UNIVERSITÉ BORDEAUX 1 Sciences Technologies

Master SDRP
Réseau Avancé
Partie 3

Sécurité des systèmes d'information

Philippe Gros Session 2005

Objectif du cours

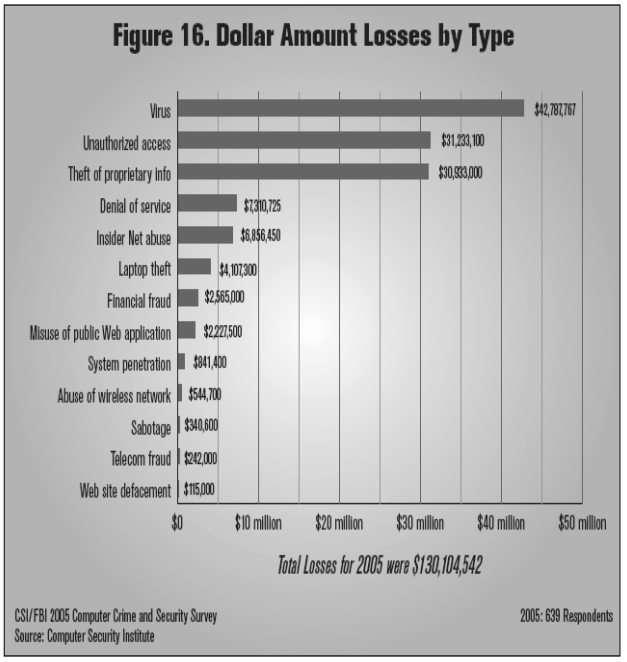
- *Etre en mesure d'évaluer les risques inhérents aux systèmes d'information et de décrire les principes d'agression et les parades à mettre en place*
- *Donner des éléments de réflexion pour la mise en place d'une politique de sécurité*

Plan du cours

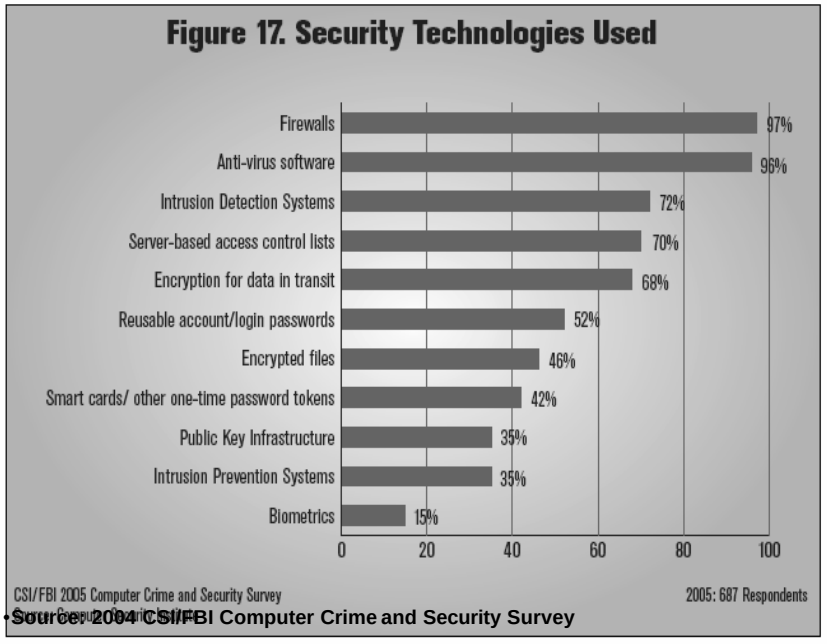
- ***Introduction à la sécurité des systèmes d'information***
- *Définitions: Les fondamentaux de la sécurité*
- *Identification des risques et des menaces*
- *Cryptographie et stéganographie*
- *Sécurité des réseaux : garde-barrière, système de détection d'intrusions et leurre (Honeypot)*
- *Réseaux sans fils : problématiques et solutions*
- *Réseaux privés virtuels (VPN) : technologies disponibles*
- *Sécurité logique : gestion des mots de passe et authentification unique (Single Sign On)*
- *Sécurité des sites Web, des serveurs et des postes de travail*
- *Incidents de sécurité : plan d'action préventif et comment réagir*
- *Plan de sécurité : analyse de risques, méthodes de sécurisation, rôle des audits et mise en œuvre*
- *Élaboration d'une politique de sécurité : norme ISO 17799*
- *Références, bibliographie et glossaire*

Introduction

- *Sondage annuel effectué aux États-Unis par le* Computer Security Institute *(CSI) en association avec le* Federal Bureau of Investigation's *(FBI).*
- *Basé sur les réponses de 689 responsables de sécurité informatique de corporations américaines, d'agences gouvernementales, d'institutions financières, d'institutions médicales et d'universités. (493 en 2004)*
- *http://www.gocsi.com*

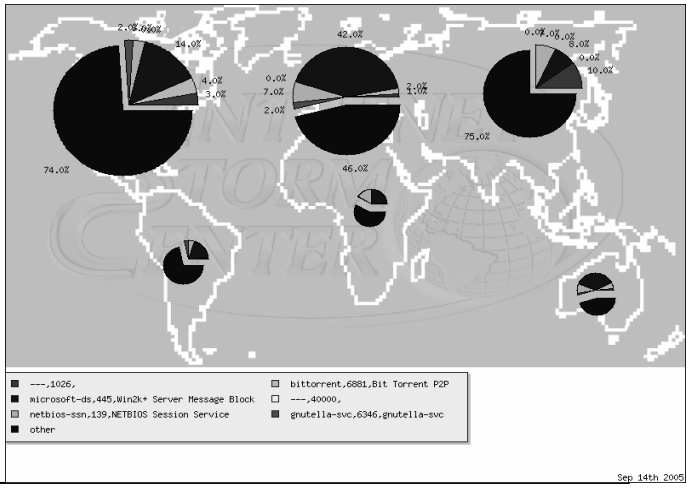


- **Source: 2005 CSI/FBI Computer**
- **Crime and Security Survey**

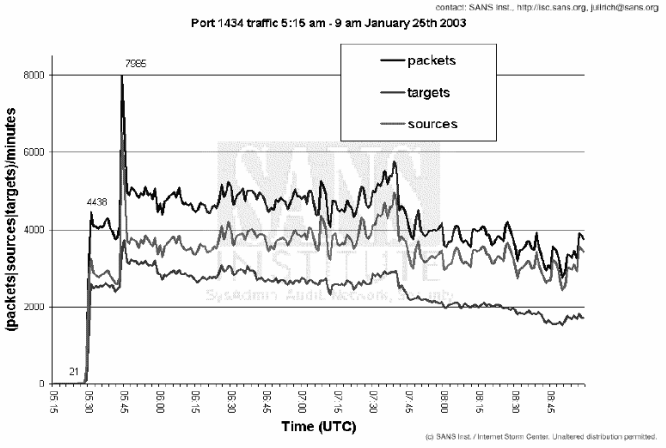


- **Source: 2004 CSI/FBI Computer Crime and Security Survey**

Les applications les plus attaquées au 16 09 2005



Conséquence d'une attaque assymétrique: le blocage de l'internet par Sapphire Worm



Plan du cours

- *Introduction à la sécurité des systèmes d'information*
- ***Définitions: Les fondamentaux de la sécurité***
- *Identification des risques et des menaces*
- *Cryptographie et stéganographie*
- *Sécurité des réseaux : garde-barrière, système de détection d'intrusions et leurre (Honeypot)*
- *Réseaux sans fils : problématiques et solutions*
- *Réseaux privés virtuels (VPN) : technologies disponibles*
- *Sécurité logique : gestion des mots de passe et authentification unique (Single Sign On)*
- *Sécurité des sites Web, des serveurs et des postes de travail*
- *Incidents de sécurité : plan d'action préventif et comment réagir*
- *Plan de sécurité : analyse de risques, méthodes de sécurisation, rôle des audits et mise en œuvre*
- *Élaboration d'une politique de sécurité : norme ISO 17799*
- *Références, bibliographie et glossaire*

Les fondamentaux de la sécurité

- Authentification : vérification de l'identité des utilisateurs ou des processus techniques avant toute interaction entre le système (ou l'application ou la base de données) et les utilisateurs (ou processus).
- Contrôle d'accès : contrôle de l'accès des utilisateurs aux applications et aux informations.
- Intégrité de l'environnement : protection de l'environnement technique contenant ou gérant les informations.
- Intégrité des informations : protection contre toute modification non autorisée d'informations critiques.
- Confidentialité : prévention de toute divulgation non autorisée d'informations sensibles.
- Disponibilité : assurance que l'accès aux informations critiques est maintenu.
- Audit : enregistrement des activités permettant la reconstitution des transactions ou des processus.
- Non répudiation : authentification de l'origine et du destinataire des transactions ou processus.

Définition d'un Système Sur selon le NSSC

« Un système sûr est un système qui, à travers l'utilisation de dispositifs de sécurité, permet de contrôler l'accès à l'information de telle manière que seuls les individus dûment habilités ou les programmes exécutés sous la responsabilité de ces individus, puissent lire, écrire, créer ou détruire de l'information »

Définition du NCSC (National Computer Security Center)

Plan du cours

- *Introduction à la sécurité des systèmes d'information*
- *Définitions: Les fondamentaux de la sécurité*
- ***Identification des risques et des menaces***
- *Cryptographie et stéganographie*
- *Sécurité des réseaux : garde-barrière, système de détection d'intrusions et leurre (Honeypot)*
- *Réseaux sans fils : problématiques et solutions*
- *Réseaux privés virtuels (VPN) : technologies disponibles*
- *Sécurité logique : gestion des mots de passe et authentification unique (Single Sign On)*
- *Sécurité des sites Web, des serveurs et des postes de travail*
- *Incidents de sécurité : plan d'action préventif et comment réagir*
- *Plan de sécurité : analyse de risques, méthodes de sécurisation, rôle des audits et mise en œuvre*
- *Élaboration d'une politique de sécurité : norme ISO 17799*
- *Références, bibliographie et glossaire*

Qui sont les attaquants potentiels?

