République Algérienne Démocratique et Populaire
Ministère de l'enseignement Supérieur et de la recherche scientifique
Université Hassiba Benbouali de Chlef
Faculté de Technologie
Département d'électronique

Polycopié de cours destiné aux étudiants
Licence 3 en télécommunication

Matière : Sécurité de l'information

Présenté par :

Dr. MEFTAH Elhadi

Année universitaire : 2021 –2022

Table des matières

Table des figures

Liste des tableaux

Abréviations

A

AES	Advanced Encryption Standard
ACL	Access Control List
ADSL	Asymmetrical bit rate Digital Subscriber Line
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode

B

BGP	Border Gateway Protocol

C

CCNA	Cisco Certified Network Associate
CCNP	Cisco Certified Network Professionnal
CCIE	Cisco Certified Internetwork Expert
CE	Customer Edge
CEF	Cisco Express Forwarding
CPU	Central Processing Unit
CoS	Classe of Service

D

DES	Data Encryption Standard
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System/Service
DMZ	DeMilitarized Zone

E

EAP	Extensible Authentication Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol

	F
FAI	Fournisseur d'Accès Internet.
FEC	Forwarding Equivalency Calss
FIB	Forwarding Information Base
FR	Frame Relay
	G
GRE	Generic Routing Encapsulation
	H
HTTPS	Hypertext Transfer ProtocolSecure Sockets
	I
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers.
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Organization for Standardization.
ISP	Internet Service Provider
	L
L2TP	Layer 2 Tunneling Protocol
L2F	Layer 2 Forwarding
L2TP	Layer Two Tunneling Protocol
LAN	Local Area Network
	M
MAC	Message Authentification Code
MIC	Michaël
	N
NAT	Network Adress Traduction
	O
OSI	Open Systems Interconnection

P

PEAP	Protected EAP
PKI	Public Key Infrastructure
PPP	Point-to-Point Protocol
PPTP	Point To Point Tunneling Protocol

Q

QoS	Quality of Service

R

RADIUS	Remote Authentication Dial-In User Server
RC4	Rivest Cipher 4
RNIS	Réseau Numérique à Intégration de Services
RSA	Rivest Shamir Adleman

S

STP	Spanning Tree Protocol
SSID	Service set identifier
SSH	Secure Shell
SSL	Secure Socket Layer

T

TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTLS	Tunneled Transport Layer Security

V

VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VTP	VLAN Trunking Protocol

W

WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WIFI	Wireless Fidelity
WPA	Wi-Fi protected access

Avant Propos

Ce polycopié de cours de la matière *Sécurité de l'information* (UED 3.2) est destiné aux étudiants de la troisième année Licence LMD , filière : *Télécommunications*, spécialité : *Télécommunications* . Il est conforme au programme agréé par le ministère de l'enseignement supérieur et de la recherche scientifique .

La croissance explosive des systèmes informatiques et de leurs interconnexions via les réseaux a accru la dépendance des entreprises et des individus vis-à-vis des informations stockées et transmises par ces systèmes. Cette évolution a conduit à une prise de conscience accrue de la nécessité de protéger les données et les ressources contre la divulgation, de garantir l'authenticité des données et des messages et de protéger les systèmes contre les attaques basées sur les réseaux. En outre, les disciplines de la cryptographie et de la sécurité des réseaux ont gagné en maturité, ce qui a conduit au développement d'applications pratiques et facilement disponibles pour assurer la sécurité des réseaux.

L'objectif de ce polycopié est de fournir un aperçu concret des principes et des méthodes de cryptographie et de sécurité des réseaux. De plus, les questions de base à traiter par une capacité de sécurité des réseaux sont explorées en fournissant un tutoriel et un aperçu de la cryptographie et de la technologie de sécurité des réseaux. Bien que ce polycopié de cours puisse être lu d'un bout à l'autre, il a été élaboré pour être flexible et permettre de passer d'un chapitre à l'autre. Toutefois, pour ceux qui ont l'intention de lire tous les chapitres, l'ordre du polycopié est une excellente séquence à suivre. Les chapitres I à VI couvrent les sujets :

— **Chapitre I – Introduction à la sécurité de l'information** : Ce chapitre aborde la manière de développer une politique de sécurité réseau complète visant à contrer les menaces sur la sécurité de l'information. Il présente également les menaces possibles et explique comment décrire et mettre en œuvre le processus d'élaboration d'une politique de sécurité. Ainsi, il expose les objectifs de la sécurité de l'information : Confidentialité, Intégrité, Disponibilité,les mesures de sécurité.

— **Chapitre II – Concepts de cryptographie et de cryptanalyse :** Ce chapitre présente les concepts de la cryptographie et englobe le cryptanalyse. Les étudiants apprendront les algorithmes, Cryptographie symétrique, Cryptographie asymétrique, Cryptographie conventionnelle, Chiffrement et déchiffrement (par bloc, par flot, Intégrité et authenticité).

— **Chapitre III – La sécurité du Pare-feu (Firewall) :** Ce chapitre constitue une introduction aux pare-feu. Les étudiants découvrent les différentes générations et catégories de pare-feu et apprennent comment ceux-ci sont déployés dans les entreprises. Ainsi , les politiques de sécurité, Outils dans les pare-feux.

— **Chapitre IV – La sécurité de la commutation :** L'objet de ce chapitre est de présenter les réseaux locaux virtuels (Virtual Local Area Network – VLAN). C'est à dire la segmentation des réseaux permise par les commutateurs, une segmentation qui n'est plus physique mais uniquement logique. Ce chapitre propose aussi les attaques et réponses de couche "liaison de données".

— **Chapitre V – Réseaux privés virtuels (VPN)** : Ce chapitre présente les concepts de réseaux privés virtuels (VPN). Il couvre des sujets tels que les concepts, les technologies et les termes utilisés par les VPN, les différents types de VPN, Les protocoles. Il aborde également la manière dont les VPN utilisent la tunnellisation pour supporter leurs fonctions, ainsi que les problèmes de sécurité liés au déploiement des VPN.

— **Chapitre VI – Sécurité des réseaux sans fil :** Ce chapitre offre une vue d'ensemble de la problématique de sécurité dans un réseau sans fil et présente quelques-unes des solutions simples pour un niveau élémentaire de sécurité. Il présente la solution WEP comme étant la première solution de sécurité proposée par le standard 802.11, malheureusement complètement insuffisante. Toutefois, elle est encore très répandue et doit donc être présentée. De plus, il détaille le protocole 802.1x dont le rôle est d'identifier les utilisateurs et de préparer une connexion sécurisée. Ce protocole simple et générique est à la base de nombreuses solutions de sécurité dont le WPA..

I. Introduction à la sécurité de l'information

Depuis que les êtres humains ont cessé d'effectuer des travaux manuels et ont été remplacés par des machines, la sécurité de l'information constitue la principale préoccupation. Aujourd'hui, c'est la plus grande préoccupation de ceux qui ont ou veulent créer une société, et conserver leurs informations de manière sécurisée et intégrée. Lorsque les informations étaient écrites sur papier, il était facile de les conserver puisqu'elles étaient enfermées dans un endroit sûr et que personne ne les touchait. Cependant, avec l'évolution de la technologie, les informations sont désormais stockées sur des supports numériques, ce qui les rend plus vulnérables au vol et à la perte. Dans ce contexte, il est de plus en plus nécessaire de mettre en œuvre des politiques de sécurité, permettant ainsi l'utilisation de ces informations. Dans ce chapitre, nous discuterons des règles et des normes qui doivent être respectées pour maintenir la fiabilité et la sécurité de l'information.

I.1 Qu'est-ce que la sécurité ?

I.1.1 Sécurité

Au quotidien, l'être humain est toujours à la recherche de la sécurité. Lorsqu'il quitte son domicile, lorsqu'il traverse une rue en faisant attention, lorsqu'il construit une maison dans un endroit plus paisible où il n'y a pas de violence, lorsqu'il achète une voiture avec de grands éléments de sécurité. Dans le domaine des technologies de l'information, la préoccupation en matière de sécurité concerne l'information. Il est nécessaire qu'ils soient sûrs et fiables pour que la prise de décision des responsables de l'entreprise soit plus précise et augmente ainsi les bénéfices de l'entreprise.

> **Notation I.1.1** Le meilleur concept de sécurité peut être que l'on trouve dans le dictionnaire Le Robert "**sécurité**(*nom féminin*) : 1. État d'esprit confiant et tranquille d'une personne qui se croit, se sent à l'abri du danger. 2. Situation tranquille qui résulte de l'absence réelle de danger."

I.1.2 Information

Chaque jour, l'homme désire davantage d'informations et de connaissances, consultant des livres, des panneaux, TV, journal, internet. En bref, partout où il va, il acquiert des informations. Une information est une connaissance sur un certain sujet, sur une personne ou une organisation. C'est un élément important, de valeur, c'est l'actif le plus précieux pour une organisation et s'il n'est pas conservé, il entraînera de grandes pertes. Actuellement, la plus grande préoccupation est de protéger les informations, car de nombreuses personnes et entreprises concurrentes tentent de les détourner.

> **Notation I.1.2** Selon le dictionnaire le Robert "**Information**(*nom féminin*) : 1. Renseignement (sur qqn, sur qqch.). *Des informations confidentielles*. 2. Renseignement ou évènement qu'on porte à la connaissance d'une personne, d'un public."

I.1.3 Sécurité de l'information

On parle de sécurité de l'information lorsque toutes les données et informations importantes pour une personne ou une organisation sont à l'abri des menaces, qu'elles soient physiques ou logiques. La meilleure définition du concept de sécurité de l'information se trouve sur le site internet lemagit.fr, et se résume comme suit :

"La sécurité de l'information (infosécurité, infosec) est un ensemble de stratégies de gestion

des processus et politiques visant à protéger, détecter, recenser et contrer les menaces ciblant les informations numériques ou non. Parmi ses responsabilités, l'infosécurité doit établir un ensemble de processus d'entreprise qui protègeront les actifs informationnels indépendamment du format ou de l'état des informations (en transit, en cours de traitement ou stockées au repos)."
Lorsqu'on pense à la sécurité de l'information, il est important de se rappeler qu'il faut maintenir l'intégrité, la disponibilité, la confidentialité des informations et la non-répudiation. Ces quatre principes seront examinés plus en détail dans la section I.3 de ce chapitre.

Une bonne exploitation de la sécurité de l'information apportera de nombreux avantages à la société et lui permettra de poursuivre son travail. Avec l'évolution de la technologie, le monde peut se connecter plus facilement et échanger des informations. Toutefois, le risque de les perdre est plus grand, car de nombreuses personnes ont la capacité d'envahir les systèmes et de dérober ou de modifier ces informations. Il est impératif de penser à la sécurité de l'information, sous peine de causer des dommages considérables à l'organisation. Mais pour cela, tous les utilisateurs et les employés de l'entreprise doivent être conscients de l'importance de l'information.

I.2 Menaces et Attaques

Une menace est tout ce qui peut mettre en danger vos données et vos informations. Ces menaces peuvent provenir de deux sources : internes et externes. Les menaces internes sont présentes dans les activités quotidiennes de l'organisation, que l'on soit connecté ou non à Internet. Comme exemple de menaces internes, on peut citer :

- **Contamination par un virus informatique par l'intermédiaire d'une simple disquette** - l'utilisation de disquettes infectées par des virus peut entraîner un mauvais fonctionnement de l'ordinateur infecté, et perturber l'exécution du travail.
- **Incendies** - ils peuvent se produire n'importe où, il suffit d'une étincelle. Les pertes peuvent être énormes si aucune mesure n'est prise pour contenir ou prévenir les incendies. Outre la perte de toutes les informations, la structure du bâtiment de l'entreprise peut également être endommagée.
- **Employés mal formés** - les employés qui n'ont pas été formés pour manipuler les équipements de l'entreprise peuvent endommager involontairement ces derniers, entraînant la perte d'informations.
- **Divulgation des mots de passe des employés** - certains employés notent toujours leurs mots de passe sur des morceaux de papier ou dans des fichiers texte sur leur ordinateur.

Une personne s'introduisant dans l'entreprise pourra facilement voler ou endommager les informations contenues dans les ordinateurs.

— **Déchets informatiques** - les documents contenant des informations sur l'entreprise ou les plans de travail ne devraient pas être simplement "jeté à la poubelle", car toute personne qui entre dans la salle peuvent les trouver et les utiliser à des fins abusives.

— **Utilisation abusive des services Internet au nom de l'entreprise** - employés qui accèdent à Facebook, MSN, pour sûr laissent leurs e-mails, pages bibliographiques...

Les menaces externes sont toutes les attaques qui proviennent de l'extérieur de l'environnement physique de l'entreprise. Ils sont les principaux responsables de la perte d'informations de l'entreprise. Comme exemple de menaces externes, nous avons les intrus, qui sont des personnes qui utilisent leurs dons pour contourner les techniques de sécurité des entreprises. Il existe plusieurs les types, mais les plus courants sont :

— **Hacker** - personne qui s'introduit dans des systèmes défectueux pour voler les informations d'autres personnes.

— **Cracker** - contrairement au hacker, il s'introduit dans les ordinateurs et les modifie, détourne les connexions et met même certains services hors ligne.

— **Phreaker** - il s'agit d'individus ayant de grandes connaissances en téléphonie et qui utilisent ces dons pour passer des appels sans payer.

— **Lammer** - il s'agit de personnes qui utilisent des programmes pour s'introduire sur des sites Internet.

En général, ces personnes ne piratent pas les systèmes juste pour le plaisir, ils ont généralement l'intention de voler des informations soit pour se venger, soit pour voler de l'argent, soit pour faire de l'espionnage industriel. Il existe plusieurs menaces contre la sécurité de l'information, comme le montre la figure I.1. Les plus courants sont les virus populaires avec 66%, les employés mécontents avec 53% et la divulgation des mots de passe avec 51%. Il est possible de voir à quel point ces menaces ont un lien avec l'être humain, principale cause de pertes pour les entreprises.

Quelques exemples de vulnérabilités :

— **Physique** - Mauvaise planification des salles de centre de données et sécurité non conforme aux normes. Les salles de centre de données construites dans des zones menacées d'effondrement ou sans sécurité nécessaire risquent d'être détruites ou envahies.

— **Naturel** - Lorsque les biens de l'entreprise sont susceptibles d'être endommagés par une

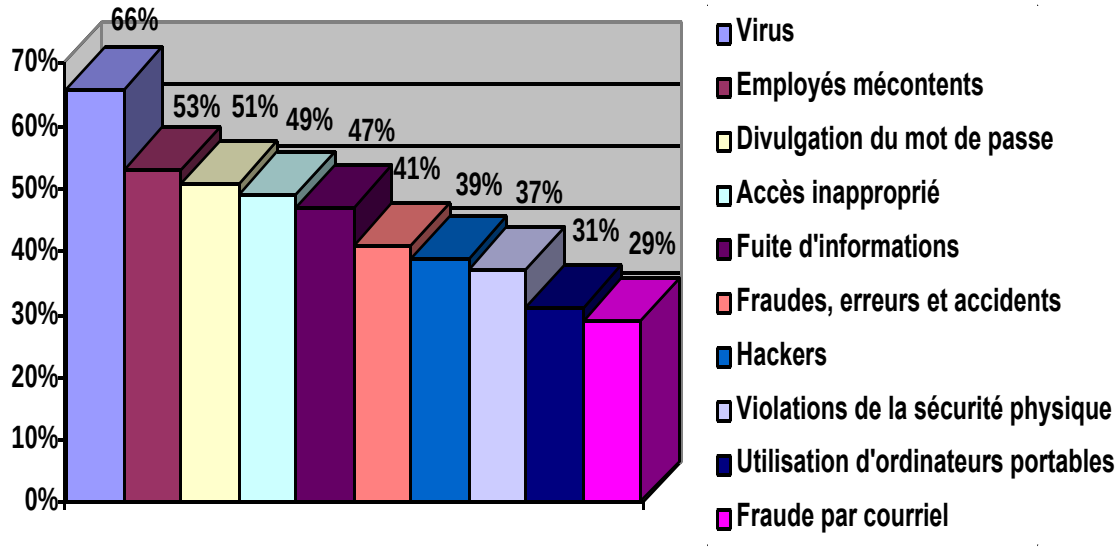


FIGURE I.1 – Principales menaces pour la sécurité de l'information.

inondation, des poussières, une tempête, l'humidité, la température. Les appareils de stockage d'informations peuvent être facilement endommagés par la poussière ou l'eau et la perte d'informations peut être irrécupérable.

— **Logiciel** - Installation et configuration médiocres. Une installation ou une configuration inadéquate peut entraîner la perte de données importantes ou permettre à des intrus de pénétrer dans le système.

— **Supports** - Les disquettes, les CD, les DVD sont des supports fragiles et sont facilement endommagés par les chocs, les rayures ou le magnétisme, ce qui entraîne une perte d'informations.

— **Communication** - Causée par une perte de communication ou un accès non autorisé. La perte temporaire de communication causée par le dysfonctionnement d'un équipement et l'accès d'employés à des zones non autorisées peut endommager les informations ou retarder l'accès, l'envoi et la réception des données.

— **Humaine** - Causée par une mauvaise pratique, un manque de formation, un manque de sensibilisation. Les professionnels qui endommagent ou perdent des informations en ne sachant pas comment utiliser les logiciels et les équipements.

I.3 Les objectifs de la sécurité de l'information

La sécurité de l'information a pour objectif de protéger toutes les données et informations d'une entreprise ou d'une personne contre toute menace. On évoque essentiellement cinq principes : la confidentialité des informations, l'intégrité des données, la disponibilité, la non-répudiation et l'authentification, comme illustré dans la figure I.2.

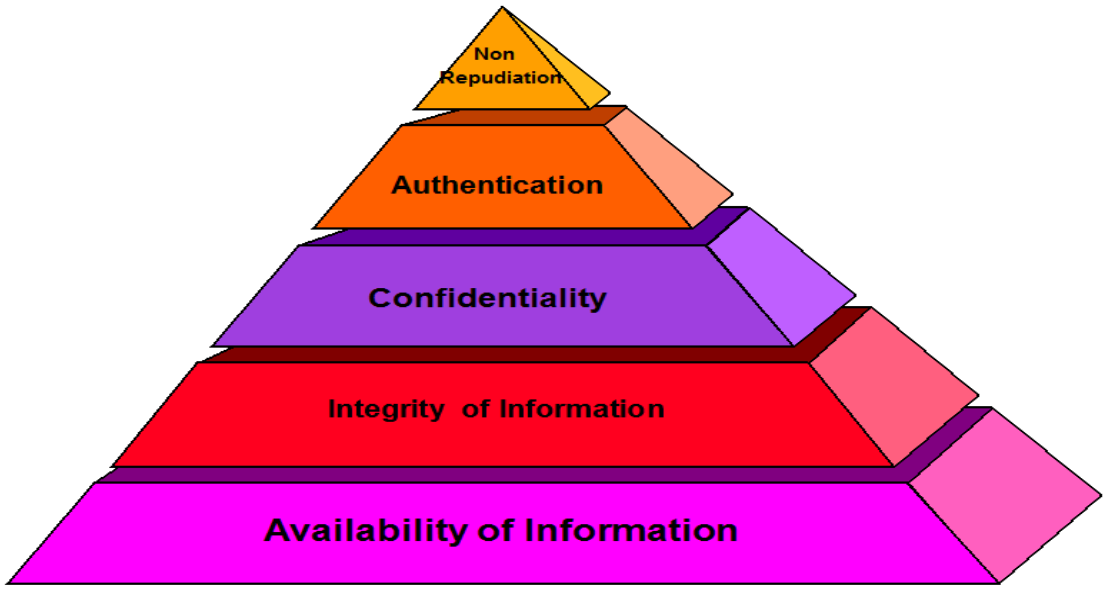


FIGURE I.2 – Dimensions de la sécurité de l'information.

I.3.1 Confidentialité

Les informations ne doivent être accessibles qu'aux personnes autorisées. N'importe quel utilisateur ne peut pas avoir accès à des informations dont seuls les dirigeants de l'entreprise peuvent disposer. Sinon, des données précieuses peuvent tomber entre les mains de personnes qui ont l'intention de nuire à l'entreprise.

I.3.2 Intégrité

Les informations seront toujours exactes et complètes lors de leur consultation. Dans le cas contraire, toutes les idées et tous les plans de l'entreprise risquent de ne pas aboutir et donc de causer et ainsi causer de grandes pertes.

I.3.3 Disponibilité

La certitude que les personnes autorisées à accéder à l'information peuvent le faire sans aucune sorte d'entrave. Cette disponibilité est importante car l'employé qui a besoin d'accéder

à certaines données pour accomplir une tâche, dispose de toutes les données dont il a besoin. Sinon, une bonne négociation peut être être perdu

I.3.4 Non-répudiation

Lors de l'envoi d'un message, l'expéditeur ou le destinataire peut dire qu'il n'a pas envoyé ou n'a pas reçu un tel message. Il en va de même pour ceux qui négocient et nient ensuite avoir négocié. Pour s'assurer que la négociation ou l'envoi du message a bien eu lieu, on utilise le procédé de la non-répudiation. La non-répudiation placée dans un contrat vise à protéger les parties d'un retrait probable sans paiement d'amendes de résiliation et même si quelqu'un signe un contrat numérique, et prétend plus tard qu'il n'a pas conclu l'affaire.

I.3.5 Authentification

L'authentification consiste simplement à vérifier qu'une entité (qu'il s'agisse d'un utilisateur, d'un autre système ou d'un autre programme) est bien celle qu'elle prétend être. L'exemple le plus évident d'authentification est lorsqu'un utilisateur final fournit un nom d'utilisateur et un mot de passe. Le mot de passe permet vraisemblablement de vérifier qu'il s'agit bien de cet utilisateur. Cependant, à mesure que les failles de sécurité se généralisent, un simple nom d'utilisateur et un mot de passe ne suffisent plus. Les mots de passe peuvent être devinés, écrits ou exposés de manière similaire.

I.4 Les mesures de sécurité

Les processus et outils suivants sont assez faciles à mettre en place, même pour les plus petites entreprises. Combinés, ils nous donneront un niveau de sécurité de base contre les risques informatiques les plus courants.

I.4.1 Utilisez des mots de passe forts

Des mots de passe forts sont essentiels à une bonne sécurité en ligne. Rendez votre mot de passe difficile à comprendre en :

- Utilisant une combinaison de lettres majuscules et minuscules, de chiffres et de symboles
- Utilisant entre 8 et 12 caractères
- Évitant l'utilisation de données personnelles
- Changez-le régulièrement

— Ne l'utilisez jamais pour plusieurs comptes

— Utiliser l'authentification à deux facteurs

Créez *une politique de mot de passe* pour l'entreprise afin d'aider le personnel à respecter les meilleures pratiques en matière de sécurité.

I.4.2 Contrôler l'accès

Assurez-vous que les personnes ne peuvent accéder qu'aux données et services auxquels ils sont autorisés. Par exemple, vous pouvez

— Contrôler l'accès physique aux locaux et au réseau d'ordinateurs

— Restreindre l'accès aux utilisateurs non autorisés

— Limiter l'accès aux données ou aux services par des contrôles d'application

— Restreindre ce qui peut être copié du système et enregistré sur des dispositifs de stockage

— Limiter l'envoi et la réception de certains types de pièces jointes aux courriels.

Les systèmes d'exploitation et les logiciels de réseau modernes permettent de réaliser la plupart de ces tâches, mais vous devrez gérer l'enregistrement des utilisateurs et les systèmes d'authentification des utilisateurs (par exemple, les mots de passe).

I.4.3 Installez un pare-feu

Les pare-feu sont des barrières efficaces entre votre ordinateur et l'internet, et l'un des principaux obstacles à la propagation des cybermenaces telles que les virus et les logiciels malveillants. Il est donc essentiel de configurer correctement les dispositifs de pare-feu et de vérifier régulièrement qu'ils disposent des dernières mises à jour logicielles et micrologicielles, faute de quoi ils risquent de se révéler inefficaces.

I.4.4 Utilisez un logiciel de sécurité

Il est conseillé d'utiliser des logiciels de sécurité, tels que des programmes anti-spyware, anti-malware et anti-virus, pour détecter et supprimer les codes malveillants qui s'introduisent dans le réseau. Apprenez à détecter les spams, les logiciels malveillants et les attaques de virus.

I.4.5 Mettez régulièrement à jour les programmes et les systèmes

Les mises à jour contiennent des améliorations de sécurité essentielles qui contribuent à la protection contre les bugs et les vulnérabilités connus. Veillez à maintenir vos logiciels et vos appareils à jour pour éviter d'être la proie des criminels.

I.4.6 Surveillez les intrusions

Vous pouvez utiliser des détecteurs d'intrusion pour surveiller le système et les activités inhabituelles du réseau. Si un système de détection soupçonne une violation potentielle de la sécurité, il peut générer une alarme, telle qu'une alerte par courrier électronique, en fonction du type d'activité qu'il a identifié.

I.4.7 Sensibilisez vos employés

Vos employés ont la responsabilité de contribuer à la sécurité de votre entreprise. Veillez à ce qu'ils comprennent leur rôle et les politiques et procédures applicables, et assurez-leur une sensibilisation et une formation régulières à la cybersécurité.

II. Concepts de cryptographie et de cryptanalyse

La cryptographie est la science qui permet de garder les secrets secrets. Supposons qu'un expéditeur, désigné ici et dans ce qui suit par *Alice* (selon l'usage courant), souhaite envoyer un message M à un récepteur, appelé *Bob*. Elle utilise un canal de communication non sécurisé. Par exemple, le canal peut être un réseau informatique ou une ligne téléphonique. ou une ligne téléphonique. Il y a un problème si le message contient des informations confidentielles. Le message peut être intercepté et lu par une personne qui écoute aux portes. Ou, pire encore, l'adversaire, que l'on appelle ici *Eve*, pourrait être en mesure de modifier le message pendant la transmission de telle sorte que le destinataire légitime Bob ne détecte pas la manipulation.

Ce chapitre est un tutoriel sur les nombreux et divers aspects de la cryptographie. Il ne cherche pas à transmettre tous les détails et subtilités inhérents au sujet. Son but est d'introduire les questions et les principes de base et d'orienter le lecteur vers les chapitres appropriés du polycopie pour des traitements plus complets.

II.1 Principes de la cryptographie

La cryptologie est la science qui traite de la communication en présence d'adversaires. Le but d'un système cryptographique est de chiffrer un texte clair M en un cryptogramme C au moyen d'une clé K[1]. Ce cryptogramme est ensuite transmis à son destinataire sur le canal. Le destinataire légitime doit pouvoir déchiffrer le cryptogramme C à l'aide de la clé K pour obtenir le texte clair. La figure II.1 illustre le fonctionnement d'un tel système cryptographique. On remarque que cette figure rappelle le schéma de communication de Shannon. Il s'agit en effet d'une des problématiques traitées par la théorie de l'information, celle du secret.

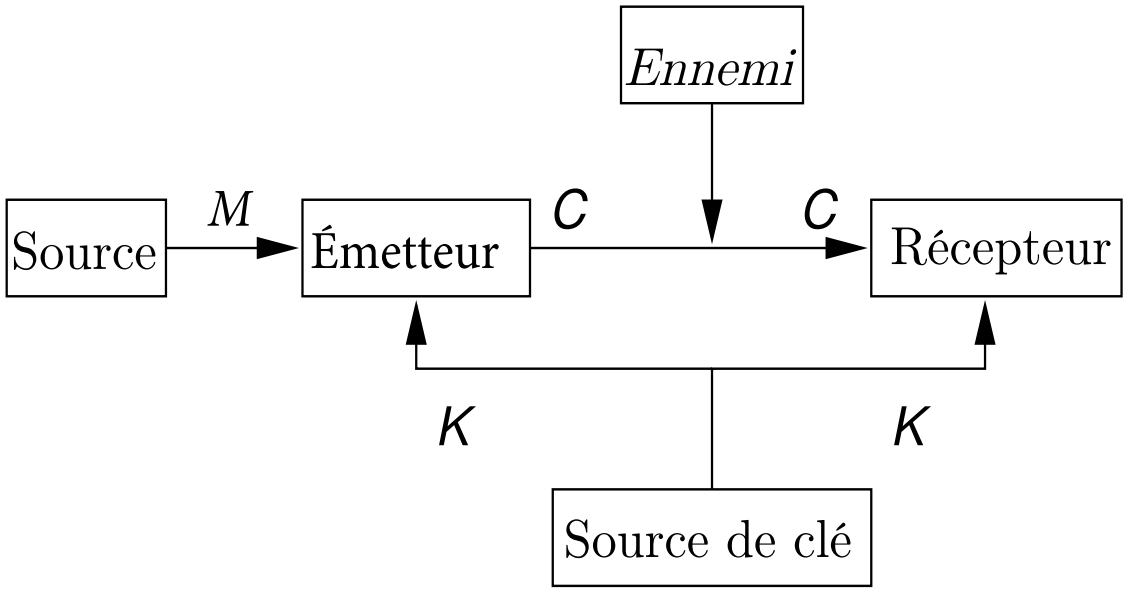


FIGURE II.1 – Modèle de Shannon pour le secret.

Cependant, un ennemi (le *cryptanalyste*) (qui ne connaît évidemment pas la clé K) ne doit pas être en mesure de *décrypter* le cryptogramme, en d'autres termes de réaliser une opération de *cryptanalyse* qui lui permette de retrouver le clair sans connaître la clé. Ce dernier peut tenter de cryptanalyser selon différentes techniques d'attaques, classées par ordre de difficultés décroissant :

— à cryptogramme connu : le cryptanalyste connaît une longue portion de cryptogramme ;
— à couples clairs/cryptogrammes connus : le cryptanalyste connaît un petit nombre de couples clairs/cryptogrammes ;
— à clair choisi : le cryptanalyste dispose du mécanisme de chiffrement et chiffre des clairs de son choix pour obtenir des informations sur la clé.

1. M pour plaintext, C pour cïphertext et K pour key *en anglais*.

Il est possible de résumer la philosophie de la cryptographie moderne par le principe de Kerchoff (1883) :

La sécurité d'un système de chiffre ne doit pas dépendre du secret de l'algorithme mais seulement du secret de la clé.

Une solution classique du problème de la cryptographie repose sur les systèmes de chiffrement à clé secrète composés de :

- un espace de messages $\mathscr{M}$: ensemble des mots sur l'alphabet des messages clairs ;
- un espace de cryptogrammes $\mathscr{C}$: ensemble des cryptogrammes sur l'alphabet des cryptogrammes ;
- un espace de clés $\mathscr{K}$: ensemble des clés sur un alphabet ;
- un algorithme de chiffrement qui est une application $E : \mathscr{K} \times \mathscr{M} \to \mathscr{C}$;
- un algorithme de déchiffrement qui est une application $D : \mathscr{K} \times \mathscr{C} \to \mathscr{M}$.

Les deux algorithmes E et D doivent vérifier que $D(K, E(K, M)) = M$, $\forall K \in \mathscr{K}$, $\forall M \in \mathscr{M}$.

Pour utiliser un tel système de chiffrement, les deux parties doivent s'entendre sur une clé particulière K qu'ils conservent secrète. L'émetteur envoie un cryptogramme $C = E(K, M)$ qui est reçu par le destinataire qui effectue l'opération $D(K, C) = M$ pour retrouver le clair M.

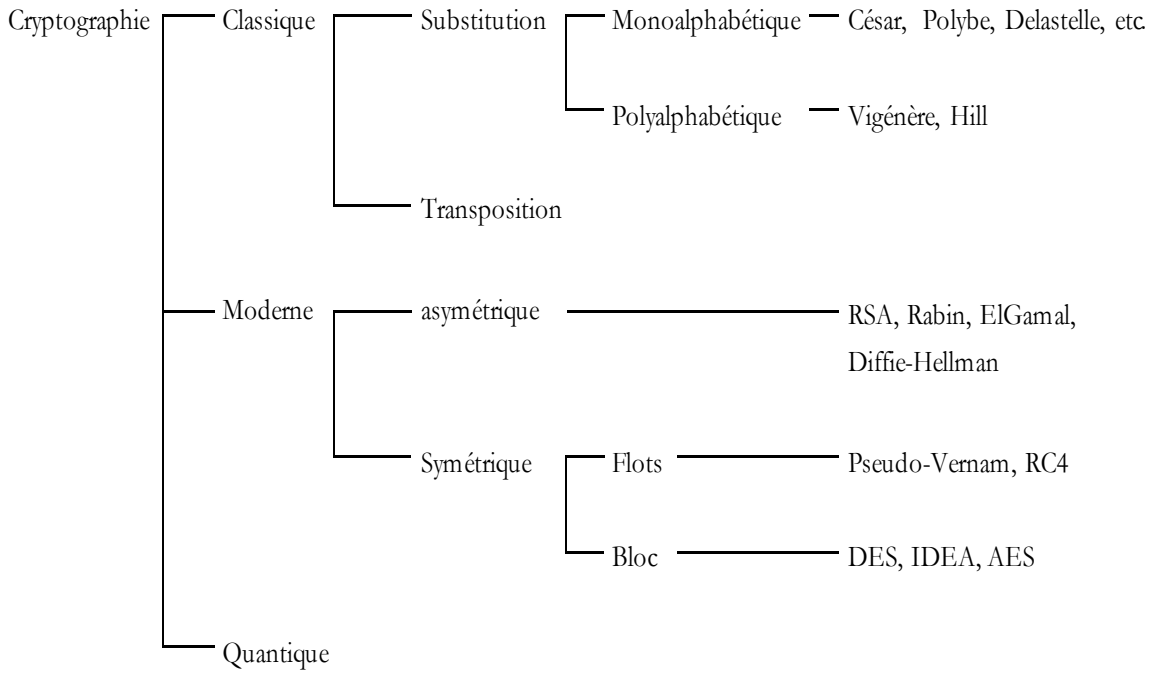


FIGURE II.2 – Classification des systèmes cryptographiques.

