Sécurité des systèmes informatiques : aspects pratiques

Michaël Hoste

16 janvier 2008

Table des matières

1 La sécurité informatique à l'ère d'Internet

1.1 Prise de conscience

La sécurité informatique est un sujet très préoccupant, prioritaire. C'est un problème général : "Sécurité des réseaux et de l'information : proposition pour une approche politique européenne". Cest un facteur essentiel du développement économique et social. Plusieurs organismes sont créés pour surveiller ça de près (CERT : *Computer Emergency Response Team*).

1.2 Evolution des réseaux informatiques

- *70's* : s'échanger des données, traiter des données à distance. Ordinateurs de type *Mainframes* à architecture propriétaire. Peu d'échange vers l'extérieur. La sécurité est physique (contrôles d'accès).
- *80's* : Avènement du "Personal Computer". Prises de conscience des risques car les PCs devaient être reliés aux systèmes centraux.
- *fin 80's* : Structures disparates des réseaux. Besoin de normalisation à l'aide de systèmes ouverts.
- *90's* : La révolution internet est en marche. Le protocole IP va apporter une solution aux problèmes d'interconnexion des systèmes hétérogènes.
- *Aujourd'hui* : Internet s'est imposé comme le réseau des réseaux. De nouvelles contraintes de sécurité s'imposent.

Intranet/Extranet :

- *Intranet* : intérieur de l'entreprise : délimiter les territoires publics et privés pour ne pas mettre en péril la sécurité de l'entreprise.
- *Extranet* : Ouvrir son Intranet aux clients et aux fournisseurs (VPN).

1.3 Problèmes de sécurité

Internet et ses protocoles n'ont pas été développés dans une optique de sécurité. La sécurité est une réflexion d'après coup, ce qui la rend difficile à mettre en place.

1.3.1 Attaques

Internet repose sur *TCP/IP* (pile de protocoles). Les agressions exploitent les faiblesses de certains protocoles.

- *IP SPOOFING* : usurpation d'identité pour accéder à un système (adresse source modifiée)
- *DNS SPOOFING* : rediriger l'utilisateur vers un site pirate dont il a le contrôle.
- *DoS (Deny of Service)* : dégrader un service en l'inondant de trafic.
- *Buffer's overflow* : Provoque l'arrêt d'un programme en écrivant dans un buffer plus de données qu'il ne peut en contenir afin de détruire des parties du code de l'application. Introduire un autre code malicieux.
- *Attaques SYN* : Exploite le *Three Way Handshake* de TCP.
- *Teardrop* : envoi de paquets TCP qui se recouvrent.
- *TCP sequence number attaq* : attaque basée sur la prédiction du numéro de séquence dans le mécanisme de négociation *Three Way Handshake* de TCP.
- *Smurf* : ping flooding
- *Attaques ICMP* : utilisé pour échanger des messages de contrôle et par des outils de diagnostic.
- *Attaques ARP* : modifie les tables dynamiques des machines du réseau.

1.3.2 Ecoutes

SNIFFER est une écoute clandestine avec des logiciels qui permettent d'examiner les paquets.

1.3.3 Autres problèmes

- Downloading (contrôles activeX)
- Emails (spamming, attachements, ...)

- Passwords
- Virus
- Accès physiques au PC (password après inactivité, encrypter les fichiers)
- Destruction des données.
- Problème des deamons (désactiver ceux qui ne sont pas utiles).
- SPAMs.

1.3.4 Exemples de faiblesse

- Manque de précautions (pas de firewall)
- Mauvaise configuration des serveurs laissant un trou de sécurité.
- Trous de sécurités dans les applications
- Protocoles de communications non sécurisés.

1.4 Entreprise et Informatique

- Les entreprises sont dépendantes de leur système d'information. L'informatique et le réseau sont des outils indispensables. Les systèmes d'information sont vulnérables !
- Il faut protéger les systèmes.
- Il faut donc établir une certaine politique de sécurité.

2 Politique de sécurité

2.1 Objet de la sécurité informatique

On attend d'un système d'information
- Qu'il soit *disponible* au niveau des ressources matérielles et logicielles (redondance, sauvegarde, ...).
- Qu'il assure *la confidentialité et l'intégrité des données.*

On met donc en place une stratégie globale de sécurisation ainsi qu'une *politique de sécurité.* On doit l'envisager de *façon globale*, via une approche *top-down.*

2.2 La politique de sécurité

Une politique de sécurité est un ensemble de règles établies sur base d'une *analyse de risques.*
- *mesures préventives* : minimiser la survenue des risques
- *mesures correctives* : faire face à leur éventuelle apparition.

