Rapport de stage

Guillaume Valadon

26 juin 2000

Table des matières

I Boreal Communications **3**

1 Présentation de la société **4**

2 Les domaines d'activité **6**
2.1 Administration des systèmes de l'information 6
2.2 Architecture des réseaux de communication 6
2.3 Sécurité des réseaux 6

3 Le savoir faire **8**

4 Les références **9**

5 Le stage **11**

II La sécurité **12**

6 L'enjeu **13**

7 La politique de sécurité **14**
7.1 La prévention 14
7.2 La protection 14
7.3 La définition du coût et du temps de reprise 15

8 Les menaces **16**
8.1 Les menaces 16
8.2 Ce qui est menacé 17

9 Types d'attaques **18**
9.1 Définitions préliminaires 18
9.2 Interruption 21
9.2.1 Exemple n°1 : SYN Flood 22
9.2.2 Exemple n°2 : Smurf 22
9.2.3 Exemple n°3 : Trinoo & TFN 23
9.3 Interception 24
9.4 Modification 26
9.5 Insertion 27

10 La sécurité en pratique **28**

III IPsec **31**

11 Présentation d'IPsec **32**
11.1 Définitions préalables 33

12 IP AH **34**
12.1 Description du protocole 35

13 IP ESP **37**
13.1 Description du protocole 38

14 Traitement **39**

15 IKE **40**

IV Conclusion **41**

Première partie

Boreal Communications

Chapitre 1

Présentation de la société

Depuis 1994, année de sa création, BOREAL Communications affiche une croissance soutenue qui se caractérise en 1998 par une très forte augmentation de capital (passage de 2,5 MF à 10 MF en avril 1998) et l'ouverture de deux agences en France à Lyon et à Toulouse.

Le chiffre d'affaires de Boréal Communications, en constante progression depuis sa création, double chaque année depuis 2 ans :

1994	230 kF
1995	250 kF
1996	500 kF
1997	1500 kF
1998	3600 kF

En janvier 2000, le rapprochement de BOREAL Communications et de IB Trois, groupe spécialisé dans le financement, l'intégration et le remarketing de solutions informatiques à valeur ajoutée, donne naissance à une nouvelle entité : IB-Group.com.

La répartition de l'activité selon les différents secteurs du marché est la suivante :

31%	telcos
26%	industrie
15%	service
9%	administration
19%	finance

On peut diviser l'activité de l'entreprise en deux grandes parties :
- commerciale
- production

La divison commerciale regroupe des commerciaux et des ingénieurs avant-vente. Les commerciaux réalisent la prospection et la détermination des besoins, les avant-vente quant à eux vont faire de la préconisation. Ils apportent leurs connaissances techniques aux besoins du client, et définissent la solution la plus

adaptée.

La production couvre les trois domaines d'activité du monde des réseaux et des systèmes d'informations :
- Administration des systèmes de l'information
- Architecture des réseaux de communication
- Sécurité des réseaux

A ces activités, s'ajoute également la télé-administration permettant la supervision et l'administration de systèmes à distance.

Boreal Communications a initié un partenariat actif avec les acteurs majeurs du marché, dont :
- CISCO
- FOUNDRY Networks
- Arrowpoint
- CABLETRON
- CheckPoint
- ISS (Internet Security Systems)
- MatraNet
- RSA
- SUN

Chapitre 2

Les domaines d'activité

2.1 Administration des systèmes de l'information

Il s'agit de l'étude et mise en place de plates formes d'administration et de supervision centralisées ou distribuées, gérant de manière interactive tous les éléments constitutifs des biens de l'entreprise.

2.2 Architecture des réseaux de communication

Il s'agit de la conception de réseaux (LAN et WAN) en prenant en compte l'existant, en définissant l'architecture cible et en employant les moyens suivants :

- hauts débits
- commutation de niveaux 3, 4 et 7, commutateurs intelligents
- caches hautes performances
- VLANs
- VPN
- Sondes d'analyse
- GigaBit ethernet
- ATM

Ainsi que l'étude de dimensionnement réseau et systèmes en fonction des applications.

2.3 Sécurité des réseaux

Il s'agit de l'audit, de la conception, du déploiement et de l'exploitation des plates-formes de sécurité compatibles avec la politique sécurité de l'entreprise et intégrant :

- Accompagnement certification ITSEC
- Audit
- Détection d'attaques en temps réel
- Audit de failles et certification

- Test d'intrusion
- Authentification dynamique
- Cryptage
- Firewall et filtrage
- Signature numérique
- Analyse de logs
- Antivirus
- Administration centrale des firewalls et des systèmes de sécurité

Chapitre 3

Le savoir faire

Boréal Communications a pour objectif de développer l'ensemble de son savoir-faire en représentant les plus grands acteurs du marché, et d'en assurer l'intégration.

Etudes A partir de l'expression des besoins, de l'existant et des contraintes, l'activité études préconise un ensemble de solutions pour la conception du réseau d'entreprise ou du système d'information. L'étude est concrétisée par un rédactionnel synthétisant l'ensemble des recommandations.

Audit Expertise Un spécialiste réseau intervient sur le site pour identifier et prendre en compte l'existant. Cette démarche se fait en étroite coopération avec les équipes en place et apporte un point de vue extérieur, permettant de cibler la nature des opérations à venir.

Cette activité fait l'objet d'un rapport précis sur l'état du réseau et sur les mesures à prendre à court, moyen et long terme. Elle couvre le précâblage, le réseau actif, la sécurité / sauvegarde et l'administration réseau, systèmes et applications.

Intégration / Réalisation Cette prestation est fondée sur une méthodologie et sur l'expérience des équipes d'ingénieurs et techniciens du département production.

Télé-Administration Avec la mise en place d'une plate-forme de supervision déportée, hébergée dans le centre de supervision de la société, la télé-administration permet la maîtrise du système d'information de l'entreprise 24 h/24. Elle fournit également des comptes-rendus et analyses sur l'activité du système.

Chapitre 4

Les références

Architecture réseaux & systemes

Abm Amro & Philips Audit technique. Etude d'évolution de l'architecture, maquettage et déploiement d'une architecture de campus (3 sites parisiens) en ethernet, fast ethernet, giga ethernet et phase de migration avec interconnexion vers un backbone ATM Token Ring. Gestion de projet de l'étude jusqu'à la recette de l'architecture.

Rhone Poulenc Rorher Déploiement d'un backbone ATM.

Price Waterhouse Refonte de l'architecture réseau entièrement commutée sur un backbone giga ethernet.

Administration réseaux & systemes

Credit du Nord Mise en place de solutions d'administration des systèmes, bases de données et applicatifs de l'ensemble des serveurs du Crédit du Nord et intégration dans leur framework existant.

Cegetel Mise en oeuvre de l'administration centralisée du NOC. Corrélation d'événements sur plusieurs milliers d'équipements.

Cedel (Luxembourg) Mise en place d'une solution d'administration de réseaux permettant le filtrage des alarmes et la supervision des différentes plates-formes.

Sécurité

Cabinet d'assurances Sécurisation et mise en place d'un serveur Web et d'un serveur de messageries Internet. Définition du nouveau plan d'adressage du réseau. Configuration de la politique d'accès (droits d'accès, backup). Mise en place et configuration d'un firewall gérant les flux.

Secteur carte a puce Audit de sécurité du réseau WAN en environnement X25, Numéris et Transfix. Etude des flux et sécurisation des données : chiffrement et authentification. Installation de routeurs sécurisés, BorderGuard. Formation des utilisateurs.

Secteur industriel Etude des solutions de sécurité dans le cadre de la mise en oeuvre d'une architecture Intranet/Internet.

