

## Administration Système et Réseaux, Sécurité

### Cryptographie, tunnels

Philippe Harrand

<sup>1</sup>Département Informatique  
Pôle Sciences et Technologies

<sup>2</sup>Direction Territoriale Sud Ouest  
France Télécom

8 décembre 2007

## Cryptographie, Tunnels

### Cryptographie

Définitions

Authentification

Confidentialité

Confidentialité ET authentification

SSL / TLS

### Tunnels

SSH

IPSEC

OpenVPN

## Chiffrement

- ▶ algorithme public
  - ▶ Chiffrement ⇒ rendre incompréhensible un document en utilisant un algorithme public
  - ▶ Déchiffrement ⇒ restituer le document original
- ▶ Utilisation de **clefs**
- ▶ Chiffrement Symétrique
  - ▶ Chiffrement / Déchiffrement ⇒ même clef
  - ▶ Connue de tous les protagonistes
- ▶ Chiffrement Asymétrique
  - ▶ Chiffrement ⇒ Clef privée
  - ▶ Déchiffrement ⇒ Clef publique
  - ▶ Ou l'inverse
- ▶ Chiffrement symétrique moins gourmand en ressources et en bande passante

## Hachage

Appliqué à un fichier ou à un texte, le haché produit un mot

- ▶ de taille fixée par l'algorithme utilisé
- ▶ irréversible (l'original ne peut pas être reconstitué)
- ▶ unique (2 originaux différents ne produisent jamais le même mot)

## Signature

- ▶ Message envoyé accompagné d'un haché (MD5 ou SHA1)
- ▶ Chiffré avec la clef privée de l'expéditeur
- ▶ Le destinataire recalcule le haché à partir du message envoyé en clair
- ▶ S'il arriv à déchiffrer le haché avec la clef publique de l'expéditeur cela prouve l'identité de l'expéditeur
- ▶ Si le haché calculé est égal à celui envoyé, cela prouve que le message n'a pas été modifié pendant le transfert
- ▶ Mais le contenu du message a pu être lu

## Certificats

- ▶ Les clefs publiques peuvent être stockées chez des « tiers de confiance »
- ▶ Ceux-ci délivrent les clefs publiques accompagnées d'informations sur leurs propriétaires
- ▶ le tout signé avec les clefs privées des dits tiers
- ▶ Les clefs publiques de ces tiers de confiance sont authentifiées par des « autorités racines »
- ▶ Vous devez faire confiance aux "autorités racines"
- ▶ A l'intérieur d'un intranet, vous pouvez diffuser de tels certificats « racine » qui n'auront bien sûr de valeur qu'à l'intérieur de l'entreprise...
- ▶ /usr/share/ssl/certs/ca-bundle.crt

## Confidentialité

- ▶ Le message est chiffré par l'expéditeur avec la clef publique du destinataire
- ▶ Seul le détenteur de la clef privée pourra le déchiffrer
- ▶ N'importe qui peut obtenir la clef publique
- ▶ Le destinataire ne sait donc pas qui a envoyé le message

## Confidentialité ET authentification

- ▶ Méthode 1
  - ▶ Le message est haché par l'expéditeur et « signé » avec sa clef privée
  - ▶ Puis le message est chiffré avec la clef publique du destinataire
  - ▶ Le destinataire est le seul à pouvoir déchiffrer le message
  - ▶ Le haché étant déchiffré avec la clef publique de l'expéditeur, il est le seul à avoir pu l'envoyer
  - ▶ Coûteux en ressources : deux chiffrements/déchiffrements
  - ▶ A réserver aux messages uniques
- ▶ Méthode 2 :
  - ▶ Le chiffrement du dialogue est réalisé avec une clef symétrique temporaire dite « de session »
  - ▶ Changer la clef de session avec une fréquence supérieure au volume de données nécessaire pour la casser
  - ▶ Clef de session envoyé par la méthode 1

## Généralités

- ▶ SSL/TLS ⇒ authentification mutuelle serveur et client, chiffrement, vérification de l'intégrité
- ▶ **Secure Socket Layer** créé par Netscape
- ▶ Diffusé en 1994
- ▶ Racheté par l'**IETF** en 2001
- ▶ Rebaptisé **Transport Layer Security**
- ▶ SSL ⇒ V3
- ▶ TLS ⇒ V1.0
- ▶ SSL est utilisé sur des ports TCP spéciaux (443 https, 995 pop3s, 636 ldaps)
- ▶ TLS est négocié par les applicatifs
- ▶ Openssl implémente les deux

## Fonctionnement

- ▶ Le client se connecte au serveur et lui demande de s'authentifier
- ▶ Le client envoie également la liste des cryptosystèmes supportés
- ▶ Le serveur envoie un certificat au client, contenant sa clé publique, signée par une autorité de certification (CA)
- ▶ Ainsi que le nom du cryptosystème le plus haut dans la liste avec lequel il est compatible
- ▶ Le client **vérifie la validité du certificat**
- ▶ Crée une clé pseudo-aléatoire, la chiffre à l'aide de la clé publique du serveur
- ▶ Le serveur déchiffre la clé de session avec sa clé privée

## VPN

- ▶ **Virtual Private Network**
- ▶ Relie de 2 à N réseaux physiques éloignés
- ▶ ~~Par le Réseau Téléphonique Commuté~~
- ▶ Par Liaisons Louées
- ▶ Par Internet
- ▶ De façon transparente
- ▶ **Et sécurisée**

