Sécurité et TCP IP

Réseau Avancé

Novembre 2007

1- Introduction
Objectifs

- ***Définir la notion de sécurité et les termes qui y sont reliés***
- ***Connaître des sites et trouver de l'information pour une veille active et efficace***
- ***Connaître les failles de TCP/IP les plus utilisées***
- ***Savoir auditer la sécurité***

Les enjeux de la Sécurité

- *Le système d'information doit être disponible en permanence, toute entreprise de nos jours dépend de cette disponibilité. Sans système d'information, l'information n'est généralement pas ou peu utilisable.*
- *La sécurité est devenue une activité informatique à part entière.*
  - *Tout informaticien, quelque soit son rôle, ne peut ignorer les menaces que représentent les multiples et nombreuses tentatives d'accès non autorisés que subissent en permanence les systèmes d'information.*
- *Différencier la notion de système d'information de système informatique:*
  - *Système d'information = Ensemble des actifs informationnels*
  - *Système informatique = Restriction aux éléments traitant des données informatisées*
- *Un rôle important: le responsable de la sécurité du système d'information (RSSI)*

Le Responsable de la Sécurité du Système d'Information

- *Il peut être rattaché directement au directoire d'un compagnie ou dépendre du Directeur du Système d'Information (Chief Information Officer)*
- *Le RSSI assure un rôle de conseil, d'assistance, d'information, de formation et d'alerte.*
- *Il effectue un travail de veille technologique et réglementaire sur son domaine*
- *Il propose des évolutions pour garantir la sécurité logique et physique du système d'information* ***dans son ensemble****.*

Définition de la Sécurité

Suivant le cœur de métier (Core Business) d'une entreprise,la sécurité informatique peut regrouper les besoins suivants :

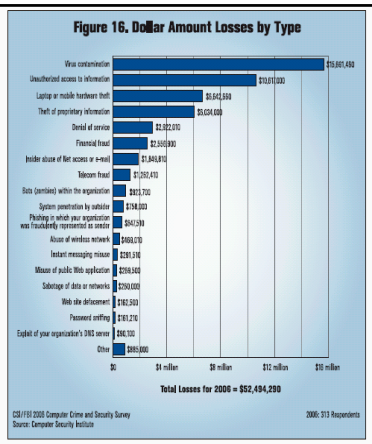
- *La confidentialité :*
  - *L'authentification, les contrôles d'accès.*
- *La disponibilité du système d'information*
- *L'intégrité du système d'information*
- *La non répudiation ou la traçabilité des traitements:*
  - *Non répudiation = garantir qu'une opération est bien le fait de son auteur.*
  - *Traçabilité = pouvoir connaître qui ou quel traitement est intervenu sur une donnée*

La sécurité est globale

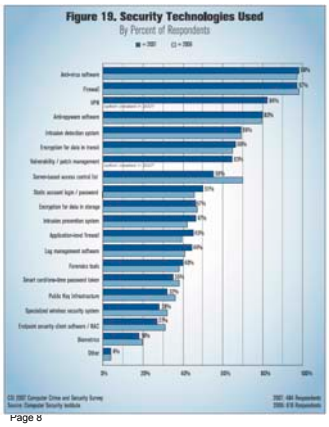
- *Sécurité des réseaux :*
  - *technologie s'appliquant à tous les niveaux d'un système informatique => systémique*
  - *matériel, réseau, système d'exploitation, logiciel, utilisateur…*
    - *toutes les composantes doivent être sécurisées*
- *Niveau de sécurité est proportionnel au niveau de sécurité du maillon le plus faible*
- *Niveau de sécurité est inversement proportionnel à la facilité d'utilisation*
- *Sécurité égale gestion du risque égale « pas une technologie, mais un processus »*

La sécurité doit être vue comme un processus de sécurisation

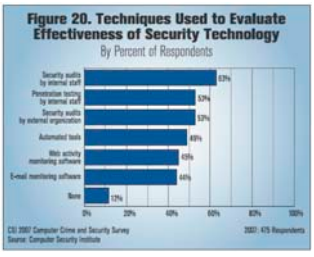
Source: 2007 CSI/FBI Computer Crime and Security Survey



•**Source: 2007 CSI/FBI Computer Crime and Security Survey**



Les technologies de remédiation employées



Les statistiques du Computer Emergency Response Team (CERT)

- CERT http://www.cert.org/stats

Vulnerabilities reported

1995-1999

Année	*1995*	*1996*	*1997*	*1998*	*1999 **
Vulnérabilités	*171*	*345*	*311*	*262*	*417*

2000-2003

Année	*2000*	*2001*	*2002*	*2003*
vulnérabilités	*1090*	*2437*	*4129*	*3784*

2004: ***3780*** **2005 :** ***5990*** **2006:*****8064***

La terminologie de la sécurité

Quelques définitions de termes reliés à la sécurité

- *Hacker:*
  - *bidouilleur en anglais est un expert dans son domaine. Le mot hacker est utilisé pour designer une personne maîtrisant totalement l'art de la programmation et la connaissance détaillée des systèmes.*
- *Cracker:*
  - *Le **cracker** (**craqueur** ou **casseur**) est une personne dont le passe-temps est de craquer (casser) les sécurités des logiciels, notamment les partagiciels (qui nécessitent des clés d'enregistrement).*

Black/White Hats

- *Les hackers se divisent communément en deux catégories : les **black hats** et les **white hats**.*
  - *Black Hats:Cherchent des vulnérabilités ou des cracks pour pénétrer un système et/ou l'utiliser à des fins illégales.*
  - *White Hats: Cherchent des vulnérabilités et préviennent la communauté des experts en sécurité ou les vendeurs de logiciels des problèmes découverts.*

Autres définitions

- ***Le Crasher Informatique :***
  - ➲ *Le **crasher** appartient à la famille des hackeurs. C'est un pirate informatique qui efface les données "pour le plaisir", sans pour autant en vouloir à la victime qui est le plus souvent choisie au hasard.*
- ***Script Kidies:***
  - *En informatique, **script kiddie** est un terme péjoratif pour désigner un pirate qui utilise des programmes qu'il n'a pas créés lui-même.*
  - *Les script kiddies, bien que ne possédant pas de compétences informatiques particulières, peuvent causer des dégâts assez importants.*
- ***Phreakers:***
  - *Un **phreaker** est un expert en adaptation des lignes téléphoniques, principalement pour donner des appels gratuitement ou anonymement.*

Les failles les plus courantes
Les 14 principales vulnérabilités selon « Halte aux Hackers »

1. *Routeur mal configuré permettant la fuite d'informations ICMP, netbios …*
2. *Accès à distance mal protégés*
3. *Informations visibles de l'extérieur fournis par les services comme DNS, SMTP, finger, SNMP, netbios, telnet …*
4. *Services visibles et inutiles comme DNS, SMTP, FTP, RPC*
5. *Mots de passe trop simples, répétés sur plusieurs machines par « simplification »*
6. *Comptes d'utilisateurs ou de services avec des droits excessifs.*
7. *Serveurs WEB ou FTP permettant d'obtenir des droits supplémentaire sur le serveur hôte comme ASP, CGI*
8. *Un pare-feu (firewall) mal configuré permettant un accès direct au réseau interne ou en utilisant un serveur de la zone protégée (DMZ).*
9. *Logiciels utilisés avec la configuration par défaut et sans mise à jour.*
10. *Droits et accès trop laxistes aux fichiers et répertoires via des partages comme NFS ou Windows.*
11. *Des relations de confiance trop laxistes entre machines permettant un accès non autorisé.*
12. *Utiliser un service non sécurisé et sans authentification (XWindow).*
13. *Capacité de détection, de surveillance et d'établissement de connections inappropriés au niveau du réseau et/ou de l'hôte.*
14. *Absences de règles, procédures, directives de sécurité bien diffusées, acceptées et comprises par le personnel.*

Comment se protéger: vue rapide
Avec des outils

- *Outil de détection des 20 principales vulnérabilités du SANS Qualys https://sans20.qualys.com/*
- *Nessus est un outil de détection de vulnérabilité gratuit.*
  - *Nessus est utilisable sur toutes les plateformes Linux/Unix et Windows.*
- *Antivirus*
- *Anti-adware*

  http://www.securitepublique.gc.ca/prg/em/ccirc/index-fra.aspx

Comment se protéger: vue rapide 2
Avec des méthodes

- ***Machine très exposée***
  - *(serveur accessible par Internet/Intranet/Extranet)*
  - *Installation minimale !*
  - *Pas de systèmes d'exploitation non sécurisée !*
  - *Installation sécurisée des programmes sensibles.*
  - *Mise en place de correctifs de durcissement (protection contre l'administrateur!).*
  - *Supprimer les programmes non utiles après installation.*
  - *Mise à jour immédiate après avertissement de sécurité.*
  - *Contrôle fréquent, idéalement par un système externe.*

Comment se protéger: vue rapide 3
Avec des méthodes

- ***Machine sensible***
  - *(serveur central, base de données, serveur applicatif)*
  - *Installation minimaliste (préférable).*
  - *Protection renforcée autour des applications sensibles (SGBD, WEB).*
  - *Installation sécurisée des programmes sensibles.*
  - *Mise à jour immédiate après avertissement de sécurité.*
  - *Contrôle fréquent, idéalement par un système externe.*
- ***Machine de bureau***
  - *Politique de sécurité lue, commentée, analysée, comprise !!!*
  - *Voir section anti virus dans les pages précédentes.*
  - *Si besoin limiter les fonctionnalités pour interdire ce qui est potentiellement dangereux.*

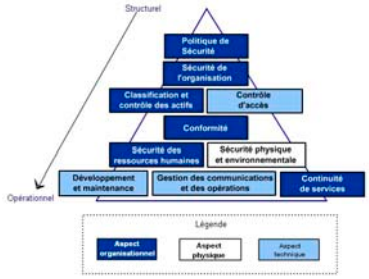
Politique de sécurité

- *Nécessaire pour protéger le système d'information*
- *4 objectifs principaux*
  - *L'intégrité*
  - *La confidentialité*
  - *La disponibilité*
  - *La non répudiation*
- *Mise en place*
  - *Tous les acteurs sont concernés !*
- *Attention aux maillons « faibles »*

Politique de sécurité 2

- *Approche globale*
  - *Sécurité physique*
  - *Sécurité logique*
  - *Sécurité des applications*
  - *Sécurité physique*
    - ➲*S'assurer que tous les utilisateurs y participent.*

Politique de sécurité 3: ISO 27001



Audit, pratiques, tests, le suivi de la sécurité

- *Nécessaire pour assurer la continuité de la protection du système d'information.*
  - *Pratiquer régulièrement une évaluation de la sécurité Internet.*
  - *Utiliser des outils d'audits.*
  - *Obtenir la possibilité de pratiquer les audits.*
- *Assurer le suivi de la sécurité*
  - *Être abonné à plusieurs listes de diffusions consacrées à la sécurité informatique.*
  - *Faire les mises à jour recommandées régulièrement.*
- *Avoir un plan de récupération*
  - *Rédiger un plan de récupération.*
  - *Pratiquer le plan de récupération (exercice incendie!).*

Résumé

- *La sécurité est un processus global, attention au maillon faible !*
- *Un hacker est un programmeur expert.*
- *Un cracker enlève les protections des logiciels.*
- *Un crasher, un script kiddie et autres black hats est un individu ou un groupe nuisible qui détruit les systèmes qui tombe sous ses « coups ».*
- *Les failles les plus courantes; 14 selon « halte aux hackers » 20 selon le SANS institute*
- *Se protéger, rapidement …*
- *Établir une politique de sécurité même simpliste est une nécessité.*
- *Le suivi de la sécurité est important ! Audits, mise en situation, exercices doivent faire partie des tâches de maintenance du système d'information.*

La sécurité c'est avant tout : LA GESTION DU RISQUE

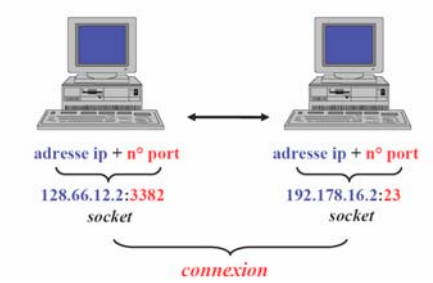
-2- Rappel TCP/IP

- ***Objectifs***
  - ***Voir un rappel du modèle TCP/IP, du modèle OSI, les différences …***
  - ***Voir un rappel du protocole IP***
  - ***Voir un rappel du protocole TCP***
  - ***Voir un rappel de ICMP le rôle de HTTP, la messagerie***

