

# LA SÉCURITÉ INFORMATIQUE

2<sup>ème</sup> partie

Par F. Bernard



**BSD Ingénierie**

9, avenue de Laumière 75019 Paris - ☎ (33) 01 42 38 19 20 - courriel : [formation@bsdi.fr](mailto:formation@bsdi.fr)

## Table des matières

1.	Le piratage : .....	3
2.	Virus et compagnie .....	5
3.	Sécurité sur un réseau.....	9
4.	Glossaire : Termes du Web.....	16
5.	Documentations et liens.....	19

Marques enregistrées :  
Windows®, Excel et Word sont des marques enregistrées de Microsoft Corporation

## 1. Le piratage :

*Remarque préalable à ce chapitre : les informations, démonstrations, références, travaux pratiques et liens sur le Web vous sont communiquées dans le seul but de vous sensibiliser aux domaines de la sécurité. En aucun cas vous ne devrez faire usage de ces éléments en dehors de ce cours. Dans le cas contraire votre seule responsabilité sera engagée face aux risques encourus détaillés dans ce cours (voir le chapitre juridique).*

### 1.1. Les acteurs : Hacker, Cracker, etc.

#### 1.1.1. Définitions

##### a. Hacker

Un hacker se définit de plusieurs façons, selon le site <http://membres.lycos.fr/antihacker2000/>, "c'est avant tout une personne parfaitement initiée aux langages de programmation qui tentera de pénétrer les systèmes afin d'en déceler les faiblesses et de les signaler aux propriétaires ou/et aux utilisateurs. Ce hacker agit par goût du sport, pour la beauté du geste et dans l'intérêt de la sécurité sur internet. En cela, il est respectable et les mauvais procès qui sont lancés contre eux ne servent à cacher que le manque de vigilance, de technicité, de conscience professionnelle des administrateurs de sites. Ce type de hacker est nécessaire au web, vital, dirais-je, car il force les fournisseurs d'applications à livrer aux utilisateurs des produits fiables et mieux finis. Mais définir un hacker d'aujourd'hui n'est plus aussi simple qu'il y a quelques années. Car, parmi ces génies du code, sont venus se glisser des individus prompts à se servir de leur "science" pour satisfaire leur ego et un goût morbide de destruction."

Un hacker débutant est nommé "lamer".

##### b. Cracker

Au départ il désigne un logiciel qui égraine des mots de passe jusqu'à ce qu'il en trouve un valide. Le plus connu de ces programmes se nomme crackjack.

Mais "cracker" désigne aussi un programmeur spécialisé dans le cassage de code, de mots de passes ou de protection de logiciels. Un cracker utilise une world List. Ce pirate informatique cherche aussi à pénétrer les réseaux informatiques à des fins de malveillance ou de malversation, comme accéder aux serveurs d'applications ou aux systèmes d'informations d'une entreprise. Le Cracking qualifie le comportement des pirates de systèmes informatiques, tel que le spoofing IP. A ne pas confondre avec Hacker !

#### 1.1.2. Actions

Si l'on considère le Cracker comme celui qui a le mauvais rôle il advient que certains hackers glissent vers le cracking, soit par défi, soit par opportunité.

D'autres dénominations fleurissent, comme cyberpunk, qui a une connotation de revendication politique et sociale en référence au mouvement "punk".

A noter aussi les phreakers qui piratent les communications téléphoniques (Steve Wozniak fut le créateur de la blue box avant de créer Apple).

Dans tous les cas la limite est rendue floue tant par la difficulté à détailler les actions elles-mêmes (méthode, mode d'intrusion, complicité, gain et préjudice) que les résultats (exploités réellement ou seulement rendus possibles). La justice se base souvent sur les faits mais aussi sur la potentialité des dommages. Les peines encourues se veulent exemplaires d'autant qu'il est difficile de comptabiliser le ratio entre les délits connus et ceux qui restent dans l'ombre (défaillances des cartes de crédits, des sites comportant des données stratégiques,...).

Nous étudierons l'aspect sécuritaire sans nous pencher sur le cracker sus défini qui a une activité à laquelle nous réserverons seulement un débat de quelques minutes.

### Commentaires

Les hackers utilisent des outils qui peuvent permettre de connaître les caractéristiques de la cible : BackOrifice ou SubSeven (et dérivés).

Les outils communs tels que Ping, Tracert, Netstat et Net view permettent une première approche.

Voir à ce sujet différentes pistes sont explicitées :

- ✓ Intrusion par fragmentation IP (fragrouter sous Linux)
- ✓ Les pots de miels (honey pots)

### Notes

## 1.2. Les logiciels et les matériels

*Après une rapide définition des travaux pratiques sont lancés. Pour chaque groupe une synthèse de leurs travaux est présentée à tous.*

### 1.2.1. Scanner

Ce logiciel détecte les ports ouverts sur une adresse IP (ou une plage d'adresse). Il est le premier pas vers une intrusion.

### 1.2.2. Sniffers

C'est un logiciel capable de lire les paquets de différents protocoles. Le logiciel demande à la carte réseau la remontée des paquets indépendamment de l'adresse IP sur laquelle il est installé. Son usage peut être licite pour diagnostiquer des problèmes sur un réseau, et dans ce cas son usage doit être validé par le responsable SI au risque de se voir reprocher son usage... ou tout simplement illicite lorsqu'il permet de capturer les noms d'utilisateur et les mots de passe.

**Attention :** *la seule présence d'un sniffer sur votre PC peut être considérée comme une présomption d'actions illicites (surtout si vous n'êtes pas en charge de sécurité ou de maintenance réseaux) et vous pouvez vous voir appliquer les clauses signées lors de votre embauche (voir la partie juridique).*

### 1.2.3. Perceurs de mots de passe

Ces logiciels établissent des requêtes d'ouverture de session en testant une multitude de mots de passe basés sur des annuaires.

La création de mots de passe doit répondre à un minimum de sécurité.

