Mise en sécurité des communications(suite)

Fred Hémery

IUT Béthune
Département
Réseaux &
Télécommunications

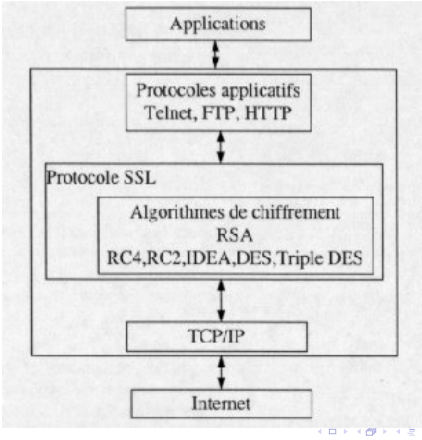
TRC8 Sécurité Avancée — 06/07

Plan

Le protocole SSL

- **SSL** : *Secure Sockets Layer* a été développé par la société Netscape et repris par l'IETF (*Internet Engineering Task Force*) pour définir un standard de sécurité appelé TLS (*Transport Layer Secure*).
- Le protocole SSL permet l'authentification du client et/ou du serveur et/ou le chiffrement des données échangées qui permet de garantir la confidentialité des données mais aussi leur intégrité.
- Le protocole SSL est utilisé au dessus de la couche transport TCP/IP et permet de sécuriser les protocoles de la couche application comme HTTP, LDAP, SMTP, IMAP, NNTP, ...
- Le protocole SSL peut se diviser en 2 sous protocoles :
  - L'encodage (record)
  - La négociation (handshare)

Le protocole SSL



Le protocole SSL

- L'encodage
  - SSL utilise différents algorithmes de chiffrement au cours du déroulement du protocole :
    - L'authentification
    - L'échange des certificats
    - L'échange de clés symétriques
  - SSL utilise les certificats pour l'authentification et ensuite échanger des clés symétriques
  - Les clé symétriques (clés de session) sont alors utilisées pour la confidentialité
- La négociation
  - Elle permet de déterminer les algorithmes de chiffrement les plus adaptés aux communications entre le client et le serveur (RC2,RC4, 3DES, MD5, SHA-1)

Le protocole SSL

Déroulement du protocole

1. Le client envoie au serveur sa version SSL (3.0), ses paramètres de chiffrement, des informations aléatoires et des informations de gestion
2. Le serveur renvoie sa version de SSL, ses paramètres de chiffrement, des informations aléatoires et des infos de gestion. Il envoie également son certificat. De plus si le client demande des informations confidentielles, il demande au client d'envoyer son certificat
3. Le client authentifie le serveur (il peut refuser la connexion en cas d'échec)
4. Le client envoie une pré clé secrète (symétrique) à l'aide du certificat du serveur. Si le serveur a demandé au client de s'identifier, celui-ci renvoie un bloc de données signé avec son certificat

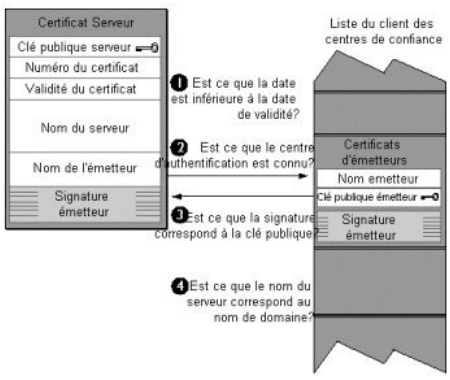
Le protocole SSL

Déroulement du protocole (suite)

5. Le serveur authentifie le client (si l'échange le demande). Il utilise sa clé privée pour récupérer la pré clé secrète . Le serveur effectue des actions (le client aussi) pour obtenir la clé secrète.
6. Le client et le serveur utilise la clé secrète pour générer des clés de session qui sont les clés symétriques utilisées pour le chiffrement et le déchiffrement des données et l'intégrité.
7. Le client prévient le **serveur** que les prochaines données seront chiffrées avec la clé de session, puis envoie un message chiffré pour indiquer la fin de la négociation.
8. Le serveur prévient le **client** que les prochaines données seront chiffrées avec la clé de session, puis envoie un message chiffré pour indiquer la fin de la négociation.
9. La phase de négociation est alors terminée.

Le protocole SSL

Authentification du serveur par le client



Plan

VPN

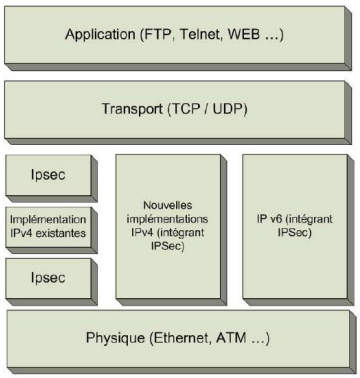
Introduction

- Création d'une liaison sécurisée sur un support qui ne l'est pas
- Fonctions
  - Authentification
  - Intégrité
  - Confidentialité
  - Autorisation
- Avantages
  - Coût
  - Compatible avec les technologies de niveau 2
  - Facilité de déploiement

GRE : Generic Routing Encapsulation, L2TP : Layer 2 Tunneling Protocol

- GRE : Utilisé en conjonction avec PPTP (*Point-to-point tunneling protocol*) pour créer des Réseaux Privés Virtuels.
- L2TP : est un protocole de tunnellisation de niveau 2
- Ce protocole permet de transporter des connexions du niveau 2 au niveau 7 du modèle OSI
- Le transport de ces connexions se fait grâce à des tunnels IP/UDP, le port UDP utilisé en standard est le 1701.
- Un même tunnel peut transporter plusieurs connexions.
- Au départ, L2TP a été défini pour transporter des connexions PPP