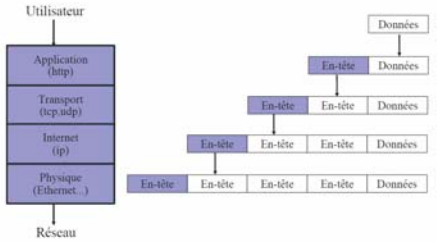
Historique

- *1969: la DARP (Defense Advanced Research Agensy) commande le développement d'un réseau de communication destiné à:*
  - *Résister à une attaque nucléaire*
  - *Fonctionnement de la manière la plus autonome*
- *Les Principes de base:*
  - *Mode client serveur et intéropérabilité*
- *Les protocoles TCP (RFC795) et IP (RFC 791) sont finalisés en 1980 dans un environnement sur => pas de sécurisation des échanges*

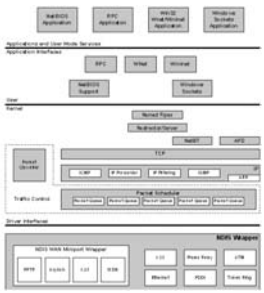
Rappel des principes de fonctionnement



L'encapsulation



Implémentation de TCP/IP avec Microsoft Windows Server 2003



- **http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/networking/tcpip03.mspx**

La couche physique

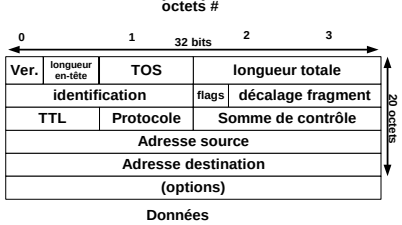
- *Protocoles:*
  - *Ethernet,*
  - *PPP,*
  - *Frame Relay*
  - *ADSL*
  - *Docsis (Cable Modem)*
  - *Wifi*

Protocoles IP

- *IP sert à interconnecter des réseaux indépendants*
  - *Caractéristiques*
    - ➲ *possibilité de segmentation et de réassemblage*
    - ➲ *mode datagramme sans garantie d'acheminement et de séquencement*
    - ➲ *Détection d'erreurs mais pas de correction*
    - ➲ *Contrôle de flux (limité), destruction des datagrammes en cas de manque de ressource dans les noeuds ou si durée de vie trop longue*
    - ➲ *Possibilité de connaître les chemins suivis et de choisir un chemin particulier*
    - ➲ *Possibilité de donner des niveaux de priorité aux datagrammes*

Rappel sur IP

- *Structure d'un paquet IP*



Rappel sur IP

- *Version*
  - *Version du protocole, = 4 pour IPv4*
- *Longueur en-tête*
  - *Longueur en multiple de 32 bits ; normalement = 5*
- *TOS*
  - Type Of Service*.*
- *Longueur totale*
- *Identification*
  - *Identifie uniquement chaque datagramme envoyé*

Rappel sur IP

- *Flags (3 bits)*
  - *Bit 0: réservé, doit être laissé à zéro*
  - *Bit 1: (AF) 0 = Fragmentation possible, 1 = Non fractionnable.*
  - *Bit 2: (DF) 0 = Dernier fragment, 1 = Fragment intermédiaire.*

```
0   1   2
|   | A| D |
| 0 | F | F |
```

- *Décalage fragment*
  - *Position de ce fragment relatif au début du datagramme original*
- *TTL*
  - Time To Live*. Compteur décrémenté par chaque aiguilleur traversé*
- *Protocole*
  - *Type de protocole dans le datagramme IP*

Rappel sur IP

- *Somme de contrôle*
  - *Somme de contrôle de l'en-tête IP*
- *Options*
  - *Optionnel, rarement utilisé*

Rappel sur IP

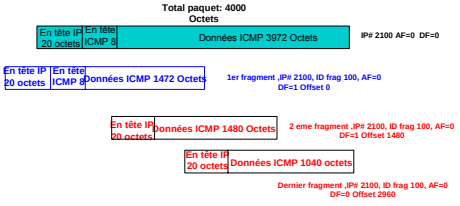
- *Options: route à suivre*
  - *Options source routing:*
    - ➲*Loose Source Routing: spécifier de 1 à 8 aiguilleurs vers la destination*
    - ➲*Strict Source Routing: spécifier le chemin exact (8 aiguilleurs maximum) vers la destination*
  - *Option Record Route: Chaque routeur inscrit son @ip dans le paquet*

La fragmentation

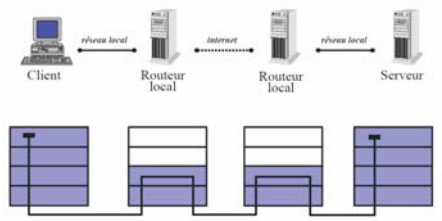
- *Selon la norme un paquet IP peut avoir une longueur de 65535 octets.*
- *En général les stack TCP/IP ne créent pas des paquets > 4000 octets.*
- *Le Maximum Transmit Unit (MTU) d 'un réseau décrit la longueur maximale admissible par un réseau IP sur un réseau donné.*

La fragmentation

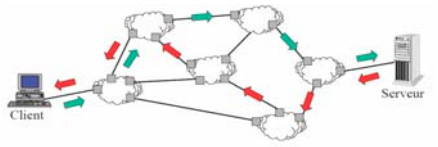
- *Exemple de Fragmentation: Soit un paquet ICMP de 4000 octets et un MTU de 1500 octets.*



Le routage IP

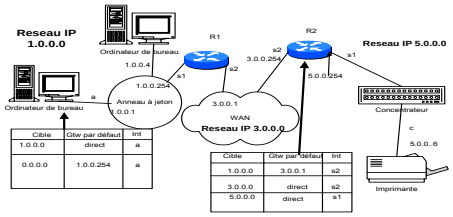


Le routage IP



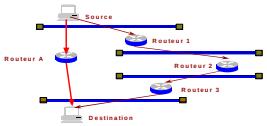
- *Les aiguilleurs choisissent le meilleur chemin à chaque paquet reçu*
- *Les hôtes ne déterminent pas le chemin à prendre (exception: option Source Routing)*

Le routage IP



Routage RIP

- *Exemple de protocole de routage RIP V1 (Routing Information Protocol)*
- *2 routes possibles*
  - *S->R1->R2->R3->D*
  - *S->A->D*
- *RIP choisira le nombre de sauts (hops) le plus courts avec un maximum de 15*



ICMP

- *Contrôle de flux*
- *Détection des réseaux, hôtes et ports inaccessibles*
- *Redirection des routes*

Sécuriser ICMP?

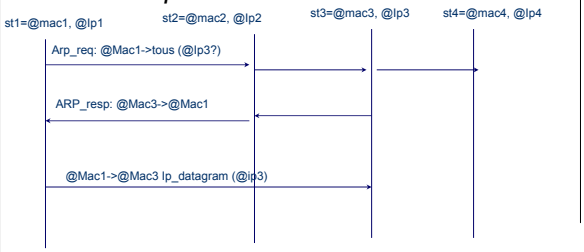
- *Comment sécuriser :*
  - *passerelle de sécurité (filtrage)*
  - *Routeurs (répondre à Ping?)*
  - *Réserver aux serveurs publics depuis l'internet*
- *Limiter le plus possible son utilisation*
  - *Mais a des conséquences pour les usagers*
    - ➲ ***traceroute***
    - ➲ ***ping***
  - *Et pour le protocole*
    - ➲ *Path MTU discovery*

Protocoles ARP et RARP

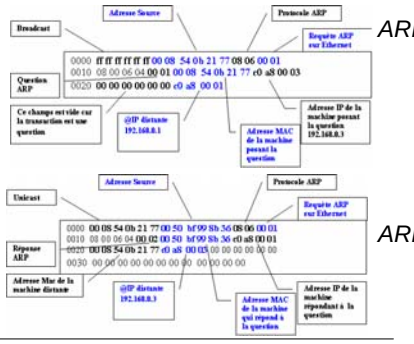
- *Problème*
  - *Les hôtes connaissent l'adresse de réseau de leur destination mais ignorent les adresses de couches 2 (MAC) pour les atteindre et construire les trames Ethernet. C'est à ARP et RARP de les aider à les découvrir.*
    - ➲*Cette correspondance est alors mémorisée dans la table ARP des hôtes.*

Protocoles ARP et RARP

- *Cinématique de ARP*



Les requêtes ARP



ARP Request

ARP Reply

Protocoles ARP et RARP: exemples

- *Pour afficher les tables du cache ARP de toutes les interfaces,* ***arp –a***
- *Pour afficher la table du cache ARP de l'interface dont l'adresse IP est 10.0.0.99,* ***arp -a -N 10.0.0.99***
- *Pour ajouter dans le cache ARP une entrée statique qui résout l'adresse IP 10.0.0.80 en l'adresse physique 00-AA-00-4F-2A-9C* ***arp -s 10.0.0.80 00-AA-00-4F-2A-9C***

Protocoles ARP et RARP (suite)

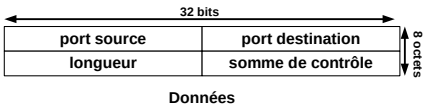
- *Le protocole RARP a la cinématique inverse. Il permet de trouver l'adresse IP quand on connaît l'adresse MAC du destinataire.*
- *Il sert par exemple à demander à un serveur BOOTP ou DHCP (Dynamic Host Control Protocol) l'attribution d'une adresse IP.*

UDP

- *Protocole sans connexion*
- *N'offre aucune fiabilité*
- *Une connexion UDP/IP est caractérisée par le quadruplet adresses et numéros de port*
  - *Adresse IP source*
  - *Numéro de port de la source*
  - *Adresse IP destination*
  - *Numéro de port de la destination*

UDP

- *UDP :* User Datagram Protocol
- *Structure d'un paquet UDP*



UDP

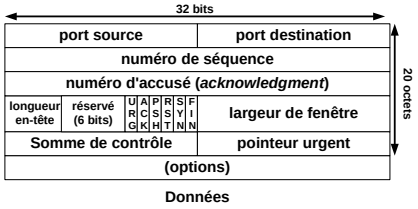
- *Port source*
- *Port destination*
- *Longueur*
  - *longueur de l'en-tête UDP + les données*
- *Somme de contrôle*
  - *effectuée sur l'en-tête UDP et les données*

TCP

- *Protocole avec connexion*
- *Un circuit doit être établi avant la transmission de données*
- *Une connexion TCP/IP est caractérisée par un quadruplet*

TCP

- *Structure d'un paquet TCP*

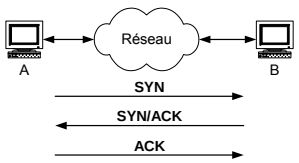


TCP

- *Numéro de séquence*
  - *Identifie un flux de données*
  - *Nombre aléatoire initialement et incrémentation à chaque transmission*
- *Numéro d'accusé (*acknowledgment*)*
  - *Utilisé lorsqu'une connexion est établie.*

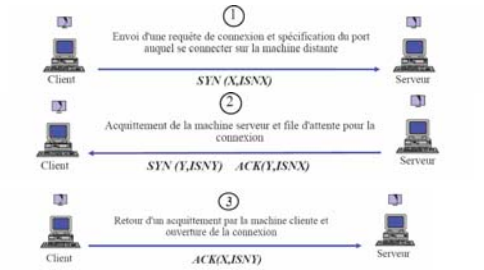
TCP

- *Établissement d'une connexion TCP/IP*



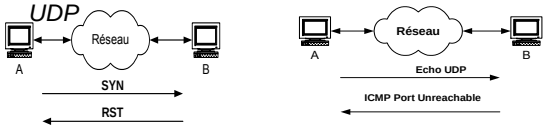
Les paquets suivants auront le drapeau ACK = 1

Établissement d'une connexion TCP/IP



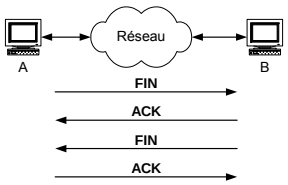
Refus d'une connexion

- *Refus d'une connexion TCP et d'un flux UDP*

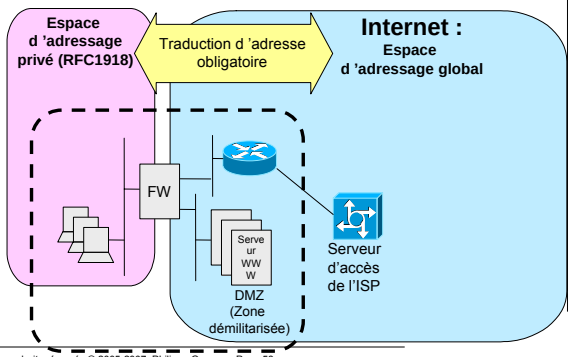


TCP

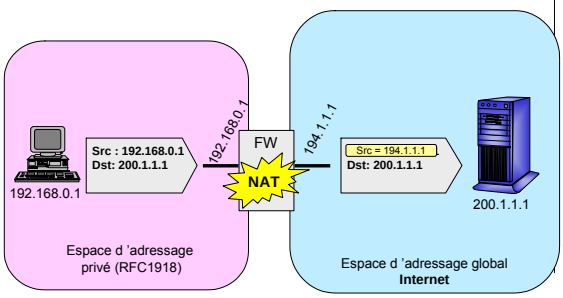
- *Fermeture d'une connexion TCP/IP*



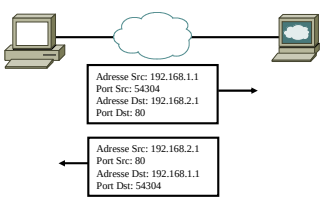
adressage: adresses privées



adressage: NAT



Connexion HTTP



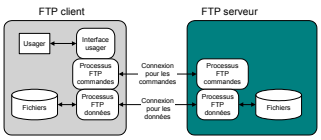
Le protocole HTTP sert de « transporteur »