Quelques exemples de stratégie de création de mots de passe :

- ✓ Génération à l'aide d'une phrase "germe"
- ✓ Génération aléatoire par un programme simple : Excel. TP d'application

Notes

#### 1.2.4. Exercices et Travaux pratiques sur le sniffer

Notes et commentaires

## 2. Virus et compagnie

### 2.1. Définitions et fonctionnement

#### 2.1.1. Présentation

Sous le terme "virus" se cache un nombre important de moyens mis en œuvre pour effectuer des tâches non explicitement demandées par l'utilisateur. On retient en particulier les actions suivantes :

##### a. La bombe logicielle

Il s'agit d'un logiciel qui effectue des tâches plus ou moins gênantes, voire destructrices, lorsque certaines conditions sont remplies (d'où le terme "bombe").

Les conditions sont très variables, elles sont en général basées sur le temps : laps de temps, périodicité, heure ou date déterminée.

Les tâches peuvent être :

- ✓ L'altération ou la suppression de données,
- ✓ La modification de données
- ✓ Le transfert de données

Étude à titre d'exemple du virus CIH

- ✓ Historique

Il est appelé "Tchernobyl" puisqu'il se déclenche le 26 avril dans sa version initiale (CIH V1.2 TTIT), le 26 juin ou tout 26 d'un mois courant

Analyse de ce virus sur le plan :

- ✓ Technique
  - Auteur : Chen Ing-Hau, élève ingénieur en informatique à TTIT (Taiwan Tatung Institut of Technology)
  - Principe : Infection des exécutables 32 bits au format PE (Portable Executable de Microsoft®). Sa taille est de 1003 octets. Utilise les zones de codes vides (de type NOP).
  - Phase d'infection : Le format PE se prête particulièrement bien aux infections virales car il contient en en-tête TOUTES les informations permettant de placer un nouveau code dans les "trous" existants (gestion de blocs de 64ko).

- Reproduction : En exécutant un fichier infecté le virus prend la main sur l'Int 03H (debugg et privilèges Ring0), réassemble son code en mémoire vive. Il est prêt à infecter tout nouvel exécutable.
- Attaque : En testant la coïncidence de la valeur du jour dans la CMOS du BIOS et celle prévue par le virus il lance l'attaque sur le PC en écrivant sur les 128 octets du BIOS (cf. "matériel" ci-dessous).
- Nota : La propagation est surtout due aux sites de jeux (sites ftp de sharwares, démos commerciales (SiN d'Activision en particulier))
- ✓ Financier : c'est celui qui a causé le plus de dégâts à ce jour (CodeRed a un pouvoir infectieux plus grand mais est moins dommageable). En effet après le passage de CIH la réparation concerne le matériel (carte mère ou BIOS, disque dur) et les données contenues dans les disques touchés. Le préjudice en terme de productivité a été très important. Quelques chiffres : 1 million de PC en 1999, surtout en Asie où les dégâts en Corée du Sud sont estimés à 250 G USD
- ✓ Matériel : peut-on endommager du matériel avec un virus logiciel ?
  - L'attaque du BIOS par modification de la zone de code de boot.  
Principe d'écriture sur EEPROM : nécessité d'avoir une tension d'écriture supérieure aux 2,7 volts de lecture qui est souvent disponible sur la carte mère (Vpp de 5 ou 12 volts et procédure EnableEEPROMToWrite)  
Écriture sur l'EEPROM par les fonctions IN et OUT et la procédure IOForEEPROM) de 128 octets dans la zone BootstrapLoader Int 19H)  
Conséquences : l'EEPROM du BIOS est en général soudé sur la carte mère, l'échange de cette dernière est donc moins coûteux que de désouder... à moins d'avoir une version flashable.
  - Pour CIH le taux de succès de destruction du BIOS est évalué à 5%.
  - L'attaque du disque dur par effacement du premier Mo peut aussi être considéré comme une atteinte physique car le disque apparaît alors comme "inutilisable".
  - L'attaque des disques durs et floppy est possible en les sollicitant en dehors de leurs plages de fonctionnement (mouvements de tête à un rythme élevé, entraînant un échauffement et une détérioration. A noter que certains contrôleurs limitent ces actions)

#### b. Le salami

C'est une "technique" ancienne qui consiste à détourner des fonds résultants des différences entre les sommes affichables / imprimables et les sommes réelles. Elle a donné lieu au premier "vol" financier par informatique

#### c. Le superzapping

Il s'agit d'un utilitaire mis au point par les centres informatiques pour éviter les contraintes de sécurité mises en place dans leurs applications. Elles facilitent leurs actions telles que celles de correction (patches), recherches de dysfonctionnement (traces, dumps), vidage de mémoire et réinitialisation d'applications.

Ces logiciels sont évidemment confidentiels et à usage restreint, mais leur existence est déjà une source d'accès à des fonctionnalités de "super-utilisateur" qu'il est souvent difficile de modifier même en cas de départ d'un ingénieur système.

Ce sont aussi les révélateurs des fameuses "back doors" qui existent à l'insu de l'utilisateur.

#### d. Les trappes

C'est une forme différente du cas précédent, mais dont les conséquences restent identiques. Les trappes ("Trap doors") existent dans tous les programmes, même dans ceux de haute sécurité ou de haute technologie (... et même et surtout eux !) afin de permettre des mises au points et corrections.

Nota pour ces deux technique : Un mot de passe est souvent nécessaire, c'est le seul rempart ! les hackers adorent ces passages !

#### e. Le cheval de Troie

Il s'agit d'un programme "normal", souvent un utilitaire (et le plus souvent encore gratuit, ex : Kazaa, MSIE, Telnet sur Sun fut modifié un temps avec un cheval de Troie)

f. Le Déni de Service (Deni of Service – DoS)

Il s'agit d'une défaillance d'un système en réseau à la suite d'un envoi de nombreuses (trop) requêtes. Quatre moyens d'attaque sont classiquement répertoriés :

- ✓ ICMP flood (flood signifie inondation)
- ✓ Smurf
- ✓ TCP SYN flood
- ✓ UDP flood

Notes
-------

g. L'hébergement caché

Sur un serveur en réseau, et en particulier ayant un lien continu avec Internet, il est possible de placer à l'insu du gestionnaire de ce site des fichiers de données (images ou données illégales) ou bien des logiciels illicites ou nuisibles.

Par définition la loi implique sur le plan judiciaire (civil et pénal) le gestionnaire du site mal géré.

