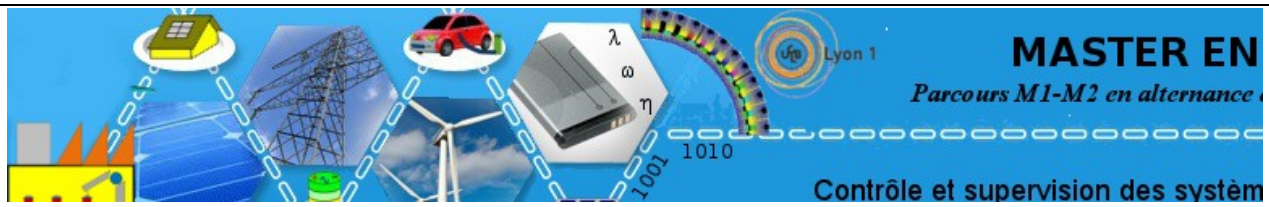


Master Energie, Sécurité des Réseaux, Jean-Marc THIRIET

Jean-marc.thiriet@univ-grenoble-alpes.fr

CHAPITRE 1. Analyse de risques

Sécurité physique

- Normes de sécurité
- Protection des sources énergétiques (alimentation…)
- Protection de l'environnement (incendie, température, humidité…)
- Protection des accès
  - Protection physique des équipements
  - Locaux de répartition
  - Tableaux de connexion, infrastructure câblée,
  - Traçabilité des accès dans les locaux
- Sûreté de fonctionnement et fiabilité des matériels
- Redondance physique
- Marquage des matériels
- Plans de maintenance préventive (tests…) et corrective (pièces de rechange…)

Sécurité de l'exploitation

- = bon fonctionnement du système
- Plan de sauvegarde
- Plan de secours
- Plan de continuité
- Plan de tests
- Inventaires réguliers et si possible dynamiques
- Gestion du parc informatique
- Gestion des configurations et des mises à jour
- Gestion des incidents et suivis jusqu'à leur résolution
- Automatisation, contrôle et suivi de l'exploitation
- Analyse des fichiers de journalisation et de comptabilité
- Gestion des contrats de maintenance
- Séparation des environnements de développement, d'industrialisation et de production des applicatifs
- Connectivité fiable et de qualité
- Infrastructure réseau sécurisée

Sécurité logique

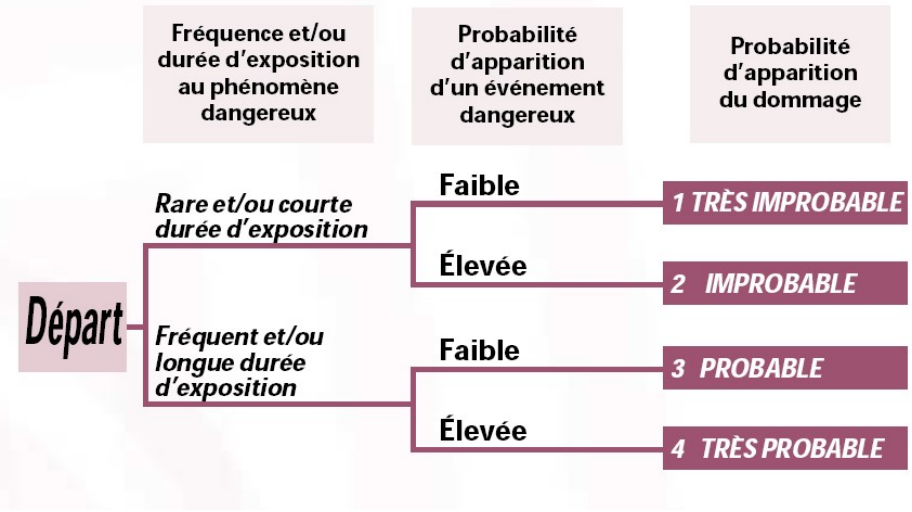
- Mécanismes de sécurité par logiciel
  - Identification
  - Authentification
  - Autorisation
- Dispositifs mis en place pour garantir la confidentialité et l'intégrité
  - Cryptographie
  - Gestion efficace des mots de passe
  - Antivirus
  - Sauvegarde des informations sensibles
- Classification des données
  - Degré de sensibilité (normale, confidentielle…)

Sécurité applicative

- Méthodologie de développement (respect des normes de développement propres à la technologie employée)
- Robustesse des applications
- Contrôles programmés, tests
- Sécurité des progiciels (choix des fournisseurs, interface de sécurité)
- Contrats avec les sous-traitants (clauses d'engagement de responsabilité)
- Plan de migration des applications critiques
- Validation et audit des programmes
- Qualité et pertinence des données
- Plan d'assurance sécurité

