Securitatea retelelor

Universitatea “Transilvania” din Brasov

Capitolul : SSL und TLS

4. Network Security

costel.aldea@unitbv.ro

4. Network Security

costel.aldea@unitbv.ro

SSL (Secure Socket Layer)

- Construirea conexiuni HTTP autentificate și criptate între client și server de web .
- este suportat de majoritatea browserelor Web acceptate (https:// ...)
- Inițial dezvoltat de Netscape Communications Versiunea 3 (SSLv3) publică standardul Internet "de facto “
- Grup de lucru TLS al IETF a dezvoltat o "Common Standard" (aproximativ SSLv3.1)
- De asemenea a dezvoltat conexiuni Secure FTP, e-mail și Telnet posibil folosind protocolul SSL
- Functii:
    1. Autentificarea partenerilor de comunicare (semnătură digitală)
    2. Transfer de date confidențiale (criptare payload)
    3. Integritatea datelor (HashValue, MAC).
- Negocierea procesului și a cheii de sesiune este o parte integrata a Componentei de protocol (spre deosebire de IPSec)

SSL ...

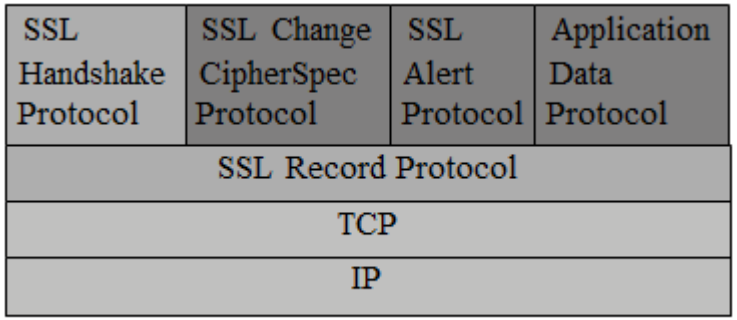
- Compuși cu ajutorul unui "Handshakes" în mai multi pași.

- Constă din două straturi (protocol cu două straturi), situată imediat deasupra stratului de TCP / IP :

  stratul superior: strat de aplicare (inclusiv part-protocoale)

