TELECOM PARIS
école nationale supérieure des télécommunications

CNRS CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

SSL/TLS:
Secure Socket Layer/Transport Layer Secure
Quelques éléments d'analyse

GRES'2006
Bordeaux 12 Mai 2006

Ahmed Serhrouchni
ENST-PARIS
CNRS

Plan

- **Introduction (10 minutes)**
  - Les services de sécurité
  - Typologie des solutions de sécurité
  - Typologie des attaques
  - Contexte et situation du protocole SSL/TLS
- **Le protocole SSL/TLS (40 minutes)**
  - Architecture
  - Services
  - Les protocoles de SSL/TLS
  - Une attaque sur SSL/TLS
  - Évaluation
- **Conclusion (10 minutes)**

Introduction: Les services de sécurité

- Confidentialité
- Intégrité
- Authentification
- Non-rejeu
- Identification
- Non-répudiation
- Contre l'analyse de trafic
- Horodatage

Introduction: Typologie des solutions de sécurité

- Solution par extension
- Solution transparente
- Solution par signalisation
- Solution de type traitement locale

Introduction: Typologie des attaques

- Choix d'implémentation — Patchs
  - Buffer overflow, Ping of death, land, Teardrop …
- Design des protocoles — Filtrage, …
  - Smurf, email :bombing, spamming, ftp bounce ,TCP con. Killing
- Usurpation d'adresse ou d'identité — Authentification,
  - Sniffing, ARP spoofing, IP spoofing, TCP hijacking, email spoofing, dns cache poisoning, web spoofing
- Défaut d'implémentation — Patchs
  - **Voulue (chevaux de Troie, virus, …)**
  - **Non voulue**

Introduction: Contexte et situation du protocole SSL/TLS

- **SSL défini par *netsacpe* et intégré au browser**
  - Première version de SSL testé en interne
  - Première version de SSL diffusé : V2 (1994)
  - Version actuelle V3
- **IETF au sein du groupe Transport Layer Security**
  - RFC2246 The TLS Protocol version 1.0
  - RFC4346 The TLS Protocol version 1.1
  - RFC4279 Pre-Shared Key Ciphersuites for TLS
  - draft-ietf-tls-rfc4346-bis-00.txt version 1.2
- **Standard au sein du WAP Forum Wireless Transport Layer Security (WTLS)**

Introduction: Contexte et situation du protocole SSL/TLS

- **Protocole SSL/TLS au niveau applicatif**
  - Basé sur TCP
  - Une récente version sur UDP
- **Intègrè directement aux applications**
- **API la plus répandue Openssl (programmation très proche des sockets)**
- **TLS en évolution …**

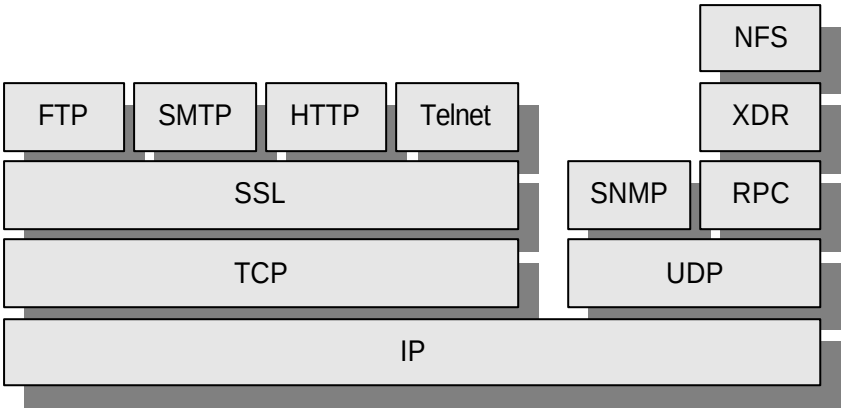
Introduction: Contexte et situation du protocole SSL/TLS

Nom de l'API	Fournisseur	Adresse
AOLserver 2.3	America Online. Inc	http://www.aolserver.com
Alibaba 2.0	Computer Software Manufacturers	http://www.csm.co.at /alibaba/
Apache 1.3	The Apache Group	http://www.apache.org
Commerce Server/400 1.0	I/NET, Inc.	http://www.inetmi.com
Enterprise Server 3.0	Novonyx	http://www.novonyx.com
EnterpriseWeb Secure/VM	Beyond-Software Incorpora	http://www.beyond-software.com
Internet Information Server	Microsoft Corp.	http://www.microsoft.com/iis
Java Server 1.1	Sun Microsystems	http://www.java.sun.com
Lotus Domino Go Webserv 4.6.1	IBM	http://www.ibm.com
Netscape Enterprise Server 3	Netscape Communications	http://www. netscape.com
Oracle Web Application Serv 3.01	Oracle Corp.	http://www.oracle.com /products
Roxen Challenger 1.2b I	Idonex	http://www.roxen.com
SSLava	Phaos Technologies	http://www.phaos.com /main.htm
WebSite Professional 2.2	O'Reilly Software	http://www.website.oreilly.com /
WebTen 2.1	Tenon Intersystems	http://www.tenon.com/products/webten
Zeus Web Application Serv	Zeus Technology	http://www.zeustech.net