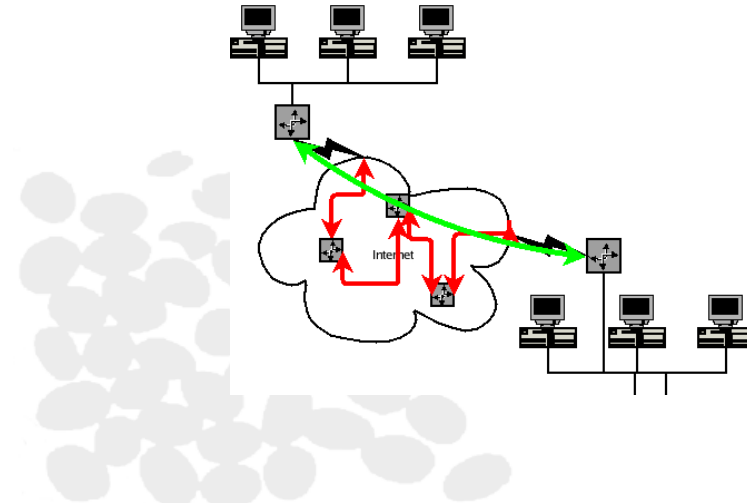
## Tunnel



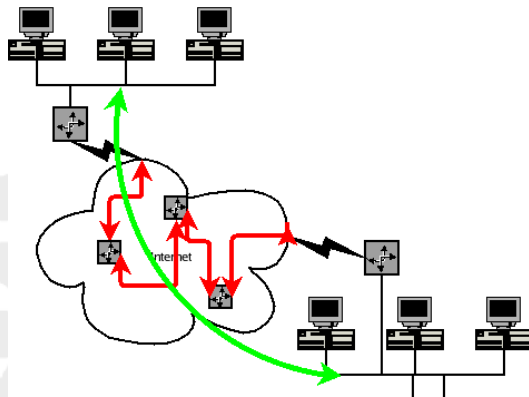
## Tunnel

- ▶ Relie 2 réseaux directement à travers un internet
- ▶ Le plus souvent chiffré
- ▶ 2 sortes de tunnels
  - ▶ Routés
  - ▶ "Pontés"

## Tunnel routé



## Tunnel ponté



## Tunnel routé

- ▶ le tunnel transporte la couche 3 du message original
- ▶ Route spécifique
- ▶ Adresses réseaux différentes
- ▶ Pas de broadcast

## Tunnel "ponté"

- ▶ le tunnel transporte la couche 2 du message original
- ▶ Adresses réseaux identiques
- ▶ Transporte n'importe quel niveau 3
- ▶ Broadcast
- ▶ Transparence complète

## SSH

- ▶ **Secure SHell**
- ▶ Telnet sécurisé
- ▶ authentification du serveur par Clef publique/privée (RSA)
- ▶ Authentification du client par
  - ▶ Clef publique/privée (Défi)
  - ▶ Mot de passe
- ▶ Applications
  - ▶ Export X11
  - ▶ SFTP
  - ▶ SSHFS
  - ▶ Transfert de ports TCP (tunnel)
  - ▶ Sauts
  - ▶ Franchissement de firewalls

## IPSEC

- ▶ Authentifier et chiffrer les données
- ▶ Défini pour IPV6
- ▶ Adapté à IPV4
- ▶ Problèmes avec le NAT
- ▶ Plusieurs sous protocoles

## IPSEC

- ▶ Mode transport
  - ▶ Protège les échanges entre deux machines
  - ▶ Traverse le NAT
- ▶ Mode tunnel
  - ▶ Encapsule les paquets chiffrés dans de nouveaux en-tête IPv4/IPv6
  - ▶ Conçu pour les passerelles VPN
  - ▶ Masque les adresses IP réelles
  - ▶ Protège contre le rejeu
- ▶ IPSEC est inclus dans les noyaux 2.6

## Associations de Sécurité

- ▶ Conserve les paramètres de sécurité d'une connexion
  - ▶ authentification des pairs
  - ▶ Méthodes de chiffrement
  - ▶ Clefs
  - ▶ ...
- ▶ **ISAKMP**
  - ▶ Internet **S**ecurity **A**ssociation and **K**ey **M**anagement **P**rotocol
  - ▶ Etablir, négocier, modifier ou supprimer des Associations de Sécurité (**SA**)
  - ▶ Utilise **IKE**
- ▶ **IKE**
  - ▶ Internet **K**ey **E**xchange...
  - ▶ Permet l'établissement des **SA**
  - ▶ La **SA** peut être créée manuellement

## Protection des données

- ▶ **AH**
  - ▶ (Authentication Header), authenticité des paquets en leur inscrivant une somme de contrôle (de l'en-tête IP jusqu'à la fin du paquet) chiffrée
  - ▶ Intégrité des données transmises
  - ▶ protection contre le rejeu
- ▶ **ESP**
  - ▶ Encapsulating **S**ecurity **P**ayload chiffre toutes les données de la couche 4
  - ▶ ESP encapsule les données entre un en-tête et un en-queue
  - ▶ En mode tunnel, les données sont un paquet IP
- ▶ **IPcomp**
  - ▶ **I**P **P**ayload **c**ompression permet de compresser un paquet avant de le chiffrer avec ESP

## OpenVPN

- ▶ Espace utilisateur
- ▶ Mode "routé" ou "ponté"
- ▶ Simple à mettre en oeuvre
- ▶ Livré avec scripts de démarrage