

COURS SUR SSL/TLS

DESCRIPTION

Très riche en contenu explicite, ce cours jette les bases du protocole utilisé aujourd'hui pour la sécurisation des échanges entre machines sur le réseau à savoir : le protocole SSL ou TLS. Dans ce cours, vous appréhendez les mécanismes cryptographiques mis en place pour établir une session TLS et les étapes successives dans l'établissement de cette session. Le fameux « **handshake** » en TLS est exposé de façon détaillée avec ses messages tels que le client hello et le server hello pour vous permettre de bien comprendre le principe du TLS. Nous abordons aussi dans ce cours la question suivante : comment sont conçues les différentes clés (secrets) utilisées dans les échanges. Il s'agit ici d'algorithmes cryptographiques robustes implémentant des calculs mathématiques assez complexes et aboutissant aux fonctions cryptographiques que sont le hashage, le chiffrement et le déchiffrement. Enfin nous abordons aussi la PKI (Public Key Infrastructure) et les autres protocoles qui composent le TLS tels ALERT protocol, CCS protocol et RECORD protocol. Pour terminer, ce cours vous donne de bonnes bases pour aborder sereinement les aspects de sécurité beaucoup plus complexes tout au long de votre carrière d'ingénieur.

PREREQUIS

Modèle TCP/IP

Notion de cryptographie (algorithmes de hashage, signature numérique, chiffrement etc)

CONTENU

INTRODUCTION

POURQUOI LE TLS

ETAPES ET ACTEURS DANS UNE TRANSACTION

CONTEXTE

ARCHITECTURE

PORTS AU DESSUS DE SSL

SERVICES DE SSL

- Authenticité de serveur

- Confidentialité des données

- Intégrité des données

COMMENT SSL ASSURE T IL SES SERVICES

Chiffrement/déchiffrement

Algorithmes

Signature numérique

Certificats numériques

PKI

Chiffrement/déchiffrement RSA

ETAPES D'UNE TRANSACTION SSL/TLS

LES SOUS PROTOCOLES TLS

Handshake

Client Hello/server hello

Alert

CCS

Record

CERTIFICAT X509

AUTHENTIFICATION SERVER

REVOCACTION D'UN CERTIFICAT

CALCULS DES PARAMETRES DE SECURITE

Construction du Master secret

Génération des autres secrets

Utilization des secrets

Clés secrètes d'une session SSL

SSL RECORD PROTOCOL

SSL ALERT PROTOCOL

SSL CHANGE CIPHER SPEC PROTOCOL

FAIBLESSES DE SSL/TLS