

# Etude bibliographique sur les firewalls

Olivier PAUL

Etude effectuée dans le département  
Réseaux et systèmes multimédias  
de Telecom Bretagne  
sous la direction de Mr. Pierre ROLIN

Mars 1996



# Table des matières

<b>1</b>	<b>Introduction</b>	<b>3</b>
1.1	Objectif de cette bibliographie . . . . .	3
1.2	Quels problèmes résoudre? . . . . .	3
1.3	Qu'est ce qu'un firewall? . . . . .	5
<b>2</b>	<b>Services de sécurité</b>	<b>6</b>
2.1	Services ISO . . . . .	6
2.2	Services non ISO . . . . .	7
<b>3</b>	<b>Mécanismes de mise en œuvre</b>	<b>9</b>
3.1	Mécanismes ISO . . . . .	9
3.1.1	Les mécanismes de chiffrement . . . . .	9
3.1.2	Le mécanisme de signature numérique . . . . .	10
3.1.3	Les mécanismes d'intégrité . . . . .	11
3.1.4	Les mécanismes de contrôle d'accès . . . . .	12
3.1.5	Le mécanisme d'échange d'authentification . . . . .	13
3.1.6	Le mécanisme de bourrage . . . . .	15
3.1.7	Le mécanisme de contrôle de routage . . . . .	15
3.1.8	Le mécanisme de notarisation . . . . .	15
3.1.9	Les mécanismes de gestion des clefs . . . . .	16
3.1.10	Le mécanisme de détection d'évènements . . . . .	17
3.2	Mécanismes non ISO . . . . .	18
3.2.1	Le mécanisme d'audit de sécurité . . . . .	18
3.2.2	Les mécanismes de contrôle de contenu . . . . .	19
3.2.3	Les mécanismes de dissimulation d'informations . . . . .	19
<b>4</b>	<b>Produits diffusés</b>	<b>20</b>
4.1	Relations entre services et mécanismes . . . . .	21
4.2	Relations entre services et couches . . . . .	24
<b>5</b>	<b>Conclusion</b>	<b>26</b>

# Chapitre 1

## Introduction

### 1.1 Objectif de cette bibliographie

Cette bibliographie a pour objectif de décrire l'état de l'art en matière de firewall.

Pour cela nous présenterons d'abord les problèmes que celui-ci est censé résoudre ainsi qu'une définition générale des firewalls.

Nous décrirons les services pouvant théoriquement être fournis par les firewalls ainsi que les mécanismes utilisés pour cela.

Nous établirons ensuite les liens entre services, mécanismes et couches dans certains produits commerciaux.

Pour finir nous montrerons en quoi les firewalls répondent aux problèmes développés en introduction.

### 1.2 Quels problèmes résoudre ?

L'interconnexion d'une machine ou d'un réseau à un système ouvert accroît les risques d'attaque pour plusieurs raisons:

- L'attaque peut être menée depuis un nombre de points plus important.
- Le système n'est plus physiquement protégeable étant donné son étendue.
- Les ordinateurs reliés au réseau sont d'autant plus exposés qu'ils offrent un grand nombre de services. La complexité de ceux-ci les rend dangereux.

Dans internet cela se traduit par un certain nombre de problèmes décrits dans [CB94]:

- Le vol de mots de passe.  
Les attaquants récupèrent le fichier contenant les mots de passe. Ils trouvent ensuite les mots de passe les plus faibles au moyen d'une attaque par

dictionnaire.

Il est par exemple possible de récupérer un fichier de mot de passe par *FTP* et d'en extraire les mots de passe les plus faibles par un utilitaire comme *crack* ou *cops*.

Le vol de mot de passe peut également être fait par écoute passive d'une voie sur lesquels ceux-ci circulent.

- Les attaques "sociales".

Les attaquants cherchent à emprunter l'identité de quelqu'un et à se servir de celle-ci afin de faire exécuter à une autre personne des actions allant à l'encontre de la sécurité.

Par exemple un attaquant peut écrire une lettre à un utilisateur en se faisant passer pour un administrateur en lui demandant de changer son mot de passe ou encore de lui fournir celui-ci sous un prétexte quelconque.

- Les erreurs et les portes dérobées.

Les attaquants trouvent soit par l'analyse d'un système, soit par hasard une erreur ou une porte dérobée. Celle-ci est exploitée pour acquérir des droits sur le système.

Les bugs de certaines versions de *sendmail* ou de *finger* constituent des exemples de logiciels permettant ce type d'attaque.

- Les problèmes d'authentification.

Les logiciels font souvent confiance à l'adresse IP pour attribuer des droits à un utilisateur. Malheureusement cette adresse peut être facilement modifiée et ne constitue pas un moyen d'authentification valide. Un attaquant peut utiliser ce type d'erreur pour avoir accès à une machine en utilisant le fait que celle-ci se base sur cette information pour effectuer du contrôle d'accès.

C'est ce qui se passe dans le cas de *rlogin*, une commande unix permettant de se connecter à une machine distante sans se réauthentifier.

- La divulgation d'informations.

La divulgation d'information peut constituer une menace non seulement directe dans le cas d'informations sensibles (plans techniques, fichier de clientèle, ...) mais également indirecte car elle peut mettre en jeu la sécurité d'un système:

- soit pour réaliser des attaques classiques en récupérant certaines informations comme les adresses des machines d'une entreprise ou les fichiers de mots de passe. Ceci peut être fait au moyen des services *DNS* ou *NIS*.
- soit pour réaliser des attaques "sociales" en prenant des informations sur le possesseur d'un compte. Celles-ci peuvent être obtenues par des services comme *finger* ou *WWW*.

- Les dénis de service.

Les dénis de service sont des attaques qui ne permettent pas d'obtenir des droits sur un système mais qui relèvent plutôt du vandalisme. L'exemple le plus simple de ce type d'attaque est la saturation d'une station au moyen de mails.