Le but est de sensibiliser aux risques et d'élaborer une structure afin de faire respecter les règles.

Recommendations
- *Nommer un responsable* au sein du service IT.
- Elaborer la politique *avec les autres corps de métier.*
- Avoir une *vision globale.*
- Réaliser *un inventaire* des matériels et logiciels.
- La politique doit être *compréhensible* et définir des zones de responsabilité à chacun des acteurs.

2.3 Gestion des risques

- *But* : déterminer les mesures de sécurité appropriées pour l'entreprise en fonction des risques encourus.
- *Méthode* :
  1. Identifier les ressources sensibles de l'entreprise et les classer en fonction de leur sensibilité.
  2. Procéder au recensement de tous les éléments qui constituent le système d'information ou qui intéragissent avec.
  3. Analyser les menaces, les vulnérabilités et des risques.
  4. Décider le niveau de risque acceptable.
  5. Mettre en place des solutions pour minimiser les risques identifiés et pour assurer la reprise en cas de sinistre.

6. Vérifier que les mesures de sécurité ne nuisent pas trop aux performances.
7. Auditer la solution de sécurité.

2.4 Mise en oeuvre pratique

Il existe plusieurs modèles de politiques de sécurité : *MEHARI* et *CobiT* en sont deux.

2.5 Quelques recommendations du CLUSIF

- Traiter les données confidentielles uniquement sur des postes non connectés au réseau.
- Ne pas stocker les données confidentielles sur un PC portable.
- Stocker ces données usr des disques durs amovibles qu'on placera dans un coffre.
- Chiffrer les données

3 Les domaines de la sécurité

3.1 Sécurité physique

Elle concerne le contrôle de l'environnement (locaux, alimentation, conditionnement d'air, ...) et des systèmes (matériels, cables, ...). Respect des normes et mise en place d'une politique de sécurité.

3.2 Sécurité de l'exploitation

Elle concerne le bon fonctionnement et la disponibilité des systèmes. Généralement une bonne procédure de sauvegarde (plan de survie, plan de reprise).

3.3 Sécurité applicative

Typiquement la problématique de l'an 2000. Cas typique de mauvaise conception applicative.

3.4 Sécurité logique

Contrôle d'accès logique (identification, authentification, ...) : gestion efficace des mots de passe, concerne la protection contre les virus, ...

3.5 Sécurité des télécoms

Repose sur l'exploitation de connexions fiables et de qualité de bout en bout.

4 Cryptographie et sécurité

4.1 La cryptographie

Définition : science de protection de l'information (écriture et lecture de messages codés) via des algorithmes et d'une valeur secrète appelée *clé*. Les algorithmes sont connus mais la clé est secrète.

La cryptographie possède 3 méthodes fondamentales :

- SKCS : Le chiffrement *symétrique* (1 clé secrète).
- PKCS : Le chiffrement *asymétrique* ou à clé publique (2 clés : une publique et une privée).
- La *fonction de hashage*.

4.2 Architecture de la sécurité informatique

Principaux services de la sécurité informatique :

- *Confidentialité*
- *Intégrité* : se prémunir contre toute modification de données.
- *Disponibilité*
- *Authentification* : identifier l'utilisateur avant de lui donner accès.

- *Contrôle d'accès* : autorisations et privilèges de chacun.
- *Non répudiation* : ne pas pouvoir nier une action qu'on a faite.
- *Accounting* : voir ce que les gens font et pouvoir retracer ce qui s'est passé en cas d'attaque.

4.3 Algorithmes de chiffrement

Un texte chiffré s'appelle un *Cypher*.
La robustesse du système de chiffrement dépend de l'algorithme utilisé et de la longueur de la clé.

4.3.1 Types d'algorithme de chiffrement

- A clé *symétrique*
  - DES
  - 3DES
  - AES
  - RC2, RC4
  - IDEA
- A clé *asymétrique* ou publique
  - RSA
  - Diffie-Hellman

4.3.2 Chiffrement symétrique (SKCS)

A et B se partagent une clé pour les transactions de A vers B. Une autre clé sera utilisée pour les transactions de B vers A.