Audit - Expertise

Auguste Thouard Analyse de l'impact sur le réseau et l'ensemble des sites d'Auguste Thouard d'une nouvelle application métiers pour le groupe. Définition, déploiement et migration de l'ensemble des architectures Lan et Wan, ainsi que des systèmes d'administration du SI.

Polygram Analyse de l'existant et audit des flux pour identifier et corriger des problèmes de performance liés à des aspects de configuration d'équipements réseaux et de défauts de certains applicatifs.

ISP / Operateurs Telecoms

None Networks (Freesbee) Etude, conception, mise en place du NOC de None Networks (réseau de commutation interne en Gigabit Ethernet) ainsi que maintenance avec garantie de continuité de services et de taux de disponibilité.

Integra Etude de conception et mise en place du centre d'hébergement des 350 serveurs de commerce électronique d'Integra.

France Telecom Interactive Etude et réalisation des politiques de sécurité et de filtrage des services Wanadoo, mise en place des systèmes de commutation de niveaux 2 et 3, étude et mise en place des plates-formes d'administration, étude et conception des outils de qualité de Services (FTI et Transpac).

Cegetel Conception, dimensionnement et mise en place du NOC Centre de Supervision de Cegetel pour les réseaux Internet, Frame Relay et accès commutés (mise en place des plates-formes d'administration, moteurs de corrélations, outils de qualités de services et de trakking, optimisations des fonctionnement des bases de données.

Lyberty Surf Réalisation du portail (audit, déploiement en architecture, administration et sécurité).

Chapitre 5

Le stage

Dès le début de mon stage, j'ai été acceuilli chaleureusement par l'ensemble du département sécurité. Sous la conduite de mon maître de stage Olivier Geoffre, j'ai pu découvrir de nombreuses facettes de la sécurité informatique.

J'ai ainsi eu la chance d'avoir accès à différents produits comme les firewalls FireWall-1 de Checkpoint et le boîtier NetSCreen 100 sur lequel nous avons décéler un deni de service au niveau de la console d'administration. J'ai également participé au maquettage d'une solution de filtrage d'URL à base de procy cache pour un parc de 20000 utilisateurs.

Je me suis de plus familarisé avec les concepts du chiffrement comme les algorithmes de hachage, à clés publiques, à clés secrètes, ainsi que les infrastructures à clés publiques (PKI : Public Keys Infrastructure).

Je vais donc présenter dans une première partie ce que j'ai pu retenir et comprendre de la sécurité. Je présenterais enfin une description du protocole IPsec sur lequel j'ai été amené à me documenter durant le stage.

Deuxième partie

La sécurité

Chapitre 6

L'enjeu

Les systèmes d'information stockent, traitent, et transmettent de l'information. C'est eux que l'on va chercher à protéger en raison du poids économique qu'ils représentent.

Typiquement un arrêt de service représente une perte sèche pour l'entreprise. Une banque utilisant un réseau pour passer des ordres d'achat ou de vente peut perdre plusieurs millions de francs par heure. La perte d'un système stockant la comptabilité d'une entreprise, ou des dossiers nécessaires à son activité peut se révéler dramatique. Il en va de même pour un système stockant la comptabilité d'une entreprise, ou des dossiers nécessaires à son activité.

L'image de marque d'une société peut également être compromise s'il est possible d'accéder à des données sensibles sans aucune protection. En 1999 par exemple, une société proposant de commander des fleurs via l'Internet s'était faite voler sa base clients contenant des numéros de cartes bleues ainsi que leurs dates d'expiration.

Il se peut également que le réseau d'une entreprise puisse être le point de départ d'attaques visant d'autres machines sur l'Internet. Sa crédibilité serait immédiatement remise en question, car elle n'a pas su se protéger convenablement et qu'elle ne maîtrise pas ce qui se passe sur son réseau.

L'enjeu de la sécurité est la protection du système d'information dont la perte ou l'arrêt de service sont souvent synonymes de pertes financières.

Chapitre 7

La politique de sécurité

La politique de sécurité va permettre de connaître et de mesurer les risques. On peut la définir selon trois points :
- la prévention
- la protection
- la définition du coût et du temps de reprise

Il s'agit d'un ensemble de décisions définissant l'attitude sécuritaire d'une organisation.

7.1 La prévention

Elle consiste à réunir des renseignements sur le système d'information. Il s'agit d'un inventaire de l'existant, ceci afin de connaître les risques auxquels on est exposé.

C'est une étape importante de la politique de sécurité qui va autoriser la détection précise des failles du système, et les erreurs de conception.

Savoir quelle version d'un système d'exploitation ou d'un service est en production sur une machine va permettre de le sécuriser en conséquence.

Cette phase va être réalisée grâce un audit sur site en collaboration avec l'équipe technique du client.

7.2 La protection

Après avoir déterminé la nature des systèmes en production, on va pouvoir apporte une solution adaptée. La protection pourra être effectuée de différentes façons, par exemple grâce à un firewall ou à une administration plus restrictive du service (on fera en sorte qu'un serveur smtp ne relaye que les mails de son domaine).

7.3 La définition du coût et du temps de reprise

Il se peut que la protection d'un système ne puisse être possible. On applique le principe suivant :

> *Le coût d'une politique de sécurité ne doit pas dépasser le coût de reprise.*

Ainsi, si l'arrêt de service d'un serveur de base de donnée durant une heure représente 50 kF de perte, il n'est pas résonnable d'investir dans un système redondant.

Chapitre 8

Les menaces

Nous venons de définir l'enjeu ainsi que la politique de sécurité, il convient dès lors d'expliquer ce qui menace le système d'information.

8.1 Les menaces

les menaces intentionnelles

Deux questions simples permettent de déterminer ces menaces :
- qui/pourquoi ? : le type de l'attaquant
- comment ? : la technique d'attaque

Le profil de l'attaquant peut aussi bien être une étudiante cherchant à s'amuser qu'un espion à la solde d'une société concurrente. Les attaques employées seront décrites dans un chapitre ultérieur.

Les menaces intentionelles se manifestent de différentes manières dont par exemple :

Accès illégitime : c'est une utilisation illégitime du système d'information. ex : un calculateur d'une université pourrait être utilisé par des tiers.

Vol : il s'apparente au vol physique, mais est très difficile à détecter tant les données numériques sont faciles à recopier.

Perturbation : il s'agit de la modification intentionelle des données ou du flux de donées afin de modifier le fonctionnement normal du système d'information.

Les menaces accidentelles

Elles regroupent à la fois les événements naturels à caractère catastophique comme les inondations, les incendies, mais aussi les erreurs de saisie ainsi que tous les types d'erreurs que l'on peut imaginer.

Sans aucune alimentation redondante, une coupure de courant peut à la fois rendre inacessible un serveur mais aussi détruire ses données de façon

irrémédiable. Pour pallier à cette menace, on peut par exemple prévoir un groupe électrogène et effectuer des sauvegardes de façon régulière.

8.2 Ce qui est menacé

Trois aspects d'un système d'information peuvent-être compromis :
- l'intégrité
- la confidentialité
- la disponibilité

L'intégrité concerne les données du système d'information. Elle vise à s'assurer qu'elles n'ont pas été altérées.

La confidentialité permet de s'assurer que l'on ne peut accéder aux données sans autorisation. Celle-ci se manifeste généralement sous forme d'un mot de passe.

La disponibilité d'un système d'information est sa capacité à effectuer à chaque instant les actions qu'on lui demande.

Chapitre 9

Types d'attaques

Le flux normal représente une communication s'effectuant sans problème entre Alice et Bib :

Ces types d'attaques représentent en fait les moyens par lesquels les menaces vont s'effectuer.