### **1.3 Qu'est ce qu'un firewall?**

Un firewall est un dispositif qui permet de protéger une machine ou un ensemble de machines d'attaques non directes.

Un firewall se place généralement entre le réseau interne considéré comme sûr et qu'il a pour but de protéger et le réseau externe qui sera considéré comme non sûr. Le réseau externe peut être un réseau public ou un réseau privé.

Dans la pratique les firewalls sont formés d'un ou plusieurs éléments. Ces éléments sont assemblés de manière à fournir des services de sécurité.

## Chapitre 2

# Services de sécurité

La norme ISO 7498-2 [ISO90] introduit plusieurs services de sécurité relatifs à l'interconnexion des systèmes ouverts. A ceux-ci on peut ajouter un certain nombre de services non-ISO.

### 2.1 Services ISO

- authentification de l'entité homologue.  
Ce service est fourni lors de l'établissement de la phase de transfert de données d'une connexion pour confirmer à une entité que l'entité homologue est bien l'entité déclarée.  
Ce service garantit uniquement qu'une entité n'essaie pas de se déguiser ou de rejouer une ancienne connexion de façon non autorisée.  
L'authentification peut être unilatérale ou mutuelle.
- authentification de l'origine des données.  
Le service d'authentification de l'origine des données confirme la source d'une unité de donnée. Cela signifie que chaque unité de donnée possède une preuve d'identité ou une partie de preuve d'identité.
- contrôle d'accès.  
Ce service assure une protection contre une utilisation non autorisée des ressources accessibles par une entité ou un groupe d'entités. Ce type de protection peut être appliqué pour différents type d'accès à une ressource ou pour tous les types d'accès.  
Ce service a été le premier fourni par les firewalls et constitue encore aujourd'hui leur fonction principale.
- confidentialité des données.  
Le service de confidentialité des données assure la protection des données

contre toute divulgation non autorisée.

La confidentialité peut être de plusieurs types:

- En mode connexion ou sans connexion.  
la confidentialité en mode connexion assure la protection des données à protéger au cours d'une connexion.  
la confidentialité en mode sans connexion assure la protection des données à protéger dans une unité de donnée de service.
- Totale ou sélective par champ.  
La confidentialité totale protège toutes les données de l'utilisateur.  
La confidentialité sélective par champ assure la protection de champs sélectionnés dans les données de l'utilisateur.

- confidentialité du flux de données.  
Ce service assure la protection des informations qui pourraient être dérivées de l'observation des flux de données.
- intégrité des données.  
Le service d'intégrité des données permet de détecter toute donnée modifiée, insérée, supprimée ou rejouée.  
Le contrôle d'intégrité peut se faire:

- En mode connexion ou en mode sans connexion.
- Avec reprise ou sans reprise.
- De manière totale ou sélective par champ.

Il est à noter que dans le cadre d'une communication en mode sans connexion, seule la modification d'une unité de donnée ou d'un champ sélectionné peut être détectée.

- non répudiation avec preuve de l'origine.  
Le destinataire reçoit la preuve de l'origine des données. Cette preuve le protège de toute tentative de l'expéditeur de nier le fait d'avoir envoyé les unités de données ou leur contenu.
- non répudiation avec preuve de remise.  
L'expéditeur des données reçoit la preuve de la remise des données. Cette preuve le protège de toute tentative du destinataire de nier le fait d'avoir reçu les unités de données ou leur contenu.

## 2.2 Services non ISO

- innocuité des données.  
Ce service assure que les données échangées ne constituent pas une menace.  
Les menaces peuvent être de plusieurs ordres (économique, sécurité...).

- intégrité du système.  
Le service d'intégrité du système assure le fait que le système n'a pas été modifié de façon non autorisée.
- disponibilité du système.  
Ce service assure que l'accès par une entité, un utilisateur ou un processus autorisé aux services offerts par le système doit toujours être possible.
- auditabilité.  
Le service d'auditabilité assure la capacité du système à fournir des rapports concernant l'activité du système et de ses usagers.

## Chapitre 3

# Mécanismes de mise en œuvre

La norme ISO 7498-2 [ISO90] décrit un ensemble de mécanismes qui, associés à certains mécanismes non ISO, permettent de fournir les services décrits précédemment:

### 3.1 Mécanismes ISO

#### 3.1.1 Les mécanismes de chiffrement

Les algorithmes de chiffrement peuvent se classer en trois catégories

- algorithmes de chiffrement réversibles symétriques.

Ces algorithmes utilisent une clé secrète. Ils sont dits symétriques car la connaissance de la clé de chiffrement implique la connaissance de la clé de déchiffrement et vice-versa.

L'algorithme à clé secrète le plus connu est le DES il a été proposé en 1977 par le NBS dans [NBS77]. Il est basé sur une série de permutations. Cependant l'augmentation de puissance des machines pourrait dans l'avenir remettre la sécurité du DES en cause (en raison d'une longueur de clé trop faible).

Pour répondre à ce problème des algorithmes plus récents comme IDEA (proposé en 1992 dans [Lai92]) et SKIPJACK (proposé en 1994 dans [NIS94]) sont de plus en plus fréquemment utilisés.

- algorithmes de chiffrement réversibles asymétriques.

Ces algorithmes utilisent des clés publiques et des clés privées. Ils sont

dits asymétriques car la connaissance de la clef privée ou clef de chiffrement à partir de la clef publique ou clef de déchiffrement est difficile et vice-versa. Leurs principes d'utilisation ont été présentés pour la première fois en 1976 dans [DH76].

L'algorithme à clef publique le plus connu est RSA ([RR78]) et est basé sur le problème du logarithme discret.

