Le protocole SSL

AMYN BENNAMANE

MIF30 – CRYPTOGRAPHIE
M1 INFORMATIQUE UCBL
20 MAI2009

Sommaire

- Introduction
- Fonctionnement
- Structure
  - Couche Basse
  - Couche Haute
- Attaques
- Conclusion

Introduction

- Objectifs :
  - Intégrité
  - Confidentialité
  - Authenticité
- Versions
  - 1996 : SSL 2
  - 1999 : SSL 3
  - 2001 : TSL 1
- Très utilisé de nos jours

Fonctionnement

- Client-Serveur

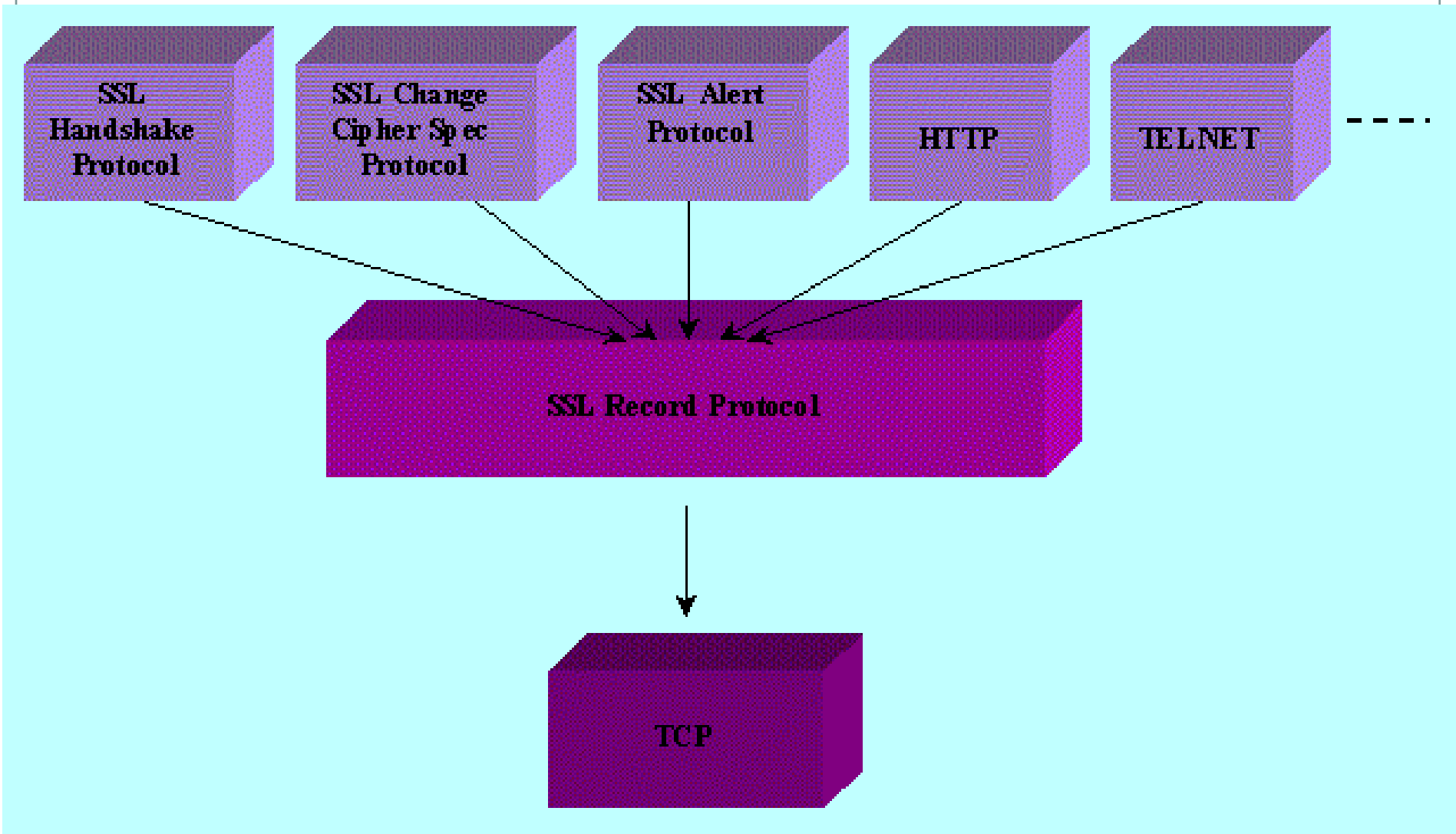
- Authentification par certificat (initiale)
- Application de codes d'intégrité
- Application de chiffrement