**2.2. Logiciels espions, spam, bombing**

2.2.1. Logiciels espions

Ces logiciels restent discrets mais ils collectent vos habitudes de navigation... et bien d'autres chose (noms, listes d'adresses, mots de passe) et les envoient lors d'une connexion sur Internet.

2.2.2. Spam

Ce sont des messages non sollicités. La CNIL a une réponse à ces action. Voir le site [www.cnil.fr](http://www.cnil.fr)

2.2.3. Bombing

Cela concerne l'envoi en quantité importante de messages vers une série limitée, voire une seule, boîte à lettres. Cette action est évidemment interdite et entraîne en général la clôture du compte du fautif. Aussi les mail-bombeurs utilisent-ils des adresses gratuites !

Notes et commentaires, visites de sites, informations au groupe
---

**2.3. Anti-virus et protections :**

2.3.1. Anti-virus

a. Remarque préliminaire

Le premier anti-virus c'est vous !

Cette phrase revient souvent, mais elle correspond à une fermeture au monde extérieur peu conciliable avec les contingences du monde moderne. Cependant vous devez être vigilants, en particulier :

- ✓ lors de l'ouverture des courriels et des pièces jointes de votre messagerie (applets à l'ouverture, fichiers exécutables)
- ✓ lors de vos promenades sur le net : les téléchargements sont la source privilégiée des virus.

#### b. Principe(s)

Plusieurs principes sont mis en application pour détecter les virus :

- ✓ La détection de signature
- ✓ L'analyse heuristique
- ✓ L'analyse comportementale
- ✓ La combinaison de plusieurs des stratégies ci-dessus

#### c. Mise en place et justification technique

Analyse et Travaux pratiques  
Commentaires

### 2.3.2. Les différents fire-walls ou pare-feu

#### a. Définition et objectifs

Sous les termes "garde-barrière", "pare-feu" ou "firewall" se cachent un concept et un grand nombre de techniques.

Le firewall a pour mission :

- ✓ d'assurer une protection en cas d'intrusion
- ✓ restreindre le nombre de ports ouverts
- ✓ restreindre les fonctionnalités entrantes et/ou sortantes.

#### b. Les firewalls matériels

Un firewall matériel est constitué des éléments (tout ou partie) suivants :

- ✓ Un ou plusieurs routeurs assurant le filtrage
- ✓ Une ou plusieurs machine nommée(s) "bastion" qui assure(nt) les fonctions de :
  - Passerelle applicative ("proxy")
  - Authentification des paquets entrants
  - Audit ("log") des flux

Un grand nombre de marques et de modèles existe sur le marché français, à titre d'exemple les documentations présentées concernent CISCO, ZYXEL, DLINK, SYMANTEC et 3COM.

Le firewall en démonstration est un VP100 de SYMANTEC.

#### c. Les firewalls logiciels

Le firewall logiciel correspond souvent à un usage limité à un réseau de faible taille (quelques postes d'un TPE). Il ne traite pas les paquets mais les activités révélées par les demandes de services à travers les ports fonctionnels de la couche 5 du système OSI.

Plusieurs sociétés diffusent ce type de logiciel, en particulier Norton Internet Security de SYMANTEC ou MacAfee Internet Security de network Associates. Zone Alarm et Ad-Ware sont gratuits et s'intègre dans Windows®.

### 2.3.3. Les zones démitalarisées DMZ

En amont du firewall il est nécessaire de traiter les paquets entrant et sortant afin de vérifier s'ils ne renferment pas des codes malveillants, ou si les paquets entrants sont "conformement" aux autorisations prévues par la DSI (Direction des Systèmes d'Information, qui peut bloquer des fonctionnalités depuis l'extérieur alors qu'elles sont autorisées en interne, limiter à certaines sources connues, etc.).

Les serveurs Web de la société sont souvent placés dans cette zone.

Le firewall sépare cette zone de l'entreprise.

L'analyse dans cette zone met en œuvre différentes techniques, elles sont généralement très orientées sur le contenu des messages, dont on retiendra principalement qu'elles :

- ✓ Analysent la nature des pièces jointes
- ✓ Détruisent ou placent en quarantaine les fichiers suspects (le degré de suspicion est TRES variable d'une DMZ à une autre !)
- ✓ Avertissent le destinataire du blocage.

En ce qui concerne les malveillances, plusieurs techniques sont mises en jeu dans cette zone, on retiendra les très efficaces "pot de miel" (en anglais "honey pots"), ces outils permettent

- ✓ L'analyse des paquets (structure, émetteur, destinataire, objet)
- ✓ La trace des incursions et la simulation de réponses associées
- ✓ La surveillance du trafic et des flux

Notes

## 3. Sécurité sur un réseau

### 3.1. Retour sur le modèle ISO

Voir le cours "Architecture des réseaux – Modèle OSI". Questions, réponses.

### 3.2. Les réseaux privés virtuels VPN

#### 3.2.1. Connexions VPN.

Il existe deux types de connexions VPN:

- ✓ **La connexion VPN en accès distant.**

Une connexion VPN en accès distant est effectuée par un client en accès distant qui se connecte à un réseau privé. Le serveur VPN donne accès à ses ressources ou à ma totalité du réseau auquel il est raccordé. Les paquets sont envoyés du client VPN vers le serveur VPN.

Le client s'authentifie auprès du serveur d'accès distant (ou VPN), et dans le cas d'une authentification mutuelle, le serveur s'authentifie auprès du client.

- ✓ **La connexion VPN de routeur à routeur.**

Une connexion VPN routeur à routeur, permet de connecter deux portions d'un réseau privé. Le serveur VPN fournit une connexion routée, aux utilisateurs du réseau LAN.

#### 3.2.2. Propriétés des connexions VPN.

Les connexions VPN qui utilisent PPTP et L2TP ont les propriétés suivantes:

- ✓ Encapsulation
- ✓ Authentification
- ✓ Cryptage des données
- ✓ Attribution des adresses et des serveurs de nom.

✓ **Encapsulation**

La technologie VPN fournit un moyen d'encapsulation des données privées avec un en-tête qui permet aux données de traverser l'interréseau de transit.

