4. Network Security

Capitolul : SSL und TLS

Prof. Dr. Ulrich Bühler

4. Network Security

SSL (Secure Socket Layer)

- Aufbau authentisierter und verschlüsselter HTTP-Verbindungen zwischen Web-Client und Web-Server
- wird von den meisten WWW-Browsern unterstützt (https://...)
- Ursprünglich von Netscape Communications entwickelt Version 3 (SSLv3) öffentlicher de facto Internet Standard
- TLS-Arbeitsgruppe des IETF entwickelt einen ‚Common Standard' (quasi SSLv3.1)
- Auch sichere ftp-, eMail und Telnet-Verbindungen über SSL-Protokoll möglich
- Funktionen:
  - Authentifikation der Kommunikationspartner (digital signature)
  - Vertrauliche Datenübertragung (payload encryption)
  - Integrität der Daten (hashvalue, MAC)

- Aushandeln der Verfahren und der Sitzungsschlüssel ist integraler Protokollbestandteil (Unterschied zu IPSec)

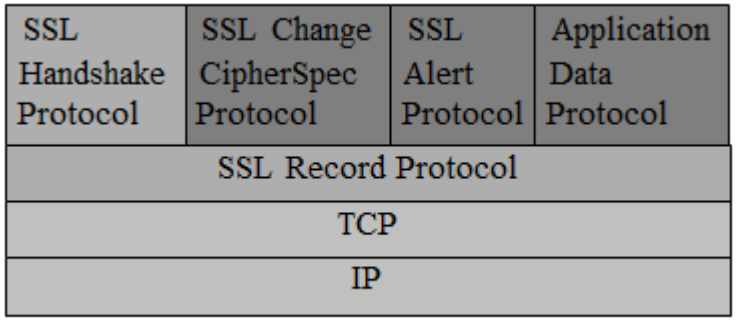
SSL ...

- Verbindungen werden mittels eines Handshakes in mehreren Schritten aufgebaut.
- Besteht aus 2 Schichten (Zwei-Schichten-Protokoll) unmittelbar über der TCP/IP-Schicht angesiedelt:

  obere Schicht: Anwendungsschicht (inkl. Teilprotokolle)

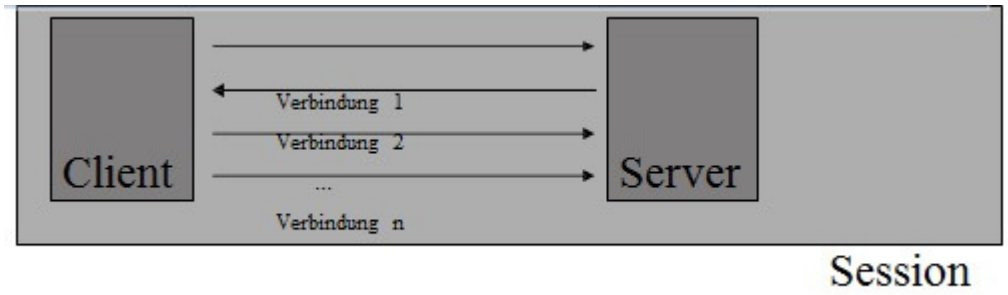
  untere Schicht: Verschlüsselungsschicht

