IT-Sicherheit

- Sicherheit vernetzter Systeme -

Kapitel 12: Netzsicherheit - Schicht 4: Transport Layer SSL / TLS

Inhalt

- Transport Layer Funktionen
- Secure Socket Layer (SSL); Transport Layer Security (TLS) - Historie
- SSL / TLS Protokol Architektur
  - SSL / TLS Record Protocol
  - SSL / TLS Handshake Protocol
  - Schlüsselerzeugung
- SSL / TLS Anwendung

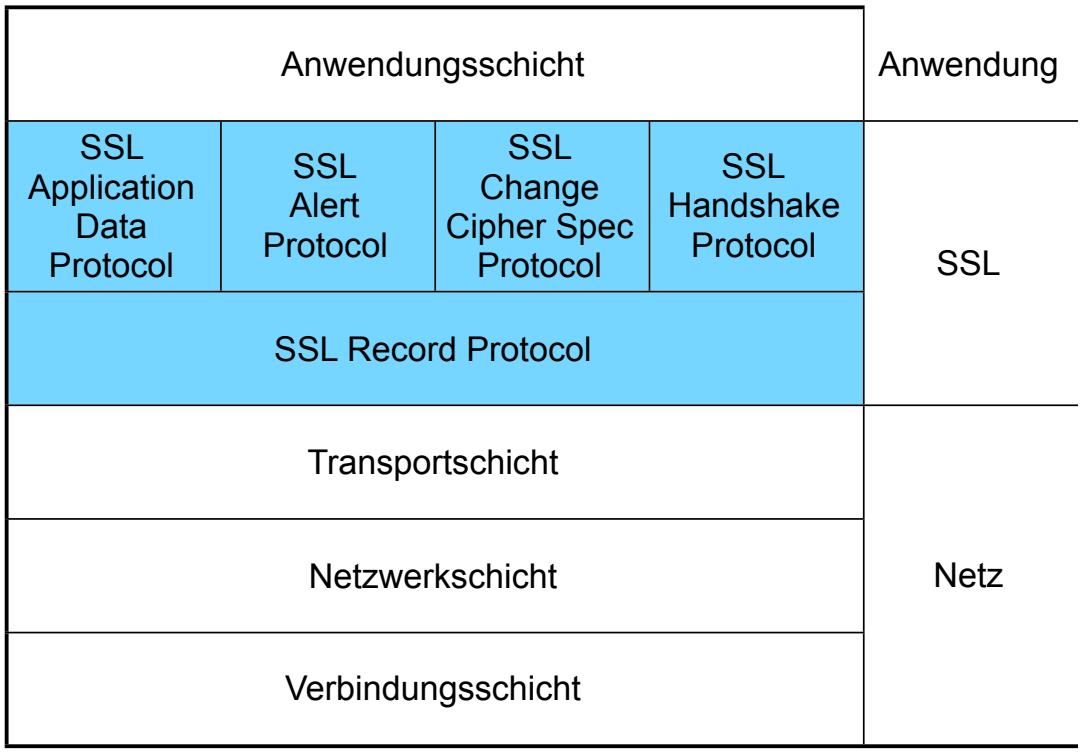
Transport Layer

- Nach OSI: Transportdienst zwischen Endsystemen; Ende-zu-Ende
  - Sicherer Transport von
  - Nachrichten der Endteilnehmer
- In der Internet-Welt: Ende zu Ende Verbindung zwischen Anwendungen
  - OSI-Schichten 5, 6 und 7 fallen in der Anwendungsschicht zusammen
  - Ports definieren die Prozesse (Dienste) der Anwendungsschicht
- Sicherungsprotokolle der Transportschicht
  - Setzten auf TCP oder UDP auf
  - Realisieren zum Teil die Funktionalität der Sitzunggschicht
  - Liegen zwischen Transport Layer und Application Layer

Secure Socket Layer (SSL) Historie

- Ab 1994 ursprünglich entwickelt um HTTP-Verkehr zu sichern (https); Entwickelt von Netscape und ab SSL v2 in deren Browser integriert
- 1995 Internet Explorer mit PCT (Private Communication Technology)
- SSL v3: Protokollverbesserungen (aus PCT) und de-facto Standard
- Kann beliebige Anwendungen sichern (nicht nur HTTP)
- IETF entwickelt, basierend auf SSL, ab 1996 Transport Layer Security (TLS)
  - SSL gehört der Firma Netscape
  - IETF basierte freie Spezifikation
  - TLS 1.0 und SSL 3.0 sind nahezu identisch
  - SSL und TLS werden häufig synonym gebraucht
  - TLS v1.1 [RFC 4346]