- *Internes à l'organisation:*
  - *Employés*
  - *Anciens employés*
  - *Temporaires*
  - *Sous traitants*
- *Pirates/hackers*
- *Criminels*
- *Concurrents*
- *Gouvernements*
- *Terroristes*

Définition des menaces

- *Activités qui représentent des dangers possibles pour une organisation*
- *Elles peuvent prendre de nombreuses formes et provenir de divers horizons*
- *Il est impossible de se protéger contre toutes les menaces*
- *Il faut donc tenir compte des plus probables et des plus dangereuses pour ses objectifs et en fonction des meilleures pratiques de son industrie*

Les menaces: Codes malicieux

- *Un code malicieux ou Malware est une attaque logicielle:*
  - *Virus*
  - *Vers*
  - *Chevaux de Troies (Trojan)*
  - *Espiogiciels (Spywares)*

Les menaces: Les Virus ou Vers

- *Il existe cinq catégories principales de virus:*
  - *Les **virus systèmes** visent le secteur de partition ou le secteur de démarrage des disques durs et des disquettes*
  - *les **virus programmes** s'attaquent aux exécutables binaires compilés*
  - *les **macrovirus** s'intéressent aux documents qui peuvent contenir des routines automatisables et programmables*

Les menaces: Les Virus ou Vers

- *les **virus de script** s'attaquent aux programmes écrits en langage interprété via des combinaisons de commandes et d'instructions préétablies ;*
- *les **vers**, infection typique des réseaux, s'infiltrent en mémoire et se propagent ainsi d'ordinateurs en ordinateur.*

- *Inoculation par fichiers attachés aux courriels, chat, downloads et sur tous supports amovibles (disquettes, clés USB, CD ou DVD ..)*

Les menaces: Les Trojans

- *Programmes développés pour apparaître comme un service à l'écoute sur un port TCP ou UDP contenant le code malicieux*
- *Souvent permet de prendre la main à distance sur les postes compromis (exemple Subseven BackOrifice)*
- *Peut utiliser les vulnérabilités des OS*
- *Les pirates vont souvent procéder à un balayage à l'aveugle des réseaux afin de trouver des postes compromis (Rbot-GR: webcam)*
- *Vecteur d'attaque: courriel, attachement vérolé*

Les menaces: Les spywares

- *Programmes déposés ou fichiers (cookies) sur un PC récupérant des données utilisateurs ainsi que les habitudes de navigation sur l'Internet.*
- *Objectifs: créer une base pour un usage commercial ou marketing.*
- *Vecteur d'attaque: Freeware ou Shareware ou mêmes logiciels commerciaux et jeux.*
  - *Les anti virus ne sont pas tous capables de les répérer ou de les éradiquer => nécessité d'utiliser des logiciels spécialisés vendus en plus des offres anti virus.*

Autres menaces logicielles

- ***Code mobiles hostiles:***
  - *Sous le terme de code mobile hostile sont regroupés les applets Java, les objets Active-X malveillants et certains espiogiciel.*
  - *C'est au travers de brèche de sécurité qu'ils se manifestent. Plusieurs types d'attaques sont possibles :*
  - *Modifications du système ou des données,*
  - *Envoi de mails mal intentionnés ;*
  - *Saturation ou détournement des ressources système ;*
  - *Perturbations diverses (messages, sons,…)*
  - *Implantation de chevaux de Troie ou de virus.*

Autres menaces logicielles

- ***Bombes logiques:***
  - ***Une bombe logique est un programme contenant une fonction malveillante généralement associée à un déclenchement différée. Cette fonction a été rajoutée de façon illicite à un programme hôte qui conserve son apparence anodine et son fonctionnement correct jusqu'au moment choisi par le programmeur.***

Autres menaces logicielles

- ***Outils d'attaque réseau:***
  - ***Par abus de langage, d'autres programmes malveillants sont parfois apparentés aux Chevaux de Troie et détectés comme tels par les antivirus. Il s'agit, entre autres, des renifleurs de trafic, des outils pour « déni de service » et des craqueurs de mot de passe***

Les Vulnérabilités

- *Faiblesses qui permettent aux menaces de se manifester*
- *Doivent être associées avec des menaces pour avoir un impact*
- *Peuvent être éliminées si elles sont connues*

Définition du risque

- ***Risques= menaces * vulnérabilités***

- *Risque résiduels= risques acceptés et quantifiés en fonction d'une analyse d'impact et de sa probabilité d'occurrence*

Identification des risques

- ➲*Absence d'authentification*
- ➲*Absence d'intégrité des messages échangés, y compris perte de communication (panne du réseau ou dénis de service)*
- ➲*Absence de confidentialité*
- ➲*Répudiation des messages*

Identification des risques suite

- *Accès non autorisé*
  - *Employé*
  - *Concurrent*
  - *Pirate*
  - ➲*Vol, modification ou perte de données*
- *Espionnage des transmissions*
  - *On lit, intercepte ou dévie les données transmises sur le réseau*
  - *Les nouveaux outils des pirates: spyware et phishing*
  - ➲*Vol, modification ou perte d'information*

Identification des risques suite

- *Déni de service*
  - *Blocage d'un serveur*

  ➲*Arrêt du service, donc perte de productivité*
- *Autres risques importants*
  - *Sinistre des locaux*
  - *Vol des équipements*
  - *La protection des personnes est primordiale … sans oublier la sécurité des biens en cas d'alertes et exercices*

  ➲*Disparition physique des équipements*

Protection de l'accès aux informations

- *Garantir l'accès aux informations à travers*

  ➲*Connectivité*

  ➲*Performance*

  ➲*Disponibilité du système*

  ➲*Intégrité des données*

  ➲*Transparence à l'utilisateur*

Description des principaux types d'attaques Réseau

- *Le DNS (Domain Name Service) associe chaque nom de de domaine (ex:forces.gc.ca à l'adresse IP d'un serveur)*
- *Le service DNS est très vulnérable*
  - ➲*Modification des données du DNS*
  - ➲*Déni de service*
  - ➲*Récupération des informations afin de préparer des attaques plus évoluées*

Principaux types d'attaques Réseau

- *Exploitation du médium de transmission (perte de confidentialité)*
  - *Espionnage des lignes d'accès de modem*
  - *Espionnage des LANs et WLans(sniffer)*
    - *Externe : Pirate chez un fournisseur d'accès*
    - *Interne : Employé ou consultant*

Principaux types d'attaques Réseaux

- *Exploitation des faiblesses du protocole*
  - *IP spoofing*
    - *Usurpation d'adresse*

      (perte d'authentification)
  - *Usurpation de session (Man in the middle)*
    - *Les informations de sessions dans une requête applicative (par exemple cookie de session) sont modifiées*

      ➲ *perte d'authentification*
  - *À plus haut niveau :*

    ➲ *attaques sur les protocoles de routage RIP/OSPF/BGP*

Principaux types d'attaques Réseaux

- *Exploitation des faiblesses des services IP standards*
  - *SMTP / POP3 / IMAP*
    - *Envoi et réception de messages falsifiés (pas de contrôle d'identité)*
    - *Les «Vers» qui paralysèrent l'Internet: Code Red,Blaster…*
  - *NFS / SMB*
    - *Partage de fichiers (détournement des services de contrôle d'accès)*

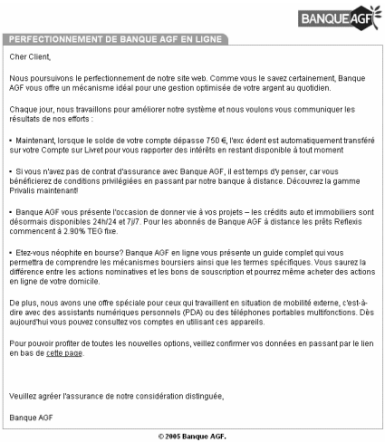
Description des principaux types d'attaques systèmes

- *Exploitation des faiblesses des services UNIX*
  - *Services d'accès distants faibles*
    - *Telnet,rlogin, rcp, rsh*
    - *SSH V1*
- *SNMP V1 (administration des équipements à distance)*
  - *Sécurité faible : mots de passe en clair sur le réseau*
  - *Snmp deamon attaquable sur les aiguilleurs Cisco*

Les attaques de plus haut niveau: le phishing ou hameçonnage

- Le Phishing est une technique utilisée pour dérober des mots de passes, n° de carte bancaire ou tout autre code...
- Pour ce faire, le pirate crée une copie d'une page connue (par exemple : le site d'une banque, site de messagerie, etc...)
- L'utilisateur distrait qui ne pense pas à regarder l'adresse du site dans la barre d'adresse, croyant envoyer son n° de carte sur le site de la banque, l'enverra au pirate

Exemple de phising:Attaque contre la banque AGF du 13 09 2006



BANQUE AGF

PERFECTIONNEMENT DE BANQUE AGF EN LIGNE

Cher Client,

Nous poursuivons le perfectionnement de notre site web. Comme vous le savez certainement, Banque AGF vous offre un mécanisme idéal pour une gestion optimisée de votre argent au quotidien.

Chaque jour, nous travaillons pour améliorer notre système et nous voulons vous communiquer les résultats de nos efforts :

• Maintenant, lorsque le solde de votre compte dépasse 750 €, l'excédent est automatiquement transféré sur votre Compte sur Livret pour vous rapporter des intérêts en restant disponible à tout moment

• Si vous n'avez pas de contrat d'assurance avec Banque AGF, il est temps d'y penser, car vous bénéficierez de conditions privilégiées en passant par notre banque à distance. Découvrez la gamme Privalis maintenant!

• Banque AGF vous présente l'occasion de donner vie à vos projets – les crédits auto et immobiliers sont désormais disponibles 24h/24 et 7j/7. Pour les abonnés de Banque AGF à distance les prêts Reflexis commencent à 2.90% TEG fixe.

• Etez-vous néophite en bourse? Banque AGF en ligne vous présente un guide complet qui vous permettra de comprendre les mécanismes boursiers ainsi que les termes spécifiques. Vous saurez la différence entre les actions nominatives et les bons de souscription et pourrez même acheter des actions en ligne de votre domicile.

