# Exigences pour les protocoles sécurité

Sécurité des réseaux, systèmes et objets connectés - M. GBENOU

## Introduction

Dans le domaine de la sécurité, des réseaux (KevBeros, SSL, SSH, SFTP (transfert de fichier), IPSEC (routeur, cryptage… etc.)) il existe plusieurs solutions.

L’IETF a permis l’élaboration des protocoles SSL/TLC (RFC 3546) défini pour les réseaux mobiles.

Actuellement les applications essayent de choisir suivant particularité de chaque protocole de sécurité celles qui correspond le plus à leurs besoins. Par conséquent la conception ou le développement de nouveaux protocoles de sécurité exige une définition claire des exigences et des services que peut présenter ce protocole. Pour cela un nouveau protocole de sécurité peut partager avec les autres solutions certains services tels que l’authentification, l’intégrité et la confidentialité. Mais il doit aussi avoir c’est propres avantages qu’il le diffère des solutions existants.

## Exigences en termes de sécurité

### 1 – Choix des mécanismes cryptographiques :

Dans la plupart des protocoles de sécurités on peut diviser les cryptographies en 2 grandes catégories :

1 - Phase d’initialisation : Basé sur le chiffrement asymétrique clé public/privé

2 - Initialisation des données : Alors que cette phase est basé sur le chiffrement symétrique (clé secret)

La technologie du chiffrement asymétrique est moins performante que celle du chiffrement symétrique (voir figure 1) on utilise en général le chiffrement symétrique pour chiffrer les données ou l’information dont on doit protéger la confidentialité et l’intégrité. A travers la phase d’initialisation une liste d’algorithmes de chiffrement de hachage et de signature est négociée entre les 2 communicateurs. Un protocole de sécurité doit assurer la négociation de cette liste mais en incluant les algorithmes jugé sûr.

Pour les algorithmes à chiffrement symétrique une attaque exhaustive est hors de portée dès que l’espace des clés et suffisant grand minimum 64 bits soit 8 octets.

Pour les algorithmes à chiffrement asymétrique la sécurité repose principalement sur la factorisation le grand entier « n » le plus grand nombre ordinaire factorisé à ce jour et un nombre de 576 bits soit 72 octets.