D'autres problèmes ont été proposés pour construire des algorithmes de chiffrement (comme par exemple le problème du sac à dos donné dans [MH78]) mais leur "complexité" est moins grande ce qui fait qu'ils sont moins utilisés.

L'inconvénient des algorithmes à clef publique est que les temps de calcul des fonctions sont nettement plus importants que dans le cas des algorithmes à clef privée ce qui les rend inadaptés au transfert de volumes importants de données.

- algorithmes de chiffrement irréversibles.  
Ils peuvent utiliser ou non une clef. Celle-ci peut être publique ou secrète. Une application des algorithmes de chiffrement irréversible est par exemple le stockage de mots de passe.

Les mécanismes de chiffrement peuvent être mis en œuvre à plusieurs niveaux (couches 1,3,4 et 7 du modèle OSI). Ainsi [Azi94] et [IB93] proposent un chiffrement au niveau 3. [MJR94] utilise lui un chiffrement au niveau physique dans le cas de liaison point à point. [Zim92] présente lui un mécanisme de niveau application, PGP, adapté à la protection des mails.

### 3.1.2 Le mécanisme de signature numérique

Le mécanisme de signature numérique peut être décomposé en deux parties:

- Une procédure de signature.  
Pour cela le signataire utilise une information qui lui est propre.
- Une procédure de vérification.  
Pour cela on utilise des procédures et une information qui sont disponibles dans le public. Cette information ne permet pas de déduire l'information du signataire.

Les fonctions à clef publique peuvent constituer des fonctions de signature. Cependant des fonctions propres ont été proposées. Elles sont construites de telles sorte qu'elles produisent un message de taille fixe à partir d'une clef et d'un message de longueur variable. La plus connue est DSS, elle reste cependant peu utilisée en pratique.

Des solutions intermédiaires existent, elles consistent à utiliser une fonction qui produit à partir d'un message de longueur variable un résumé. Ce résumé est ensuite chiffré. Les fonctions de ce type les plus connues sont MD2 ([Kal92]),

MD4 ([Riv92a]), MD5 ([Riv92b]) et SHA (proposée par le NIST et la NSA).

Ce mécanisme sert généralement à fournir le service d'authentification de l'origine des données. Il peut dans ce cas être mis en œuvre à des niveaux divers. Ainsi [IB93] et [Azi94] utilisent ce mécanisme au niveau réseau alors que [Lin93] propose l'utilisation de ce mécanisme au niveau application dans PEM pour la protection des mails.

[Spa94] et [RS93] utilisent ce mécanisme afin de fournir le service d'intégrité du système.

[Che94] propose une méthode de signature intéressante utilisant un mécanisme immunologique humain. Les auteurs utilisent une copie inverse du contenu à protéger. La copie inverse protégeant le contenu et vice-versa. En choisissant le nombre de copies (ce nombre est généralement assez faible) il est possible de déterminer la probabilité de détection d'attaques.

### 3.1.3 Les mécanismes d'intégrité

On peut décomposer les mécanismes d'intégrité en deux catégories:

- Ceux qui permettent d'assurer l'intégrité d'une unité de donnée.  
Il consiste à ajouter une quantité d'information redondante à chaque unité de donnée. Cette information redondante peut être une information supplémentaire (par exemple un code de contrôle par bloc) ou une valeur de contrôle cryptographique.  
A la réception de l'unité de donnée, l'entité homologue effectue le même calcul et vérifie la correspondance du résultat du calcul et de l'information redondante reçue.  
En cas de non correspondance, des mécanismes de reprise sur erreur peuvent être mis en œuvre.
- Ceux qui permettent d'assurer l'intégrité d'un flot d'unités de données.
  - Dans le cas d'une communication en mode connexion, afin d'assurer une protection contre l'insertion ou la perte d'unités de données, le fait de rejouer et la protection contre les erreurs de séquençement on peut utiliser la numérotation, l'horodatage ou le chaînage cryptographique (par exemple avec un DES en mode CBC).
  - Dans le cas d'une communication en mode sans connexion, il est possible d'assurer une certaine protection contre le fait de rejouer en utilisant l'horodatage.

Par exemple [IB93] utilise un mécanisme de signature au niveau réseau afin de garantir l'intégrité d'une unité de donnée et utilise une numérotation des unités de donnée afin de garantir le fait de ne pas rejouer.

[Lin93] et [Zim92] utilisent une valeur de contrôle cryptographique au niveau application afin de garantir l'intégrité des mails.

### 3.1.4 Les mécanismes de contrôle d'accès

Les mécanismes de contrôle d'accès peuvent utiliser l'identité authentifiée d'une entité ou des informations relatives à l'entité (appartenance à un groupe) ou des capacités de l'entité (par exemple un ticket) pour déterminer et appliquer les droits d'accès de l'entité.

Dans la pratique le mécanisme se décompose souvent en deux parties:

- Le contrôle d'accès aux services.

La politique la plus courante est celle dite du garde-barrière. Bien que cette politique existe depuis longtemps de manière informelle (notamment par l'utilisation de filtres de niveau paquet), [Ran92] est le premier à décrire une conjonction de plusieurs types de filtres pour former un ensemble cohérent rendant cette politique. Elle consiste à faire passer toutes les communications par un serveur d'accès. Celui-ci examine les communications une par une et leur accorde ou non un droit d'accès en fonction de plusieurs paramètres (date, heure, service demandé, adresse source, ...).

Pratiquement ce mécanisme de contrôle d'accès peut prendre plusieurs formes:

- Utilisation de filtres au niveau paquet:

Il s'agit d'une solution peu onéreuse. Le filtrage des communications se fait au moyen d'une définition fixe des unités de données autorisées ou non autorisées. C'est la solution adoptée dans [RS93]. Malheureusement, comme le montre [Cha92], cette solution n'est pas très fiable car le filtre ne possède pas de contexte, c'est à dire d'un ensemble d'informations qui lui permet de faire le lien entre paquets et connexions.