- *DES* : créé en 1977 par le gouvernement américain. Clé secrète de 56 bits et chiffrement par blocs de 64 bits.
  - *Avantages* : clé de chiffrement et de déchiffrement est la même, méthode très rapide (solutions hardware).
  - *Inconvénients* : Problème de distribution fiable des clés, grand nombre de clés.
- *3DES* : créé en 1998 car *DES* est devenu vulnérable à cause de l'amélioration des performances des ordinateurs.

Permet la *confidentialité*.

4.3.3 Chiffrement asymétrique à clé publique (PKCS)

A et B possèdent chacun une paire de clés : une clé privée + une clé publique. Les clés publiques sont distribuées et accessibles à tout le monde. Un message chiffré avec une clé de la paire peu être déchiffré avec l'autre clé.

- *RSA* : basé sur des grands nombres premiers.
  - *Avantages* : distribution facile des clés (annuaire).
  - *Inconvénients* : lenteur, le chiffrement des messages longs est beaucoup plus lent qu'avec DES.

Permet la *confidentialité*, l'*authentification* et la *non-répudiation*.
exemple : A crypte avec la clé publique de B, B décrypte avec sa clé privée.

4.3.4 Combinaison de SKCS et de PKCS

On combine la facilité de distribution des clés de PKCS avec la rapidité de SKCS. On n'utilise donc que le chiffrement à clé publique pour échanger de façon sécurisée une clé secrète entre deux partenaires.

4.3.5 Signature digitale

- Elle utilise une fonction de hashage pour générer un code de longueur fixe sur base d'un texte de longueur variable. (empreinte)
- Les algorithmes sont les suivants : *MD4*, *MD5*, *RSA*, *SHA*.
- *Signature digitale* : un condensé de message signé avec la clé privée de l'expéditeur et qui est joint au document.

Permet l'*intégrité* des données + l'authentification de l'expéditeur (*non répudiation*).

4.3.6 Certificats numériques, CA et PKI.

Il se pose le problème de *l'authenticité des clés publiques*. Comment peut-on être sûr que la clé publique d'Alice appartient bien à Alice.
L'infrastructure de gestion des clés (*PKI - Public Key Infrastructure*) répond à cette demande.

- *Autorité de certification* : organisme digne de confiance qui confirme au moyen d'un *certificat* l'association entre une clé publique et son propriétaire.
- *Certificat numérique* : associe l'identité d'une personne ou d'une organisation à une paire de clés (privée, publique). la clé privée n'est pas divulguée et n'est connue que par son propriétaire alors que la clé publique l'est. Il est publié dans des annuaires de types *LDAP*.

4.3.7 Protocoles standardisés et autres

- *SSL* (*Secure Socket Layer*) : permet de sécuriser des protocoles applicatifs qui s'appuyent sur TCP/IP.
- *SSH* : *Secure Shell* : connexions à distance sécurisée.
- *S/MIME* (*Secure Multi Purpose Internet Mail*) : utilise des certificats pour signer et chiffrer les messages.
- *SET* (*Secure Electronics Transaction*) : Sécurisation des paiements par cartes bancaires sur Internet.
- *PGP* : E-Mail sécurisé

5 Aspects pratiques et recommandations

5.1 L'authentification

Authentification : processus qui permet de valider une identité. Les méthodes d'authentification les plus courantes se basent sur "ce que l'on connait", "ce que l'on possède" et "ce que l'on est".

- Les mots de passe *:*
  - Les *attaques possibles* sont *:* attaque en force, usurpation d'adresse, sniffers de paquets, ...
  - Mots de passe *dynamiques* (One time password) : mot de passe valable qu'une fois, même si il est capturé, il ne sera d'aucune utilité en pratique
    - *Time-based token* : synchronisation d'horloge entre le dispositif du client et le générateur de token du serveur.
    - *Challenge-response token cards* : Challenge généré par le serveur envoyé sur le token du client qui lui répondra.
  - *Biométrie* : s'intéresse à la mesure des caractéristiques des êtres vivants et à leur traitement statistique.
    - *Analyse morphologique* : empreintes, main, oeil, ...
    - *Analyse comportementale* : signature dynamique, dynamique de frappe au clavier.
  - *SSO* (*Single Sign On*) : Un seul login/pass pour toutes les applications en se basant sur un référentiel d'authentification commun.
  - *Single Logon* : Certains préfèrent cette approche qui consiste en un seul login/pass mais qui doit être introduit chaque fois qu'on se connecte sur une nouvelle application.
  - Authentification basée sur la *localisation*.