De plus, nous avons une offre spéciale pour ceux qui travaillent en situation de mobilité externe, c'est-à-dire avec des assistants numériques personnels (PDA) ou des téléphones portables multifonctions. Dès aujourd'hui vous pouvez consultez vos comptes en utilisant ces appareils.

Pour pouvoir profiter de toutes les nouvelles options, veillez confirmer vos données en passant par le lien en bas de cette page.

Veuillez agréer l'assurance de notre considération distinguée,

Banque AOF

© 2005 Banque AGF.

<< Pour accéder à vos comptes en toute sécurité

J'ai oublié mes codes d'accès

Bien protéger vos codes d'accès

BANQUE AGF

COMPTE BANCAIRE | EPARGNE | PLACEMENT

Accès en toute sécurité

Nous vous remercions pour votre intérêt à nos nouvelles options.

Afin de vous inscrire, veuillez entrer vos données dans la forme ci-dessous

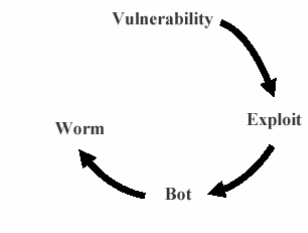
Numéro personnel

Code secret

Envoyer

Accueil | Devenir client | Qui sommes-nous ? | Contact | Plan du site | Sécurité | Mentions légales | FAQ | Glossaire | Recrutement | Webmaster

Le cycle de développement des menaces



- *Le temps de développement se réduit:*
  - *2 semaines pour Blaster et Sobig*
  - *3 jours pour le vers WITTY!*

La Protection de l'accès aux informations

- *Garantir la sécurité par*
  - ➲*Contrôle de l'accès*
    - *Authentification des intervenants*
    - *Autorisation des accès*
    - *Comptabilisation et journalisation des transactions*
  - ➲*Confidentialité de l'information*
  - ➲*Rétroactivité*
    - *Alarmes*
  - ➲*Proactivité*
    - *Audit et prévention*

Plan du cours

- Introduction à la sécurité des systèmes d'information
- *Définitions: Les fondamentaux de la sécurité*
- Identification des risques et des menaces
- ***Cryptographie et stéganographie***
- *Sécurité des réseaux : garde-barrière, système de détection d'intrusions et leurre (Honeypot)*
- *Réseaux sans fils : problématiques et solutions*
- *Réseaux privés virtuels (VPN) : technologies disponibles*
- *Sécurité logique : gestion des mots de passe et authentification unique (Single Sign On)*
- *Sécurité des sites Web, des serveurs et des postes de travail*
- *Incidents de sécurité : plan d'action préventif et comment réagir*
- *Plan de sécurité : analyse de risques, méthodes de sécurisation, rôle des audits et mise en œuvre*
- *Élaboration d'une politique de sécurité : norme ISO 17799*
- *Références, bibliographie et glossaire*

Cryptographie: Quelques définitions

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

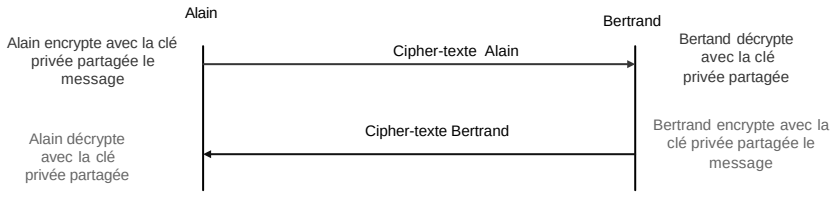
Buts de la cryptographie

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

Les 3 types d'encryption

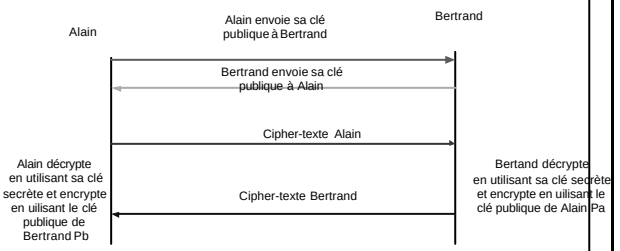
- *Clé secréte partagée:*
  - *Symétrique*
  - *En général la clé est unique*
- *Clés publiques:*
  - *Assymétrique*
  - *Paire de clés (privée et publique)*
- *Hash:*
  - *Pas de clé (en général)*
  - *Algorithme à sens unique*

Chiffrement symétrique



Cryptage:Chiffrement assymétrique

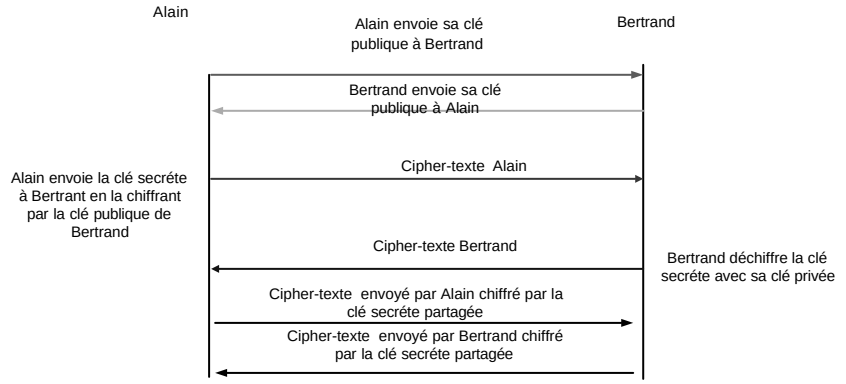
- *Une paire de clé par personne:*
  - *Publique sert à chiffrer*
  - *Privée sert à déchiffrer.*
  - *Impossible de de déchiffrer avec la clé publique*



Combinaison des 2 méthodes

- *Le chiffrement symétrique est très rapide mais implique qu'une clé secréte soit partagée entre les Alain et Bertrand*
- *Le chiffrement assymétrique est beaucoup plus lent (>100 fois), il n' y pas besoin d'avoir une clé secréte partagée.*
- *La combinaison des 2 méthodes est un bon choix: Création d'une clé secréte dite de session, envoi de cette clé secréte par un seul chiffrement assymétrique.*

Chiffrement combiné assymétrique + symétrique (SSL par exemple)



Listes des algorithmes

- *Symétriques:Triple_DES (Data Encrytion Standart, AES(Advanced Encryption Standart)*
- *Assymétriques: RSA(Rivest+Shamir), ECC (Ellyptic Curve Cryposystem)*
- *Hashes: HMAC, MD2,MD4,MD5,**RIPEMD_160, SHA***

Steganographie

- *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*

Plan du cours

- *Introduction à la sécurité des systèmes d'information*
- *Définitions: Les fondamentaux de la sécurité*
- *Identification des risques et des menaces*
- *Cryptographie et stéganographie*
- ***Sécurité des réseaux : garde-barrière, système de détection d'intrusions et leurre (Honeypot)***
- *Réseaux sans fils : problématiques et solutions*
- *Réseaux privés virtuels (VPN) : technologies disponibles*
- *Sécurité logique : gestion des mots de passe et authentification unique (Single Sign On)*
- *Sécurité des sites Web, des serveurs et des postes de travail*
- *Incidents de sécurité : plan d'action préventif et comment réagir*
- *Plan de sécurité : analyse de risques, méthodes de sécurisation, rôle des audits et mise en œuvre*
- *Élaboration d'une politique de sécurité : norme ISO 17799*
- *Références, bibliographie et glossaire*

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.*

Garde-barrières suite

- *Utilité*
  - *Efficace pour prévenir et identifier*
    - ➲*les accès non autorisés provenant de réseaux publics*
      - *sessions interactives (telnet, rlogin, rsh...)*
      - *transferts de données (FTP, E-Mail...)*
    - ➲*l'utilisation abusive du réseau*
      - *utilisateurs provenant de l'intérieur / extérieur*
      - *facilite les vérifications et la journalisation*

Garde-barrières suite

- *Limites*
  - *Inefficace lorsque*
    - ➲*les activités répréhensibles ont lieu à l'intérieur des limites du garde-barrière*
    - ➲*l'information peut transiter par d'autres canaux que le garde-barrière*
      - *disquettes, bandes magnétiques*
      - *lignes téléphoniques*
      - *imprimés mis au rebut*

Garde-barrières suite

- *Faiblesses dans le cas*
  - *des attaques programmées*
    - ➲ *virus, chevaux de Troie, vers, bombes logiques*
  - *des attaques par voie de données*
    - ➲ *extensions MIME, macros Excel, postscript*
  - *des attaques de type «refus de service»*
  - *Des attaques de types SQL injection ou de commandes applicatives malformées (requêtes HTTP par exemple)*
  - *des nouveaux types d'attaques*

Technologies de garde-barrières

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

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.)*

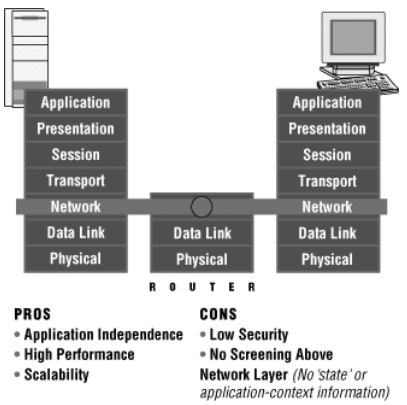
Filtrage de paquets **suite**

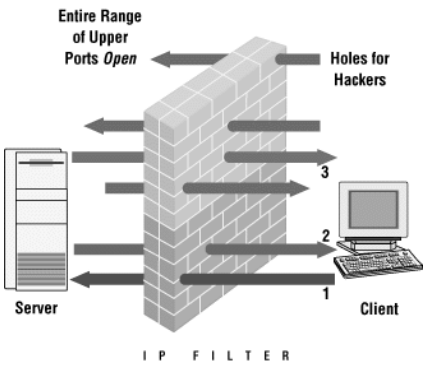
- *Avantages*
  - *Peu coûteux*
  - *Fonctionnalités de filtrage implantées en standard dans les routeurs*
  - *On a déjà le routeur pour établir la connexion vers l'extérieur*
  - *Première ligne de défense*