✓ **Authentification**

Pour les connexions VPN l'authentification prend deux formes:

- Authentification des utilisateurs

Pour que la connexion VPN soit établie, le serveur VPN authentifie le client VPN qui tente la connexion et vérifie que ce client a les autorisations appropriées. En cas d'authentification mutuelle le client VPN authentifie aussi le serveur VPN, ce qui fournit une protection contre les VPN "imposteurs" non autorisés sur le réseau.

- Authentification & intégrité des données

Pour vérifier que les données envoyées sur une connexion VPN proviennent de notre destinataire autorisé et quelles n'ont pas été modifiées pendant le transit, les données peuvent contenir un total de contrôle cryptographique basé sur une clé connue seulement de l'émetteur et du récepteur.

✓ **Cryptage des données**

Pour assurer la confidentialité des données au cours de leur traversée de l'interréseau, elles sont cryptées par l'émetteur. L'émetteur et le récepteur partagent une clé qui permet de crypter et de décrypter les données. Si quelqu'un parvenait à intercepter des paquets sur l'interréseau public, il ne pourra pas les décrypter sans la clé de cryptage. La longueur de la clé est un paramètre important de sécurité, en effet plus la clé est longue plus elle sera difficile à obtenir.

✓ **Attribution des adresses et des serveurs de noms.**

Quand un serveur VPN est configuré, il crée une interface virtuelle qui représente l'interface sur laquelle toutes les connexions VPN sont effectuées. Quand un client établit une connexion VPN, une interface virtuelle est créée sur le client, elle représente l'interface connectée au serveur VPN. Les deux interfaces virtuelles, celle du serveur et celle du client se connectent ce qui crée la connexion VPN point à point.

Les interfaces virtuelles doivent avoir des adresses IP valides. L'attribution de ces adresses est faite par le serveur VPN. Il peut obtenir des adresses d'un serveur DHCP (Dynamic Host Configuration Protocol) présent sur le réseau, soit avoir un pool statique d'adresse IP défini par l'administrateur.

L'attribution de serveurs de nom, soit DNS (Domain name server) soit WINS (Windows Internet Name Service), ont lieu pendant l'établissement de la connexion. Le client VPN obtient les adresses IP des serveurs DNS et WINS par le serveur VPN pour l'intranet auquel le serveur VPN est raccordé.

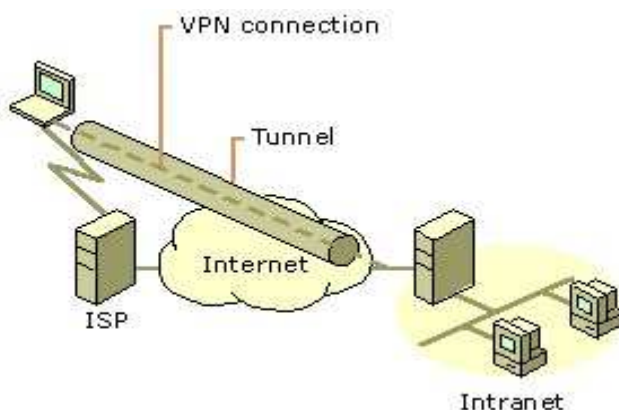
### 3.2.3. Connexion VPN sur Internet et sur intranet

Cette partie vous présente différents cas dans lesquels une connexion VPN peut être utile. Les connexions VPN peuvent être basées soit sur Internet soit sur un intranet.

✓ **Connexions VPN basées sur Internet**

L'utilisation d'une connexion VPN sur Internet permet d'éviter les frais de communications longue distance (comme pour les serveurs RAS par exemple), tout en profitant de la couverture mondiale d'Internet.

- **Accès distant sur Internet**  
Plutôt que d'effectuer un appel longue distance vers un serveur RAS, le client peut appeler un numéro de



FAI (Fournisseur d'Accès à Internet) local. En utilisant la connexion physique établie avec le FAI local, le client démarre une connexion VPN à travers Internet avec le serveur VPN de son entreprise. Lorsque la connexion VPN est créée, le client peut accéder aux ressources de l'intranet privé.

Fig 2.1 connexion VPN connectant un client à un intranet privé.

○ **Connexion de réseaux sur internet.**

Quand des réseaux sont connectés sur Internet, un routeur envoie des paquets à un autre routeur sur une connexion VPN.

Plutôt que d'utiliser des liaisons grande distance dédiées entre agences, les routeurs d'agence sont connectés à Internet en utilisant des liaisons grande distance dédiées jusqu'au FAI local. Une connexion VPN routeur à routeur est alors démarrée par l'un des routeurs à travers Internet. Une fois connecté, les routeurs fournissent une connexion routée entre les deux agences.

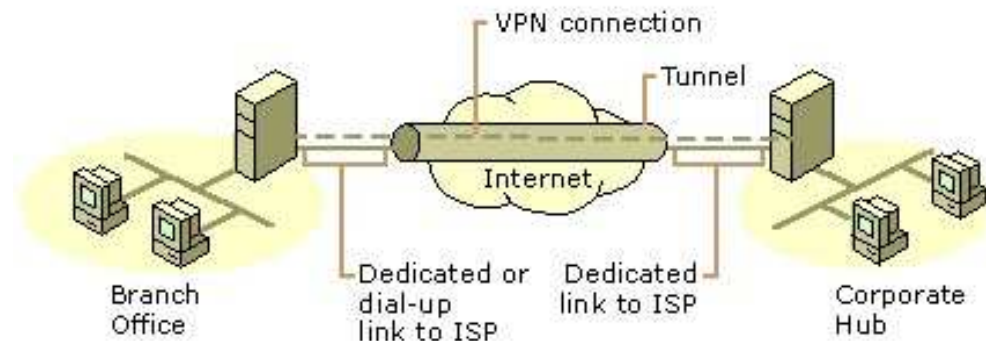


Fig 2.2 VPN connectant deux sites sur Internet.

✓ **Connections VPN un intranet.**

○ **Accès distant sur un intranet**

Dans certaines entreprises, les données d'un service, sont si sensibles que le segment de réseau est physiquement déconnecté du reste de l'intranet de l'organisation. Cela protège les données du service mais pose un problème de connectivité pour les employés du service qui voudraient avoir accès aux ressources présentes sur le LAN.