SSL : liste non exhaustive d'APIs

Nom de l'API	Fournisseur	Adresse
AOLserver 2.3	America Online. Inc	http://www.aolserver.com
Alibaba 2.0	Computer Software Manufacturers	http://www.csm.co.at /alibaba/
Apache 1.3	The Apache Group	http://www.apache.org
Commerce Server/400 1.00	I/NET, Inc.	http://www.inetmi.com
Enterprise Server 3.0	Novonyx	http://www.novonyx.com
EnterpriseWeb Secure/VM	Beyond-Software Incorpora	http://www.beyond-software.com
Internet Information Server	Microsoft Corp.	http://www.microsoft.com/iis
Java Server 1.1	Sun Microsystems	http://www.java.sun.com
Lotus Domino Go Webserv 4.6.1	IBM	http://www.ibm.com
Netscape Enterprise Server 3	Netscape Communications	http://www. netscape.com
Oracle Web Application Serv 3.01	Oracle Corp.	http://www.oracle.com /products
Roxen Challenger 1.2b l	Idonex	http://www.roxen.com
SSLava	Phaos Technologies	http://www.phaos.com /main.htm
WebSite Professional 2.2	O'Reilly Software	http://www.website.oreilly.com /
WebTen 2.1	Tenon Intersystems	http://www.tenon.com/products/webten
Zeus Web Application Serv	Zeus Technology	http://www.zeustech.net

Le protocole SSL/TLS : Architecture



Le protocole SSL/TLS : Architecture

Protocole sécurisé	Port	Protocole non sécurisé	Application
HTTPS	443	HTTP	Transactions requête-réponse sécurisées
SSMTP	465	SMTP	Messagerie électronique
NNTPS	563	NNTP	News sur le réseau Internet
LDAPS	636	LDAP	Annuaire X.500 allégé
POP3S	995	POP3	Accès distant à la boîte aux lettres avec rapatriement des messages
COPS-TLS	3183	COPS	Gestion par politiques

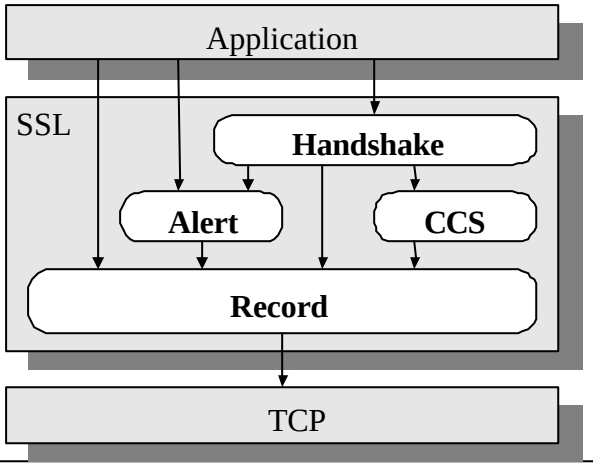
Le protocole SSL/TLS : Architecture

Protocole sécurisé	Port	Protocole non sécurisé	Application
FTP-DATA	889	FTP	Transfert de fichiers
FTPS	990	FTP	Contrôle du transfert de fichiers
IMAPS	991	IMAP4	Accès distant à la boîte aux lettres avec ou sans rapatriement des messages
TELNETS	992	Telnet	Protocole d'accès distant à un système informatique
IRCS	993	IRC	Protocole de conférence par l'écrit

Le protocole SSL/TLS : Services

- **Authentification**
  - Serveur (obligatoire), client (optionnel)
  - Utilisation de certificat X509 V3
  - A l'établissement de la session.
- **Confidentialité**
  - Algorithme de chiffrement symétrique négocié, clé généré à l'établissement de la session.
- **Intégrité**
  - Fonction de hachage avec clé secrète : hmac(clé secrète, h, Message)
- **Non Rejeu**
  - Numéro de séquence

Le protocole SSL/TLS : les protocoles



Le protocole SSL/TLS : Handshake (1/6)

- **Authentification du serveur et éventuellement du client,**
- **Négociation des algorithmes de chiffrement et de hachage, échange d'un secret,**
- **Génération des clés.**

Le protocole SSL/TLS : Handshake (2/6)

Message	Type de message	Sens de transmission	Signification
HelloRequest	optionnel	serveur → client	Ce message demande au client d'entamer le Handshake.
ClientHello	obligatoire	client → serveur	Ce message contient : le numéro de version du protocole SSL ; le nombre aléatoire : client_random ; l'identificateur de session : session_ID ; la liste des suites de chiffrement choisies par le client ; la liste des méthodes de compression choisies par le client.
ServerHello	obligatoire	serveur → client	Ce message contient : le numéro de version du protocole SSL ; un nombre aléatoire : serveur_random ; l'identificateur de session : session_ID ; une suite de chiffrement ; une méthode de compression.