Actuellement, les cryptosystèmes sont classés en deux catégories (*c.f.* figure II.2) : classique (comprenant entre autre, la substitution et la transposition) et moderne relatif aux techniques complexes symétriques et asymétriques. Les techniques asymétriques emploient des clés publiques basées sur les nombres premiers, tandis que les techniques symétriques utilisent des clés privées du même principe de la cryptographie classique, néanmoins, elles sont plus longues et nombreuses avec des algorithmes de chiffrement plus complexes. Cependant, la cryptographie classique demeure un référentiel de développement des techniques à clés secrètes. Elle est également utilisable dans certains environnements à risque modéré et ce, grâce à la simplicité de ses algorithmes et sa rapidité de chiffrement

II.2 Cryptographie symétrique

Le chiffrement à clé symétrique, également appelé chiffrement conventionnel ou chiffrement à clé **secrète**, assure le secret lorsque deux parties, par exemple Alice et Bob, communiquent entre eux. Un adversaire qui intercepte un message ne peut obtenir aucune information significative sur son contenu.

Pour établir leur canal de communication sécurisé, *Alice* et *Bob* se mettent d'abord d'accord sur une clé K. Ils gardent leur clé partagée K secrète. Avant d'envoyer un message M à Bob, Alice chiffre M en utilisant l'algorithme de chiffrement E et la clé K. Elle obtient le texte chiffré $C = E(K,M)$ et envoie C à Bob. En utilisant l'algorithme de algorithme de décryptage D et la même clé K, Bob déchiffre C pour récupérer le texte en clair $M = D(K,C)$.

On parle de cryptage symétrique, car les deux partenaires de communication utilisent la même clé K pour le cryptage et le décryptage. Les algorithmes de chiffrement et de décryptage E et D sont publiquement connus. Toute personne qui connaît la clé peut décrypter les messages chiffrés. Par conséquent, la clé K doit être tenue secrète.

Un problème fondamental dans un schéma symétrique est de savoir comment Alice et Bob peuvent convenir d'une clé secrète partagée K de manière sûre et éfficace. Pour cet échange de clés, les méthodes de la cryptographie à clé publique sont nécessaires, ce que nous abordons dans la section suivante. Il n'existait aucune solution au problème de l'échange de clés, jusqu'à ce que le concept révolutionnaire de la cryptographie à clé publique soit découvert il y a 40 ans.

Examinons de plus près les éléments essentiels d'un schéma de cryptage symétrique, à l'aide de la figure II.3. Nous exigeons que le texte en clair M puisse être récupéré de manière unique à partir du texte chiffré C. Cela signifie que pour une clé K fixe, le schéma de chiffrement doit être

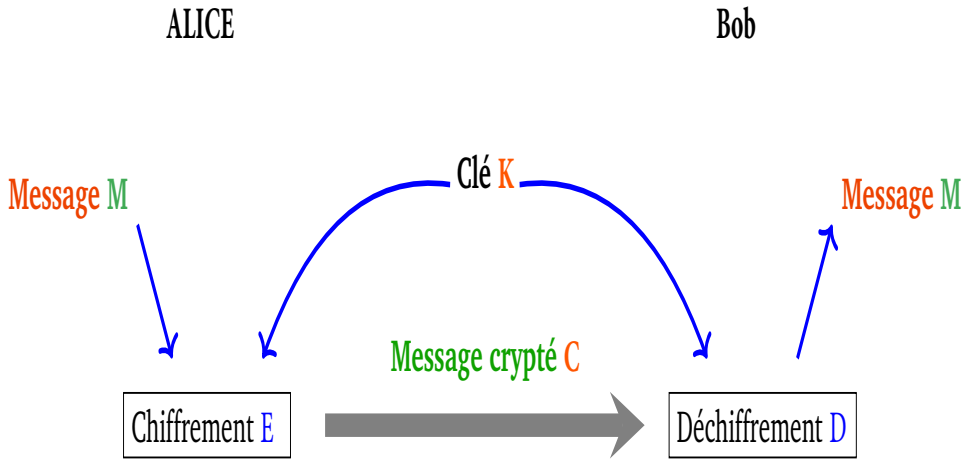


FIGURE II.3 – Modèle simplifié de la cryptographie symétrique.

bijectif. Mathématiquement, le cryptage symétrique peut être considéré comme suit.

Definition II.2.1 Un schéma de cryptage à clé symétrique consiste en une correspondance

$$E : \mathscr{K} \times \mathscr{M} \to \mathscr{C}$$

telle que pour chaque $\forall K \in \mathscr{K}$, la correspondance

$$E_K : \mathscr{M} \to \mathscr{C},\ M \to E(K,M)$$

est inversible. Les éléments $M \in \mathscr{M}$ sont les *plainexts* (aussi appelés *messages*). C est l'ensemble des *ciphertexts* ou cryptogrammes, les éléments $K \in \mathscr{K}$ sont les clés. E_K est appelée la fonction de chiffrement par rapport à la clé K. L'inverse fonction $D_K := E_K^{-1}$ est appelée la fonction de décryptage. On suppose qu'il existe des algorithmes éfficaces pour calculer E_K et D_K.

La clé K est partagée entre les partenaires de communication et maintenue secrète. Une exigence de sécurité de base concernant la fonction de chiffrement E_K consiste à ce que, sans connaître la clé K, il soit impossible d'exécuter avec succès la fonction de déchiffrement D_K. Exemples importants de systèmes de cryptage à clé symétrique : Le tampon à usage unique de Vernam, DES (Data Encryption Standard) et AES (Advanced Encryption. Standard).

II.3 Cryptographie asymétrique

La cryptographie asymétrique, encore appelée cryptographie à clé publique, est une découverte récente dans l'histoire du chiffrement, qui a véritablement révolutionné ce domaine. En effet, d'une part elle a permit de résoudre le problème crucial de l'échange des clés de chiffrement symétrique, et d'autre part elle a apporté une solution au probléme de l'authentification.

Les principes de la cryptographie à clé publique ont été établis par *Whitfield Diffie* et *Martin Hellmann*, dans un article devenu célèbre intitulé *New directions in cryptography* et publié en 1976. Un an plus tard, un tel système est réalisé en pratique, par *Ron Rivest, Adi Shamir* et *Leonard Adleman*, c'est le système cryptographique **RSA**, toujours utilisé de nos jours. Depuis, plusieurs autres systèmes de cryptographie asymétrique ont été découverts, que nous n'étudierons pas dans le cadre de ce cours.

Décrivons d'abord les principes généraux d'un chiffrement asymétrique. Dans un tel système, les protagonistes possèdent chacun une clé qui lui est propre. Ainsi, dans le schéma classique de communication entre Alice et Bob, Alice possède une clé K_A et Bob possède une clé K_B. Chaque clé est constituée de deux parties : une partie secrète (ou privée) et une partie publique. Ainsi

$$\begin{aligned} K_A &= \left(K_A^{priv}, K_A^{pub}\right) \\ K_B &= \left(K_B^{priv}, K_B^{pub}\right) \end{aligned}$$

Comme leur nom l'indique, les clés privées K_A^{priv} et K_B^{priv} ne doivent être connues que de leur propriétaire, soit respectivement Alice et Bob, tandis que les clés publiques sont accessibles à tous.

On a de plus deux fonctions : une de chiffrement E et une de déchiffrement D. À la différence d'un système symétrique, elles sont paramétrées chacune par seulement une partie de la clé. Plus précisément, E est paramétrée par la partie publique K^{pub} et D est paramétrée par la partie privée K^{priv}. Autrement dit, on demande que l'application inverse de $E_{K^{pub}}$ soit $D_{K^{priv}}$.

Ainsi, si Alice souhaite envoyer un message à Bob, elle chiffre son message M par :

$$C = E_{K_B^{pub}}(M)$$

Bob reçoit le chiffré C, et le déchiffre avec sa clé privée :

$$M = D_{K_B^{priv}}(C)$$

En effet, puisque $D_{K_B^{priv}} = E^{-1}_{K_B^{pub}}$, on a bien

$$D_{K_B^{priv}}(C) = D_{K_B^{priv}}\left(E_{K_B^{pub}}(M)\right) = M$$

Notons que Alice, pour chiffrer M, a utilisé la clé publique de *Bob*, et n'a pas eu besoin de sa clé privée.

En retour, si Bob souhaite répondre à *Alice*, il utilisera la clé publique d'Alice pour chiffrer sa réponse, et Alice devra déchiffrer à l'aide de sa propre clé privée. Pour que ce système soit sûr, l'opposant *Eve* ne doit pas pouvoir déchiffrer les messages chiffrés qu'il peut intercepter. Pour cela, il est nécessaire qu'il ne puisse pas calculer la partie privée d'une clé à partir de sa partie publique (à laquelle il a accès bien sûr). Ainsi, il ne doit pas pouvoir calculer K_B^{priv} à partir de K_B^{pub} ou K_A^{priv} à partir de K_A^{pub}.

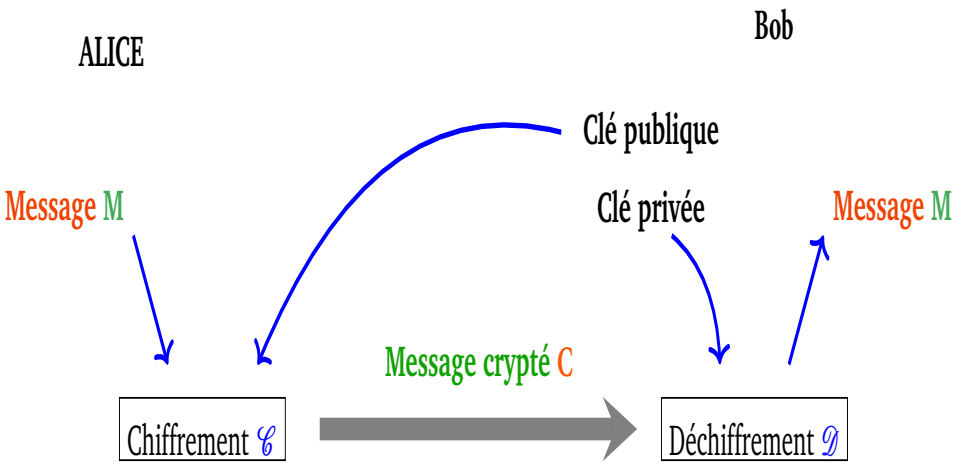


FIGURE II.4 – Modèle simplifié de la cryptographie asymétrique.

En général, la sécurité d'un système cryptographique asymétrique repose sur la difficulté calculatoire d'une opération mathématique. Par exemple, RSA repose sur la difficulté de la factorisation des grands entiers.

II.3.1 Le chiffrement RSA

Definition II.3.1 Une clé RSA $K = \left(K^{priv}, K^{pub}\right)$ est définie à partir des paramètres suivants :

— p et q sont deux (grands) nombres premiers distincts et de même taille binaire.

— e et d sont des entiers tels que $ed = 1 \bmod (p-1)(q-1)$.

— $N = pq$.

Alors

$$K^{pub} = (N, e) \quad \text{et} \quad K^{priv} = d.$$

Les messages clairs et chiffrés sont identifiés à des éléments de $\mathbb{Z}/N\mathbb{Z}$. Les fonctions de chiffrement et de déchiffrement sont définies par :

$$\begin{aligned} E_{K^{pub}} \quad : \quad & \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z} \\ M \quad \mapsto \quad & M^e \bmod N \end{aligned}$$

et

$$\begin{aligned} D_{K^{priv}} \quad : \quad & \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z} \\ C \quad \mapsto \quad & C^d \bmod N \end{aligned}$$

Theorem II.3.1 Avec les notations précédentes, on a bien, pour tout $M \in \mathbb{Z}/N\mathbb{Z}$

$$D_{K^{priv}}\left(E_{K^{pub}}(M)\right) = M$$

Démonstration. On va supposer pour simplifier la démonstration, que M est un entier premier à N, autrement dit que $M \in (\mathbb{Z}/N\mathbb{Z})^*$. D'après les hypothèses, $ed = 1 \bmod (p-1)(q-1)$, donc il existe un entier a tel que $ed = 1 + a(p-1)(q-1)$. On a :

$$\begin{aligned} D_{K^{priv}}\left(E_{K^{pub}}(M)\right) &= D_{K^{priv}}\left(M^e\right) \\ &= (M^e)^d \bmod N \\ &= M^{ed} \bmod N \\ &= M^{1+a(p-1)(q-1)} \bmod N \\ &= M\left(M^{(p-1)(q-1)}\right)^a \bmod N \end{aligned}$$

Puisque $N = pq$, et que p et q sont des premiers distincts, d'aprés la proposition A.1.4, $\phi(N) = \phi(pq) = (p-1)(q-1)$. D'après le théorème d'Euler A.1.3, comme on suppose $pgcd(M,N) = 1$.

$$\left(M^{(p-1)(q-1)}\right)^a \bmod N = 1 \bmod N.$$

Donc

$$D_{K^{priv}}\left(E_{K^{pub}}(M)\right) = M \bmod N$$

■

R Plaçons nous maintenant du point de vue de l'opposant *Eve*. Celle-ci connait e et N, mais pas d, qui lui servirait à déchiffrer. Supposons maintenant que *Eve* soit capable de factoriser N. Cela signifie qu'elle peut calculer les nombres premiers p et q tels que $N = pq$. Alors il peut en déduire $C := (p-1)(q-1)$, puis, en effectuant l'algorithme d'Euclide étendu entre e et C, il peut calculer $d = e^{-1} \bmod C$. Il est donc nécessaire, pour que le chiffrement RSA soit sûr, que N ne puisse pas être factorisé. Dans la pratique, on choisit les paramètres de sorte que l'entier N soit de l'ordre de 1024 bits. Le système RSA repose sur la dissymétrie calculatoire des deux opérations suivantes, en quelque sorte inverses l'une de l'autre :

1. Choisir deux nombres premiers p et q de 512 bits et calculer $N = pq$
2. Étant donné N un entier de 1024 bits ayant exactement deux facteurs premiers, calculer ces facteurs.

Il existe des algorithmes rapides pour effectuer la première opération, alors que la deuxième est impossible à réaliser (en un temps raisonnable) avec les méthodes connues à l'heure actuelle.

II.3.2 L'authentification RSA

Supposons maintenant que Bob veuille transmettre un message M à *Alice*, en garantissant à Alice qu'il est bien l'auteur de ce message. Il s'agit ici d'une problématique, l'authentification, totalement différente de celle de la confidentialité. En effet, cette fois, *Bob* ne souhaite pas empêcher l'opposant *Eve* de prendre connaissance de M. Il souhaite empêcher *Eve* de pouvoir se faire passer pour lui, par exemple en communicant avec Alice en prétendant être Bob.

Voici comment il peut procéder : il calcule $S := D_{K_B^{priv}}(M)$ et transmet à Alice le couple (M,S). Alice, pour se convaincre que le couple (M,S) provient bien de Bob, vérifie que

$$E_{K_B^{pub}}(S) = M$$

En effet, on a

$$E_{K_B^{pub}}(S) = M \iff S = D_{K_B^{priv}}(M)$$

ce qui montre à Alice que S a bien été obtenu à l'aide de K_B^{priv} , que Bob est la seule personne à détenir.

II.4 Cryptographie conventionnelle

Dans cette section , nous examinons un échantillon de ce que l'on pourrait appeler les techniques de cryptage conventionnelles. L'étude de ces techniques nous permet d'illustrer

les approches de base du cryptage symétrique utilisées aujourd'hui et les types d'attaques cryptanalytiques à prévoir.

Les deux éléments de base de toutes les techniques de cryptage sont la substitution et la transposition, que nous examinons dans les deux sous-sections suivantes. Enfin, nous discutons d'un système qui combine à la fois la substitution et la transposition.

II.4.1 Chiffrement par substitution

Une technique de substitution est une technique dans laquelle les lettres du texte en clair sont remplacées par d'autres lettres, des chiffres ou des symboles1. Si le texte en clair est considéré comme une séquence de bits, la substitution consiste à remplacer les bits du texte en clair par des bits du texte chiffré.

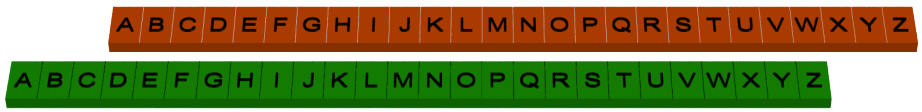
Chiffrement de César

L'utilisation la plus ancienne et la plus simple d'un chiffrement par substitution est celle de Jules César. Le chiffrement de César, nommé aussi chiffrement par décalage, consiste à remplacer chaque lettre de l'alphabet par la lettre qui se trouve trois places plus bas dans l'alphabet. Par exemple,

En clair : meet me after the toga party

Chiffré : PHHW PH DIWHU WKH WRJD

Notez que l'alphabet est enveloppé, de sorte que la lettre qui suit **Z** est **A**. On peut définir la transformation en énumérant toutes les possibilités, comme suit :



Attribuons un équivalent numérique à chaque lettre :

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

L'algorithme peut alors être exprimé comme suit. Pour chaque lettre du texte en clair M , on substitue la lettre du texte chiffré C :

$$C = E(3,M) = (M+3) \bmod 26$$

Un décalage peut être de n'importe quel montant, de sorte que l'algorithme général de César est le suivant

$$C = E(K,M) = (M+K) \bmod 26$$

où K prend une valeur comprise entre 1 et 25. L'algorithme de décryptage est simplement

$$M = D(K,C) = (C-K) \bmod 26$$

Si l'on sait qu'un texte chiffré donné est un chiffrement César, alors une cryptanalyse par force brute est facilement réalisable : il suffit d'essayer les 25 clés possibles. Trois aspects importants de ce problème nous ont permis d'utiliser une cryptanalyse par force brute :

1. Les algorithmes de chiffrement et de déchiffrement sont connus.
2. Il n'y a que 25 clés à essayer.
3. La langue du texte en clair est connue et facilement reconnaissable.

Chiffrement mono-alphabétique

Avec seulement 25 clés possibles, le chiffrement de César est loin d'être sûr. Une substitution monoalphabétique est un chiffrement dans lequel chaque occurrence d'un symbole de texte en clair est remplacée par un symbole de texte chiffré correspondant pour générer un texte chiffré. La clé d'un tel chiffrement est une table de correspondance ou une fonction à partir de laquelle la correspondance est calculée. Un chiffrement affine $E(x) = (ax+b) \bmod 26$ est un exemple de substitution monoalphabétique.

Example II.1 Chiffrer ITS COOL avec $E(x) = (5x+8) \bmod 26$ ∎

Solution II.1 En remplissant le tableau suivant, on obtient

En clair	I	T	S	C	O	O	L
x	8	19	18	2	14	14	11
$5x+8$	48	103	98	18	78	78	63
$(5x+8) \bmod 26$	22	25	20	18	0	0	11
Chiffré	W	Z	U	S	A	A	L

∎

Si $y = E(x) = (ax+b) \bmod 26$, alors nous pouvons "résoudre x en fonction de y" et ainsi déterminer $E^{-1}(y)$. Autrement dit, si $y = (ax+b) \bmod 26$, alors $y-b = ax \pmod{26}$, ou de façon équivalente $ax = (y-b) \pmod{26}$. En utilisant nos résultats précédents, nous voyons que si nous multiplions les deux côtés par $a^{-1} \pmod{26}$, alors $x = a^{-1}(y-b) \pmod{26}$ et donc notre fonction

de déchiffrement est

$$E^{-1}(y) = a^{-1}(y-b)(\text{mod}\,26)$$

Example II.2 Déchiffrer HPCCXAQ si la fonction de chiffrement est $E(x) = (5x+8)\,\text{mod}\,26$

■

Solution II.2 On commence par trouver la fonction de déchiffrement. Puisque $5x = 1(\text{mod}\,26)$ est résolu avec $x = 21(\text{mod}\,26)$ nous voyons $5^{-1}(\text{mod}) = 21$. Par conséquent,

$$E^{-1}(y) = 21(y-8)(\text{mod}\,26)$$

En remplissant le tableau suivant, on obtient

Chiffré	H	P	C	C	X	A	Q
y	7	15	2	2	23	0	16
$(y-8)$	-1	7	-6	-6	15	-8	8
$21(y-8)$	-21	147	-126	-126	315	-168	168
$21(y-8)(\text{mod}\,26)$	5	17	4	4	3	14	12
En clair	F	R	E	E	D	O	M

■

Chiffrement poly-alphabétique

Une autre façon d'améliorer la technique monoalphabétique simple consiste à utiliser différentes substitutions mono-alphabétiques à mesure que l'on avance dans le message en clair. Cette approche est généralement appelée chiffrement par substitution poly-alphabétique. Toutes ces techniques ont les caractéristiques suivantes en commun :

1. Un ensemble de règles de substitution mono-alphabétique connexes est utilisé.
2. Une clé détermine quelle règle particulière est choisie pour une transformation donnée.

Le cryptosystème du carré de Vigenère est un exemple de substitution polyalphabétique. C'est-à-dire que différentes lettres du texte en clair sont cryptées avec des alphabets de substitution différents.

Clé secrète : les correspondants se mettent d'accord sur un mot-clé.

Pour chiffrer : Écrire le mot clé à plusieurs reprises à côté du texte en clair, convertir le texte en clair et les lettres du mot-clé en leurs équivalents numériques (0 pour **A**, 25 pour Z) et les additionner modulo 26.

Example II.3 Si le mot clé est WIND et le texte en clair est GO AHEAD MAKE MY DAY, alors le texte chiffré est

En clair	G	O	A	H	E	A	D	M	A	K	E	M	Y	D	A	Y
M	6	14	0	7	4	0	3	12	0	10	4	12	24	3	0	24
clé	W	I	N	D	W	I	N	D	W	I	N	D	W	I	N	D
K	22	8	13	3	22	8	13	3	22	8	13	3	22	8	13	3
$(M+K) \bmod 26$	2	22	13	10	0	8	16	15	2	18	7	15	22	11	13	1
Chiffré	C	W	N	K	A	I	Q	P	W	S	R	P	U	L	N	B

■

Pour déchiffrer : Écrire le mot clé à plusieurs reprises à côté du texte chiffré, convertir le texte chiffré et les lettres du mot clé en leurs équivalents numériques et les soustraire modulo 26. les lettres du mot clé en leurs équivalents numériques, et les soustraire modulo 26.

Example II.4 Si le mot clé est BAR et le texte en clair est DEJUPCVSUJFWJCZME, alors le déchiffrement est

Chiffré	D	E	J	U	P	C	V	S	U	J	F	W	J	C	Z	M	E
C	3	4	9	0	15	2	21	18	20	9	5	22	9	2	25	12	4
clé	B	A	R	B	A	R	B	A	R	B	A	R	B	A	R	B	A
K	1	0	17	1	0	17	1	0	17	1	0	17	1	0	17	1	0
$(C-K)$	2	4	-8	19	15	-15	20	18	3	8	5	5	8	2	8	11	4
$(C-K) \bmod 26$	2	4	18	15	15	11	20	18	3	8	5	5	8	2	8	11	4
En clair	C	E	S	T	P	L	U	S	D	I	F	F	I	C	I	L	E

■

Chiffrement de Hill

On décrit maintenant un autre système cryptographique polyalphabétique appelé chiffrement de Hill. Soit m un entier strictement positif, et soit $\mathscr{C} = \mathscr{M} \in (\mathbb{Z}/26\mathbb{Z})^m$. L'idée consiste à transformer m caractères d'un bloc de texte clair en m caractères d'un bloc de texte chiffré par des *combinaisons linéaires.*

Si $m = 2$, alors pour un bloc de texte clair $x = (x_1, x_2)$, on obtient un bloc de texte chiffré $y = (y_1, y_2)$ où y_1 et y_2 sont obtenus comme combinaisons linéaires de x_1 et x_2. Par exemple, $y_1 = 11x_1 + 3x_2$, $y_2 = 8x_1 + 7x_2$. (L'addition et la multiplication sont réalisées dans $\mathbb{Z}/26\mathbb{Z}$.). On peut bien entend écrire cela en sous la forme d'un produit matriciel :

$$(y_1, y_2) = (x_1, x_2) \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$$

En général, on prend une matrice carrée de taille $m \times m$ pour clé K. Si le coefficient (i, j) de la matrice est $k_{i,j}$, on écrit $K = (k_{i,j})$. Pour $x = (x_1, \cdots, x_m) \in \mathscr{M}$, et $K \in \mathscr{M}$, on calcule

$y = E(x,K) = (y_1, \cdots, y_m)$ ainsi

$$(y_1, \cdots, y_m) = (x_1, \cdots, x_m) \begin{pmatrix} k_{1,1} & \cdots & k_{1,m} \\ \vdots & \ddots & \vdots \\ k_{m,1} & \cdots & k_{m,m} \end{pmatrix}$$

C'est-à-dire que l'on calcule $y = xK$. On dit que le texte chiffré est obtenu par une transformation linéaire. Pour voir comment le procédé de chiffrement fonctionne, on doit trouver comment calculer x à partir de y. Si vous vous souvenez de vos cours d'algèbres linéaires, alors vous savez que l'on utilise la matrice inverse K^{-1}. En effet, le texte clair est calculé par la formule $x = yK^{-1}$.

Theorem II.4.1 Si $A = (a_{i,j})$ est une matrice 2×2 à coefficients dans $\mathbb{Z}/26\mathbb{Z}$ telle que $\det A$ est inversible modulo 26. Alors on a

$$A^{-1} = (\det A)^{-1} \begin{pmatrix} a_{2,2} & -a_{1,2} \\ -a_{2,1} & a_{1,1} \end{pmatrix}$$

Example II.5 considérons la matrice $A = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$, on a

$$\begin{aligned} \det A &= 11 \times 7 - 3 \times 8 (\mathrm{mod}\, 26) \\ &= 53 (\mathrm{mod}\, 26) \\ &= 1 (\mathrm{mod}\, 26) \end{aligned}$$

Alors, $A^{-1} = (1)^{-1} \begin{pmatrix} 7 & -8 \\ -3 & 11 \end{pmatrix} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$ ∎

II.4.2 Chiffrement par transposition

Une autre grande catégorie de chiffres «historiques» est celle des chiffres à transposition. Dans ces derniers, au lieu de faire des substitutions de lettres comme précédemment, on va modifier la position relative des différentes lettres du clair pour obtenir le cryptogramme, un peu à la manière d'un anagramme. Ainsi, une transposition réalise une permutation des caractères clairs. Dans ce cas, il doit obligatoirement y avoir correspondance entre l'alphabet des clairs et l'alphabet des cryptogrammes : $\mathscr{A}_C = \mathscr{A}_M$.

Definition II.4.1 Un chiffrement à transposition est défini par la fonction f qui, pour une clé K donnée (une permutation), modifie la position i du clair M en la position $K(i)$ dans le cryptogramme C :

$$\begin{aligned} f &: \mathscr{A}_C = \mathscr{A}_M \\ K &: \mathbb{Z}/N\mathbb{Z} \\ C_i &: f(M_i) = M_{K(i)} \quad \forall i, \quad 0 \leq i \leq |M| \end{aligned}$$

Example II.6 A partir d'une phrase-clé, on définit une clé numérique comme suit [2] :

T	R	A	N	S	P	O	S	I	T	I	O	N
12	9	1	40	10	8	6	11	2	13	3	7	5

On chiffre le clair : «le chiffrement est l'opération qui consiste à transformer un texte clair en un texte inintelligible appelé texte chiffré». Pour cela, on range les lettres du clair dans un tableau qui a autant de colonnes que la longueur de la clé numérique obtenue à partir de la phrase-clé :

12	9	1	40	10	8	6	11	2	13	3	7	5
L	E	C	H	I	F	F	R	E	M	E	N	T
E	S	T	L	O	P	E	R	A	T	I	O	N
Q	U	I	C	O	N	S	I	S	T	E	A	T
R	A	N	S	F	O	R	M	E	R	U	N	T
E	X	T	E	C	L	A	I	R	E	N	U	N
T	E	X	T	I	N	I	N	T	E	L	L	I
G	I	B	L	E	A	P	P	L	E	T	E	X
T	E	C	H	I	F	F	R	E				

On inscrit ensuite les colonnes prises dans l'ordre défini par la clé pour obtenir le cryptogramme rangé par groupe de cinq lettres :

CTINT XITEA SERNP FEIEU NELEH LCSET
BETNT TNLTF ESRAN AINOA NULEF PNOLI
EHESU AXEGX IOOFC ELCRR IMIIP FLEQR
ETIEM TTRET ER

■

II.5 Chiffrement et déchiffrement

Les méthodes de chiffrement symétrique, encore appelé chiffrement conventionnel ou chiffrement à clé secrète, se divisent naturellement en deux familles, le chiffrement par bloc (« block cipher ») et le chiffrement par flot (« stream cipher »), décrites ci-dessous.

2. Ici la clé est codé selon l'ordre de l'apparition de l'alphabet.

II.5.1 Chiffrement par bloc

Une primitive de chiffrement par bloc est un algorithme traitant les données à chiffrer par blocs de taille fixée. On notera k le nombre de bits de ces blocs de données ; typiquement, cette taille vaut 64 ou 128 bits en pratique. Un tel mécanisme permet donc uniquement de combiner une suite de k bits de données avec une clé de n bits afin d'obtenir un bloc de données chiffrées de même taille k que le bloc de données claires.

L'une des principales propriétés attendues d'un mécanisme de chiffrement par bloc est d'être facilement inversible si l'on dispose de la clé secrète de chiffrement. On veut également que, sans informations sur la clé secrète, il soit impossible en pratique de retrouver de l'information sur le message d'origine. Seuls les détenteurs de la clé secrète doivent être capables de transformer des données claires en données chiffrées et, inversement, des données chiffrées en données claires.

Example II.7 L'un des exemples les plus connus d'algorithme de chiffrement par bloc est le DES défini en 1977 par le NIST, institut de normalisation américain, comme standard de chiffrement à usage commercial. Il traite des blocs de $k = 64bits$ au moyen de clés de $n = 56bits$. La sécurité du DES a fait couler depuis lors beaucoup d'encre. Cet algorithme peut cependant être considéré comme particulièrement bien conçu, la meilleure attaque pratique connue étant la recherche exhaustive sur les clés. La taille de ces clés est cependant sous-dimensionnée, ce qui rend aujourd'hui cette attaque réalisable, au moyen d'une machine dédiée, en quelques heures seulement.

On utilise cependant toujours couramment le DES mais sous la forme du « triple DES », une variante utilisant des clés de 112 bits, inattaquable par recherche exhaustive. L'objectif à moyen terme est cependant de le remplacer par l'AES, sélectionné par le NIST au terme d'une compétition internationale. L'AES est conçu pour traiter des blocs de $128bits$ au moyen de clés de $128, 192$ ou $256bits$.

Plus généralement, un algorithme de chiffrement par bloc combine des opérations de **substitution**, visant à remplacer des symboles par d'autres afin d'en cacher le sens, avec des opérations de **permutation** échangeant la position des symboles. Ces deux principes sont historiquement très anciens mais demeurent encore valables aujourd'hui, toute primitive de chiffrement par bloc pouvant être vue comme une combinaison intelligente de ces deux opérations. ∎

À ce niveau, il convient de comprendre précisément ce que permet de faire un algorithme de chiffrement par bloc, et surtout ce qu'il ne permet pas. Tout d'abord, un tel algorithme permet uniquement de traiter des blocs de taille fixe, relativement petite. Par conséquent, afin de chiffrer

des messages de taille quelconque, il convient de définir comment le message doit être codé en une suite de blocs de taille fixe. Ceci implique de définir très précisément comment répartir l'information de tels messages en une suite de bits de longueur exactement un multiple de la taille k du bloc élémentaire. On appelle cette opération le « padding » ou le « bourrage ».

De plus, un algorithme de chiffrement par bloc est fondamentalement déterministe : à partir d'un bloc de données et d'une clé secrète, il produit toujours le même bloc de chiffré. Ainsi, un attaquant passif observant deux blocs de chiffré identiques peut immédiatement en déduire que les blocs de message clair correspondants sont identiques, sans pour autant apprendre la moindre information sur ce clair. Dans certaines circonstances, une telle information est cependant sufsante pour attaquer un système.

Example II.8 À titre d'exemple, imaginons un système bancaire où, afin de vérifier la validité d'un PIN code (« Personal Identification Number ») à quatre chiffres de carte de crédit, ce code est chiffré et envoyé à un central bancaire. Si l'on utilise un simple chiffrement par bloc avec une clé bancaire fixe, à chaque PIN code va correspondre un unique chiffré. On peut dès lors imaginer par exemple qu'un attaquant observant les communications apprendra immédiatement qui a le même PIN code que lui. ∎

Afin de traiter des messages de taille quelconque et d'assurer la confidentialité globale de ces messages, et pas uniquement une confidentialité « par bloc », il convient donc de définir un **mode opératoire** précisant comment convertir le message en une suite de blocs ainsi que le mode de chiffrement de ces blocs afin d'obtenir finalement le message chiffré.

R Notons que la définition d'un tel mode opératoire n'a nul besoin de tenir compte des détails de l'algorithme de chiffrement par bloc employé ; seul la taille k des blocs est réellement nécessaire. Notons encore qu'afin de rompre le caractère déterministe du chiffrement, il est nécessaire de « randomiser » le processus, c'est-à-dire d'introduire une valeur aléatoire.

Example II.9 Le mode opératoire le plus connu est le CBC (« cipher-block chaining »). Une des nombreuses variantes fonctionne de la manière suivante : afin de chiffrer un message formé d'une suite de bits, on commence par ajouter à droite un bit valant 1 et autant de 0 que nécessaire afin d'obtenir un nombre total de bits multiple de la taille du bloc. Notons $x_1, x_2, \cdots, x_t$ les t blocs de message clair ainsi obtenus. On choisit ensuite un bloc aléatoire, noté IV pour « initial vector », indépendant du message et des précédents chiffrements. Si l'on note $E_K(x)$ le résultat du chiffrement du bloc x avec la clé K, le chiffré $(c_0, c_1, c_2, \cdots, c_t)$ du message est obtenu en posant $c_0 = IV$ et en calculant successivement $c_i = E_K(c_{i-1} \oplus xi)$pour i allant de 1 à t (l'opérateur «

ou-exclusif » noté « $\oplus$ » représente l'addition bit à bit, sans retenue). Graphiquement, on obtient la représentation symbolique de la figure II.5. ∎

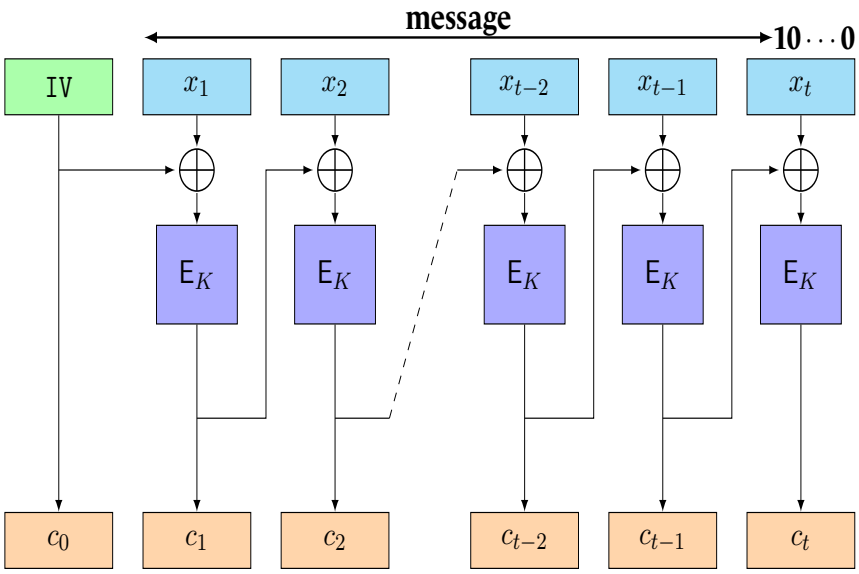


FIGURE II.5 – Mode opératoire CBC.