Une connexion VPN peut résoudre ce problème, grâce à deux points essentiels, le cryptage des données et le contrôle des accès aux ressources, ainsi seuls les utilisateurs ayant les autorisations suffisantes pourront avoir accès aux données sensibles. Pour les utilisateurs qui n'ont pas les autorisations pour établir une connexion VPN, le segment de réseau séparé est caché.

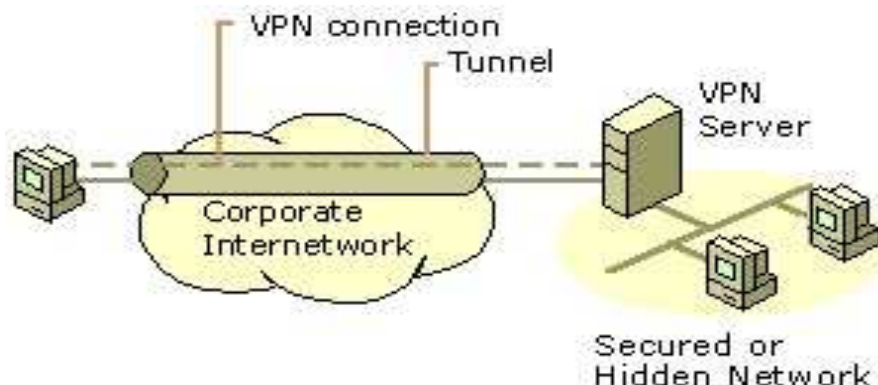


Fig 2.3 VPN permettant l'accès sécurisé à un intranet.

- Connexion de réseaux sur un intranet.  
On peut aussi imaginer connecter deux réseaux sur un intranet en utilisant une connexion VPN routeur à routeur. Ce type de VPN peut être nécessaire par exemple pour que deux départements dans des endroits séparés, et dont les données sont sensibles, puissent communiquer entre eux.

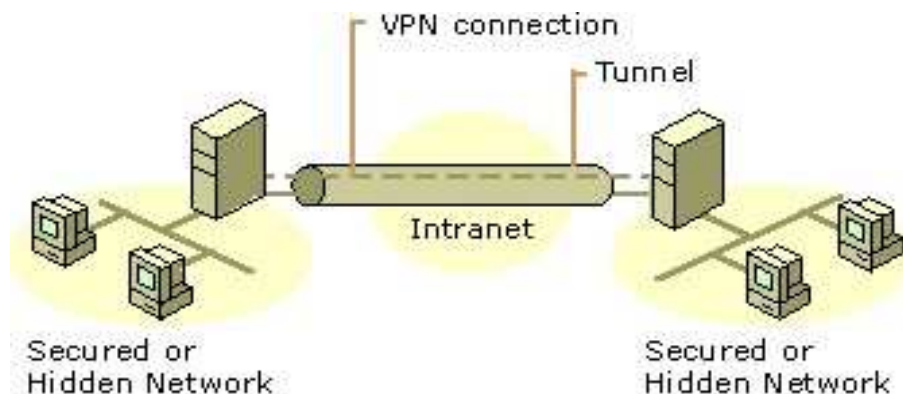


Fig 2.4 VPN connectant deux réseaux sur un intranet.

### 3.3. Sécurité des différentes couches

#### 3.3.1. La couche physique : le câblage

On a vu les possibilités d'intervention dans les locaux, il suffit de mettre en lumière ici les possibilités d'agression sur les supports physiques eux-mêmes.

Commentaires
--------------

#### 3.3.2. Les couches logicielles : les couches "transport"

Ces couches sont gérées par des systèmes électroniques ayant leur logique interne sur lesquelles on peut envisager plusieurs actions les rendant inopérants.

Commentaires
--------------

### 3.4. Cryptage

Jusqu'à récemment encore, la **cryptographie par clé symétrique** était utilisée pour sécuriser les informations transmises sur les réseaux publics. Cette méthode implique le cryptage et le décryptage d'un message à l'aide d'une même **clé**, connue des deux parties uniquement afin de conserver son caractère confidentiel. La clé est transmise d'une partie à l'autre par envoi séparé, et encoure le risque d'être détournée.

Avec la **cryptographie par clé publique**, des clés distinctes sont utilisées pour crypter et décrypter un message, de telle sorte que le message codé seulement soit transmis. Chaque partie dans une transaction dispose d'une paire de clés qui est constituée de deux clés en relation spécifique l'une avec l'autre. L'une des clés permet de crypter un message tandis que l'autre permet de le décrypter. L'une de ces clés est rendue publique tandis que l'autre est privée. Un message crypté à l'aide d'une clé publique ne peut pas être décrypté à l'aide de la même clé, mais uniquement à l'aide de la clé privée qui lui correspond. Si vous signez une transaction avec votre banque à l'aide d'une clé privée, la banque peut la lire avec la clé publique correspondante et sait que vous seul pouvez l'avoir envoyée. Ceci est l'équivalent d'une **signature numérique**.

Le cryptage par clé publique réduit le risque d'interception d'informations privées, en permettant aux parties de s'identifier formellement au moyen des signatures numériques.

L'un des standard les plus connu est le RSA (du nom des trois "inventeurs" : Rivest, Shamir et Adi) mais qui a en fait été découverte en 1973, soit 5 ans auparavant en Grande-Bretagne par C. Cocks. Le RSA est fondé sur la difficulté à factoriser des grands nombres. Il y a trois phases dans le protocole RSA :

- ✓ La création des clés : une publique et une privée
- ✓ Le chiffrement avec la clé publique
- ✓ Le déchiffrement par le destinataire avec sa clé privée

Il faut noter que le protocole RSA peut aussi servir à l'authentification d'une source.

D'autres moyens de cryptage permettent de cacher des informations dans des images, c'est la stéganographie.

Travaux pratiques, commentaires

### 3.5. **Authentification**

La certification d'un document électronique signé débute par l'examen du « certificat » de l'auteur présumé du document. Le certificat est un document d'identité électronique attestant du lien entre une identité et une clé publique.