5.2 Les firewalls

Définition générale : un dispositif de sécurité (hardware/software) qui l'on interpose entre un *trusted network* et un *untrusted network*. Il est capable d'analyser les flux de trafic et de les filtrer sur base de règles. On peut s'en servir pour séparer deux réseaux ou pour sécuriser son propre ordinateur.

- C'est un point de passage *obligé*.
  - Chaque paquet va être contrôlé individuellement selon certaines règles.
- *Limitations*
  - le firewall ne sait protéger que le trafic qui passe par lui-même. Il ne protège donc pas des menaces internes (social engineering)
  - Modems dial-up accèdent via des chemins détournés.
  - Plus le firewall aura du travail à faire, plus les performances du système vont chuter.
- Firewall de type *Packet Filters* : agit au niveau de la *couche réseau*. Les paquets IP vont être filtrés sur les attributs suivants : adresse IP, ports TCP ou UDP, type de protocole (UDP, TCP), direction de l'initialisation de la connexion TCP.
  - *Avantages* : disponible dans tous les routeurs, peu cher, bonne performance.
  - *Inconvénients* : Gestion à la main des tables de filtrage, IP Spoofing, faible niveau de sécurité.
- Firewall de type *Application-level gateways* : agissent au niveau de la couche application. Utilisent des proxys et seuls les logiciels qui utilisent des proxys peuvent fonctionner, tous les autres seront bloqués.

  - *Avantages* : ils empêchent tout contact direct entre deux réseaux et ce dans les deux sens. Masquent les serveurs internes, examinent l'en-tête et le contenu des paquets.
  - *Inconvénients* : tout le traffic passe par le proxy (étranglement), un proxy est nécéssaire pour chaque application
- Quelques configurations de firewalls
  - *Screening routeur* : routeur sur lequel on peut activer la fonction "packet filtering"
  - *Dual homed gateway* : système avec 2 interfaces réseau. Pas de routage d'informations entre le réseau privé et le réseau public. Les services et accès sont fournis par les serveurs proxy installés sur le gateway. Le *Bastion host* est le système installé dans un endroit critique, vulnérable. Visible de l'internet. S'il est compromis, il ne fautp as que l'Intranet le soit.
  - *Screened host firewall* : Combine un screening routeur avec un *application gateway*. On configure de telle sorte que seul le *bastion host* soit visible d'Internet. Seul les services indispensables sont disponibles sur celui-ci.
- Le filtrage des routeurs CISCO
  - *Liste d'accès* : accepter ou refuser du trafic spécifique en entrée ou en sortie du réseau d'entreprise.
  - *1-99* : liste d'accès IP standards (se basent sur l'adresse IP source des paquets).
  - *100-199* : liste d'accès IP étendues (se basent sur l'adresse IP source et IP destination des paquets)
- *Liste d'accès IP standards* : se basent sur l'adresse IP source des paquets.

5.3 Détection et prévention d'intrusion

- *IDS* (*Intrusion Detection System*) : en complément aux autres dispositifs de sécurité, inspecte le contenu du trafic autorisé. Utilise un tracking des activités des utilisateurs pour détecter les tentatives d'intrusion sur base de signatures connues.
- *IPS* (*Intrusion Prevention System*) : tente en plus d'identifier et de bloquer des attaques encore inconnues en temps réel.

