Chapitre 4

PROTOCOLES SÉCURISÉS

Introduction

- **Protocoles sécurisés**
  - Inclus dans la couche application

Modèle TCP/IP	Pile de protocoles
4 – couche application	HTTP, SMTP, FTP, SSH, IRC, SNMP, DHCP, POP3 …
	HTML, MIME, ASCII
	TLS, SSL, NetBIOS, SET, Secure Shell SSH, RTSP, S-HTTP
3 – couche de transport	TCP, UDP, SCTP, RTP, DCCP …
2 – couche internet	IPv4, IPv6, ARP, IPX …
1 – couche d'accès réseau	Ethernet, 802.11 WiFi, Token ring, FDDI …
	Câble, fibre optique, ondes radio ….

Protocole SSL / TLS

Protocoles

- **SSL**
  - Introduction
  - Propriétés
  - SSL et TLS
- **SSH**
- **S-HTTP**
- **SET**
- **S/MIME**

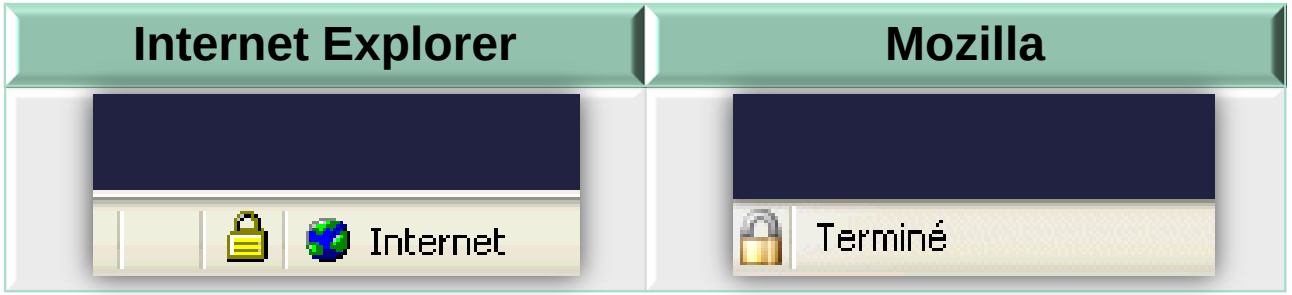
- **Introduction à SSL**
  - SSL = Secure Sockets Layers
  - Standard SSL :
    - mis au point par Netscape,
    - en collaboration avec Mastercard, Bank of America, MCI et Silicon Graphics.
  - Procédé de :
    - sécurisation des transactions effectuées via Internet.
    - cryptographie par clef publique afin de garantir la sécurité de la transmission de données sur internet.
  - Principe :
    - Etablir un canal de communication sécurisé (chiffré) entre deux machines (un client et un serveur) après une étape d'authentification.

Protocole SSL / TLS

Protocoles

- **SSL**
  - Introduction
  - Propriétés
  - SSL et TLS
- **SSH**
- **S-HTTP**
- **SET**
- **S/MIME**

- **Propriétés**
  - Système SSL indépendant du protocole utilisé, pouvant sécuriser :
    - des transactions faites par le protocole HTTP,
    - des connexions via le protocole FTP, POP ou IMAP.
  - SSL est transparent pour l'utilisateur.
  - SSL supporté par la quasi intégralité des navigateurs.



  - URL d'un serveur web securisé par SSL :
    - Commence par https://
    - Le « s » signifie « secured / sécurisé ».

Protocole SSL / TLS

Protocoles

- **SSL**
  - Introduction
  - Propriétés
  - SSL et TLS
- **SSH**
- **S-HTTP**
- **SET**
- **S/MIME**

- **SSL 2.0**
  - Principe de la création de la clé de session :
    1. Connexion du client au site marchand sécurisé par SSL :
       - Demande de authentification.
       - Envoi de la liste des cryptosystèmes qu'il supporte, triée par ordre décroissant selon la longueur des clés.
    2. Réponse du serveur au client :
       - Envoi un certificat au client, contenant la clé publique du serveur, signée par une autorité de certification (CA),
       - Envoi du nom du cryptosystème le plus haut dans la liste avec lequel il est compatible.
    3. Réponse du client au serveur :
       - Vérification de la validité du certificat
       - Création d'une clé secrète aléatoire
       - Chiffrement de la clé à l'aide de la clé publique du serveur
       - Envoi du résultat (la clé de session) au serveur
       - Le serveur est en mesure de déchiffrer la clé de session avec sa clé privée.