Un certificat mentionne au minimum l'identité en question et la clé publique qui lui est associée. Il peut également mentionner une date d'expiration et un numéro de série.

Le certificat est signé électroniquement par l'autorité émettrice, qu'on appelle aussi « autorité certifiante » (en anglais « *Certifying Authority (CA)* »). Cette autorité est un organisme ayant un intérêt quelconque à se porter garant de certaines identités.

Voir aussi les paiements sécurisés :

- ✓ [www.paybox.com](http://www.paybox.com)
- ✓ [www.payline.com](http://www.payline.com)

Analyse des moyens mis à disposition sur le net : Mode d'utilisation, notion subjective de sécurité, à qui fait-on confiance, comment ?

Commentaires

### 3.6. *Serveur proxy et filtrage*

Sous forme de synthèse de ce qui a été détaillé ci-dessous on trouve des systèmes de filtrage applicatif qui traite le contenu du paquet au niveau applicatif avant de le faire agir sur le réseau de l'entreprise. Ce niveau de surveillance requiert une puissance de traitement importante et une gestion des anomalies par des règles qui demandent une mise en place et une mise à jour coûteuse en ressources humaines.

Ces configurations conviennent mieux aux applications traitant les flux entrants (site Web de documentation pure, et non de transactions). Voir sous Linux TIS FWTK.

### 3.7. *Les protocoles IP V4, IP V6 et IPSec*

#### 3.7.1. Comparaison entre IP V4 et IP V6

L'étude des datagrammes IP V4 et V6 a montré plusieurs différences qui touchent :

- ✓ L'adressage étendu sur 128 bits au lieu de 32 bits en V4,
- ✓ Une simplification de l'en-tête qui tient aux faits suivants :
  - Longueur fixe de 8 champs de 40 octets au lieu d'une longueur variable allant de 20 à 60 octets et 11 champs dans les 20 premiers octets pour IP V4.
  - La somme de contrôle est supprimée (elle est en fait reportée sur la couche supérieure)
  - La prise en charge des extensions et des options est améliorée en séparant les options de routage sur le nœud de destination de celles nécessaires aux nœuds intermédiaires
  - La gestion des flux : elle n'existe pas avec IP V4 qui est conçu pour des paquets indépendants (routes optimisées par chaque nœud). IP V6 intègre une notion de flux.
- ✓ Analyse comparée : IP V6 bénéficie de l'expérience acquise par l'usage mondial d'IP V4. Il évite les problèmes liés aux "viols de couche" (gestion des flux sous V4 en utilisant les informations contenues dans les datagrammes TCP, ou même dans la définition des ports !). La somme de contrôle est calculée à chaque nœud et le mode de traitement des options n'est pas optimum (voir les datagrammes).

Notes

### 3.8. *IPSec*

#### 3.8.1. Définition

Le besoin de mise en sécurité des données contenues dans les datagrammes a donné naissance à l'IPSec. Les modalités de mise en sécurité d'une communication donne lui à plusieurs étapes :

- ✓ Dialogue de décision de passage en IPSec
  - ✓ Négociation de la gestion du chiffrement et des attributs associés
- ISAKMP définit ce type de transaction (RFC 2408). Il définit, crée et supprime les SA (Security Associations).

Une SA est une connexion qui fournit une connexion unidirectionnelle de services de sécurité au trafic qu'elle transporte. Il y a deux mécanismes qui peuvent être associés à une SA, mais un seul par SA :

- ✓ AH (Authentication Header)
- ✓ ESP (Encrypting security Payload)

Pour un trafic bi-directionnel il faut deux SA !

ISAKMP a recours à des certificats numériques fortes, sans lesquels la SA est suspecte.

#### 3.8.2. Fonctionnalité d'une SA

Les SA permettent par principe de déjouer les DoS (Denial of Service) par la création de jetons (cookies) échangés avant le transfert de données encryptées.

## La sécurité informatique

Le vol de connexions est géré par la liaison entre l'authentification et les échanges de clés.  
L'insertion est elle aussi gérée par le protocole.  
Dans les deux cas la SA est détruite et les anomalies remontent vers l'émetteur de la SA.

Une AH place un header supplémentaire (encapsulation) sur un datagramme TCP. Il est opérationnel sous IP V6.  
L'utilisation de AH dans un tunnel est plus que légitime, elle rationalise le concept en tunnel sécurisé.

### **3.9. Aspect juridique**

#### **3.9.1. La charte individuelle d'entreprise**

Une charte de sécurité en entreprise peut apporter des solutions aux problèmes liés à la sécurité informatique en entreprise, car :

- ✓ Elle attire l'attention sur les dangers liés à l'utilisation de matériels informatiques
- ✓ Elle définit les responsabilités
- ✓ Elle définit les sanctions applicables en cas de manquement.

Au moment de l'embauche et lors des changements de poste créant un usage de matériels informatiques il est utile (voire fortement conseillé...) de faire signer une charte telle que celle proposée sur notre site.

#### **3.9.2. Informations diverses**

L'usage de certains logiciels comme en particulier les "sniffeurs" tombe sous le coup de la loi.

Ne pas oublier que la loi sur la propriété littéraire et artistique du 3/07/1985 protège Internet.

En ce qui concerne les attaques de type "hacker" l'article 323-1 précise : " Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 15.000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de deux ans d'emprisonnement et de 30.000 euros d'amende. "