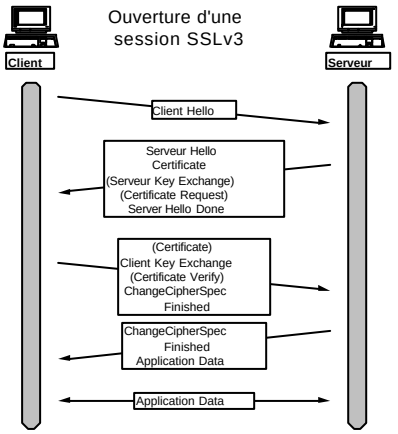
Le protocole SSL/TLS : Handshake (3/6)

Certificate	Optionnel	serveur → client client → serveur	Ce message contient le certificat du serveur ou celui du client si le serveur le lui réclame et que le client en possède un.
ServerKeyExchange	Optionnel	serveur → client	Ce message est envoyé par le serveur que s'il ne possède aucun certificat, ou seulement un certificat de signature.
CertificateRequest	Optionnel	serveur → client	Par ce message, le serveur réclame un certificat au client.
ServerHelloDone	Obligatoire	serveur → client	Ce message signale la fin de l'envoi des messages ServerHello et subséquents.

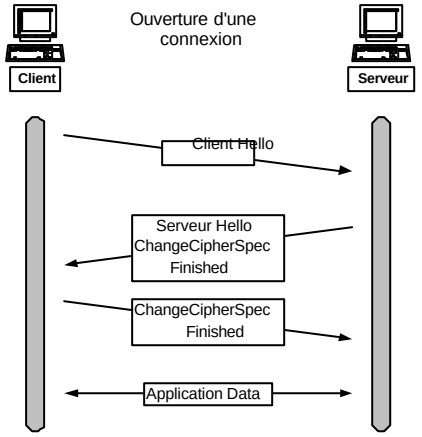
Le protocole SSL/TLS : Handshake (4/6)

ClientKeyExchange	Obligatoire	client → serveur	Ce message contient le PreMasterSecret crypté à l'aide de la clé publique du serveur.
CertificateVerify	Optionnel	client → serveur	Ce message permet une vérification explicite du certificat du client.
Finished	obligatoire	serveur → client client → serveur	Ce message signale la fin du protocole Handshake et le début de l'émission des données protégées avec les nouveaux paramètres négociés.

Le protocole SSL/TLS : Handshake (5/6)



Le protocole SSL/TLS : Handshake (6/6)



Le protocole SSL/TLS : *ChangeCipherSpec (CCS)*

- ***ChangeCipherSpec* signale au *Record* toute modification des paramètres de sécurité,**
- **Constitué d'un message (1 octet)**

Le protocole SSL/TLS : Le protocole *Record*

- **Reçoit les données des couches supérieures : (*Handshake*, *Alert*, *CCS*, HTTP, FTP ...), et les transmet au protocole TCP.**
- **Après application de :**
  - la fragmentation des données en blocs de taille maximum de 2^{14} octets
  - la compression des données, fonction prévue mais non supportée actuellement
  - la génération d'un condensât pour assurer le service d'intégrité
  - le chiffrement des données pour assurer le service de confidentialité

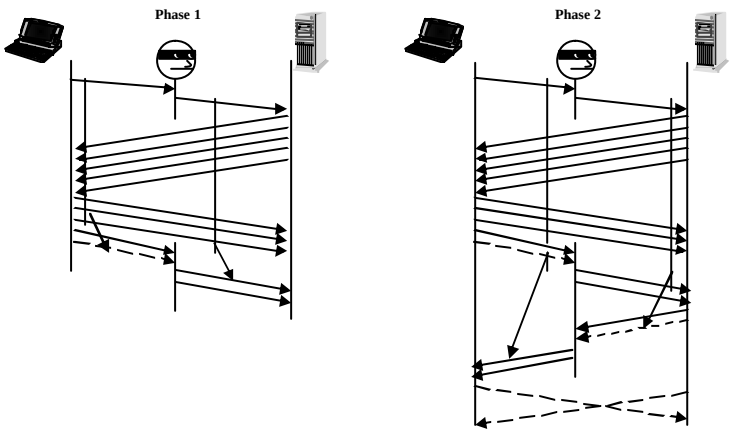
Le protocole SSL/TLS : Le protocole *Alert*