9.1 Définitions préliminaires

Au niveau du réseau

L'IP spoofing littéralement parodie d'IP permet à une machine possédant l'adresse IP E d'utiliser l'IP d'Alice afin de masquer sa véritable identité à une machine B.

Cette technique est possible car dans IP aucun mécanisme ne permet de déterminer l'identité de l'émetteur. N'importe qui peut donc se faire passer pour Alice.

Un autre problème relatif à l'implémentation d'IP dans les systèmes d'exploitation est la fragmentation. On supposera que la pile IP conserve les données les plus récentes (ex : Linux).

3000o de données TCP doivent être transportés, IP va devoir limiter la taille de celles-ci à 1000o par paquets. On aura alors :

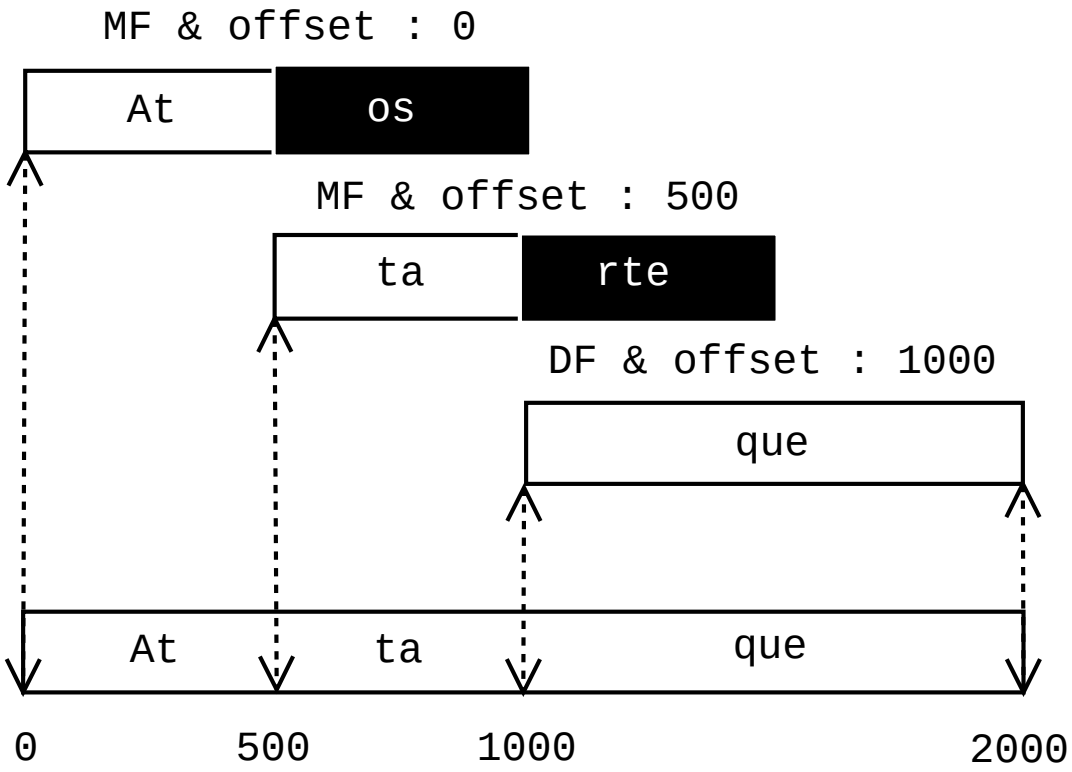
Premier paquet : MF & offset : 0

Deuxièmre paquet : MF & offset : 1000

Troisième paquet : DF & offset : 2000

A la reception de ce paquet, tout se passe bien la pile du recpteur refragemente les 3000o de données.

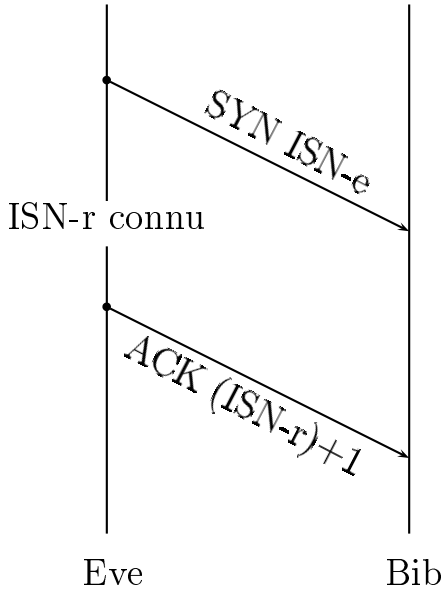
On peut lancer une attaque qui peut rester indétectée par une sonde (cf. la sécurité en pratique) en jouant sur les paramètres des paquets (on n'a représenté ici que les données et les champs significatifs de l'entête IP) :



Ainsi, à partir de paquets apparement anodins, une attaque vient d'arriver à destination peut-être sans avoir été détectée. On pourrait aussi compliquer la chose en envoyant les fragments dans le désordre.

TCP apporte un problème majeur à l'utilisation de cette technique lors d'une attaque : le numéro de séquence (ISN). Celui-ci assure entre autre que la réception des données se fait dans le bon ordre. Si A envoie un paquet ne possédant pas l'ISN correct, il sera rejeté par E. La triple poignée de main est donc impossible à établir, la connection ne se fera pas.

De plus, il est peu probable que E se faisant passer pour A afin se connecter à E reçoive la réponse de E qui sera destinée à B. La seule manière pour A de pouvoir établir cette connection sera de deviner l'ISN envoyé par E.



Cette prédiction de séquence est parfois possible car le choix de l'ISN au moment de la connection se fait de façon peu aléatoire, voire pas du tout.

Au niveau du système

La manière la plus efficace de compromettre un système est d'utiliser ses failles. Elles sont souvent induites par des erreurs de conception au niveau des applications.

Lors d'un appel à une fonction, le registre IP (Instruction Pointer) pointant sur l'instruction à exécuter après la fonction est sauvegardé dans la pile.

Imaginons maintenant que notre fonction déclare une variable sstr. Lors de l'appel de la fonction les registres IP puis EBP sont sauvegardés, l'espace pour sstr est alors alloué dans la pile. L'utilisateur peut soumettre un paramètre lors de l'execution du programme, celui-ci sera rangé dans sstr grâce à la fonction strcpy().

Soit le programme suivant :

```
$ cat exemple.c
#include<stdio.h>

void fonction(char* pouet) {
char sstr[8];

strcpy(sstr,pouet); /* fonction à la source du problème */

printf("Paramètre : %s\n",pouet);
```

```
}

main (int argc, char** argv) {
int i ;

if ( argc == 2 ) {
       char *lstr = argv[1] ; /* on range le paramètre dans lstr */
       fonction(lstr) ; /* on appele la fonction */
}

}
```

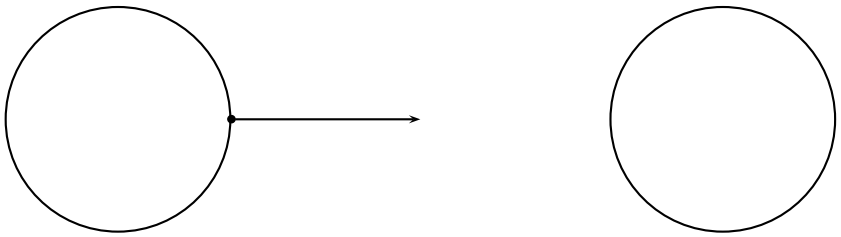
Mais que se passe-t-il si le gentil utilisateur soumet plus de 8 caractères, par exemple 17 :

```
$ ./exemple AAAAAAAAAAAAAAAAA
Segmentation fault (core dumped)
```

IP vient d'être écrasé, donc forcément ça crash. Un attaquant malicieux va alors chercher à fixer IP à une valeur souhaitée afin de faire executer le code voulu à la cible, celui-ci se trouvant au début du buffer alloué dans la pile.