- Echanges sécurisés

Structure

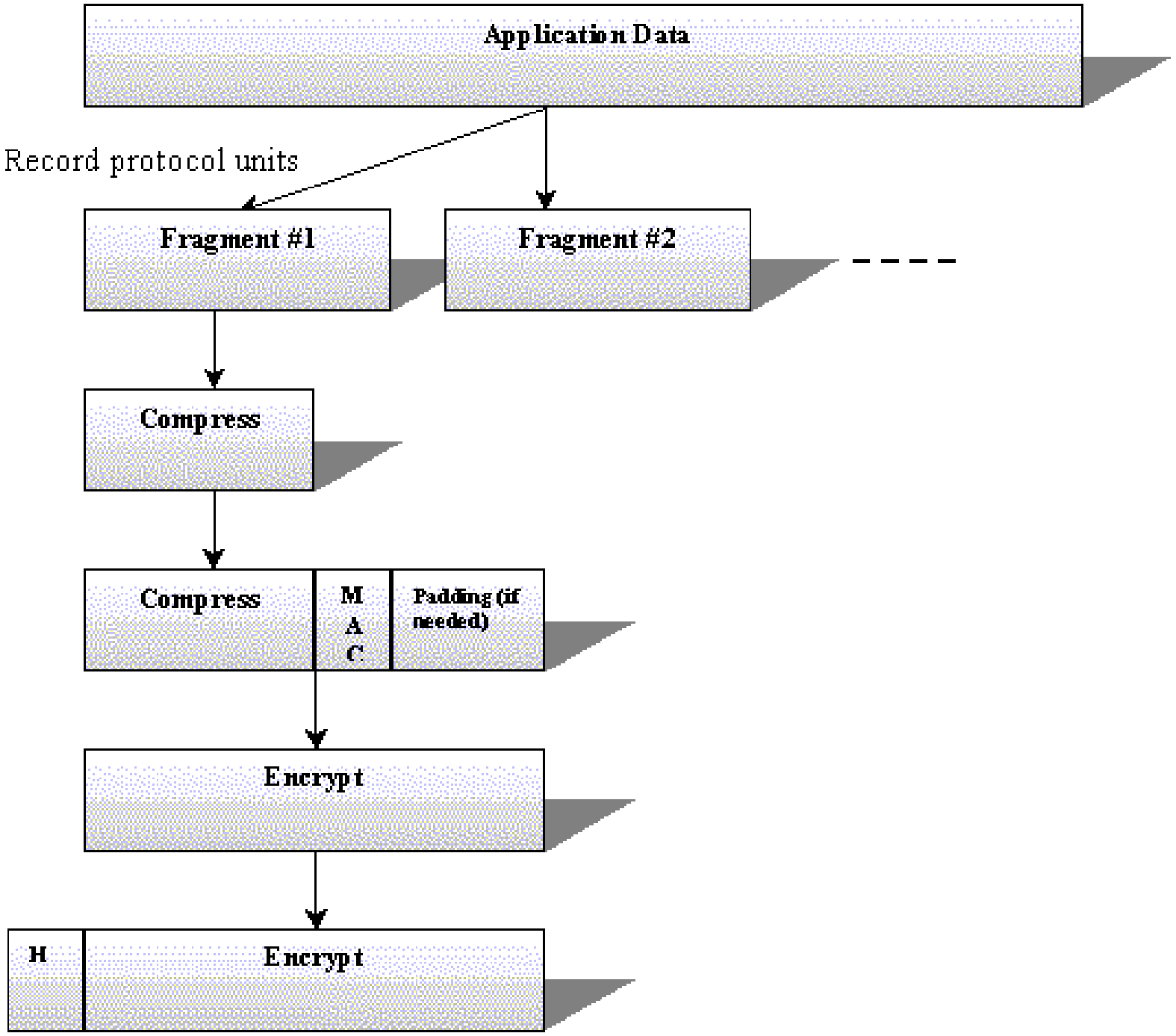
- Situé : Couche Session/Transport

- 2 sous-couches :
  - Hansdshake protocole (gestion de la conexion)
  - Record Protocol (transfert des données)


SSL Handshake Protocol
SSL Change Cipher Spec Protocol
SSL Alert Protocol
HTTP
TELNET
SSL Record Protocol
TCP

Couche Basse
Record protocol

- Record protocol = couche basse
- Rend les services suivants :
  - Fragmentation
  - Compression (Optionelle)
  - Signature (MAC - Message Authentication Code)
  - Chiffrement
- (Et inversement)


Application Data
Record protocol units
Fragment #1
Fragment #2
Compress
Compress
M
A
C
Padding (if needed)
Encrypt
H
Encrypt