- Utilisation de filtres de niveau application.

Au lieu d'utiliser un principe général pour toutes les unités de données, on utilise un filtre application par application. Ce filtre contrôle l'accès en fonction des actions exécutées. [GWT93] présente plusieurs exemples de filtres de niveau application conçus pour X11, FTP, TELNET... . Le problème du filtre de niveau application provient de sa complexité qui le rend potentiellement dangereux, mais également du nombre limité de filtres disponibles.

- Utilisation de filtres de niveau circuit.

C'est une solution intermédiaire. Le filtrage des communications se fait de la même manière que dans le cas d'un filtre de paquets mais dans ce cas le serveur d'accès possède un contexte.

SOCKS (présenté dans [KK92]) est un exemple de filtre de niveau circuit. Il est composé d'une bibliothèque destinée à remplacer la bibliothèque des sockets et d'un serveur situé sur le firewall.

Il est à noter qu'il est possible de séparer autorisation d'accès et application du contrôle d'accès. C'est ce qui se produit dans tous les systèmes utilisant des capacités. Ainsi [RM94] propose un mécanisme utilisant un serveur de tickets, le mécanisme de contrôle d'accès se faisant au niveau réseau.

[PR94] propose une approche différente de celle du garde-barrière qui considère que la majorité des communications sont honnêtes. Ceci conduit à autoriser toutes les communications puis à les interrompre en cas de danger au moyen d'un analyseur de sécurité placé en parallèle.

- Le contrôle d'accès proprement dit c'est à dire l'accès des sujets aux objets du système.

Plusieurs modèles ont été proposés. Ils utilisent souvent une conjonction des politique de contrôle d'accès discrétionnaire et de contrôle d'accès obligatoire.

En théorie les filtres de niveau application décrits ci-dessus devraient remplir cette tâche. Cependant pour des raisons de complexité c'est rarement le cas.

A part dans certains cas particuliers (voir [Cor94b] et [Cor94a]) le firewall n'effectue pas de contrôle d'accès sur les objets ou sujets du réseau interne (pour des raisons de performances).

### 3.1.5 Le mécanisme d'échange d'authentification

Le mécanisme d'échange d'authentification varie fortement suivant le niveau de l'entité à authentifier.

- En matière d'authentification des personnes [CK95] cite trois façons d'authentifier un individu:
  - Soit par quelque chose que l'individu sait.
  - Soit par quelque chose que l'individu possède.
  - Soit par une caractéristique physique de l'individu.

La solution habituelle proposée dans les systèmes d'exploitation se base sur la première approche. Elle utilise un mot de passe associé à l'identifiant de la personne désirant utiliser un système. Le mot de passe est stocké sous forme codée dans le système.

Malheureusement cette solution n'est pas fiable et cela pour plusieurs raisons:

- le mot de passe est souvent transmis en clair, il est donc possible de le récupérer en faisant de l'écoute passive sur la ligne sur laquelle il

circule puis de rejouer.

- [Kle90] montre qu'il est possible de trouver en moyenne 25% des mots de passe par une attaque par dictionnaire.

[Kle90] cite les solutions proposées à ce problème:

- Utilisation d'algorithmes de chiffrement des mots de passe plus lents.
- Utilisation de "sel", c'est à dire d'une partie variable dans les clefs servant à coder les mots de passe.
- Génération automatique de mots de passe.
- Dissimulation des fichiers de mots de passe.

Mais note qu'aucune n'est véritablement satisfaisante puisqu'elles ne règlent pas le problème de l'écoute passive. Cependant certains concepteurs de firewalls considérant cette éventualité comme peu probable propose une authentification basée sur ce principe (voir [cor95], [Rap92a] et [Rap92b]).

Afin d'éviter le problème de l'écoute passive des mots de passe [Lam81] propose l'utilisation de fonction irréversibles afin de générer des mots de passe ne pouvant servir qu'une fois. Une implémentation de ce mécanisme, *S/KEY* a été décrite dans [Hal95]. Comme nous le verrons au chapitre suivant, cette solution est fréquemment utilisée en pratique.

Des solutions ne reposant pas ou pas uniquement sur une connaissance ont été proposées:

- Utilisation de calculatrices cryptographiques.  
elles permettent le calcul de fonctions cryptographiques sans utilisation d'un lecteur de carte.
- Utilisation de cartes.
- Utilisation de cartes associées à un code.  
le code servant à authentifier l'utilisateur vis-a-vis de la carte, celle-ci servant à authentifier l'utilisateur vis-a-vis du système.
- Utilisation de données biométriques (empreinte digitale, empreinte de la voix, signature, empreinte de la rétine de l'œil ...).

[RM93] propose une extension des mécanismes utilisant des cartes à puces en décrivant un mécanisme d'authentification mutuelle basé sur l'utilisation d'une carte à puce non personnelle protégée par un PIN. Cette méthode a cependant l'inconvénient d'obliger l'utilisateur à effectuer des calculs.

Dans la pratique ces mécanismes sont souvent mis en œuvre au niveau de la couche application.

- les mécanismes d'authentification des machines reposent principalement sur le chiffrement d'un message ou sur sa signature; le message chiffré ou signé servant d'authentifiant. On peut utiliser pour cela des fonctions à clefs, soit publiques, soit privées.

[CK95] présente les méthodes les plus courantes. Parmi celles-ci on peut distinguer deux classes:

- Mécanismes d'authentification directs:  
Les algorithmes proposés permettent l'authentification unilatérale ou mutuelle des entités homologues. Ils se basent sur l'utilisation de clefs et de nonces c'est à dire de variables ne servant qu'une fois.
- Mécanismes d'authentification au moyen d'un intermédiaire:  
On utilise ces mécanismes pour résoudre des problèmes de gestion de clefs.