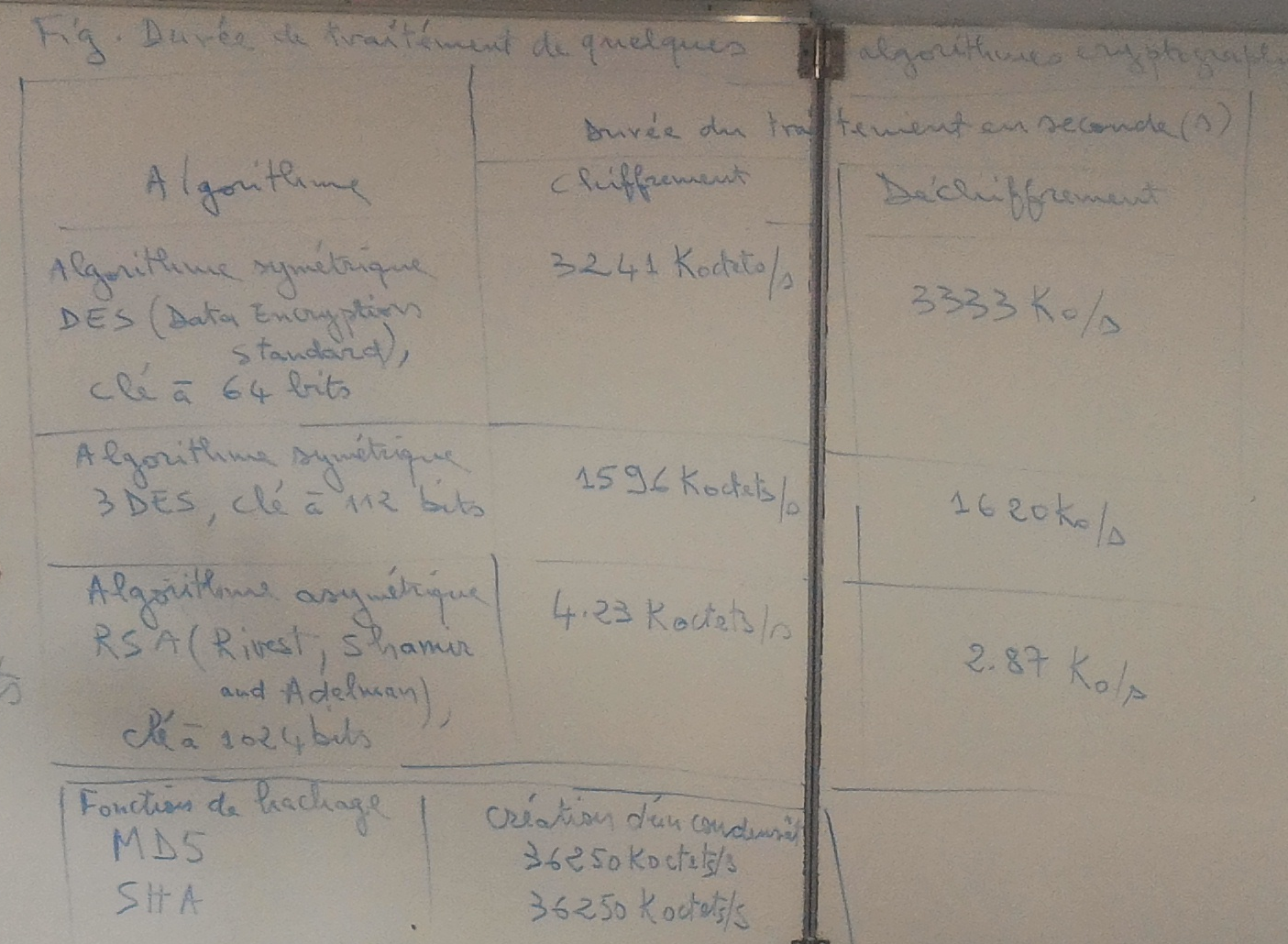


Figure n°1

### 2 – Authentification / identification

Le service d’authentification permet d’assurer qu’une communication est authentique. Alors on peut distinguer 2 types d’authentifications :

1 - Authentification d’un tiers : Consiste pour ce dernier à prouver son identité.

2 - Authentification de la source de données : Toujours vérifier la source de données avant de diffuser. Sert à prouver que la donnée reçue vienne bien de tel émetteur déclarer.

La signature numérique peut servir aussi à l’identification. L’authentification nécessite de fournir une identification est de la prouver. Sur la plupart des réseaux le mécanisme d’authentification utilise une paire loggin/mdp (le plus souvent utilisé). Cependant en raison de la vulnérabilité constamment associé à l’utilisation des mots de passes.

Il est souvent recommandé de recourir à des mécanismes plus robustes tel que l’authentification par des certificats ISO-9594, des clés publiques (RIV78) ou à travers des centres de distributions de clés (RFC 1510) (SMS envoyé par les banques lors d’achat… etc.).

### 3 – Intégrité

L’intégrité ce rapport à la protection contre les changements et altérations. Il y a intégrité si les données émises sont identique à celle reçu. Des différences peuvent apparaitre si quelqu’un tente de modifier ces données ou tout simplement s’il y a des problèmes de réception ou de transmission.

Ces techniques utilisées pour faire face à ceux-là sont les bits parité/LRC/URC/CRC… Ces mécanismes ne peuvent garantir absolument l’intégrité. Il est possible que les données altérer et la même sommes de contrôle. Il est aussi possible que l’attaquant/hacker modifier les données et recalculer le résultat des fonctions de hachage (empreinte digital). Pour que seul l’expéditeur soit capable de modifier l’emprunt a utilisé des fonctions de hachage avec des clés secrètes ou privée. Dans ce cas on garantit à la fois l’intégrité et l’authentification. Ces 2 services de sécurité sont souvent fournis par les mêmes mécanismes pour la simple raison qui n’ont de sens qu’accompagner l’un de l’autre.

### 4 – Confidentialité

La confidentialité c’est un service de sécurité consistant à s’assurer que seule la personne autoriser pour prendre connaissances des données.

Pour obtenir ce service ont utilisé généralement le chiffrement de données à l’aide de la cryptographie. Si seules les données sont chiffrées une oreille espionne peut tout de même écouter les informations de l’entête.

Elle peut ainsi, à partir des adresses sources et destinations identifier les tiers communicants et analyser leurs communications :

- Fréquence des envois, quantité de données échanges…

On parle de protection contre l’analyse de trafic lorsqu’en plus de la confidentialité ont garantie l’impossibilité de connaitre ces informations.

L’authentification, l’intégrité et la confidentialité vont souvent ensemble et offre la base des services de sécurité.

### 5 – Non-répudiation

On distingue 2 types de services de non-répudiation :

1. La non-répudiation de l’origine qui protège un destinataire confronté à un expéditeur niant avoir reçu un message.
2. La non-répudiation de la réception qui joue le rôle inverse du précédent. A savoir démontrer que le destinataire a bien reçu le message envoyé par l’expéditeur.

Dans le cas de cryptographie à clé publique chaque utilisateur et le seul et unique détendeur de la clé privé. Ainsi, tout message accompagner de la signature électronique d’un utilisateur ne pourra être répudié par celui-ci à moins que tous le système n’est était pénétré.