Cet exemple de mode opératoire illustre la phase initiale de padding, consistant à compléter le message par un bit valant 1 suivi de bits nuls. Il montre également que l'emploi de données aléatoires, via l'IV, permet de rendre le chiffrement non déterministe. Ainsi, le chiffrement du même message deux fois de suite n'a qu'une chance infime d'utiliser le même IV et par conséquent l'ensemble du chiffré va différer à cause du mécanisme de rebouclage faisant intervenir le bloc de chiffré c_{i-1} lors du chiffrement du bloc de message clair x_i. Notons encore que dans cette variante du mode CBC, l'IV est transmis en clair, sans avoir besoin d'être chiffré. Afin de déchiffrer un message $(c_0, c_1, c_2, \cdots, c_t)$, il suft de calculer $xi = c_{i-1} \oplus D_K(c_i)$ pour i allant de 1 à t, $D_K(c)$ désignant le déchiffré du bloc c avec la clé secrète K. Il est facile de vérifier que le message ainsi obtenu est bien le message initial.

R Notons enfin que ce mode a naturellement une propriété d'auto-synchronisation ; si des blocs de chiffré sont perdus en cours de transmission, il suft d'obtenir deux blocs successifs intacts afin de pouvoir reprendre correctement le déchiffrement.

II.5.2 Chiffrement par flot

Les primitives de chiffrement par flot utilisent une approche différente du chiffrement par bloc au sens où elles considèrent généralement le message à chiffrer comme une suite de bits qui sont combinés de manière simple (généralement un « ou-exclusif bit à bit ») avec une séquence de bits dérivée de la clé secrète (et dans la plupart des cas également d'un vecteur d'initialisation).

Les algorithmes de chiffrement par flot s'inspirent du chiffrement de *Vernam* qui est à la fois très simple, très sûr et inutilisable en pratique. Si l'on considère un message représenté sous la forme d'une suite de bits $m_1, m_2, m_3, \ldots$ ainsi qu'une clé également vue comme une suite de bits $k_1, k_2, k_3, \ldots$, le chiffré du message est alors très simplement obtenu au moyen de l'opération de « ou-exclusif bit à bit » (appelée le XOR), où le $i-ème$ bit de chiffré ci s'obtient par addition (sans retenue) du $i-ème$ bit de message avec le $i-ème$ bit de clé, soit $c_i = m_i \oplus k_i$. Ainsi $0 \oplus 0 = 0, 0 \oplus 1 = 1 \oplus 0 = 1$ et $1 \oplus 1 = 0$, le dernier cas étant le seul où l'opération XOR diffère de l'addition classique. Afin de déchiffrer, il suft d'appliquer la même opération de ou-exclusif bit à bit du chiffré avec la clé secrète car $c_i \oplus k_i = (m_i \oplus k_i) \oplus k_i = m_i \oplus (k_i \oplus k_i) = m_i \oplus 0 = m_i$, en remarquant que, quelle que soit la valeur k_i de chaque bit de clé, $k_i \oplus k_i$ vaut toujours 0. Le chiffrement du message M est illustré dans la figure II.6.

Il est facile de démontrer que le chiffrement de *Vernam* est parfaitement sûr, en termes de confidentialité, si la clé est au moins de même taille que le message à chiffrer et n'est utilisée qu'une seule fois. Ceci restreint évidemment considérablement les applications envisageables à cause de la taille de la clé à partager entre émetteur et destinataire ; dans la plupart des cas, cette mise en accord de clé secrète pose un problème similaire à la transmission sécurisée du message lui-même.

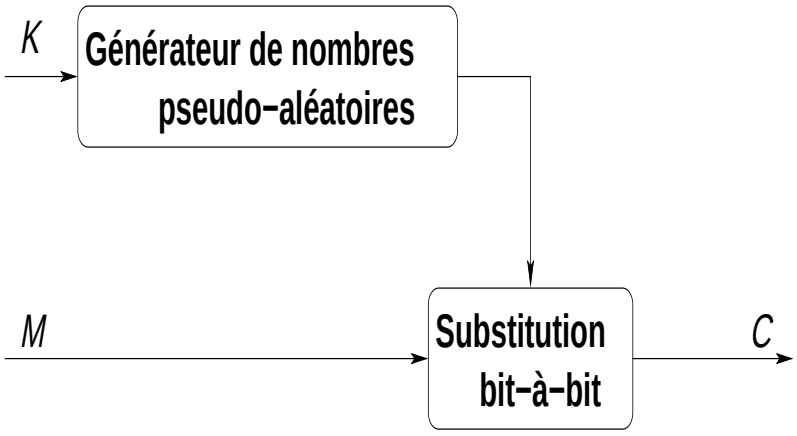


FIGURE II.6 – Chiffrement symétrique par flot.

L'idée maîtresse du chiffrement par flot est d'utiliser des clés de petite taille, typiquement de l'ordre de $128bits$, et d'en dériver de manière déterministe, et par conséquent parfaitement reproductible, des suites d'allure aléatoire pouvant être utilisées comme des clés de même longueur que le message avec l'algorithme de chiffrement de *Vernam*. Le déchiffrement agit ensuite de même, en générant la même suite à partir de la clé secrète. Le chiffrement par flot dérivé de l'algorithme de *Vernam* fournit un exemple simple et particulièrement éloquent du fait qu'assurer la confidentialité, même de manière parfaite, n'entraîne pas automatiquement une protection en intégrité du message transmis. En effet, si un attaquant désire inverser un bit de message clair, c'est-à-dire transformer un 0 en 1 ou inversement, il lui suft d'ajouter 1 au bit de chiffré c_i et donc de transmettre $\acute{c}_i = c_i \oplus 1$. Lors du déchiffrement, le destinataire va calculer $\acute{c}_i \oplus k_i = c_i \oplus 1 \oplus k_i = m_i \oplus 1$; si m_i vaut 0 le résultat obtenu est un 1 et, inversement, si mi vaut 1 le résultat est $1 \oplus 1 = 0$. Par conséquent, même si l'attaquant n'a aucune idée de la valeur du bit modifié, il peut à coup sûr et sans effort l'inverser.

On parle de chiffrement par **flot synchrone** lorsque la suite chiffrante est calculée à partir de la clé secrète, indépendamment du message à chiffrer. Inversement, les algorithmes de chiffrement par **flot asynchrones**, ou **auto-synchronisants** utilisent des suites chiffrantes dépendant de la clé secrète mais également d'un certain nombre de bits de texte chiffré. L'intérêt avancé pour une telle approche est de permettre une sorte de resynchronisation automatique du déchiffrement, même si des portions de message chiffré sont perdues lors de la transmission.

R Notons qu'une telle propriété tient plus de la correction d'erreurs de transmission que d'une quelconque protection de nature cryptographique des données. On peut dès lors s'interroger sur l'adéquation de telles techniques ainsi que sur la menace réelle qu'elle vise à éviter. Notons également que certains modes opératoires de chiffrement par bloc, tel que le mode CBC vu précédemment, possèdent aussi cette propriété d'auto-synchronisation à condition que des blocs entiers soient perdus. Le plus célèbre exemple d'un tel chiffrement est l'algorithme RC4 (*Rivest Cipher 4*), utilisé dans la conception de plusieurs protocoles notamment le SSL, Netscape, WEP, WPA, etc

II.5.3 Intégrité et authenticité

Des techniques cryptographiques symétriques permettent également de garantir l'intégrité de données transmises, qu'elles soient déjà protégées en confidentialité ou non. De tels mécanismes visent à garantir qu'aucune altération des données n'a eu lieu au cours de leur transmission. L'inadéquation des mécanismes de chiffrement pour garantir une telle intégrité des données a

déjà été mentionnée. Notons par ailleurs que les méthodes cryptographiques visent en général à se prémunir face à des attaques volontaires, potentiellement intelligentes, par opposition aux techniques de codage et aux protocoles de transmission visant à détecter ou à corriger des erreurs aléatoires et involontaires.

Plus précisément, la principale technique permettant d'assurer l'intégrité des données consiste à calculer un code d'**authentification** de message (souvent appelé MAC pour « *Message Authentication Code* ») à partir des données à protéger et d'une clé secrète partagée avec celui à qui le message est destiné. Ce code d'authentification, typiquement long de 128 bits, est ensuite ajouté au message et transmis. Après réception, le code d'authentification est recalculé à l'aide de la clé secrète et du message reçu, potentiellement corrompu. Le résultat obtenu est comparé au MAC reçu ; s'ils sont identiques, il est extrêmement probable que les données sont intègres et proviennent donc de la bonne personne.

R Il faut insister sur la différence conceptuelle fondamentale existant entre chiffrement et calcul de code d'authentification de message. Par contre, à un niveau plus technique, de nombreuses similarités peuvent réapparaître. L'algorithme le plus connu de calcul de MAC est le CBC-MAC. Le code d'authentification est alors simplement calculé en appliquant le mode de chiffrement CBC (décrit figure II.5) au message, sans utiliser de vecteur d'initialisation (IV), et en ne conservant comme valeur de MAC que le dernier bloc de chiffré, surchiffré avec une clé $\acute{K}$, différente de celle utilisée dans la chaîne CBC. Graphiquement, on obtient la représentation symbolique de la figure II.7. On voit clairement que toute modification, même minime, du message à protéger engendre un résultat totalement différent comme MAC. Il faut cependant se garder de penser qu'un tel mécanisme est sûr, dans un sens général, sur cette simple impression initiale, car une telle analyse ne constitue pas une preuve de sécurité.

La protection de l'**intégrité** d'un message garantit également, vis-à-vis du destinataire, son authenticité car la connaissance de la clé secrète est nécessaire pour générer des MAC corrects. Par contre, cette authentification n'a pas de valeur vis-à-vis d'un tiers car rien ne permet de savoir par quel détenteur de la clé secrète un MAC est réellement généré. De plus, toute vérification par un tiers nécessite de lui révéler la clé secrète utilisée. Ceci est intrinsèquement lié à la nature symétrique du mécanisme.

On désigne parfois les codes d'authentification de message sous le terme de **signature symétrique** mais il doit être bien entendu que ce qualificatif de signature est impropre pour la simple raison que la propriété de non-répudiation n'est pas assurée. Actuellement, seuls les

mécanismes asymétriques, qui évitent justement que la connaissance de la clé secrète ne soit nécessaire pour vérifier la validité d'une signature, peuvent réellement rendre de tels services de sécurité.

R Notons enfin qu'un code d'authentification de message valide ne permet que de garantir l'authenticité de ce message. Si l'on souhaite assurer l'intégrité et l'authenticité d'un ensemble de messages formant une communication, et éviter par exemple le rejeu ou la suppression de certains messages accompagnés de MACs valides, il convient de soigner les méthodes de chaînage employées.

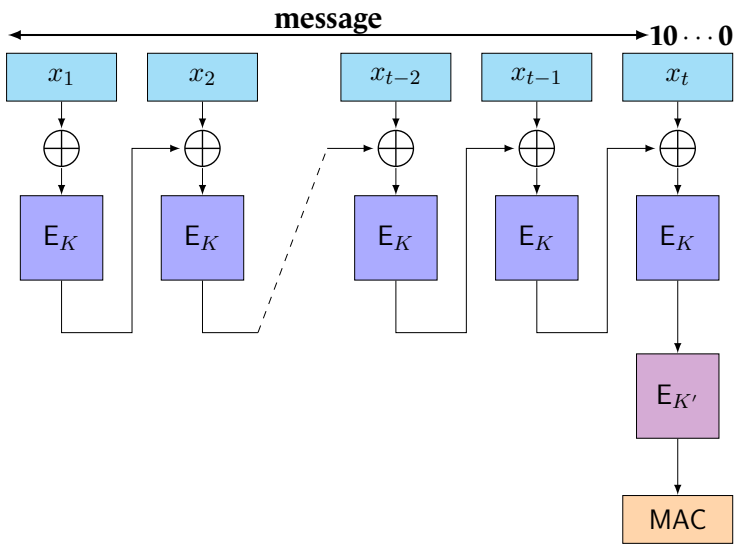


FIGURE II.7 – Mode opératoire CBC-MAC.

III. La sécurité du Parefeu (Firewall)

La connectivité Internet n'est plus optionnelle pour les entreprises. Les informations et les services disponibles sont essentiels pour celles-ci. De plus, les utilisateurs individuels au sein de l'organisation veulent et ont besoin d'un accès à Internet, et si cet accès n'est pas fourni par leur réseau local, ils utiliseront un accès commuté depuis leurs PC vers un fournisseur de services Internet (ISP). Toutefois, même si l'accès à Internet présente des avantages pour l'organisation, il permet au monde extérieur d'atteindre et d'interagir avec les ressources du réseau local. Cela crée une menace à l'entreprise. Une alternative largement acceptée, ou du moins un complément aux services de sécurité basés sur l'hôte, est le pare-feu, qui est inséré entre le réseau local et l'Internet pour établir un lien contrôlé et ériger un mur ou un périmètre de sécurité externe. L'objectif de ce périmètre est de protéger le réseau des locaux contre les attaques basées sur l'Internet et de fournir un point de blocage simple où la sécurité et l'audit peuvent être imposés.

III.1 Définitions de base d'un pare-feux

Un firewall est un dispositif séparant un réseau considéré comme "sûr" d'un réseau en principe "hostile". Le cas le plus fréquent est l'accès à Internet, mais cela permet de séparer aussi différents départements d'une même société. Ce dispositif est constitué de matériels, routeurs et ordinateurs, et de logiciels pour la partie active et la configuration. Les pare-feu ont pour fonction de séparer un réseau de telle sorte que le trafic échangé entre ce réseau et l'extérieur soit contrôlé et que d'éventuelles attaques soient ainsi empêchées.

Un pare-feu est un ensemble de composants placé entre deux réseaux ayant les propriétés suivantes :

— Tout le trafic transitant entre les deux réseaux passe nécessairement par le pare-feu.

— Seul le trafic explicitement autorisé par la politique de sécurité appliquée localement est autorisé à passer au travers du pare-feu.

En théorie, il serait possible de filtrer les communications à partir des postes de travail. Cependant, ces derniers hébergent généralement un grand nombre de logiciels qui sont autant de failles de sécurité potentielles car ces logiciels sont plus ou moins bien développés et configurés. De plus, la gestion d'un parc d'ordinateurs auxquels ont accès une multitude d'utilisateurs est difficile. C'est pourquoi il est préférable, en plus de la sécurité mise en place au niveau des postes de travail, de centraliser la sécurité dans un équipement spécialisé dédié à la sécurité et de placer cet équipement à la frontière du site. Pour pénétrer dans le site, la sécurité de cet équipement devra d'abord être déjouée. Bien évidemment, pour assurer le meilleur niveau de sécurité, il est nécessaire de faire tourner un minimum de logiciels sur le pare-feu, de le configurer avec la plus grande précaution et de bien suivre les évolutions de ces logiciels afin d'éviter d'utiliser des versions obsolètes pour lesquelles des failles de sécurité auraient été découvertes.

Les pare-feu remplissent deux fonctions de sécurité de base :

— **Filtrage des paquets**−Déterminer s'il faut autoriser ou refuser le passage de paquets d'informations numériques, en fonction des règles de politique de sécurité établies.

— **Proxy d'application**−Fournir des services réseau aux utilisateurs tout en protégeant les différents ordinateurs hôtes. Pour ce faire, le flux IP (c'est-à-dire le trafic entrant et sortant du réseau).

Les pare-feu peuvent être complexes, mais si on comprend bien chacune de ces deux fonctions, on sera en mesure de choisir le bon pare-feu et de le configurer pour protéger un ordinateur ou un réseau. La figure III.1 illustre un pare-feu placé dans le périmètre d'un réseau.

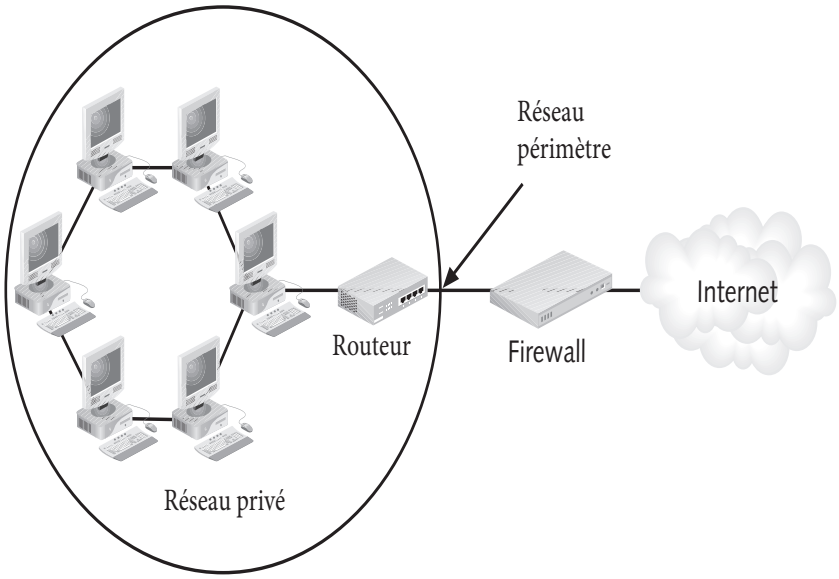


FIGURE III.1 – Pare-feu au niveau du périmètre.

III.2 Les politiques de sécurité

Afin de comprendre le fonctionnement d'un pare-feu, il faut avoir une idée générale de la gamme de menaces contre lesquelles il faut protéger notre réseau, et des tâches de sécurité que le pare-feu peut effectuer.

III.2.1 Restreindre l'accès depuis l'extérieur du réseau

L'objectif le plus évident d'un pare-feu est de réguler les paquets d'informations qui peuvent entrer sur le réseau. Pour ce faire, un pare-feu examine chaque paquet pour déterminer s'il répond aux critères "autorisés" nécessaires. Ces critères peuvent être des protocoles ou des adresses IP (Internet Protocol) figurant sur une liste "approuvée". Tout ce qui ne figure pas sur la liste est exclu. Ce type de filtrage de paquets est abordé plus en détail plus loin dans ce chapitre.

Un pare-feu qui effectue un filtrage des paquets (ce que font pratiquement tous les pare-feu) protège les réseaux contre les attaques par balayage de port. Un port est une sous-adresse réseau (à laquelle est attribué un nombre compris entre 0 et 65535) par laquelle un type particulier de données est autorisé à passer. Au cours d'une attaque par balayage de port, un logiciel spécial examine une série d'adresses réseau et tente de se connecter à chacune d'elles. Si une connexion est établie, elle donne une cible à l'attaquant. Un pare-feu correctement configuré n'autorise que les les tentatives de connexion autorisées aux ports du réseau qu'il protège.

III.2.2 Restreindre l'accès non autorisé depuis l'intérieur du réseau

Il est parfois plus facile de protéger un réseau contre l'Internet que contre une attaque interne. Qu'ils soient mécontents, malhonnêtes ou simplement ignorants des procédures de sécurité appropriées, les employés peuvent être une source majeure de problèmes :

- Les employés qui apportent au bureau des supports mobiles (clés USB, CD/DVD, etc.) ; qui contiennent des fichiers infectés par des virus.
- Les employés qui accèdent aux ordinateurs du bureau depuis leurs domiciles en utilisant des logiciels d'accès à distance qui contournent le pare-feu du périmètre.
- Les attaquants qui obtiennent des informations confidentielles en contactant les employés et en les trompant en les amenant à communiquer de des mots de passe, des adresses IP, des noms de serveurs et ainsi de suite - c'est ce qu'on appelle l'ingénierie sociale. l'ingénierie sociale.
- Des administrateurs de pare-feu mal formés qui pourraient, par exemple, configurer le pare-feu pour filtrer certains paquets IP tout en laissant passer les paquets qui arrivent en fragments.
- Les employés qui reçoivent des messages électroniques avec des pièces jointes exécutables, dont le téléchargement et l'exécution par l'employé peuvent lancer un programme susceptible de se propager à d'autres ordinateurs utilisant le carnet d'adresses électroniques du destinataire.

R Les pare-feu ne peuvent pas empêcher toutes les menaces internes. Il est possible de configurer un pare-feu pour qu'il reconnaisse les paquets ou pour empêcher l'accès aux fichiers protégés depuis des hôtes internes ou externes. Notez toutefois que l'accès à distance et les attaques d'ingénierie sociale ne peuvent être évités que par la formation et la sensibilisation aux procédures de sécurité. et la sensibilisation aux procédures de sécurité.

III.2.3 Limiter l'accès des employés aux hôtes externes

Parallèlement à la restriction du trafic externe du réseau, les pare-feu peuvent autoriser de manière sélective le trafic de l'intérieur du réseau vers Internet ou un autre réseau, afin de permettre un contrôle plus précis de l'utilisation des ressources externes par les employés du réseau. En d'autres termes, le pare-feu peut agir comme un serveur mandataire qui établit des connexions d'application de haut niveau pour le compte des hôtes internes et d'autres machines. Un seul produit pare-feu peut assurer à la fois le filtrage des paquets sortants (illustré à la figure III.2) et des services proxy sortants.

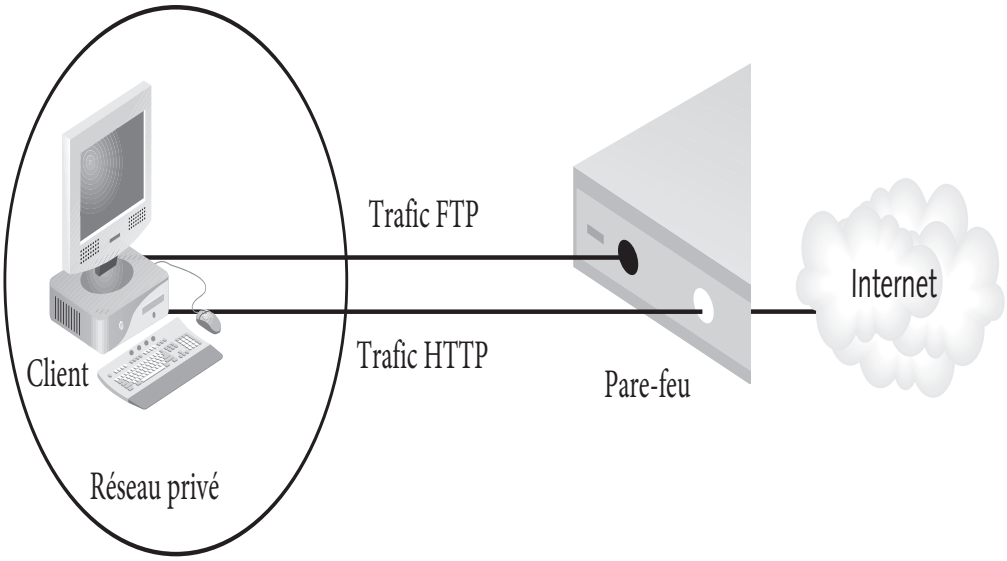


FIGURE III.2 – Filtrage des paquets sortants.

Les applications proxies peuvent restreindre les utilisateurs internes qui veulent accéder sans restriction à l'Internet. Certains utilisateurs techniquement sophistiqués pourraient être en mesure de contourner les mesures de sécurité que vous avez mises en place. Ils pourraient, par exemple, se connecter au bureau en utilisant l'accès à distance, ouvrant ainsi une faille de sécurité. ouvrant ainsi une faille de sécurité. Ce type de trafic peut très bien traverser le pare-feu sans être contrôlé et présente un risque de sécurité évident, car les réseaux domestiques sont rarement aussi bien défendus que les réseaux d'entreprise, et les attaquants peuvent être en mesure d'attaquer d'abord le réseau domestique d'un utilisateur et ainsi d'accéder au réseau d'entreprise, plus précieux.

III.2.4 Assurer l'authentification

L'authentification consiste à se connecter à un serveur avec un nom d'utilisateur et un mot de passe avant d'être autorisé à accéder à des informations protégées. Seuls les utilisateurs qui ont enregistré leur nom d'utilisateur et leur mot de passe sont reconnus par le serveur et autorisés à entrer. Le processus d'authentification peut également être effectué au niveau du pare-feu et faire appel au cryptage pour protéger les noms d'utilisateur et les mots de passe transmis du client au serveur (ou du client au pare-feu).

III.2.5 Contribuer aux réseaux privés virtuels

Un pare-feu est un point d'extrémité idéal pour un VPN (Virtual Private Network), qui relie les réseaux de deux entreprises par l'internet. Un VPN est l'un des moyens les plus sûrs d'échanger des informations en ligne. Pour en savoir plus sur les VPN, consultez la suite de le chapitre V.

III.3 Composants du pare-feu

Un pare-feu peut contenir de nombreux composants, notamment un filtre de paquets, un serveur proxy, un système d'authentification et un logiciel qui effectue la traduction d'adresses de réseau NAT (Network Address Translation) ou de port PAT (Port Address Translation). Certains pare-feu peuvent crypter le trafic et d'autres aident à établir des VPN. Certains pare-feu sont regroupés dans un dispositif matériel qui fonctionne également comme un routeur. Les pare-feu proprement dits font souvent partie de configurations de sécurité à composants multiples. Les systèmes de protection les plus efficaces utilisés par les grands réseaux d'entreprise n'emploient pas un seul mais plusieurs pare-feu. Ils combinent les pare-feu avec des routeurs et d'autres composants pour délimiter des zones de confiance telles qu'un sous-réseau blindé, également appelé zone démilitarisée (DMZ), positionné entre le réseau interne et le monde extérieur.

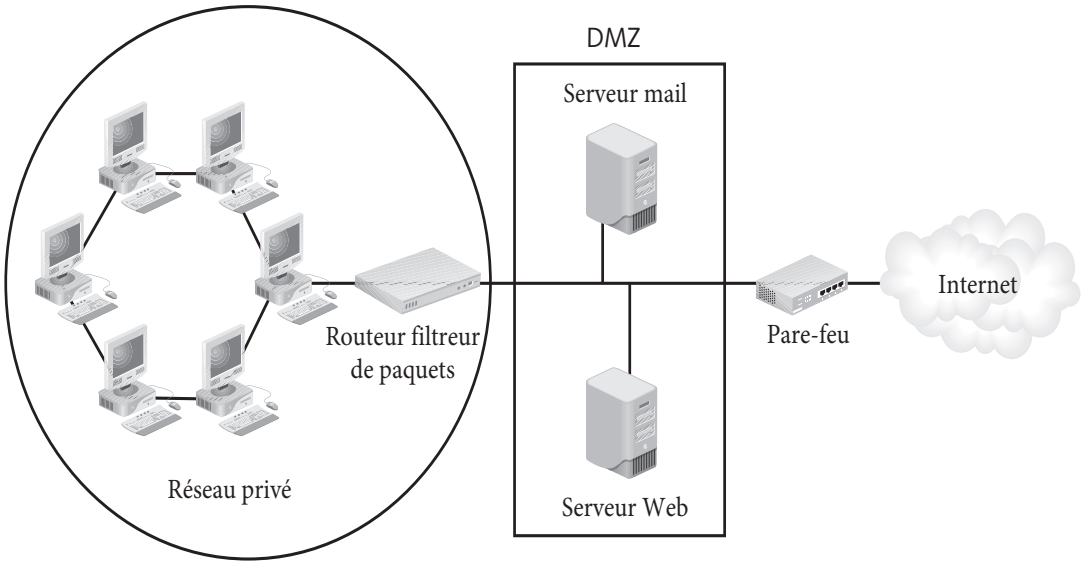


FIGURE III.3 – Réseaux DMZ.

De nombreux pare-feu utilisent des hôtes bastion, c'est-à-dire des machines qui ne possèdent pas de services inutiles, mais seulement les éléments essentiels. Un réseau qui doit se connecter à Internet peut avoir un hôte bastion et un réseau de service (autre terme pour sous-réseau blindé). Ensemble, ils constituent la seule partie de l'organisation exposée à Internet. La figure III.3 illustre une telle configuration.

III.4 Outils dans les pare-feux

Les pare-feu fonctionnent de différentes manières, et certains d'entre eux utilisent plusieurs approches, ce qui explique en partie leur efficacité. L'une des façons d'aborder le fonctionnement des pare-feu est d'utiliser le modèle d'interconnexion des systèmes ouverts (OSI) à sept couches. La figure III.4 donne quelques exemples de fonctions de pare-feu et les couches correspondantes du modèle OSI sur lesquelles elles fonctionnent.

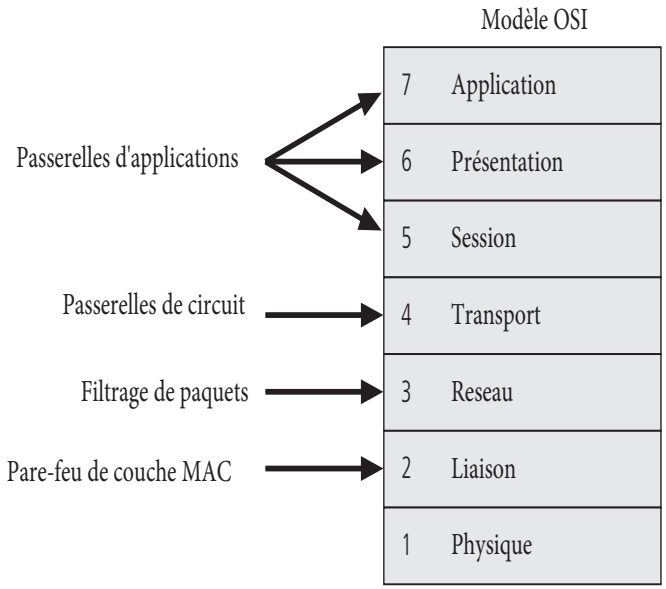


FIGURE III.4 – Pare-feu dans le modèle OSI.

Selon la couche du réseau sur laquelle un pare-feu fonctionne, les pare-feu peuvent être classés en deux catégories :

— **Les pare-feu de la couche réseau :** Les pare-feu de la couche réseau sont soit construits sur un routeur, soit placés immédiatement après le routeur.

— **Les pare-feu de la couche application** : Les pare-feu de la couche application sont basés sur un code programmé qui sert à réguler l'interaction des utilisateurs d'un réseau interne avec Internet. Les sous-sections suivantes présentent ces pare-feu en détail.

III.4.1 Pare-feu de la couche réseau

Les pare-feu de la couche réseau sont installés sur les routeurs, qui assurent une connectivité permanente entre un réseau interne et l'Internet. Lorsqu'un pare-feu est installé sur un routeur, l'administrateur réseau peut configurer les règles de contrôle d'accès sur le routeur afin de contrôler l'accès aux informations via le pare-feu. Dans ce scénario, les pare-feu de la couche réseau contrôlent le trafic Internet à l'aide de listes de contrôle d'accès configurées sur les routeurs. Ces pare-feu filtrent le trafic sur la base de l'adresse source, de l'adresse de destination, du type de protocole et du numéro de port du client qui a fait la demande. Les paquets de données qui correspondent aux règles de contrôle d'accès autorisées sont autorisés à traverser le réseau. Le pare-feu rejette les paquets qui ne sont pas conformes à ces règles ou renvoie un message ICMP (Internet Control Message Protocol) à l'expéditeur du message.

Les modèles de pare-feu simples examinent deux composants de l'en-tête du paquet : l'adresse de destination et l'adresse source. Ils appliquent des règles de restrictions d'adresses, c'est-à-dire des règles conçues pour empêcher les paquets ayant des adresses spécifiques ou incomplètes de passer à travers le dispositif. Ces restrictions sont définies dans des listes de contrôle d'accès (ACL), qui sont créées et modifiées par les administrateurs du pare-feu. par les administrateurs du pare-feu. La figure III.5 montre comment un routeur de filtrage de paquets peut être utilisé comme un simple pare-feu pour filtrer pour filtrer les paquets de données des connexions entrantes et permettre aux connexions sortantes d'accéder librement au réseau public.

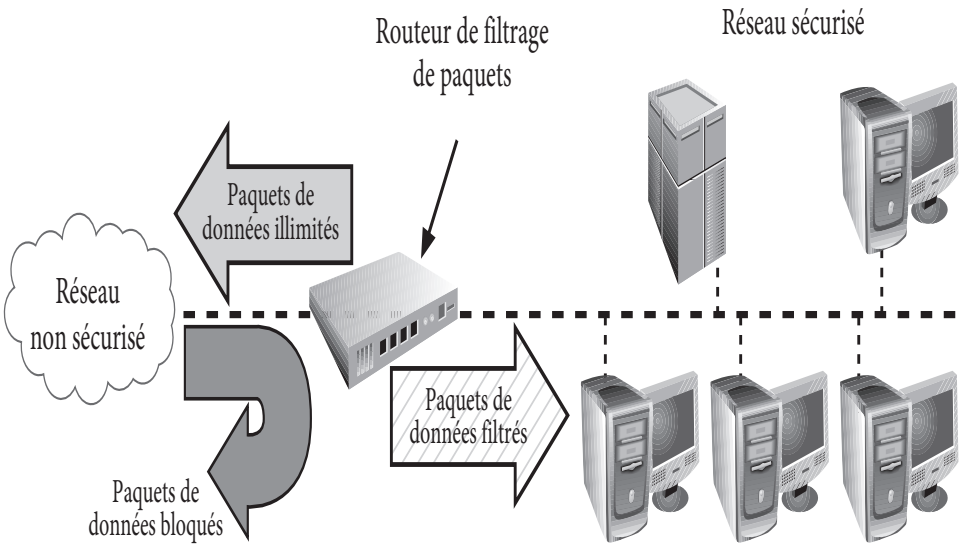


FIGURE III.5 – Routeur de filtrage de paquets.