En pratique ces mécanismes peuvent être mis en œuvre aux niveaux 3, 4 et 7 du modèle OSI.

### **3.1.6 Le mécanisme de bourrage**

Il consiste à produire des instances de communication parasites, des unités de données parasites et/ou des données parasites dans les unités de données afin de fournir une protection contre l'analyse de trafic. Ce mécanisme est peu utilisé en pratique.

### **3.1.7 Le mécanisme de contrôle de routage**

Le contrôle de routage est un mécanisme permettant le choix d'une route pour aller d'une entité à l'autre. Le choix de cette route peut être fait de manière à n'utiliser que des sous-réseaux et liaisons physiquement sûrs. Ce mécanisme est également peu utilisé en pratique.

### **3.1.8 Le mécanisme de notarisation**

Il consiste à utiliser un intermédiaire dans lequel les deux parties font confiance. Celui-ci détient les informations nécessaires pour fournir la garantie d'une propriété de manière vérifiable.

Le notaire effectue les actions suivantes:

- Vérification de l'identité des entités.

- Vérification de leurs droits.
- Signification de leurs devoirs.
- Il impose la procédure à suivre.
- Il certifie l'acte authentique.
- Il date l'acte.
- Enregistrement des actes.

Pour effectuer ces actions il peut utiliser les mécanismes de chiffrement, de signature numérique et d'intégrité des données associés à des algorithmes de notarisation. Ceux-ci varient suivant que l'on utilise la cryptographie à clef publique ou à clef privée et suivant les droits que l'on désire accorder au notaire (par exemple le fait que le notaire puisse ou non lire les actes).

[PR94] propose une forme de notarisation rendant les services de non répudiation avec preuve de remise et de non répudiation avec preuve de l'origine en utilisant le mécanisme de signature numérique.

Il est à noter que certaines formes de signatures (voir [CK95]) bien que permettant l'authentification ne fournissent pas une preuve de l'origine.

### 3.1.9 Les mécanismes de gestion des clefs

Les mécanismes de gestion des clefs sont utilisés par les mécanismes utilisant des techniques cryptographiques.

Le problème rencontré dans le cas de l'utilisation de cryptographie à clef privée est la multiplication des clefs puisque si il existe  $n$  systèmes désirant communiquer entre eux  $(n(n - 1))/2$  clefs différentes devront être utilisées. Ce problème n'apparaît pas dans le cas d'utilisation de clefs publiques puisque dans ce cas  $(n - 1)$  paires de clefs suffiront.

[Azi94] propose une solution basée sur un échange Diffie-Hellman n'ayant lieu qu'une fois afin de générer une clef privée commune. Une sous-clef privée est générée à partir de la clef produite par l'échange DH.

Cependant le problème de la distribution des clefs n'est pas résolu. L'utilisation d'un intermédiaire permet de trouver une solution à ce problème dans le cas de clefs secrètes.

En effet il suffit pour chaque partie de connaître la clef permettant de dialoguer avec son intermédiaire soit  $n$  clefs en tout.

Une solution consiste à utiliser un serveur de clefs (KDC) partageant une clef secrète avec chacun des noeuds.

Dans le cas des clefs publiques ce n'est pas le nombre de clefs qui est gênant mais le fait qu'étant donné que les clefs sont publiques il est possible de modifier la clef de quelqu'un afin de se faire passer pour lui. La solution dans ce cas consiste à utiliser une entité digne de confiance certifiant les clefs qu'elle distribue.

Afin de tenir compte du nombre important d'entités pouvant avoir à communiquer entre elles, des solutions utilisant plusieurs intermédiaires ont été proposées.

### 3.1.10 Le mécanisme de détection d'évènements

La détection d'évènements comprend la détection de violations apparentes de la sécurité mais également la détection d'évènements normaux. La détection d'évènements normaux est faite pour plusieurs raisons:

- Une suite d'évènements normaux peut conduire à une violation de la sécurité. Ceci se produit dans le cas d'erreur de conception du système ou même du matériel (ainsi [OS95] montre que grâce à certaines erreurs présentes dans les processeurs de la famille 80x86 des suites d'instructions peuvent conduire à des violations de la sécurité).
- La fréquence ou l'horaire d'apparition d'un évènement normal peut constituer un indice du fait qu'il s'agit d'un évènement hostile.

Le mécanisme de détection d'évènement peut se faire:

- Par des mécanismes propres au système (mécanismes du noyau).
- Par les services eux mêmes.
- Par des applications spécialisées.

[CB94] propose l'utilisation d'un utilitaire de détection d'évènements; *TCP-wrapper* afin de combler les faiblesses d'*inetd*.

[SCH95] propose une méthode intéressante permettant de détecter les connexions "de rebond" (connexions qui permettent à un attaquant de se dissimuler) en utilisant les mécanismes de signature numérique afin de pouvoir localiser les intrus en associant à chaque connexion une signature et en comparant ces signatures.

Les évènements détectés sont centralisés et sauvegardés dans un fichier appelé journal de sécurité.

## 3.2 Mécanismes non ISO

### 3.2.1 Le mécanisme d’audit de sécurité

Il consiste à analyser les événements contenus dans le journal de sécurité afin de tenter d’y découvrir des attaques éventuelles. Cette analyse peut se faire à posteriori ou en temps réel.