TD-1. Approche pour l'analyse de risques

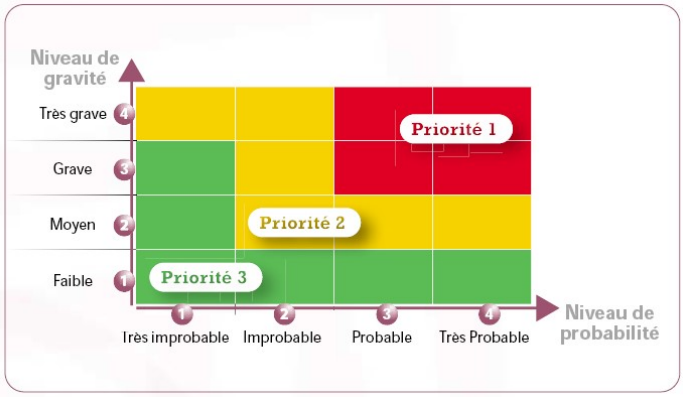
1. Estimation de la **probabilité** d'occurrence d'une défaillance



Depending on the type of company or the application, sometimes we take into account only the frequency and/or the duration of the danger:

1. very improbable (once per year)
2. improbable (once per month)
3. probable (once per week)
4. very probable (once per day)

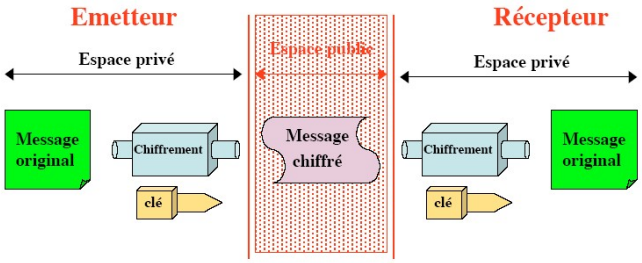
2. Risks evaluation, evaluation of the **gravity**



3. Frame for the risks analysis

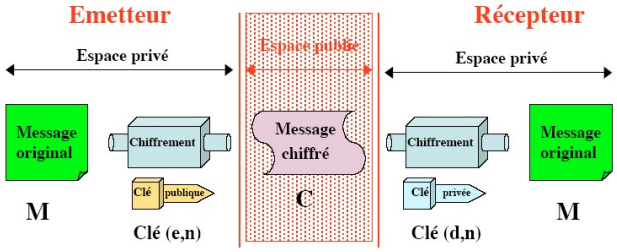
Danger (cause)	Dangerous situation	Dangerous event	Risk of…	Consequence	Risk estimation		Risk evaluation	Observations (what to do?)
					Severity (1 to 4)	**Proba** (1 to 4)	Priorities (1 to 3)	

CHAPITRE 2. CRYPTOGRAPHIE



✓**La même clé est utilisée pour chiffrer et déchiffrer**
✓**Problème : TRANSFERT de la clé**

Figure 1 : Chiffrement : type symétrique (clé privée)



✓**Le chiffrement est effectué avec la clé publique**
✓**Garantie : que « SEUL » le détenteur de la clé privée peut lire le message**

Figure 2 : Chiffrement : type asymétrique (clé publique)

- Soit un alphabet {A, B, C, D}

texte t / clé k	A B C D
A	C D B A
B	D C A B
C	C A B D
D	B D A C

Texte clair : ABCBACCBA ACBB
Clé : DBBCBAACD DBBC

Texte crypté : BCAADBBAB BACA

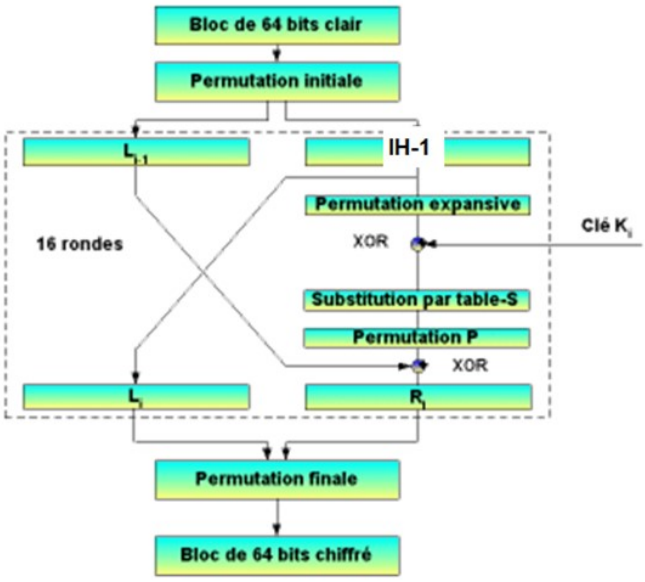
- Nécessite des clés de très grande taille pour être peu vulnérable…

Figure 3 : Exemples de codage : les codes poly-alphabétiques

- $(b_n) = (2, 6, 3, 2, 1, 0, 5, 0, 3, 7)$
- F= 01001010 10010101 00101001 00010100 11010110 11110001
- Et
- F'= 01101000 10000101 00001001 01010100 01010010 01100000