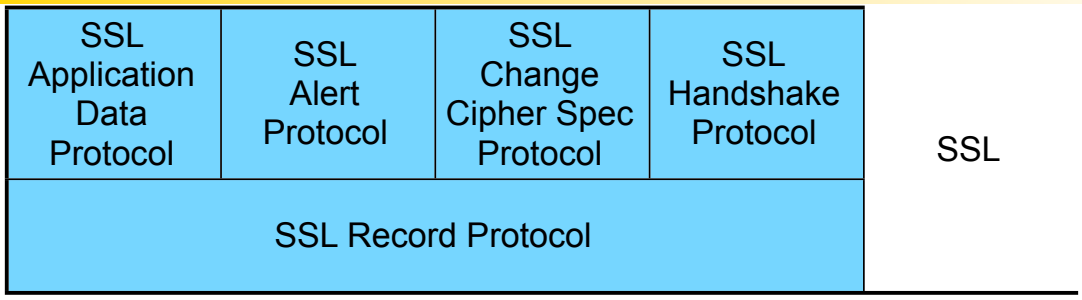
SSL/TLS Einordnung



SSL / TLS Überblick

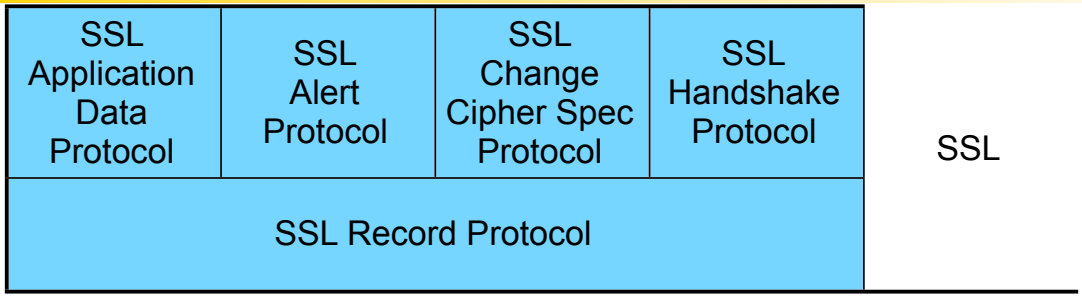
- Authentisierung
  - Vor der eigentlichen Kommunikation ist eine Authentisierung möglich
  - Einseitig oder auch zweiseitig
- Vertraulichkeit der Nutzdaten
  - Falls während des Sitzungsaufbaus vereinbart
  - Verschiedene Verschlüsselungsverfahren: RC2, RC4, DES, 3DES, DES40, IDEA, AES
- Integrität der Nutzdaten
  - Kryptographischer Hash-Wert, parametrisiert mit Schlüssel: HMAC
  - Algorithmen: MD5, SHA

SSL/TLS Protokoll Architektur



- Application Data Protocol
  - Datenübermittlung zwischen Anwedung und SSL
  - Zugriff auf Record Protocol
- Alert Protocol:
  - Warn- und Fehlermeldungen
- Change Cipher Spec Protocol
  - Änderung der Krypto-Verfahren
  - Initialisierung und Einigung auf neu zu verwendede Verfahren

SSL/TLS Protokoll Architektur (Forts.)



- Handshake Protokol:
  - Authentisierung
  - Schlüsselaustausch
  - Vereinbarung der Parameter
- Record Protocol
  - Fragmentierung
  - Kompression der Klartext-Daten (optional)
  - Verschlüsselung (optional)
  - Integritätssicherung (optional)

SSL/TLS Record Protocol

7	15	23	31
Type	Major Version	Minor Version	Length
Length	Data		

- Type
  - Change Cipher Spec (20)
  - Alert (21)
  - Handshake (22)
  - Application Data (23)
- Major und Minor Version (z.B. 3, 2 für TLS 1.1)
- Length: Länge der Daten in Byte