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/

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*

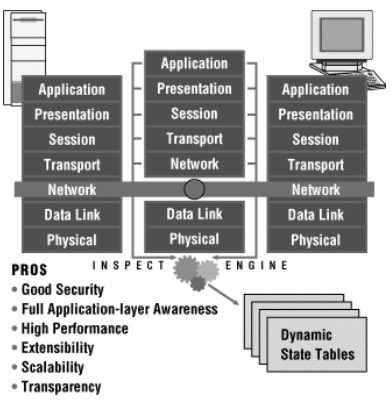
Filtrage avec inspection d'état

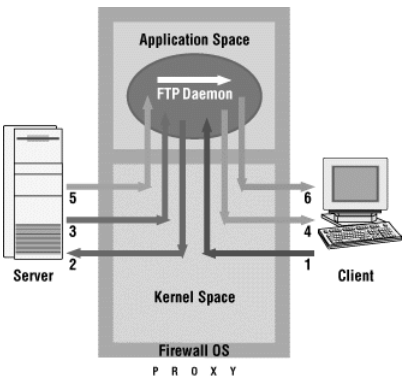
suite

- *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/

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*

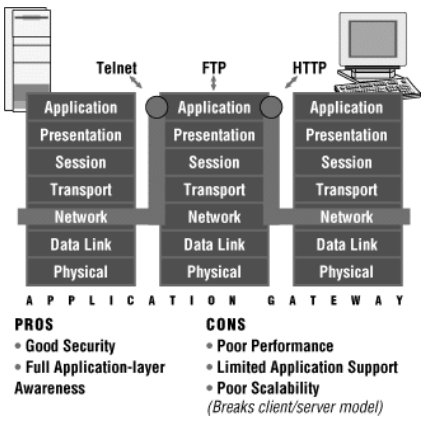
Serveur mandataire (proxy) suite

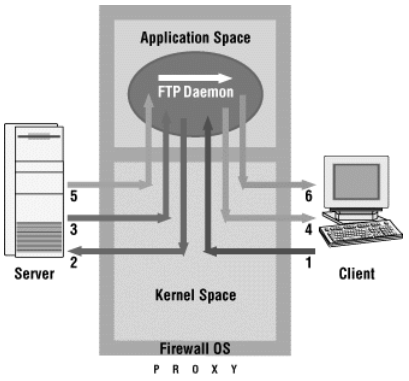
- *Avantages*
  - *Le réseau « interne » est masqué, seul le proxy est visible de l'extérieur*
  - *Authentification des usagers / services et source / destination*
  - *Possibilité de filtrage des données en transit (URL, courrier)*
  - *Possibilité de journalisation*
  - *Fonction de « cache »*

Serveur mandataire (proxy) 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) fin





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

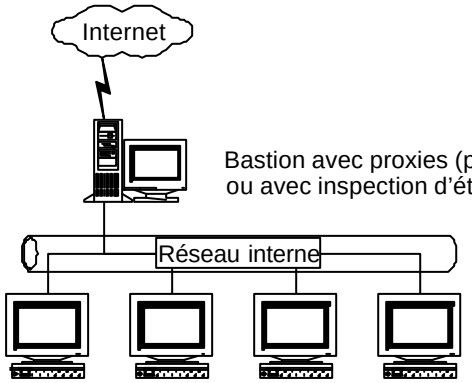
Architectures de garde-barrière

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

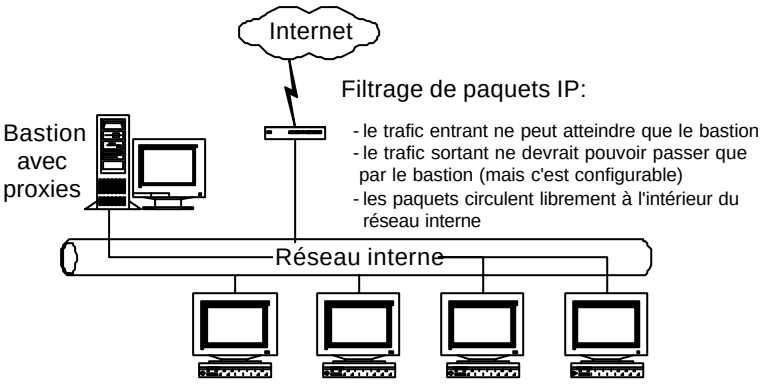
Architectures de garde-barrière

- *Bastion*
  - *Machine à risque qui a été sécurisée pour résister à des attaques sur laquelle on va installer le logiciel de garde-barrière*
  - *Soit* une appliance *intégrant un logiciel du marché*
  - *Soit un PC avec un OS sécurisé (Linux Iptable, FreeBsd ipfilter)*

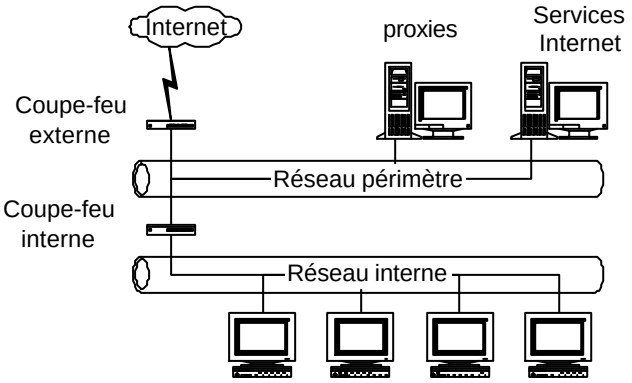
Dual-Homed gateway



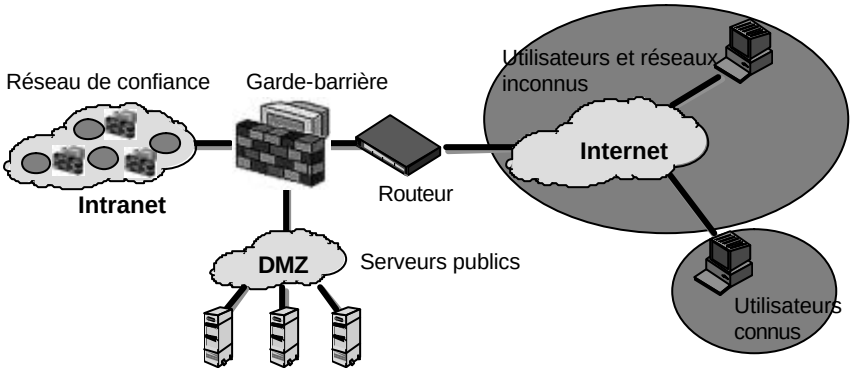
Screened Host



Screened Subnet



Garde-barrières multi zones



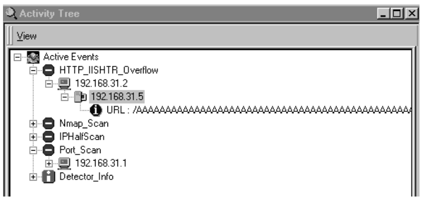
Un changement de paragdigme

Les Firewalls et les VPNs ne suffisent pas à protéger une organisation

Les nouvelles technologies de gardes barrières

- *Les gardes barrières dits applicatifs vont scruter les requêtes de hauts niveaux: SQL, GET HTTP etc..*
- Iliance, DMZ Shield, Airlock , Deny all,

La détection d'intrusion: pourquoi?

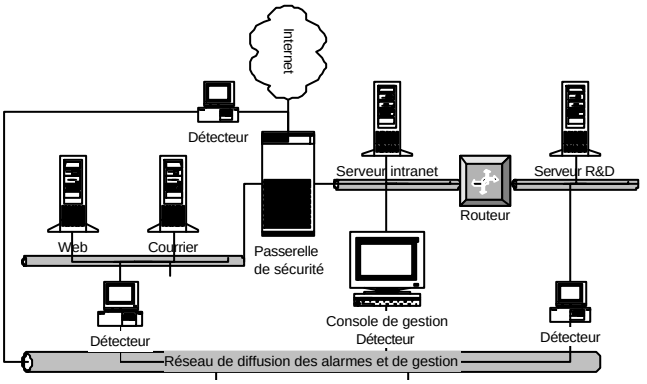


- *Un garde barrière aura du mal à arrêter les attaques applicatives.*
- *Exemple: les buffers overflow, les requêtes applicatives mal formées*

Il est impossible de protéger complètement un système

- *TOUT programme a des failles de sécurité*
- *Les nouveaux produits apportent généralement de nouveaux bogues*
- *Les failles de sécurité sont publiées régulièrement dans Internet*
- *De même que les programmes pour exploiter ces failles...*

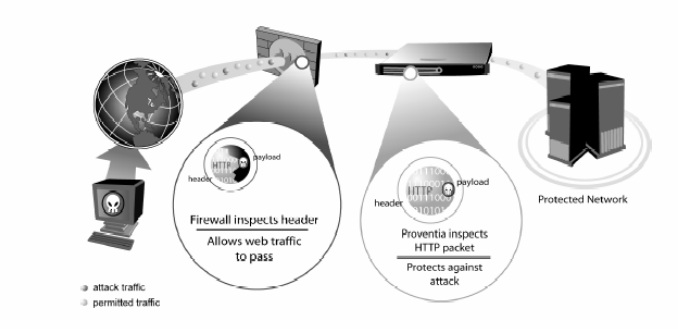
Détection d'intrusion



- *Source: Cours Détection d'intrusion dans les réseaux TCP-IP*

Une nouvelle génération d'IDS réseau: IDS en coupure les IPS Information Protection Systems

- *Source: ISS Proventia User Guide*



Surveillance et pro-activité

- *Il faut surveiller les systèmes*
  - *Journaux d'exploitation*
  - *Alarmes et outils d'analyse des journaux*
  - *Contrôle de la sécurité locale*
  - *Logiciels de contrôle de la sécurité réseau*
  - *Détecteurs d'intrusion (temps réel ou différé)*