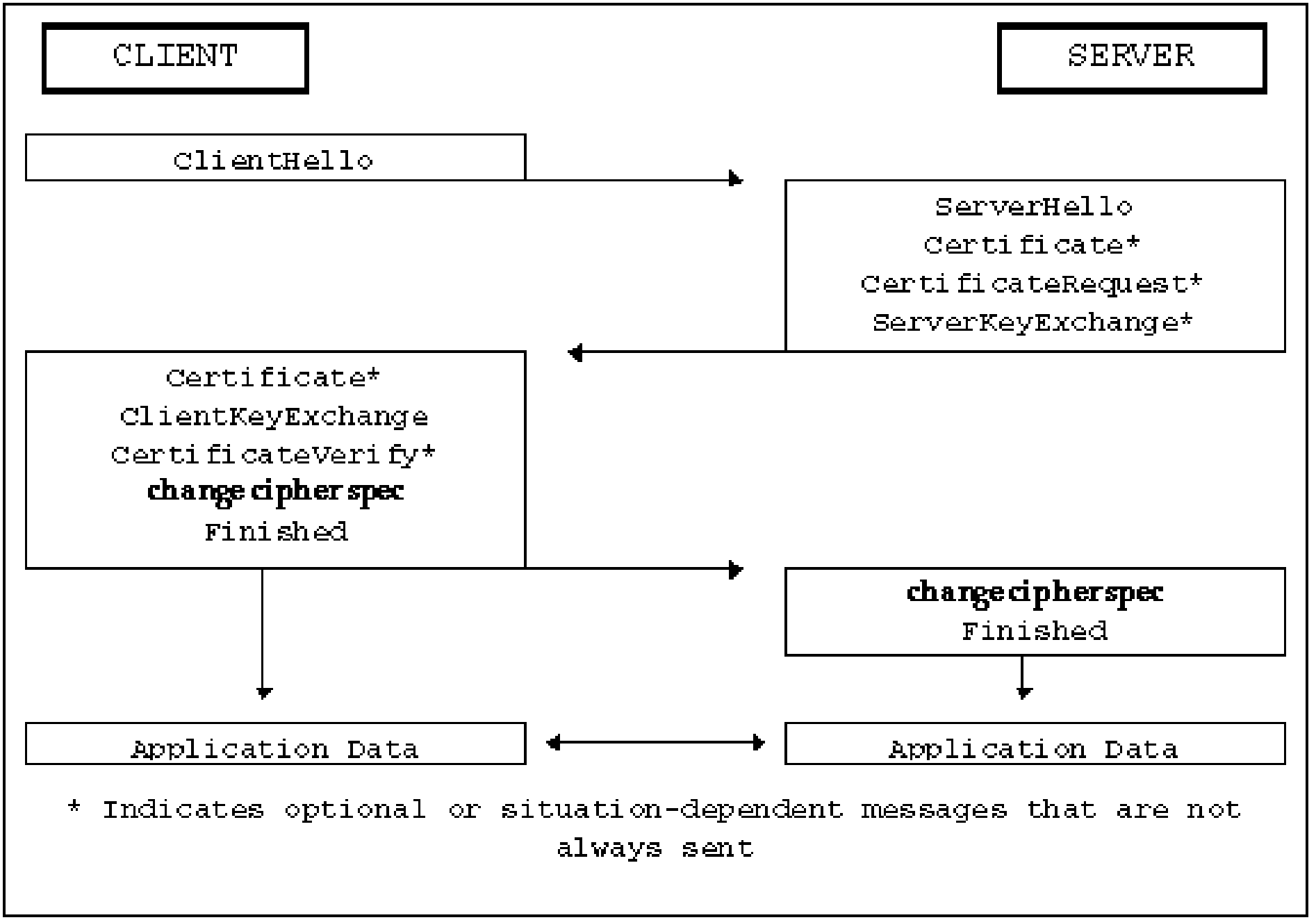
Couche Basse (2)
Record protocol

Type	Minor version	Major version	Record Length (< 2^{14}o)	Record Data
8 bits	8bits	8 bits	16 bits	< 2^{14} octets

Donnée du protocole supérieur (*Handshake Protocol*)