Bit 2 Bit 6 Bit 3 Bit 2 …

Figure 4 : Inversion de bits suivant une suite aléatoire : exemple



Application des Algorithmes asymétriques

- https://www.cs.drexel.edu/~jpopyack/IntroCS/HW/RSAWorksheet.html
- On va encrypter le message '**HELLO**'. On va prendre le code ASCII (en décimal) de chaque caractère et on les met bout à bout:
  - **m = 72-69-76-76-79 (en base 10)**
- Ensuite, il faut découper le message en blocs qui comportent moins de chiffres que **n**.
- **n** comporte 4 chiffres, on va donc découper notre message en blocs de 3 chiffres:
  - 726 976 767 900
    (on complète avec des zéros)
- Ensuite on encrypte chacun de ces blocs:
  - 726^13 mod **21209** = 11600
    976^13 mod **21209** = 5705
    767^13 mod **21209** = 16590
    900^13 mod **21209** = 3565
    Le message encrypté est **11600.5705.16590.3565**. On peut le décrypter avec d:
  - 11600^1609 mod **21209** = 726 (si 1 bit est corrompu 11601^1609 mod 21209 = 6051)
    5705^1609 mod **21209** = 976
    16590^1609 mod **21209** = 767
    3565^1609 mod **21209** = 900
- C'est à dire la suite de chiffre **726976767900**.
  On retrouve notre message en clair **72 69 76 76 79** : '**HELLO**'.

Cryptage asymétrique : Génération d'une clé de partage

- Deux utilisateurs vont concevoir une clé commune qui ne servira qu'à eux seuls

ASPECT ASSYMETRIQUE

- Ils choisissent un nombre premier p et un entier a (a et p n'étant pas forcément confidentiels)
- Ensuite chacun choisit un entier X appartenant à [1, p-1] et calcule l'entier $Y=a^X \bmod p$
- On obtient deux couples (X_1,Y_1) et (X_2, Y_2) où les valeurs Y_1 et Y_2 vont être publiées

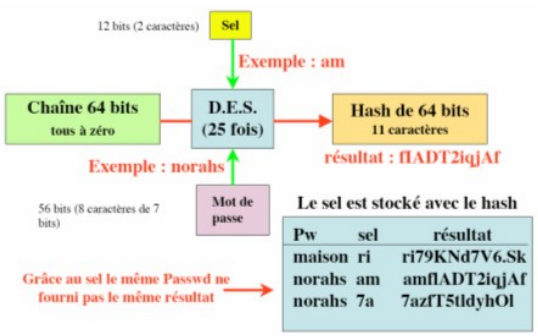
ASPECT HYBRIDE

- Chacun d'eux peut alors calculer la clé $c=a^{X1.X2} \bmod p$ car $c=(Y1^{X2} \bmod p)=(Y2^{X1} \bmod p)$
- R : Chacun ignore le X de l'autre
- La sécurité vient du fait qu'il est impossible en un temps raisonnable de découvrir la clé c par le calcul d'un logarithme discret (infaisable en un temps raisonnable compte tenu de la taille de p)

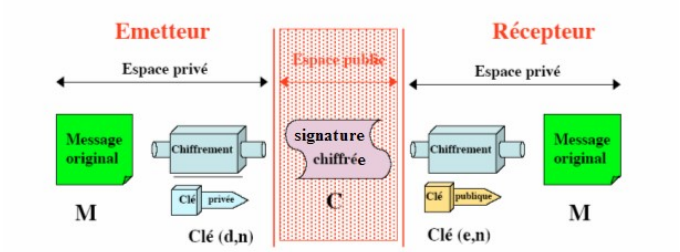
ASPECT SYMETRIQUE

- Les utilisateurs peuvent maintenant échanger leurs données de manière cryptée en utilisant un système symétrique grâce à la clé commune c.

- Le hash consiste à crypter 25 fois une chaîne de caractère vide, en utilisant le mot de passe comme clé
- Par exemple : DES utilise une clé de 56 bits, donc 7 bits sont pris sur le mot de passe et les caractères après le 8ème sont ignorés
- Un « gain de sel » est ajouté afin d'éviter que le même mot de passe utilisé par deux utilisateurs différents ne génère la même somme de contrôle



- Hash sur un système Unix



✓**Pour signer un message, on peut le chiffrer avec la clé privée !**

✓**Le déchiffrement avec la clé publique prouve que seul le détenteur de la clé privée a pu créer la signature.**

✓**Signer un message = chiffrer un message**

- Il n'est pas nécessaire de chiffrer un message complet pour le signer, il suffit de chiffrer son « hash »
- La résistance aux collisions de la fonction de « hashage » garantit que c'est bien ce document qui a été signé

Figure 6 : Principes de signature

Principaux paramètres d'un certificat numérique selon norme X509v3

1. Version du certificat
2. Numéro de série
3. Algorithme utilisé pour signer le certificat
4. Nom de l'organisme qui a géré le certificat
   - Le couple numéro de série-nom de l'organisme doit être unique
5. Période de validité
6. Nom du propriétaire du certificat
7. Clé publique du propriétaire
8. Informations additionnelles concernant le propriétaire ou les mécanismes de chiffrement
9. Signature du certificat
10. Algorithme et paramètres utilisés pour la signature ainsi que la signature

TD 2 Chiffrement

Ex 1 : Cryptage : Inversion des bits suivant une suite aléatoire

Crypter “MASTER” (M=’4D’, A=’41’, S=’53’, T=’54’, E=’45’, R=’52’ en code ASCII hexadécimal) avec la clé (suite aléatoire) (a_n) = (11,20,3,19,24,33,4,145,69,15…) en utilisant la méthode de l'inversion des bits suivant une suite aléatoire sur des paquets de 8 bits.