Ce code est appelé shellcode et est dépendant de la plate-forme sur laquelle tourne l'application vulnérable car il est écrit en assembleur. Il permet de prendre la main sur la machine avec le maximum de droits possible. Ainsi, si on peut se servir d'un buffer assez grand pour écraser IP dans une application appartenant à root, il est fort probable que l'on devienne root. L'utilisation de strcpy() est fréquente et constitue une erreur de conception. On peut y remédier en utilisant strncpy() qui permet de spécifier la longueur de la chaine que l'on souhaite copier.

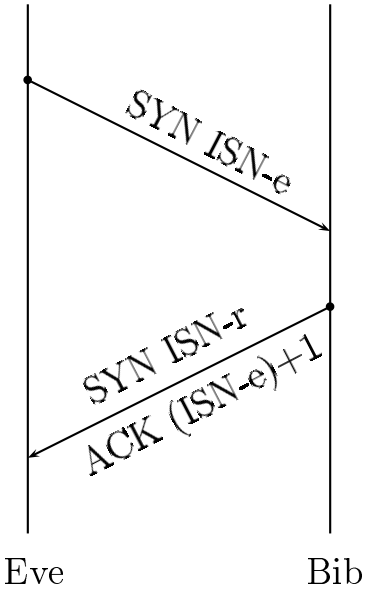
9.2 Interruption



L'attaque vise ici à interrompre la communication entre Alice et Bib en empêchant Bib de répondre aux requêtes d'Alice. Le plus souvent, on va la surcharger en lui envoyant de fausses requêtes. C'est ce que l'on appele un DoS : Denial of Service (Deni de Service).

9.2.1 Exemple n°1 : SYN Flood

L'attaquant cherche à saturer la table des connections en attente de Bib en envoyant des fausses demandes de connections.



Bib ne reçoit jamais d'ACK. Au bout d'un certain temps, elle ne peut plus accepter de connections supplémentaires.

Le logiciel firewall-1 de Checkpoint permet de se protéger contre ce type d'attaque en jouant sur le timeout TCP. On va le fixer à une valeur plus faible que sur la station à protéger. Ce système n'est cependant pas très au point car il est gourmand en ressources système.

Une sonde détectant ce type d'attaque pourrait demander au firewall de bloquer ces demandes de connection. Cependant si l'attaquant spoofe l'adresse source du paquet en utilisant celle du firewall, l'attaquant peut bloquer tout le trafic sur le réseau. Les sondes réagissant aux attaques ne sont pas forcément idéales dans notre cas.

9.2.2 Exemple n°2 : Smurf

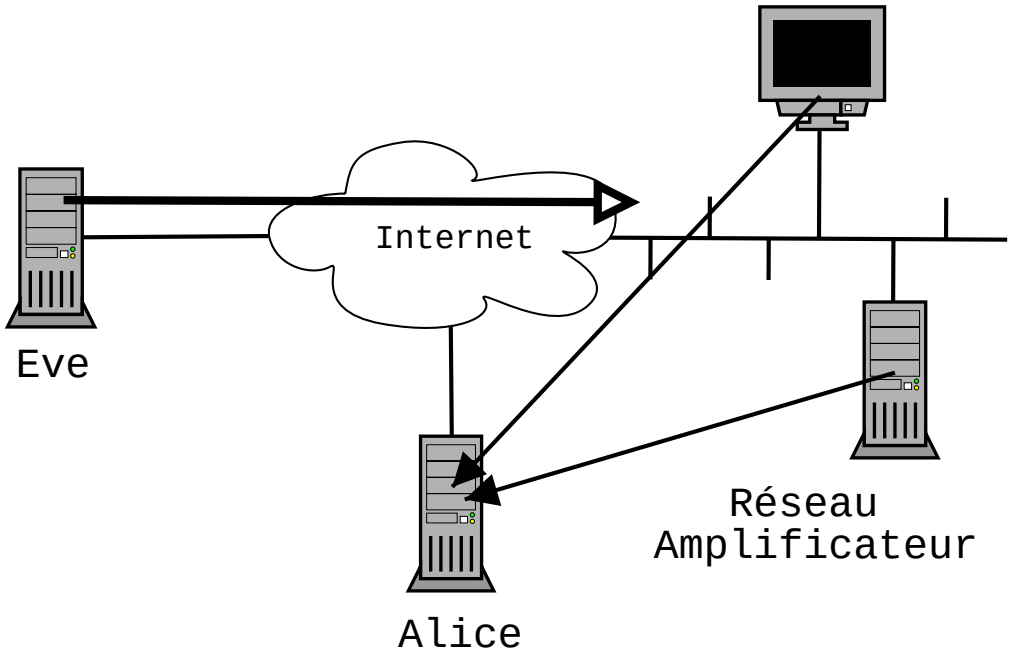
Toutes les classes d'adresses IP possèdent une adresse de broadcast. Si Eve envoie un paquet icmp echo_req à cette adresse de broadcast (tous les bits accordés aux hôtes sont à un), l'ensemble des machines du même réseau vont lui répondre en lui renvoyant des icmp echo_reply.

Voici la sortie de la commande ping sur ma machine :

```
$ ping 192.168.3.255
```

```
PING 192.168.3.255 (192.168.3.255) : 56 data bytes
64 bytes from 192.168.3.254 : icmp_seq=0 ttl=255 time=0.3 ms
64 bytes from 192.168.3.5 : icmp_seq=0 ttl=255 time=0.7 ms
64 bytes from 192.168.3.4 : icmp_seq=0 ttl=255 time=0.8 ms
```

On voit que 3 machines ont répondu à ma demande.



Si Eve décide de se faire passer pour Alice en spoofant son IP, elle va pouvoir rediriger toute les réponses sur cette dernière.

Pour un paquet envoyé au réseau amplificateur, on aura N paquets en sortie où N est le nombre de machines du réseau.

On peut dès lors facilement imaginer qu'en envoyant plusieurs paquets spoofés sur différents réseaux amplificateurs, Alice va être très rapidement saturée et ne pourra plus répondre aux autres requêtes.

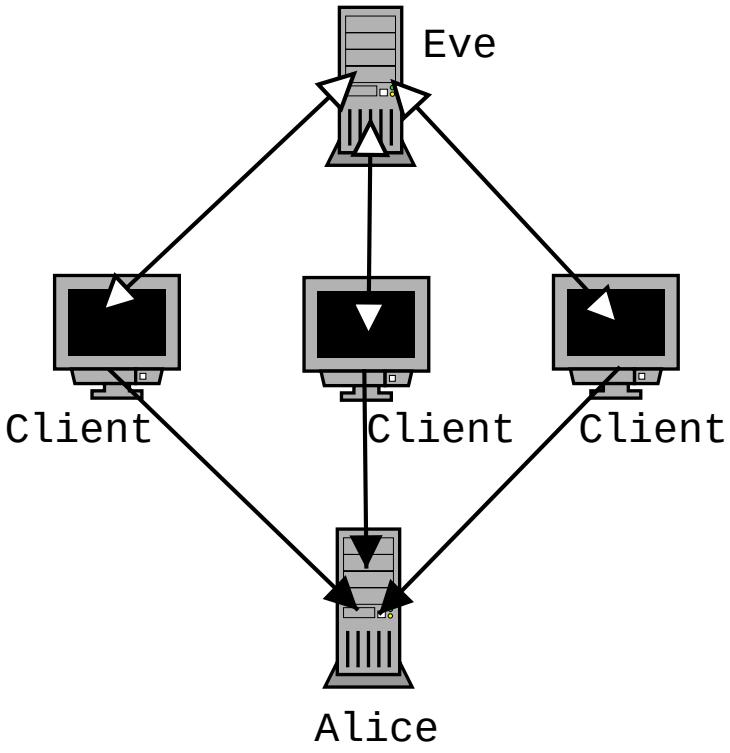
La protection contre cette attaque est l'affaire de tous les administrateurs. Ils se doivent d'empêcher les routeurs qu'ils gèrent de router les paquets à destination d'une IP de broadcast.