Un avantage important des pare-feu de la couche réseau réside dans le fait que la vitesse de traitement des paquets de données est importante, car il y a très peu de journalisation ou d'analyse des paquets de données. Ces pare-feu sont également capables de prendre en charge une plus grande base d'utilisateurs que les pare-feu de la couche application, sur lesquels se porte la sous-section suivante.

D'autre part, le log généré par le pare-feu étant limité, les administrateurs réseau ne sont pas en mesure d'effectuer une analyse détaillée de l'activité sur le réseau. Un autre inconvénient des pare-feu de la couche réseau est que, étant donné qu'ils sont déployés au niveau de la couche réseau, ils sont incapables de comprendre les protocoles au niveau des applications et sont donc moins efficaces pour empêcher les données indésirables de pénétrer dans un réseau privé. Comme on le verra dans la prochaine sous-section, un pare-feu de la couche application résout certains des problèmes associés aux pare-feu de la couche réseau.

R ICMP est un protocole de rapport d'erreur utilisé par une passerelle pour informer le serveur qu'une erreur s'est produite lors du traitement du message.

III.4.2 Pare-feu de la couche d'application

Un autre type de protection par pare-feu est la passerelle de couche d'application (applicatif), également connue sous le nom de serveur proxy. ou serveur proxy. La passerelle de la couche application fonctionne au niveau de la couche Application, la couche supérieure du modèle OSI. Les passerelles de la couche application peuvent contrôler la façon dont les applications à l'intérieur du réseau accèdent aux réseaux externes en mettant en place des services proxy. Ce service se substitue au client (c'est-à-dire qu'il agit en tant que proxy), en effectuant des demandes de pages Web ou en envoyant et en recevant des courriers électroniques pour le compte d'utilisateurs individuels, qui sont ainsi protégés d'une connexion directe à Internet. Cette protection minimise l'effet des virus, des vers, des chevaux de Troie et autres logiciels malveillants.

Le pare-feu de la couche application exécute un logiciel spécial qui lui permet d'agir en tant que proxy pour une demande de service spécifique. À titre d'exemple, une entreprise qui exploite un serveur Web peut éviter d'exposer le serveur au trafic direct des utilisateurs en installant un tel serveur proxy, configuré avec l'URL du domaine enregistré. Ce serveur proxy reçoit les demandes de pages Web, accède au serveur Web au nom du client externe et renvoie les pages demandées aux utilisateurs. Ces serveurs peuvent stocker les pages les plus récemment

consultées dans leurs caches internes et sont donc également appelés serveurs de cache. Les avantages de ce type de mise en œuvre sont importants. Tout d'abord, le serveur proxy est placé dans une zone non sécurisée du réseau ou dans la zone démilitarisée (DMZ) - une zone intermédiaire entre un réseau fiable et un réseau non fiable - de sorte que c'est lui, et non le serveur Web, qui est exposé aux niveaux de risque plus élevés des réseaux moins fiables. Des routeurs de filtrage supplémentaires peuvent être mis en place derrière le serveur proxy, limitant l'accès au système interne le plus sûr et protégeant ainsi davantage les systèmes internes. Un pare-feu de couche d'application est généralement déployé sur un serveur dédié qui dispose d'un accès Internet. Tous les autres ordinateurs accèdent à Internet par le biais du serveur dédié. La figure III.6 illustre une mise en œuvre des pare-feu de la couche application.

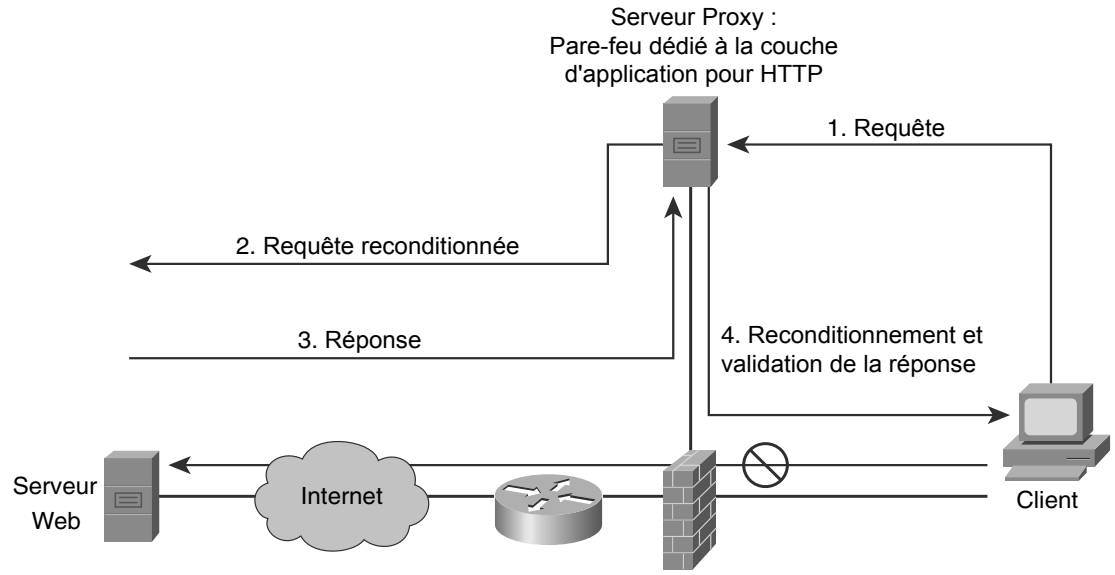


FIGURE III.6 – Processus de communication du serveur proxy.

Example III.1 Parmi les exemples les plus courants d'implémentation d'un serveur proxy, on trouve un pare-feu qui bloque toutes les demandes et les réponses aux demandes de pages et de services Web provenant des ordinateurs internes de son entreprise et qui fait en sorte que toutes ces demandes et réponses soient transmises à des ordinateurs intermédiaires (ou proxies) situés dans les zones moins protégées du réseau de l'entreprise. Cette technique est encore largement utilisée pour mettre en œuvre des fonctions de commerce électronique, bien que la plupart des utilisateurs de cette technologie aient évolué pour tirer parti de l'approche DMZ abordée plus loin. ∎

La principale faiblesse des pare-feu applicatifs est qu'ils sont conçus pour un protocole spécifique et ne peuvent pas être facilement reconfigurés pour se protéger des attaques sur d'autres protocoles. Étant donné que les pare-feu d'application travaillent au niveau de la couche application (d'où leur nom), ils sont généralement limités à une seule application (par exemple, FTP, Telnet, HTTP, SMTP, SNMP). Le temps et les ressources nécessaires pour lire chaque paquet jusqu'à la couche applicative diminuent la capacité de ces pare-feu à gérer plusieurs types d'applications.

Un pare-feu de couche applicative vous offre toutefois un avantage particulièrement précieux en matière de sécurité. Contrairement à un filtre de paquets, qui décide d'autoriser ou de refuser une demande sur la base des informations contenues dans l'en-tête du paquet, le pare-feu comprend le contenu des données demandées. Elle peut être configurée pour autoriser ou refuser (les deux actions peuvent être entreprises à la suite du filtrage) un contenu spécifique, tel que des virus et des exécutables.

Le filtrage du contenu n'est que l'une des tâches complexes que les pare-feu de la couche application peuvent accomplir, ce qui leur permet d'aller bien au-delà du simple blocage d'adresses IP spécifiques. Voici quelques-unes des autres tâches qu'elles peuvent accomplir :

— *Équilibrage du trafic* - Lorsqu'un réseau possède plus d'une adresse d'entrée, le nombre de connexions attribuées à chacune d'elles peut être géré pour assurer une répartition uniforme du trafic. Les grandes entreprises installent généralement plusieurs pare-feu et répartissent le trafic entre eux.

— *Mappage d'adresses IP* - Il s'agit d'un certain type de NAT ou de PAT dans lequel une adresse IP statique attribuée par un FAI est mappée à l'adresse IP privée d'un ordinateur sur le réseau local ; il est parfois appelé vectorisation d'adresses ou mappage d'adresses IP statiques. L'avantage de cette méthode pour un réseau interne est de protéger les adresses IP internes réelles contre les regards indiscrets de clients externes non autorisés.

— *Filtrage du contenu* - Un serveur proxy d'application peut être configuré pour filtrer sur certains critères détaillés. Il est possible de bloquer les fichiers qui ont un certain nom de fichier ou une partie de ce nom, un mot clé, une pièce jointe à un courriel ou un type de contenu.

— *Filtrage des URL* - Il est également possible de bloquer le nom du système de nom de domaine (DNS) d'un site, tel que www.univ-chlef.dz.

III.4.3 Hôte à double réseau

Un par-feu d'hôte à double réseau est établie autour d'un ordinateur à double réseau, qui a au moins deux interfaces. Un tel hôte pourrait agir comme un routeur entre les réseaux auxquels sont attachées les interfaces ; il est capable d'acheminer les paquets d'IP d'un réseau à l'autre. Cependant, il faut désactiver cette fonction de routage pour implémenter une architecture de type hôte à double réseau. Ainsi, des paquets d'IP d'un réseau (comme l'Internet) ne sont pas directement conduits à l'autre réseau (par exemple le réseau interne protégé). Les systèmes à l'intérieur du firewall peuvent communiquer avec l'hôte à double réseau, ainsi que les systèmes en dehors du firewall c'est à dire ce qui est situé sur l'internet, mais ces systèmes ne peuvent pas communiquer directement avec l'un à l'autre. Le trafic d'IP entre eux est complètement bloqué. La figure III.7 permet de représenter l'architecture de l'hôte à double réseau

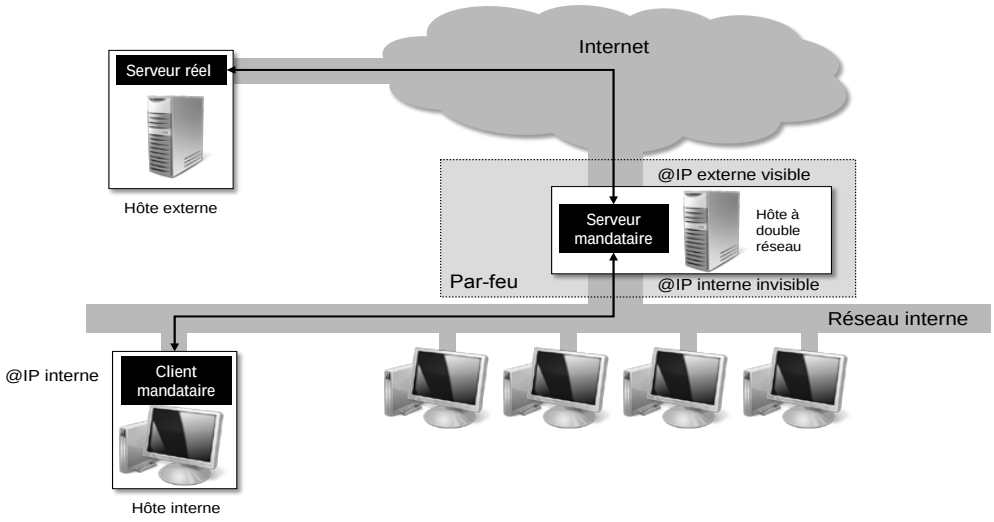


FIGURE III.7 – Par-feu d'hôte à double réseau.

Les hôtes à double réseau peuvent fournir un niveau très élevé de contrôle. Si on ne permet à aucun paquet d'aller directement entre les réseaux externes et internes, on est sûr que tout paquet du réseau interne qui provient d'une source extérieure prouve l'existence d'erreur. Dans certains cas, l'hôte à double réseau permettra de rejeter cette connexion qui prétend être pour un service particulier, mais qui ne contient pas réellement le bon genre de données. Cependant, il faut un travail considérable pour bénéficier des avantages potentiels des hôtes à double réseau. les hôtes à double réseau ne peuvent fournir des services que par mandatement (proxying), ou en laissant les utilisateurs se connecter directement sur l'hôte. Le mandatement est moins problématique

mais peut ne pas être disponible pour tous les services qui vous intéressent. L'architecture de sous-réseau à écran qu'on va décrire au dessous offre quelques options supplémentaires pour fournir des services nouveau.

III.4.4 Par-feu avec bastion

Toutes les connexions en provenance de l'Internet passent forcément par le bastion qui se trouve sur le réseau interne. Les clients du réseau interne peuvent accéder directement à l'Internet pour les services non mandatés par le bastion, sinon ils passent obligatoirement par les proxies du bastion. Considérant qu'un par-feu d'hôte à double écran fournit des services depuis un hôte qui est attaché aux réseaux multiples, mais dont le routage est désactivé, un par-feu d'hôte à écran fournit des services depuis un hôte qui est attaché seulement au réseau interne, à l'aide d'un routeur séparé. Dans cette architecture, la sécurité primaire est fournie par le filtrage de paquet. (Par exemple, le filtrage de paquet est ce qui empêche les gens de contourner les serveurs mandataires pour établir des connexions directes). La figure III.8 montre une version simplifiée d' un par-feu avec bastion.

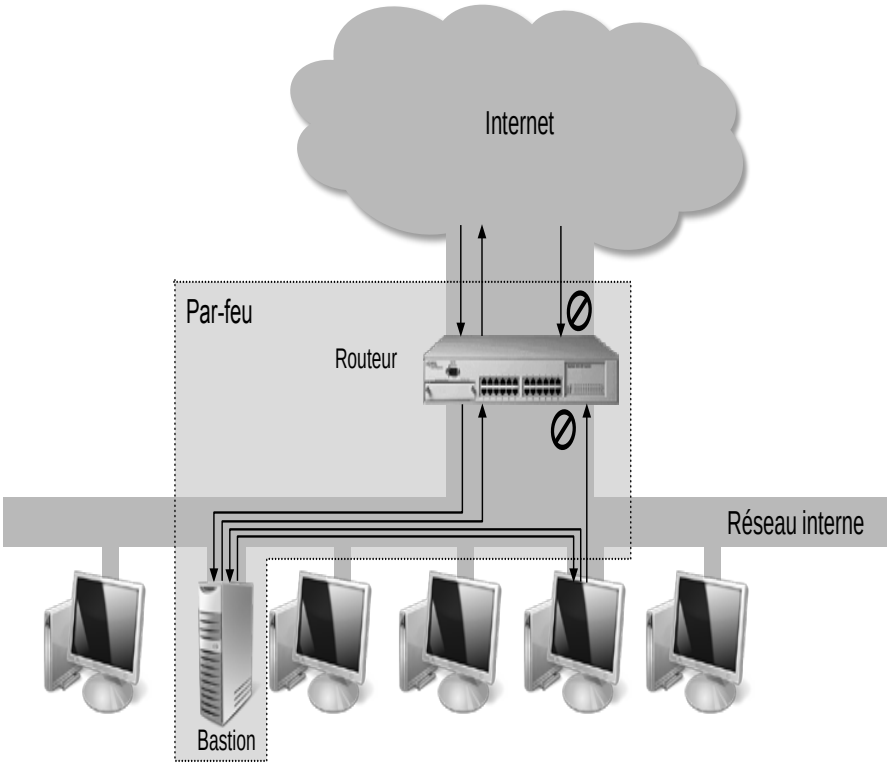


FIGURE III.8 – Par-feu avec bastion.

Le par-feu avec bastion peut servir comme un Serveur pour un ensemble de services prédéfinis :

— Service toile (HTTP), service de noms (DNS), service de messagerie ....
— Le bastion peut agir en rendant directement le service concerné.
— Le bastion peut agir en relayant les requêtes vers d'autres serveurs après avoir effectué un contôle d'accès applicatif (proxy-serveur).
— Le bastion doit être incontournable pour l'ensemble des services prévus.

En outre, le bastion peut également être exploité pour la détection des intrusions :

— Analyse des communications pour détecter des attaques : IDS ('Intrusion Detection System').
— Fonction pot de miel (Honeypot) : un service semblant attractif pour un attaquant et qui n'est en réalité qu'un piège pour détecter l'attaquant.

III.4.5 Par-feu à zone démilitarisée

On utilise un sous-réseau à part pour isoler les bastions : c'est la zone démilitarisée (DMZ). Il est possible de fusionner routeur interne et externe. Même si le bastion est percé, l'intrus est isolé dans la DMZ et ne peut pas accéder au réseau interne facilement (il n'est pas possible d'usurper une machine du réseau interne par exemple). La DMZ fait ainsi office de « zone tampon » entre le réseau à protéger et le réseau hostile. La figure III.9 montre la position d'une DMZ au sein d'un réseau. Les serveurs situés dans la DMZ sont appelés « bastions » en raison de leur position d'avant poste dans le réseau de l'entreprise.

La politique de sécurité mise en œuvre sur la DMZ est généralement la suivante :

— Trafic du réseau externe vers la DMZ autorisé.
— Trafic du réseau externe vers le réseau interne interdit
— Trafic du réseau interne vers la DMZ autorisé.
— Trafic du réseau interne vers le réseau externe autorisé.
— Trafic de la DMZ vers le réseau interne interdit.
— Trafic de la DMZ vers le réseau externe interdit.

R La DMZ possède donc un niveau de sécurité intermédiaire, mais son niveau de sécurité n'est pas suffisant pour y stocker des données critiques dans l'entreprise. Il est à noter qu'il est possible de mettre en place des DMZ en interne afin de cloisonner le réseau interne selon différents niveaux de protection et ainsi éviter les intrusions venant de l'intérieur.

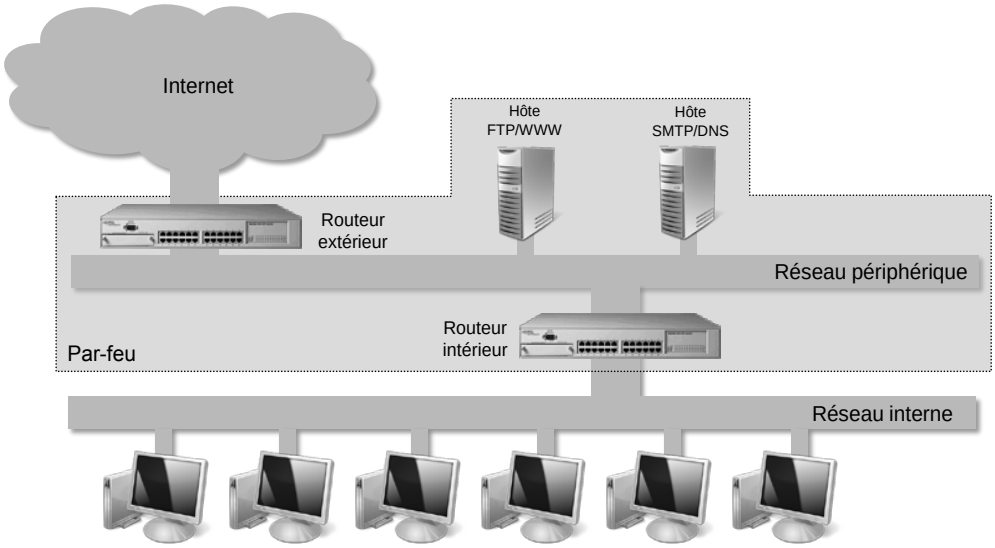


FIGURE III.9 – Par-feu à zone démilitarisée.

VLAN VIRTUAL LOCAL AREA NETWORK

IV. La sécurité de la commutation

De nombreuses entreprises mettent en œuvre une politique de sécurité complète couvrant plusieurs des couches OSI, de la couche application à la sécurité IP. Le modèle OSI a été conçu pour permettre aux différentes couches de travailler sans se connaître. Malheureusement, si une couche est attaquée, les communications sont compromises sans que les autres couches ne soient conscientes du problème. La sécurité est aussi forte que le maillon le plus faible. En ce qui concerne les réseaux, la couche 2 peut être un maillon très faible. Ce chapitre se concentre sur les questions de sécurité entourant la couche 2, sa compréhension et sa prévention. Étant donné qu'un pourcentage important des attaques de réseau provient de l'intérieur du pare-feu de l'entreprise, il est essentiel d'explorer ce ventre mou du réseau de données pour toute conception de réseau sécurisée. Les problèmes de sécurité abordés dans ce chapitre comprennent l'ARP spoofing, Saturation de la table d'apprentissage (MAC flooding), le saut de VLAN, les attaques DHCP et les problèmes liés au protocole Spanning Tree. Les attaques par déni de service (DoS) sont également une préoccupation majeure car elles peuvent provenir de sources internes et externes. Le point central est de comprendre comment les attaques fonctionnent et quelles techniques peuvent être utilisées pour atténuer ce type d'attaques du point de vue de la sécurité.

IV.1 Notions sur les VLANs

Ethernet a été longtemps synonyme de réseau local. Cette limitation géographique s'explique par la technique d'accès. Pour s'assurer que la collision a été bien perçue par la station d'émission avant qu'elle se déconnecte, la norme Ethernet exige que 64 octets au minimum soient émis, ce qui limite le temps aller-retour sur le support physique au temps de transmission de ces 512 bits. À partir du moment où l'on passe en commutation, la distance maximale n'a plus de sens. On utilise parfois le terme de WLAN (Wide LAN) pour indiquer que la distance maximale se trouve désormais dans le champ des réseaux étendus. Ethernet a dû évoluer pour atteindre les possibilités offertes par ses concurrents. La norme d'adressage a été modifiée, par exemple, passant de plat et absolu à hiérarchique. Cette révolution est aujourd'hui consacrée par la norme *IEEE 802.1q*, qui permet d'étendre la zone d'adressage grâce à un niveau hiérarchique supplémentaire. On appelle cette nouvelle solution de structuration du réseau un VLAN (Virtual LAN).

Definition IV.1.1 VLAN (Virtual LAN).– Réseau logique dans lequel sont regroupés des clients qui ont des intérêts communs. La définition d'un VLAN a pendant longtemps été un domaine de diffusion : la trame émise par l'un des membres est automatiquement diffusée vers l'ensemble des autres membres du VLAN.

Les réseaux locaux virtuels ont pour rôle initial de permettre une configuration et une administration plus faciles des grands réseaux d'entreprise construits autour de nombreux ponts. Il existe plusieurs stratégies d'application pour ces réseaux virtuels. Le VLAN introduit une notion de segmentation des grands réseaux, les utilisateurs étant regroupés suivant des critères à déterminer. Un logiciel d'administration doit être disponible pour la gestion des adresses et des commutateurs. Le VLAN peut être défini comme un domaine de broadcast, dans lequel l'adresse de diffusion atteint toutes les stations appartenant au VLAN. Les communications à l'intérieur du VLAN peuvent être sécurisées, et celles entre deux VLAN distincts contrôlées. Plusieurs types de VLAN ont été définis suivant les regroupements des stations du système :

IV.1.1 VLAN de niveau physique

Les VLAN de niveau physique, ou de niveau 1, regroupent les stations appartenant aux mêmes réseaux physiques ou à plusieurs réseaux physiques mais reliés par une gestion commune des adresses. Une machine est rattachée à un port au travers de sa carte Ethernet. Un port est donc affecté à un VLAN unique. Cette solution très statique garantit une bonne étanchéité entre

VLAN pour peu que les commutateurs soient dotés d'une programmation ne permettant pas aux trames Ethernet d'être acceptées ou nom en fonction de l'adresse VLAN. Elle manque cependant de souplesse puisqu'un utilisateur ne peut s'adresser qu'aux utilisateurs du même VLAN .

La figure IV.1 illustre le fonctionnement d'un VLAN de niveau physique. On voit que les machines sont rattachées entre elles par le biais des ports des deux commutateurs. La mobilité d'une machine devient assez complexe puisqu'il faut associer le nouveau port au VLAN de la machine. De plus, si plusieurs utilisateurs se servent d'une même machine mais n'utilisent pas le même VLAN , la gestion devient particulièrement complexe puisqu'il faut reprogrammer le lien entre numéro de port et VLAN.

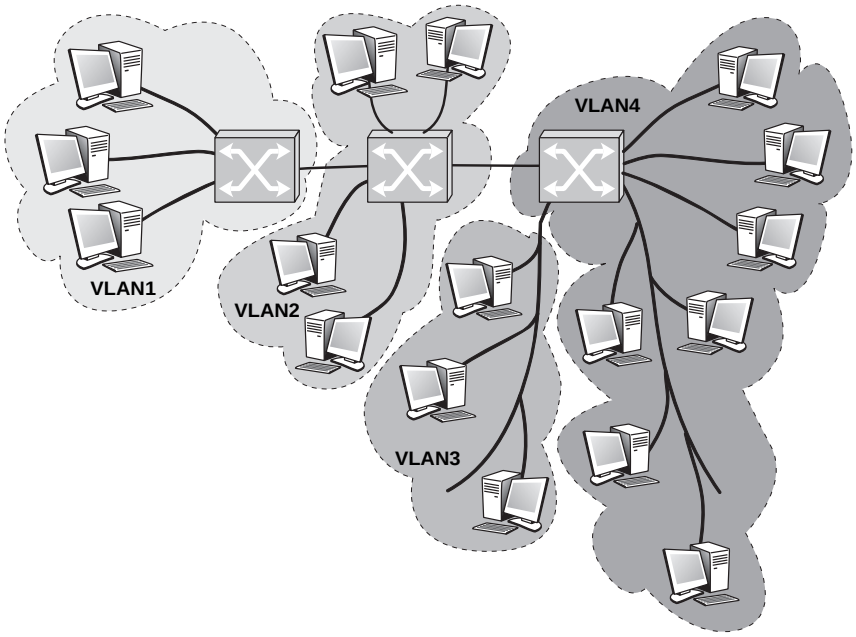


FIGURE IV.1 – VLAN de niveau physique.

IV.1.2 VLAN de niveau trame

Pour réaliser des VLAN de niveau trame(liaison), ou plus exactement de niveau MAC (Media Access Control) , ou encore de niveau 2, ont des adresses MAC qui regroupent les stations appartenant au même VLAN . En fonction de la table de commutation, qui associe des adresses MAC, pouvant être vues comme des références, à des ports de sortie, les trames sont acheminées vers les machines appartenant au VLAN. Les tables de commutation deviennent un peu plus complexes, puisque, associées à un même numéro de VLAN , il peut y avoir plusieurs adresses MAC et donc une émission de la trame sur plusieurs ports de sortie du commutateur.

De nouveau, on peut accepter ou interdire par programmation qu'une machine associée à un VLAN puisse émettre hors de son VLAN . Un des avantages des VLAN de niveau trame est la plus grande souplesse qu'ils offrent pour gérer la mobilité des terminaux associés à des VLAN . Il suffit de reprogrammer les commutateurs pour modifier les tables de commutation. Cette reprogrammation peut s'effectuer automatiquement par apprentissage. Un exemple de VLAN de niveau trame est illustré à la figure IV.2.

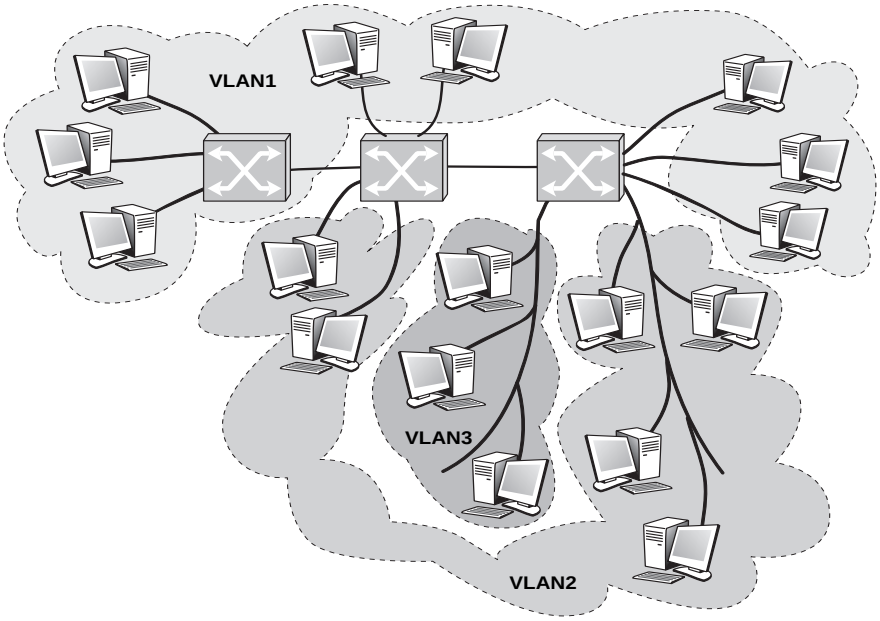


FIGURE IV.2 – VLAN de niveau trame.

IV.1.3 VLAN de niveau paquet

Les VLAN de niveau paquet, ou VLAN de niveau 3, correspondent à des regroupements de stations suivant leur adresse de niveau 3. Cette adresse de niveau 3 peut être une adresse IP ou une sous-adresse de l'adresse IP, que l'on appelle masque de sous-réseau IP. Il faut, dans ce cas, faire correspondre l'adresse de niveau paquet et celle de niveau trame. Les protocoles de type ARP (Address Resolution Protocol) effectuent cette correspondance d'adresse. Deux réseaux VLAN sont illustrés à la figure 36 ; la difficulté vient de la diffusion vers les seuls utilisateurs $1, 2$ et 5 lorsqu'un membre du VLAN 1 émet et, de même, de la diffusion vers les seuls utilisateurs $3, 4, 6$ et 7 lorsqu'un membre du VLAN 2 émet.

Lorsqu'un établissement de grande taille veut structurer son réseau, il peut créer des réseaux virtuels suivant des critères qui lui sont propres. Généralement, un critère géographique est retenu pour réaliser une communication simple entre les différents sites de l'établissement. L'adresse

du VLAN est alors ajoutée dans la structure de la trame Ethernet ou de la trame d'une autre technologie, puisque la structuration en VLAN ne concerne pas uniquement les environnements Ethernet.

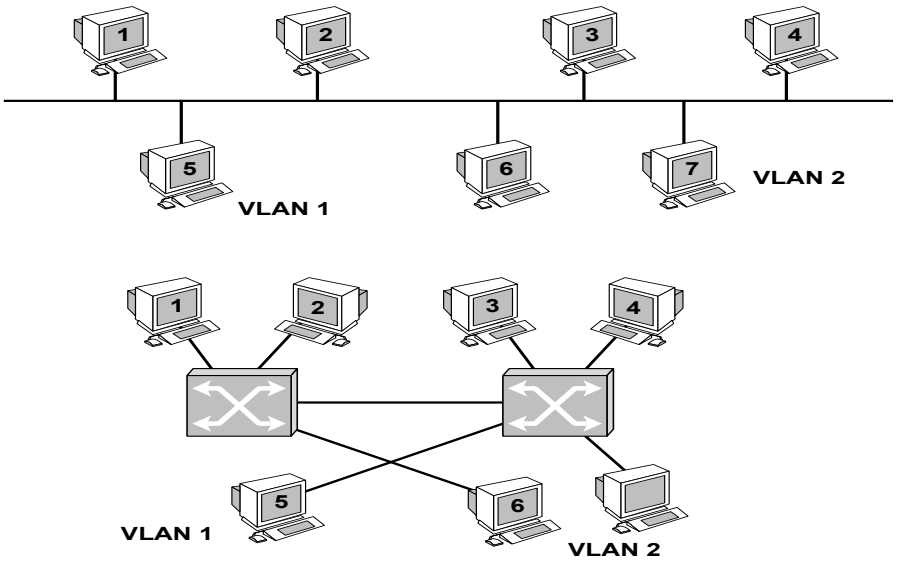


FIGURE IV.3 – Deux topologies de VLAN.

IV.2 Identification des VLAN (802.1Q)

IV.2.1 Principe

Lorsqu'un réseau comporte plusieurs commutateurs, chaque commutateur doit pouvoir localiser toutes les machines (*table d'acheminement*) et connaître le VLAN d'appartenance de la source et du destinataire (*filtrage de trafic*). Lorsque le réseau est important, les tables peuvent devenir très grandes et pénaliser les performances. Il est plus efficace d'étiqueter les trames. L'étiquette identifie le VLAN de la station source, le commutateur n'a plus alors qu'à connaître les VLAN d'appartenance des stations qui lui sont raccordées. Ainsi, on distingue deux types d'équipement, ceux qui savent gérer l'étiquetage et qui ont donc connaissance des VLAN (les VLAN *aware*) et ceux qui ignorent cette appartenance (VLAN *unaware*). Dans le réseau de la figure IV.4 cohabitent des équipements awares et unawares. Les trames émises par les équipements awares sont marquées (*tagged*), celles émises par les équipements unawares ne sont pas marquées (*untagged*). La mixité des équipements nécessite que soit défini un VLAN par défaut : le VLAN auquel sont rattachés les équipements unawares (VLAN **C** de la figure IV.4). Lorsqu'un équipement aware reçoit une trame marquée à destination d'un équipement unaware, il en extrait le tag.

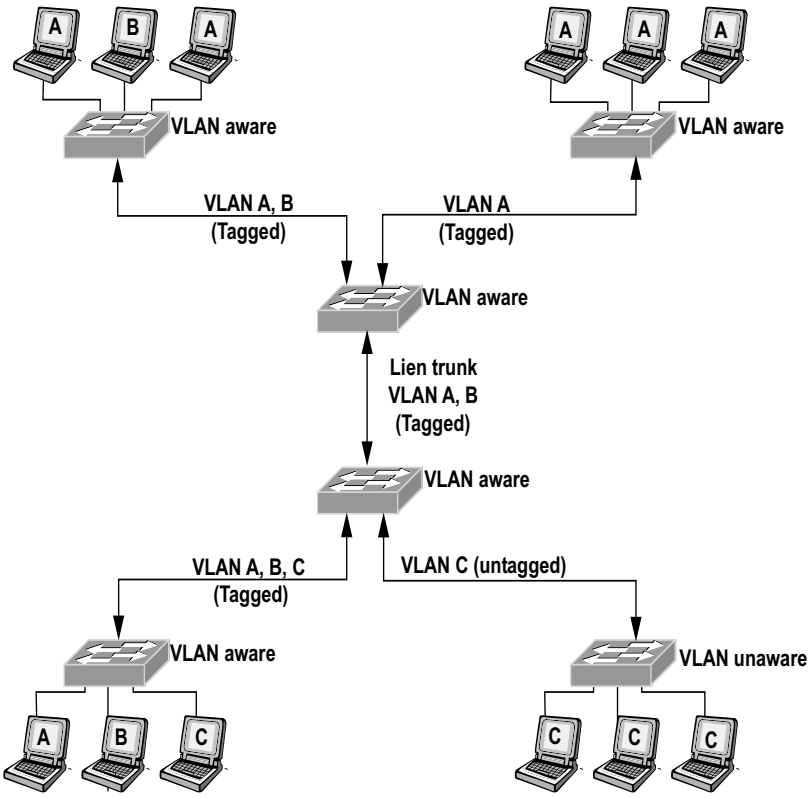


FIGURE IV.4 – Principe de l'étiquetage des trames dans les VLAN.