- *Pour contourner les politiques de sécurité empêchant UDP (et d'autres protocoles : IRC…),*
  - *beaucoup de produits et protocoles utilisent HTTP comme protocole de transport*
  - *ce qui réduit au minimum la capacité de filtrer des passerelles; elles deviennent aveugles*
  - *Finalement, tous les « trous » d'une passerelle ou d'un pare-feu peuvent servir !*
- *Tous les protocoles qui imposent une « ouverture » dans le parefeu (intentionnelle ou imposée) peuvent, bien évidemment, servir à « transporter » des attaques de tout type.*

Le cas particulier de FTP

- ***Port source choisi par le serveur***
  - *FTP utilise un port de contrôle pour négocier les informations entre le client et le serveur*
  - *Par défaut, le serveur FTP choisit le port source*
- *Les passerelles doivent donc avoir un module spécial pour traiter ce cas et écouter la session de contrôle*
- *Le mode passif permet au client de choisir le port source*
- *Beaucoup d'autres protocoles utilisent des ports dynamiques, des ports de rendez-vous, etc. pour leurs connexions*
  - *Les passerelles doivent avoir des modules spéciaux pour chacun d'eux, de manière à écouter les sessions de contrôle*
  - *Si la session de contrôle est chiffrée de bout en bout, alors la passerelle ne peut pas écouter*

FTP normal



Résumé du chapitre 2

- *Le modèle TCP/IP à été conçu dans les années 70.*
- *Le modèle TCP/IP comporte 4 couches vs les 7 couches du modèle OSI.*
- *Diverses faiblesses dans IP; routage basé sur l'adresse de destination.*
- *Certains champs de l'entête IP sont exploitables pour des attaques.*
- *Les faiblesses de TCP, de UDP.*
- *ICMP est faillible*
- *http est devenu un protocole de transport.*

Objectifs Chapitre 3

- ***Connaître les faiblesses et les méthodes d'attaques couramment utilisées.***
- ***Voir quelques exemples d'attaques par déni de services commentés.***
- ***Voir quelques exemples d'attaques par vol de connexion.***
- ***Connaître quelques techniques de la gestion des risques***

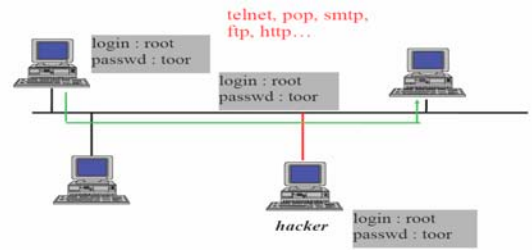
Les menaces de la couche physique

- *Ecoute du réseau (sniffing)*
- *Usurpation d'adresses physiques*
  - *ARP cache Poisonning (par exemple pour contourner les limites du sniffing sur une switch)*

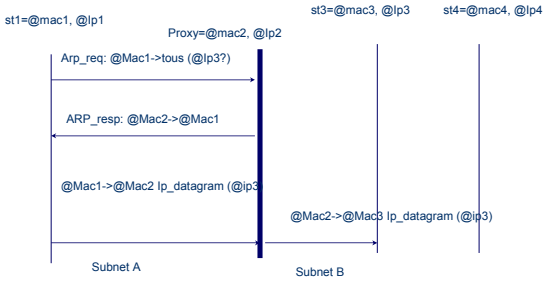
Méthodes d'attaques

- ***Intrusion***
  - *Exploitation de failles, erreurs de configuration*
- ***Abus de droits légitimes***
  - *Utilisation abusive de fonctionnalité*
- ***Action physique***
  - *Destruction, altération d'éléments matériels, câble, vol de disques …*
- ***Usurpation d'identité***
  - *Utilisation abusive d'une fausse identité ou vol d'une vraie identité*
- ***Injection de code***
  - *Installation et exécution d'un programme, module destiné à écouter, surveiller, voler des informations confidentielles*
- ***Ecoute***
  - *Ecoute passive et clandestine pour récupérer des informations*

Ecoute du réseau



Usurpation d'adresses MAC



Les menaces de la couche physique: remédiation

- *Utilisation de switchs avec Vlans et authentification des cartes réseaux (802.1x)*
- *Table ARP statique*

Les faiblesses de la couche réseau

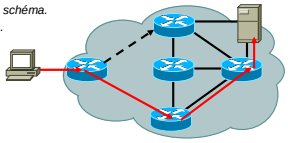
- *Usurpation d'adresses (Ip Spoofing)*
- *Mauvaise fragmentation IP*
- *Attaque sur le routage*
- *Dénis de service:*
  - *Ping de la mort*
  - *Smurf attaque*
- *Tunneling dans les paquets ICMP (Tunnel loki)*

Les menaces de la couche Transport

- *Dénis de services:*
  - *SYN flooding*
  - *Land bug*
  - *AckStorm (FW1), UDP Flood (IOS)*
- *Balayage de ports et d'adresses (nmap)*
- *Identification d'OS (nmap, Nessus, Queso)*
- *Usurpation de session par prédiction des numéros de séquences (juggernaut,hijact)*

Les faiblesses de la couche réseau

- *capacité pour un intrus de rediriger le trafic où il le désire*
  - *Trajet normal en grisé par le bas du schéma.*
  - *Trajet dévié (flèche en pointillé noir).*

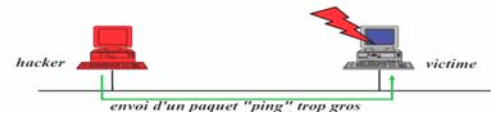


Dénis de service

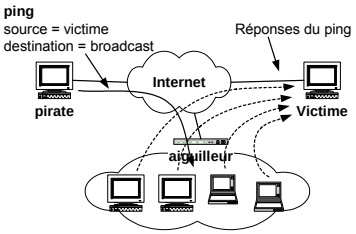
- *Teardrop, NewTear, Boink, Ping of Death*
  - *Envoient 2 fragments IP dont un fragment est trop petit*
  - *La pile IP essaie d'assembler les fragments : crash*
  - *Affectent plusieurs systèmes dont Windows et Linux*

Ping of death

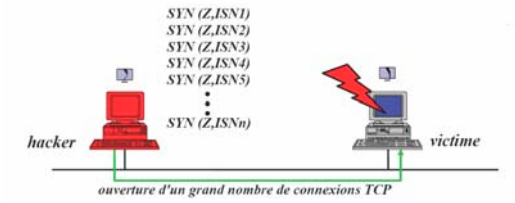
- *Attaque qui utilise un bug dans le processus de ré assemblage de paquets fragmentés:*
  - *Le paquet fera plus de 65535 octets => Crash stack IP ou le système d'opération!*



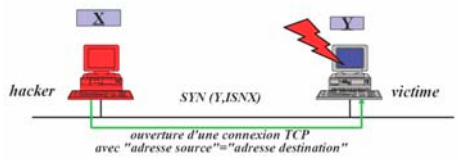
Déni de service : Smurf



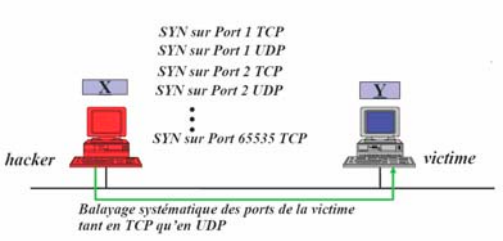
Syn. Flood



Attaque Land



Balayage de ports



Les menaces des couches réseaux et transports: remédiation

- *Mise à jour des applications et OS*
- *Firewall personnel et de réseau*
- *Utilisation de protocoles sécurisés: SSH v2, IPSec*
- *Interdire le source routing (filtrage sur les aiguilleurs)*
- *Filtrer les broadcasts directs (ex 120.255.255.255) sur les aiguilleurs*

Les menaces de la couche applicative

- *Cheveaux de Troie*
- *Backdoor: Porte dérobée*
- *Virus, Vers: Sapphire (un paquet UDP de 404 octets, Code Red 4 Ko)*
- *Failles applicatives: bogues, buffer overflow*
- *Détournement de protocoles pour cacher de l'information: Tunnel HTTP*

Réseaux de Zombies (Botnet)

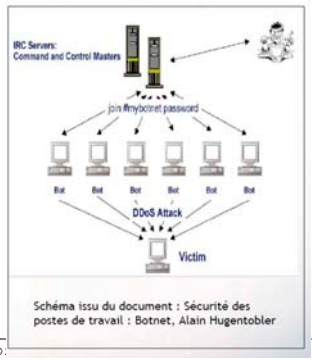


Schéma issu du document : Sécurité des postes de travail : Botnet, Alain Hugentobler

Les menaces de la couche applicative: remédiation

- *Sensibilisation du personnel*
- *Mise à jour des applications et OS*
- *Firewall personnel*
- *Antivirus et antispyware (à jour)*
- *Utilisation de Proxy analysant les flux*

Résumé du chapitre 3

- ***Les faiblesses des protocoles sont multiples, accès distant, réseau…***
- ***Les méthodes d'attaques sont nombreuses, intrusion, injection de code, exploitation de failles …***
- ***Quelques exemples d'attaques par déni de services : synflood, nuke, land, teardrop, smurf, déni de service distribué.***
- ***Quelques exemples d'outils permettant de tester le vol de connexion : hunt, juggernaut, P.A.T.H.***
- ***Il est facile de trouver sur Internet des outils exploitant les failles et mauvaises implémentations de TCP/IP.***

Objectifs du chapitre 4

- ***Comprendre le principe de la défense en profondeur***
- ***Comprendre ce qu'est une passerelle de sécurité, les règles de filtrage***
- ***Comprendre l'architecture et le type des passerelles de sécurité***
- ***Avoir un aperçu des configurations possibles***
- ***Avoir des spécifications comparatives de produits existant***

Un constat

- *En réseau pas de solution unique miracle*
- *Toutes les couches protectrices peuvent être contournées*
- *Il est donc nécessaire d'avoir plusieurs niveaux de protection*

La Défense en profondeur

Protection uniforme

- *Utilisation de plusieurs technologies (firewall, VPN, IDS/IPS, antivirus)*
- *Pas de zone plus protégée qu'une autre => protection uniforme des actifs informationnels*

Architecture très sensible à des attaquants internes!