Ex 2 : Principe de Kerckhoffs

En 1883, Auguste Kerckhoffs a établi un principe fondamental de la cryptographie : "il faut qu'un système cryptographique n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi". Expliquer ce principe.

Ex 3 : Recherche exhaustive (attaque par force brute) de clefs symétriques

Sachant qu’une certaine machine peut tester en moyenne 400 000 combinaisons par seconde, de combien de temps a besoin cette machine pour retrouver par une recherche exhaustive une clé de 56 bits, combien de temps mettrait-elle pour trouver une clé de 40 bits ? une clé de 112 bits ?

Ex 4 : Chiffrement symétrique et asymétrique

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

1. Quel est le nombre minimal de clés symétriques nécessaires ?
2. Donner le nom d'un algorithme de chiffrement symétrique reconnu.

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

3. Quel est le nombre minimal de couples de clés asymétriques nécessaires pour que chaque membre puisse envoyer et recevoir des informations chiffrées et/ou signées ? Si l'on considère que chacun peut communiquer avec tout le monde, combien de clés privées et publiques chaque utilisateur devra-t-il détenir
4. Bob souhaite envoyer des informations chiffrées et signées à Alice (Bob et Alice appartiennent tous les deux au groupe). Quelle(s) clé(s) Bob doit-il utiliser ?
5. Donner le nom d'un algorithme de chiffrement asymétrique reconnu.

Le groupe décide finalement d'utiliser un système hybride pour le chiffrement (c'est-à-dire qui utilise la cryptographie symétrique et asymétrique).

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

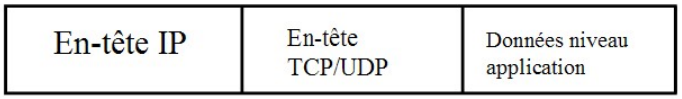
Ex 5 : Perte d'une clé privée

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

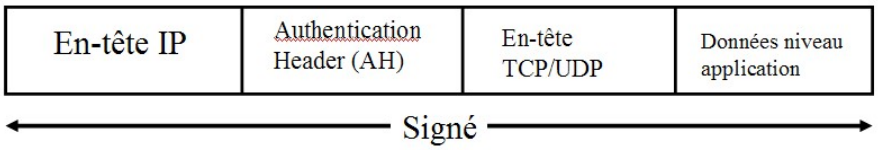
1. Peut-il encore envoyer des courriers électroniques chiffrés ? Décrypter les messages reçus ?
2. Peut-il encore signer les courriers électroniques qu'il envoie ? Vérifier les signatures des courriers électroniques qu'il reçoit ?
3. A quoi peut encore servir la clé publique de notre utilisateur ?
4. Que doit-il faire pour être à nouveau capable d'effectuer toutes les opérations mentionnées ci-dessus ?

CHAPITRE 3. PROTOCOLES DE SECURITE

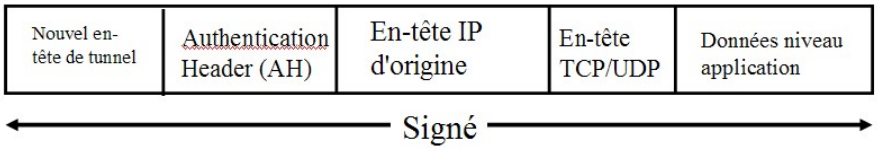
trame IPv4



trame AH en mode transport

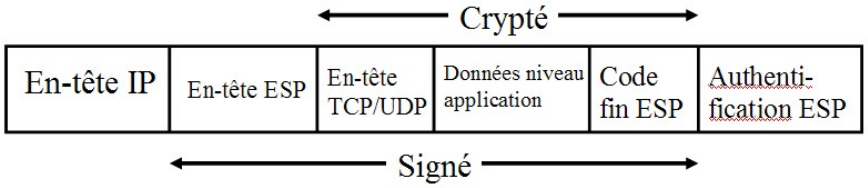


trame AH en mode tunnel

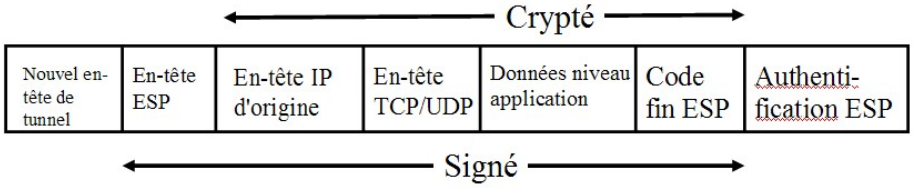


Protocole AH

- Format d'une trame ESP en mode transport



- Format d'une trame ESP en mode tunnel



Protocole ESP

Stratégies IPSec par défaut

(ex Windows Server)