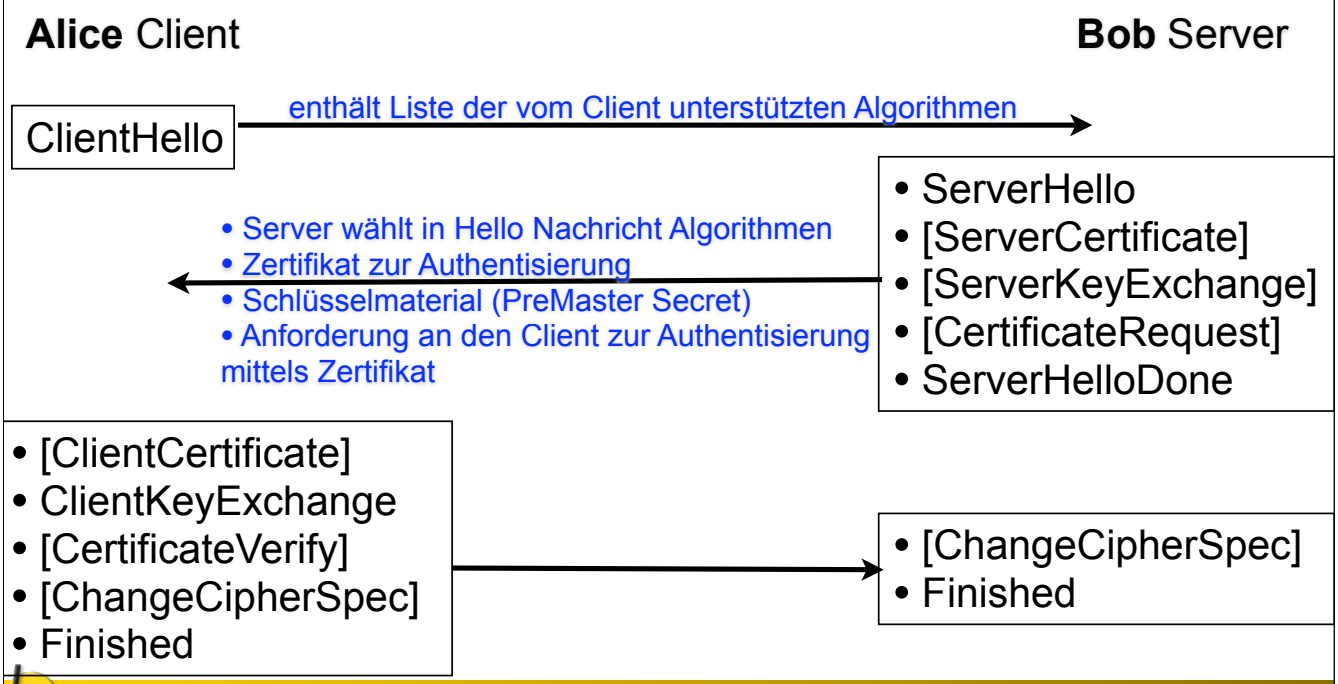
SSL/TLS Record Protocol

7	15	23	31
Type	Major Version	Minor Version	Length
Length	Data		

- Sender
  1. Fragmentierung der Nutz-Daten in max 2^{14} Byte
  2. Kompression der Daten (Default-Algorithmus *null*)
  3. Integritätssicherung mittels HMAC
  4. Verschlüsselung
- Empfänger:
  - Entschlüsselung; Integritäts-Check; Dekompression; Defragmentierung; Auslieferung an höhere Schicht

SSL/TLS Handshake Protokoll

- Zweck: Authentisierung, Algorithmenauswahl, Schlüsselmaterial



SSL/TLS Handshake Protocol: Schlüsselerzeugung

- Schlüssel werden aus dem PreMasterSecret abgeleitet
- PreMasterSecret (variable Länge) wird erzeugt:
  - **RSA**: Zufallszahl; mit dem öffentlichen Schlüssel des Servers verschlüsselt übertragen
  - **Diffie-Hellman**: Übertragung der Diffie-Hellman Gruppe unverschlüsselt; falls nicht schon in Zertifikat enthalten; Erzeugung des PreMasterSecret über Diffie-Hellman Verfahren
- MasterSecret (immer 48 Byte) wird aus PremasterSec. erzeugt
  - MasterSecret = PRF (PreMasterSecret, „Master Secret“, ClientHello.random + ServerHello.random)