Protection par zones

- *Protection de zone sensible au sein d'un réseau ouvert ou déjà protégé*
  - *VLANS, listes d'accès, firewall, VPN, IDS/IPS, antivirus*
- *Bon contre des intrusions internes mais souvent difficile à gérer*

Protection par vecteur d'attaques

- *Fermeture des ports USB*
- *Interdiction d'utiliser des médias amovibles…*
- *Modem fonction en appel en call back*
  - *A utiliser en complément d'autres moyens de défense!*

Protection Centrée sur l'information

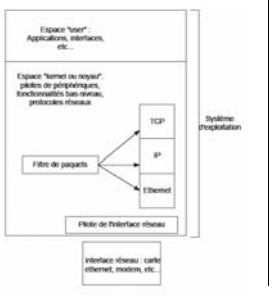
- *Protection en pelure d'ognon!*
  - *La donnée par des règles d'accès (J2EE, .Net)*
  - *L'application (bonne pratique de développement)*
  - *Le host (host IDS, durcissement d'OS..)*
  - *Le réseau (Firewall, VPN)*
    - ➲*Une défense globlale*

Ne pas protéger en périphérie ….c'est

- *Appliquer la sécurité seulement sur les ordinateurs*
  - *nécessite un effort important*
  - *est vulnérable à tout changement, même minime, d'un seul ordinateur (qui peut alors servir de tremplin pour une attaque)*
  - *n'évite pas les attaques de base*
- *Appliquer la sécurité à la périphérie des réseaux*
  - *sur les routeurs*
  - *sur les passerelles de sécurité*

Garde-barrières

- *Définition*
- *Technologies de garde-barrières*
- *Architectures de garde-barrières*



Garde-barrières

- *Définition*
  - *Mécanisme qui permet le passage sélectif du flux d'information entre deux réseaux suivant une politique de contrôles d'accès*
    - ➲ *réseau externe (public, potentiellement hostile)*
    - ➲ *réseau interne (privé)*
  - *Facteurs de décision*
    - ➲ *nature du service (protocole), origine et destination, autorisations, heures, etc.*

Technologies de garde-barrières

- *Filtrage de paquets*
- *Serveur mandataire (proxy)*
- *Filtrage avec inspection d'état*

Filtrage de paquets

- *Définition*
  - *Opère au niveau de l'en-tête de chaque paquet*
  - *Règles permettant de décider si on route ou on bloque le paquet*
  - *Règles basées sur*
    - ➲*les adresses source et destination*
    - ➲*les ports source et destination*
    - ➲*les protocoles (UDP, TCP, ICMP, etc.)*

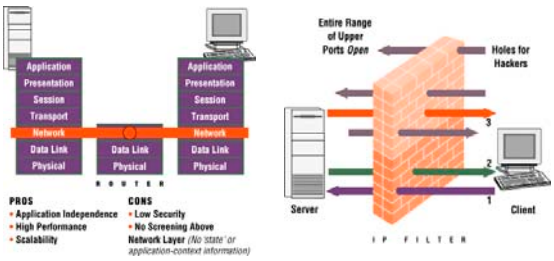
Filtrage de paquets suite

- *Avantages*
  - *Peu coûteux*
  - *Fonctionnalités de filtrage implantées en standard dans les routeurs*
  - *On a déjà le routeur pour établir la connexion vers l'extérieur*
  - *Première ligne de défense*

Filtrage de paquets suite

- *Inconvénients*
  - *Nécessite une très bonne connaissance des protocoles et du langage de programmation des routeurs*
  - *Implantation complexe devant tenir compte des divers scénarios d'échange*
  - *Protocoles difficiles à sécuriser: FTP, X, ...*
  - *Pas d'authentification en général*
  - *Pas de journalisation*

Filtrage de paquets suite



Source : http://www.checkpoint.com/

Serveur mandataire (proxy)

- *Logiciel permettant de relayer des requêtes entre un réseau interne et un réseau externe*
  - *on parle aussi de passerelle applicative ou de relayage de service*
- *Aucun trafic ne passe directement du réseau externe vers le réseau interne*

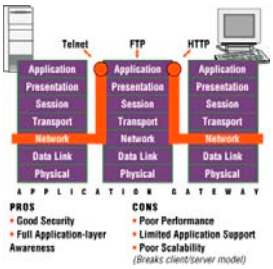
Serveur mandataire (proxy) suite

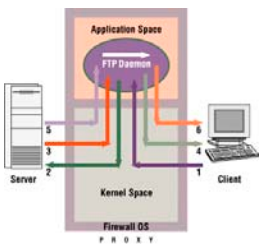
- *Inconvénients*
  - *Peu de transparence pour l'utilisateur (nécessite souvent une configuration spécifique des clients)*
  - *Nécessite un proxy pour chaque nouveau service*
  - *Beaucoup d'applications non supportées (ne supporte pas UDP)*
  - *Lent*

Serveur mandataire (proxy) suite

- *Avantages*
  - *Le réseau « interne » est masqué, seul le proxy est visible de l'extérieur*
  - *Authentification des usagers / services et source / destination*
  - *Possibilité de filtrage des données en transit (URL, courrier)*
  - *Possibilité de journalisation*
  - *Fonction de « cache »*

Serveur mandataire (proxy) fin





Source : http://www.checkpoint.com/

Filtrage avec inspection d'état

- *Filtrage de paquets avec connaissance du niveau applicatif*
  - *s'intéresse à la continuité du flux*
- *Permet de faire de la translation d'adresses (NAT)*
  - *one-to-one ou one-to-many*

Filtrage avec inspection d'état suite

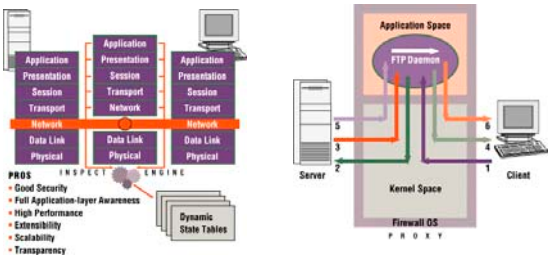
- *Principales caractéristiques*
  - *Masque le réseau interne*
  - *Authentification des usagers / services et source / destination*
  - *Possibilité de filtrage des données en transit (URL, courrier)*
  - *Possibilité de journalisation*

Filtrage avec inspection d'état suite

- *Haute performance*
- *Complètement transparent pour les utilisateurs*
- *Permet l'utilisation de commande comme ping, traceroute*

Filtrage avec inspection d'état

suite

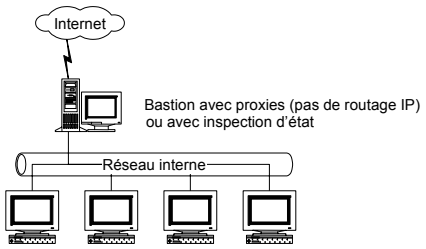


Source : http://www.checkpoint.com/

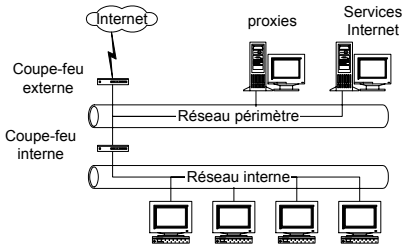
Architectures de garde-barrière

- *3 architectures classiques*
  - *Dual-Homed Gateway*
  - *Screened Host*
  - *Screened Subnet*

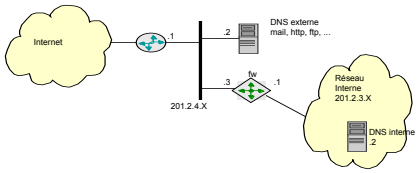
Dual-Homed gateway



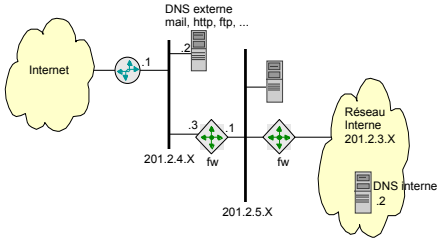
Screened Subnet



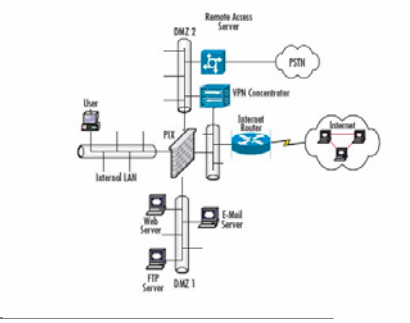
Exemple 1: passerelle de sécurité et routeur



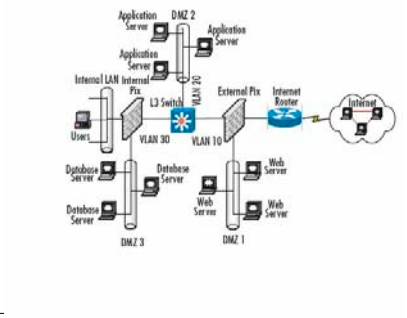
Exemple 2: passerelle de sécurité, routeur et réseau intermédiaire



Exemple 3:Multi zones



Exemple 4: Routeur filtrant+2 firewalls+Vlans



Multiples passerelles

- *Cas : siège social et plusieurs bureaux distribués géographiquement avec un réseau privé les reliant*
  - *pour accès Internet des bureaux,*
    - ➲ *trafic Internet passe par le réseau privé et sort au siège social*
      - *meilleur contrôle*
      - *un seul point de sécurité externe à surveiller*
      - *trafic Internet via réseau privé est coûteux, car liens privés plus chers que liens Internet la plupart du temps*
    - ➲ *trafic Internet sort par une passerelle de sécurité pour chaque bureau*
      - *moins coûteux pour les liens privés*
      - *plusieurs points de contrôle de sécurité : plus difficiles à gérer*
    - ➲ *compromis possible : passerelle de sécurité pour chaque bureau, mais configuration limitée à une diode (aucun trafic vers l'interne)*

Que faire des DNS?

- *DNS externe pour la résolution des ordinateurs publics*
- *DNS interne pour la résolution interne et relais pour externe; c'est l'externe qui va résoudre les adresses Internet (forwarder)*
- *Passerelle ne laisse passer que les requêtes du DNS interne vers externe*
- *Préférablement (d'un point de vue sécurité), ni l'externe, ni l'interne sur la passerelle de sécurité*
- *La sécurité de la passerelle ne doit pas dépendre du DNS*

Filtrage anti-spoofing

- **Protection contre les adresses IP sources falsifiées**
- **Politique :**
  - **Un paquet arrivant sur une interface réseau doit posséder une adresse IP source conforme à cette provenance - sauf routage asymétrique**
    - ➲ Ex : Un paquet arrivant depuis l'Internet avec une adresse source « interne » sera rejeté. Encore faut-il que le filtre ait la connaissance des adresses IP internes !
    - ➲ Généralement, le mot clef **any** sera à proscrire...
  - **Peu d'attaques font usage de falsification d'adresse IP source, en dehors des attaques par déni de service, contre lesquelles on ne lutte généralement pas avec de simples règles de filtrage => Syndefendeur chez FW1**

Filtrage sur l'entête IP

- **Adresse source (attention : l'adresse source peut être**
- **falsifiée)**
- **Adresse destination**
- **Type de protocole (TCP, UDP, ICMP, AH, ESP, autre.)**
- **Options diverses (source routing) et fragmentation**
  - seul le premier fragment contient les informations d'en-tête des protocoles des couches supérieures à IP
    - ➲ auparavant, seul le premier fragment était filtré ; les fragments suivants n'étaient pas filtrés
    - ➲ il existait, par le passé, de nombreuses attaques basées sur la fragmentation, il convient donc que ce soit le firewall qui assure le réassemblage des paquets pour l'ensemble des machines qu'il protège, voire qu' il assure une normalisation de trafic
- **les piles modernes ne tolèrent plus les fragments en deçà d'une certaine taille (Linux 2.6 et champ IP ID à zéro pour les segments TCP SYN)**

Filtrage TCP

- **Port TCP source**
  - notion de ports éphémères : ports aléatoires supérieurs à 1024 pour les clients, dont la plage varie d'un système d'exploitation à l'autre
- **Port TCP destination**
  - limiter les connexions aux seuls ports sur lesquels on fait tourner des serveurs fiables
  - certains services utilisent des ports aléatoires supérieurs à 1024 pour les serveurs (RPC)
- **Signalisation TCP et flags (SYN, ACK, PSH, FIN, RST, URG)**
  - pour bloquer une connexion entrante, il suffit d'en bloquer le premier paquet entrant qui a ACK=0 (permet d'accepter des paquets entrants sans accepter de connexions entrantes)
- **Il y a une notion de connexion TCP qui identifie tous les segments d'une même communication**

Filtrage UDP

- **Port UDP source**
- **Port UDP destination**
- **Pas de signalisation**
  - **typiquement, pas de bits «SYN» ou «ACK»**
    - ➲ pas de notion de **sens d'initiation de connexion**
  - **aucun moyen de distinguer un premier datagramme d'un client externe vers un serveur interne d'une réponse d'un serveur externe à un client interne**
- **Pas de notion de connexion : les protocoles basés sur UDP sont du style question/réponse (DNS par exemple**
  - Notion de session fondée sur le pseudo-header UDP et une fenêtre de temps

Filtrage sur les entêtes ICMP

- **En-tête ICMP**
  - **type et code de message ICMP (echo-request type 8 /**
- **code 0 par exemple)**
  - **messages ICMP générés par le noyau = = pas de notion d'application = = pas de port source ni de port destination, ni aucun autre protocole au-dessusde lui**
  - hors usages dérivés type «tunnels sur ICMP» avec loki (Phrack49, 08/ 11/ 1996)
  - attention aux règles implicites Check-Point FW-1 (ICMP autorisé par défaut, sans restriction sur les adresses source et destination) !