Plan du cours

- *Introduction à la sécurité des systèmes d'information*
- *Définitions: Les fondamentaux de la sécurité*
- *Identification des risques et des menaces*
- *Cryptographie et stéganographie*
- *Sécurité des réseaux : garde-barrière, système de détection d'intrusions et leurre (Honeypot)*
- ***Réseaux sans fils : problématiques et solutions***
- *Réseaux privés virtuels (VPN) : technologies disponibles*
- *Sécurité logique : gestion des mots de passe et authentification unique (Single Sign On)*
- *Sécurité des sites Web, des serveurs et des postes de travail*
- *Incidents de sécurité : plan d'action préventif et comment réagir*
- *Plan de sécurité : analyse de risques, méthodes de sécurisation, rôle des audits et mise en œuvre*
- *Élaboration d'une politique de sécurité : norme ISO 17799*
- *Références, bibliographie et glossaire*

Principaux types d'attaques suite

- *Exploitation des faiblesses du protocole 802.11*
  - *802.11 a b ou g sont des protocoles avec peu de protection.*
  - *Une majorité de réseaux accepte une interconnexion en mode broadcast*

Principaux types d'attaques
suite

- *Rappels sur 802.11:*
  - *2 modes de connections ad-hoc (entre 2 interfaces Wlans) et infrastructures (entre un hub AP ou Access Point et plusieurs interfaces Wlans)*
  - *Dans le mode Infrastructure AP peut envoyer 10 fois par secondes une trame de contrôle contenant le SSID (Service Set Identifier). Tout interface Wlans est capable de récupérer ce SSID et se connecter sur le réseau sans autre authentification.*

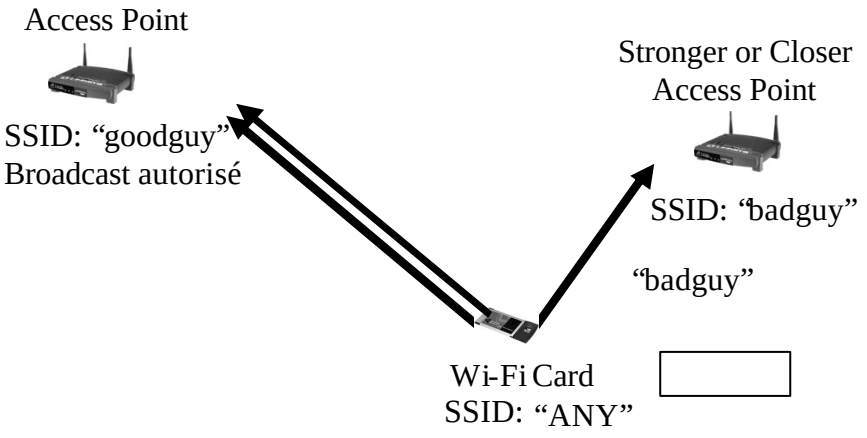
Principaux types d'attaques: 802.11: Faiblesse du WEP

- *Wireled Equivalent Privacy (WEP) est un protocole offrant une authentification des utilisateurs et un chiffrement des données*
- *L'algorithme de chiffrement est RC4.*
- *Airsnort permet de casser la clé de chiffrement après avoir récupérer entre 500 Mo à 1 Go de données.*
- *Airsnort agit comme un sniffer: il est indétectable!*

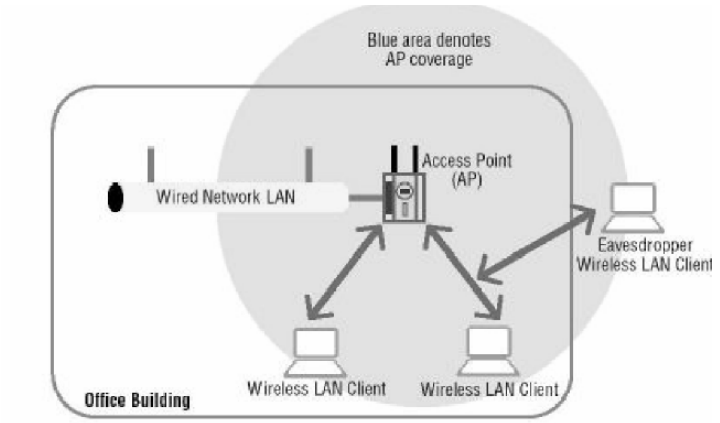
Principaux types d'attaques: le cas du wireless: accès ouverts

- *Rogue AP = un point d'accès non autorisé*
- *Risques Traditionnels*
  - *corporate back-doors*
  - *corporate espionage*
- *Risques liés aux points d"accès ouverts ou Hotspots*
  - *DoS*
  - *Vol de droits et habilitations (credentials)*

Principaux types d'attaques: le cas du wireless: Cas du Rogue Airpoint



Principaux types d'attaques: le cas du wireless: Wire Wilde Drive



Principaux types d'attaques: 802.11: Résultats du premier World Wilde Drive

Du 31 Aout au 7 Septembre 2002. 100 personnes ont participé dans 22 zones différentes à travers 6 pays et 2 Continents.

CATEGORY	*TOTAL*	*PERCENT*
TOTAL APs FOUND	*9374*	*100*
WEP Enabled	*2825*	*30.13*
No WEP Enabled	*6549*	*69.86*
Default SSID	*2768*	*29.53*
Default SSID and No WEP	*2497*	*26.64*
Unique SSIDs	*3672*	*39.17*
Most Common SSID	*1778*	*18.97*
Second Most Common SSID	*623*	*6.65*

Principaux types d'attaques: 802.11: Résultats du deuxième World Wilde Drive

Du 26 Octobre au 2 Novembre 2002. 200 personnes ont participé dans 32 zones différentes à travers 7 pays et 4 Continents.

CATEGORY	*TOTAL*	*PERCENT*	*PERCENT CHANGE*
TOTAL APs FOUND	*24958*	*100*	*N/A*
WEP Enabled	*6970*	*27.92*	*-2.21*
No WEP Enabled	*17988*	*72.07*	*+2.21*
Default SSID	*8802*	*35.27*	*+5.74*
Default SSID and No WEP	*7847*	*31.44*	*+4.8*
Most Common SSID	*5310*	*21.28*	*+2.31*
Second Most Common SSID	*2048*	*8.21*	*+1.56*

Principaux types d'attaques: 802.11: Le War Driving

- Quadrillage d'une ville avec un ordinateur portable, une carte

802.11b/g et une antenne externe

- De nombreux logiciels sont disponibles
- Un récepteurs GPS pour la localisation
- Les stationnements visiteurs; plus de sécurité physique à outrepasser
- Conséquences
- Ecoute de trafic
- Insertion de trafic
- Introduction d'une station ou d'un serveur illicite dans le
- réseau
- Rebonds

Wlans: une ébauche de solution

- Gérer ses réseaux sans fil
- Au minimum, utiliser le mécanisme de sécurité de WEP
- Auditer et surveiller les réseaux sans fil
- Surveillance, Recherche, Audit, Antennes, Outils
- Authentifier les utilisateurs de réseaux sans fil
- Chiffrer les données
- Architecturer correctement ses réseaux sans fil

Wlans: une ébauche de solution

- Amélioration de la sécurité des Wlans dans les réseaux d'entreprise:
  - WPA (Wifi Protector Access) + TKIP: Temporal Key Integrity Protocol: change les clés WEP sur une base temporelle
  - 802.1x: Identifie l'utilisateur à partir d'une base de donnée (par exemple radius)
  - WPA2: standardisé en Juin 2004 remplace RC4 par AES => exige beaucoup de ressources et sûrement une mise à niveau hardware

Plan du cours

- *Introduction à la sécurité des systèmes d'information*
- *Définitions: Les fondamentaux de la sécurité*
- *Identification des risques et des menaces*
- *Cryptographie et stéganographie*
- *Sécurité des réseaux : garde-barrière, système de détection d'intrusions et leurre (Honeypot)*
- *Réseaux sans fils : problématiques et solutions*
- ***Réseaux privés virtuels (VPN) : technologies disponibles***
- *Sécurité logique : gestion des mots de passe et authentification unique (Single Sign On)*
- *Sécurité des sites Web, des serveurs et des postes de travail*
- *Incidents de sécurité : plan d'action préventif et comment réagir*
- *Plan de sécurité : analyse de risques, méthodes de sécurisation, rôle des audits et mise en œuvre*
- *Élaboration d'une politique de sécurité : norme ISO 17799*
- *Références, bibliographie et glossaire*

Réseau privé virtuel (RPV)

- *Le réseau public (Internet) sert au transport des informations*
  - *on élimine les liens dédiés*
- *Création d'un ou plusieurs «tunnels» sécurisés entre deux sites (ou plus)*
- *Les tunnels véhiculent le trafic entre les différents sites*
  - *on donne l'illusion qu'il ne s'agit que d'un réseau*

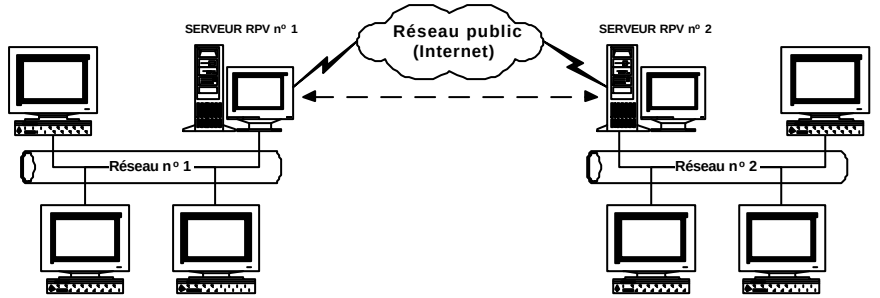
Principe du tunnel

- *Chiffrement et déchiffrement effectués aux extrémités d'un lien sécurisé (le tunnel)*
- *Tout le trafic à protéger passe par le tunnel et doit subir ce chiffrage*
- *Le tunnel devient un lien réseau à part entière*