Protocole SSL / TLS

Protocoles

- **SSL**
  - Introduction
  - Propriétés
  - SSL et TLS
- **SSH**
- **S-HTTP**
- **SET**
- **S/MIME**

- **SSL 3.0**
  - Authentification mutuelle entre le serveur et le client
- **TLS 1.0**
  - Correspondant à SSL 3.1
  - SSL 3.0 et TLS 1.0 non interopérables
    - Compatibilité ascendant de TLS avec SSL.
  - TLS diffère de SSL pour générer les clés symétriques :
    - Génération plus sécurisée dans TLS que dans SSL 3.0
  - Par abus de langage, on parle de SSL pour désigner indifféremment SSL ou TLS.
  - Nouvelles versions :
    - TLS 1.1 en 2006
    - TLS 1.2 en 2008

Protocole SSH

Protocoles

- **SSL**
- **SSH**
  - Telnet / SSH
  - SSH
  - Principe
  - Canal sécurisé
  - Authentification
- **S-HTTP**
- **SET**
- **S/MIME**

- **Introduction**
  - Protocole Telnet
    - Permet d'effectuer ces tâches distantes possédaent l'inconvénient majeur de faire circuler en clair sur le réseau les informations échangées.
    - Attaques faciles
      - Ainsi, un pirate situé sur un réseau entre l'utilisateur et la machine distante a la possibilité d'écouter le traffic,
      - le pirate obtient un accès à un compte sur la machine distante et peut éventuellemen et étendre ses privilèges sur la machine afin d'obtenir un accès administrateur (root).
  - Protocole SSH (Secure Shell)
    - Permet à des utilisateurs (ou bien des services TCP/IP) d'accéder à un machine à travers une communication chiffrée (appelée tunnel).

Protocole SSH

Protocoles

- **SSL**
- **SSH**
  - Telnet / SSH
  - SSH
  - Principe
  - Canal sécurisé
  - Authentification
- **S-HTTP**
- **SET**
- **S/MIME**

- **Le protocole SSH**
  - SSH = Secure Shell
  - Mis au point en 1995 par le Finlandais Tatu Ylönen.
  - Intérêt :
    - Permet à un client d'ouvrir une session interactive sur une machine distante (serveur) afin d'envoyer des commandes ou des fichiers de manière sécurisée :
      - Les données circulant entre le client et le serveur sont chiffrées, ce qui garantit leur confidentialité.
      - Le client et le serveur s'authentifient mutuellement.

Protocole SSH

Protocoles

- **SSL**
- **SSH**
  - Telnet / SSH
  - SSH
  - Principe
  - Canal sécurisé
  - Authentification
- **S-HTTP**
- **SET**
- **S/MIME**

- **Le protocole SSH**
  - Version 1 : SSH1
    - proposée dès 1995
    - alternative aux sessions interactives (shells) telles que Telnet, rsh, rlogin et rexec.
    - faille permettant à un pirate d'insérer des données dans le flux chiffré.
  - Version 2 : SSH2
    - proposée en 1997
    - solution de transfert de fichiers sécurisé
      - SFTP, Secure File Transfer Protocol.

Protocole SSH

- **Fonctionnement de SSH**
  - Etablissement d'une connexion SSH :
    1. Le serveur et le client s'identifient mutuellement afin de mettre en place un canal sécurisé (couche de transport sécurisée).
    2. Le client s'authentifie auprès du serveur pour obtenir une session.

Protocole SSH

Protocoles

- **SSL**
- **SSH**
  - Telnet / SSH
  - SSH
  - Principe
  - Canal sécurisé
  - Authentification
- **S-HTTP**
- **SET**
- **S/MIME**

- **Mise en place du canal sécurisé**
  1. phase de négociation entre le client et le serveur :
     - s'entendre sur les méthodes de chiffrement à utiliser.
  2. le serveur envoie sa clé publique d'hôte (host key) au client.
  3. le client génère une clé de session de 256 bits chiffrée grâce à la clé publique du serveur
  4. envoie au serveur la clé de session chiffrée ainsi que l'algorithme utilisé.
  5. le serveur déchiffre la clé de session grâce à sa clé privée
  6. le serveur envoie un message de confirmation chiffré à l'aide de la clé de session.
  7. Les communications sont chiffrées grâce à un algorithme de chiffrement symétrique en utilisant la clé de session