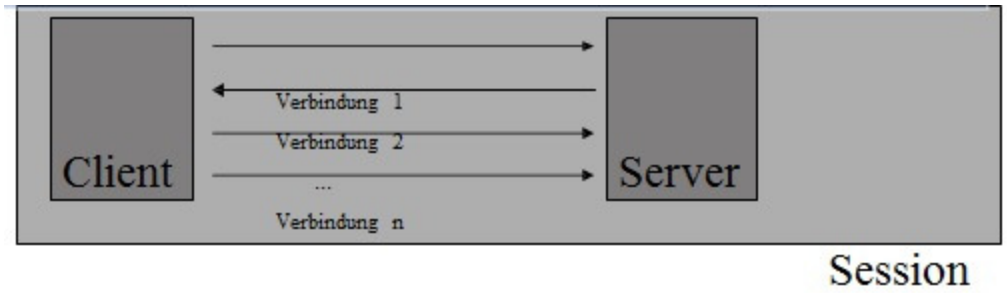
  strat inferior: strat de criptare

- Transparent la protocoalele de la nivelul aplicație



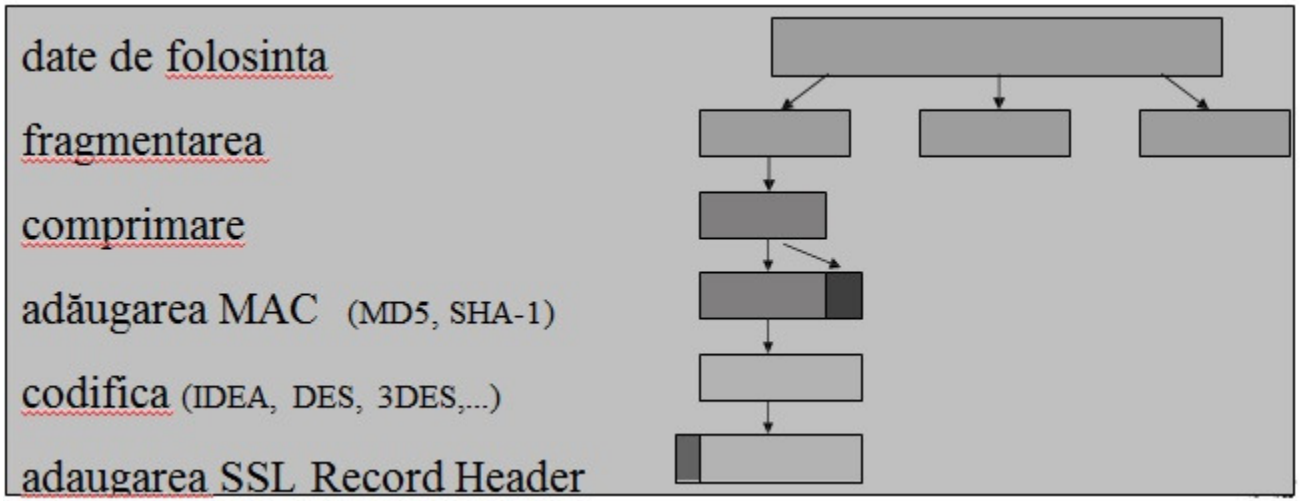
SSL Session (Client-Server)

- cuprinde o multitudine de conexiuni pentru schimbul de date
- Se initializeaza prin protocolul "Handshake" (mai multe faze)
- Protocol "Handshake" pentru autentificarea pe server si a clientului (optional) si a acordului parametriilor de securitate pentru legaturile sesiunii
- Ulterior se face schimb de date folosind protocolul SSL Record



SSL Record Protocol

Integritate a datelor prin adăugarea funcție hash (MAC)
Confidentialitatea datelor (criptare simetrică) la înregistrare



SSL Change Cipher Spec si Alert Protocol

Change Cipher SpecProtocol

•Procedurile convenite sunt comunicate catere stratul de inregistrare a protocolului.

•Modifica Cipher Suite al protocolului de inregistrare.

Alert Protocol

Trimiterea de avertismente

- Conexiune va rămâne, dar nu mai mult în acest noua sesiune.
- Eroare de certificat, certificat expirat, nu mai solicitare de a trimitere, ...

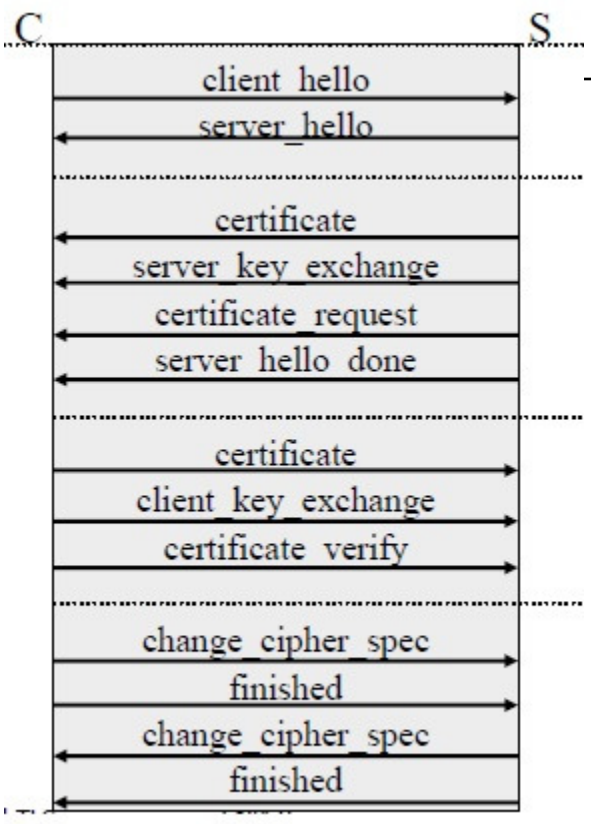
Tratamentul de Erori

- Conexiunea este terminată imediat
- MAC gresit , parametru "Handshake" incorect (Parametru de securitate) .....