- Transparent für die Protokolle der Anwendungsschicht



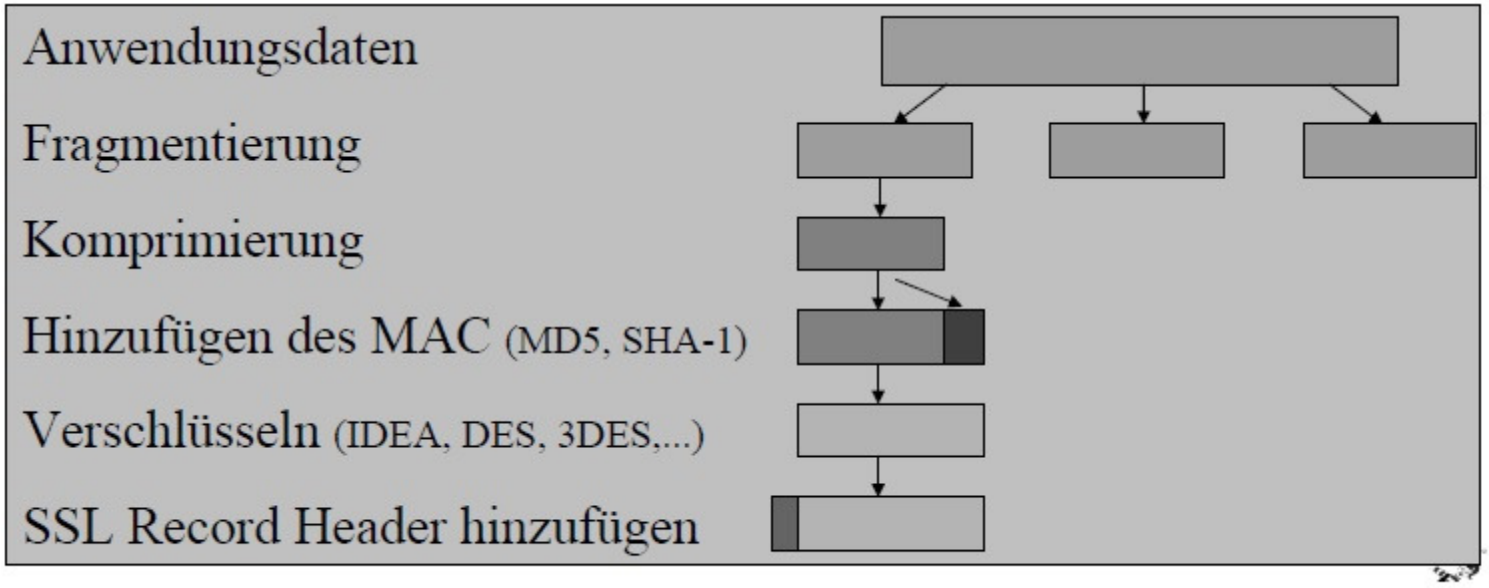
SSL Session (Client-Server Beziehung)

- besteht aus mehreren Verbindungen zum Austausch von Daten.
- Wird durch Handshake Protokoll initiiert (mehrere Phasen).
- Handshake protocol zur Authentifikation des Servers und des Clients (optional) und zur Vereinbarung der Sicherheitsparameter für die Verbindungen der Session (cipher suite)
- Anschließend Datenaustausch mittels SSL Record protocol



SSL Record Protocol

- Integrität der Daten durch Hinzufügen des Hashwertes (MAC)
- Vertraulichkeit der Daten (symmetrische Verschlüsselung) im Record



SSL Change Cipher Spec und Alert Protocol

Change Cipher SpecProtocol

•Vereinbarte Verfahren werden der Record-Protocol-Schicht mitgeteilt

•Änderungen der Cipher Suite des Record Protocols

Alert Protocol

Versenden von Warnungen

- Verbindung bleibt bestehen, aber keine neuen mehr in dieser Session
- Zertifikatsfehler, Zertifikat abgelaufen, kein Sendewunsch mehr, ...

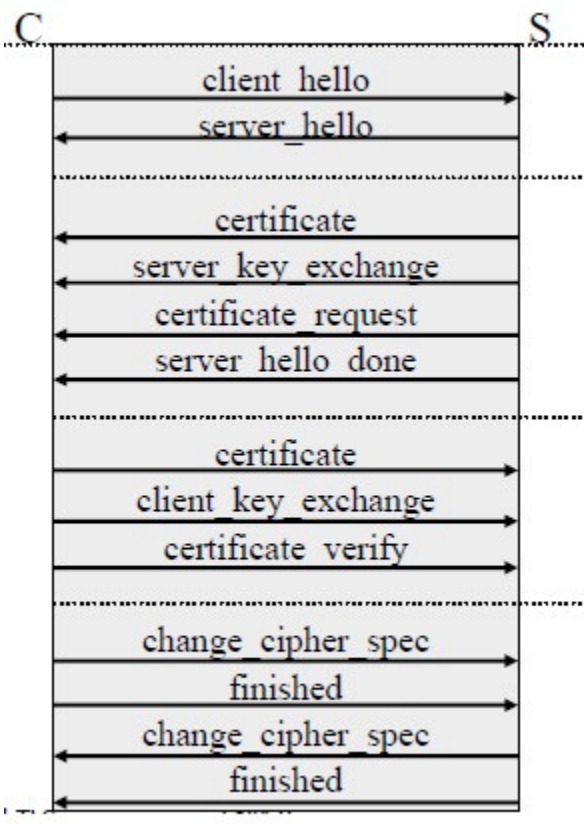
Behandlung von Fehlern

- Verbindung wird sofort beendet
- Falscher MAC, Handshake Parameter falsch (Sicherheitsparameter), ...