Construction d'un RPV

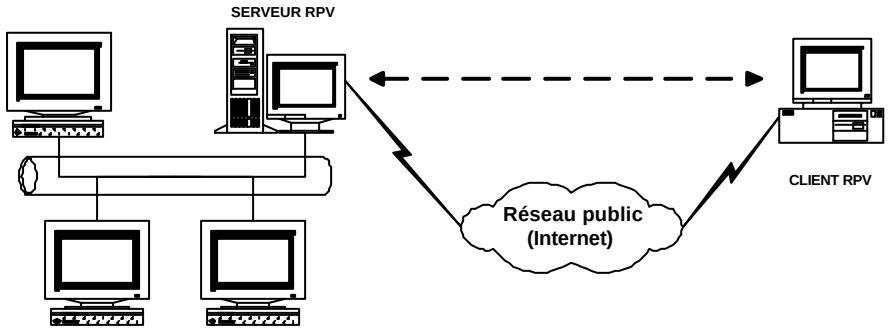
- *Diverses alternatives*
  - *Ordinateur (Windows NT/2000/XP ou Unix) + logiciel*
    - ➲ *garde-barrière avec fonctionnalités RPV*
    - ➲ *serveur de RPV*
  - *Équipement spécialisé (routeur)*
- *Gestion du réseau privé virtuel*
  - *par l'organisme ou l'entreprise*
  - *par le fournisseur d'accès à Internet*

Tunnel de serveur à serveur



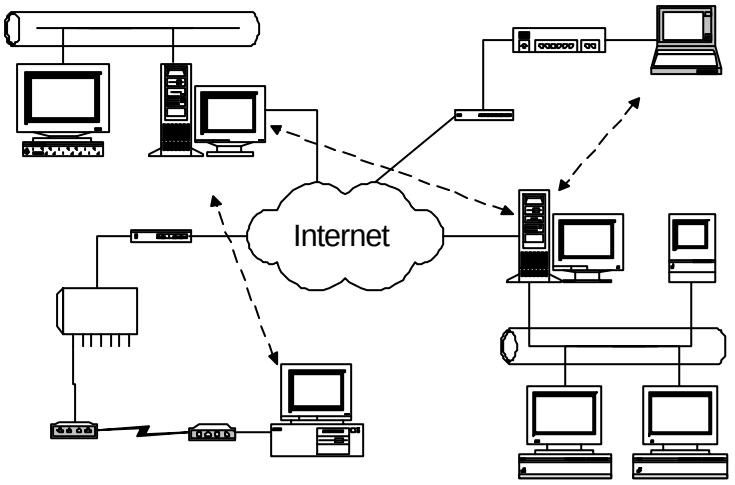
- *Utilisé pour relier des sites distants*
- *Protection des réseaux (garde-barrières)*
- *Mécanisme transparent aux utilisateurs*

Tunnel de client à serveur



- *Utilisé typiquement pour le télétravail*
- *L'utilisateur intervient dans le mécanisme d'établissement du tunnel*

Schéma d'ensemble



Technologies disponibles

- *PPTP*
- *IPSec*
- *L2TP*

PPTP

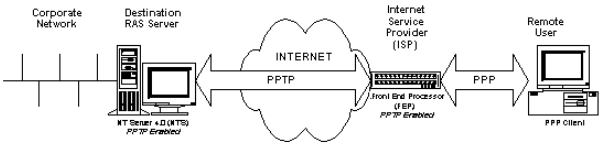
- *Point-to-Point Tunneling Protocol*
  - *Basé sur le protocole PPP*
  - *Permet l'utilisation transparente des protocoles IP, IPX, NetBEUI, AppleTalk, etc dans le tunnel*
    - ➲*http://www.schneier.com/paper-pptpv2-fr.html*

PPTP suite

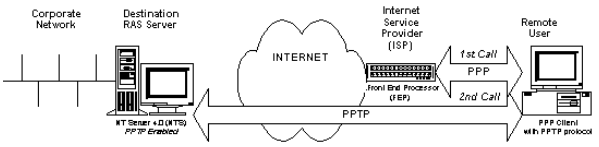
- *Solutions disponibles*
  - *Microsoft*
    - ➲*serveur: Windows NT/2000/XP*
    - ➲*client: Windows 95 / 98 / NT/2000/XP*

PPTP suite

- *Tunnel établi par le FSI*



- *Tunnel établi par l'utilisateur*



IPSec

- *Internet Protocol Security*
  - *Élaboré pour la sécurisation de IPv6, la prochaine génération du protocole IP*
  - *Ensemble de RFC dont*
    - ➲*IP Security Document Roadmap: RFC2411*
    - ➲*Security Architecture: RFC2401*
    - ➲*IP Authentication Header: RFC2402*
    - ➲*IP Encapsulating Security Payload: RFC2406*
    - ➲*Internet Key Exchange (IKE): RFC2409*

IPSec suite

- *Très bonne interopérabilité*
- *Fonctionne à la couche 3*
  - *Prévu pour l'utilisation du protocole IP dans le tunnel*
    - ➲*Les protocoles IPX, NetBEUI, AppleTalk doivent être encapsulés*
- *Impose l'utilisation du protocole IP sur le lien de communication*
- *Est en train de s'imposer*

IPSec suite

- *Solutions disponibles (certifiées ICSA)*
  - *Les manufacturiers de routeurs (Lucent/Ascend, Cisco, Nortel Networks, …)*
  - *Symantec Firewall Enterprise*
  - *Check Point avec Firewall -1 / VPN-1*
  - *IBM avec SecureWay Firewall / AIX*

L2TP

- *Layer Two Tunneling Protocol*
  - *Basé sur le protocole PPP*
  - *Successeur de PPTP et de L2F*
    - ➲*Combinaison des deux protocoles*
  - *RFC2661 de l'IETF*

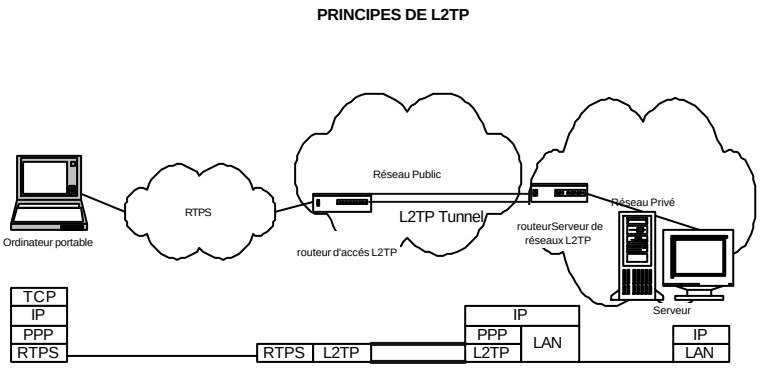
L2TP suite

- *Autres sources d'information*
  - *www.cisco.com/warp/public/732/l2tp*
  - *www.3com.com/enterprise/*
- *Avantages de L2TP*
  - *Disponible aussi bien sur un lien de communication IP que relais de trames, X25, ATM*
  - *Permet l'utilisation transparente des protocoles IP, IPX, NetBEUI, SNA, AppleTalk, etc dans le tunnel*

L2TP suite

- *L2TP et IPSec sont complémentaires*
- *Solutions disponibles*
  - *Cisco avec IOS*
  - *Microsoft avec Windows 2000/XP/2003*
  - *Nortel Networks avec Contivity*

L2TP: Exemple de Tunneling



Résumé

- *Permet de relier des réseaux éloignés comme s'ils n'en formaient qu'un en utilisant Internet plutôt que des liens dédiés*
- *Des problèmes à ne pas sous estimer*
  - *la bande passante garantie*
  - *la qualité de service*

Plan du cours

- *Introduction à la sécurité des systèmes d'information*
- *Définitions: Les fondamentaux de la sécurité*
- *Identification des risques et des menaces*
- *Cryptographie et stéganographie*
- *Sécurité des réseaux : garde-barrière, système de détection d'intrusions et leurre (Honeypot)*
- *Réseaux sans fils : problématiques et solutions*
- *Réseaux privés virtuels (VPN) : technologies disponibles*
- ***Sécurité logique : gestion des mots de passe et authentification unique (Single Sign On)***
- *Sécurité des sites Web, des serveurs et des postes de travail*
- *Incidents de sécurité : plan d'action préventif et comment réagir*
- *Plan de sécurité : analyse de risques, méthodes de sécurisation, rôle des audits et mise en œuvre*
- *Élaboration d'une politique de sécurité : norme ISO 17799*
- *Références, bibliographie et glossaire*

Classification des modes d'authentification

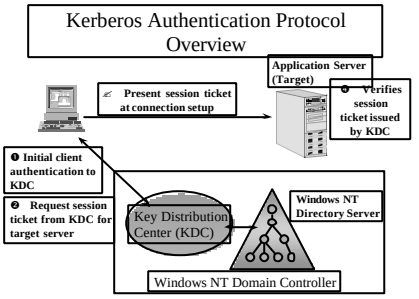
Utilisateur	Moyen d'authentification	Niveau de confiance	Accès à des privilèges
Anonyme	Pas d' authentification	Inexistant	Non
Générique	Mot de passe partagé	Faible	
Individuelle	Identifiant / mot de passe	Moyen	Oui
Authentification forte	Carte à Token/certificat	elevé	oui

Exemple de Mécanisme d'authentification forte

- *Hardware Token*
  - *synchronisé dans le temps ou défi-réponse*
    - ➲*RSASecureID, Cryptocard,Scrypto*
    - ➲*www.rsasecurity.com, www.cryptocard.com,* **www.scryptosystems.com**

Mécanismes d'authentification s

- *Kerberos*
  - *Authentification de l'utilisateur et du serveur*
  - *Échange de clés cryptées au lieu d'un mot de passe*
  - http://www.faqs.org/faqs/kerberos-faq/user/



Source: Microsoft® Windows NT® Distributed Security Services: Secure Networking using Windows NT Server Distributed Services Technology Preview

Mécanismes d'authentification

- *RADIUS, TACACS+*
  - `www.freeradius.org`
  - http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scprt2/sctcacs.htm
- *Mot de passe à usage unique (One Time Password): S/KEY*
  - `www.ietf.org/html.charters/otp-charter.html`

Le Single Sign On

- *Le mécanisme d'authentification et/ou d'autorisation est délégué à un serveur de sécurité.*
- *Une fois authentifié, l'information et les droits sont propagés à l'ensemble des serveurs => plus besoin de s'authentifier sur chacun d'eux*
- *Exemples de produits: Tivoly Access Manager, Netigrity …*

Plan du cours

- *Introduction à la sécurité des systèmes d'information*
- *Définitions: Les fondamentaux de la sécurité*
- *Identification des risques et des menaces*
- *Cryptographie et stéganographie*
- *Sécurité des réseaux : garde-barrière, système de détection d'intrusions et leurre (Honeypot)*
- *Réseaux sans fils : problématiques et solutions*
- *Réseaux privés virtuels (VPN) : technologies disponibles*
- *Sécurité logique : gestion des mots de passe et authentification unique (Single Sign On)*
- ***Sécurité des sites Web, des serveurs et des postes de travail***
- *Incidents de sécurité : plan d'action préventif et comment réagir*
- *Plan de sécurité : analyse de risques, méthodes de sécurisation, rôle des audits et mise en œuvre*
- *Élaboration d'une politique de sécurité : norme ISO 17799*
- *Références, bibliographie et glossaire*

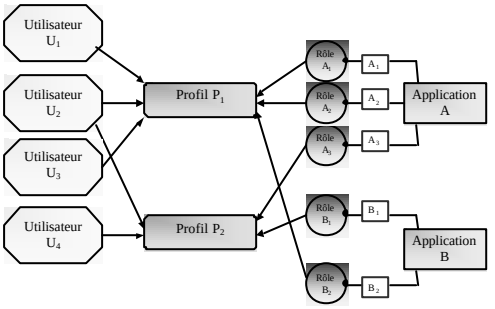
Un exemple de protection des données par la sécurité J2EE.