Protocole SSH

Protocoles

- **SSL**
- **SSH**
  - Telnet / SSH
  - SSH
  - Principe
  - Canal sécurisé
  - Authentification
- **S-HTTP**
- **SET**
- **S/MIME**

- **L'authentification**
  - Une fois la connexion sécurisée mise en place entre le client et le serveur, le client doit s'identifier sur le serveur afin d'obtenir un droit d'accès.
  - Il existe plusieurs méthodes :
    - La plus connue : le traditionnel mot de passe.
      1. Le client envoie au serveur en mode « sécurisé » :
         - un nom d'utilisateur ,
         - et un mot de passe
      2. Le serveur vérifie si l'utilisateur concerné a accès à la machine et si le mot de passe fourni est valide
    - La moins connue : l'utilisation de clés publiques.
      1. Si l'authentification par clé est choisie par le client, le serveur va créer un challenge,
      2. Si ce dernier parvient à déchiffrer le challenge avec sa clé privée, le serveur va donner un accès au client

Protocole Secure HTTP (S-HTTP)

Protocoles

- **SSL**
- **SSH**
- **S-HTTP**
  - Introduction
  - Principe
  - S-HTTP / SSL
- **SET**
- **S/MIME**

- **Introduction**
  - S-HTTP (Secure HTTP) :
    - procédé de sécurisation des transactions HTTP
    - mis au point en 1994 par l'EIT (Enterprise Integration Technologies).
    - Fournit une sécurisation des échanges lors de transactions de commerce électronique en cryptant les messages afin de garantir aux clients la confidentialité de :
      - leur numéro de carte bancaire,
      - ou de tout autre information personnelle.

Protocole Secure HTTP (S-HTTP)

Protocoles

- **SSL**
- **SSH**
- **S-HTTP**
  - Introduction
  - Principe
  - S-HTTP / SSL
- **SET**
- **S/MIME**

- **Fonctionnement de S-HTTP**
  - Messages S-HTTP basés sur trois composantes :
    1. Le message HTTP
    2. Les préférences cryptographiques de l'envoyeur
    3. Les préférences du destinataire
  - Décryptage S-HTTP par le destinataire :
    1. Analyse des en-têtes du message afin de déterminer le type de méthode qui a été utilisé pour crypter le message.
    2. Puis déchiffrement du message grâce à :
       - Ses préférences cryptographiques actuelles et précédentes,
       - Les préférences cryptographiques précédentes de l'expéditeur

Protocole Secure HTTP (S-HTTP)

Protocoles

- **SSL**
- **SSH**
- **S-HTTP**
  - Introduction
  - Principe
  - S-HTTP / SSL
- **SET**
- **S/MIME**

- **Complémentarité de S-HTTP et SSL**
  - SSL et S-HTTP
    - SSL :
      - Couche de chiffrement.
      - Indépendant de l'application utilisée.
      - Chiffre l'intégralité de la communication.
    - S-HTTP :
      - Combinaison de HTTP avec couche de chiffrement
      - Marquage individuel des documents HTML à l'aide de certificats.
      - Très fortement lié au protocole HTTP.
      - Chiffre individuellement chaque message.
    - Complémentarité :
      - SSL permet de sécuriser la connexion internet,
      - tandis que S-HTTP permet de fournir des échanges HTTP sécurisés.

Protocole SET

Protocoles

- **SSL**
- **SSH**
- **S-HTTP**
- **SET**
  - Introduction
  - Principe
- **S/MIME**

- **Introduction**
  - SET :
    - Secure Electronic Transaction
    - Protocole de sécurisation des transactions électroniques
    - Mis au point par Visa et MasterCard
    - S'appuie sur le standard SSL.
  - SET est basé sur l'utilisation de :
    - une signature électronique au niveau de l'acheteur,
    - et une transaction mettant en jeu :
      - non seulement l'acheteur et le vendeur,
      - mais aussi leurs banques respectives.

Protocole SET

Protocoles

- **SSL**
- **SSH**
- **S-HTTP**
- **SET**
  - Introduction
  - Principe
- **S/MIME**

- **Principe d'une transaction sécurisée avec SET**

1. Les données sont envoyées par le client au serveur du vendeur

2. Le vendeur ne récupère que la commande.

3. Le numéro de carte bleue est envoyée directement à la banque du commerçant pour :
   - être en mesure de lire les coordonnées bancaires de l'acheteur,
   - et donc contacter sa banque afin de les vérifier en temps réel.

