Chapitre 6 : Sécurité des co
hautes

(sécurité et parallélisme)

Plan

- TLS
- SET

1. TLS

- Historique
  - SSL = Secure Socket Layer
  - défini par Netscape
  - normalisé en tant que TLS
- TLS = Transport Layer Security
  - entre TCP et l'application
  - utilisation : HTTP, FTP, SMTP, telnet, et
  - TLS = SSL v3.1

Services de TLS

- Services de sécurité
  - authentification du serveur (certificats)
  - confidentialité (chiffrement symétrique, à la création de la session)
  - intégrité (HMAC)
  - authentification optionnelle du client
  - non rejeu (numéro de séquence)

Services de TLS

- Autres services
  - transparence des protocoles supérieurs
  - spontanéïté : connexion transparente à serveur

Sous-protocoles de SS

- Sous-protocoles de SSL
  - handshake : responsable de la négocia
  - change cypher : responsable de change chiffrement
  - alert : responsable d'informer en cas d'a
  - record : responsable de chiffrer

Mécanisme

- Mécanisme
  - client envoie message Hello : chiffreme
    disponibles
  - serveur envoie message Hello : chiffren
    certificat + clé publique
  - client vérifie le certificat
  - client envoie une clé de chiffrement sym
    chiffrée avec la clé publique du serveur
  - serveur récupère la clé de chiffrement s
  - communication chiffrée avec la clé sym

SSL vs IPSec

- Avantages
  - SSL ne nécessite pas la modification de
    TCP/IP
  - SSL supporte le NAT
  - SSL traverse les firewalls et les proxys

SSL vs SSH

- SSH = Secure Shell
  - port 22
  - peut servir à redirer une communicatior tunnel sécurisé
  - cryptographie asymétrique
  - utilisé par SCP et SFTP ou pour faire u
- Inconvénient de SSH
  - pas d'authentification
  - vérifier les clés publiques

SSL vs SSH

- Différences
  - SSL orienté texte, SSH orienté fichiers
  - SSL négocie et chiffre, SSH permet un distance + transfert de fichiers
  - SSL basé sur des PKI, SSH permet plu schémas d'authentification

SSL et VPN

- SSL n'est pas adapté pour un VPN
  - SSL utilise un nouveau port par applica
- Solution : webify
  - on transforme au format web un protoc quelconque (FTP, etc.)
- Solution : MTLS = Multiplexing TLS
  - mise en place d'une session sécurisée
  - établissement de plusieurs sessions sé un protocole de requête/réponse

Inconvénients de SSL

- Inconvénients
  - une seule authentification en début de s
  - certificat non nécessaire pour le client
  - plus de signature après le handshake