SSL / TLS Schlüsselgenerierung

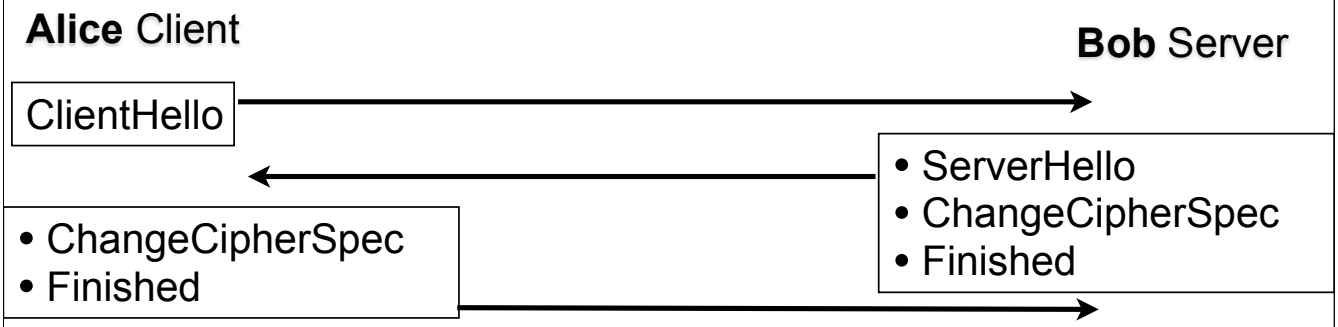
- KeyBlock = PRF (SecurityParameter.MasterSecret,
  „key expansion“,
  SecurityParameter.ServerRandom +
  SecurityParameter.ClientRandom)
- Der KeyBlock wird in folgende Teilblöcke zerlegt
  - client_write_MAC_secret [SecurityParameter.HashSize]
  - server_write_MAC_secret [SecurityParameter.HashSize]
  - client_write_key [SecurityParameter.KeyMaterialLength]
  - server_write_key [SecurityParameter.KeyMaterialLength]
- SSL erlaubt Schlüsselerzeugung auch ohne Authentisierung
  - In diesem Fall Man-in-the-Middle-Attack möglich und nicht erkennbar

SSL/TLS: Pseudo Random Function (PRF)

- Pseudo-Random Function (PRF); gebildet aus MD5 und SHA
- PRF soll Sicherheit bieten auch wenn MD5 oder SHA „gebrochen“ werden
- Expansionsfunktion P_hash(secret, seed)
  - Durch iterative Anwendung Schlüsselmaterial in beliebiger Länge
  - P_hash(secret,seed) = HMAC_hash(secret, A(1) | seed) |
    HMAC_hash(secret, A(2) | seed) |
    ...
    HMAC_hash(secret, A(n) | seed) mit
  - A(0) = seed
    A(i) = HMAC_hash(secret, A(i-1));
- PRF(secret, label, seed) = P_MD5(S1, label + seed) XOR
  P_SHA-1(S2, label + seed)
  - mit secret zerlegt in zwei Teilstrings S1 und S2

SSL Abbreviated Handshake

- Erlaubt Wiederverwendung und Duplizierung eines bestehenden Sicherheitskontextes
- HTTP 1.0; Jedes Item einer Webseite wird über eigene TCP Verbindung übertragen



- ClientHello enthält SessionID der zu duplizierenden Session
- Falls Server SessionID findet und duplizieren will sendet er SessionID in ServerHello zurück

SSL/TLS Anwendung

- Auswahl an SSL gesicherten Diensten

Port	gesicherter Dienst	Protokoll
443	HTTP	https
465, 587	SMTP (Mail)	ssmtp oder smtps
585,993	IMAP	imap4-ssl
636	LDAP	ldaps
989, 990	FTP	ftps
992	Telnet	telnets
995	POP3	pop3s

Einschub: OpenSSL Security Alert [07-Jan-2009]

- Incorrect checks for malformed signatures
- Systems affected:
  - OpenSSL prior to release 0.9.8.j
- Description / Impact:
  - Imlementaion error : malformed signature can be treated as a good signature rather than an error
- Impact:
  - Man in the middle attack
  - Bypassing validation
- Solution:
  - Upgade to OpenSSL 0.9.8j
  -
- Quelle:
  - `http://www.openssl.org/news/secadv_20090107.txt`