SSL Handshake Protocol

- La inițierea unei sesiuni
- Este tratată înainte de schimbul efectiv de date aplicare
- Autentificarea de server și client
- Acordul din Cipher Suite
- Se compune din patru etape principale (vezi urmatorul slide)
- După finalizarea schimbului de date începe în conformitate cu acordurile de securitate
- Dezavantaj: acord cu privire la cel mai mare numitor comun, astfel încât algoritmi foarte slabi pot fi utilizati

SSL Handshake Protocol Ablauf



Etapa 1

Înlocuiți resurse de siguranță, printre altele, versiunea Protocolului, Session ID, Cipher Suite, numere aleatoare, Compresie

Etapa 2

Aici, serverul trimite certificatul său , are loc schimbul de chei certificate si eventual serverul poate solicita de la client un certificat . Serverul semnaleaza sfarsitul fazei de transmisie

Etapa 3

Materialul cheie a clientilor verifica certificatul serverului

Etapa 4

Cipher Suite este inversata si protocolul HandShake este finalizat

SSL Handshake Etapa 1

- Versiunea: cea mai recenta versiune SSL susținută de către client
- Numere aleatoare: 32 bit timp timbru + 28 bit de numere aleatorii rS , rC
- Session ID : servește pentru a reînnoi parametrii de sesiune (ID> 0) sau pentru a construi o nouă legătură într-o nouă sesiune (ID = 0)
- Lista de priorități Cipher Suite :

Key-Exchange Methode : RSA, Diffie-Hellman
algoritm de criptare: RC4, RC2, DES, 3DES, DES40, IDEA, Fortezza
Algoritm-MAC : MD5 sau SHA-1
Chiffre-Typ : Block- sau Stromchiffre
hashing : kein (0 Byte), MD5 (16) sau SHA-1 (20)

Lista de priorități pentru metoda de compresie

SSL Handshake Etapa 2 - 4

- Sunt realizate metode de schimb "uzuale" și de verificare
- "Master Secret" este folosit ca material de bază pentru criptarea negociabila
- Fiecare mesaj este protejat de un MAC fata de parametrii actuali precum si de Valorile din mesajele anterioare .
- Mesajele din Die server_finish und client_finish conțin un nou hash a tuturor mesajelor anterioare schimbate (!)

Generarea de chei SSL și schimbul de chei

- Mesajul client Key Exchange conține informații de bază ca Pre-Master Secret Pre (48 de biți), care este transmis criptat de către RSA
- Calcularea "Master Secret" (48 de biți) prin intermediul unor funcții hash :

$$ms := MD5(pre \mid SHA(A \mid pre \mid r_C \mid r_S)) \mid$$
$$MD5(pre \mid SHA(BB \mid pre \mid r_c \mid r_S)) \mid \; MD5(pre \mid SHA(CCC \mid pre \mid r_C \mid r_S))$$

- Atât cheia de calcul a valorii hash MAC și cheia de criptare a înregistrărilor referitoare la client și partea de server sunt calculate pentru fiecare compus din ms secrete de master, aceasta este o secvență de blocuri cheie KB generat până când toate conexiunile "livrările" sunt :

$$kb := MD5(ms \mid SHA(A \mid ms \mid r_S \mid r_C)) \mid$$
$$MD5(ms \mid SHA(BB \mid ms \mid r_S \mid r_C)) \mid MD5(ms \mid SHA(CCC \mid ms \mid r_S \mid r_C)) \mid [...]$$

TLS (Transport Level Security)

- Propus Standard Internet (RFC 2246)

Diferențele de SSLv3

•Numărul de versiune : Număr versiune majoră: 3, Număr de versiune scuzata : 1

•Mesaj de autentificare Cod HMAC în toate domeniile, precum și în numărul de versiune SSLv3 + a versiunii TLS folosit

•Coduri noi de alertă

de exemplu: CA Necunoscut, versiunea de protocol necunoscuta , cifru prea slab

•Cipher Suite

Fortezza nu mai este acceptat (uneori, de asemenea, AES)

•Calcule criptografice

MasterSecret este distribuit diferit, o nouă funcție de numere aleatorii