- Client (en réponse seule)
  - Permet de faire transiter le trafic normalement, une seule règle "règle de réponse par défaut", permettant de négocier le trafic IPSec si l'hôte distant le propose
- Serveur (demander la sécurité)
  - Règle 1 : négociation pour le trafic IPSec entrant comme sortant ; si la machine distante ne prend pas IPSec => communication non sécurisée
  - Règle 2 : transmission du trafic ICMP sans négociation de sécurité
  - Règle 3 : règle de réponse par défaut (voir ci-dessus)
- Serveur (nécessite la sécurité)
  - Règle 1 : négociation pour le trafic IPSec entrant comme sortant ; si la machine distante ne prend pas IPSec => communication interrompue
  - Règle 2 : transmission du trafic ICMP sans négociation de sécurité
  - Règle 3 : règle de réponse par défaut (voir ci-dessus)
- Règle de réponse par défaut

– Permet de négocier la sécurité avec tout hôte désirant communiquer de façon sécurisée

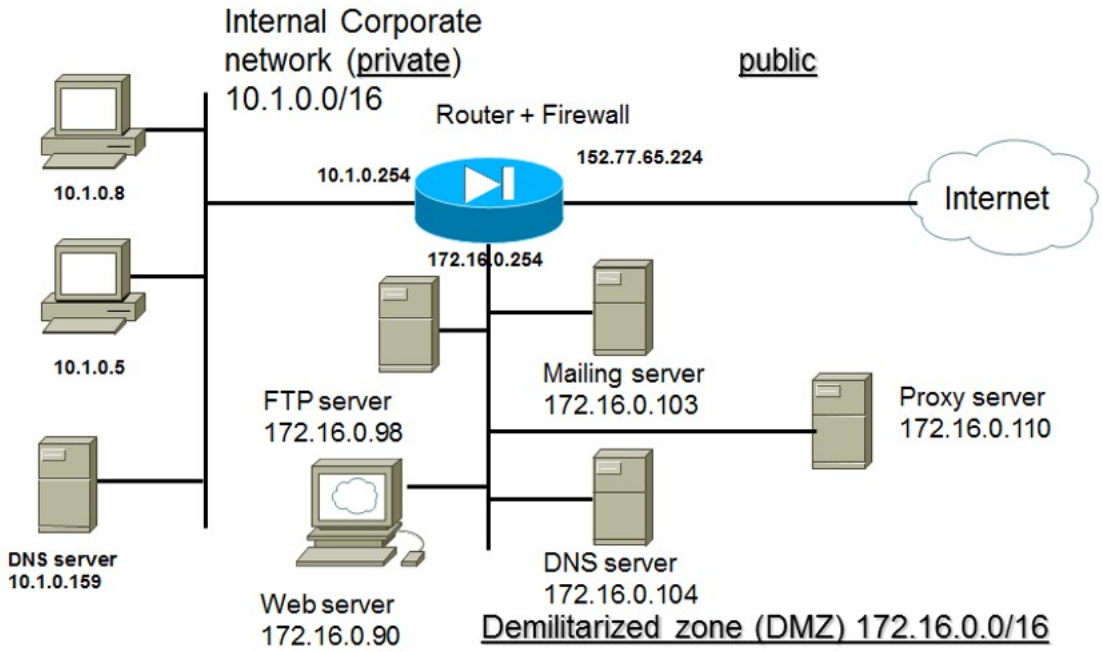
Sens du trafic 	**Aucune stratégie**	**Stratégie client (en réponse seule)**	**Stratégie serveur (demander la sécurité)**	**Stratégie serveur (nécessite la sécurité)**
Aucune stratégie	Non sécurisé	Non sécurisé	Non sécurisé	Echec
Stratégie client (en réponse seule)	Non sécurisé	Non sécurisé	Sécurisé (1)	Sécurisé (1)
Stratégie serveur (demander la sécurité)	Non sécurisé	Sécurisé	Sécurisé	Sécurisé
Stratégie serveur (nécessite la sécurité)	Echec	Sécurisé	Sécurisé	Sécurisé