IV.2.2 La norme IEEE 802.1p/Q

Un VLAN correspond à un domaine de broadcast. Cependant, lorsque plusieurs VLAN sont définis sur un même segment cette définition est mise en défaut. Il est évidemment possible d'imaginer que le commutateur transforme le broadcast en une rafale d'unicasts. La solution adoptée par l'IEEE est toute différente : un seul VLAN peut être déclaré par port, les VLAN sont définis dans les normes 802.1Q et 802.1p (802.1p/Q[1]) qui introduisent quatre octets supplémentaires dans la trame MAC afin d'identifier les VLAN (VLAN tagging) et de gérer 8 niveaux de priorité (Qualité of Service, QoS). La figure IV.5 illustre l'étiquetage d'une trame MAC des réseaux de type 802.3.

La trame 802.1p/Q augmente la taille de la trame 802.3. La taille maximale passe de 1518 à 1522 octets. Ce format limite l'usage de la trame en interne au commutateur et au dialogue intercommutateur (cf. figure IV.6). Pour garantir la compatibilité avec l'existant, le marquage des trames est vu comme une encapsulation supplémentaire. Ainsi, le champ VPID (VLAN Protocol ID) est similaire au champ Ethertype de la trame 802.3, il identifie le format 802.1p/Q,

1. 802.1Q concerne les VLAN, 802.1p concerne la qualité de service.

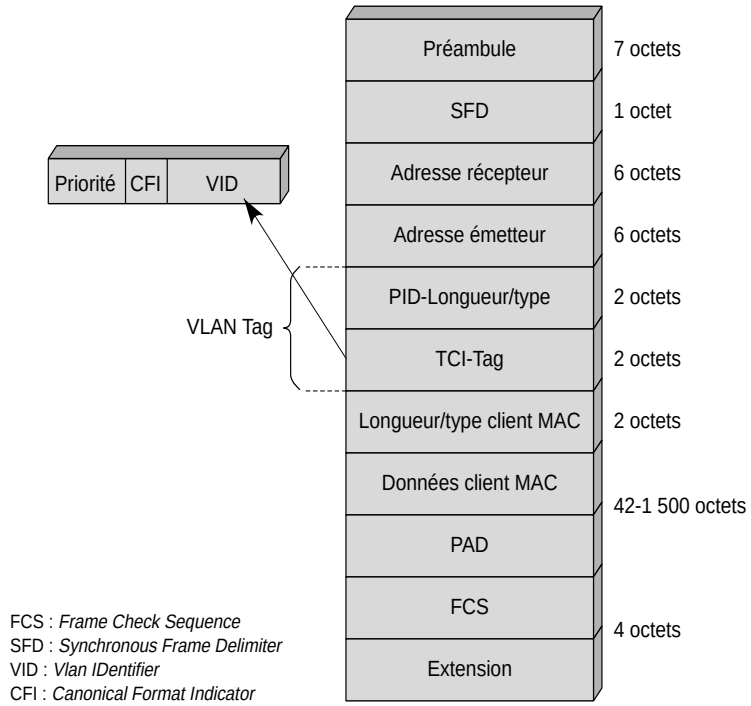


FIGURE IV.5 – Le format de la trame Ethernet VLAN.

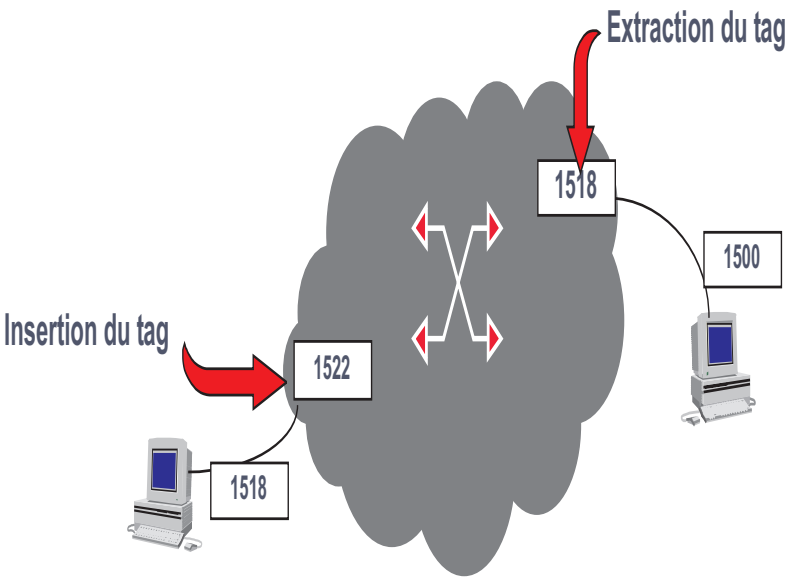


FIGURE IV.6 – Identification des VLAN interne au réseau.

sa valeur est fixée à 0×8100. Les deux octets suivants permettent de définir huit niveaux de priorité (User Priority). Les commutateurs de dernière génération disposent de plusieurs files d'attente les trames sont affectées à telle ou telle file suivant leur niveau de priorité. Le bit CFI (Canonical Format Identifier) est, en principe, inutilisé dans les réseaux 802.3, il doit être mis à 0.

Dans les réseaux Token Ring, à 1, il indique que les données du champ routage par la source sont au format non canonique. Le champ VID (VLAN IDentifier) identifie sur douze bits le VLAN destination. L'introduction de quatre octets supplémentaires implique que les commutateurs d'entrée et de sortie recalculent le FCS. On commence à trouver des cartes transporteurs capables de supporter le tagging.

IV.3 Avantages des VLAN

La productivité des utilisateurs et l'adaptabilité du réseau sont importants pour la croissance et la réussite de l'entreprise. Les VLAN permettent d'adapter un réseau selon les objectifs de l'entreprise. Les principaux avantages des VLAN sont les suivants :

- **Sécurité** : les groupes contenant des données sensibles sont séparés du reste du réseau, ce qui diminue les risques de violation de confidentialité. Comme l'illustre la figure, les ordinateurs du personnel enseignant se trouvent sur le VLAN 10 et sont complètement séparés du trafic des données des étudiants et des invités.
- **Réduction des coûts** : des économies sont réalisées grâce à une diminution des mises à niveau onéreuses du réseau et à l'utilisation plus efficace de la bande passante et des liaisons montantes existantes.
- **Meilleures performances** : le fait de diviser des réseaux linéaires de couche 2 en plusieurs groupes de travail logiques (domaines de diffusion) réduit la quantité de trafic inutile sur le réseau et augmente les performances.
- **Réduction des domaines de diffusion** : la division d'un réseau en VLAN réduit le nombre de périphériques dans le domaine de diffusion. Comme l'illustre la figure IV.7, il y a six ordinateurs dans ce réseau, mais seulement trois domaines de diffusion : Personnel, Étudiant et Invité.
- **Efficacité accrue du personnel informatique** : les VLAN facilitent la gestion du réseau, car les utilisateurs ayant des besoins réseau similaires partagent le même VLAN. Lorsque vous configurez un nouveau commutateur, toutes les stratégies et procédures déjà configurées pour le VLAN correspondant sont implémentées lorsque les ports sont affectés. Le personnel informatique peut aussi identifier facilement la fonction d'un VLAN en lui donnant un nom approprié. Dans la figure IV.7, pour qu'ils puissent être facilement identifiables, le VLAN 10 a été nommé « Personnel », le VLAN 20, « Étudiant » et le VLAN 30, « Invité ».

— **Gestion simplifiée de projets et d'applications** : les VLAN rassemblent des utilisateurs et des périphériques réseau pour prendre en charge des impératifs commerciaux ou géographiques. La séparation des fonctions facilite la gestion d'un projet ou l'utilisation d'une application spécialisée. Une plate-forme de développement d'e-learning pour le personnel enseignant est un exemple de ce type d'application.

Chaque VLAN d'un réseau commuté correspond à un réseau IP ; par conséquent, la conception VLAN doit tenir compte de la mise en œuvre d'un système d'adressage hiérarchique. L'adressage réseau hiérarchique signifie que les numéros de réseau IP sont appliqués aux segments réseau ou VLAN dans un ordre tenant compte de l'ensemble du réseau. Les blocs d'adresses réseau contiguës sont réservés et configurés sur les périphériques situés dans une zone spécifique du réseau.

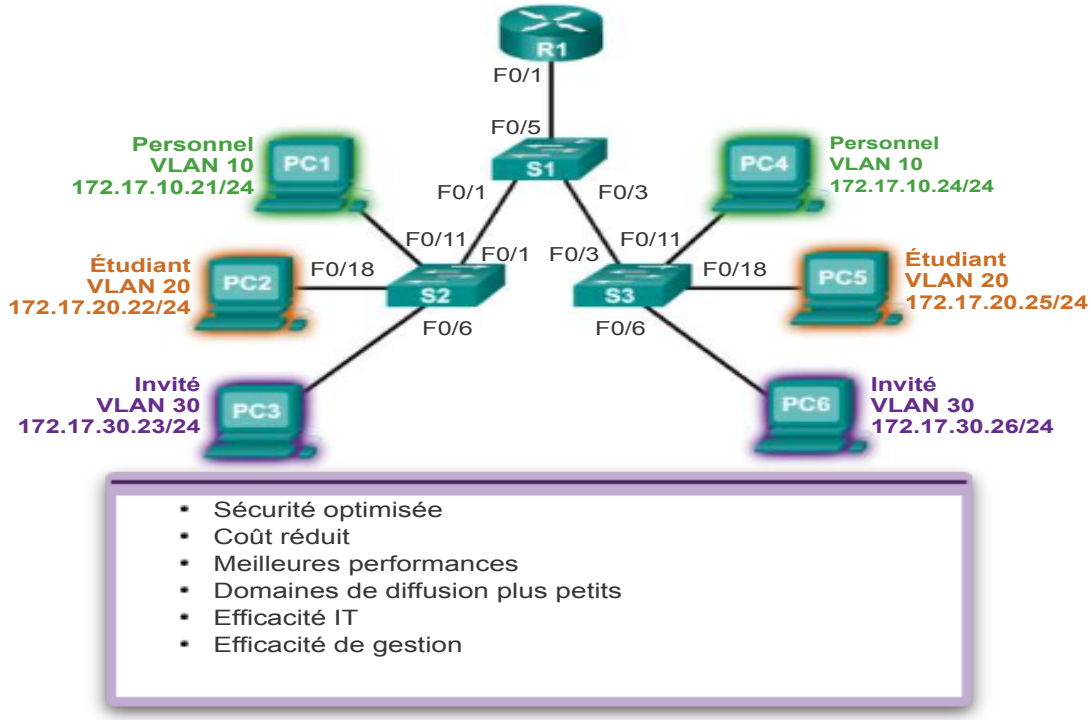


FIGURE IV.7 – Avantages des VLAN.

IV.4 Attaques au niveau de la couche liaison de données

La couche liaison de donnees dans les reseaux Ethernet est très sujette à plusieurs attaques. Les attaques les plus courantes sont -

IV.4.1 Usurpation ARP (ARP Spoofing)

Address Resolution Protocol (ARP) est un protocole utilise pour mapper une adresse IP à une adresse machine physique reconnaissable dans l'Ethernet local. Lorsqu'un ordinateur hôte doit trouver une adresse MAC (Media Access Control) physique pour une adresse IP, il diffuse une requête ARP. L'autre hôte qui possède l'adresse IP envoie un message de réponse ARP avec son adresse physique. Chaque machine hôte sur le réseau maintient une table, appelée "cache ARP". Le tableau contient l'adresse IP et les adresses MAC associées des autres hôtes du réseau.

Étant donne que l'ARP est un protocole sans état, chaque fois qu'un hôte obtient une réponse ARP d'un autre hôte, même s'il n'a pas envoyé de demande ARP, il accepte cette entrée ARP et met à jour son cache ARP. Le processus de modification du cache ARP d'un hôte cible avec une entrée falsifiée appelée empoisonnement ARP ou usurpation ARP. L'usurpation ARP peut permettre à un attaquant de se faire passer pour un hôte légitime, puis d'intercepter des trames de données sur un réseau, de modifier ou arrête-les. Souvent, l'attaque est utilisée pour lancer d'autres attaques telles que l'homme du milieu, le détournement de session ou le déni de service.

IV.4.2 Inondation MAC (MAC Flooding)

Chaque commutateur dans le Ethernet possède une table de mémoire adressable par contenu (CAM) qui stocke les adresses MAC, les numéros de port de commutation et d'autres informations. La table a une taille fixe. Dans l'attaque par inondation MAC, l'attaquant inonde le commutateur d'adresses MAC à l'aide de paquets ARP falsifies jusqu'à ce que la table CAM soit pleine. Une fois que CAM est inonde, le commutateur passe en mode concentrateur et commence à diffuser le trafic qui n'ont pas d'entrée CAM. L'attaquant qui se trouve sur le même réseau reçoit désormais toutes les trames destinées uniquement à un hôte spécifique.

IV.4.3 Vol de port

Les commutateurs Ethernet ont la capacité d'apprendre et de lier des adresses MAC aux ports. Lorsqu'un commutateur reçoit du trafic provenant d'un port avec une adresse source MAC, il lie le numéro de port et cette adresse MAC. L'attaque de vol de port exploite cette capacité des commutateurs. L'attaquant inonde le commutateur avec des trames ARP falsifiées avec l'adresse

MAC de l'hôte cible comme adresse source. Le commutateur est dupe de croire que l'hôte cible est sur le port, sur lequel un attaquant est réellement connecte. Désormais, toutes les trames de données destinées à l'hôte cible sont envoyées au port de commutateur de l'attaquant et non à l'hôte cible. . Ainsi, l'attaquant reçoit désormais toutes les trames qui étaient en fait destinées uniquement à l'hôte cible.

IV.4.4 Attaques DHCP

Le protocole de configuration d'hôte dynamique (DHCP) n'est pas un protocole de liaison de données mais des solutions pour Les attaques DHCP sont également utiles pour contrecarrer les attaques de couche 2. DHCP est utilise pour allouer dynamiquement des adresses IP aux ordinateurs pour une période de temps spécifique. Il est possible d'attaquer les serveurs DHCP en provoquant un déni de service sur le réseau ou en usurpant l'identité du serveur DHCP. Dans une attaque de famine DHCP, l'attaquant demande toutes les adresses DHCP disponibles. Cela entraîne un déni de service à l'hôte légitime sur le réseau.

Dans une attaque d'usurpation DHCP,l'attaquant peut déployer un serveur DHCP non autorise pour fournir des adresses aux clients. Ici, l'attaquant peut fournir aux machines hôtes une passerelle par défaut rouge avec les réponses DHCP. Les trames de données de l'hôte sont désormais guidées vers la passerelle rouge où l'attaquant peut intercepter tous les packages et répondre à la passerelle réelle ou les supprimer.

IV.4.5 Autres attaques

En plus des attaques populaires ci-dessus, il existe d'autres attaques telles que la diffusion basée sur la couche 2, le deni de service (DoS), le clonage MAC.

— Dans l'attaque de diffusion, l'attaquant envoie des réponses ARP usurpées aux hôtes du réseau. Ces réponses ARP définissent l'adresse MAC de la passerelle par défaut sur l'adresse de diffusion. Cela provoque la diffusion de tout le trafic sortant, ce qui permet de renifler l'attaquant assis sur le même Ethernet. Ce type d'attaque affecte également la capacité du réseau.

— Dans les attaques DoS basées sur la couche 2, l'attaquant met à jour les caches ARP des hôtes du réseau avec des adresses MAC inexistantes. L'ajout MAC Chaque carte d'interface réseau d'un réseau est censée être unique au monde. Cependant, il peut facilement être modifie en activant le clonage MAC. L'attaquant désactive l'hôte cible via une attaque DoS, puis utilise les adresses IP et MAC de l'hôte cible.

— L'attaquant exécute les attaques pour lancer les attaques de niveau supérieur afin de compromettre la sécurité des informations voyageant sur réseau. Il peut intercepter toutes les trames et pourrait lire les données de trame. L'attaquant peut agir en tant qu'intermédiaire et modifier les données ou simplement supprimer la trame menant à DoS. Il peut détourner la session en cours entre l'hôte cible et d'autres machines et communiquer des informations erronées.

IV.5 Réponses aux attaques (Securisation de couche liaison de données)

Nous avons discute de certaines attaques largement connues à Data Link Layer dans la precedente section. Plusieurs methodes ont ete developpees pour attenuer ces types d'attaques. Certaines des methodes importantes sont

IV.5.1 Securité des ports

Il s'agit d'une fonctionnalité de sécurité de couche 2 disponible sur les commutateurs Ethernet intelligents. Cela implique de lier un port physique d'un commutateur à une ou plusieurs adresses MAC spécifiques. Tout le monde peut accéder à un réseau non sécurisé en connectant simplement l'hôte à l'un des ports de commutateur disponibles. Mais, la sécurité des ports peut sécuriser l'accès à la couche 2.

Par défaut, la sécurité des ports limite le nombre d'adresses MAC d'entrée à un. Cependant, il est possible d'autoriser plusieurs hôtes autorises à se connecter à partir de ce port via la configuration. Les adresses MAC autorisées par interface peuvent être configurées statiquement. Une alternative pratique consiste à activer l'apprentissage d'adresse MAC "collant " où les adresses MAC seront apprises dynamiquement par le port du commutateur jusqu'à ce que la limite maximale pour le port soit atteinte. Pour assurer la sécurité, réaction au changement de la ou les adresses MAC spécifiées sur un port ou les adresses excédentaires sur un port peuvent être contrôlées de différentes manières. Le port peut être configuré pour arrêter ou bloquer les adresses MAC qui dépassent une limite spécifiée. La meilleure pratique recommandée consiste à fermer le port. La sécurité des ports empêche les inondations MAC et les attaques de clonage.

IV.5.2 Surveillance DHCP (DHCP Snooping)

Nous avons vu que l'usurpation DHCP est une attaque où l'attaquant écoute les demandes DHCP de l'hôte sur le réseau et y répond avec une fausse réponse DHCP avant que la réponse DHCP autorisée ne parvienne à l'hôte.

L'espionnage DHCP peut empêcher de telles attaques. L'espionnage DHCP est une fonction de commutation. Le commutateur peut être configuré pour déterminer quels ports de commutateur peuvent répondre aux demandes DHCP. Les ports de commutateur sont identifiés comme des ports approuvés ou non approuvés. Seuls les ports qui se connectent à un serveur DHCP autorisé sont configurés comme «de confiance» et autorisés à envoyer tous les types de messages DHCP. Tous les autres ports du commutateur ne sont pas approuvés et peuvent envoyer uniquement des requêtes DHCP. Si une réponse DHCP est vue sur un port non approuvé, le port est arrêté.

IV.5.3 Prevention de l'usurpation d'ARP

La méthode de sécurité des ports peut empêcher les inondations MAC et les attaques de clonage. Cependant, cela n'empêche pas l'usurpation ARP. La sécurité des ports valide l'adresse MAC source dans l'en-tête de trame, mais les trames ARP contiennent un champ source MAC supplémentaire dans la charge utile de données, et l'hôte utilise ce champ pour remplir leur cache ARP. Certaines méthodes pour empêcher l'usurpation ARP sont répertoriées comme suit.

1. **ARP statique** - L'une des actions recommandées consiste à utiliser des entrées ARP statiques dans la table ARP hôte. Les entrées ARP statiques sont des entrées permanentes dans un cache ARP. Cependant, cette méthode n'est pas pratique. En outre, il ne permet pas l'utilisation de certains protocoles DHCP car l'IP statique doit être utilisée pour tous les hôtes du réseau de couche 2.
2. **Système de détection d'intrusion** - La méthode de défense consiste à utiliser le système de détection d'intrusion (IDS) configuré pour détecter des quantités élevées de trafic ARP. Cependant, IDS est enclin à signaler des faux positifs.
3. **Inspection ARP dynamique** - Cette méthode de prévention de l'usurpation ARP est similaire à l'espionnage DHCP. Il utilise des ports approuvés et non approuvés. Les réponses ARP sont autorisées dans l'interface du commutateur uniquement sur les ports approuvés. Si une réponse ARP arrive au commutateur sur un port non approuvé, le contenu du paquet de réponse ARP est comparé à la table de liaison DHCP pour vérifier sa précision. Si la réponse ARP n'est pas valide, la réponse ARP est supprimée et le port est désactivé.

IV.5.4 Securisation du protocole Spanning Tree

Le protocole Spanning Tree (STP) est un protocole de gestion de liaison de couche 2. L'objectif principal de STP est de s'assurer qu'il n'y a pas de boucles de flux de données lorsque le réseau a des chemins redondants. Généralement, les chemins redondants sont construits pour assurer la fiabilité du réseau. Mais ils peuvent former des boucles mortelles qui peuvent conduire à une attaque DoS dans le réseau.

Protocole Spanning Tree

Afin de fournir la redondance de chemin souhaitée, ainsi que pour éviter une condition de boucle, STP définit une arborescence qui couvre tous les commutateurs d'un réseau. STP force certaines liaisons de données redondantes dans un état bloqué et conserve d'autres liaisons dans un état de transfert.

Si une liaison à l'état de transmission tombe en panne, STP reconfigure le réseau et redéfinit les chemins de données en activant le chemin de secours approprié. STP s'exécute sur les ponts et les commutateurs déployés sur le réseau. Tous les commutateurs échangent des informations pour la sélection du commutateur racine et pour la configuration ultérieure du réseau. Les BPDU (Bridge Protocol Data Unit) transportent ces informations. Grâce à l'échange de BPDU, tous les commutateurs du réseau élisent un pont/commutateur racine qui devient le point focal du réseau et contrôle les liaisons bloquées et transmises.

Attaques sur STP

1. Prise en charge du pont racine. C'est l'un des types d'attaque les plus perturbateurs de la couche 2. Par défaut, un commutateur LAN prend tout BPDU envoyé par le commutateur voisin à sa valeur nominale. Soit dit en passant, STP est fiable, sans état et ne fournit aucun mécanisme d'authentification solide.
2. Une fois en mode d'attaque racine, le commutateur attaquant envoie un BPDU toutes les 2 secondes avec la même priorité que le pont racine actuel, mais avec une adresse MAC légèrement inférieure numériquement, ce qui garantit sa victoire dans le processus d'élection du pont racine. Le commutateur attaquant peut lancer une attaque DoS soit en ne reconnaissant pas correctement les autres commutateurs provoquant une inondation de BPDU, soit en soumettant les commutateurs à un processus excessif de BPDUS en prétendant être root à la fois et se rétracter rapidement.
3. DoS utilisant Flood of Configuration BPDU. Le commutateur attaquant ne tente pas de

prendre le relais en tant que root. Au lieu de cela, il génère un grand nombre de BPDU par seconde, ce qui entraîne une utilisation très élevée du processeur sur les commutateurs.

Empêcher les attaques sur STP

Heureusement, la contre-mesure d'une attaque par prise de contrôle racine est simple et directe. Deux fonctionnalités aident à vaincre une attaque de prise de contrôle racine.

1. **Root Guard** - Root Guard restreint les ports de commutation à partir desquels le pont racine peut être négocié. Si un port «root-guard-enabled» reçoit des BPDU supérieurs à ceux que le pont racine actuel envoie, alors ce port est déplacé vers un état incohérent racine, et aucun trafic de données n'est transféré sur ce port. La protection racine est mieux déployée vers les ports qui se connectent à des commutateurs qui ne devraient pas prendre le relais en tant que pont racine.
2. **BPDU-Guard** - BPDU guard est utilisé pour protéger le réseau contre les problèmes pouvant être causés par la réception de BPDU sur les ports d'accès. Ce sont les ports qui ne devraient pas les recevoir. La protection BPDU est mieux déployée vers les ports face à l'utilisateur pour empêcher l'insertion d'un commutateur escroc par un attaquant.

IV.5.5 Securisation du VLAN

Dans les réseaux locaux, les réseaux locaux virtuels (VLAN) sont parfois configurés comme mesure de sécurité pour limiter le nombre d'hôtes sensibles aux attaques de couche 2. Les VLAN créent des limites de réseau, sur lesquelles le trafic de diffusion (ARP, DHCP) ne peut pas traverser. Dans une attaque par saut de VLAN, un attaquant sur un VLAN peut accéder au trafic sur d'autres VLAN qui ne seraient normalement pas accessibles. Il contournerait un périphérique de couche 3 (routeur) lors de la communication d'un VLAN à un autre, ce qui irait à l'encontre de l'objectif de la création de VLAN. Le saut de VLAN peut être effectué par deux méthodes ; commuter l'usurpation d'identité et le double étiquetage.

Usurpation de commutateur

Cela peut se produire lorsque le port du commutateur, auquel l'attaquant est connecté, est en mode «jonction» ou «négociation automatique». L'attaquant agit comme un commutateur et ajoute des en-têtes d'encapsulation 802.1Q avec des balises VLAN pour les VLAN distants cibles à ses trames sortantes. Le commutateur de réception interprète ces trames comme provenant d'un autre commutateur 802.1Q et transfère les trames dans le VLAN cible. Les deux mesures préventives contre les attaques d'usurpation de commutateur consistent à définir les ports de périphérie en mode d'accès statique et à désactiver la négociation automatique sur tous les ports.

Double marquage

Dans cette attaque, un attaquant connecté sur le port VLAN natif du commutateur ajoute deux balises VLAN dans l'en-tête de la trame. La première balise est du VLAN natif et la seconde est pour le VLAN cible. Lorsque le premier commutateur reçoit les trames de l'attaquant, il supprime la première balise car les trames du VLAN natif sont transmises sans balise sur le port de jonction.

— Étant donné que la deuxième balise n'a jamais été supprimée par le premier commutateur, le commutateur de réception identifie la balise restante comme destination VLAN et transfère les trames à l'hôte cible dans ce VLAN. La double attaque de marquage exploite le concept de VLAN natif. Étant donné que le VLAN 1 est le VLAN par défaut pour les ports d'accès et le VLAN natif par défaut sur les lignes réseau, c'est une cible facile.

— La première mesure de prévention consiste à supprimer tous les ports d'accès du VLAN 1 par défaut, car le port de l'attaquant doit correspondre à celui du VLAN natif du commutateur. La deuxième mesure de prévention consiste à affecter le VLAN natif sur toutes les lignes de commutation à certains VLAN inutilisés, par exemple VLAN id 999. Enfin, tous les commutateurs doivent être configurés pour effectuer un balisage explicite des trames VLAN natives sur le port de jonction.

V. Réseaux privés virtuels (VPN)

Dans le chapitre II page 1, on a évoqué le recours aux techniques cryptographiques pour le cryptage de certains messages, mais ceci est loin d'être la seule utilisation de cette technique, mais ce n'est en aucun cas le seul usage de cette technique. On peut imaginer, et de plus en plus c'est ce qui sera réalisé, le chiffrement systématique de toutes les communications en réseau. Si l'on procède ainsi, chiffrer message par message serait très inefficace : on choisira plutôt de chiffrer le flux de l'ensemble du trafic sur un ou plusieurs itinéraires donnés, cela constituera un réseau privé virtuel, ou VPN, comme *Virtual Private Network*. Il s'agira par exemple d'établir un canal chiffré entre deux nœuds quelconques de l'Internet, ces nœuds pouvant eux-mêmes être des routeurs d'entrée de réseaux. On aura ainsi établi une sorte de tunnel qui, à travers l'Internet, reliera deux parties éloignées l'une de l'autre du réseau d'une même entreprise pour donner l'illusion de leur contiguïté. Mais le chiffrement permet aussi d'établir un VPN personnel pour un utilisateur, par exemple entre son ordinateur portable et le réseau local de l'entreprise.

V.1 Principe de fonctionnement d'un VPN

Les réseaux privés virtuels sont souvent désignés par le terme anglais VPN (Virtual Private Network). Le service VPN permet la connectivité de plusieurs réseaux privés par l'intermédiaire d'une infrastructure publique partagée. L'objectif principal du service VPN est de faciliter les communications internes d'une entreprise multisites et les communications entre des entreprises partenaires (clients, fournisseurs). Avant la généralisation des technologies IP, ce service était assuré par des réseaux de type $X25$, Frame-Relay ou ATM. Les caractéristiques d'un réseau privé virtuel doivent être comparées à celles d'un réseau réellement privé en terme de débit, de temps de latence, de la jigue, de fiabilité et de sécurité.

La figure V.1 donne une représentation de trois VPN qui permettent d'interconnecter les sites, répartis géographiquement, de trois entreprises via une infrastructure partagée. Ainsi, le VPN A interconnecte les sites 1 et 2 de l'entreprise **A** ; le VPN **B** interconnecte les sites 1 et 2 de l'entreprise **B**, etc.La figure V.2 donne une autre représentation logique d'un autre réseau, où tous les sites appartenant au même VPN sont virtuellement regroupés.

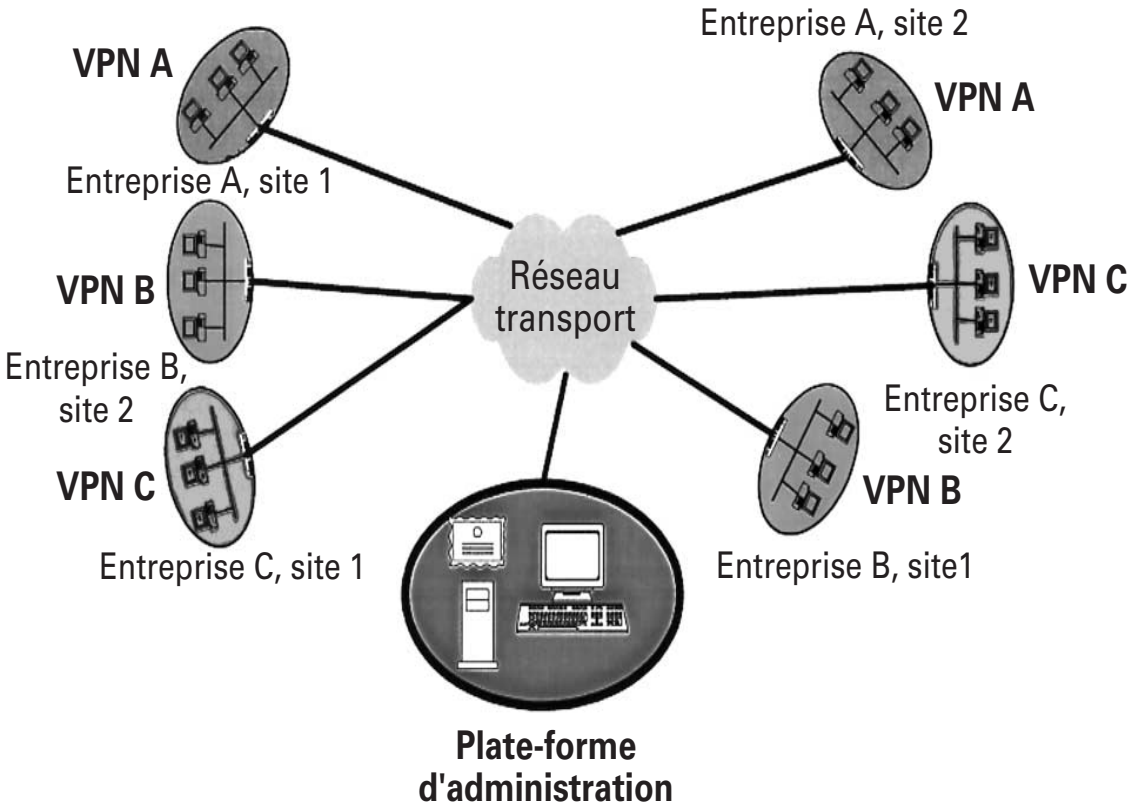


FIGURE V.1 – Modélisation des VPN.

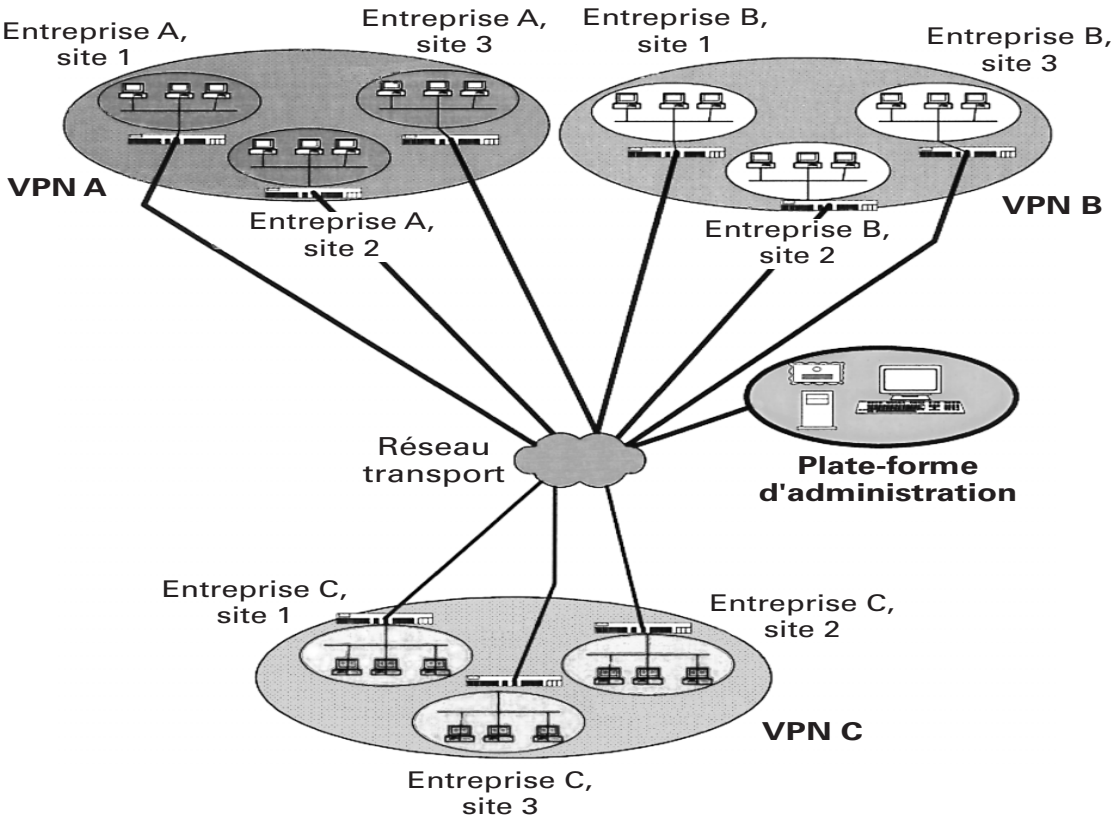


FIGURE V.2 – Modélisation logique de VPN.