SSL Handshake Protocol

- Zur Initiierung einer Session
- Wird vor eigentlichem Austausch der Anwendungsdaten abgewickelt
- Authentifizierung des Servers und des Clients
- Vereinbarung der Cipher Suite
- Besteht aus 4 Hauptphasen (siehe nächste Folie)
- Nach Abschluß beginnt der Datenaustausch entsprechend der Sicherheitsvereinbarungen
- Nachteil: Einigung auf den größten gemeinsamen Nenner, so dass sehr schwache Algorithmen eingesetzt werden können

SSL Handshake Protocol Ablauf



Phase 1

Sicherheits-Ressourcen austauschen, u.a. Protokollversion, Session ID, Cipher Suite, Zufallszahlen, Komprimierung

Phase 2

Hier sendet der Server sein Zertifikat, Schlüsselaustausch findet statt, und evtl. kann der Server vom Client auch ein Zertifikat verlangen. Der Server signalisiert das Ende seiner Sendephase.

Phase 3

Client sendet sein Zertifikat (falls verlangt). Schlüsselmaterial des Clients, Verifizierung des Server-Zertifikats.

Phase 4

CipherSuite wird gewechselt und das HandshakeProtocol abgeschlossen.

SSL Handshake Etapa 1

- Version: Die höchste SSL-Version, die der Client unterstützt
- Zufallszahlen: 32 Bit Zeitstempel + 28 Bit Zufallszahl rS , rC
- Session ID: Dient zum Erneuern der Session-Parameter (ID>0) oder zum Aufbau einer neuen Verbindung in einer neuen Sitzung (ID=0)
- Cipher Suite Prioritätenliste:

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)

Prioritätenliste für Kompressionsverfahren

SSL Handshake Etapa 2 - 4

- „Übliche“ Austausch- sowie Verifizierungsmethoden werden durchgeführt
- „Master Secret“ als Basismaterial zur Verschlüsselung wird verhandelt
- Jede Nachricht wird durch einen MAC über aktuelle (vor allem Zufällige) Parameter sowie Werte aus vorhergehenden Nachrichten geschützt .
- Die server_finish und client_finish Nachrichten enthalten noch einmal einen Hash über alle (!) vorhergehenden ausgetauschten Nachrichten.

Generarea de chei SSL și schimbul de chei

- Client Key Exchange -Nachricht enthält als Basisinformation das Pre-Master Secret Pre (48 Bit), das verschlüsselt nach dem RSA übertragen wird
- Berechnung des Master Secret (48 Bit) mittels der Hashfunktionen :

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

- Aus dem Master-Secret ms werden sowohl der Schlüssel für die Berechnung des MAC-Hashwertes als auch der Schlüssel für die Verschlüsselung der Records auf Client- und Serverseite für jede Verbindung berechnet; dazu wird eine Folge von Schlüsselblöcken kb erzeugt bis alle Verbindungen „versorgt“ sind:

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

TLS (Transport Level Security)

- Proposed Internet Standard (RFC 2246)

Diferențele de SSLv3

•Versionsnummer Hauptversionsnummer: 3, Niedere Versionsnummer: 1
•Message Authentication Code HMAC, alle Felder wie auch in SSLv3 + Versionsnummer der verwendeten TLS-Version
•Neue Alert Codes
z.B.: Unbekannte CA, Protokollversion unbekannt, Zu schwache Chiffre
•Cipher Suite
Fortezza wird nicht mehr unterstützt (irgendwann auch AES)
•Kryptographische Berechnungen
MasterSecret wird anders gehasht, neue Zufallszahlenfunktion