Décisions du système de filtrage

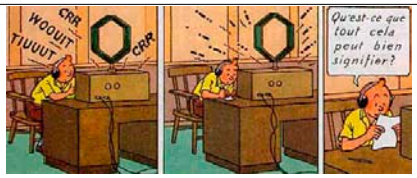
- **Laisser passer les paquets,**
  - **à destination d'un processus local**
  - **à destination d'une pile TCP/ IP distante (filtrage puis routage ?)**
- **Rejeter les paquets**
  - **envoyer des codes d'erreur ICMP en cas de rejet de paquets(codes "hôte administrativement incorrect" ou "réseauadministrativement incorrect")**
  - **envoyer des segments TCP RST, pour les connexions TCP**
- **Rejeter les paquets sans renvoyer de message d'erreur (l'attaquant voit un timeout)**
- **Enregistrer les actions**

Configuration des règles de filtrage

- **Permission par défaut et refus par défaut**
  - ☹ **permission par défaut : ce qui n'est pas explicitementinterdit est autorisé**
  - ☺ **refus par défaut : ce qui n'est pas explicitement autorisé est interdit**
- **Gérer la bi-directionnalité des connexions**
  - **de nombreuses attaques peuvent réussir si l'agresseurpeut envoyer des paquets, même s'il n'a pas de réponse**
    - ➲ ex. : attaques par deni de service, avec une adresse IP source généralement falsifiée
    - ➲ ex. : tunnels sur signalisation TCP (RST ou ACK)
- **Les règles de filtrage sont ordonnées de manière séquentielle**

Résumé du chapitre 4

- *Filtrage au niveau des routeurs, des passerelles*
- *Architecture des passerelles; OS, OS modifié durci… boite noire*
- *Pas de services sur les passerelles, le strict minimum*
- *Les différentes topologies des passerelles*
- *Cas des passerelles multiples et du DNS*
- *Comparaison logique des routeurs et des passerelles*
- *Quelques produits*
- *Une passerelle améliore la sécurité mais ne l'est pas forcément !*



Chiffrement et Architecture de PKI **(Public Key Infrastructure)**

Objectifs du chapitre 5

- ***Connaître les moyens de cryptographie les plus utilisés***
- ***Comprendre les notions de clés symétriques, asymétriques et leurs algorithmes***
- ***Voir les applications de la cryptographie; signature électronique, hachage.***
- ***Comprendre les principes de la stéganographie***

A quoi sert la cryptographie ?

Définition selon le dictionnaire Hachette :

- *Le terme "cryptographie" provient du grec Kruptos, "caché", et de graphein, "écrire".*

- ***Cryptographie:***
  - *Ensemble des procédés permettant de transformer un message écrit, dit clair, en un autre message, dit chiffré, ou crypté.*
- *La cryptographie permet d'empêcher de voir ou de comprendre des messages, des fichiers voire des systèmes complets comme un système de fichiers.*

Cryptographie: Quelques définitions

- *Cryptographie = littéralement écriture cachée*
- *Crypter ou chiffrer un texte :*
  - *Plaintext -> Cyphertext*
- *Déchiffrer ou décrypter est l'action inverse*

Cryptographie: Exemple simple

- *Texte clair: ABCDEFGHIJKLMNOPQRSTUVWXYZ*
- *Texte codé: WXEHYZTKCPJIUADGLQMNRSFVBO*
- *A ->W, B->X, C-> E ….*
- *Le texte clair suivant est*
  UN PETIT ROSEAU M'A SUFFI POUR FAIRE FREMIR L'HERBE HAUTE ET TOUT LE PRE ET LES DOUX SAULES ET LE RUISSEAU QUI CHANTE AUSSSI.
- *Le texte codé sera : MT JCGLG UZVCNM S'N VMWWL JZMU WNLUC WUCSLU Q'DCUYC DNMGC CG GZMG QC JUC CG QCV OZMB VNMQCV CG QC UMLVVCNM RML IDNTGC NMVVVL.*

Buts de la cryptographie

- *Confidentialité => chiffrement*
- *Intégrité des données => signature électronique*
- *Authentification => Chiffrement et signature électronique*
- *Non Répudiation => Signature Electronique*

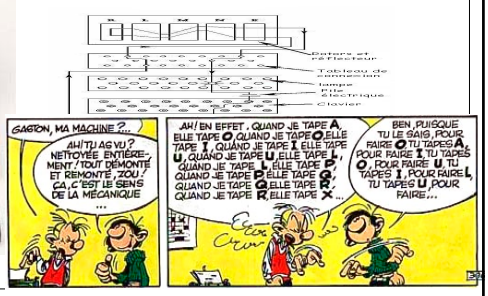
Les 3 types de chiffrement

- *Clé secrète partagée:*
  - *Symétrique*
  - *En général la clé est unique*
- *Clés publiques:*
  - *Asymétrique*
  - *Paire de clés (privée et publique)*
- *Hash:*
  - *Pas de clé (en général)*
  - *Algorithme à sens unique*

Un peu d'histoire
Le chiffrement symétrique

- *Les mécanismes symétriques ou à clé privée,*
  - *Clé unique au chiffrement et au déchiffrement.*
    - ➲ *Les plus anciens.*
    - ➲ *Les plus fragiles.*
    - ➲ *Comment transporter la clé?*
- *Le plus ancien, en Perse 1600 avant JC*
- *Le plus connu,*
  - *le code de César substitution mono-alphabétique*
- *Plus sophistiqué,*
  - *le code de Vigenère au 16ème siècle*
  - *Substitution poly-alphabétique*
- *Plus impressionnant, ENIGMA pendant la seconde guerre mondiale,*
  - *Force: 10^{16} à 10^{20} possibilités*
  - *Faiblesse: chiffrement lié au matériel*

ENIGMA : Un rôle considérable pendant la seconde guerre mondiale.

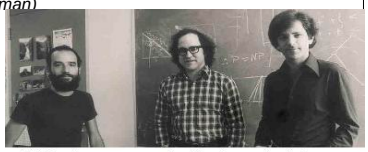


Les mécanismes à clé privés ou chiffrement symétrique

- *Le DES (Data Encryption Standard)*
  - *Clé de 40 ou 56 bits*
  - *Déclaré obsolète par la NSA*
- *Le Triple DES*
  - *Clé théorique de 168 bits par 3 itérations de DES*
  - *Déclaré obsolète par la NSA*
- *AES:* Advanced Encryption Standard
  - *L'algorithme prend en entrée un bloc de 128 bits (16 octets), la clé fait 128, 192 ou 256 bits*
  - *Pas d'attaque connue réussie*

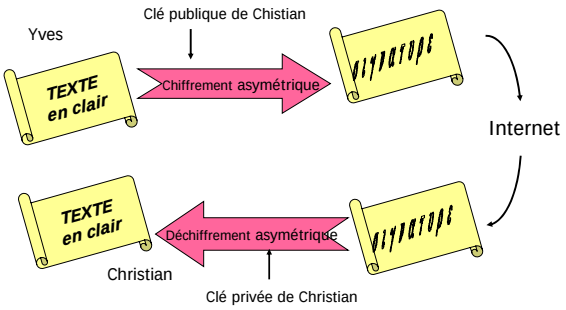
Les mécanismes asymétriques ou à clé publique et clé privé .

- *Une révolution conceptuelle*
  - *Il existe 2 clés pouvant chiffrer et déchiffrer*
    - ➲ *Une clé restera secrète*
    - ➲ *Une clé deviendra publiable*
    - ➲ *Les deux clés ne peuvent se déduirent*
  - *Fondés sur des propriétés mathématiques particulières (par exemple la difficulté de décomposer les grands nombres en facteurs premiers RSA Rivest, Shamir & Adleman)*
    - ➲ *Clé privée très difficile à trouver à partir de la clé publique.*
    - ➲ *Difficulté accrue par la longueur.*

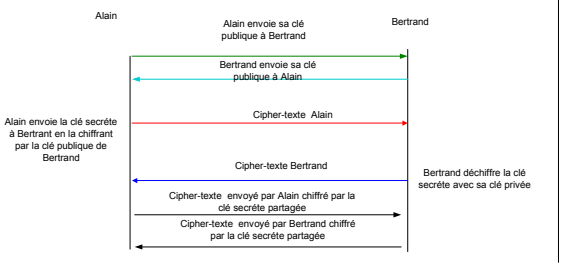


Adi Shamir Ron Rivest Len Adleman

Un échange confidentiel asymétrique



Chiffrement combiné asymétrique + symétrique (SSL par exemple)



L'authentification, l'intégrité et la non répudiation

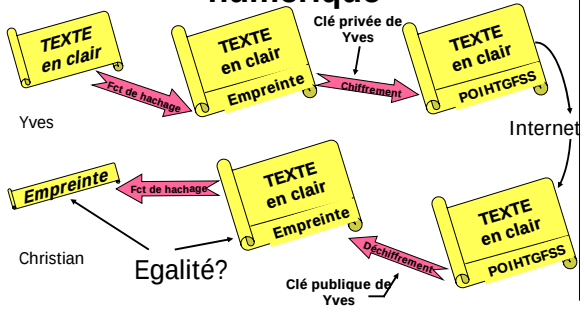
- *Assurée par la signature électronique*
  - *Applique une fonction mathématique qui permet de créer le sceau (empreinte, hash ou condensat) d'une entité informatique (fichier, document,…)*
    - ➲*Sceau de taille beaucoup plus petite que le message lui-même*
    - ➲*Utilise une fonction de hachage (appliquée sur le document)*
    - ➲*Génère une suite de bits de taille fixe (très petite)*
    - ➲*Empreinte ou condensé*
    - ➲*Un bit du texte initial modifié génère une empreinte différente*

Les algorithmes de hash

- *MD5 (Message Digest) : empreinte de 128 bits*
- *SHA-1 (Secure Hash Algorithm) : empreinte de 160 bits*
- *SHA-2 empreinte de 256 bits.*

- *Transmis au destinataire,*
  - ➲*Le sceau permet de vérifier l'intégrité de l'information sur laquelle il a été calculé*

Transmission de la signature numérique



Stéganographie

- *Technique permettant de dissimuler un texte ou une information dans un document:*
  - *Document Word*
  - *Images JPEG*
  - *Films Mpegs…*
  - *Il n'y a pas de moyens faciles de détecter ce type de pratiques*

Typologie de la stéganographie

- *3 méthodes:*
  - *Injection => on rajoute des nouveaux éléments dans un fichier, une image*
  - *Substitution => exemple: on substitue des couleurs dans une image*
  - *Création d'un nouveau fichier*

Résumé chapitre 5

- *La cryptologie est utilisée depuis la nuit des temps !*
- *La cryptographie assure la confidentialité, l'intégrité, l'authentification et la non répudiation*
- *Les algorithmes à clés symétriques.*
- *Les algorithmes à clés symétriques appelés aussi à clés publiques permettent de communiquer de façon sécuritaire par simple échange de clé publique.*
- *Application directe de la cryptographie; la signature électronique, le hachage, les certificats.*
- *Il est aussi possible de cacher de l'information dans une autre: c'est la stéganographie*

Chapitre 6: Les espaces de confiances

PKI: Public Key Infrastructure

ICP: Infrastructures à Clé Publique

Répond à la question suivante.

- *Comment Distribuer et Assurer l'authentification des clés?*
- *C'est le rôle du certificat.*
  - *Assure la liaison entre la clé publique et l'identité de son propriétaire.*
    - ➲*Grâce à un document normalisé,*
      - *dûment rempli,*
      - *joint à la clé publique du certifié,*
      - *et signé par la clé privée du certifiant.*
  - *Assure la propriété*
    - ➲*de la clé publique utilisée pour le chiffrage du message et le déchiffrage de la signature*
    - ➲*de la clé privée utilisée pour le chiffrage de la signature.*

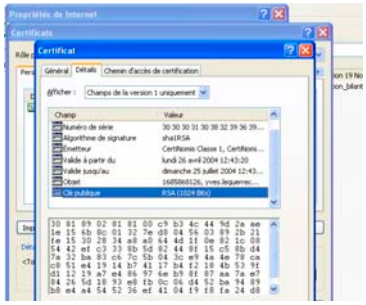
Le rôle de l'Autorité de Certification

- *La Certification est assurée par soit un réseau de connaissances, soit par une autorité de confiance.*
  - ➲*Appelée une Autorité de Certification.*
    - *– Répond à une politique de certification publiée.*
  - ➲*Délivre des certificats en y apposant sa signature avec sa clé privée.*
  - ➲*Les certificats deviennent utilisables pour l'identification, le chiffrement et la signature*

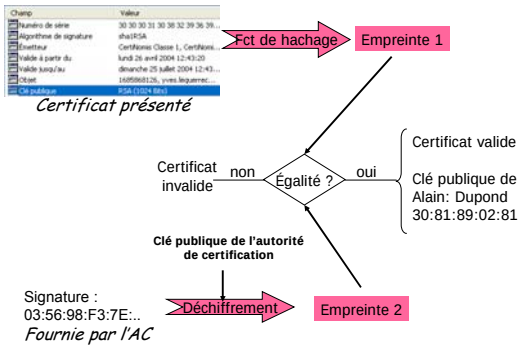
Contenu d'un certificat

- *Le format de certificat défini par la norme ISO X509v3*
- *Doit notamment contenir les informations suivantes*
  - *Version du certificat*
  - *Numéro de série du certificat*
  - *Description de l'algorithme de signature de l'organisme émetteur du certificat*
  - *Nom de l'organisme émetteur du certificat*
  - *Période de validité*
  - *Nom de l'utilisateur à qui appartient le certificat*
  - *Clé publique de l'utilisateur*
  - *Description de l'algorithme à utiliser avec la clé publique*
  - *Signature de l'organisme émetteur du certificat*
  - *Extensions*