Notes

#### 4. Glossaire : Termes du Web

Termes	Définitions
Arobase @	Utilisé surtout pour les adresses électroniques. Ex : formation@bsdi.fr
Adresse de courrier électronique	C'est l'adresse où vous recevez votre courrier électronique (vos e-mail). Chaque utilisateur d'Internet peut en avoir plusieurs, mais toutes sont uniques. Ex : webmaster@bsdi.fr
Adresse IP	Code informatique composé de 4 séries de 3 chiffres identifiant tout ordinateur connecté sur Internet. Ce code est remplacé par l'adresse Web ou URL pour simplifier la navigation.
Adresse Web	Adresse permettant d'accéder à un site Internet, du type http://www.bsdi.fr. L'adresse s'appelle URL en anglais. Elle s'inscrit toujours sans espace. Généralement, c'est le nom du site suivi de .fr (site français) ou .com (site international de commerce) et généralement précédé de www (World Wide Web).
Applet	Programme écrit en Java qui s'exécute sur l'ordinateur de l'utilisateur de manière transparente. Surtout utilisé pour les animations.
Bande passante	La bande passante mesure la quantité d'informations pouvant circuler sur le réseau. Exprimée en MHz, plus est elle élevée, plus la circulation est fluide.
Baud	Unité de mesure de transmission de données (identique à bps : bit par seconde) utilisé principalement pour les modems
Bookmark	Identique à Signet. Repère des navigateurs (appelés aussi Favoris) qui permettent de garder en mémoire l'adresse des sites Web visités afin d'y retourner plus facilement.
Bps	Bit par seconde (voir Baud)
Browser	Terme anglais désignant le navigateur.(voir ce terme)
Cadre	Ou frame en anglais. Utilisés pour scinder les pages Web, principalement pour séparer le menu du contexte. Les navigateurs anciens ne savent pas les interpréter.
Chat	Terme anglais signifiant "bavardage". Via un logiciel IRC (Internet Relay Chat), vous pouvez dialoguer (sur l'écran) en direct avec d'autres connectés.
Commerce électronique	Activité de commerce via Internet qui suppose une galerie de vente virtuelle et un système de paiement sécurisé.
Compression	Opération visant à réduire la taille des fichiers, le plus souvent avant de les transférer, minimisant ainsi les temps de chargement.
Cookie	Petits fichiers logés à votre insu sur votre disque dur qui permettent à certains sites Web de récupérer des informations sur vos habitudes de connexion, de sites visités, etc... Vous pouvez désactiver ces cookies dans vos navigateurs.
Coupe-feu	Ou pare-feu, et firewall en anglais. Système de sécurité contre les intrusions dans votre réseau informatique via Internet. Recommandé en cas de données confidentielles, importantes ou en réseau.
Courriel (Courrier électronique)	La messagerie électronique est l'aspect d'Internet le plus séduisant et le plus utilisé. C'est une poste virtuelle qui autorise l'envoi de courrier aux quatre coins du monde pour le prix d'une communication locale. On peut y joindre des photos numérisés, des fichiers textes et tout autre document sous forme numérique.
DNS	En anglais : Domain Name Server. Sorte d'annuaire recensant tous les sites Web de la planète, faisant le lien entre les adresses Web et les adresses IP.
E-mail	Terme désignant un message électronique

Extranet	Extension d'un Intranet à des partenaires de l'entreprise. C'est en quelque sorte un Internet limité aux relations professionnelles d'une entreprise.
FAQ	Frequently Asked Questions en anglais. Questions les plus fréquemment posées regroupées pour apporter une aide basique aux personnes débutantes sur un sujet donné.
Favori	Voir Bookmark
Firewall	Voir coupe-feu
Forums	Où groupes de discussions (en anglais : newsgroup). Salons virtuels où chacun, en fonction de ses préférences, peut laisser des messages électroniques et lire ceux des autres abonnés (gratuit). Chaque forum traite d'un sujet particulier.
Fournisseur d'accès	Société qui vous propose un abonnement pour vous connecter à Internet.
Frame	Voir cadre
FTP	En anglais : File Transfer Protocol. Procédure de transferts de fichiers entre ordinateurs, très utilisé pour le téléchargement de pages Web.
GIF	Format d'images utilisé sur le Web pour les graphismes autres que les photos. C'est un format compressé.
Groupes de discussions	Voir Forums
Hit	Connexion à une page Web. L'audience d'un site se mesure en nombre de hits, ce qui ne veut pas dire que la page a été lue et que tout le site a été visité.
Homepage	En anglais : page d'accueil. Page sur lequel l'internaute arrive sur un site Web.
HTML	En anglais : Hyper Text Markup Language. C'est le langage de programmation d'Internet.
Hypertexte	Fondement du multimédia et de l'interactivité. Le lien hypertexte permet la navigation dans des documents en cliquant sur du texte ou des images. Cette navigation peut être locale (sur différents documents d'un ordinateur) ou sur le Web, reliant entre eux des sites distants.
Imap	En anglais : Internet Message Access Protocol. Protocole utilisé pour la messagerie électronique. A terme, va remplacer POP3.
Internaute	Appartenant vraisemblablement à une espèce aquatique en voie de développement, l'internaute surfe sur le Web, navigue sur Internet via son navigateur, se fait quelquefois mener en bateau, mais il a l'air heureux comme un poisson dans l'eau !
Internet	Le réseau des réseaux ! Internet est un gigantesque réseau informatique qui n'obéit à aucune règle particulière et qui n'appartient à aucun pouvoir politique, privé ou public, ce qui explique son développement. A noter qu'Internet regroupe plusieurs parties, dont les plus connues sont la messagerie électronique, le Web et FTP.
Intranet	Intranet est un réseau interne à une entreprise reprenant l'architecture et l'aspect d'Internet accessible par des établissements distants. L'entreprise peut alors offrir en temps réel les mêmes informations à tous ses salariés. En principe, sur un Intranet, il y a toujours une passerelle vers Internet.
IRC	Voir Chat
Java	Langage de programmation facilitant l'écriture d'animations sur le Web. Les programmes sont appelés applet.
JPEG	Format d'images employé principalement pour les photos sur le Web.