Il existe plusieurs approches d’analyse du journal d’audit de sécurité:

- Approches comportementales:  
Ces approches visent à détecter des attaques utilisant une vulnérabilité inconnue. Plusieurs méthodes existent mais la plus utilisée est la méthode statistique. Elle modélise le comportement d’un utilisateur et vérifie que son comportement ne varie pas de manière significative dans le temps vis à vis du modèle.
- Approches basées sur des scénarios:  
Ces approches cherchent à trouver dans le journal d’audit des commandes ou des suites de commandes exploitant une vulnérabilité connue. Dans ce cas également plusieurs méthodes existent:
  - La plus simple est le pattern-matching. Dans cette méthode le journal d’audit est vu comme une suite de caractères dans laquelle une attaque est constituée par une ou plusieurs sous-suites de caractères.
  - La méthode utilisant les systèmes experts utilise trois types de règles; un premier concerne ce qui est suspect, un second concerne les failles de sécurité connues et un troisième code le savoir de l’officier de sécurité en matière de détection d’intrusion.
  - La dernière méthode utilise des algorithmes génétiques afin d’isoler les parties du journal de sécurité les plus à mêmes de représenter des risques.

Dans la pratique ce sont les approches basées sur des scénarios utilisant le pattern-matching qui sont les plus utilisées. Dans la plupart des cas le pattern-matching est mis en œuvre au niveau de *syslogd*. Celui-ci est modifié de telle sorte qu’il puisse reconnaître en temps réel certains événements ou certaines suites d’événements décrits au moyen d’expressions régulières.

[Igl93] constitue un exemple d’approche proche de celle basée sur des scénarios utilisant les systèmes experts. Elle utilise un ensemble de règles et d’états. Chaque règle permettant de passer d’un état à un autre lors de l’exécution d’une action. Chaque état représentant l’état de “compromission” courant du système. Cette approche a le mérite de pouvoir être utilisée en temps réel.

### 3.2.2 Les mécanismes de contrôle de contenu

Les mécanismes de contrôle de contenu consistent à analyser le contenu des unités de données transmises afin d'en supprimer les données sensibles.

De nombreux produits commerciaux proposent :

- Suppression ou filtrage des informations concernant la topologie du réseau interne.
- Suppression ou filtrage des informations concernant les usagers du réseau interne.

[Cor94a] propose une analyse statistique des unités de données afin d'en retirer celles pouvant présenter un danger. Il propose également l'utilisation d'anti-virus sur les fichiers binaires transmis.

### 3.2.3 Les mécanismes de dissimulation d'informations

La plupart des produits commerciaux utilisent des mécanismes de dissimulation d'informations afin de limiter les risques de fuite d'informations sensibles.

Parmi ceux-ci les suivants sont fréquemment utilisés :

- Utilisation de bases d'informations différentes pour le réseau interne et le réseau externe (Par exemple [Dig94a] utilise deux serveurs DNS).
- Utilisation de services sur le firewall diffusant des informations préalablement filtrées (par exemple [CB94] cite un serveur *finger* regroupant toutes les informations concernant les usagers du réseau interne).
- Remplacement d'informations sensibles par des informations erronées (par exemple [Cor94a] utilise des faux fichiers de mots de passe pour tromper d'éventuels attaquants, ceci permettant de les repérer par la suite).

## Chapitre 4

# Produits diffusés

Nous étudions dans ce chapitre neuf firewalls commerciaux ou universitaires. Les articles, rapports techniques et documentations nous ayant servis sont présentés par la liste suivante:

- [is93] et [is96]: TIS firewall toolkit et le TIS Gauntlet.
- [RS93]: TAMU security package.
- [Dig94b], [Dig94a] et [Dig93]: DEC Seal.
- [Sun95], [mic95b] et [mic95a]: SUN Sunscreen SPF-100.
- [Rap92b] et [Rap92a]: Raptor Eagle.
- [cor95]: SOS Brimstone firewall.
- [Tec95]: Borderware firewall.
- [Cor94b] et [Cor94a]: SCC Sidewinder.

A partir de ces documents, on peut faire une comparaison des produits étudiés. Les tableaux 4.1 et 4.2 présentent les résultats obtenus.

## 4.1 Relations entre services et mécanismes

Services	Produits								
	Tis Fire- wall toolkit	Tis Gaunt- let	TAMU Secu- rity package	DEC Seal	SUN Suns- screen SPF- 100	Raptor Eagle	SOS Brim- stone	Border- ware Firewall	SCC Side- winder
Authen- tification de l'entité homologue	EA (1) (2)	EA (1) (2)	Non	Non	Non	EA (2) (3)	EA (1) (2) (3)	EA (2)	EA (4)
Authen- tification de l'origine des données	Non	S C (5)	Non	Non	S C (6)	Non	Non	Non	Non
Contrôle d'accès	CA (7) (11)	CA (8) (7) (11)	CA (9) (11)	CA (7) (8) (9) (11)	CA (9) (11)	CA (7) (8) (11)	CA (7) (8) (11)	CA (7) (9) (11)	CA (10)
Confiden- tialité des données	Non	C (12)	Non	Non	C (13)	Non	Non	Non	Non
Confiden- tialité du flux de données	Non	Non	Non	Non	Non	Non	Non	Non	Non
Intégrité des données	Non	S C I (14)	Non	Non	S C I (15)	Non	Non	Non	Non
Non répu- diation avec preuve de l'origine	Non	S (16)	Non	Non	S (17)	Non	Non	Non	Non
Non répu- diation avec preuve de remise	Non	Non	Non	Non	Non	Non	Non	Non	Non
Innocuité des données	Non	AC DI (18) (19)	Non	DI (19)	Non	AC DI (18) (19)	DI (19)	AC DI (18) (19)	AC DI (18) (20) (25)
Intégrité du système	DE (22)	DE S (21) (22)	S (21)	Non	Non	DE S (21) (22)	DE (22)	Non	Non