Examen de l'interaction entre les règles

Chapitre 4 : Types d'attaques

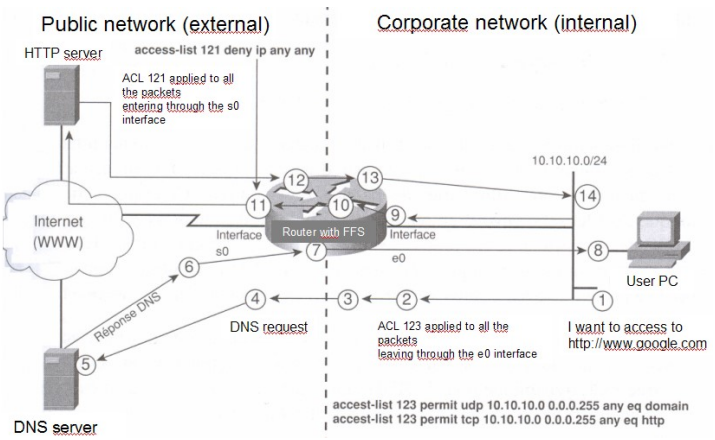
- DoS (Denial of service, déni de service) : Faire décroître la capacité du système
- DDoS (Distributed DoS) : idem mais avec une attaque provenant de plusieurs emplacements (http://grc.com/dos/grcdos.htm)
- SYN Flood: l'attaquant inonde un système de paquets de synchronisation SYN afin d'initier des requêtes de connexion jamais terminées => forte exploitation des ressources processeur, mémoire, carte réseau => déni de service
- UDP Flood: attaque qui submerge un système de paquets UDP et le ralentit pour l'empêcher de traiter les demandes de connexion valides (souvent sur le port 53 DNS) (ICMP Flood : idem pour submerger un système de messages ICMP (Internet Control Message Protocol) en utilisant l'utilitaire Ping)
- Scan de ports : Paquets envoyés en utilisant des numéros de port afin de scanner les services disponibles dans l'espoir qu'un port réponde
- Ping of Death: possibilité de « pinger » avec un paquet d'une taille exagérément démesurée pouvant provoquer tout un éventail de réactions incontrôlées de la part du système ciblé : déni de service, plantage, gel ou redémarrage
- Eavesdropping : le but est de violer la confidentialité de la communication (en sniffant des paquets sur le réseau local ou en interceptant des communications sans fil)
- Man-in-the-middle : l'attaquant agit envers les deux extrémités de la communication comme s'il était l'interlocuteur attendu : conséquences néfastes sur la confidentialité et éventuellement l'intégrité
- Java/ActiveX/ZIP/EXE: composants Java ou Active X malveillants cachés dans des pages Web, chevaux de Troie dissimulé dans un fichier ZIP/TAR ou EXE
- Breaking into a system: en violant l'authentification ou le contrôle d'accès, l'attaquant obtient la possibilité de contrôler la communication : conséquences sur la confidentialité et l'intégrité
- Virus : court-circuite l'authentification et le contrôle d'accès dans le but d'exécuter du code destructeur : conséquences sur la disponibilité de la machine et/ou du réseau
- Chevaux de Troie (trojan) : virus caché dans une fonction habituellement utilisée, programme s'exécutant sur la machine piratée pour envoyer de l'information au pirate
- Vers (Worm) : explore et exploite automatiquement les failles d'un système, sans action d'utilisateur : entraîne des problèmes de disponibilité
- TOIP : 3 types d'attaques (Over IP, Voicemail (répondeur), Administrateur)

Chapitre 5 : Pare-feu, notion de zone démilitarisée



Example of filtering rules

```
ip address 192.168.254.1/30
ip address group 121 in
access-list 121 permit tcp any any eq 22
access-list 121 permit udp any any gt 1023
access-list 121 permit icmp any any gt 1023
access-list 121 permit icmp any any echo-reply
access-list 121 permit icmp any any time-exceeded
access-list 121 permit icmp any any packet-too-big
access-list 121 permit tcp any 64.24.14.60 eq ftp
access-list 121 permit tcp any 64.24.14.61 eq smtp
access-list 121 permit tcp any 64.24.14.61 eq domain
access-list 121 permit udp 64.24.14.61 eq domain
```



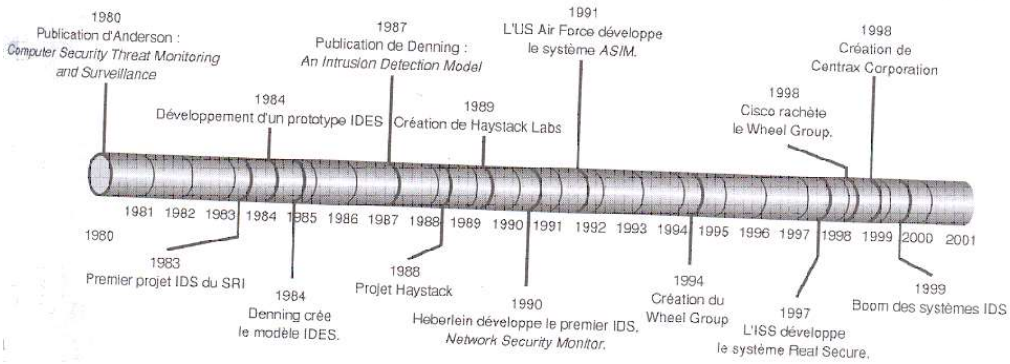
Principe de base pour la configuration d'un pare-feu

- Moindre privilège : ne pas accorder aux utilisateurs du réseau protégé par le pare-feu des droits dont ils n'ont pas la nécessité ; interdire par exemple le peer-to-peer dans le cadre d'une entreprise
- Interdiction par défaut : interdire par défaut tout transit à travers le pare-feu et ne laisser passer que celui qui est explicitement autorisé, évitant ainsi tout transit involontairement intercepté
- Défense en profondeur : utiliser les moyens de protection à tous les niveaux possibles, par exemple en analysant et filtrant tout ce qui peut l'être au niveau du pare-feu. Ce principe évite de laisser entrer dans le réseau des communications indésirables, même si un autre moyen de contrôle est utilisé plus en profondeur dans le réseau
- Goulet d'étranglement : toutes les communications entrant et sortant du réseau doivent transiter par le pare-feu. Il ne faut pas de points d'entrée ou de sortie du réseau non contrôlés, comme par exemple des modems sauvages
- Simplicité : les règles de filtrage du pare-feu doivent être les plus simples et les plus compréhensibles possibles afin d'éviter toute erreur de la part de l'administrateur ou de ses successeurs
- Participation des utilisateurs : les utilisateurs doivent être impliqués dans la mise en place du pare-feu. Ils doivent en effet exprimer leurs besoins et recevoir en échange les raisons et les objectifs de l'installation d'un tel dispositif ; les contraintes afférentes au pare-feu seront ainsi mieux acceptées.