5.4 Sécurisation des accès distants

- *Accès dial-in* : concerne les utilisateurs distants qui veulent se connecter aux serveurs de l'entreprise.
  - *Direct dial-in* : on utilise le réseau téléphonique commuté.
  - *Virtual dial-in* : on a accès via l'infrastructure publique d'un ISP.
- *NAS* (*Network Access Server*)
  - *Architecture AAA* : Authentification, autorisation, accounting et auditing
  - *Authentification des utilisateurs*
    - *PPP* (*Point to Point Protocol*) : encapsulation de paquets IP sur es lignes asynchrones.
    - *PAP* (*Password Authentication Protocol*) : Le client établit un lien PPP avec NAS qui lui notifie d'utiliser PAP. Puis le client envoit son login/pass en PAP et le serveur accepte ou rejette l'utilisateur. (two-way handshake).
    - *CHAP* (*Challenge Handshake Authentication Protocol*) : connexion via un three-way handshake.
  - *Environnements complexes d'accès distants*
    - Les protocoles des serveurs de sécurité : RADIUS, TACACS, KERBEROS
  - *TACACS+* : Protocole client-serveur (le client TACACS+ est le NAS, le serveur est un serveur Unix par ex.). Supporte PAP, CHAP.
  - *RADIUS* : utilise UDP, supporte PAP, CHAP.
- *VPN* (*Virtual Private Network*) : technique qui permet de relier des sites distants de façon sécurisée en utilisant les connexions Internet comme support. C'est un réseau privé logique qui travaille sur l'infrastruture d'un réseau public.
  - *2 applications principales* :
    - Connectivité de site à site.
    - Connectivité accès distant.
  - *Avantages* : sécurité (communications chiffrées de bout en bout), efficacité (communications compressées) et économie (internet comme support)
  - VPN entre deux gateways (réseaux), entre un hote distant et un gateway ou entre deux hotes A et B.
- *Tunneling* : établissement d'une connexion virtuelle entre 2 extrémités et encapsulation des paquets d'un réseau dans les paquets d'un protocole routable d'un autre réseau. Au point de destination, on retire l'encapsulation et le message original est injecté dans le réseau.

- les VPN peuvent être réalisés à différents niveaux du modèle OSI :
  - *Application* : SMIME
  - *Session* : SSL, SSH
  - *L3* : IP layer standards (réseau : IPSEC, SKIP, ISAKMP,...)
    - *IPSEC* : version sécurisée du protocole IP qui embarque des headers supplémentaires pour la sécurité.
  - *L2* : frame layer standards (liaison de données : L2F, L2TP, PPTP).
    - *L2F* (CISCO) : connexion PPP avec un ISP et le NAS accepte ou non au moyen de PAP ou CHAP.
    - *PPTP* (Microsoft) : permet d'encapsuler PPP sur un réseau IP
    - *L2TP* (norme) : création d'un standard unique basé sur les deux précédents.
  - *Physique* : Module hardware de chiffrement
- *Mode tunnel* : le plus sécurisé, IP Header et IP data sont chiffrés et seules les adresses des gateways sont visibles.
- *Mode transport* : les données sont chiffrées mais pas le IP header, on voit clair le protocole, l'adresse source et l'adresse de destination.

5.5 Sécurisation de la messagerie électronique

- *Les protocoles* : POP3, IMAP, SMTP, MIME.
- *Quelques vulnérabilités* : serveurs de courrier mal configurés, diffusion de SPAM. MIME : transport de fichiers exécutables (vecteur de propagation de virus)
- *A l'UMH* : utilisation de MIMEDefang pour la gestion de la sécurité des mails.
- *Listes noires* (*blacklist*) : listes mises à jour de relais ouverts et d'adresses connues de spammers. Rejeter les connexions SMTP en provenance de ces serveurs
- *Analyse de contenu, analyse bayésienne.*

5.6 Les virus et autres intrus

- Quelques définitions :
  - *Virus* : programme qui se comporte de façon imprévisible et qui va exercer une action nuisible.
  - *Ver* : programme qui s'auto-reproduit, se déplace dans le réseau.
  - *Bombe logique* : déclanchement différé.
  - *Canulars* (*hoaxes*) : messages de fausse alerte de virus (ou autres).
  - *Cheval de Troie* (*trojans*) : programme nuisible caché dans un autre.
- Comment fonctionne un anti-virus ?
  - *Les scanners de fichiers* : recherchent les signatures des virus en temps réel ou à la demande.
  - *Les vérificateurs d'intégrité* : surveillent l'intégrité de certains fichiers (exécutables) en associant à ces fichiers une empreinte numérique.
  - *Les moniteurs de comportement* : résident en mémoire afin de détecter tout comportement suspect

5.7 Les réseaux sans fil

- *Avantages* : facilité de déploiement, grande souplesse, mobilité.
- 2 modes de fonctionnement
  - *Mode infrastructure* : access point général sur lequel toutes les cellules sont connectées.
  - *Mode ad-hoc* : mode point à point entre des équipements sans fil.
- Protocoles de sécurité
  - *IEEE 802.1X* : contrôle d'accès physique à un réseau local.
- Confidentialité et intégrité
  - *WEP* : tout le monde utilise la même clé de 64 ou 128 bits (RC4).
  - *WPA* : RC4 + clé de 128 bits
  - *WPA2* : algorithme AES mais problème de compatibilité avec le matériel en place
  - *IEEE 802.11i* : norme à finaliser.