Exemple de contenu de certificat



Principe de vérification

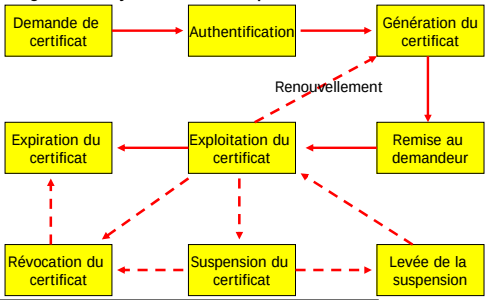


La chaîne de confiance

- *L'autorité de certification certifie l'identité des entités qui lui en font la demande.*
- *Une entité analysant un certificat se doit alors de vérifier la validité du certificat de l'autorité l'ayant émis et la chaîne de confiance.*
- *Si l'AC a été certifiée par une AC mère, alors il faut aussi vérifier cette dernière, et ainsi de suite jusqu'à l'autorité en laquelle l'entité a entièrement confiance: l'AC racine.*
- *les navigateurs sont pré-configurés pour faire confiance aux AC Racine bien connues*
- *Une AC définit pour chaque certificat :*
  - *leur durée de vie,*
  - *leur renouvellement,*
  - *et conserve la liste des certificats antérieurement émis, non périmés mais n'étant plus valides*

L'infrastructure à clé publique PKI gère la vie du certificat

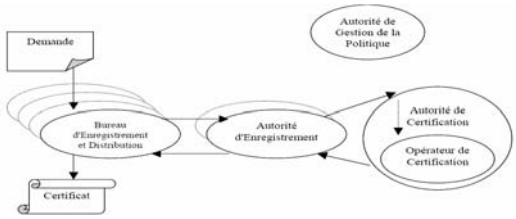
- **Désigne l'ensemble des moyens et ressources nécessaires à la gestion du cycle de vie et à l'exploitation des certificats.**



Les composants de la PKI

- *L'autorité de Certification*
  - *Entité responsable, est engagée par sa politique de Certification.*
  - *Création du certificat pour le détenteur d'une clé secrète (cette fonction de fabrication peut être déportée sur une entité tierce, l'opérateur de certification).*
  - *Publication et archivage de certificats*
  - *Révocation du certificat*
  - *Interface avec les autres AC (reconnaissance mutuelle des certificats).*
- *L'Autorité d 'Enregistrement*
  - *Bureau d'Enregistrement*
- *L'Autorité de Validation*
- *L'Autorité d'Horodatage*
- *L'Autorité d'Archivage*

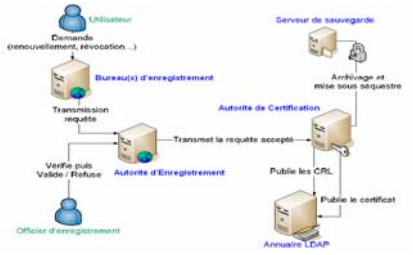
PKI/ICP



Niveau actuel des certificats

- *classe 1*
  - *adresse e-mail du demandeur requise;*
- *classe 2*
  - *preuve de l'identité requise (photocopie de carte d'identité par exemple);*
- *classe 3*
  - *présentation physique du demandeur obligatoire.*

Les Composantes du Processus



La synthèse

- *Vers une nouvelle organisation de la chaîne de confiance*
  - *AC Autorité Certification*
  - *AE Autorité d'Enregistrement*
  - *OC Opérateur Certification*
  - *AV Autorité de Validation*
  - *AH Autorité d'Horodatage*
  - *Tiers Archiveur*

Chapitre 7

Les Réseaux Virtuels Privés
Virtual Private Network

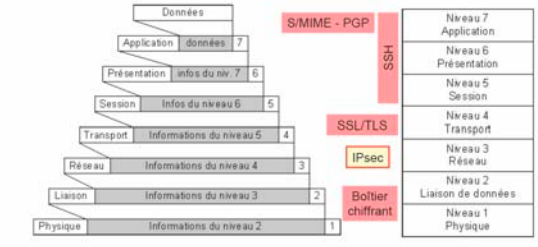
Objectifs

- **Après avoir terminé cette leçon, vous serez en mesure de :**
- **Voir ou se situe IPSEC dans le modèle TCP/IP.**
- **Connaître les services et applications offerts par le VPN.**
- **Connaître les différents modes de IPSEC.**
- **Comment se place IPSEC, AH, ESP dans un paquet.**
- **Voir les impacts du VPN et les produits du marché.**

Définition

- *Le **Réseau privé virtuel** (VPN ou Virtual Private Network), est une extension des réseaux locaux qui procure une norme de sécurité en télécommunications.*
  - *Utilisation d' nternet comme support de transmission en utilisant un protocole de « tunnelisation » (en anglais tunneling),*
  - *Encapsulant des données à transmettre de façon chiffrée.*
  - *Réseau privé virtuel => désigne le réseau ainsi artificiellement créé.*
    - ➲ *Ce réseau est dit virtuel car il relie deux réseaux « physiques » (réseaux locaux) par une liaison non fiable (Internet), et privé car seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent « voir » les données*

IPSec comparé aux autres protocoles de chiffrement



IPSec

ISO		Exemples
5,6,7	Application	SMTP,HTTP,DNS
4	Transport	TCP/UDP
3	Réseau	IP ← IPsec
1, 2	Physique	Ethernet

- ***IPsec***
- *Sécurité au niveau IP*
  - *peu importe le protocole supérieur*
  - *toutes les applications en bénéficient*
  - *Ne nécessite aucune modification aux applications*
- *Aujourd'hui, on doit modifier la pile IPv4 pour installer IPsec*
  - *les produits s'installent dans la pile réseau*
- *Les versions les plus récentes des systèmes d'exploitations offrent IPsec*

IPSec: Services de sécurité

- *Services de sécurité offerts sont*
  - *Confidentialité*
  - *Authentification de l'origine des paquets*
  - *Intégrité des données*
  - *Protection contre le rejeu*
  - *Contrôle d'accès*
- *Ces services sont basés sur des mécanismes cryptographiques qui leur confèrent un niveau de sécurité élevé lorsqu'ils sont utilisés avec des algorithmes forts.*
- *Granularité de la sécurité offerte par IPSec :*
  - *poste à poste*
  - *poste à passerelle*
  - *passerelle à passerelle*

IPSec: exemples de réseau

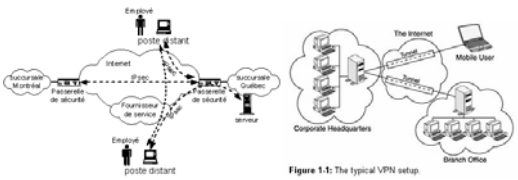


Figure 1.1: The typical VPN setup.

Association de sécurité (SA)

- Paramètres d'une association de sécurité :
  - protocoles utilisés
  - algorithmes et clés utilisés pour générer l'extension d'authentification
  - algorithmes et clés utilisés pour générer l'extension de confidentialité
  - durée de vie de l'association de sécurité
  - le mode de communication (tunnel, transport)

Association de sécurité (SA)

- On identifie chaque SA par :
  - l'adresse de destination
  - le protocole de sécurité utilisé (AH ou ESP)
  - un index unique, le SPI (***Security Parameter Index***)
- Une SA est unidirectionnelle ou bidirectionnelle

Security Policy Database (SPD) et Security Association Database (SAD)

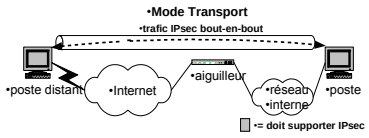
- SPD:
  - Base composée de deux listes : trafic entrant et trafic sortant
  - Chaque liste est composée de filtres IP (adresse source, destination, protocole) et du comportement à suivre :
    - ➲ refuser
    - ➲accepter
    - ➲ sécuriser (via un protocole IPsec)
- SAD: Base dynamique composée de toutes les SA actives

Mode transport et tunnel

- Mode transport
  - communication IPsec bout-en-bout
    - ➲ Protège uniquement le contenu du paquet IP sans toucher à l'en-tête; ce mode n'est utilisable que sur les équipements terminaux (postes clients, serveurs).
- Mode tunnel
  - communication IPsec au moyen d'une passerelle de sécurité
    - ➲ Permet la création de tunnels par encapsulation de chaque paquet IP dans un nouveau paquet. Ainsi, la protection porte sur tous les champs des paquets IP arrivant à l'entrée d'un tunnel, y compris sur les champs d'en-têtes (adresses source et destination par exemple). Ce mode est utilisé par les équipements réseau (routeurs, gardes-barrières,…)

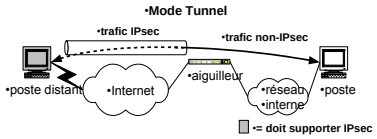
Mode transport

- *Offre une protection pour les protocoles de couche supérieure (TCP,UDP, ICMP)*
- *Utilisé pour protéger une communication bout-en-bout*
- *Les routeurs ou les passerelles entre les deux partenaires IPsec n'interviennent pas dans la communication IPsec*
  - *N'ont pas besoin de supporter IPsec*

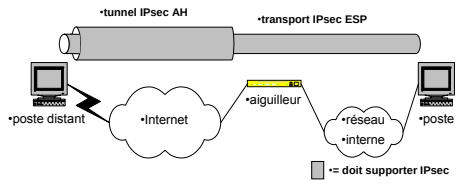


Mode tunnel

- Offre une protection sur le paquet IP entier
- Le paquet original circule dans un tunnel IPsec
  - Cache la destination finale du paquet
  - Offre une protection contre l'analyse du trafic
- Pas bout-en-bout : destination finale du paquet n'est pas le partenaire IPsec
  - ex. : passerelle de sécurité



Mode combiné



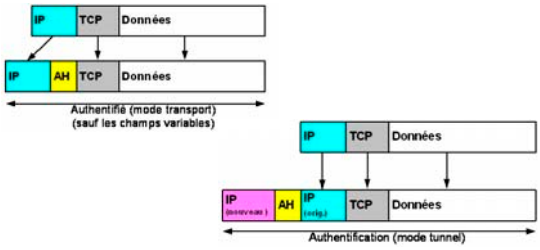
Protocoles

- IPsec dispose de 2 protocoles pour sécuriser les communications :
  - **AH (Authentication Header)** : permet d'assurerl'intégrité et l'authentification du paquet IP
  - **ESP (Encapsulating Security Payload)** :permet d'assurer l'intégrité, la confidentialité etl'authentification du paquet IP

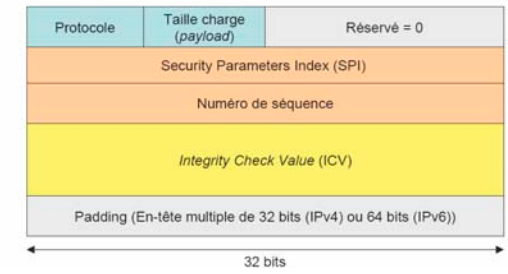
IP Authentication Header (AH)

- Défini dans la RFC 2402 (11/1998)
- Fourni pour les paquets IP les mécanismes desécurité suivant :
  - **intégrité**
  - **authentification** (origine)
  - **anti-rejeu** (optionnel)
- Protocole / En-tête suivant (Next Header) : 51

IP Authentication Header (AH)



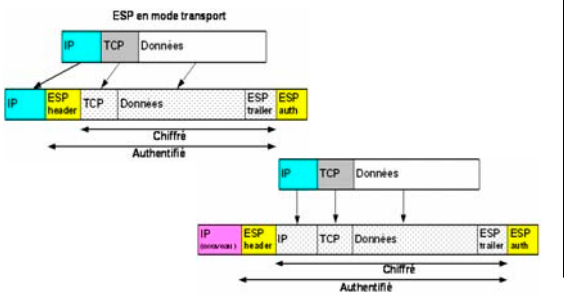
Pourquoi AH n'est pas compatible avec le NAT



Encapsulated Security Payload (ESP)

- Défini dans la RFC 2406 (11/1998)
- Fourni pour les paquets IP les mécanismes de sécurité suivant :
  - **confidentialité**
  - **intégrité** (limitée)
  - **authentification** (origine)
  - **anti-rejeu** (optionnel)
- Protocole / En-tête suivant (Next Header) : 50

ESP Transport et Tunnel



Internet Key Exchange (IKE)