Couche Haute
Handshake Protocole

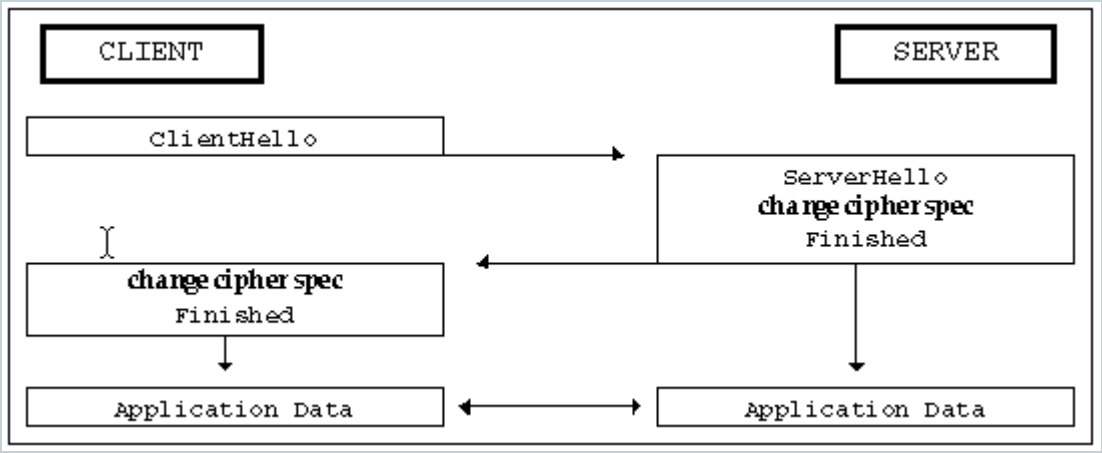
- Sous-couche haute de SSL
- Services rendus:
  - Authentification (forte)
  - Etablissement de la connexion
- Principe : Déclarer un contexte de variables
  - Numéros de messages
  - Clés de chiffrement


CLIENT
SERVER
ClientHello
ServerHello
Certificate*
CertificateRequest*
ServerKeyExchange*
Certificate*
ClientKeyExchange
CertificateVerify*
change cipher spec
Finished
change cipher spec
Finished
Application Data
Application Data
* Indicates optional or situation-dependent messages that are not always sent

Couche Haute (2)
Change Cipher Spec Protocol

- Niveau : couche haute de SSL
- Service rendu :
  - Changer de mode de chiffrement

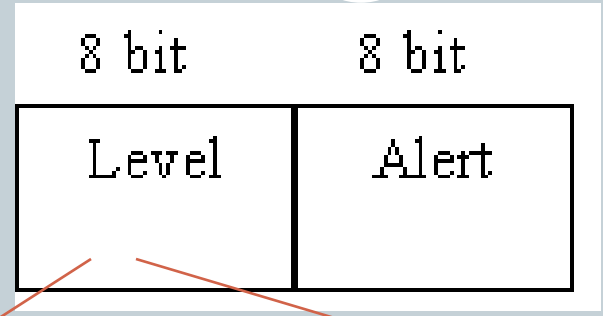
Change Cipher Spec Protocol



Couche Haute (3)
Alert Protocol

- Niveau : couche Haute de SSL
- Service rendu :
  - Signaler une erreur

Couche Haute (4)
Alert Protocol



Fatal Alert	Warning Alert
Unexpected_message- an inappropriate message was received.	**close_notify-** notifies recipient that the sender terminates the connection.
Bad_record_mac- bad MAC calculation.	**no_certificate-** the client has no appropriate certificate.
Decompression_failure- the length after decompression exceeded its maximum.	**bad_certificate-**the received certificate is damaged.
Handshake_failure- indicates an error in negotiation of security parameters.	**Unsupported_ certificate-**the certificate is of unsupported type.
Illegal_parameter- inconsistency within fields of the Handshake protocol.	**Certificate_revoked-** the certificate was canceled by its signer.
	Certificate_expired- the certificate validity expired.
	Certificate_unknown- an unexpected matter arose in processing the certificate, making it unacceptable.

Attaques

- SSL 2 obsolète
- SSL 3/TLS très sécurisé
  - Sans grosse faille intrinsèque
- Vulnérabilités dues à l'utilisateur

Attaques (2)

- Analyse de trafic
  - Pas géré
- Copier-coller
  - MAC dépend de seq+session+peer
- CipherSuite/Version Rollback
  - CipherSuite handshake fixe
  - Version : RSA contient indicateur v3

Attaques(3)

- Short block
  - Pas de short block
- Homme du milieu (« MITM »)
  - Authentification rigoureuse
- Dictionary attacks
  - This attack works in a situation when an attacker knows some of the plain text in the original message. In this case, an attacker would try to encrypt the known part of the plain text with every possible key until he found occurrences in the cipher text itself. If one is found, the whole message can be decrypted with the suitable key.
  - SSL prevents this attack by using strong encryption algorithms, like IDEA (128 bits) or 3DES (168 bits).

Conclusion

- SSL est très efficace
- Très utilisé
- A connaitre et à utiliser

- Attention à l'authentification