- *Les profils et droits d''accès aux applications sont définis dans un référentiel utilisateur de sécurité (annuaires LDAP, bases de données,…)*
- *Peut réaliser une authentification*
- *Contrôles d'accès à des ressources Web (URLs ou portles) ou à des méthodes d'EJBs (Enterpise Java Bean) reposant sur la notion des rôles J2EE.*

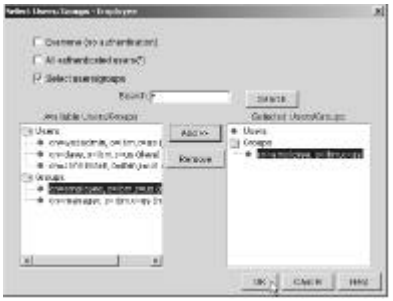
Un exemple de protection des données par la sécurité J2EE.

- ***J2EE:*** *Java 2 Enterprise Edition : standard Java pour le développement d'applications*
- *Composants (J2EE) : il s'agit du composant applicatif qui intègre la logique métier*
- *Containers (J2EE) : les containers assurent l'interface entre les clients et les composants en fournissant les services transactionnels et la gestion des ressources, l'utilisation de containers permet de simplifier le développement des composants et reportant certaines spécifications au déploiement.*
- *Connecteurs (J2EE) : les connecteurs définissent un jeu d'API pour permettre l'interopérabilité de la plate-forme J2EE avec des applications existantes (par exemple connecteur ODBC pour accéder à des bases de donnée..)*

Un exemple de protection des données par la sécurité J2EE. Rôles et Profils

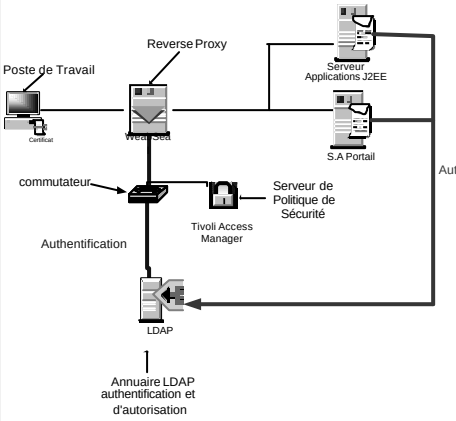


J2EE: Protection par déclaration dans les serveurs WEB ou d'applications



- *Exemple de déclaration d'un groupe d'utilisateur pouvant accéder à une ressource protégée dans un serveur d'application IBM (Websphere)*

Protection Intranet par serveur de sécurité Tivoli Access Manager



- *Les utilisateurs sont authentifiés dans la base LDAP par Webseal*
- *Les droits d'accès sont vérifiés selon J2EE par les serveurs et portails dans LDAP*

Les gardes barrières personnels

- *6 pare-feux choisis parmi les principaux acteurs du marché*
  - *Integrity Desktop de Checkpoint*
  - *Real Secure Desktop d'ISS*
  - *Windows XP Firewall de Microsoft*
  - *Desktop Firewall de McAfee*
  - *Secure Enterprise de Sygate*
  - *Client Security de Symantec*

Les gardes barrières personnels: Les critères de choix

- *Niveau de filtrage*
  - *Le pare-feu exerce-t-il un filtrage au niveau réseau (filtrage des flux de communication) et/ou au niveau applicatif (contrôle des accès aux applications et de l'activité liée à ces accès) ?*
- *Prévention d'intrusion (IPS)*
  - *Le pare-feu analyse-t-il l'activité sur les ports du poste de travail afin de prévenir de toute tentative d'intrusion (fonctionnement en mode proactif et non réactif) ?*
- *Protocoles supportés*
- *Configuration de réseaux dits de confiance*
  - *Le pare-feu permet-il de définir des réseaux nécessitant des règles de filtrage allégées*
- *Détection d'Application Hooking*
  - *L'Application Hooking est un mécanisme qui permet à une application malveillante (spyware, cheval de troie, ver…) d'utiliser une application à laquelle l'utilisateur à le droit d'accéder*

Les gardes barrières personnels: Les critères de choix

- *Politiques par profil de connexion*
  - *Le pare-feu est-il capable de gérer plusieurs politiques en fonction du type de connexion ou du profil de l'utilisateur?*
- *Mode de quarantaine*
  - *Le pare-feu est-il compatible avec un outil de contrôle de conformité permettant de gérer la mise en quarantaine du poste si ce dernier n'est pas à jour ?*
- *Audit / Mode apprentissage*
  - *Le pare-feu est-il capable d'analyser l'activité du poste nomade et de l'utilisateur pour créer ses propres règles de filtrage ?*
- *Monitoring local et centralisé*
- *Administration centralisée Anti_virus et Garde barrière*
  - *Le pare-feu est-il compatible avec une console d'administration centralisée permettant également de gérer un antivirus*

Tableau comparatif

	Checkpoint Integrity Desktop	Real Secure Desktop	Microsoft Windows XP Firewall	McAfee Desktop Firewall	Sygate Secure Entreprise	Symantec
+	- Produit utilisant le moteur de Zone Alarm, très performant - Compatible avec l'outil de contrôle de conformité de Checkpoint - Pare-feu réseau et applicatif	- Pare-feu et IPS - Mode d'analyse de type comportemental - Administration centralisée	- Produit intégré à Windows XP et gratuit	- Nombre de protocoles supportés - Pare-feu réseau et applicatif - Contrôle de conformité via la console ePo compatible avec Virus Scan - Gestion des signatures MD5	- Pare-feu réseau et applicatif - Administration centralisée - Contrôle de conformité et mise en quarantaine - Obligation de mise à jour possible - Possibilité de définir des politiques différentes en fonction de la localisation du poste	- Pare-feu réseau et applicatif - Administration centralisée - Mise en quarantaine - Compatibilité avec de nombreux produits de sécurité
-	- Pas d'administration centralisée commune avec l'antivirus McAfee - Monitoring local et centralisé insuffisant - Surveillance limitée aux protocoles IP - Customisation des politiques limitée - Deux politiques seulement (intérieux et extérieur) sans distinction en fonction des interfaces réseaux (ADSL, EDGE, GPRS...)	- Pas d'administration centralisée commune avec l'antivirus McAfee - Pas de mode de quarantaine - Mauvaise cohabitation avec d'autres logiciels antivirus - Monitoring local et centralisé insuffisant - Pas de corrélation d'évènements (risque de générer de trop nombreuses alertes : difficulté d'exploitation)	- Inadapté pour l'usage en entreprise - Pas d'administration centralisée - Pas de filtrage sur la couche application - Pas de mode de quarantaine - Peu de fonctionnalités en général	- Une seule politique pour toutes les interfaces réseau - Fonctionnalités de détection d'intrusion limitées	- Pas d'administration centralisée commune avec l'antivirus McAfee - Pas de support pour les protocoles non IP - Monitoring local et centralisé insuffisant	- Pas de support pour de multiples interfaces réseau - Impossibilité de créer des politiques par profils de connexions réseaux - Pas d'auto-apprentissage sur la couche réseau

Plan du cours

- *Introduction à la sécurité des systèmes d'information*
- *Définitions: Les fondamentaux de la sécurité*
- *Identification des risques et des menaces*
- *Cryptographie et stéganographie*
- *Sécurité des réseaux : garde-barrière, système de détection d'intrusions et leurre (Honeypot)*
- *Réseaux sans fils : problématiques et solutions*
- *Réseaux privés virtuels (VPN) : technologies disponibles*
- *Sécurité logique : gestion des mots de passe et authentification unique (Single Sign On)*
- *Sécurité des sites Web, des serveurs et des postes de travail*
- ***Incidents de sécurité : plan d'action préventif et comment réagir***
- *Plan de sécurité : analyse de risques, méthodes de sécurisation, rôle des audits et mise en œuvre*
- *Élaboration d'une politique de sécurité : norme ISO 17799*
- *Références, bibliographie et glossaire*

Comment gérer un incident

- *1 Se préparer*
- *2 Identifier l'incident*
- *3 Limiter le problème*
- *4 Eradiquer le problème*
- *5 Plan de reprise d'activité? (Disater Rercovery Plan)*
- *6 Post Mortem*

Se préparer

- *PLANIFICATION*
- *Avoir une politique claire en cas de problèmes*
- *Avoir le support de la hiérachie*
- *Avoir définie une cellule de crise (qui ? Comment?)*
- *Connaître à qui on doit s'adresser: GRC? SQ?*

Se préparer

- *Avoir un Plan de Reprise d'activité ou un Plan de continuité d'affaires*
- *Avoir des procédures bien établies et connus*
- *Avoir des back up des systèmes critiques*
- *Procéder à des simulations et des tests au moins une fois par an*