Rappel : adressage privé

- Adresses de l'internet (IPv4)
  - Théorie, 2^{32} adresses (~4,3 Mds d'adresse)
  - Pratique
    - Adresses publiques : ~3,2 Mds
    - Adresses réservées : test…
    - Adresses privées : réservées pour les réseaux internes (non accessibles de l'extérieur)
      - 10.0.0.0 à 10.255.255.255 (préfixe 10/8)
      - 172.16.0.0 à 172.31.255.255 (préfixe 172.16/12)
      - 192.168.0.0 à 192.168.255.255 (préfixe 192.168/16)

CHAPITRE 6 : systèmes de détection d'intrusion



Historique du développement des IDS

NIDS (réseaux) : Network-based ID systems, Détection d'intrusion basée réseau (NIDS) : le NIDS réside sur un segment discret du réseau et surveille le trafic sur ce segment. Il consiste habituellement en un matériel réseau avec une carte réseau (NIC) qui *intercepte et analyse* les paquets réseau en temps réel. Les cartes d'interface réseau sont en général en mode promiscuité (promiscuous mode), elles sont alors en mode « furtif » afin qu'elles n'aient pas d'adresse IP.

HIDS (hôtes) : Host-based ID systems (systèmes de détection d'intrusion basé sur l'hôte): utilise de petits programmes qui résident sur un hôte (serveur web, serveur messagerie…) :

- Supervise le système d'exploitation
- Détecte les activités inapropriées
- Écrit dans les fichiers de log (historiques)
- Déclenche des alarmes

IDSs basés sur la signature

- *Signature-based IDSs*: signature ou stockage des attributs caractérisant une attaque

Signatures basées sur les anomalies ou le comportement

- *Statistical anomaly-based or behavior-based IDSs*: détecte dynamiquement les déviations par rapport aux motifs appris (comportement normal de l'utilisateur) et déclenche une alarme lorsqu'une tentative d'intrusion se déroule

Pots de miel

- Honeyd http://www.honeyd.org
- Projet Honeynet http://www.honeypot.net

Evaluation des vulnérabilités et test de pénétration internes

Méthodologie d'évaluation

- Doit être conduite sur site
- Doit se concentrer sur les risques internes associés aux stratégies, procédures, hôtes et applications
- Actions minimales à effectuer (voir transparents)

Evaluation des vulnérabilités et test de pénétration externes

Les mêmes qu'en interne +

- Évaluation conduite là où le réseau interagit avec l'extérieur
  - Connexions à internet
  - Réseaux sans fil
  - Systèmes de téléphonie
- On retrouve tout ce qui a été dit pour les attaques internes +
  - Recourir aux techniques de firewalking, wardialing et wardriving le cas échéant
- Il est pertinent d'envisager simultanément une évaluation interne et externe

Outils d'analyse des vulnérabilités

- Nessus: www.nessus.org, www.tenable.com
- Retina : www.eeye.com
- Open VAS : www.openvas.org
- SAINT : http://saintcorporation.com
- GFI Languard: www.gfi.com
- Qualys FreeScan: www.qualys.com
- Core Impact: www.coresecurity.com
- MBSA: http://technet.microsoft.com
- Wikto: www.sensepost.com
- Nikto: http://cirt.net/niko2
- WebInspect: http://download.spidynamics.com/webinspect/default.html
- Acunetix: www.acunetix.com
- SecurityMetrics (mobile) : www.securitymetrics.com
- Retina for mobile: www.beyondtrust.com

Outils de tests de pénétration

- Core Impact
- Metasploit
- ExploitTree
- CANVAS

Chapitre 7. Stratégies et politique de sécurité

- La politique de sécurité exprime une volonté de la part de la direction de protéger les valeurs informationnelles et les ressources technologiques
- Cette protection sera assurée par:
  - Règles (classification de l'information)
  - Outils : chiffrement, pare-feu…
  - Contrats : clauses et obligations
  - Enregistrement, preuve, authentification, identification, marquage, tatouage…
  - Dépôts de marques, brevets, protection de droit d'auteur
- En complément, elle pourra prévoir :
  - De dissuader par des règles et des contrôles
  - De réagir par l'existence de plans de secours, de continuité et de reprise
  - De gérer des incidents majeurs par un plan de gestion de crise
  - De poursuivre en justice
  - De gérer les performances et attentes des utilisateurs (=> c'est en fait ici de l'administration)