9.2.3 Exemple n°3 : Trinoo & TFN

Trinoo & TFN sont des logiciels fournissant un DDoS par le biais de clients et de serveurs.

Les clients sont placés sur les machines souvent à l'insu des administrateurs. Ils sont faciles à détecter car ils se logent sur des ports spécifiques, cependant

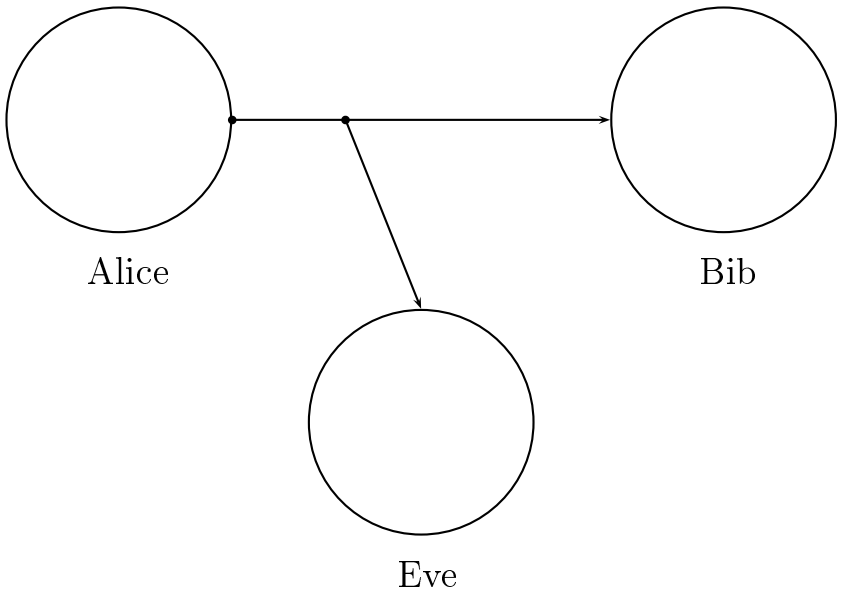
peu d'administrateurs s'en donnent la peine. Eve va commander les clients par le biais de commandes simples, et leur demander de lancer leurs attaques. Les clients sont généralement utilisables par tout le monde bien que protégés par mot de passe.



Des attaques de différentes natures peuvent être lancées comme le SYN Flood, le smurf, et l'UDP Flood. On peut également demander au client de spoofer leur adresse IP afin qu'ils soient plus difficilement détectables.

9.3 Interception

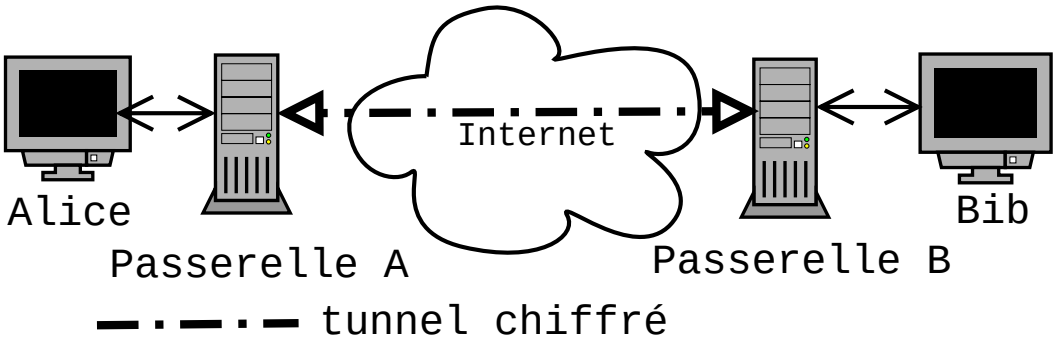
Il s'agit de l'espionnage des échanges entre Alice et Bib.



Sur un réseau local, une machine peut enregistrer l'ensemble du trafic y circulant, ceci est dû au fait que toutes les machines émettent sur le même brin . De même, si le chemin du paquet emprunte une zone compromise où cette machine espionne tous les échanges. La communication entre les deux machines n'est donc pas fiable, tout le monde ayant accès aux données envoyées ainsi qu'aux logins et mots de passes.

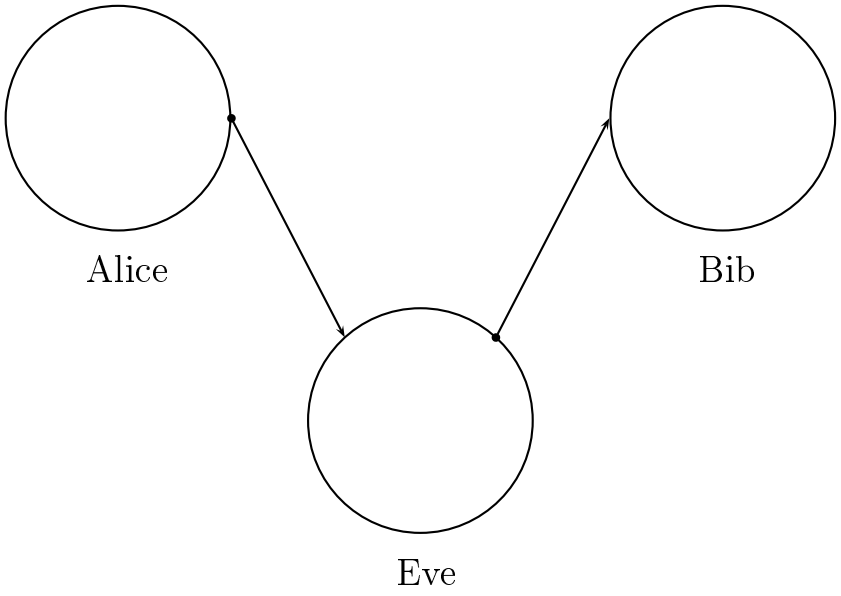
Pour s'assurer de la confidentialité de l'échange, on peut y intégrer le chiffrement. Le protocole ssl va permettre de sécuriser de nombreux protocoles au niveau tcp comme telnet (que l'on appele alors SSH : Secure Shell), imap, pop3, et HTTP. Cependant s'il l'on ne souhaite pas intégrer le chiffrement au niveau de la machine, on peut utiliser ce que l'on appele des tunnels également appelés VPN's (Virtual Private Network).

Le trafic entre Alice et Bib appartenant à des réseaux différents va être redirigé vers des passerelles qui chiffreront les paquets et les encapsuleront dans un nouveau paquet IP à destination du réseau distant. Les données circulant sur l'internet seront donc illisibles par un tiers. Les seules informations que l'on connaitra alors seront les IP des deux passerelles.