Identifier l'incident

- *Alarmes des IDS?*
- *Alarmes sur les logs?*
- *Signes de pollution virales*
- *….. En résumé tout ce qui n'est pas normal est un indice*
  - *=> avoir une équipe ou un officier de sécurité chargé de qualifier une attaque*
  - *Attention aux fausses alertes*

Contenir l'attaque

- *Cellule de crise peut prendre la décision d'isoler un réseau, un serveur*
- *Prendre des preuves pour une éventuelle poursuite en cours*
- *Changer les principaux mots de passe*

Eradiquer le problème

- *Installer une version saine des systèmes*
- *Surveiller le comportement du réseau et des systèmes pour chercher un éventuel signe de renouveau de l'incident*

Plan de Reprise d'Activité

- *A ne pas négliger*
- *Le tester*
- *Définir qui donne le go*
- *….Et comment procéder à un retour arrière*

Post Mortem

- *Apprendre de nos erreurs*
- *Affinir la politique de sécurité*
- *Communiquer aux bons intervenants les résultats de l'étude*
- *Prévenir aux besoins les autorités*

Indicateur Infocon (Presidential Decision Directive Protection 63)

Niveau	Description	Acteurs
Vert	Temps de paix informatique	
Jaune	Premiers niveaux d'attaques	Décision locale aux organisations Ou Décision présidentielle
Orange	Alerte grave: mobilisation des organismes de défenses informatiques	Décision locale aux organisations avec approbation présidentielle
Rouge	Statut de temps de guerre: Toutes les organismes fédéraux sont en position de Disaster Recovery	Décision présidentielle: État d'urgence nationale

Plan du cours

- *Introduction à la sécurité des systèmes d'information*
- *Définitions: Les fondamentaux de la sécurité*
- *Identification des risques et des menaces*
- *Cryptographie et stéganographie*
- *Sécurité des réseaux : garde-barrière, système de détection d'intrusions et leurre (Honeypot)*
- *Réseaux sans fils : problématiques et solutions*
- *Réseaux privés virtuels (VPN) : technologies disponibles*
- *Sécurité logique : gestion des mots de passe et authentification unique (Single Sign On)*
- *Sécurité des sites Web, des serveurs et des postes de travail*
- *Incidents de sécurité : plan d'action préventif et comment réagir*
- ***Plan de sécurité : analyse de risques, méthodes de sécurisation, rôle des audits et mise en œuvre***
- *Élaboration d'une politique de sécurité : norme ISO 17799*
- *Références, bibliographie et glossaire*

L'analyse de risque

- *Appliquer la méthode:*
  - ***D**isponibilité*
  - ***I**ntégrité*
  - ***C**onfidentialité*
  - ***T**raçabilité*

Plan de sécurité

- *Méthodes de sécurisation*
- *Rôle des audits*
- *Éléments de réflexion*
- *Mise en œuvre*

Méthodes de sécurisation

- *Méthode ascendante (rapide)*
  - ➲ ***on considère que les risques sont connus***
  - *analyse du réseau, des procédures de traitement et des pratiques des utilisateurs*
  - *se placer en position d'attaquant et lister les possibilités d'intrusion*
  - *résumer les faiblesses trouvées pour en dériver des règles de sécurité (mots de passe, transferts de données, garde-barrière...)*
  - *documenter et faire appliquer les règles*

Méthodes de sécurisation suite

- *Méthode descendante (plus systématique)*
  - *Classifier l'information (publique, confidentielle, secrète), les ressources du réseau, les services utilisés pour quantifier leur importance*
  - *Analyser les mesures de sécurité actuelles et les pratiques courantes*
  - *Définir des objectifs de sécurité (disponibilité, confidentialité, intégrité…)*
  - *Évaluer les risques*
  - *Évaluer l'impact des menaces*
  - *Calculer le risque (rapport de la probabilité et de l'impact)*
  - *Analyser les contraintes extérieures (légales, contractuelles, budgétaires)*

Méthodes de sécurisation suite

- *Méthode descendante (suite)*
  - *Déterminer une stratégie*
    - ➲ *maintenir les risques à un niveau acceptable par rapport aux contraintes (y compris techniques ou organisationnelles)*
  - *Implanter la stratégie*
    - ➲ *règles de sécurité*
    - ➲ *organisation des responsabilités*
    - ➲ *techniques de protection (reconfiguration, filtrage, cryptage)*
    - ➲ *mise en œuvre à grande échelle*
    - ➲ *formation des personnes*
  - *Réévaluer régulièrement la validité de la stratégie*
    - ➲ *procédures de test*
    - ➲ *intrusions simulées*
    - ➲ *correctifs*

Rôle des audits

- *Réagir aux tentatives d'intrusions réelles*
- *Valider la politique de sécurité*
- *Détecter des nouvelles failles de sécurité*
- *Corriger la politique de sécurité*

- *La mise à jour régulière des mécanismes de sécurité est aussi importante que la décision de sécuriser un réseau*

•Source : Adaptive Security (ISS)

Réflexions

- *La sécurité absolue n'existe pas*
- *Aucun garde-barrière n'est fiable à 100% (sauf peut-être le modèle « pince coupante »)*

Réflexions suite

- *Deux rôles différents :*
  - *l'administrateur réseau doit s'assurer du bon fonctionnement du réseau et de l'efficacité des échanges (optimisation, transparence, souplesse)*
  - *Le responsable de la sécurité doit garantir l'application de la politique de sécurité parfois au détriment des considérations précédentes*

Réflexions suite

- *La sécurisation d'un réseau ne se limite pas à la sécurisation de l'accès Internet. Il ne faut pas oublier :*
  - ➲*les accès distants par modem*
  - ➲*les accès au réseau local*
    - *intervenant extérieur disposant d'un accès à une machine du réseau interne*
    - *tiers ayant été autorisé à accéder à certaines ressources internes*
  - ➲*la formation des usagers (respecter les normes et méfiance vis à vis du « social engineering »)*

Réflexions suite

- *Les extensions du réseau d'entreprise (VPN ou accès distant sécurisé) doivent être intégrées dans la politique de sécurité*
  - *La programmation des garde-barrières doit être modifiée en conséquence*

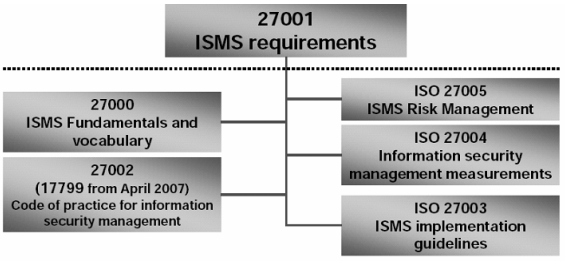
Réflexions suite

- *Le contrôle de l'accès à l'information peut être assuré par*
  - *des garde-barrières / authentificateurs multiples, y compris à l'interne*
  - *des logiciels spécialisés (ex: SiteMinder TIvoly Access Manager)*
  - *mais aussi les mécanismes de contrôle propres au système d'exploitation qui gère la ressource (permissions de fichiers, droits d'utilisateurs sous NT, Unix ou Novell)*

Plan du cours

- *Introduction à la sécurité des systèmes d'information*
- *Définitions: Les fondamentaux de la sécurité*
- *Identification des risques et des menaces*
- *Cryptographie et stéganographie*
- *Sécurité des réseaux : garde-barrière, système de détection d'intrusions et leurre (Honeypot)*
- *Réseaux sans fils : problématiques et solutions*
- *Réseaux privés virtuels (VPN) : technologies disponibles*
- *Sécurité logique : gestion des mots de passe et authentification unique (Single Sign On)*
- *Sécurité des sites Web, des serveurs et des postes de travail*
- *Incidents de sécurité : plan d'action préventif et comment réagir*
- *Plan de sécurité : analyse de risques, méthodes de sécurisation, rôle des audits et mise en œuvre*
- ***Élaboration d'une politique de sécurité : norme ISO 17799***
- *Références, bibliographie et glossaire*

Nouvelle norme ISO 27001



- *ISO 17797 est caduque depuis le 15 Octobre 2005. Il est remplacé par ISMS 27002.*
- *Par mesure transitoire toutes les certificats et les certifications en cours seront valident jusqu'en avril 2007*

La Norme ISO 17799

- *Deuxième version du BS7799*
- *Une norme en deux parties:*
  - *Les bonnes pratiques*
  - *Les recommandations opérationnelles*

La Norme ISO 17799 suite

- La norme ISO demande d'établir un cadre de travail qui servira de base au système de sécurité de l'information:
  - Politique de sécurité
  - Champ d'application
  - Inventaire des actifs
  - Évaluation des risques
    - ➲ **risques= valeurs de l'actif*menaces*vulnérabilités**
  - Management des risques
  - Sélection des contrôles
  - Déclaration de mise en oeuvre
  - Revue régulière de la mise en oeuvre

La Norme ISO 17799 suite

- *Politique de sécurité et champ d'application.*
  - *Définition des objectifs, du champ d'application et des responsabilités en matière de sécurité.*

La Norme ISO 17799 suite

- La notion d'actif est très élargie :
  - information (fichiers, manuel utilisateur, etc.)
  - équipements hardware et software supports papier
- infrastructures
- collaborateurs dont la fonction est critique
- image et réputation de l'entreprise.
- Évaluation de la valeur de chaque actif

La Norme ISO 17799 suite

- **Menaces** : cause potentielle d'incident accidentel ou intentionnel
- **Vulnérabilité:** faiblesses du systèmen permettant à la menace de se réaliser

La Norme ISO 17799 suite

ISO 17799 demande de prendre en compte 127 contrôles

1. Politique de sécurité.
2. Organisation
3. Gestion des actifs
4. Gestion du personnel
5. Sécurité physique
6. Gestion des communications et des opérations
7. Gestion des accès
8. Développement et maintenance système
9. Plan de continuation
10. Contrôle de la conformité.

➲Auxquels d'autres contrôles jugés nécessaires peuvent être ajoutés.

La Norme ISO 17799 suite

Risque
=
valeur de l'actif x menaces x vulnérabilité.

Exemple de classement du risque :

Menace identifiée	Impact sur l'actif concerné	Probabilité d'occurrence	Mesure du risque	Classement du risque
A	5	2	10	2
B	2	4	8	3
C	3	5	15	1
D	1	3	3	5