- **Le protocole *Alert* peut être invoqué :**
  - par l'application, par exemple pour signaler la fin d'une connexion
  - par le protocole *Handshake* suite à un problème survenu au cours de son déroulement
- **par la couche *Record* directement, par exemple si l'intégrité d'un message est mise en doute**

Le protocole SSL/TLS : Le protocole *Alert* (2)

Message	Contexte	Type
bad_certificate	échec de vérification d'un certificat	fatal
bad_record_mac	réception d'un MAC erroné	fatal
certificate_expired	certificat périmé	fatal
certificate_revoked	certificat mis en opposition (révoqué)	fatal
certificate_unknown	certificat invalide pour d'autres motifs que ceux précisés précédemment	fatal
close_notify	interruption volontaire de session	fatal
decompression_failure	les données appliquées à la fonction de décompression sont invalides (par exemple, trop longues)	fatal
handshake_failure	impossibilité de négocier des paramètres satisfaisants	fatal
illegal_parameter	un paramètre échangé au cours du protocole Handshake dépasse les bornes admises ou ne concorde pas avec les autres paramètres	fatal
no_certificate	réponse négative à une requête de certificat	avertissement ou fatal
unexpected_message	arrivée inopportune d'un message	fatal
unsupported_certificate	le certificat reçu n'est pas reconnu par le destinataire	avertissement ou fatal

Le protocole SSL/TLS : une attaque



Le protocole SSL/TLS : évaluation (1/3)

- **Les choix pour les calculs de la charge cryptographique de SSL:**
  - algorithme de chiffrement du protocole record : DES 64 bits en mode CBC ;
  - algorithme de chiffrement asymétrique : RSA 1024 bits ;
  - fonction de hachage : MD5 ;
  - itinéraire de certification comprenant une seule étape ;
  - certificat du serveur : autorité de certification unique, déjà connue du client (un seul certificat dans le message *Certificate*) ;
  - taille des informations contenues, du message *Certificate* : 500 octets (notons que la taille des informations du certificat est dans la plupart des cas inférieure) ;
  - seule le serveur est certifié.

Le protocole SSL/TLS : evaluation (2/3)

Opération	Temps de calcul pour le client (ms)	Temps de calcul pour le serveur (ms)	Total (ms)
Ouverture d'une nouvelle session (Handshake complet)	18,94	16,9	35,85
Rafraîchissement d'une session (Handshake simplifié)	0,11	0,11	0,22
Ouverture d'une nouvelle connexion	0,079	0,071	0,15
Temps de calcul pour 16Ko de données (chiffrement ou déchiffrement, élaboration et vérification du MAC)	5,5	5,3	10,8

Le protocole SSL/TLS : evaluation (3/3)

Serveur et Version				Apache SSLLeay 08.0	Jigsaw 2.0 Beta 1	Microsoft IIS/4.0	Netscape Entreprise3.0L	Netscape Entreprise 3.0F	SSLava Beta 1
	Suite	Export	Code						
	RC4-40 MD5	✓	0x03	●	●	●	●	●	●
	RC4-128 MD5		0x04	●	●	●	●		●
	RC4- 128 SHA		0x05	●	●	●			●
RSA	RC2 CBC-40 MD5	✓	0x06	●	●	●	●	●	
	IDEA CBC SHA		0x07	●	●				
	DES40 CBC SHA	✓	0x08	●	●	●			●
	DESCBC SHA		0x09	●	●	●	●		●
	3DES EDE CBC SHA		0x0A	●	●	●	●		
	DES40 CBC SHA	✓	0x0B		●				
DH et DSA	DES CBC SHA		0x0C		●				
	3DES EDE CBC SHA		0x0D		●				
	DES40 CBC SHA	✓	0x0E		●				
DH et RSA	DES CBC SHA		0x0F		●				
	3DES EDE CBC SHA		0x10		●				
	DES40 CBC SHA	✓	0x11		●				
DHE et DSA	DES CBC SHA		0x12		●				
	3DES EDE CBC SHA		0x13		●				
	DES40 CBC SHA	✓	0x14		●	●			
DHE et RSA	DES CBC SHA		0x15		●	●			
	3DES EDE CBC SHA		0x16		●	●			

Conclusion

Critères	SSL
Applications	générale
Certificat du client	optionnelle
Longueur de la clé RSA	variable
Longueur de la clé DES	vriable
Signature des données	non
Clé DES unique pour chaque message	non
Négociation des algorithmes cryptographiques	oui
Mise en oeuvre de mécanisme de compression des données	oui
Authentification des participants	optionnelle

Conclusion

- **Une seule authentification au début de la session, certificat non nécessaire pour le client**
- **Facile d'usage et transparent aux utilisateurs**
- **Pas de signature après le *HandShake***
- **A chaque application son instance**
- **Possibilité d'analyse du trafic**
- **Absence de regulation pour le déploiement des certificats.**