IPsec

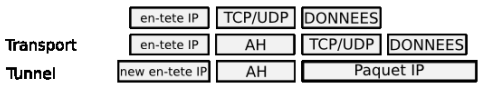


IPsec : Introduction

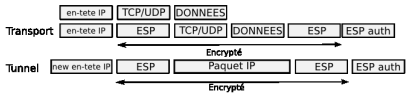
- Le protocole IPsec est de niveau 3 (couche réseau)
  - Il est obligatoire dans la version 6 de IP
  - Mise en oeuvre au niveau de chaque équipement (sécurité de bout en bout)
  - Permet de mettre en oeuvre les services de confidentialité, authentification et interdit le rejeu.
- IPSEC (Internet Protocol Security) est un standard de l'IETF
- Les protocoles et algorithmes
  - Authentification : DSS (Digital Signature Standard) ou RSA
  - Intégrité (fonction de hachage) : HMAC, LD5, HMAC-SHA-1, HMAC-RIPEMD-160, HMAC-DES
  - Confidentialité : DES, 3DES, RC5, IDEA, CAST, Blowfish
- Fonctionne suivant 2 modes :
  - **Tunnel** : le paquet IP est encapsulé et chiffré dans un nouveau paquet IP
  - **Transport** : l'en-tête IP n'est pas modifié, seul le contenu est chiffrés

IPsec : Introduction

- Les services sont mis en oeuvre en utilisant 2 mécanismes :
  - AH : Authentification Header (RFC 2402), qui permet uniquement l'authentification et l'intégrité



  - ESP : Encapsulating Security Payload (RFC 2406), qui permet l'authentification , l'intégrité et la confidentialité



IPsec : SA

- Pour définir les choix qui seront faits, on utilise un SA (*Security Association*)
  - Type de protection (AH, ESP)
  - Algorithme authentification (AH, ESP)
  - Algorithme confidentialité (ESP)
  - Les clés en usage
  - La durée de vie des clés
  - La durée de vie de la SA
  - Le séquençage des datagrammes
- Il faut 2 SA pour un flux (1 par direction)
- La négociation du SA utilise un autre protocole : ISAKMP/IKE
  - ISAKMP (*Internet Security Association and Key Managment Protocol*) permet le stockage des SA, construction des messages
  - IKE (*Internet Key Exchange*) permet l'échange des clés. Utilise ISAKMP.

VPN

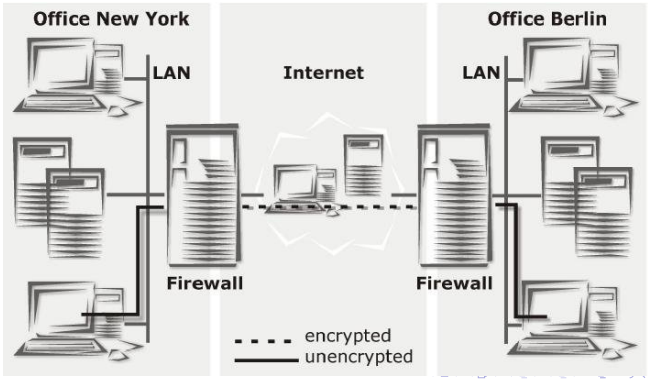
- VPN : *Virtual Private Network* est une connexion entre deux réseaux traversant un réseau non sécurisé (Internet).
- Il interdit à une tiers personne de lire ou modifier les informations qui circulent. Le logiciel qui met en oeuvre VPN implémente l'authentification, l'échange de clés et le chiffrement des informations comme spécifié dans le standard IPSec.
- Un tunnel IP sécurisé est composé de deux Associations de sécurité (SA : Security Association), une SA par direction.
- Une SA représente 3 composants :
  - Un SPI ; Security Parameter Index
  - L'adresse IP du destinataire, et
  - Un AH (Security Protocol Authentication Header) ou un ESP (Encapsulation Security Payload)

VPN

- La gestion des clés échangées se fait à l'aide du protocole IKE : (*Internet Key Exchange*) qui propose en autre 3 types d'échange
  - IKE with Preshared Keys (PSK) : les clés sécrètes sont échangées avant l'établissement de la connexion
  - IKE with RSA Keys (RSA) : les points de connexions génèrent chacun une clé publique associée à une clé privée. Les clés publiques sont ensuite échangées.
  - IKE with X.509 certificate (X509) : comme précédemment, avec en plus une certification de la clé publique.
- L'échange de clés se fait en utilisant le port 500 du protocole UDP puis le protocole IP 51 pour AH et 50 pour ESP.

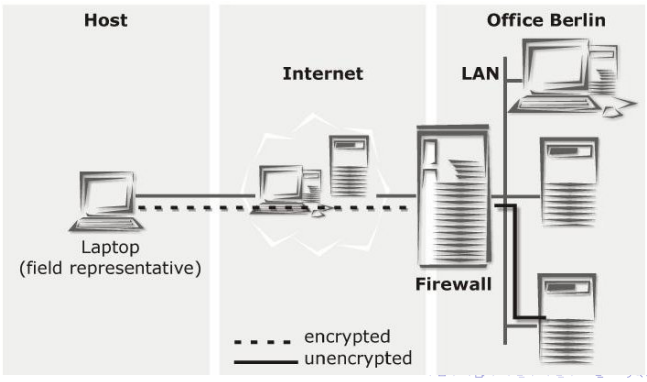
VPN

Un connexion entre deux réseaux



VPN

Une machine vers un réseau (télétravail par exemple)



VPN

Une machine vers une machine