A l’opposer la non-répudiation n’est pas directement acquise dans les systèmes utilisant des clés secrets. La clé de chiffrement étant distribuée par le serveur de distribution de clés aux 2 parties un utilisateur peut nier avoir envoyé le message en question en alléguant que la clé secret partagé a été divulgué par une compromission du destinataire soit par une attaque réussie contre le serveur de distribution de clés.

La non-répudiation de la réception peut se faire en obliger le destinataire a envoyé un accusé signer et horodaté.

### 6 – Protection contre les attaques actives et passives

La catégorie principale d’attaque sur les protocoles de sécurité et l’attaque active. Cette attaque la modification du flot de données ou la création d’un flot frauduleux.

**Attaque actives :**

1 - L’homme du milieu : C’est une attaque qui a lieu lorsqu’une entité prétend être une autre entité. Dans la plupart du temps c’est avec un détournement de flux pour rediriger le flux des 2 bouts vers lui. Ceci afin de surveiller tous les trafics réseaux et de le modifier à sa guise ou l’obtention de toutes types d’informations.

2 - Le rejeu de packets : Il implique la capture passive de données et la retransmission ultérieur en vue de produire un effet non autorisé (Surcharger, bloquer le réseau… etc.). Pour empêcher ce types d’attaque on utilise les nombres aléatoires dans les messages envoyés.

3 - La modification des messages : Celui-ci signifie que certaines portion de message légitime sont altérer (message tronquer), retarder ou bien réorganiser. Ce type de message est souvent utiliser avec UDP. Par exemple c’est le cas du protocole ISAKMP.

4 - Le déni de services : Cette attaque porte bien son nom puisque elle aboutira à l’indisponibilité des services, de la machine visée ou même du réseau visé. Cette attaque vise surtout l’exploitation d’une mauvaise implémentation du protocole ou des faiblesses de celui-ci. Le déni de services peut prendre 2 formes :

a – Vise la vulnérabilité des protocoles de transports qu’ils utilisent. Tels que les attaques sur le protocole IP SPOFY et TCP SYNFlooding, UDPFlooding.

b – Porte sur la phase d’initialisation de ces protocoles comme le protocole IKE, HandShake utiliser par CCTLS (réseaux bancaire principalement)...

**Attaque passives :**

Cette catégorie d’attaques est plus difficile à détecter car elle ne pose aucune altération des données. Le but est de collecter des informations qui ont été transmisse, afin d’analyser le contenue et ensuite de mener des attaques actives (Cheval de Troie). Ainsi grâce aux attaques dites passives il est possible de récupérer les informations (tels que l’IP, Port, environnement de travail… etc.) pour mener l’attaque active.

### 7 – La protection d’identité

La vérification efficace des évènements liées à la sécurité ce fonde aussi sur la capacité d’identifier chaque utilisateurs, donc il est très important que chaque utilisateur d’internet est une identité distinct. L’identité distincte de l’utilisateur est une combinaison qui donne le nom de l’utilisateur et possiblement celui de son ordinateur, de son organisation et de son pays.

Donc cela va permettre de protéger le réseau contre les attaques malveillantes qui va provoquer un disfonctionnement de mon réseau. Dans la plupart des cas l’identité du récepteur généralement un générateur (serveur) est publique pour cela il y a un protocole doit surtout protéger l’identité de l’initiateur (généralement les clients).

### 8 – Protection des échanges ou la protection du réseau

Par rapport au couche OSI (Open System Interconnexion) de l’ISO le protocole et service de sécurité son insérer a divers emplacement de la pile de communication.

Tableau emplacement des protocoles dans le modèle OSI :

|  |  |
| --- | --- |
| Couches OSI | Protocoles d’internet |
| 7 - Applications | SMTP, PoP, IMAP, http, FTP| SET |PKI |ISAKMP, IKE |
| 6 – Présentation | HTML, XML, BASE 64, MIME, CMS, SMIME| |
| 5 - Sessions | TLS | SSH |
| 4 - Transport | TCP | UDP |
| 3 – Réseau | IP, ICMP, RIP, IPSEC |
| 2 - Liaison | PAP, CHAP, RADIUS |
| 1 - Physique | Tous supports de transmissions |

Le choix de l’emplacement dépend des exigences c’est-à-dire des menaces qu’il peut rencontrer donc chaque emplacement offre des avantages et des inconvénients. Le chiffrement au milieu de la pile de communication offre un chiffrement indépendant des applications et il est transparent pour celle-ci. Le chiffrement au niveau applicatif permet de transmettre les données par l’intermédiaire de de relais multiple afin d’atteindre la destination final. Le chiffrement et le déchiffrement sont réaliser à chaque extrémité : on peut parler de communication de bout en bout.