Services	Produits								
	Tis Fire- wall toolkit	Tis Gaunt- let	TAMU Secu- rity package	DEC Seal	SUN Suns- creen SPF- 100	Raptor Eagle	SOS Brim- stone	Border- ware Firewall	SCC Side- winder
disponibilité du système	CA (23)	CA (23)	CA (23)	CA (23)	CA (23)	CA (23)	CA (23)	CA (23)	CA (23)
auditabilité	DE A (24) (26)	DE A (24) (26)	DE A (24) (26)	DE A (24) (26)	DE A (24) (26)	DE A (24) (26)	DE A (24) (26)	DE A (24) (26)	DE A (24) (26)

TAB. 4.1 - *Relations entre mécanismes et services dans des produits commerciaux*

### Liste des abréviations et numérotation utilisée:

- EA : Echange d'authentifications.
- S : Signature.
- C : Chiffrement.
- I : Mécanismes d'intégrité.
- CA : Mécanisme de contrôle d'accès.
- A : Mécanisme d'audit.
- DE : Détection d'évènements
- AC : Analyse de contenu.
- DI : Dissimulation d'information.

Afin de détailler les mécanismes utilisés, on se sert de la numérotation suivante:

- (1) Echange d'authentification par mot de passe servant une fois. (par ex S/KEY)
- (2) Echange d'authentification par carte cryptographique (par ex. SecurID) associant un PIN à une carte à puce.
- (3) Echange d'authentification par mot de passe (par ex. un mot de passe UNIX)
- (4) Echange d'authentification par carte à puce.
- (5) Signature et Chiffrement en utilisant swIPe associé au DES.
- (6) Signature et chiffrement en utilisant SKip.
- (7) Filtres de niveau application.
- (8) Filtre de niveau circuit.
- (9) Filtre de niveau paquet.
- (10) Filtres de niveau application et contrôle de l'accès aux objets et sujets du réseau internes.
- (11) Contrôle de l'accès aux objets et sujets du firewall par UNIX.
- (12) Chiffrement en utilisant swIPe associé au DES.

- (13) Chiffrement en utilisant SKip.
- (14) Signature, Chiffrement, intégrité des données en utilisant swIPe.
- (15) Signature, Chiffrement, intégrité des données en utilisant SKip associé au DES.
- (16) Signature en utilisant swIPe associé au DES.
- (17) Signature en utilisant SKip.
- (18) Renommage des en-têtes des mails.
- (19) Utilisation de deux serveurs DNS.
- (20) Analyse statistique du contenu des unités de données.
- (21) Signature du contenu du système et conservation de cette signature sur un support sûr.
- (22) Détection d'évènements pouvant nuire à l'intégrité du système en temps réel.
- (23) Le mécanisme de contrôle d'accès apporte une protection contre certains dénis de services.
- (24) Mécanisme d'audit de type: approche basée sur des scénarios utilisant le pattern-matching.
- (25) Diffusion d'informations erronées.
- (26) Détection d'évènements.

## 4.2 Relations entre services et couches

Le tableau 4.2 donne les liens entre services, et couches dans des produits commerciaux.

Les chiffres indiquent les couches dans lesquelles les services sont rendus dans les produits étudiés.

La première ligne donne les couches dans lesquelles les services pourraient être rendus (cette information est obtenue à partir du chapitre précédent).

Produits	Services							
	Authen- tification de l'en- tité homo- logue	Authen- tification de l'ori- gine des données	Contrôle d'accès	Confidentialité des données	Confidentialité du flux de données	Intégrité des données	Non répu- diation avec preuve de l'origine	Non répu- diation avec preuve de remise
Placements possibles	3 4 7	3 4 7	3 4 7	1 3 4 7		3 4 7	3 4 7	7
Tis Firewall toolkit	7		7					
Tis Gauntlet	7	3	4 7	3		3	3	
TAMU Se- curity package			3					
DEC Seal			3 4 7					
SUN Suns- creen SPF- 100		3	3	3		3	3	
Raptor Eagle	7		4 7					
SOS Brimstone	7		4 7					
Borderware Firewall	7		3 4 7					
SCC Sidewinder	7		7					

TAB. 4.2 - Relations entre services et couches

## Chapitre 5

# Conclusion

Ce document présente les raisons d'utilisation des firewalls, les services de sécurité proposés par ceux-ci et les mécanismes proposés pour rendre ces services. Il étudie ensuite l'utilisation de ces services et mécanismes ainsi que leur relations dans quelques produits commerciaux et universitaires.

Vis à vis des problèmes que nous avons exposés dans l'introduction un firewall représente une solution car:

- Il permet de séparer la machine ou le réseau à interconnecter du reste du réseau public. Cette séparation permet de distinguer un ensemble de machines sûres (les machines appartenant au réseau interne) d'un ensemble de machines non sûres (les machines appartenant au réseau externe).
- Il interdit tout trafic direct entre le réseau externe et le réseau interne afin de pouvoir contrôler non seulement les accès allant de l'extérieur vers l'intérieur mais également dans le sens contraire.
- Il souligne la nécessité d'adopter une politique de sécurité et permet de fixer celle-ci pour un ensemble de machines. Cette centralisation de la gestion de la politique de sécurité permet de limiter les risques de configurations concurrentes.
- Il centralise les points d'attaque en un seul point. Ce point propose un nombre limité de services. Ceux-ci sont simplifiés au maximum afin de garantir leur sûreté.
- Il propose un certain nombre de services de sécurité.
- Il peut avoir un rôle dissuasif sur les usagers aussi bien internes que externes.

Certains services et mécanismes peuvent sembler redondants (comme par exemple le mécanisme de contrôle de contenu et celui de dissimulation d'informations) mais cette redondance répond à des besoins différents et permet de compenser des dysfonctionnements éventuels.

La suite de mon stage permettra l'application des connaissances acquises au cours de cette bibliographie à la mise en place d'un module de sécurité ATM.