- Pour pouvoir communiquer en IPsec, il faut :
  - s'authentifier
  - se mettre d'accord sur les protocoles à utiliser
  - échanger des clés
  - gérer automatiquement les SA
- C'est le protocole IKE qui est chargé de cette tache
- RFC 2409 (11-1998)
- IKE se base sur plusieurs protocoles : ISAKMP,Oakley, SKEME

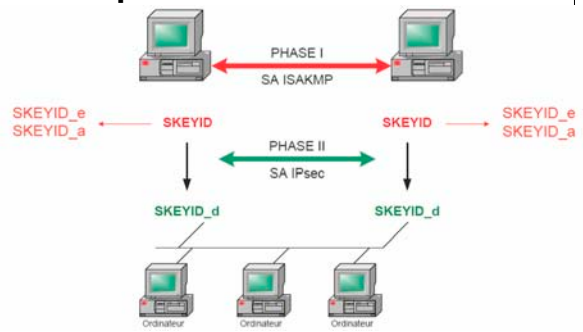
IKE - ISAKMP

- IKE se base sur ISAKMP pour la structure des échanges ISAKMP :
  - met en places les associations de sécurité (SA) : négociation, ajout, suppression
  - définit un cadre pour l'authentification et l'échange de clé (sans le définir)
  - est conçu pour être indépendant des mécanismes de sécurité
  - les implémentations sont données par le DOI (Domain of interpretation) RFC 2407 (11/1998)
  - les échanges sont appelés « Phases »
  - échanges des informations en UDP sur le port 500

IKE – Oakley et SKEME

- IKE se base sur Oakley et sur SKEME pour le contenu des échanges, mais il n'y a pas de compatibilité :
  - Oakley défini des échanges de clé et détaille les services de chacun (perfect forward secrecy (PFS), protection de l'identité, authentification). Les échanges sont appelés ***modes***
  - SKEME définie une méthode souple d'échange de clés(permettant l'anonymat, la non répudiation, et l'actualisation rapide des clés)

Implémentation RFC 2409



ISAKMP / Phase I

- **Phase I** : réalisation de l'authentification, et établissement d'une SA particulière, la SA ISAKMP (bidirectionnelle) qui servira pour les échanges futurs
  - Utilise deux modes :
    - ➲***Main mode*** (6 messages échangés)
      - Protection de l'identité des 2 points du SA
    - ➲***Aggressive Mode*** (3 messages échangés): un seul point est authentifié

ISAKMP / Phase II

- **Phase II** : établissement de 2 SA (unidirectionnelles) pour chaque types de communication IPsec
  - Utilise le **Quick Mode**
  - Les échanges de la phase II sont protégés par la SA ISAKMP

Authentification avec IKE

- RFC 2409 :
  - Pre-Shared Key
  - Digital Signatures : DSS signatures, RSA signatures
  - Public Key Encryption :
  - Encryption with RSA
  - Revised encryption with RSA
- Autres :
  - Kerberos
  - Radius

IPsec et Windows

- IPsec est nativement dans toutes les versions à partir de Windows 2000 (XP, 2003)
- Sur chaque machine on peut définir plusieurs **stratégies de sécurité IP**, mais une seule peut être activé
- Les stratégies peuvent être définies au niveau de la machine, ou déployées via un domaine 2000/2003 en utilisant les stratégies de groupe (GPO : Group Policy Object)

Résumé

- Authentification (AH) protège le trafic par contrôle d'accès.
- Confidentialité (ESP) protège le trafic par l'encryptage.
- Une association de sécurité (SA) est une structure de données qui décrit les services de sécurité utilisés entre deux entités
- Base des politiques de sécurité (SPD) est configurée par l'administrateur pour déterminer comment les services de sécurité seront appliqués
- Gestion des clés (IKE) permet une gestion automatique des SA

Chapitre 9
DNS,Telnet, FTP, TFTP

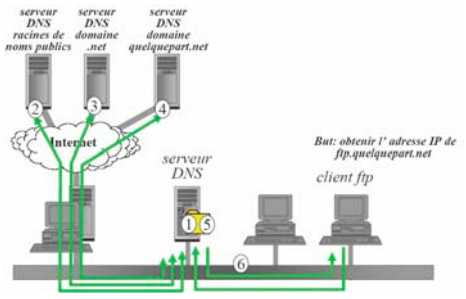
Objectifs

Après avoir terminé cette leçon, vous serez en mesure de :

Connaître les faiblesses des différents protocoles.

Mettre en place des solutions sécurisées

DNS: les requêtes



Le DNS : Domain Name Service

- **RFC 1035, port 53 (UDP ou TCP)**
- **Traduction des noms d'hôtes en adresses IP et vice-versa.**
- **Ce n'est pas un "service utilisateur" mais un service qui est mis en œuvre par les applications (SMTP, FTP, Telnet...) pour facilité la tâche des utilisateurs.**
- **Les enregistrements DNS contiennent également un grand nombre d'informations sur le réseau (sur les serveurs de mail,sur le matériel et le logiciel).**

DNS : les risques

- **Donner trop de renseignements aux agresseurs**
  - noms de machines internes et/ou externes mais explicites;
  - DNS HINFO : Informations sur les hôtes, description du matériel et de la version de l'OS;
  - TXT : Informations textuelles diverses employés par plusieurs services;
  - Demande de transfert de zone par un agresseur en se faisant passer pour le serveur secondaire.
- **Fausse réponse DNS :**
  - un agresseur change le cache du serveur DNS en indiquant qu'une adresse IP correspond au nom d'une machine qu'il possède, à la place de l'IP de la vraie machine.

DNS: Solutions Générales

- ***Dissimuler les informations au monde extérieur***
  - *mettre un serveur DNS spécifique à l'usage du monde extérieur et configurer les règles de filtrage en conséquence;*
  - *ne pas renseigner ce serveur DNS public avec des machines internes et/ou non publiques.*
  - *ne pas rendre les enregistrements HINFO sur un serveur public*
  - *désactiver les résolutions inverses sur ces serveurs publics pour masquervotre topologie*
  - *Ne pas accepter les requêtes récursives (pour un NS)*
- ***Utiliser la version la plus récente du serveur DNS (vérifier qu'elle effectue des contrôles par recherche double inverse)***
  - *Bind est une référence mais n'est pas une obligation*
- ***Mettre en place un dispositif de contrôle d'intégrité sur les serveurs DNS***

DNS: BIND sécurisé

- ***Utiliser la version la plus récente!***
- ***Masquer la version du serveur***
  - *options { version "" ;} retournera une chaîne vide à la requête dig @ip-dns version.bind chaos txt*
- ***Mettre en œuvre le principe de moindre privilège pour lelancement du serveur***
  - *Limiter les interfaces d'écoutes options {listen-on {@adresseIP};}*
  - *Utilisation d'un utilisateur non privilégié named –u @uid*
  - *Utilisation du chroot natif named –t @chemin_chroot*
- ***Désactiver les transferts de zone sauf en provenance du serveur secondaire (pour un serveur hébergeant des zones)***
  - *Création d'une acl : acl dnssecond {@ip1 ; @ip2 ;} puis options { allowtransfer {dnssecond ; };}*

DNS: BIND sécurisé

- ***Désactiver les mises à jours dynamiques options { allow-update {none;};}***
- ***Désactiver la récursion pour un serveur qui n'est pas relais :***
  - *Désactivation de la fonction options {recursion no ;};*
  - *Interdiction de requête récursive (défense en profondeur) options { allow-recursion{ none ; } ;}*
- ***Limiter la récursion pour un relais***
  - *Définition d'une ACL englobant les machines autorisées à utiliser le relais puis options { allow-recursion {@acl ;} ;*
- ***Futur : arrivée de DNSSEC (RFC 2065)***
  - *Authentification des réponses aux requêtes pour éviter la corruption des bases DNS (la base est signée hors connexion)*
  - *Authentification des données lors des transferts de zones*

Telnet

- ***Protocole standart de communication bidirectionnel (RFC 854)***
  - *Permet à l'utilisateur de se connecter sur un hôte distant (terminal virtuel) avec authentification*
- ***Principaux risques***
  - *Les mots de passe d'authentification circulent en clair ainsi que l'ensemble des commandes et de leur résultat*
  - *permet à des pirates d'obtenir des informations sur la machine cible*
    - ➲ *quel système d'exploitation est exécuté (en initiant une session Telnet sur la majeure partie des ports)*
    - ➲ *quels ports sont ouverts et quels serveurs sont exécutés sur cesports*

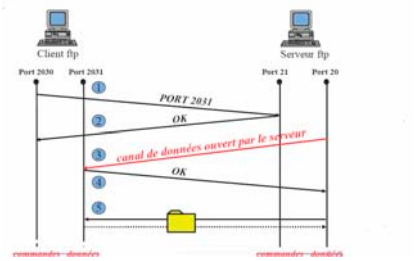
Remplacer par SSH (secure shell)

- ***Excellente solution de remplacement pour Telnet***
  - *Authentification par algorithme asymétrique*
  - *Chiffrement*
    - ➲_ *=> Non vulnérable à l'écoute Si SSH V2 utilisé*
- ***Peut déjouer de nombreuses attaques par spoofing IP car il y a authentification forte***
- ***Disponible sur divers sites Internet pour un grand nombre de plates-formes (SunOS, Linux)***
- ***Possibilité d'encapsuler d'autres protocoles au sein du tunnel SSH***

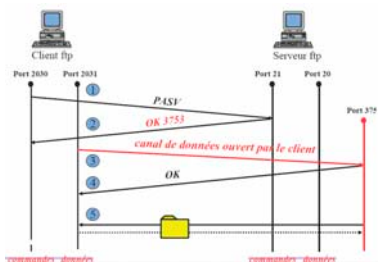
FTP: File Transfert Protocol

- ***FTP : le protocole standard de l'Internet pour le transfert defichiers (RFC 959) complété par d'autres RFC (RFC 2228,RFC 2640, RFC 2773)***
- ***Permet de transférer des fichiers d'un système à un autre ; compatible avec les différents systèmes de stockage de fichiers***
- ***Transfert fiable et efficace***

FTP Normal



FTP Passif



Principaux risque de FTP

- ***Transmission des mots de passe en clair***
- ***Pour les utilisateurs internes :***
  - *Exportation de documents internes confidentiels*
  - *Importer des fichiers dangereux (chevaux de Troie), des logiciels piratés, des jeux, des images pornographiques ...*
  - *occupation abusive des espaces disques;.*
- ***Pour les Serveurs :***
  - *Accès anonyme ou non permettant le dépôt de fichier transformera tôt ou tard le serveur en plaque tournante de contenu illicite*
  - *Accéder à des informations du système ou d'autres applicatifs en profitantd'un bogue du serveur FTP*

FTP: Les solutions

- ***Dédié une machine au serveur FTP***
- ***Restreindre les droits sur les fichiers servis***
- ***Faire passer les flux FTP via des proxies ou reverse-proxies afin de contrôler plus finement les actions autorisées (sites, commandes, authentification, etc...)***
- ***Ne jamais combiner les droits en ecture/écriture sur un répertoire***
- ***Utiliser FTP Security Extensions (RFC 2228) qui permet d'offrir une authentification forte, un contrôle d'intégrité et une confidentialité du canal de contrôle et celui de données***

TFTP : Trivial File Transfert Protocol

- ***Protocole standardisé de transfert de fichiers simplifié basé sur UDP (RFC 1350)***
- ***Conçu pour être installé sur les mémoires mortes des systèmes sans disques (terminaux X, stations de travail sans disque, routeurs)***
- ***Pas d'authentification, d'intégrité ou de confidentialité des données transmises (meilleur canal pour récupérer les mots de passe des routeurs)***
- ***A PROSCRIRE SUR LES FIREWALLS***

Résumé

- *Telnet (comme les commandes en R)est un protocole de transfert des données en clair.*
- *Ssh offre une alternative pour sécuriser le transfert de données.*
- *Ftp doit être sécurisé par authentification plus forte, SSL, VPN*

Voix sur IP: fonctionnement

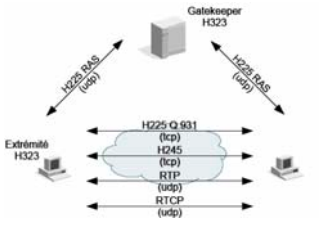
La téléphonie IP

- *H225 Remote Access*
  Serveur
  Enregistrement au
  Gatekeeper
- *H225/Q931:*

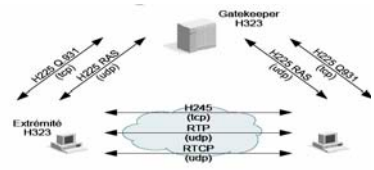
H.225 RAS	Signalisation H.225/Q.931	Contrôle H.245
UDP	TCP	
Couche réseau		
Couche liaison		