Le chiffrement est généralement utilisé pour les VPN de la façon suivante : l'algorithme de Diffie-Helmann (se référer à la section II.3 du chapitre II) est utilisé pour procéder au choix d'un secret partagé, qui constituera une clé de session pour chiffrer le trafic, et qui sera renouvelé à intervalles réguliers. Il y a en revanche une assez grande variété de solutions pour introduire le VPN dans l'architecture du réseau :

— **Couche 3** : introduire le VPN au niveau de la couche réseau (n° 3 du modèle ISO) semble la solution la plus logique : il s'agit bien de créer un réseau virtuel, après tout. C'est la solution retenue par la pile de protocoles désignés collectivement par l'acronyme IPSec, que nous décrirons à la section suivante. Les protocoles IPSec sont implantés dans le noyau du système d'exploitation, ce qui assure une plus grande sûreté de fonctionnement (face aux attaques notamment) et de meilleures performances (un protocole implanté en espace utilisateur passe son temps à recopier des tampons de mémoire entre l'espace noyau et l'espace utilisateur).

— **Couche 4** : La disponibilité de bibliothèques SSL/TLS (pour Secure Socket Layer/Transport Layer Security) àla mise en œuvre facile a encouragé le développement de VPN de couche

4 (transport), comme OpenVPN ou les tunnels SSL 2 • OpenVPN, par exemple, établit un tunnel entre deux stations, et par ce tunnel de transport il établit un lien réseau, chaque extrémité recevant une adresse IP.

— **Couche 7** : Le logiciel SSH (Secure Shell), qui comme son nom l'indique est un client de connexion à distance chiffrée, donc de couche 7, permet de créer un tunnel réseau.

— **Couche 2** : Mentionnons ici, les réseaux locaux virtuels (VLAN), que nous étudierons plus en chapitre IV : il ne s'agit pas à proprement parler de VPN, mais ils ont souvent un même usage : regrouper les stations d'un groupe de personnes qui travaillent dans la même équipe sur un réseau qui leur soit réservé, séparé des réseaux des autres équipes L2TP (L ayer Two Tunneling Protocol), comme son nom l'indique, encapsule une liaison de couche 2 (liaison de données) sur un lien réseau (couche 3).

Definition V.1.1 — Encapsulation, décapsulation et tunnellisation. L'encapsulation a lieu lorsqu'une unité de données est transmise à la couche inférieure suivante du modèle de référence OSI. Lorsqu'un paquet se déplace d'une couche inférieure vers une couche supérieure, on appelle ce processus décapsulation. Lorsqu'une unité de données se déplace latéralement dans le modèle OSI, on appelle cela tunneling. Le PPTP est un protocole de tunneling car il consiste à transporter une trame PPP à l'intérieur d'un paquet IP, qui est à son tour encapsulé dans une nouvelle trame.

V.2 Les différents types de VPN

La classification des VPN n'est pas aisée ; elle dépend des critères retenus. En prenant en compte la nature des équipements mis en œuvre pour la construction des VPN, on identifie deux catégories de VPN :

— Site à site

— Accès à distance

V.2.1 Site à site

Un VPN site à site nommé aussi *Routeur-à- Routeur VPN* , illustré à la figure V.3, est une extension d'un réseau WAN classique. Les VPN site à site connectent des réseaux entiers les uns aux autres ; par exemple, ils peuvent connecter le réseau de bureaux secondaires au réseau du siège de l'entreprise. Auparavant, une ligne louée ou une connexion Frame Relay était nécessaire

pour connecter les sites, mais comme la plupart des entreprises disposent désormais d'un accès Internet, ces connexions peuvent être remplacées par des VPN site à site.

L'avantage d'utiliser le VPN site à site est la confidentialité et la sécurité de toutes les communications ou activités qui peuvent se produire entre deux réseaux donnés appartenant à la même entreprise ou à des entreprises différentes. Et comme les VPN site à site nécessitent une authentification avant que les lignes de communication puissent être établies, ils sont parfaitement adaptés à une situation où un employé souhaite accéder à des fichiers sensibles et à d'autres types de contenu sur Internet depuis un bureau distant et/ou collaborer avec une autre entreprise sur Internet.

R Si les sites appartiennent à la même entreprise, le VPN site à site devient un **VPN intranet**. Si les sites appartiennent à des entreprises différentes, le VPN site à site devient un service **VPN extranet**.

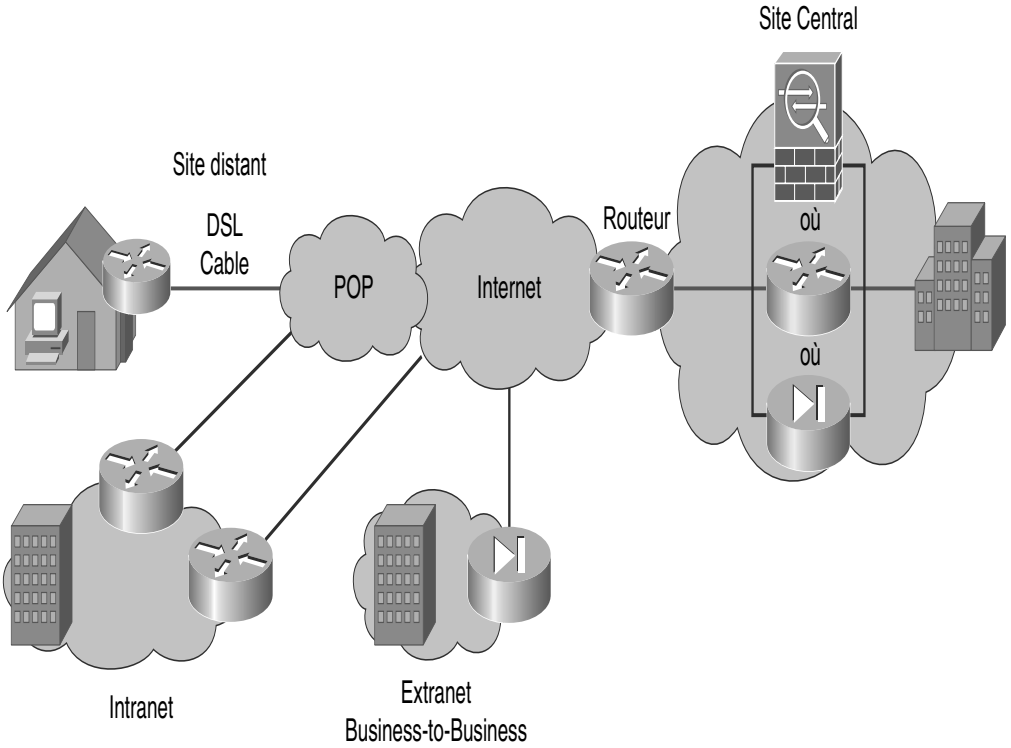


FIGURE V.3 – VPN site-à-site.

V.2.2 Accès à distance

L'accès à distance est une évolution des réseaux à commutation de circuits, tels que la bonne vieille ligne téléphonique (Plain old telephone service , POTS) ou le Réseau numérique à intégration de services (RNIS). Les VPN d'accès à distance, illustrés à la figure V.4, peuvent répondre aux besoins des télétravailleurs, des utilisateurs mobiles et du trafic extranet entre les particuliers et les entreprises. Les VPN d'accès à distance connectent des hôtes individuels qui doivent accéder au réseau de leur entreprise en toute sécurité via Internet.

Un employé d'une entreprise, lorsqu'il est en déplacement, utilise un VPN pour se connecter au réseau privé de son entreprise et accéder à distance aux fichiers et aux ressources du réseau privé. Les utilisateurs privés ou les utilisateurs à domicile du VPN utilisent principalement les services VPN pour contourner les restrictions régionales sur le web et accéder aux sites web bloqués. Les utilisateurs conscients de la sécurité de l'Internet utilisent également les services VPN pour renforcer leur sécurité et leur confidentialité sur Internet.

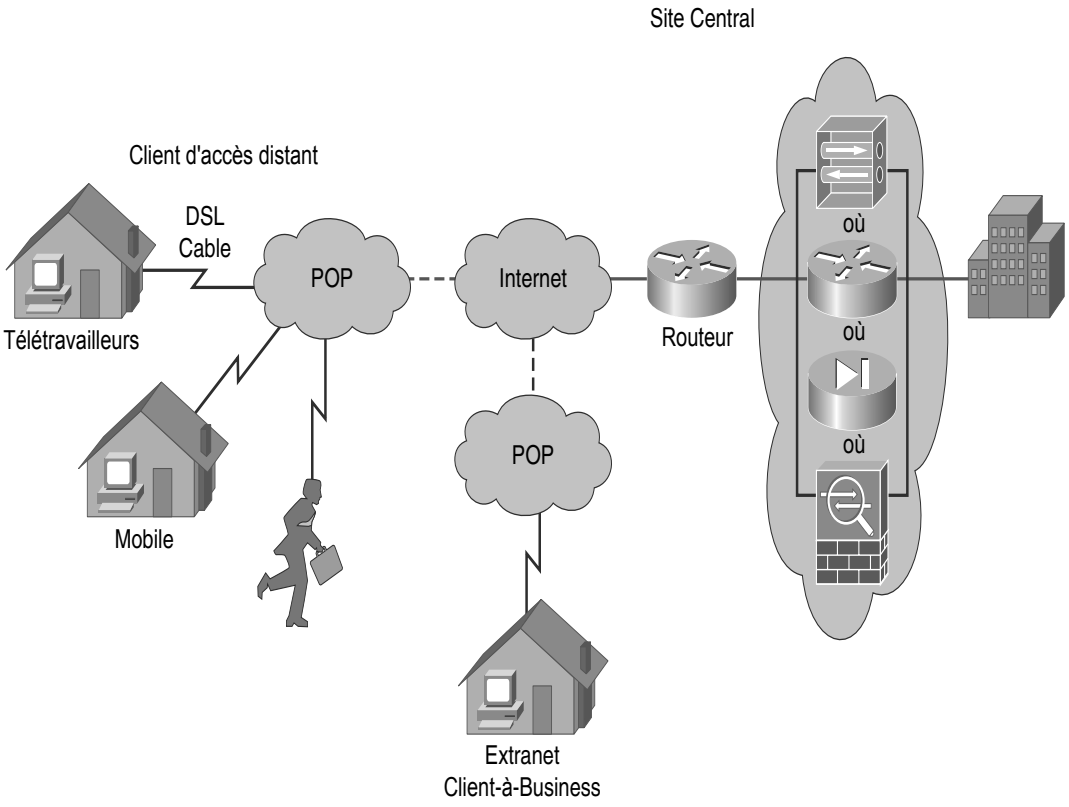


FIGURE V.4 – VPN Accès à distance.

V.3 Les protocoles utilisés

Les premiers protocoles utilisés par les VPN ont été des protocoles propriétaires tels que L2F (Layer 2 Forwarding) de Cisco, PPTP (Point to Point Tunneling Protocol) de Microsoft et L2TP (Layer 2 Tunneling Protocol), fusion des 2 précédents. Aujourd'hui le protocole standard est IPSec (IP Security) validé par l'IETF (Internet Engineering Task Force). Ces protocoles peuvent être de niveau 2 (couche liaison) tels que PPTP ou L2TP, qui permettront de gérer différents protocoles, ou de niveau 3 (couche réseau) tel IPSec, qui prendra en charge les réseaux IP uniquement.

V.3.1 PPTP – Point-to-Point Tunneling Protocol

Basé sur le protocole PPP (Point-to-Point Protocol) permettant l'accès à distance, PPTP était le protocole VPN le plus utilisé jusqu'à présent, du fait essentiellement de son intégration en standard à Windows.

Les trames PPP sont encapsulées dans une trame PPTP : elles sont alors munies d'un en-tête GRE (Internet Generic Routing Encapsulation) et IP, comme l'illustre la figure V.5. Cet en-tête est composé des adresses IP du client et du serveur VPN. Il faut remarquer que le paquet PPP encapsulé peut lui même encapsuler plusieurs types de protocoles comme TCP/IP, IPX… (on arrive ainsi à router des paquets NetBEUI, à l'origine non routable, grâce à l'encapsulation) et que c'est le serveur PPTP qui sélectionnera, dans le paquet reçu, le protocole pris en charge par son réseau privé. La gestion multiprotocole est donc importante car elle permet d'envoyer des informations sans se soucier du protocole géré par le réseau de destination.

Pour concevoir la manière dont est créé et « maintenu » un tunnel, il faut comprendre qu'il existe des données autres que celles que l'on envoie « consciemment » sur un réseau VPN : ce sont les connexions de contrôle. Pour PPTP, il s'agit essentiellement d'une connexion TCP utilisant le port 1723 qui sert à établir et à maintenir le tunnel grâce à des ordres comme *Call Request* et *Echo Request*. Le port 1723 des machines traversées doit donc impérativement être ouvert ce qui impose que les pare-feu (firewalls) dont disposent les participants soient configurés pour laisser passer le trafic sur ce port spécifique, sous peine de ne jamais réussir à créer un tunnel VPN.

Authentification

Dans un VPN il faut veiller à ce que seuls les utilisateurs authentifiés soient autorisés à se loguer au serveur PPTP distant, autrement dit à ce que quiconque appartenant à d'autres réseaux

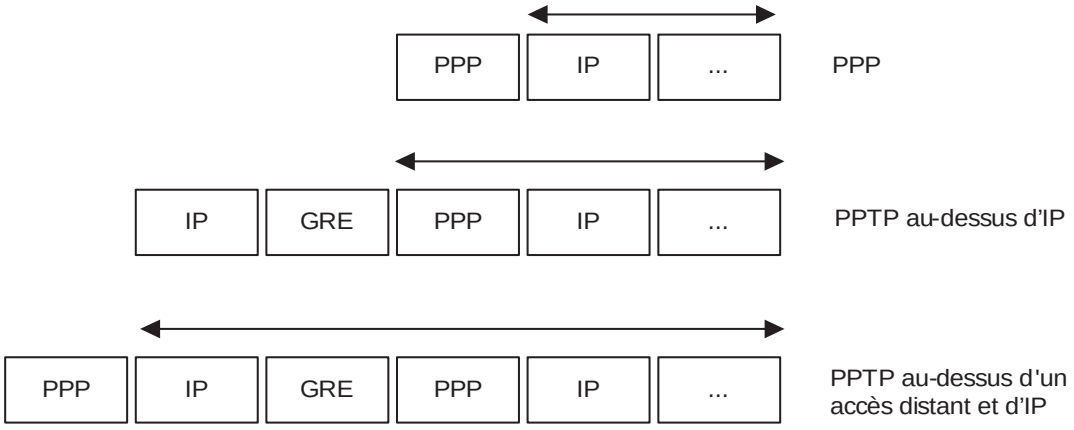


FIGURE V.5 – Encapsulation des trames PPTP dans GRE.

ne puisse avoir accès aux informations. Pour ce faire, un mécanisme d'authentification va être mis en œuvre au niveau du serveur. L'authentification sous PPTP est la même que celle utilisée par PPP, à savoir :

— **PAP** (Password Authentication Protocol) est un protocole d'authentification avec réponse en clair – et donc non sécurisé – des logins et mots de passe exigés par le serveur distant.

— **CHAP** (Challenge Handshake Authentication Protocol) ou MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) est un mécanisme d'authentification crypté, qui évite la transmission du mot de passe en clair et qui est donc sécurisé

Chiffrement de données

Pour protéger le transfert des données, on exploite un algorithme cryptographique. Les données ainsi chiffrées garantissent qu'un intrus qui en intercepterait un morceau ne puisse les exploiter. On va pour cela devoir utiliser une clé de chiffrement. Là encore PPTP va utiliser un protocole issu de PPP pour négocier le type de cryptage : CCP (Compression Control Protocol). Il existe deux méthodes :

— **Le chiffrement symétrique** utilisé par les algorithmes RSA RC4/DES/IDEA Dans le chiffrement symétrique, la même clé de session est utilisée par les 2 entités communicantes. Elle est changée de manière aléatoire au bout d'un certain temps (durée de vie de la clé).

— **Le chiffrement asymétrique** ou par clé publique (PKI, signatures numériques). Dans le chiffrement asymétrique, on utilise un protocole qui permet à chaque entité de déterminer une moitié de la clé et d'envoyer à l'autre entité les paramètres permettant de calculer la moitié manquante. On peut également se baser sur une paire de clés, une « privée » et une

« publique ». Une vigilance particulière est nécessaire en ce qui concerne l'utilisation de clés de chiffrement car la loi française ne tolère les clés que jusqu'à 128 bits et impose une demande d'autorisation au-delà.

V.3.2 L2TP – Layer 2 Tunneling Protocol

L2TP encapsule, par le biais d'un tunnel, les protocoles IP, IPX et NetBEUI, eux-mêmes encapsulés dans des paquets PPP. Il utilise pour cela des paquets IP/UDP sur les réseaux IP pour le transport des tunnels L2TP, comme illustré à la figure V.6. Contrairement à PPTP qui interconnecte des réseaux IP uniquement, L2TP permet, lui, d'interconnecter des réseaux dès que le tunnel offre une connexion point-à-point orientée paquet (Frame Relay, $X25$, ATM). En ce qui concerne la gestion des données, la grande différence avec PPTP, c'est la façon dont L2TP gère l'authentification et le cryptage. Là où PPTP utilisait les mécanismes de PPP, L2TP s'appuie sur un module « externe » (dans le sens où il peut être utilisé seul) : IPSec. On exploite donc un procédé à deux « étages » :

1. **Encapsulation par L2TP** : les trames (qui contiennent elles-mêmes des datagrammes « normaux ») sont munies d'un en-tête L2TP et UDP.
2. **Encapsulation par IPSec** : une fois la trame L2TP générée, on lui ajoute un en-tête (un trailer IPSec) ESP – module d'authentification IPSec qui permettra d'assurer l'intégrité des données et l'authentification – et enfin un en-tête IP. Comme pour PPTP, ce dernier est composé des adresses IP du client et du serveur VPN.

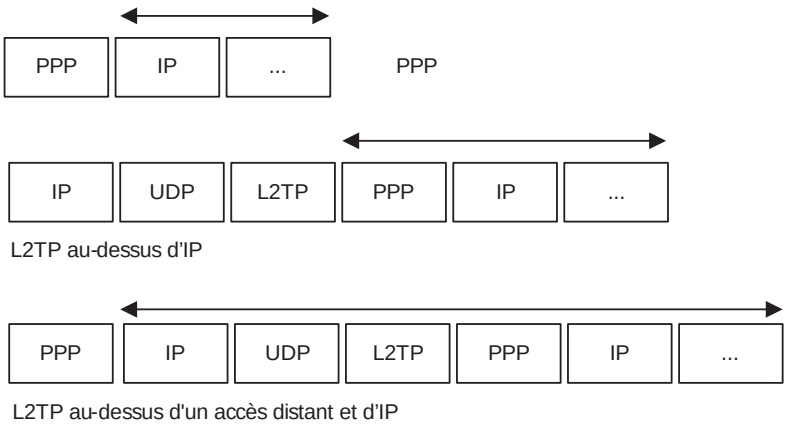


FIGURE V.6 – Encapsulation L2TP des trames PPP.

V.3.3 L2F – Laver 2 Forwarding

D'origine Cisco est un tunnel dit opérateur, il est initialisé par le fournisseur d'accès (ISP, Internet Service Provider) et se termine chez le client par un équipement spécifique. Le protocole L2F n'assure l'authentification de l'utilisateur qu'à la connexion. Le tunnel L2F ne garantit pas la confidentialité des données (pas de chiffrement). Cependant, un chiffrement utilisateur de bout en bout peut être mis en œuvre.

V.3.4 IPSec – IP Security Protocol

IPSec est le protocole qui prédomine actuellement dans les VPN car il est disponible sur de nombreuses plates-formes (NT, Linux, Novell, Macintosh...) et géré de manière native avec IPv6. Autrement dit, pas de changement de structure ni d'éventuelles incompatibilités quand le temps sera venu de passer à IPv6. Par contre, IPSec est aussi assez contraignant pour l'entreprise. Compte tenu du système de clé partagée (si on utilise ce mode d'authentification), retirer l'accès à un utilisateur en cas de départ de la société revient à faire changer la clé à l'ensemble des autres utilisateurs concernés. On peut cependant utiliser une infrastructure à clé publique mais, compte tenu de la difficulté, les entreprises déployant une PKI interne restent rares

V.3.5 SSL – TLS Socket Secure Layer – Transport Layer Security

SSL (Socket Secure Layer) est un protocole mis en oeuvre initialement par Netscape et repris par l'IETF sous le nom TLS (Transport Layer Security). Il est, au niveau des VPN, une alternative à IPSec de plus en plus présente, Essentiellement utilisé pour chiffrer la communication entre un navigateur et un serveur web, il fournit, le temps d'une session, une liaison sécurisée sur un réseau IP. Il autorise donc un accès à distance sécurisé, sans avoir à déployer un logiciel VPN client spécifique sur les ordinateurs portables ou les terminaux publics. L'utilisateur exploite simplement un navigateur web reposant sur n'importe quel système d'exploitation. Avec un VPN SSL les utilisateurs nomades peuvent avoir un accès à des applications bien déterminées sur l'intranet de leur organisation depuis n'importe quel point d'accès Internet. Cependant, l'accès aux ressources internes est plus limité que celui fourni par un VPN IPSec, puisque l'on accède uniquement aux services qui ont été définis par l'administrateur du VPN ou prévu par la société éditrice de la solution VPN SSL. Pour créer le tunnel IP à travers SSL, il suffit d'encapsuler le trafic IP dans des paquets PPP puis de rediriger ces paquets PPP dans une session SSL (Cf. figure V.7).

Le tableau V.1 résume les caractéristiques des technologies VPN décrites dans ce chapitre.

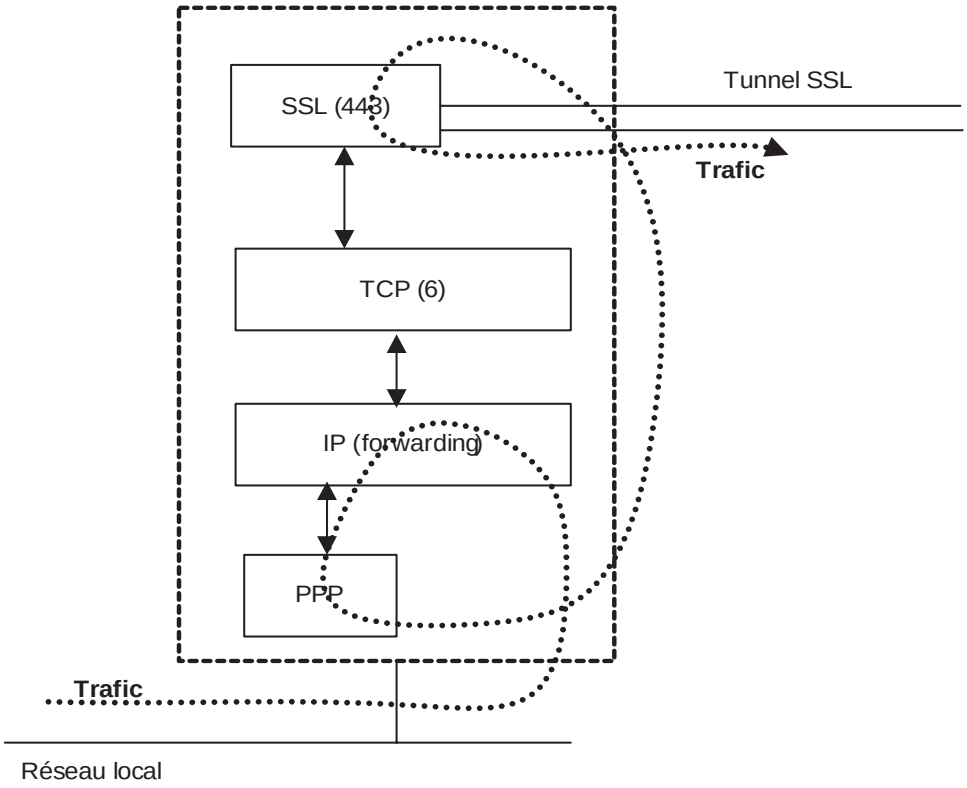


FIGURE V.7 – Tunnel IP à travers SSL.

TABLE V.1 – Comparaison de protocoles VPN

Nom	Principaux points forts	Principales faiblesses	Exemples potentiels d'utilisation
PPTP	+Peut protéger les protocoles non-IP	- Le logiciel client doit être configuré (et installé sur les hôtes sans client intégré)	Aucun
		- Présente des faiblesses connues en matière de sécurité	
		- N'offre pas une forte authentification	
		- Ne prend en charge qu'une seule session par tunnel	
L2TP	+ Peut protéger les protocoles non-IP	- Le logiciel client doit être configuré (et installé sur les hôtes sans client intégré)	Protéger les communications commutées
	+ Peut supporter plusieurs sessions par tunnel		
	+ Peut utiliser des protocoles d'authentification tels que RADIUS.		
	+ Peut utiliser IPsec pour fournir des services de cryptage et de gestion des clés.		
L2F	+ Peut protéger les protocoles non-IP	- Exige la participation de chaque fournisseur de services Internet (FAI)	Aucun
	+ Transparent pour les clients	- Ne protège pas les communications entre les clients et le FAI	
	+ Peut utiliser des protocoles d'authentification tels que RADIUS	- N'offre pas de cryptage ; doit compter sur les services de cryptage PPP, qui possèdent des faiblesses connues	
IPsec	+ Déjà pris en charge par la plupart des systèmes d'exploitation	- Ne peut protéger que les communications basées sur IP	Protéger toutes les communications entre réseaux, par exemple en supportant la connectivité d'un site distant
	+ Peut fournir une forte cryptage et d'intégrité protection	- Nécessite la configuration d'un logiciel client (et son installation sur les hôtes sans client intégré) pour les architectures hôte à passerelle et hôte à hôte.	
	+ Transparent pour les clients dans les architectures passerelle à passerelle	- Ne protège pas les communications entre les clients et la passerelle IPsec dans les architectures passerelle à passerelle.	
	+ Peut utiliser une variété de protocoles d'authentification		
SSL	+ Déjà pris en charge par tous les principaux navigateurs Web	- Ne peut protéger que les communications basées sur le protocole TCP	Aucun
	+ Peut fournir un cryptage et d'intégrité d'intégrité	- Les serveurs d'applications et les clients doivent prendre en charge SSL	
	+ Peut fournir plusieurs couches d'authentification	- Configuré sur une base d'application par application	
	+ Transparence pour les utilisateurs		
	+ Contrôle d'accès granulaire		

VI. Sécurité des réseaux sans fil

LES ondes électromagnétiques se propagent indépendamment de tout support, elles peuvent être reçues par toute station à l'écoute, aussi se prémunir contre les écoutes clandestines est l'une des préoccupations majeures de tout système de transmission sans fil (faisceaux hertziens, téléphonie mobile...). Les réseaux locaux sans fil, en particulier la norme IEEE 802.11, ont gagné beaucoup plus de terrain que prévu en très peu de temps. Cette croissance est toutefois entravée par des problèmes de sécurité ; ces problèmes sont désormais si bien connus que même les non-spécialistes y sont sensibilisés. Ce chapitre commence par une brève présentation de la sécurité, suivie d'une discussion sur certains protocoles de sécurité. Ensuite, les problèmes de sécurité dans les contre-mesures IEEE 802.11 présentes sur le marché sont abordés. La norme 802.11 prévoit la possibilité de chiffrer les données (WEP, Wired Equivalent Privacy), mais les nombreuses faiblesses du chiffrement RC4 ont conduit le comité 802.11 à éditer un nouveau standard (802.11i, WPA, Wifi Protected Access).

VI.1 Types de réseaux sans fil

Les réseaux sans fil appartiennent à plusieurs catégories, régies par des normes spécifiques :

- les réseaux dits **Wireless Local Area Network (WLAN)** ou Wi-Fi obéissent aux normes de la famille IEEE 802.11, dont la première édition date de 1997 ; ils sont destinés à faire communiquer des équipements séparés par une distance de l'ordre de quelques dizaines de mètres, par exemple dans un immeuble ; les dispositifs d'émission et de réception de ces appareils ont une puissance maximale de $100mW$ (à comparer avec celle d'un téléphone portable GSM, qui est de $1W$) ;
- les réseaux dits **Wireless Personal Area Network (WPAN)** ou Bluetooth obéissent à la norme IEEE 802.15.1 ; ils permettent des communications entre des appareils distants de quelques mètres, par exemple un téléphone et son oreillette sans fil ; les promoteurs de cette norme l'ont déjà déployée pour les assistants personnels (PDA) et ils envisagent des débouchés sur le marché du jouet et des consoles de jeu ; la puissance des émetteurs est plus faible que pour les appareils 802.11, en général $1mW$ (il existe bien une option de la norme qui permet une puissance de $100mW$, mais elle n'est pratiquement pas utilisée), et de ce fait la consommation électrique est moindre ; la norme IEEE 802.15.3 (Bluetooth2) est une évolution de la norme Bluetooth avec des débits plus rapides et des mécanismes de sécurité améliorés par rapport à 802.15.1 ;
- les réseaux dits **Wireless Metropolitan Area Network (WMAN)** obéissent à la norme802.16, plus connue sous le nom de WiMax, ou de Boucle locale radio (BLR) ; ils sont capables de relier des équipements distants de quelques kilomètres, par exemple pour se substituer aux liaisons ADSL dans les zones rurales à faible densité ;
- les réseaux dits **Wireless Wide Area Network (WWAN)** utilisent les systèmes de téléphonie sans fil tels que GSM (Global System for Mobile Communication), GPRS (General Packet Radio Service) ou UMTS (Universal Mobile Telecommunication System) comme couche de liaison de données pour constituer une infrastructure d'accès à l'Internet.

Ici, on se concentrera sur les réseaux sans fil de type 802.11.

VI.2 Vulnérabilités 802.11 spécifiques

Dans un réseau sans fil, l'écoute passive du canal et des transmissions qui s'y déroulent est évidente. Bien sûr, l'écoute comme la transmission vers le réseau n'est possible que dans le domaine de couverture du réseau sans fil, c'est-à-dire, en règle générale, sur quelques centaines

de mètres au plus. Il ne faut cependant pas oublier que des antennes directives peuvent, dans certaines conditions, augmenter considérablement la portée. Ces antennes directives permettent à une entité étrangère d'écouter ce réseau ou de lui envoyer des informations. C'est dans cette facilité supplémentaire d'interaction à distance que réside la différence majeure de sécurité entre un réseau local et un réseau local sans fil.

Les quatre attaques qui sont les plus souvent répertoriées dans les réseaux sans fil sont les suivantes :

— interception de données ;
— intrusion dans le système ;
— attaque de l'homme au milieu ;
— porte dissimulée.

VI.2.1 Interception de données

C'est l'attaque la plus classique. En l'absence de système de chiffrement efficace, il est facile de récupérer le contenu des données qui circulent sur le médium de communication. Le caractère ouvert des équipements de réseau sans fil facilite ce type d'interception. La figure VI.1 illustre une interception par une station espion. Celle-ci peut être réalisée par une station dans le domaine normal de couverture du réseau ou à distance, pour peu que la station espion soit munie d'une antenne directive.

VI.2.2 Intrusion dans le système

Cela consiste, pour un élément étranger, à se connecter au point d'accès radio puis à pénétrer dans le réseau local derrière le point d'accès. La figure VI.2 illustre des attaques d'intrusion sur un réseau sans fil. Comme pour l'écoute passive, cette attaque peut être menée dans le domaine de couverture ou à distance, grâce à une antenne directive. Les points d'accès servent à l'attaquant de point d'entrée dans le réseau, après quoi il peut tenter de pénétrer les équipements reliés au réseau. Ces deux premières attaques sont les plus classiques. Elles peuvent s'exercer en dehors de la zone de déploiement du réseau sans fil, soit parce que la portée du réseau sans fil dépasse sa zone de déploiement, soit par l'utilisation d'une antenne directionnelle. Les deux attaques suivantes nécessitent de pénétrer dans la zone de déploiement du réseau.

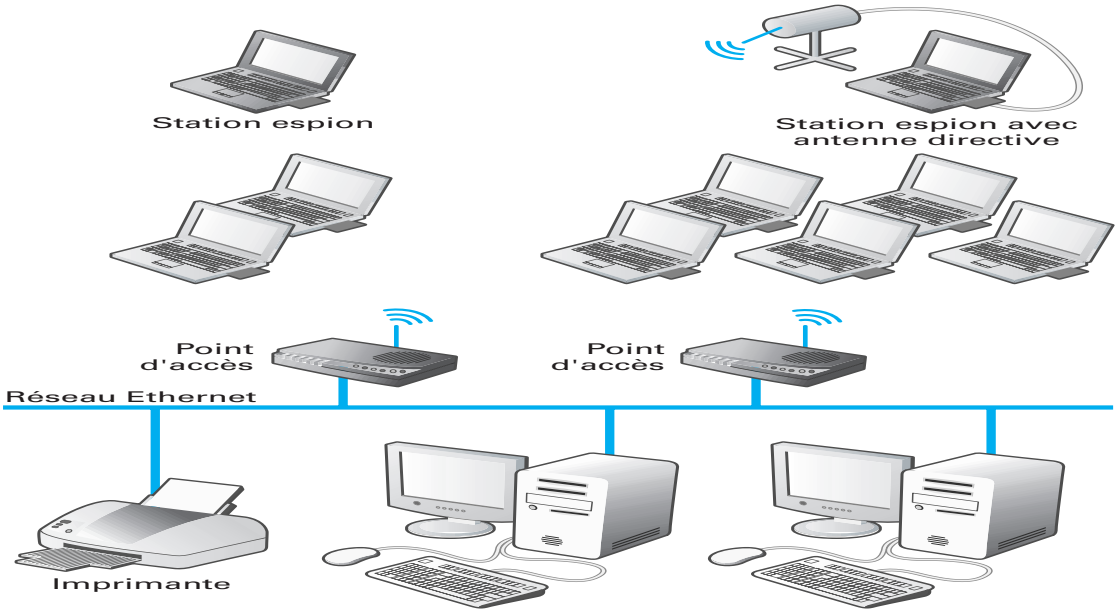


FIGURE VI.1 – Interception de données dans un réseau sans fil.