Définition de la politique de sécurité

- Simple et compréhensible
- Adoptable par un personnel préalablement sensibilisé voire formé
- Aisément réalisable
- De maintenance facile
- Vérifiable et contrôlable (périodiquement)
- Configurable et personnalisable (selon les profils des utilisateurs, les flux, le contexte, la localisation des acteurs)
- Dimension temporelle : jours ouvrés, heures de travail
- Dimension spatiale : nomadisme de certains utilisateurs

Certification ISO et sécurité

- Exemple: ISO 17799/27002 (Code de pratique pour la gestion de sécurité d'information), www.iso.org
- Planification de la continuation de l'activité
  - L'entreprise doit continuer à fonctionner normalement suite à une défaillance ou un incident majeur
- Contrôle de l'accès au système
  - Définit comment contrôler les informations
  - Définit comment détecter les activités non autorisées
- Développement et maintenance des systèmes
  - Processus de sécurisation des systèmes, logiciels, données
- Sécurité physique et environnementale
  - Protéger contre tout accès non autorisé ou action nuisible
- Conformité
  - À la loi
  - Aux règles de sécurité
- Sécurité du personnel
  - Risque d'erreurs humaines
  - Vols
  - Mauvaise utilisation
- Organisation de la sécurité
  - Décrit comment la maintenir et la gérer
- Gestion des ordinateurs et des opérations
  - Décrit comment augmenter la sécurité
- Classification et contrôle des biens
  - Appliquer et maintenir le degré de protection approprié aux données et informations de l'entreprise
- Adoption de la norme favorisée par le fait que certaines compagnies d'assurance l'imposent
  - Basée sur la gestion des risques
- Code de pratique pour la gestion de la sécurité et identification d'exigences de sécurité
  - Mais ne précise pas les manières de les réaliser
- Cette norme aborde les aspects organisationnels, humains, juridiques et technologiques
- Etape de conception, mise en œuvre et maintien de la sécurité
- www.iso.org

Domaine de sécurité de la norme ISO 17799

1. Politique de sécurité
2. Organisation de la sécurité
3. Classification et contrôle des outils
4. Sécurité et gestion des ressources humaines
5. Sécurité physique et environnementale
6. Exploitation et gestion de systèmes et de réseaux
7. Contrôle d'accès
8. Développement et maintenance des systèmes
9. Continuité de service
10. Conformité

Méthodes

- Méthodes préconisées par le CLUSIF (Club de la Sécurité de l'Information Français, http://www.clusif.asso.fr/) :
- Marion (Méthode d'Analyse des Risques Informatiques et Optimisation par Niveau)
- Méhari (Méthode Harmonisée d'Analyse des Risques)
- Méthodes de la DCSSI (Direction centrale de la sécurité des systèmes d'information : http://www.ssi.gouv.fr/fr/dcssi/)
- AFAI (Association Française de l'Audit et du Conseil Informatique), branche française de l'ISACA (Information Systems Audit and Control Association) => méthode de gouvernance et d'audit des systèmes d'information (CobiT : Control objectives for information and Technology)
- Méthode Octave

Spécification d'une stratégie de sécurité

Mission sécurité

- Concevoir un plan de sécurité en fonction d'une analyse préalable des risques
- Périmètre de vulnérabilité lié à l'usage des nouvelles technologies
- Niveau de protection adapté aux risques encourus
- Mise en œuvre et validation de l'organisation, des mesures, des outils et procédures de sécurité
- Suivi, audit, contrôle, faire évoluer le système d'information et sa sécurité
- Optimisation des performances du système d'information en fonction du niveau de sécurité requis
- Aligner les besoins avec les risques et les coûts

Principes de bases

- Principe de vocabulaire : langage commun pour la sécurité
- Principe de cohérence : intégration harmonieuse des outils (pas de juxtaposition…)
- Principe de volonté directoriale : aspect stratégique
- Principe financier : coûts vs. risque
- Simplicité et universalité : mesures souples et pouvant s'appliquer à l'ensemble du personnel
- Principe de dynamicité : intégrer l'évolution du système, des besoins et des risques
- Principe de continuum : l'organisation doit continuer à fonctionner même après la survenue d'un sinistre => procédures d'urgence et de reprise
- Principe d'évaluation, de contrôle et d'adaptation : « tableau de bord de la sécurité »

Conditions de succès

- Volonté directoriale
- Politique simple, précise, compréhensible et applicable
- Publication de la politique de sécurité
- Gestion centralisée de la sécurité (certaine automatisation des processus)
- Niveau de confiance déterminé des personnes, systèmes, outils
- Personnel sensibilisé et formé à la sécurité (haute valeur morale)
- Procédures d'enregistrement, surveillance et audit
- Volonté d'éviter de mettre les systèmes et les données en situation dangereuse
- Expression, contrôle et respect des clauses de sécurité dans les différents contrats
- Ethique des acteurs et respect des contraintes légales

Audit de la sécurité

- Contrôle du niveau de sécurité physique
- Contrôle du niveau de sécurité logique (contrôles d'accès…)
- Contrôle de la sécurité des réseaux
- Contrôle de la documentation
- Contrôle le cas échéant de la couverture de l'assurance
- Contrôle du dispositif associé au plan de secours (service minimal)