La téléphonie IP

Voix sur IP Signalisation Directe H323



Voix sur Ip: Signalisation routée vers le Gatekeeper H323



Voix sur Ip H323: un exemple d'utilisation en multipoint

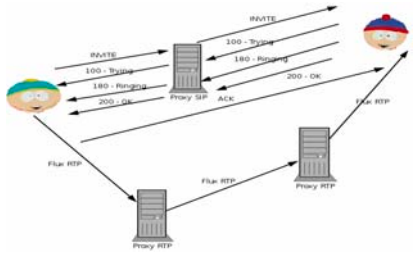
Voix sur Ip: Le protocole SIP

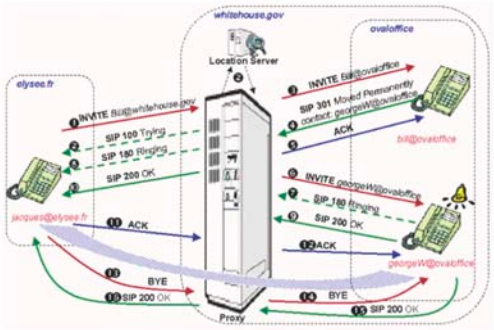
- *Protocole RFC 3261 tend à remplacer H323*
- *Sip intervient aux différentes phases de l'appel:*
  - *Localisation du terminal correspondant,*
  - *Analyse du profil et des ressources du destinataire,*
  - *Négociation du type de média (voix, vidéo, données...) et des paramètres de communication,*
  - *Disponibilité du correspondant, détermine si le poste appelé souhaite communiquer, et autorise l'appelant à le contacter.*
  - *Etablissement et suivi de l'appel, avertit les parties appelant et appelé de la demande d'ouverture de session, gestion du transfert et de la fermeture des appels.*
  - *Gestion de fonctions évoluées : cryptage, retour d'erreurs, ...*
  - *Compatible avec le multicast, via une unité de contrôle M.C.U (Multipoint Control Unit)*

Voix sur Ip: Les requêtes SIP

- *REGISTER : Enregistrement de localisation*
- *INVITE : Initier/Modifier une session*
- *ACK : Accusé de réception*
- *CANCEL : Annulation d'un INVITE en cours*
- *BYE : Finir une session*
- *OPTIONS : options proposées*
- *MESSAGE : Messagerie instantanée*

Voix sur Ip: Les requêtes SIP+RTP (Real Time Protocol)





Voix sur IP:
Quelle Implications pour la sécurité?

sommaire

le paradigme de la convergence

le rapide panorama des risques

la réalité des faits

la feuille de route de la remédiation

le paradigme de la convergence

on assiste à la convergence data/voix (et fixe/mobile) voire multi-média

on ne peut pas traiter de la sécurité de la Voix sur IP indépendamment du contexte data

la Voix sur IP s'insère dans un existant qui pèse lourd dans la sécurité de la Voix

la mutualisation des réseaux locaux et étendus, et des équipements, pèse sur la sécurité de la Voix ET des données

facteurs structurels et offres complexes

les facteurs structurels : *les protocoles ToIP (H.323, SIP, UDP) n'intègrent peu ou pas de protection par défaut*

- *niveau de sécurité offert parfois faible, car les standards sont encore en construction et les priorités initiales ne ciblaient pas la sécurité mais l'ouverture et la simplicité*
- *implémentations et utilisations des protocoles souvent complexes accrues par les évolutions rapides des protocoles.*

des implémentations perfectibles : *des versions de logiciel par plate-forme avec de nombreuses mises à jour en fonction des évolutions des protocoles, des architectures, des failles découvertes*

- *failles publiées de plus en plus nombreuses*
- *…et sûrement de plus en plus fréquentes avec l'arrivée des déploiements généralisés qui encouragent les hackers et constituent un banc d'essai plus puissant que les jeux de test en laboratoire.*

panorama des risques (1/2)

sabotages *: tenter d'interrompre un service*

- *virus sur les clients ou sur les serveurs attaquant directement le logiciel ou indirectement la plate-forme (OS)*
- *déni de service paralysie d'un composant en le submergeant de messages de service (GateKeeper)*
- *Nb : un remake de DoS web sur HTTP.*

intrusions *: capter des informations*

- *détournement de flux voix avec/sans modification par écoute/usurpation d'identité*
- *détournement /falsification de données de service : annuaire, ticket de consommation, historique*
- *Nb : analyse automatique simplifiée grâce aux outils data*
- *Nb : le phishing via VoIP arrive*

panorama des risques (2/2)

détournements *: utiliser l'infrastructure pour en tirer bénéfice*

- *fraude de consommation, usurpation de compte ou modification des tickets*
- *plate-forme de blanchiment, usurpation de compte ou modification des tickets pour masquer une opération.*
- *Nb : à quand le voice SPAM à 2 heures du matin ☺*

et si on parlait de… *: Skype et autres P2P voice à venir*

- *préemption de ressources qui peuvent conduire au DoS*
- *protocoles obscurcis qui laissent soupçonner l'intrusion*
- *le détournement de ressources pour permettre la « gratuité »*

fait 1 : la sécurité de la ToIP ne peut pas être isolée…

la téléphonie est un des services convergents, au même titre que …

- *La Messagerie*
- *La Visio Vidéo*
- *Le Collaboratif*
- *L'Instant Messaging et les SMS on line.*

conséquences : Multiplication …

- *des protocoles applicatifs*
- *de la pression sur les serveurs techniques (DNS, DHCP, annuaire)*
- *des équipements connectés*

fait 2 : Les menaces existent… mais elles doivent être comprises et anticipées

***détournement de trafic**, parce que ces ressources ont un prix…*

.

***écoute**, parce que les utilisateurs sont moins attentifs…*

.

***déni de service,** parce que les call-centers sont des points névralgiques…*

fait 3 : les architectures convergentes sont très diversifiées…

IPABX sur site

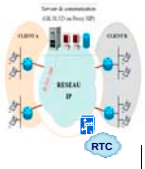
- *Équipement d'extrémité (IPBX ou PABX + passerelles IP/RTC) installé sur chaque site client, raccordé au RTC.*

IPABX centralisé

- *Fonction PABX assurée par un serveur centralisé*
- *Sites distants équipés de postes IP et de passerelle (GW) raccordés sur le LAN*

IP Centrex

- *Fonction PABX hébergée au sein du réseau opérateur (Gatekeeper)*
- *Sites clients équipés de postes téléphoniques IP raccordés sur le LAN*



fait 4 La convergence est un projet

Prise en compte de l'existant

- *Postes de travail*
- *Lan*
- *Wan*
- *Les locaux techniques*
- *Les serveurs techniques (annuaire, dns, dhcp)*

Prise en compte des organisations

- *Les processus de provisionning et d'administration*
- *Les nomades*
- *Les filiales*
- *Les environnements ouverts (salles, expos, etc)*

La feuille de route de la remédiation

Anticiper par des contre-mesures génériques

(Re)mettre l'environnement utilisateur sous contrôle

(Re)étudier l'impact sur l'environnement local

Adapter sur architecture d'interconnexion

Re)voir l'architecture partagée de sécurité

Déployer l'architecture de sécurité des services IP

Mettre en place la structure de management de la sécurité des services IP

anticiper par des contre-mesures génériques

Démarche transverse de test et validation des solutions en laboratoire, voire aller jusqu'à la certifcation

Démarche d'audit de l'environnement cible

Formation des équipes

Observatoire permanent des failles et correctifs pour diffuser les mesures

Développer un pôle d'expertise pour étudier et valider les interfaces et les systèmes de sécurité

(re) mettre l'environnement utilisateur sous contrôle

Limiter les services de voix suspects

Adapter les solutions de protection personnelle
(anti-virus, anti-spyware,Personnal Firewall)

Renforcer la politique d'authentification
- *Par 802.1X (Standart IEEE)*
- *Et/ou Authentification Radius*

Durcir les solutions de IP phone et softphone sécurisées
- *Firmware signé*
- *Verrouillage Adresse MAC*

Adapter les règles de mobilité avec :
- *Mobile VLAN : basé sur le Port, Mac, Protocole, Subnet, règle de DHCP.*
- *Et/Ou Passerelle + VPN dédié*

Crypter les flux poste - Serveur :
- *Flux média*
- *Flux signalisation*

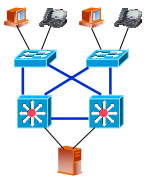
revoir l'environnement local

Protection Physique (Lieu)
- *Les routeurs, commutateurs, Communications Servers, Media Gateway doivent être protégés contre les accès physiques non autorisés.*
- *Eliminer les Hubs au profit de Switch*

Paramétrage de VLAN et de leur priorisation sur le Switch :
- *VLAN « téléphonie », construit par port, sera constitué des ports sur lesquels sont branchés les téléphones IP (protégés contre les broadcast storm, le sniffing et les attaques provenant du VLAN Data.*
- *VLAN « data », construit par port, sera constitué des ports sur lesquels sont branchés les PC. (Aucun flux Data permis (pas d'attaque DoS possible, pas de packets sniffing depuis un PC vers un Vlan Voix)*
- *VLAN « Administration » (consoles des admin. Réseaux, systèmes, sécurité)*
- *Mettre Disable ou placer les ports inutilisés dans un VLAN isolé*

revoir l'environnement local

Lorsqu'un modem est utilisé pour la maintenance
- *Eteignez-le quand il n'est pas nécessaire*
- *Faire l'audit usage de chaque connexion distante (remote connection)*



Attention particulière à l'énergie pour la continuité de service
- *Un IP phone consomme 1.000 fois plus*
- *Un switch consomme 1.000 watt*
- *PoE a des limites sauf en coût ☺*

adapter sur architecture d'interconnexion

Vérifier l'étanchéité des flux (Pourquoi pas une Certification ?)

Dissocier les flux par des VPN de service

Restreindre le routage entre les subnets Voix et Dat

Protéger les interconnections (DMZ,Firewall)

Crypter les liens inter-sites (IPsec)

revoir l'architecture partagée de sécurité

Utiliser des DHCP serveurs séparés
- *Un pour la Voix (IP phones)*
- *Un pour la Data (PCs)*

Segmenter les flux pour isoler les impacts d'attaques
- *Rate limiting*

***Dissocier serveurs opérationnels vs serveurs d'administration** (si possible)*
- *Call Manager*
- *Web d'administration*
- *Web utilisateur*

revoir l'architecture partagée de sécurité

Structurer les principes d'Administration
- *Par du management chiffré*
  - *SSH v2*
  - *SNMP v3 (2006 OXE)*
  - *HTTPS (SSL v2/v3)*
- *Gestion des users et passwords (longueur minimale, durée)*
- *Authentification forte des administrateurs*

déployer l'architecture de sécurité des services IP

Renforcer l'authentification serveur

Intégrer des Firewall optimisés

Choix de technologie : VoIP aware (H323,SiP), ***Stateful Inspection (Appliance)***

Pour réduire la latence due au filtrage des multiples polices => règles Voix sont en première position dans la table de filtrage

WARNING 1 : *Si le FW n'est pas entièrement compatible H.323/SIP, les communications téléphoniques seront totalement ou en partie bloquées.*

WARNING 2 : *en environnement hétérogènes les spécifités des protocoles génèrent une complexité*

- *Activer les fonctions anti-DoS des call manager*

déployer l'architecture de sécurité des services IP

Protéger les serveurs

Règles d'installation et de durcissement de l'OS

Application régulière des patch de sécurité (masters, sites en délégation d'exploitation)

Anti-virus,CSA,Anti-spyware, etc

Mise en œuvre de configurations spécifiques sur les produits de l'écosystème

Détection de fraude sur la taxation

Logiciel de vérification de configuration

mettre en place un management pro-actif

Développer une politique de sécurité et faire des évaluations

Evaluations Typiques PBX : politique de sécurité, accés physique, configuration du système etc.

Effectuer la consolidation des historiques (Syslog)

Vérifier périodiquement la politique de sécurité

Surveiller les flux par IDS (Intrusion Dectection System)

Systèmes de Défense Pro-Actifs en ligne

- *Analyse de comportement, protège les Serveur de communication contre les intrusions (basé sur des signatures, l'analyse de protocoles …)*
- *Elimine ces paquets et bloque tout le trafic associé à cette session (IPS)*

Prévoir une plateforme de délestage

résumé

Déployer des mécanismes de sécurité dès la conception des services
- *mécanismes IP traditionnels, mécanismes VoIP*

Tester le niveau de sécurité des équipements déployés
- *audit de code, tests intrusifs*

Sécuriser tous les équipements
- *usages incontournables de certificat, protection des équipements « hôtes » (PC, serveur)*

Manager l'évolution de son architecture
- *suivre la publication de vulnérabilité et appliquer les patchs 24h/24, 7j/7*

Faire évoluer son organisation
- *procédure incluant la téléphonie et les postes*
- *formation – rapprochement des équipes*