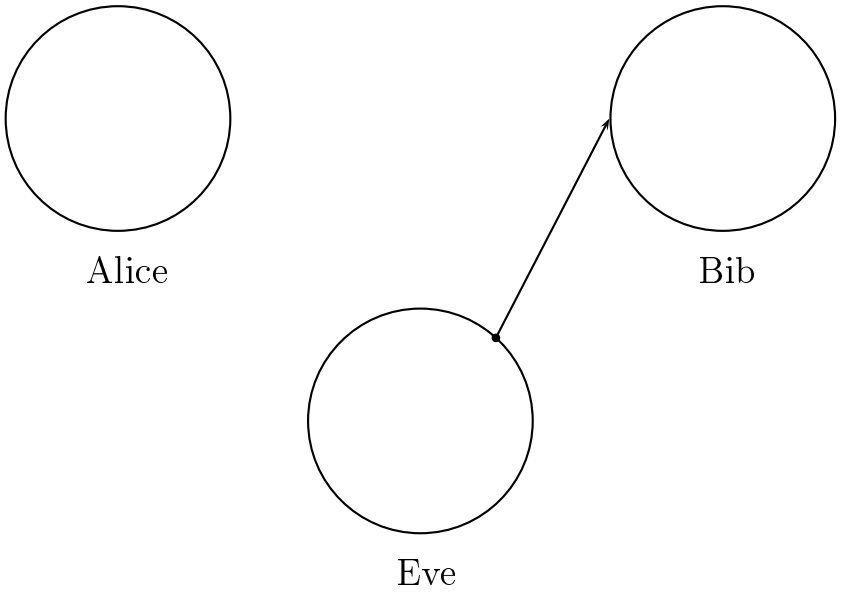
9.4 Modification

Eve va se faire passer pour Bib, intercepter le trafic et le transférer vers Bib.



Eve s'introduira dans la connection en y envoyant des données falsifiées, c'est le hijacking. Cette technique fait appel à la fois à l'interception et à l'insertion.

9.5 Insertion



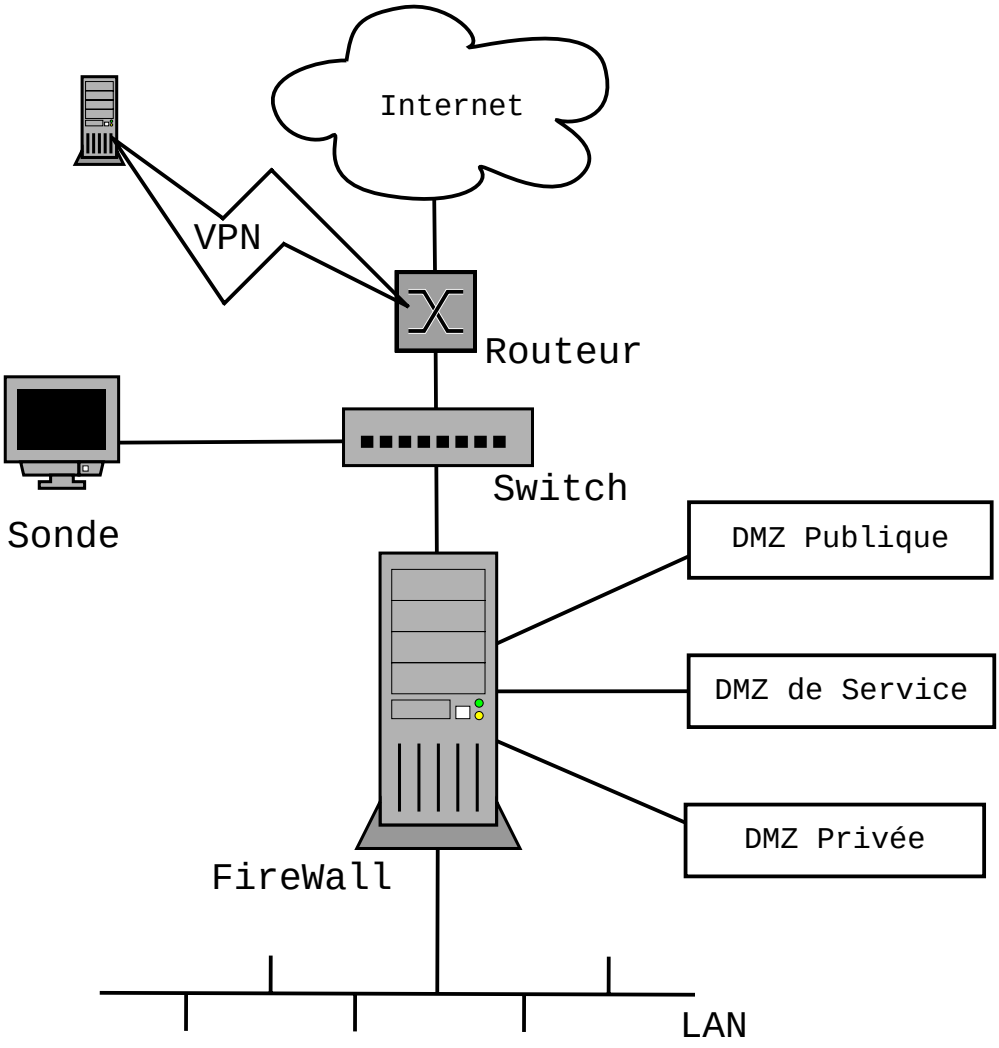
Il existe par exemple des logiciels capables de s'imiscer dans une session telnet et de prendre la main sur celle-ci.

En espionnant le réseau, Eve peut connaître des paramètres importants de l'échange entre Alice et Bib. Elle pourra par exemple en connaissant les ISN et les IP's effectuer un reset de la connection.

Certains services comme rlogin se servent de l'adresse IP source pour autoriser l'accès.

Chapitre 10

La sécurité en pratique



Le **firewall** est une plateforme de sécurité gérant les flux entre les différentes zone démilitarisées, le réseau local, et l'Internet. On désigne généralement par firewall un logiciel filtrant les paquets IP. Il en existe de différentes technologies :

routeur filtrant (ipfwadm & ipchains sous Linux) : filtre les adresses IP source et destination ainsi que les ports UDP et TCP. Il est rapide mais le filtrage n'est pas assez fin.

firewall/proxy aplicatif (M>Wall de MatraNet) : les paquets sont remontés au niveau applicatif et sont traités par des proxy's différents selon les services. Le traitement est très fin, mais ce contrôle total des données ralentit le traitement.

statefull inspection (standard de fait de CheckPoint, disponible dans FireWall-1) : les paquets sont interceptés au niveau du noyau du système d'exploitation. Ceci permet d'être beaucoup plus rapide que le système précédant tout en gardant une maîtrise totale de l'ensemble des données.

Le **routeur** va, en plus de servir de pont entre la LS et l'ethernet, permettre de réaliser des ACL (Access Lists). Celles-ci permettant de réaliser des fonctions de routeur filtrant en précisant si l'on accepte un paquet suivants les critères suivant :

le protocole de niveau supérieur

l'adresse IP source

l'adresse IP destination

le port du service

Les DMZ permettent de protéger un ensemble de machines en filtrant les flux entrant et sortant. On peut en trouver de différentes sortes :

DMZ Publique : ensemble des machines accessibles depuis l'Internet

DMZ Privée : ensemble des machines accessibles depuis le LAN

DMZ de service : on y installe les anti-virus par exemple

RMZ : point d'entrée des utilisateurs nomades sur le réseau

La **sonde** va servir d'informateur quant aux malversations se produisant sur le réseau. On utilise la fonction *port mirroring* du switch ce qui va permettre à la sonde de voir tout le trafic Internet <->Firewall. Il est aussi habituel de la brancher sur un HUB en s'assurant qu'elle ne possède pas d'IP, afin qu'elle ne puisse être la cible d'une attaque.