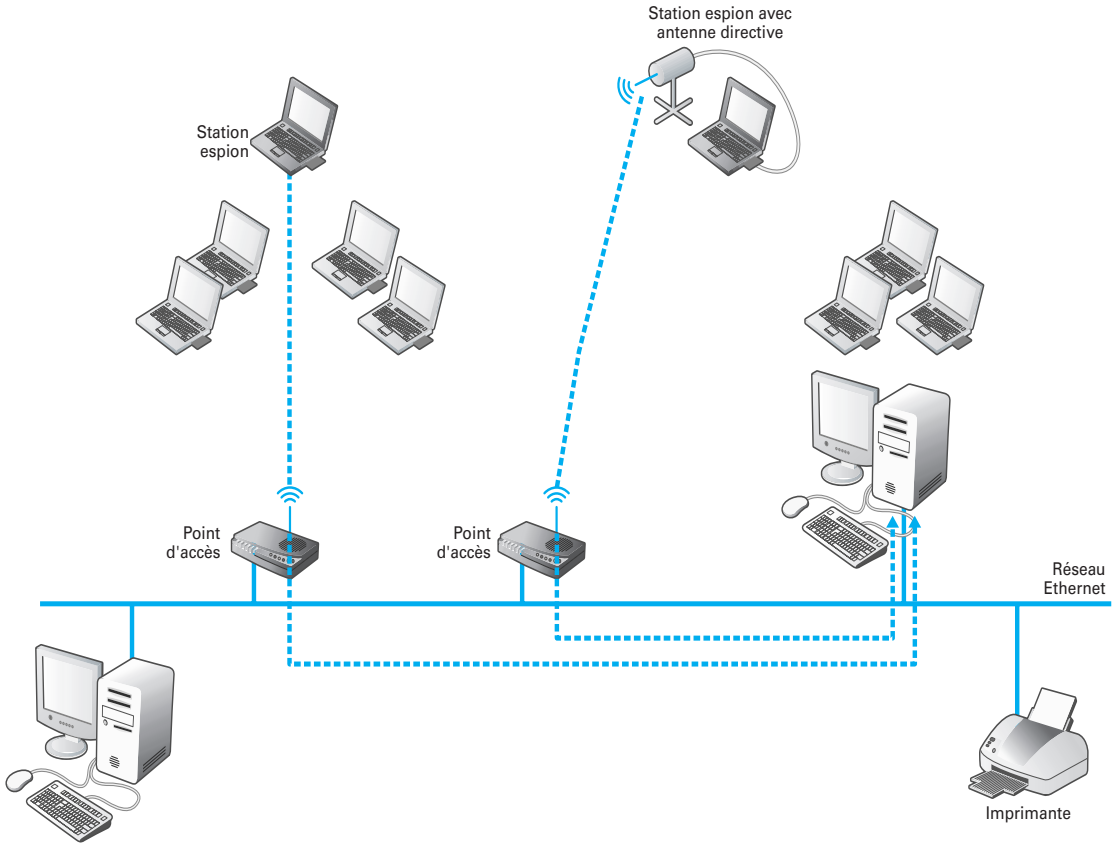


FIGURE VI.2 – Intrusions dans un réseau sans fil.

VI.2.3 Attaque de l'homme au milieu

Classique dans les réseaux, elle est particulièrement facile à mettre en œuvre dans les réseaux sans fil. Il suffit de mettre en service un point d'accès étranger au voisinage du réseau sans fil qu'on souhaite attaquer, celui-ci va servir de « cheval de Troie ». Ce point d'accès n'est pas nécessairement connecté au réseau soumis à l'attaque, il doit cependant en être proche géographiquement. Une station sans fil va naturellement pouvoir chercher à s'y connecter, livrant ainsi les clés du processus de connexion. Ces clés ayant été collectées, elles servent à un futur intrus pour pénétrer dans le réseau. Le scénario d'une telle attaque est illustré par la figure VI.3.

VI.2.4 Porte dissimulée

Cette attaque nécessite un accès physique au réseau sans fil qu'on souhaite attaquer. On va raccorder un point d'accès « félon » à ce réseau. Ce point d'accès contrôlé par l'espion ouvre une porte dissimulée et permet de pénétrer dans le réseau en contournant les mécanismes de contrôle d'accès. Après mise en place du point d'accès félon, l'attaque peut se faire dans la zone de couverture directe de ce dernier ou à distance en utilisant une antenne directionnelle. Cette attaque est illustrée par la figure VI.4.

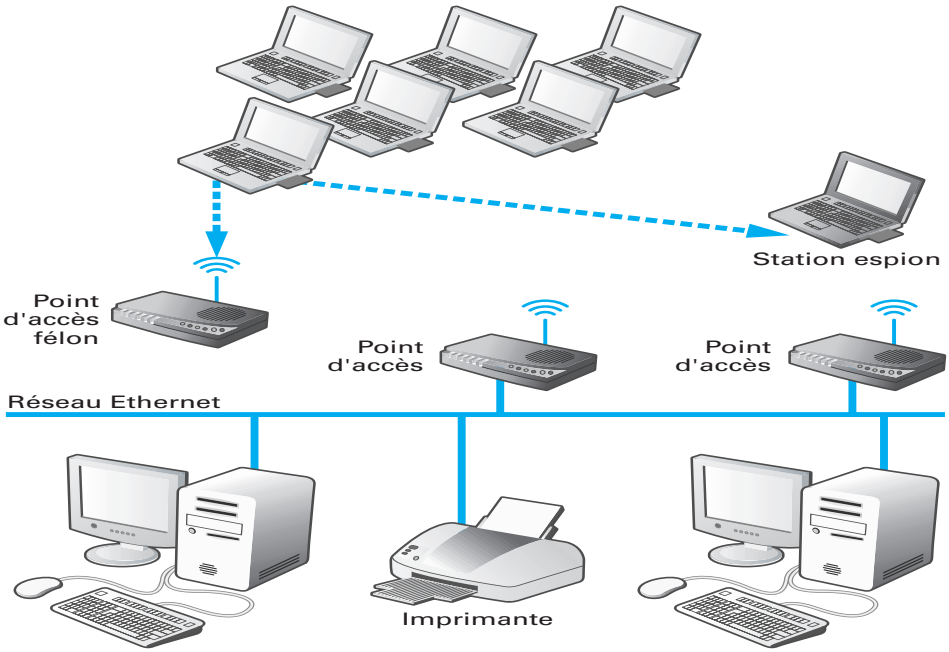


FIGURE VI.3 – Attaque de l'homme du milieu par un point d'accès malveillant.

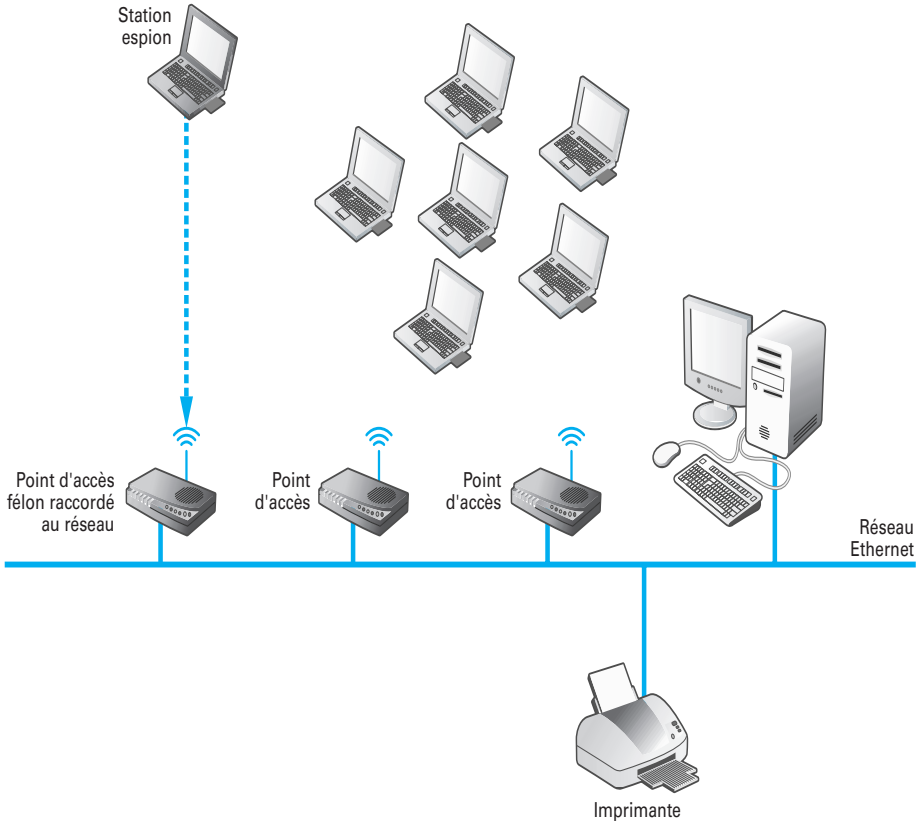


FIGURE VI.4 – Attaque de la porte dissimulée par un point d'accès malveillant.

VI.3 Mesures de sécurité adoptées par IEEE 802.11

Les systèmes de sécurité de base des réseaux radio n'utilisent pas d'algorithme de chiffrement et ne peuvent prétendre résoudre que le problème du contrôle d'accès sur un réseau sans fil. Les solutions minimales utilisent trois techniques : l'identificateur de réseau, la protection par mot de passe et la protection par l'adresse MAC IEEE.

VI.3.1 Identificateur de réseau

Cet identificateur, inclus dans la norme IEEE 802.11, permet de filtrer le trafic. Un trafic ne portant pas le même identificateur que le réseau que l'on souhaite pénétrer est ignoré par ce dernier. Il est donc nécessaire de connaître le nom du réseau pour y pénétrer. Cette protection est en fait très sommaire, car le point d'accès envoie périodiquement en clair des trames indiquant l'identité du réseau. Une écoute du réseau permet de récupérer ce nom de réseau.

VI.3.2 Mot de passe

La protection par mot de passe est bien connue. Une station cherchant à se connecter au réseau doit envoyer un mot de passe à la requête de ce réseau, ou plus généralement d'un point d'accès de celui-ci. Si le mot de passe est correct, l'accès est autorisé, sinon il est interdit. Cette protection est également extrêmement simpliste, car il est facile de capturer le mot de passe par écoute passive.

VI.3.3 Protection par adresse MAC IEEE

Cette protection consiste à n'autoriser l'accès au réseau qu'à des stations présentant une adresse MAC IEEE prédéfinie et connue du réseau. Cette protection n'est pas non plus très difficile à contourner, car l'écoute passive du réseau permet de récupérer les adresses MAC IEEE autorisées. Ensuite, de nombreuses cartes radio permettent de modifier par logiciel leur adresse MAC IEEE. Ces protections peuvent être employées seules ou en combinaison. Elles offrent une sécurité très réduite pour le contrôle d'accès mais permettent néanmoins de protéger le réseau contre un accès immédiat, puisqu'elles nécessitent une écoute préalable du réseau.

VI.4 Solutions de sécurité offertes par IEEE 802.11

Nous venons de voir que les solutions de sécurité les plus simples étaient très facilement contournables du fait qu'elles n'utilisaient pas de chiffrement. Si l'on souhaite offrir une meilleure sécurité vis-à-vis de l'écoute passive mais aussi pour l'authentification et le contrôle d'accès, l'utilisation du chiffrement est essentielle. Sans chiffrement, il est clair qu'on ne peut se défendre contre l'écoute passive. Il est tout autant difficile d'offrir des services d'authentification et de contrôle d'accès, puisque, sans chiffrement, il est possible d'écouter les séquences d'authentification et de contrôle d'accès et de les rejouer. Par la suite est présenté le système de chiffrement de la norme IEEE 802.11, appelé WEP (Wired Equivalent Privacy).

VI.4.1 WEP – Wired Equivalent Privacy

La sécurité dans IEEE 802.11 est obtenue grâce à l'algorithme de chiffrement WEP. C'est un système à clé symétrique secrète. Le chiffrement s'opère à la volée par l'application d'un « ou » exclusif sur la séquence en clair et sur une séquence pseudo-aléatoire. Pour éviter qu'un même paquet soit chiffré plusieurs fois de la même façon, le système de chiffrement d'IEEE 802.11 utilise, en plus de la clé de chiffrement statique présente dans chaque station, un vecteur d'ini

tialisation, qui change aléatoirement avec chaque trame envoyée. La clé de chiffrement statique sur 40 bits est concaténée avec le vecteur d'initialisation sur 24 bits dans la position des poids faibles. Les 8 octets ainsi formés permettent de générer la séquence pseudoaléatoire à l'aide du chiffrement classique *RC*4 (Ron's Code #4). Le processus de chiffrement est illustré par la figure VI.5.

La clé de chiffrement et le vecteur d'initialisation permettent donc de calculer une séquence pseudo-aléatoire suivant l'algorithme *RC*4. Cette séquence pseudo-aléatoire est ensuite utilisée pour chiffrer la trame par l'application bit à bit d'un « ou » exclusif (XOR) entre la trame à coder et la séquence pseudo-aléatoire. Par ailleurs, un champ de contrôle d'intégrité est calculé à partir de la trame à encoder initiale. La trame envoyée contient, outre l'en-tête habituel, un identificateur de la clé de codage, le vecteur d'initialisation, la trame cryptée par la séquence aléatoire et le champ de contrôle d'intégrité. Le champ de contrôle d'intégrité (linéaire CRC 32) est calculé sur la trame cryptée.

Le mécanisme de déchiffrement est illustré par la figure VI.6. À l'aide de l'identificateur de la clé de chiffrement et du vecteur d'initialisation, la séquence pseudo-aléatoire de chiffrement est reconstruite. L'application de cette séquence de chiffrement sur les données cryptées permet de remonter à la trame initiale. Sur cette dernière, l'algorithme de calcul du contrôle d'intégrité est appliqué. Le résultat peut ainsi être comparé avec la valeur envoyée dans la trame. En cas de correspondance entre ces deux valeurs, la trame est acceptée. Dans le cas contraire, la trame est rejetée. L'encapsulation d'une trame cryptée est illustrée par la figure VI.7. Les trois premiers octets de la trame contiennent le vecteur d'initialisation. L'octet suivant permet de reconnaître la clé de chiffrement grâce à deux bits. On trouve ensuite la trame cryptée. Les quatre derniers octets sont constitués par le champ du contrôle d'intégrité.

VI.4.2 Authentification

Il existe deux services d'authentification. Le premier service, dit système ouvert d'authentification, ne produit aucune vérification. Le second service, dit de la clé partagée, permet de s'assurer que la station qui souhaite s'authentifier possède bien la clé partagée. Cette vérification ne nécessite pas de transmettre en clair la clé mais s'appuie sur l'algorithme de chiffrement décrit précédemment.

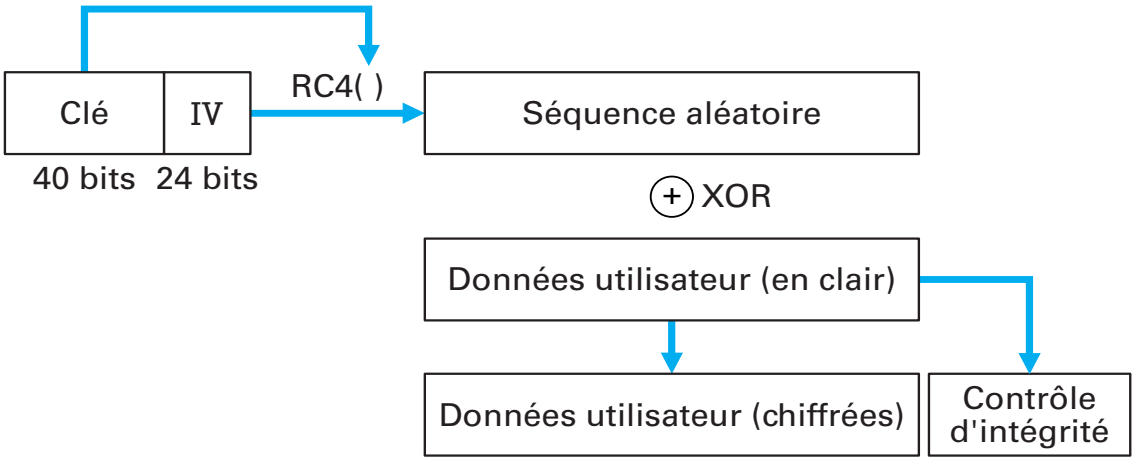


FIGURE VI.5 – Mécanisme de chiffrement.

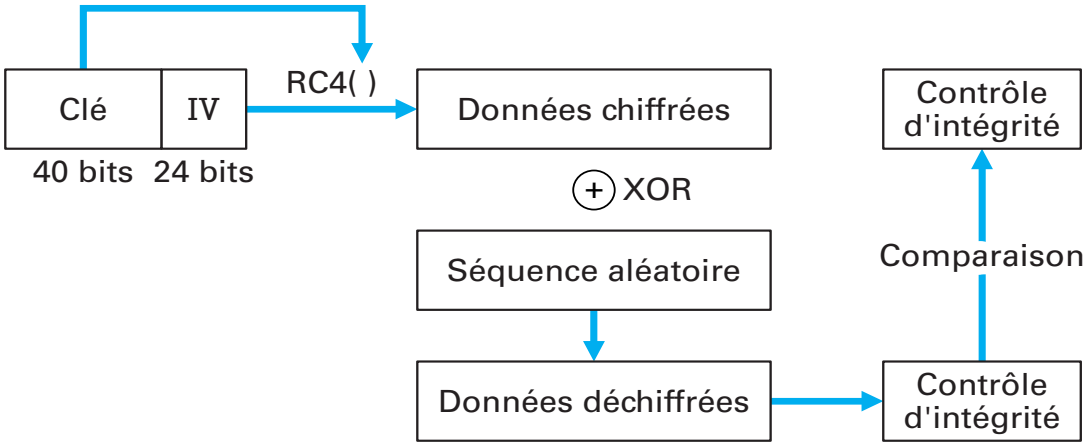


FIGURE VI.6 – Mécanisme de déchiffrement.

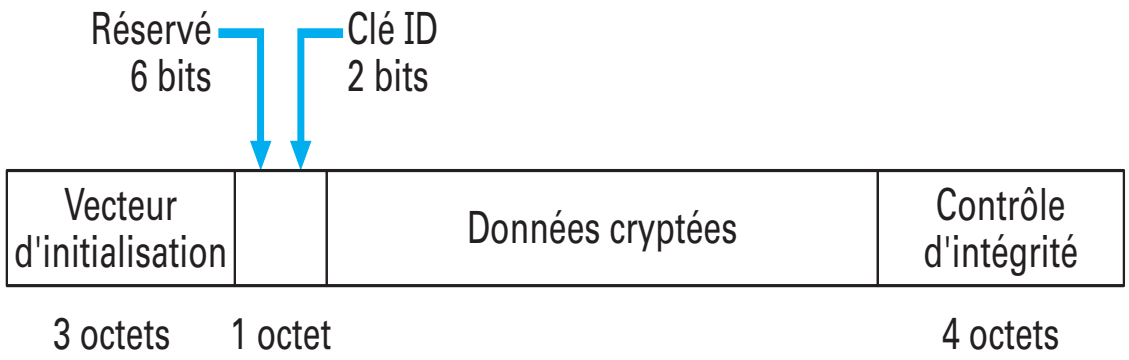


FIGURE VI.7 – Encapsulation d'une trame cryptée.

Le système ouvert d'authentification permet à une station de s'authentifier auprès d'une autre station. Pour cela, cette station envoie une requête d'authentification au point d'accès auprès duquel elle souhaite s'authentifier. Dans le système d'authentification ouvert, la réponse à cette requête doit toujours être positive, pour autant que la station réceptrice accepte ce mode d'authentification sans contrôle. L'authentification est réalisée complètement en deux messages.

L'authentification du mode ouvert est purement formelle, la seule vérification étant que ce mode soit supporté par la station qui valide l'authentification. Le système à clé partagée nécessite l'échange de quatre trames pour réaliser l'authentification. La première, envoyée par la station qui souhaite s'authentifier vers la station authentifiante, est une simple requête d'authentification qui précise, outre l'identité de celle-ci, le type d'authentification souhaité, soit ici le système à clé partagée. La deuxième trame est renvoyée par la station identifiante. Elle contient un texte aléatoire de 128 octets produit par l'algorithme de chiffrement et un vecteur d'initialisation quelconque.

Ce texte aléatoire correspond à une séquence que la station qui souhaite s'identifier doit renvoyer cryptée à la station identifiante. La troisième trame renvoyée par la station qui souhaite s'identifier contient la réplique cryptée du texte aléatoire d'essai envoyé. Cette trame contient donc un champ de contrôle d'intégrité permettant de s'assurer que la trame a été cryptée avec la bonne clé de chiffrement. La station authentifiante déchiffre la trame reçue. Si le test du contrôle d'intégrité est positif, le texte décodé est comparé avec la version envoyée. S'il y a correspondance, la station renvoie un message d'authentification réussi. Dans le cas contraire, c'est un message d'échec qui est envoyé.

VI.5 Problèmes de WEP

Des équipes de recherche ayant démontré que ce système de chiffrement était peu résistant aux attaques, nous allons donner brièvement les résultats de leurs recherches. Les principales failles du WEP peuvent être classées en trois

catégories :

— contournement de l'algorithme de contrôle d'intégrité ICV (Integrity Check Value), qui permet de s'assurer qu'une trame est cryptée convenablement et avec la bonne clé ;

— possibilité de construire des dictionnaires fournissant, en fonction d'un vecteur d'initialisation, la séquence pseudo-aléatoire de déchiffrement ;

— faille du chiffrement *RC*4 permettant de calculer directement la clé de chiffrement.

L'algorithme de contrôle d'intégrité étant linéaire, il est facile de le contourner. Supposons que nous disposions par écoute d'une trame chiffrée valide avec son champ de contrôle d'intégrité. Si nous modifions une partie de cette trame du fait de la linéarité du système de calcul du champ de contrôle d'intégrité, il suffit de calculer ce champ de contrôle d'intégrité correspondant aux modifications apportées à la trame chiffrée initiale et d'ajouter le champ de contrôle d'intégrité ainsi obtenu au champ d'intégrité de la trame chiffrée initiale pour construire une trame forgée possédant un champ de contrôle d'intégrité valide.

La technique du WEP utilise un chiffrement par « ou » exclusif avec une séquence pseudo-aléatoire produite par l'algorithme *RC*4. La graine d'initialisation pour l'algorithme *RC*4 est la concaténation de la clé symétrique de chiffrement K et du vecteur d'initialisation IV. La connaissance d'une trame cryptée et de sa version en clair permet de construire, pour le vecteur d'initialisation utilisé (IV), la séquence pseudo-aléatoire de chiffrement. Il est ensuite facile de déduire la séquence pseudo-aléatoire de chiffrement pour un autre vecteur d'initialisation $I\acute{V}$. Il suffit d'exploiter les identités suivantes :

$$\begin{aligned} RC4(y) &= RC4(x) \oplus x \oplus y \\ x &= K \parallel IV \quad \text{et} \quad y = K \parallel I\acute{V} \end{aligned}$$

avec $\parallel$ indiquant la concaténation et $\oplus$ le « ou » exclusif bit à bit. La connaissance de $RC4(x)$, la séquence aléatoire pour le vecteur d'initialisation IV, permet de calculer $RC4(y)$, la séquence aléatoire pour le vecteur d'initialisation $I\acute{V}$, sans pour autant avoir à calculer la clé de chiffrement K.

Le dernier problème est le plus grave, car il relève des difficultés inhérentes à l'algorithme de chiffrement. L'algorithme *RC*4 présente en effet des clés faibles, qui permettent de prédire avec une probabilité raisonnable certains bits de la séquence pseudo-aléatoire produite. De plus, la méthode de génération du paramètre d'initialisation x utilisé par *RC*4 dans le WEP, $x = K \parallel IV$, fournit en clair les 24 bits du paramètre d'initialisation puisqu'on connaît le vecteur d'initialisation. Suite à l'écoute passive d'un certain nombre de trames cryptées, il est dès lors possible de remonter jusqu'à la clé K de chiffrement initiale.

Il existe encore d'autres failles de conception, dont les conséquences sont généralement aussi regrettables mais qui relèvent davantage de problèmes d'implémentation que d'erreurs de conception. Par exemple, comme il existe un nombre limité de vecteurs d'initialisation $\left(2^{24}\right)$, il est facile, de trouver dans un nombre raisonnable de trames cryptées deux trames cryptées ayant le même vecteur d'initialisation.

Dans le même ordre d'idées, certaines implémentations initialisent le vecteur d'initialisation à 0 au redémarrage, ce qui facilite l'attaque sur les trames chiffrées avec le même vecteur d'initialisation.

Il existe une autre faille tout aussi gênante pour peu que l'on puisse écouter le trafic sur le réseau Ethernet derrière le point d'accès. Nous avons vu qu'il était facile de tromper le mécanisme de contrôle d'intégrité. Lorsque des trames forgées sont envoyées à un point d'accès, ce dernier relaye ces trames déchiffrées sur le réseau Ethernet câblé. Il est dès lors facile de lancer une attaque de type paquet en clair puisque la version chiffrée d'un paquet et sa version en clair, espionnée sur le réseau Ethernet, sont connues.

L'algorithme d'authentification n'est pas plus fiable. Son principe est le suivant : le point d'accès envoie un texte à la station qui souhaite s'authentifier. Cette dernière retourne ce texte chiffré par le biais du WEP. Par conséquent, si l'on connaît la clé de chiffrement ou un dictionnaire des séquences RC4 associé à cette clé, l'authentification est immédiate à obtenir. Il y a là un défaut grossier de conception, authentification et chiffrement reposant sur la même protection. Pire encore, l'authentification fournit sur un plateau à un espion une attaque de type texte en clair. En effet, le texte en clair envoyé par le point d'accès est retourné chiffré par la station qui s'authentifie, offrant ainsi à une station espion un texte en clair et sa version chiffrée.

R Les logiciels suivants sont capables de craquer le système de chiffrement WEP : **Aisnort, WEP Crack, Sniffer Wireless**.

VI.6 WPA – Wi-Fi Access Protocol et IEEE 802.11i.

Conscient des problèmes suscités par les failles de sécurité dans 802.11, un nouvel amendement 802.11*i* a été proposé sur l'amélioration de la sécurité. Cet amendement repose sur l'utilisation de différents mécanismes qui améliorent aussi bien l'authentification, le chiffrement que l'intégrité des données.

VI.6.1 IEEE 802.1x

802.1*x* est une architecture d'authentification défini par l'IEEE pour tous les réseaux issus de standards de l'IEEE 802. 802.1*x* n'a donc pas été seulement proposé pour les réseaux 802.11 mais pour tous les réseaux issus du groupe 802 Cette architecture repose sur l'utilisation du protocole d'authentification EAP (Extended Authentication Protocol) défini pour le protocole PPP et sur

l'utilisation d'un mécanisme d'authentification à savoir RADIUS (Remote Authentication Dial-ln User Service).

L'architecture 802.1*x* repose sur trois éléments : un client, un contrôleur (correspond au point d'accès dans 802.11) et un serveur d'authentification. Dans cette architecture, on suppose que le lien entre le client et le contrôleur n'est pas fiable, ainsi le contrôleur possède deux ports : un port contrôlé et un port non contrôle. Le port contrôlé qui correspond à la liaison entre le client et le contrôleur ne laisse passer que les paquets de type EAP tandis que le port non contrôlé qui relie le contrôleur au serveur d'authentification laisse passer tous les types de paquets. Une architecture incorporant la norme IEEE 802.1*x* à la norme IEEE 802.11 est illustrée par la figure VI.8. Au-dessus de la couche MAC IEEE 802.11, se trouvent la couche IEEE 802.1*x* et la couche AA (Authentication Agent). C'est cette couche qui contient le mécanisme véritable du protocole d'authentification.

L'avantage de cette technique est d'éviter les attaques de types de déni de service en rejetant tout trafic non EAP. Lorsqu'une requête EAP est envoyée du client vers le contrôleur, cette requête sera automatiquement transformée en requête RADIUS entre le contrôleur et le serveur d'authentification.

EAP a pour principal avantage de n'être qu'une enveloppe capable de transporter une multitude de schémas d'authentification tels que :

- EAP-*MD*5 qui repose sur l'utilisation de la fonction de hachage *MD*5 (Message Digest 5) ;
- EAP-TLS qui définit un tunnel TLS qui repose sur une authentification mutuelle entre le serveur d'authentification et le client sur la base d'envoi de certificats ;
- EAP-TTLS est un tunnel TLS dans lequel on incorpore un autre schéma d'authentification ;
- PEAP est un tunnel TLS encapsulé dans un autre tunnel TLS.
- LEAP (Lightweight EAP) : EAP développé par Cisco de type challenge-response basé sur un serveur RADIUS et un login/password.
- EAP-SIM : EAP utilisant le système d'authentification par carte SIM développé pour le GSM

EAP, EAP-TLS et EAP-TTLS apportent, entre autre, une gestion dynamique des clés permettant un échange de clé toutes les dix minute entre le client et le point d'accès limitant ainsi la récupération, par un attaquant, d'une quantité importante de données chiffrées utilisant la même clé lui permettant de la casser. 802.1*x* n'est destiné qu'à l'authentification des stations et ne peut en aucun cas être utilisé pour le contrôle d'intégrité ou le chiffrement des données.

FIGURE VI.8 – Architecture IEEE 802.11 incorporant IEEE 802.1*x*.

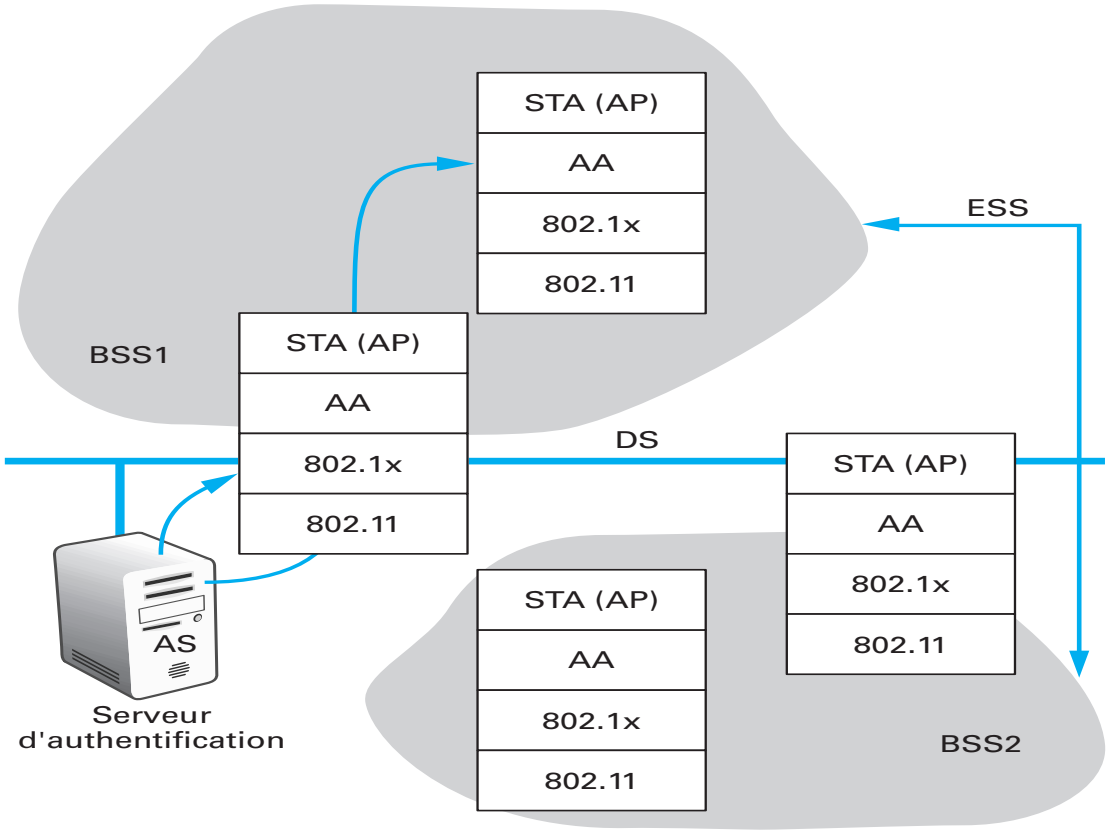


FIGURE VI.9 – Architecture d'un réseau IEEE 802.11 avec authentification IEEE 802.1x.

Le déroulement général de l'authentification est illustré par la figure VI.9. Une station (notée STA) qui souhaite s'associer à un point d'accès (noté AP) pour rejoindre le réseau envoie une requête vers ce point d'accès. Des informations d'authentification sont alors demandées à la station par le point d'accès. Les informations renvoyées par la station au point d'accès sont retransmises dans le réseau (ESS : Extended Service Set) au serveur d'authentification qui doit être atteignable par le système de distribution (noté DS) du point d'accès.

Le serveur d'authentification réalise l'authentification effective et informe le point d'accès du résultat de l'authentification. Sur le point d'accès, c'est la couche IEEE 802.1*x* qui prend en compte le filtrage des paquets reçus. Seuls les paquets provenant de stations identifiées sont traités. IEEE 802.11*i* permet d'utiliser des clés dynamiques, une fonctionnalité du protocole IEEE 802.1*x* pouvant assurer la distribution des clés. EAP-TLS permet, par exemple, à l'issue de la procédure d'authentification, de générer dynamiquement une clé de chiffrement propre à la station qui vient de s'authentifier. Cette clé est ensuite utilisée pour chiffrer les transmissions entre cette station et le point d'accès. Un renouvellement périodique et automatique des clés peut être demandé.