# Bibliographie

- [Azi94] Ashar Aziz. Simple key management for internet protocols. *IETF*, 1994.
- [CB94] B. Cheswick and S. Bellovin. *Firewalls and internet security, Repelling the wily hacker*. Addison-wesley Publishing company, 1994.
- [Cha92] D. B. Chapman. Network (in)security through ip packet filtering. *USENIX Conference Proceedings*, 1992.
- [Che94] S. Forrest A. Perelson L. Allen R. Cherukuri. Self-nonsel self discrimination in a computer. *Proceedings of the IEEE Symposium on Security and Privacy*, 1994.
- [CK95] M. Speciner C. Kaufman, R. Perlman. *Network security ,private communication in a Public World*. Prentice Hall, 1995.
- [Cor94a] Secure Computing Corporation. Network security and sidewinder. Technical report, 1994.
- [Cor94b] Secure Computing Corporation. Technical extract from the sidewinder faq. Technical report, 1994.
- [cor95] SOS corporation. Brimstone firewall package a white paper. Technical report, 1995.
- [DH76] W. Diffie and M. Hellman. New directions in cryptography. *IEEE transactions on information theory*, 1976.
- [Dig93] Digital equipment. *SEAL introductory guide*, 1993.
- [Dig94a] Digital equipment. *Digital firewall service Adminitrator's guide*, 1994.
- [Dig94b] Digital Equipment. *Digital firewall service Intoductory guide*, 1994.
- [GWT93] A. Wolman G. W. Treese. X trough the firewall,and other application relays. *USENIX Conference Proceedings*, 1993.

- [Hal95] N. M. Haller. Rfc 1760, the s/key one-time password system. Technical report, Network Working Group, 1995.
- [IB93] J. Ioannidis and M. Blaze. The architecture and implementation of network-layer security under unix. *USENIX Conference Proceedings*, 1993.
- [Igl93] R. Iglun. Ustat a real time intrusion detection system for unix. *Proceedings of the IEEE Symposium on Security and Privacy*, 1993.
- [is93] Trusted information systems. Internet firewalls ,an overview. Technical report, 1993.
- [is96] Trusted information systems. Firewall product functional summary. Technical report, 1996.
- [ISO90] ISO. Interconnection de systèmes ouverts , modèle de référence de base, partie 2: Architecture de sécurité. Technical report, AFNOR, 1990.
- [Kal92] B. Kaliski. Rfc 1319, the md2 message-digest algorithm. Technical report, Network Working Group, 1992.
- [KK92] D. Koblas and M. Koblas. Socks. *UNIX Security III Symposium*, 1992.
- [Kle90] D. V. Klein. Foiling the cracker : A survey of and improvements to password security. *USENIX Conference Proceedings*, 1990.
- [Lai92] X. Lai. *On the design and security of block ciphers*. Hartung-gorre Verlag, 1992.
- [Lam81] L. Lamport. Password authentication with insecure communication. *Communication of the ACM*, 1981.
- [Lin93] J. Linn. Rfc 1421, privacy enhancement for internet electronic mail: Part i: Message encryption and authentication procedures. Technical report, Network Working Group, 1993.
- [MH78] R. Merkle and M. Hellman. Hiding signatures in trapdoor knapsacks. *IEEE transactions on information theory*, 1978.
- [mic95a] Sun microsystems. Cryptography in public internetworks with sunscreen. Technical report, 1995.
- [mic95b] Sun microsystems. Introduction to network security and sunscreen. Technical report, 1995.

- [MJR94] F. M. Avolio M. J. Ranum. A network perimeter with secure external access. Technical report, Trusted information systems Incorporated, 1994.
- [NBS77] NBS. Data encryption standard , federal information processing standards. Technical report, NBS, 1977.
- [NIS94] NIST. Escrowed encryption standard. Technical report, NIST, 1994.
- [OS95] R. Lindell O. Sibert, P. A. Porras. The intel 80x86 processor architecture: Pitfalls for secure systems. *Proceedings of the IEEE Symposium on Security and Privacy*, 1995.
- [PR94] S. Gombault P. Rolin, L. Toutain. Network security probe. *ACM Conference on computer and communications security*, 1994.
- [Ran92] M. Ranum. A network firewall. *Proc. World Conference on System Administration and Security*, 1992.
- [Rap92a] Raptor system incorporated. *Eagle Network Security Management system administrator's guide*, 1992.
- [Rap92b] Raptor system incorporated. *Eagle Network Security Management system user's guide*, 1992.
- [Riv92a] R. Rivest. Rfc 1320, the md4 message-digest algorithm. Technical report, Network Working Group, 1992.
- [Riv92b] R. Rivest. Rfc 1321, the md5 message-digest algorithm. Technical report, Network Working Group, 1992.
- [RM93] G. Tsudik R. Molva. Authentication method with impersonal token card. *IEEE proceedings in security and privacy*, 1993.
- [RM94] E. Rutsche R. Molva. Application access control at network level. *ACM Conference on computer and communications security*, 1994.
- [RR78] L. Adleman R. Rivest, A. Shamir. A method of obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 1978.
- [RS93] K. Hess R. Safford, L. Schales. The tamu security package : An ongoing response to internet intruders in an academic environment. *USENIX Conference Proceedings*, 1993.
- [SCH95] S. Staniford-Chen and L. Todd Heberlein. Holding intruders accountable on the internet. *Proceedings of the IEEE Symposium on Security and Privacy*, 1995.

- [Spa94] G. H. Kim E. H. Spafford. The design and implementation of tripwire, a file system integrity checker. *ACM Conference on computer and communications security*, 1994.
- [Sun95] Sun microsystems. *Introduction to network security and sunscreen*, 1995.
- [Tec95] Border Network Technologies. The borderware firewall server, a white paper. Technical report, 1995.
- [Zim92] P. Zimmerman. *PGP User's guide*, 1992.