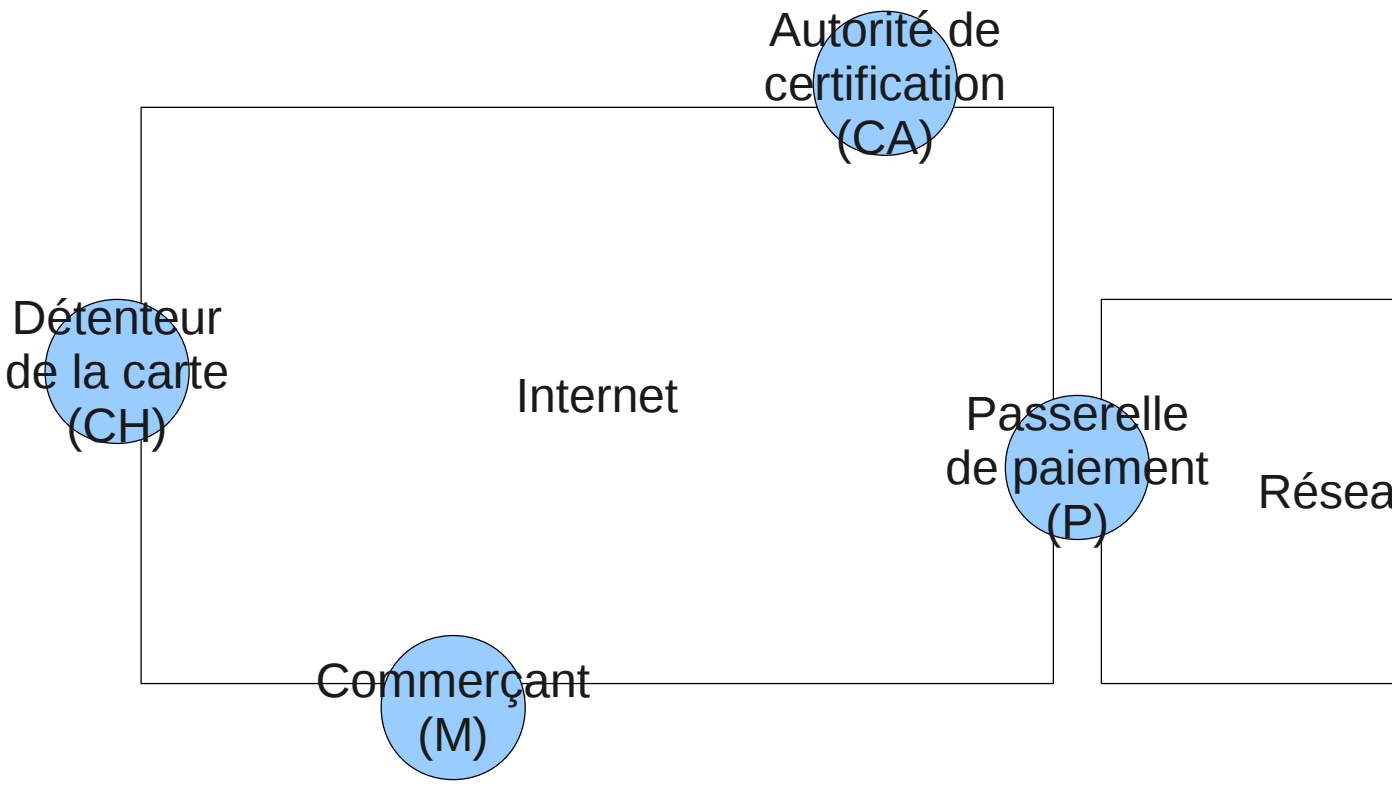
Outil de test SSL

- OpenSSL
  - openssl s_client -connect server:443
- ssldump

2. SET

- SET = Secure Electronic Transaction
  - défini par Visa et Mastercard en 1997
  - protocoles de sécurité pour le paiement bancaire sur Internet

Architecture



Services

- Services de SET
  - autentification et identification des entité
  - confidentialité des instructions de paiem
  - intégrité (hachage)
  - non répudiation
- Mécanisme
  - messages signés (condensat + clé privé l'émetteur)
  - clé symétrique déduite d'un aléa et tran l'aide de la clé publique du destinataire
  - messages chiffrés par la clé symétrique

Principe de la signature c

- Objectif
  - Alice veut envoyer M1 à Bob et M2 à C
  - Bob ne peut pas voir M2
  - Carole ne peut pas voir M1
  - Bob et Carole doivent être sûrs que ces ne sont pas modifiés

Principe de la signature c

- Mécanisme
  - Alice envoie à Bob : M1 + H(M2) + S
  - Bob vérifie que chiffr(H(H(M1)+H(M2)),)) = S
  - Alice envoie à Carole : M2 + H(M1) + S
  - Carole peut vérifier
  - Bob et Carole peuvent s'assurer que H(H(M2) correspondent à M1 et M2

Etapes et protocoles

- Etapes
  - inscription auprès du CA
  - demande d'achat
  - autorisation de paiement
  - paiement

Inscription

- SET nécessite que CH s'inscrive aup
- SET nécessite que M s'inscrive aupr

Achat

- Algorithme
  - CH envoie une requête à M
  - M envoie requête d'autorisation à P
  - P envoie autorisation à M
  - M envoie réponse à CH
  - M envoie requête à P
  - P envoie réponse à M

Opération d'achat

- Algorithme
  - CH génère OI (order information) destin
    contenant pas le numéro de carte de cr
  - CH génère PI (payment information) de
    contenant pas les informations sur l'ach
  - CH envoie à M : OI + H(OI) + chiffr(PI, K
    + H(PI) + chiffr(H(OI)|H(PI), K_priv_CH)
  - M envoie à P : H(OI) + chiffr(PI, K_pub(
    + chiffr(H(OI)|H(PI), K_priv_CH)
  - M reçoit de P un bon de paiement ou un

Opération d'achat

- Intérêt
  - M ne connait que OI, H(OI), H(PI)
  - M peut vérifier la signature
  - P ne connait que H(OI), PI et H(PI)
  - P peut vérifier la signature
  - principe de la signature duale

Compensation

- Bon de paiement nécessaire pour la compensation

Inconvénients

- Inconvénients
  - certificats lourds à vérifier
  - calculs cryptographiques lourds

Conclusion

- SSL et TLS sont des protocoles sécu
  - pas de non répudiation
  - pas de gestion de paiement
  - pas d'authentification obligatoire du clie
- SET est un protocole de paiement sé