	(extension : jpg).
Liste de diffusion	Service gratuit d'envoi d'informations à ses abonnés. Une fois inscrit sur une liste de diffusion (en anglais: mailing list), l'internaute reçoit par e-mail des informations périodiques sur le sujet qui l'intéresse.
Mél	Traduction d'email, pour messagerie électronique.
Modem	Abréviation de modulateur-démodulateur. Matériel servant à connecter un ordinateur sur un réseau via une ligne téléphonique. Il existe des modems analogiques et des modems numériques (plus onéreux, mais plus rapides). La vitesse de transmission des informations s'exprime en baud ou bps.
Moteur de recherche	Automate de recherche couplé à des bases de données gigantesques qui recensent toutes les adresses Web et les mots-clés utilisés.
Navigateur	En anglais : browser. C'est le logiciel qui sert d'interface entre l'internaute et le Web. Les navigateurs affichent l'information (les sites Web) de façon claire et structurée pour l'internaute. Les deux navigateurs les plus utilisés sont Navigator de Netscape et Internet Explorer de Microsoft.
Net	Abréviation d'Internet
Nétiquette	Code de bonne conduite sur le Web. Ces règles de savoir-vivre informelles constituent la déontologie de tous les internautes. (ou devraient ...)
Newsgroup	Voir forums ou groupes de discussion
Numéris	Nom donné par France Telecom au réseau numérique en France. Permet des connections à 128 bps par seconde (entre 28 et 56 kilobits par seconde pour une liaison analogique).
Page d'accueil	En anglais : homepage. C'est la première page d'un site Web.
Page personnelle	Pages créées par des particuliers. Elles apportent toute la richesse et la diversification qui font du Web un espace sans tabous et sans contraintes.
Page Web	Page correspondant à la visualisation d'un écran. Chaque site Web en comporte des dizaines, voire des centaines.
Pixel	Unité de mesure du plus petit point pouvant être affiché sur un écran d'ordinateur.
POP3	En anglais : Post Office Protocol. Protocole utilisé pour la messagerie pour rapatrier le courrier chez le fournisseur.
Plug-in	Application complémentaire qui traite d'un domaine particulier (son, vidéo) et que l'internaute doit télécharger pour en bénéficier.
Provider	Voir fournisseur.
Proxy	Serveur utilisé par les fournisseurs d'accès pour sécuriser les transmissions. Il a un rôle de filtre.
Push	Technique de récupération d'informations basée sur l'abonnement à des chaînes thématiques qui envoient directement l'information sans que l'internaute intervienne.
Quicktime	Logiciel permettant de visionner de la vidéo.
RealAudio	Plug-in autorisant la lecture audio.
RealPlayer	Plug-in remplaçant RealAudio et RealVideo et combinant audio et vidéo.
RealVideo	Plug-in autorisant la lecture vidéo.
Réseau	Nom donné à l'interconnexion d'ordinateurs, que ce soit local (à l'intérieur d'une entreprise) ou distant comme dans le cas d'Internet. Un réseau donne la possibilité de partager des matériels (imprimantes, modems), des logiciels, des données et de faire circuler de l'information de manière quasi instantanée.
Routeur	Matériel combinant les fonctions du modem et des fonctions d'aiguillage sur

	un réseau.
RTC	Réseau téléphonique commuté. C'est le nom des lignes de téléphone classiques en France (analogiques) par opposition aux lignes numériques (Numéris).
Signet	Voir Bookmark
Site Web	Ensemble de pages Web qui définissent un site accessible par une adresse Web.
SMTP	En anglais : Simple Mail Transport Protocol. Protocole général de diffusion, d'envoi et de réception du courrier électronique.
Spam	Technique de marketing sur le Web qui consiste à envoyer le même message à un très grand nombre de destinataires non demandeurs. Ce procédé, contraire à la Netiquette, pollue les boîtes aux lettres des internautes, encombrées par des e-mail indésirables.
Surfer	Se promener sur le Web, au gré des liens hypertextes et sans véritable objectif.
TCP/IP	Protocole de communication utilisé sur Internet, reconnu par tous les systèmes d'exploitation.
Téléchargement	Opération de récupération d'informations par transfert de fichiers entre deux ordinateurs. Les fichiers sont souvent compressés.
URL	Voir adresse Web. En anglais : Uniform Ressource Locator.
Virus	Programme ou fichier informatique capable de produire des dégâts plus ou moins importants sur l'ordinateur qui les reçoit. Leurs particularités est qu'ils se propagent dès qu'il y a échange de fichiers (par réseau ou par disquette, CD-ROM et tout système de stockage). Internet est le réseau le plus susceptible de propager des virus.
VRML	En anglais : Virtual Reality Modeling Language. Langage de programmation de création d'images en trois dimensions.
Web	Abréviation du terme anglais : World Wide Web. La partie la plus connue d'Internet. Sorte de toile d'araignée s'agrandissant sans cesse comprenant tous les sites Web de la planète. Le déplacement sur le Web se fait au moyen de liens hypertextes.
Webmaster	Personne qui a en charge le développement et la maintenance d'un site Web.
ZIP	Format de compression des fichiers très répandu.

## 5. Documentations et liens

Revue MISC (Multi-system & Internet Security Cookbook)

Dossier "Pour la sciences" L'art du secret HS de juillet/août 2002 (M 01930 – n°36)

Sécurité Internet – First Interactive – Quatre experts :B. Dunsmore, J. Brown, M. Cross et S. Cunningham (ISBN 2-84427-303-3) – 1<sup>er</sup> trimestre 2002 – [www.efirst.com](http://www.efirst.com)

Sécurité optimale – CampusPress – ISBN : 2-7440-0723-4 – site : [www.campuspress.fr](http://www.campuspress.fr)

Le site français sur le droit informatique : <http://www.legalis.net/>

Pour en savoir plus sur :

- ✓ la guerre "électronique" : <http://www.ndu.edu/inss/strforum/forum28.html>
- ✓ l'affaire Serge Humpich voir en particulier :  
<http://www.01net.com/article/132413.html>  
<http://www.legalis.net/cgi-iddn/french/affiche-legalnet.cgi?droite=actualite/affairehumpich/pagehumpich.htm>
- ✓ le jugement virtuel de l'Internet : <http://denoue.chez.tiscali.fr/> puis choisir "Le Procès"
- ✓ le virus CIH <http://www-rocq.inria.fr/codes/Eric.Filiol/index.html>
- ✓ les anti-virus : visitez les sites d'informations générales comme <http://www.secuser.com/>
- ✓ la charte de sécurité informatique : [http://www.bsdi.fr/formations/form\\_net.htm](http://www.bsdi.fr/formations/form_net.htm)
- ✓ les spam : <http://www.spamcop.com/>

- ✓ les hackers et leurs outils : <http://www.infoshackers.com>
- ✓ le cryptage et la stéganographie : StegFS
- ✓ les spy-ware : <http://abcdelasecurite.free.fr/> et aussi <http://membres.lycos.fr/spyware>
- ✓ le RSA : [www.rsa.com](http://www.rsa.com)