny ip 192.0.2.0 0.0.0.255 any
access-list 110 deny ip 192.168.0.0 0.0.255.255 any
access-list 110 permit ip any any
```

Filtrage sur routeur client

```
access-list 100 deny ip 221.4.0.0 0.0.31.255 any
access-list 100 permit icmp any any
access-list 100 permit tcp any any established
access-list 100 permit tcp any any eq 22
access-list 100 permit tcp any host 221.4.0.1 eq www
access-list 100 permit tcp any host 221.4.0.2 eq smtp
access-list 100 permit tcp any host 221.4.0.3 eq domain
access-list 100 permit udp any host 221.4.0.3 eq domain
access-list 100 permit udp any any eq ntp
access-list 100 deny udp any any eq 2049
access-list 100 permit udp any any gt 1023
access-list 100 deny ip  any any log

access-list 101 permit ip 221.4.0.0 0.0.3.255 any
access-list 101 deny ip any any log

Interface serial0/0
ip access-group 100 in
ip access-group 101 out
```

Bonnes pratiques

Mettez a jour régulièrement les OS(routeurs,switch, firewall....)
Limiter et contrôler l'accès a vos routeurs, switch et firewall...)
Sécuriser le routage (authentifier les échanges)
Toujours du ssh ou IPsec. Jamais du simple telnet
Filtrer, filtrer, filtrer
Tenez des statistiques de votre réseau
Suivez les informations des CERT (www.cert.org)
Abonnez-vous aux listes de discussions des NOG (AfNOG,NANOG)
Ne jamais paniquer

A lire

http://www.nanog.org/ispsecurity.html
http://www.ietf.org/internet-drafts/draft-jones-opsec-06.txt
CISCO ISP Essentials