Le **VPN** est un tunnel chiffré permettant de relier deux sites distants en s'appuyant sur l'Internet.

On a dit plus haut que le firewall gérait entre autres les flux de données. Nous allons ici étudier celui du FTP.

Soit un serveur FTP dans la DMZ publique. On va empêcher les flux FTP vers la DMZ mais autoriser le traffic du LAN vers la DMZ. On aura les règles

suivantes :

- LAN :FTP ->DMZ :FTP = ACCEPTER
- partout :FTP ->DMZ :FTP = INTERDIRE

Troisième partie

IPsec

Chapitre 11

Présentation d'IPsec

IPsec permet de se prémunir des attaques les plus sérieuses : l'IP spoofing et l'interception. C'est un jeu de protocole et d'algorithmes permettant de sécuriser les données au niveau d'IP. Il offre ainsi un service de chiffrement et d'authentification aux protocoles de niveaux supérieurs de façon transparente à la fois pour l'utilisateur mais aussi pour les applications. Il est facultatif en IPv4 mais obligatoire en IPv6.

IPsec se place avant et après IP dans le modèle en couches du monde IP. En effet, il traite les paquets sortants avant de les passer à IP et fait de même avec les paquets IPsec entrant.

IPsec offre des services d'intégrité des données, d'authentification de leur origine, de confidentialité, et de protection contre le rejeu. Il s'agit en fait de s'assurer que les données échangées entre deux machines à un instant t, ne pourront pas être utilisées plus tard par un tiers.

IPsec fait intervenir différents composantes :

les protocoles AH (Authentification Header) et ESP (Encription Security Payload)

les associations de sécurité

la gestion des clés

Les algorithmes de chiffrement et de hachage ne sont pas à proprement parlé des composants d'IPsec. Les protocoles AH et ESP ont en effet été conçus pour être indépendants de ces derniers. Cependant, il existe des RFC[1] décrivant les algorithmes utilisés avec AH et ESP.

Une implémentation d'IPsec opère au niveau d'une machine ou bien d'une passerelle. Il existe deux modes d'utilisation : le mode transport et le mode tunnel.

[1] Request For Comment : `ftp://ftp.ripe/net`

En mode transport, les données IP sont protégées par les mécanismes d'IPsec et de façon transparente en raison du système de protocole en couches. On a :

En mode tunnel, les données IP sont en fait un paquet. Ceci permet de relier deux sites distants - possédant éventuellement des IP privées non routables - par le biais d'un tunnel protégé en utilisant les ressources de l'Internet.

11.1 Définitions préalables

Une association de sécurité est une connection simplex offrant des services de sécurité au trafic qu'elle transporte. Une connection bi-directionnelle sécurisée recquiert 2 AS. Elles contiennent l'ensemble des paramètres associés à une communication donnée.

Une association de sécurité est définie uniquement par un SPI (Security Paramater Index, index des paramètres de sécurité) , l'adresse IP destination et le protocole à utiliser (AH ou ESP). On peut appliquer à la fois AH et ESP, on parlera alors de bundle de SA. ESP sera toujours inséré après AH dans le mode transport, afin d'authentifier les données chiffrées.

La SAD (Security Association Database) stockera ces SA et leurs paramètres respectifs.

Les SA sont configurables manuellement par l'administrateur mais ceci est peut pratique pour de grands sites, c'est pourquoi elles vont pouvoir être gérées dynamiquement. Le mécanisme de négociation des SA pour IPsec est appelé ISAKMP (Internet Security Association Key Management Protocol). Il s'agit en fait d'un ensemble de briques permettant de faire des protocoles d'échange de clés. Dans le cadre d'IPsec, on utilise IKE (Internet Key Exchange).

La SPD (Security Policy Database) va déterminer la façon dont sont traités les paquets. Elle est définie manuellement par l'administrateur. Elle est composée d'un ensemble de règles portant sur les entêtes IP et transport et indique quelle SA sera utilisée.

Chapitre 12

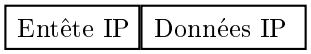
IP AH

Le protocole Authentification Header est décrit dans la rfc 2402, et fournit les fonctionnalités suivantes :

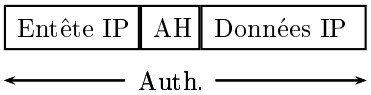
- authentification de l'origine des données (l'hôte en mode transport ou la passerelle en mode tunnel)
- intégrité de la transmission
- protection contre le rejeu

L'authentification permet à un système de déterminer assurément avec qui il communique. L'intégrité permet de s'assurer qu'il est impossible que le paquet ai été modifié durant le transport. La protection contre le rejeu permet quant à elle qu'aucune information de l'échange ne puisse être réutilisée utltérieurement par un tiers.

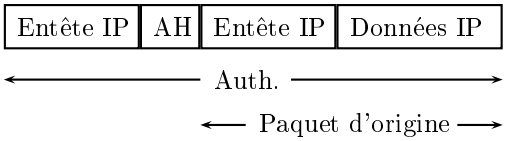
Les schémas suivants montrent à quelles parties du paquet s'applique AH :



Mode transport :

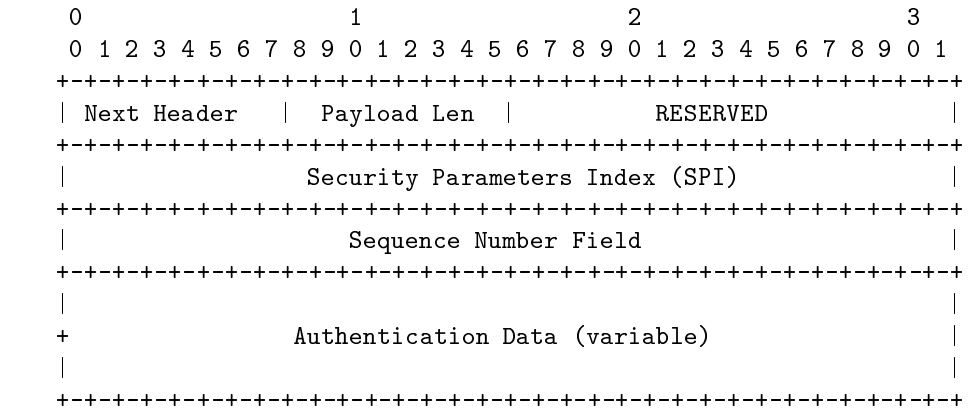


Mode tunnel :



12.1 Description du protocole

Le champ protocole de niveau supérieur de l'entête IP précédant AH contiendra la valeur 51.



Description des champs :

Next Header : type de l'entête suivant

Payload Len : longueur de l'entête AH en mots de 32 bits moins 2

Security Parameters Index (SPI) : identifie l'association de sécurité pour ce datagramme IP

Sequence Number : obligatoire, permet la protection contre le rejeu

Authentication Data : assure l'authentification et l'intégrité des données - multiple de 32 bits en IPv4

Le champ Données d'Authentification contient un ICV (Integrity Value Check : valeur de vérificayion d'intégrité). Cet ICV est calculé par l'expéditeur à partir des données à protéger grâce à un algorithme de hachage. Ce type d'algorithme permet de définir une signature unique pour chaque message, celle-ci ne pouvant redonner le message original. MD5 et SHA-1 sont ceux employés avec AH. Le DES peut également être utilisé (rfc 2405).

Les données d'authentification sont calculées sur :

les champs d'IP non modifiés durant le transit

l'entête AH (les champs autre que les données d'authentifcation)

les données de niveau supérieur

Si un champ est modifiable durant le transit, il prendra une valeur nulle pour le calcul des données d'authentification. Idem pour la data de AH.