- **Nécessité d'une signature électronique :**
  - Au niveau de l'utilisateur de la carte
  - Pour certifier qu'il s'agit bien du possesseur de cette carte.

Protocole S/MIME

Protocoles

- **SSL**
- **SSH**
- **S-HTTP**
- **SET**

- **S/MIME**
  - Introduction
  - Principe
  - Exemple

- **Introduction**
  - Standard MIME :
    - Permettre d'inclure dans les message électroniques des fichiers attachées autres que des fichiers texte.
  - S/MIME :
    - **S**ecure / **M**ultipurpose **I**nternet **M**ail **E**xtension
    - Procédé de sécurisation des échanges par courrier électronique, encapsulé au format MIME.
    - Assure l'intégrité, l'authentification, la non-répudiation et la confidentialité des messages électroniques.
    - Historique :
      - Mis au point à l'origine par la société RSA Data Security.
      - Ratifié en juillet 1999 par l'IETF, S/MIME est devenu un standard, dont les spécifications sont contenues dans les RFC 2630 à 2633.

Protocole S/MIME

Protocoles

- **SSL**
- **SSH**
- **S-HTTP**
- **SET**

- **S/MIME**
  - Introduction
  - Principe
  - Exemple

- **Principe**
  - Chiffrement à clé publique :
    - Permet ainsi de chiffrer le contenu des messages,
    - Mais ne chiffre pas la communication.
  - Chiffrement du message électronique :
    - Utilisation d'une clé de session
      - Pour chiffrer chaque partie du message
      - Insérée, dans l'en-tête de chaque partie, sous forme chiffré à l'aide de la clé publique du destinataire
    - Intérêt :
      - Seul le destinataire peut ainsi ouvrir le corps du message, à l'aide de sa clé privée.
      - Ceci assure la confidentialité et l'intégrité du message reçu.

Protocole S/MIME

Protocoles

- **SSL**
- **SSH**
- **S-HTTP**
- **SET**

- **S/MIME**
  - Introduction
  - Principe
  - Exemple

- **Principe**
  - Signature du message :
    - Chiffrée à l'aide de la clé privée de l'expéditeur.
    - Intérêt :
      - Toute personne interceptant la communication peut lire le contenu de la signature du message,
      - Mais seul l'expéditeur est capable de chiffrer un message (avec sa clé privée) déchiffrable à l'aide de sa clé publique.
      - Garantit au destinataire l'identité de l'expéditeur.

Protocole S/MIME

Protocoles

- SSL
- SSH
- S-HTTP
- SET

- S/MIME
  - Introduction
  - Principe
  - Exemple

```
MIME-Version: 1.0
Content-Type: multipart/signed;
protocol="application/x-pkcs7-signature";
micalg=sha1;
boundary="----D7B623C746311F5D683A038DC482F307«

This is an S/MIME signed message

------D7B623C746311F5D683A038DC482F307
Content-Type: text/plain

Ceci est le texte d'origine qui est signé.
------D7B623C746311F5D683A038DC482F307
Content-Type: application/x-pkcs7-signature;
name="smime.p7s«
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
filename="smime.p7s"

MIIGgQYJKoZIhvcNAQcCoIIGcjCCBm4CAQExCzAJBgUrDgMCGgUAMAsGCSqGSIb3
DQEHAaCCA7wwggO4MIICoKADAgECAgEMMA0GCSqGSIb3DQEBBAUAMIGrMQswCQYD
VQQGEwJGUjEPMA0GA1UECBMGRlJBTkNFMQ4wDAYDVQQHEwVQQVJJUzEZMBcGA1UE
ChMQVEhFIFNJR05BVFVSRSBDQTEaMBgGA1UECxMRU2lnbmF0dXJlIFNlcnZpY2Ux
HDAaBgNVBAMTE1NpZ25hdHVyZSBBdXRob3JpdHkxJjAkBgkqhkiG9w0BCQEWF2F1
dGhvcml0eUBzaWduYXR1cmUub3JnM…ygIVIs1VsPQ==

------D7B623C746311F5D683A038DC482F307--
```