Cela éliminera l'une des failles les plus importantes du WEP, qui consiste en l'utilisation d'une même clé de chiffrement dans tout le réseau. Une clé différente peut être gérée par station ou même par session, l'algorithme WEP étant conservé. IEEE 802.1*x* se charge de véhiculer les clés régulièrement modifiées, par exemple par EAPTLS. Si cette voie n'offre pas une sécurité absolue, elle rend néanmoins les attaques plus difficiles du fait du changement régulier des clés. Ces améliorations sont déjà disponibles dans des produits commerciaux. Pour sécuriser l'envoi des clés, certaines implémentations utilisent l'algorithme de Diffie-Hellman.

VI.6.2 TKIP

TKIP (Temporal Key Integrity Protocol) est un protocole proposant de résoudre les problèmes du WEP à savoir la linéarité dans le contrôle d'intégrité CRC ainsi que les clés dites faibles générées par le RC4.

Pour le contrôle d'intégrité, TKIP introduit un nouvel algorithme appelé algorithme de Michaël ou MIC qui propose un nouveau contrôle d'intégrité ne possédant pas les failles du CRC. D'autre part, TKIP implémente le Fast Packet Keying défini par RSA Security. Cette méthode permet de définir une clé de chiffrement unique basée sur l'utilisation de l'adresse MAC unique combinée à la clé secrète partagée et définissant un IV qui cette fois-ci est tiré aléatoirement.Ainsi par ces deux mécanismes, TKIP résout les principaux problèmes liés au WEP. TKIP va toutefois plus loin en introduisant la fragmentation lors de l'envoi de données chiffrées où chaque fragment sera chiffré avec une clé différente.

TKIP est indépendant de l'algorithme de chiffrement, il peut se baser sur le *RC*4 ou un autre algorithme de chiffrement. Son utilisation dans 802.11*i* le destine à utiliser en remplaçant du *RC*4, AES (Advanced Encryption System), algorithme de chiffrement réputé fiable et très rapide.

VI.6.3 WPA

Sous peine de prendre du retard, les constructeurs n'ont pas pu attendre la standardisation de la norme de sécurité 802.11*i* palliant les faiblesses du WEP. Ils ont donc tout d'abord librement amélioré le protocole par des évolutions propriétaires en gardant comme base WEP et *RC*4, seul algorithme de chiffrement compatible avec la puissance de calcul des équipements actuels Ces améliorations se sont généralement basées sur les travaux du groupe de travail IEEE 802.11*i* (volet sécurité pour le 802.11) et sont désormais regroupée sous le standard WPA.

Les améliorations classiques proposées par les améliorations propriétaires du WEP sont :

— La mise en place de systèmes de management des clés de chiffrement WEP type TKIP pour doter le WEP de clés dynamiques et uniques pour chaque utilisateur. Ces systèmes nécessitent un processus d'authentification 802.1*x*/EAP pour dériver le matériel cryptographique servant à générer la clé de base et un protocole de renouvellement des clés.

— L'ajout de contrôles d'intégrité type MIC et de systèmes de vérification des séquences pour éviter qu'un attaquant puisse forger ou rejouer facilement des paquets. Ces améliorations adressent la majeure partie des vulnérabilités du WEP. Bien implémentées, la plupart de ces solutions constructeurs « WEP amélioré » offrent un niveau de sécurité satisfaisant pour des environnements où la confidentialité absolue n'est pas vitale. Elles sont cependant très dépendantes des matériels utilisés donc peu interopérables et dans l'ensemble peu pérennes.

Partant de ce principe de remplacement du WEP, la Wi-Fi Alliance s'est concentrée dès 2002 sur le développement d'un nouveau standard de sécurité. Les principaux objectifs étaient de mettre à disposition pour les fabricants courant 2003, un standard de chiffrement sûr, efficace et interopérable, facile à mettre en œuvre et ne nécessitant pas une évolution matérielle.

Cette démarche a été effectuée en accord avec l'IEEE et a abouti à une norme de sécurité intérimaire dérivée des futurs principes du 802.11*i* nommée WPA (Wi-Fi Protected Access). Dans WPA, la partie authentification type 802.1*x*/EAP sert de base à un système de chiffrement type TKIP. Le chiffrement de WPA est basé sur du WEP amélioré avec des clés dynamiques (donc au final toujours sur l'algorithme de chiffrement *RC*4) :

— L'augmentation de la taille du vecteur d'initialisation (IV) à $48bits$ avec ajout de règles de séquence.

— La gestion dynamique des clés de chiffrement WEP en dérivant la première clé de l'authentification : chaque frame802.11 possède une clé unique de chiffrement.

— Code d'intégrité du message : système Michael qui spécifie l'utilisation d'un code MIC (Message Integrity Code) permettant de vérifier l'intégrité de la trame. Ce code de 8octets est ajouté à la valeur de vérification d'intégrité (*ICV*) de 4 octets déjà présente dans le WEP. Le champ MIC est crypté avec les données de trame et la valeur *ICV* Michael fournit également une protection contre le rejeu avec l'utilisation de compteurs spécifiques.

WPA possède une compatibilité ascendante avec le 802.11*i*. Il nécessite une simple mise à jour des parties logicielles des différents composants de l'architecture WLAN pour pouvoir être utilisé. La prochaine évolution prévue pour le chiffrement est WPA2. Identique au WPA sur la partie authentification, WPA2 propose une refonte complète de la partie chiffrement sur la base des systèmes développés pour 802.11*i*. WPA2 utilise le chiffrement AES (Advanced Encryption Standard) et le protocole CCM (composé de CTR (Counter Mode Encryption), CBC (Cipher Block Chaining) et MAC (Message Authentication Code)). WPA2 n'utilise plus *RC*4 et efface donc toute trace du WEP. CCM assure des fonctionnalités équivalentes à TKIP. WPA2 nécessite un changement hardware de tous les équipements ne disposant pas de la puissance de calcul nécessaire pour exécuter AES, ce qui est le cas de la plupart des points d'accès lourds des architectures WLAN distribuées. Les WLANs agrégés ont un net avantage car WPA2 est géré sur le switch ou l'appliance WLAN, équipement qui dispose de toute la puissance nécessaire. WPA2 ne remplacera pas immédiatement WPA, surtout si ce protocole et *RC*4 ne sont pas cassés prochainement.

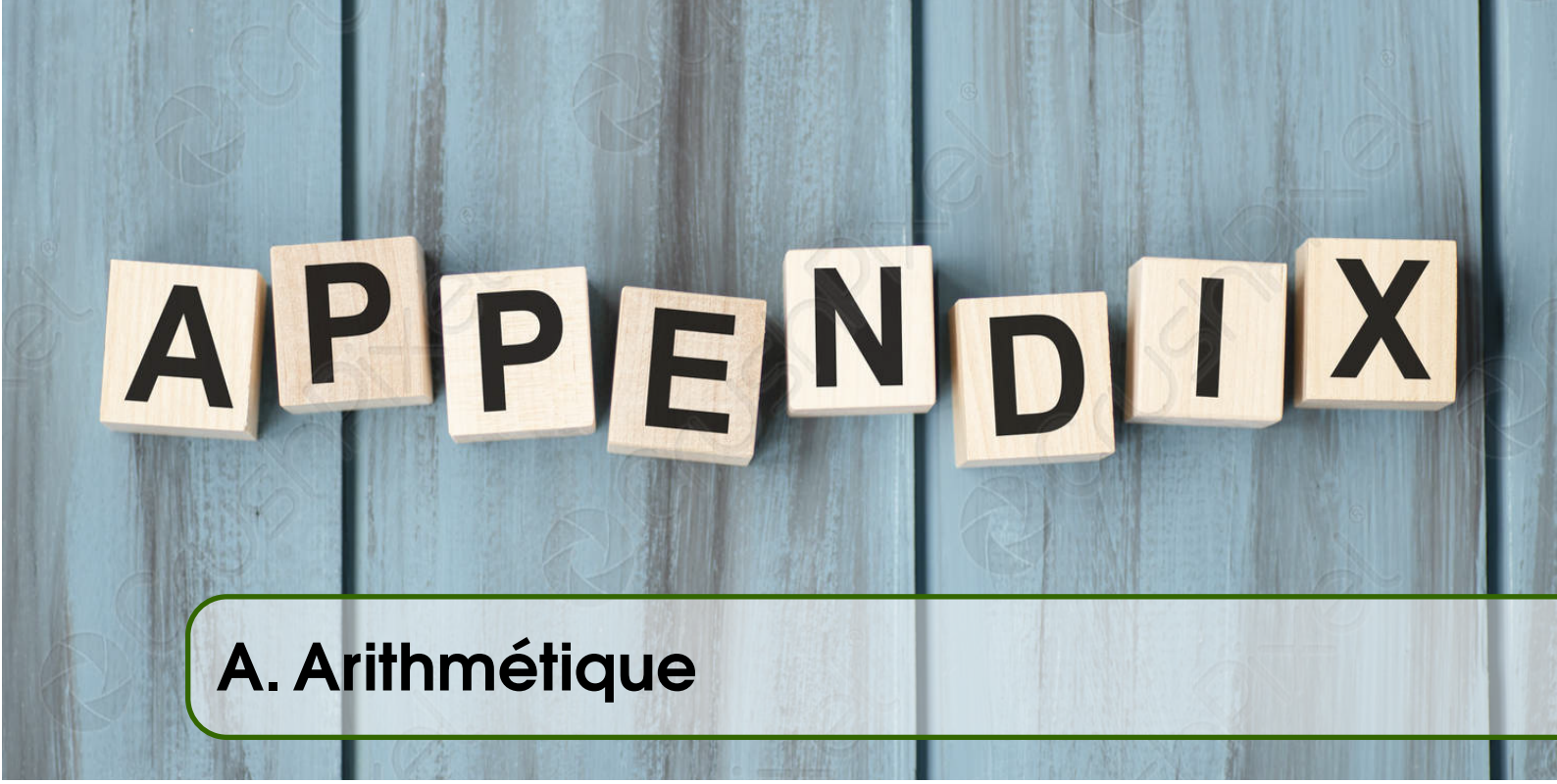
R A noter que les premières implémentations de WPA2 et d'AES commencent à être disponibles sur certains équipements. Il est cependant conseillé de conserver WPA pour le moment sur les WLANs en production.

VI.7 Chiffrement pour les WWANs/ WPANs

Dans le cadre des WWANs (Wireless Wide Area Network)ou des réseaux sans-fil étendus, et en particulier ceux sur infrastructure télécom publique, la sécurité *L*2 (Layer2, couche 2 liaison de donnée du modèle OSI) est gérée par l'opérateur. Il est important de garder à l'esprit que le chiffrement sur une communication type GSM ou GPRS est assurée par les systèmes de sécurité *L*2 uniquement sur la partie radio, entre le terminal mobile et l'antenne. En revanche, sur le réseau filaire entre l'antenne et la destination finale (le réseau de l'entreprise), le trafic traverse parfois des zones publiques peu ou pas sécurisées (réseaux inter-opérateurs, Internet...). Pour

maîtriser le chiffrement, il faut utiliser des sécurités *L*3 (Layer 3, couche 3 réseau du modèle OSI) type VPN, voir la section V.3 de chapitre V, ou du chiffrement au niveau applicatif (utilisation de SSL (Secure Sockets Layer) ou SSH (Secure Shell) par exemple).

La gestion de la confidentialité des données échangées sur un réseau ad-hoc n'a pas encore de solution satisfaisante : en effet, les possibilités de chiffrement offertes par les normes WPANs (Wireless Personal Area Network) ou les réseaux personnels sont généralement très limitées et peu paramétrables. Bluetooth propose un système de chiffrement relativement efficace mais optionnel et donc peu utilisé par les équipements. La norme 802.11 actuelle et la majorité des WPANs propriétaires ne proposent quant à eux aucun système de chiffrement correct. En attendant les prochaines solutions de chiffrement pour WPAN qui seront implémentées dans Bluetooth2 et le 802.11*i*, la meilleure protection est encore de faire en sorte qu'aucune donnée sensible ne circule sur un WPAN. La sécurité passe donc plus par la sensibilisation des utilisateurs que par un moyen technique.



A. Arithmétique

A.1 L'arithmétique pour RSA

Pour un entier n, sachant qu'il est le produit de deux nombres premiers, il est difficile de retrouver les facteurs p et q tels que $n = pq$. Le principe du chiffrement RSA, chiffrement à clé publique, repose sur cette difficulté. Dans cette partie nous mettons en place les outils mathématiques nécessaires pour le calcul des clés publique et privée ainsi que les procédés de chiffrement et déchiffrement RSA.

A.1.1 Le petit théorème de Fermat amélioré

Nous connaissons le petit théorème de Fermat

Theorem A.1.1 — Petit théorème de Fermat. Si p est un nombre premier et $a \in \mathbb{Z}$ alors $a^p \equiv a \bmod p$

et sa variante :

Notation A.1.2 Si p ne divise pas a alors $a^{p-1} \equiv 1 \bmod p$

Nous allons voir une version améliorée de ce théorème dans le cas qui nous intéresse :

Theorem A.1.3 — Indicatrice d'Euler et théorème de Fermat amélioré. Soient p et q deux nombres premiers distincts et soit $n = pq$. Pour tout $a \in \mathbb{Z}$ tel que $\text{pgcd}(a,n) = 1$ alors : $a^{(p-1)(q-1)} \equiv 1 mod n$

On note $\varphi(n) = (p-1)(q-1)$, la **fonction d'Euler**. L'hypothèse $pgcd(a,n) = 1$ équivaut ici à ce que a ne soit divisible ni par p, ni par q. Par exemple pour $p = 5, q = 7, n = 35$ et $\varphi(n) = 4 \cdot 6 = 24$. Alors pour $a = 1,2,3,4,6,8,9,11,12,13,16,17,18,...$ on a bien $a^{24} \equiv 1 \bmod 35$.

Proposition A.1.4 La fonction φ d'Euler vérifie les propriétés suivantes :

1. $\varphi(1) = 1$
2. Pour tout p premier, et tout $k \geq 1, \varphi(p^k) = p^k - p^{k-1}$.
3. Pour tout $m; n$ tels que $\text{pgcd}(m;n) = 1, \varphi(m;n) = \varphi(m)\varphi(n)$.

Démonstration. Notons $c = a^{(p-1)(q-1)}$. Calculons c modulo p :

$$c \equiv a^{(p-1)(q-1)} \equiv (a^{(p-1)})^{q-1} \equiv 1^{q-1} \equiv 1 mod\, p$$

où l'on appliquer le petit théorème de Fermat : $a^{p-1} \equiv 1 mod\, p$, car p ne divise pas a.

Calculons ce même c mais cette fois modulo q :

$$c \equiv a^{(p-1)(q-1)} \equiv (a^{(q-1)})^{p-1} \equiv 1^{p-1} \equiv 1 mod\, q$$

où l'on appliquer le petit théorème de Fermat : $a^{q-1} \equiv 1 \bmod q$, car q ne divise pas a.

Conclusion partielle : $c \equiv 1 \bmod p$ et $c \equiv 1 \bmod q$.

Nous allons en déduire que $c \equiv 1 mod\, pq$.

Comme $c \equiv 1 mod\, p$ alors il existe $\alpha \in \mathbb{Z}$ tel que $c = 1 + \alpha p$; comme $c \equiv 1 mod\, q$ alors il existe $\beta \in \mathbb{Z}$ tel que $c = 1 + \beta q$. Donc $c - 1 = \alpha p = \beta q$. De l'égalité $\alpha p = \beta q$, on tire que $p | \beta q$.

Comme p et q sont premiers entre eux (car ce sont des nombres premiers distincts) alors par le lemme de Gauss on en déduit que $p|\beta$. Il existe donc $\beta' \in \mathbb{Z}$ tel que $\beta = \beta' p$.

Ainsi $c = 1 + \beta q = 1 + \beta' pq$. Ce qui fait que $c \equiv 1 mod\, pq$, c'est exactement dire $a^{(p-1)(q-1)} \equiv 1 mod\, n$. ■

A.1.2 L'algorithme d'Euclide étendu

Nous avons déjà étudié l'algorithme d'Euclide qui repose sur le principe que $\text{pgcd}(a,b) = \text{pgcd}(b, a(\bmod b))$. On profite que assure les affectations simultanées, ce qui pour nous correspond aux suites

$$\begin{cases} a_{i+1} & = & b_i \\ b_{i+1} & \equiv & a_i \bmod b_i \end{cases}$$

initialisée par $a_0 = a$, $b_0 = b$.

Nous avons vu aussi comment « remonter » l'algorithme d'Euclide à la main pour obtenir les coefficients de Bézout u, v tels que $au + bv = pgcd(a,b)$. Cependant il nous faut une méthode plus automatique pour obtenir ces coefficients, c'est l'algorithme d'Euclide étendu.

On définit deux suites (x_i), (y_i) qui vont aboutir aux coefficients de Bézout.

L'initialisation est :

$$x_0 = 1 \qquad x_1 = 0 \qquad y_0 = 0 \qquad y_1 = 1$$

et la formule de récurrence pour $i \geq 1$:

$$x_{i+1} = x_{i-1} - q_i x_i \qquad y_{i+1} = y_{i-1} - q_i y_i$$

où q_i est le quotient de la division euclidienne de a_i par b_i.

A.1.3 Inverse modulo n

Soit $a \in \mathbb{Z}$, on dit que $x \in \mathbb{Z}$ est un inverse de a modulo n si $ax \equiv 1 \bmod n$.

Trouver un inverse de a modulo n est donc un cas particulier de l'équation $ax \equiv b \bmod n$.

Proposition A.1.5 — a admet un inverse modulo n si et seulement si a et n sont premiers entre eux.

— Si $au + nv = 1$ alors u est un inverse de a modulo n.

En d'autres termes, trouver un inverse de a modulo n revient à calculer les coefficients de Bézout associés à la paire (a,n).

Démonstration. La preuve est essentiellement une reformulation du théorème de Bézout :

$$\begin{aligned} pgcd(a,n) = 1 &\iff \exists u, v \in \mathbb{Z} \qquad au + nv = 1 \\ &\iff \exists u \in \mathbb{Z} \qquad au \equiv 1 mod n \end{aligned}$$

■

A.1.4 L'exponentiation rapide

Nous aurons besoin de calculer rapidement des puissances modulo n. Pour cela il existe une méthode beaucoup plus efficace que de calculer d'abord a^k puis de le réduire modulo n. Il faut garder à l'esprit que les entiers que l'on va manipuler ont des dizaines voire des centaines de chiffres.

Voyons la technique sur l'exemple de $5^{11} mod 14$. L'idée est de seulement calculer $5, 5^2, 5^4, 5^8 \ldots$ et de réduire modulo n à chaque fois. Pour cela on remarque que $11 = 8+2+1$ donc

$$5^{11} = 5^8 \times 5^2 \times 5^1.$$

Calculons donc les $5^{2^i} \bmod 14$:

$$\begin{aligned}
5 &\equiv 5 mod 14 \\
5^2 &\equiv 25 \equiv 11 \bmod 14 \\
5^4 &\equiv 5^2 \times 5^2 \equiv 11 \times 11 \equiv 121 \equiv 9 \bmod 14 \\
5^8 &\equiv 5^4 \times 5^4 \equiv 9 \times 9 \equiv 81 \equiv 11 \bmod 14
\end{aligned}$$

à chaque étape est effectuée une multiplication modulaire. Conséquence :

$$5^{11} \equiv 5^8 \times 5^2 \times 5^1 \equiv 11 \times 11 \times 5 \equiv 11 \times 55 \equiv 11 \times 13 \equiv 143 \equiv 3 mod 14.$$

Nous obtenons donc un calcul de $5^{11} \bmod 14$ en 5 opérations au lieu de 10 si on avait fait $5 \times 5 \times 5 \cdots$.

Voici une formulation générale de la méthode. On écrit le développement de l'exposant k en base 2 : $(k_\ell, \ldots, k_2, k_1, k_0)$ avec $k_i \in \{0,1\}$ de sorte que

$$k = \sum_{i=0}^{\ell} k_i 2^i.$$

On obtient alors

$$x^k = x^{\Sigma_{i=0}^{\ell} k_i 2^i} = \prod_{i=0}^{\ell} (x^{2^i})^{k_i}.$$

Par exemple 11 en base 2 s'écrit $(1,0,1,1)$, donc, comme on l'a vu :

$$5^{11} = (5^{2^3})^1 \times (5^{2^2})^0 \times (5^{2^1})^1 \times (5^{2^0})^1.$$

Voici un autre exemple : calculons $17^{154} \bmod 100$. Tout d'abord on décompose l'exposant $k = 154$ en base 2 : $154 = 128+16+8+2 = 2^7+2^4+2^3+2^1$, il s'écrit donc en base 2 : $(1,0,0,1,1,0,1,0)$.

Ensuite on calcule $17, 17^2, 17^4, 17^8, ..., 17^{128}$ modulo 100.

$$17 \equiv 17 \bmod 100$$
$$17^2 \equiv 17 \times 17 \equiv 289 \equiv 89 \bmod 100$$
$$17^4 \equiv 17^2 \times 17^2 \equiv 89 \times 89 \equiv 7921 \equiv 21 \bmod 100$$
$$17^8 \equiv 17^4 \times 17^4 \equiv 21 \times 21 \equiv 441 \equiv 41 \bmod 100$$
$$17^{16} \equiv 17^8 \times 17^8 \equiv 41 \times 41 \equiv 1681 \equiv 81 \bmod 100$$
$$17^{32} \equiv 17^{16} \times 17^{16} \equiv 81 \times 81 \equiv 6561 \equiv 61 \bmod 100$$
$$17^{64} \equiv 17^{32} \times 17^{32} \equiv 61 \times 61 \equiv 3721 \equiv 21 \bmod 100$$
$$17^{128} \equiv 17^{64} \times 17^{64} \equiv 21 \times 21 \equiv 441 \equiv 41 \bmod 100$$

Il ne reste qu'à rassembler :

$$17^{154} \equiv 17^{128} \times 17^{16} \times 17^8 \times 17^2 \equiv 41 \times 81 \times 41 \times 89 \equiv 3321 \times 3649 \equiv 21 \times 49 \equiv 1029 \equiv 29 \bmod 100$$

A.2 Calcul de la clé publique et de la clé privée

A.2.1 Choix de deux nombres premiers

Alice effectue, une fois pour toute, les opérations suivantes (en secret) :

— elle choisit deux nombres premiers distincts p et q (dans la pratique ce sont de très grands nombres, jusqu'à des centaines de chiffres),

— Elle calcule $n = p \times q$,

— Elle calcule $\varphi(n) = (p-1) \times (q-1)$.

Exemple 1.

— $p = 5$ et $q = 17$

— $n = p \times q = 85$

— $\varphi(n) = (p-1) \times (q-1) = 64$

Vous noterez que le calcul de $\varphi(n)$ n'est possible que si la décomposition de n sous la forme $p \times q$ est connue. D'où le caractère secret de $\varphi(n)$ même si n est connu de tous.

Exemple 2.

— $p = 101$ et $q = 103$

— $n = p \times q = 10\,403$

— $\varphi(n) = (p-1) \times (q-1) = 10\,200$

A.2.2 Choix d'un exposant et calcul de son inverse

Alice continue :

— elle choisit un exposant e tel que $pgcd(e, \varphi(n)) = 1$,

— elle calcule l'inverse d de e module $\varphi(n)$: $d \times e \equiv 1 mod \varphi(n)$. Ce calcul se fait par l'algorithme d'Euclide étendu.

Exemple 1.

— Alice choisit par exemple $e = 5$ et on a bien $pgcd(e, \varphi(n)) = pgcd(5, 64) = 1$,

— Alice applique l'algorithme d'Euclide étendu pour calculer les coefficients de Bézout correspondant à $pgcd(e, \varphi(n)) = 1$. Elle trouve $5 \times 13 + 64 \times (-1) = 1$. Donc $5 \times 13 \equiv 1 mod 64$ et l'inverse de e modulo $\varphi(n)$ est $d = 13$.

Exemple 2.

— Alice choisit par exemple $e = 7$ et on a bien $pgcd(e, \varphi(n)) = pgcd(7, 10\,200) = 1$,

— L'algorithme d'Euclide étendu pour $pgcd(e, \varphi(n)) = 1$ donne $7 \times (-1457) + 10\,200 \times 1 = 1$. Mais $-1457 \equiv 8743 mod \varphi(n)$, donc pour $d = 8743$ on a $d \times e \equiv 1 mod \varphi(n)$.

A.2.3 Clé publique

La clé publique d'Alice est constituée des deux nombres : n et e

Et comme son nom l'indique Alice communique sa clé publique au monde entier.

Exemple 1. $n = 85$ et $e = 5$

Exemple 2. $n = 10\,403$ et $e = 7$

A.2.4 Clé privée

Alice garde pour elle sa clé privée : d

Alice détruit en secret p, q et $\varphi(n)$ qui ne sont plus utiles. Elle conserve secrètement sa clé privée.

Exemple 1. $d = 13$

Exemple 2. $d = 8743$

A.3 Chiffrement du message

Bob veut envoyer un message secret à Alice. Il se débrouille pour que son message soit un entier (quitte à découper son texte en bloc et à transformer chaque bloc en un entier).

A.3.1 Message

Le message est un entier m, tel que $0 \leq m < n$.

Exemple 1. Bruno veut envoyer le message $m = 10$.

Exemple 2. Bruno veut envoyer le message $m = 1234$.

A.3.2 Message chiffré

Bruno récupère la clé publique d'Alice : n et e avec laquelle il calcule, à l'aide de l'algorithme d'exponentiation rapide, le message chiffré : $x \equiv m^e \bmod n$

Il transmet ce message x à Alice

Exemple 1. $m = 10$, $n = 85$ et $e = 5$ donc

$$x \equiv m^e \bmod n \equiv 10^5 \bmod 85$$

On peut ici faire les calculs à la main :

$$\begin{aligned} 10^2 &\equiv 100 \equiv 15 \bmod 85 \\ 10^4 &\equiv (10^2)^2 \equiv 15^2 \equiv 225 \equiv 55 \bmod 85 \\ x &\equiv 10^5 \equiv 10^4 \times 10 \equiv 55 \times 10 \equiv 550 \equiv 40 \bmod 85 \end{aligned}$$

Le message chiffré est donc $x = 40$.

Exemple 2. $m = 1234$, $n = 10\,403$ et $e = 7$ donc

$$x \equiv m^e \bmod n \equiv 1234^7 \bmod 10\,403$$

On utilise l'ordinateur pour obtenir que $x = 10\,378$.

A.4 Déchiffrement du message

Alice reçoit le message x chiffré par Bob, elle le décrypte à l'aide de sa clé privée d, par l'opération :

$m \equiv x^d \bmod n$ qui utilise également l'algorithme d'exponentiation rapide.

Nous allons prouver dans le lemme A.4.2, que par cette opération Alice retrouve bien le message original m de Bob.

Exemple 1. $c = 40$, $d = 13$, $n = 85$ donc

$$x^d \equiv (40)^{13} \bmod 85.$$

Calculons à la main $40^{13} \equiv mod 85$ on note que $13 = 8+4+1$, donc $40^{13} = 40^8 \times 40^4 \times 40$.

$$40^2 \equiv 1600 \equiv 70 \bmod 85$$
$$40^4 \equiv (40^2)^2 \equiv 70^2 \equiv 4900 \equiv 55 \bmod 85$$
$$40^8 \equiv (40^4)^2 \equiv 55^2 \equiv 3025 \equiv 50 \bmod 85$$

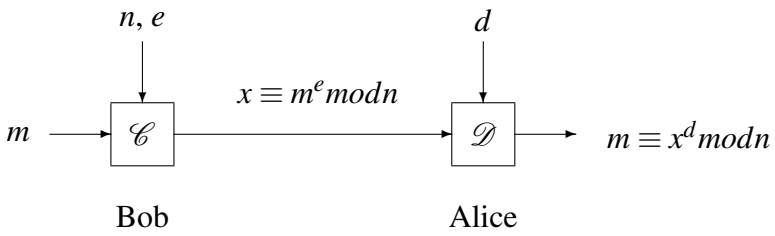
Donc

$$x^d \equiv 40^{13} \equiv 40^8 \times 40^4 \times 40 \equiv 50 \times 55 \times 40 \equiv 10 mod 85$$

qui est bien le message m de Bruno.

Exemple 2. $c = 10\,378$, $d = 8743$, $n = 10\,403$. On calcule par ordinateur $x^d \equiv (10\,378)^{8743} \bmod 10\,403$ qui vaut exactement le message original de Bruno $m = 1234$.

A.4.1 Schéma



Clés d'Alice :

— publique : n, e

— privée : d

A.4.2 Lemme de déchiffrement

Le principe de déchiffrement repose sur le petit théorème de Fermat amélioré.

Soit d l'inverse de e modulo $\varphi(n)$. Si $x \equiv m^e \bmod n$ alors $m \equiv x^d \bmod n$.

Ce lemme prouve bien que le message original m de Bruno, chiffré par clé publique d'Alice (e,n) en le message x, peut-être retrouvé par Alice à l'aide de sa clé secrète d.

Démonstration. — Que d soit l'inverse de e modulo $\varphi(n)$ signifie $d \cdot e \equiv 1 mod \varphi(n)$. Autrement dit, il existe $k \in \mathbb{Z}$ tel que $d \cdot e = 1 + k \cdot \varphi(n)$.

— On rappelle que par le petit théorème de Fermat généralisé : lorsque m et n sont premiers entre eux

$$m^{\varphi(n)} \equiv m^{(p-1)(q-1)} \equiv 1 \bmod n$$

— **Premier cas** $\text{pgcd}(m,n) = 1$.

Notons $x \equiv m^e \bmod n$ et calculons x^d :

$$x^d \equiv (m^e)^d \equiv m^{e \cdot d} \equiv m^{1+k \cdot \varphi(n)} \equiv m \cdot m^{k \cdot \varphi(n)} \equiv m \cdot (m^{\varphi(n)})^k \equiv m \cdot (1)^k \equiv m \bmod n$$

— **Deuxième cas** $pgcd(m,n) \neq 1$.

Comme n est le produit des deux nombres premiers p et q et que m est strictement plus petit que n alors si m et n ne sont pas premiers entre eux cela implique que p divise m ou bien q divise m (mais pas les deux en même temps). Faisons l'hypothèse $\text{pgcd}(m,n) = p$ et $\text{pgcd}(m,q) = 1$, le cas $\text{pgcd}(m,n) = q$ et $\text{pgcd}(m,p) = 1$ se traiterait de la même manière. Étudions $(m^e)^d$ à la fois modulo p et modulo q à l'image de ce que nous avons fait dans la preuve du théorème de Fermat amélioré.

— modulo p : $m \equiv 0 \bmod p$ et $(m^e)^d \equiv 0 mod p$ donc $(m^e)^d \equiv m \bmod p$,

— modulo q : $(m^e)^d \equiv m \times (m^{\varphi(n)})^k \equiv m \times (m^{q-1})^{(p-1)k} \equiv m \bmod q$.

Comme p et q sont deux nombres premiers distincts, ils sont premiers entre eux et on peut écrire comme dans la preuve du petit théorème de Fermat amélioré que

$$(m^e)^d \equiv m \bmod n$$

■

Références bibliographiques

Polycopiés de cours

[AF21] Bodin ARNAUD et Recher FRANÇOIS. *Exo7 Chapitre 3 : Cryptographie*. Polycopié de cours. Université Lille 1 1, 2021.

[Bac18] Christine BACHOC. *Codes et Cryptologie*. Polycopié de cours. Université Bordeaux 1, 2018.

Articles

[AD04] Mohammed ACHEMLAL et Michel DUDET. “Technologies VPN”. In : *Techniques de l’ingénieur. Sécurité des systèmes d’information* H5610 (2004).

[ANS20] ANSSI-PG-083. “Règles et recommandations concernant le : guide des mécanismes cryptographiques”. In : *Agence nationale de la sécurité des systèmes d’information* (2020).

[MüH03] Paul MÜHLETHALER. “Sécurité dans les réseaux sans fil : Norme IEEE 802.11”. In : *Techniques de l’ingénieur. Sécurité des systèmes d’information* TE7377 (2003), TE7377-1.

Livres

[Blo+13] Laurent BLOCH et al. *Sécurité informatique : Principes et méthodes à l’usage des DSI, RSSI et administrateurs*. Editions Eyrolles, 2013.

[FSK11] Niels FERGUSON, Bruce SCHNEIER et Tadayoshi KOHNO. *Cryptography engineering : design principles and practical applications*. John Wiley & Sons, 2011.

[Gér09] Aurélien GÉRON. *WiFi Professionnel-3e édition- : La norme 802.11, le déploiement, la sécurité*. Dunod, 2009.

[HH15] Delfs HANS et Knebl HELMUT. *Introduction to Cryptography : Principles and Applications*. 3rd. Springer, 2015. ISBN : 3662479737, 978-3662479735.

[Mar04] Bruno MARTIN. *Codage, cryptologie et applications*. Collection technique et scientifique des télécommunications. Presses polytechniques et universitaires romandes, 2004. ISBN : 9782880745691.

[Paq09] Catherine PAQUET. *Implementing Cisco IOS Network Security (IINS) : (CCNA Security exam 640-553) (Authorized Self-Study Guide)*. 1 Stg. Cisco Press, 2009.

[Puj14] Guy PUJOLLE. *Les réseaux*. Editions Eyrolles, 2014.

[Ser09] Claude SERVIN. *Réseaux & télécoms*. Dunod, Paris, 2009.

[Sta10] William STALLINGS. *Cryptography and Network Security : Principles and Practice*. 5th. USA : Prentice Hall Press, 2010. ISBN : 0136097049.

[WMG12] Michael E WHITMAN, Herbert J MATTORD et Andrew GREEN. *Guide to firewalls and VPNs*. Cengage Learning, 2012.

[Wri12] Tyler WRIGHTSON. *Wireless Network Security A Beginner's Guide*. McGraw Hill Professional, 2012.

Thèses de doctorat

[MEK17] Tahar MEKHAZNIA. "Analyse cryptographique par les méthodes heuristiques". Thèse de doctorat. Université Mustapha Ben Boulaid Batna 2, 2017.

[Wur15] Antoine WURCKER. "Etude de la sécurité d'algorithmes de cryptographie embarquée vis-a-vis des attaques par analyse de la consommation de courant". Thèse de doctorat. Université de Limoges, 2015.