Les champs invariants d'IP sont les suivants :

Version

Longueur de l'entête

Longeur Totale

Identification

Protocole de niveau supérieur (dans notre cas, il a 51 par valeur)

Adresse IP Source

Adresse IP Destination

Si les données d'authentification ne sont pas multiples de 32 bits (en IPv4), des octets de bourrage seront rajoutés. Ils seront comptés lors du calcul de la longeur de l'entête.

Pour vérifier la valeur des données d'authentification, le récepteur va sauvegarder sa valeur puis la mettre à zéro ainsi que celle des champs variants puis effectuer les calculs adequats. Si la valeur calculée correspond à celle reçue, le message n'a pas été altéré durant le transit et a bien été émis par l'interlocuteur défini dans la SA ad hoc.

Chapitre 13

IP ESP

Le protocole Encapsulating Security Payload est décrit dans la rfc 2406 et offre les fonctionnalités suivantes :

confidentialité

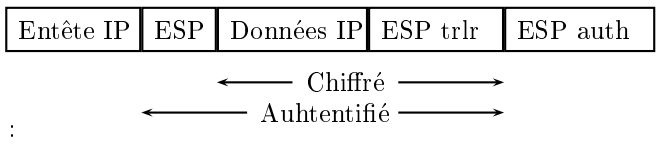
authentification de l'origine

anti-rejeu

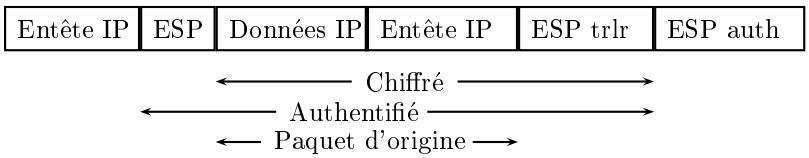
ESP fournit ce service de confidentialité à partir du chiffrement des données. Il permet aussi de gérér l'authenticité des données mais à la différence de AH elle ne porte pas sur le paquet externe. Cette fonctionnalité n'est donc pas redondante à celle de AH. Pour authentifier et chiffrer correctement des paquets, on utilisera des bundles de SA en appliquant ESP avant AH.

Tout comme AH, ESP peut s'employer en mode transport et en mode tunnel :

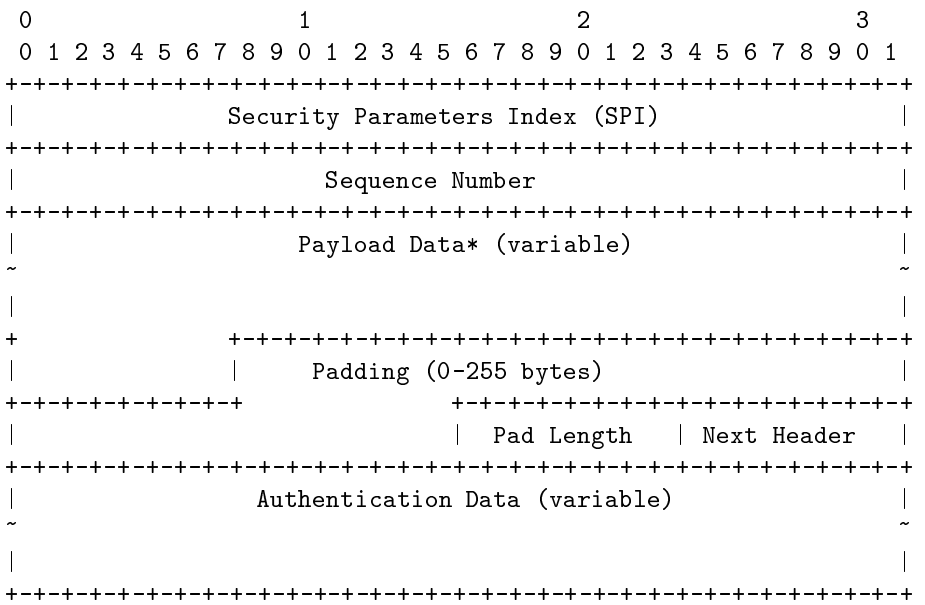
Mode transport :



Mode tunnel :



13.1 Description du protocole



Description des champs :

SPI : identifie l'association de sécurité pour ce datagramme IP

Sequence Number : permet la protection contre le rejeu

Payload Data : données protégées par les mécanismes d'ESP

Padding : bourrage relatif à l'algorihtme employé et à la taille des données à traiter

Pad Length : nombre d'octets de bourrage précédant ce champ

Next Header : type de l'entête suivant

Auhtentification Data : authentifie le paquet ESP

Padding, Pad Length, et Next Header sont appelés trailer ESP, littéralement remorque ESP.

Les données à protéger seront placées dans le champ Payload Data, des octets de bourrage seront éventuellement employés. Les champs Payload Data, Padding, Pad Length et Next Header seront chiffrés.

Si l'authentification du paquet est requise, le chiffrement sera effectué avant elle. Ceci permet au récepteur de déterminer si le paquet n'a pas été altéré durant le transport, avant de se lancer dans les coûteuses fonctions de déchiffrement du message.

Chapitre 14

Traitement

Le type de flux va déterminer un traitement particulier des données, on distingue :

traitement du flux sortant

Lorsque la couche IPsec reçoit des données à envoyer, elle va rechercher dans la SPD ce qu'elle doit en faire. Elle récupère les caractériqtiques pour cette SA et va consulter la SAD. Si elle trouve une SA correspondante, elle va l'utiliser sinon elle va faire appel à IKE afin d'en établir une nouvelle.
Le paquet sera alors envoyé.

traitement du flux entrant

Lorsque la couche IPsec reçoit un paquet, elle va vérifier s'il s'est vu appliquer un service d'IPsec. Elle va ensuite interroger la SAD afin de connaître la SA nécessaire à la vérification et/ou au déchiffrement du paquet. La SPD est alors consultée pour vérifier si la SA appliquée au paquet correspond à celle requise par les paramètres de sécurité.
Le paquet est alors passé à la couche supérieure.

Chapitre 15

IKE

IKE (Internet Key Exchange) va permettre de gérer automatiquement les associations de sécurité ainsi que les clés de session (clef dont la durée de vie est celle de la session). La gestion des clés est donc séparée des mécanismes de sécurité AH et ESP, elle n'y est liée que par les associations de sécurité. Il fonctionne indépendamment des mécanismes pour lesquels il travaille. IL est décrit dans la rfc 2408.

Ce protocole est en fait une utilisation d'ISAKMP ainsi que du système d'échange de clés Oakley.

La négociation de l'association de sécurité IPsec s'établit en deux phases :

- **phase 1** les paramètres IKE sont négociés pour créer une connection sécurisée afin de protéger les prochains échanges, les protagonistes sont authentifiés

- **phase 2** les paramètres de sécurité relatifs à une association de sécurité vont être négociés

Il existe deux modes pour la phase 1 : le main mode et l'agressive mode, et un seul pour la phase 2 : le quick mode avec ou sans une fonctionnalité de PFS. Le PFS (Perfect Forward Secrecy) permet de s'assurer que la découverte des secrets à long terme ne va pas permettre de remonter aux clés de sessions.

Quatrième partie

Conclusion

L'actualité de ces derniers mois nous a montré l'importance de la sécurité. Notamment avec l'attaque de serveurs comme ceux de Yahoo par des DDoS. Plus récemment la diffusion du virus "I love you" a remis en question de nombreuses politiques de sécurité.

La prise de conscience de la part des entreprises et des particuliers des risques qu'ils encourent a permis à la sécurité informatique de devenir l'un des domaines qui a connu et qui connaîtra la plus forte évolution ces prochaines années.