

# Secure Sockets Layer

Eren Metin Elci

3. Pforzheimer Linux Infotag

# Gliederung

- 1 Einführung
  - Motivation
  - Kryptographie
  - Zertifikate
  
- 2 Secure Sockets Layer
  - Definition
  - Handshake-Protokoll
  - Record-Protokoll

# Gliederung

- 1 Einführung
  - Motivation
  - Kryptographie
  - Zertifikate
- 2 Secure Sockets Layer
  - Definition
  - Handshake-Protokoll
  - Record-Protokoll

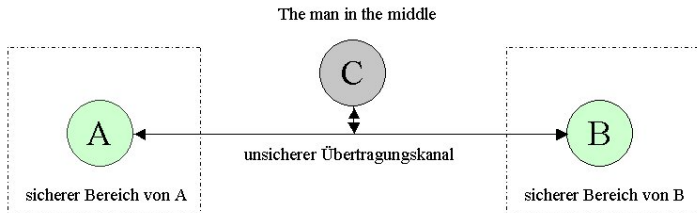
# Möglichkeiten des Internets

- Kommunikation
  - eMail
  - VoIP/Skype
  - ICQ/IRC
- eCommerce
- Online-Banking
- Steuererklärung

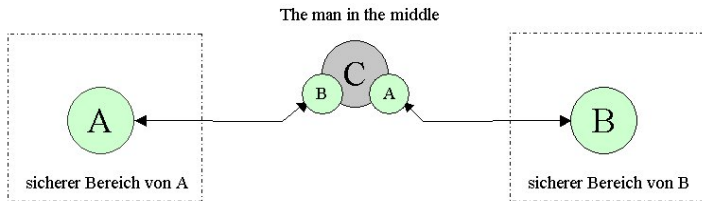
# Protokolle

- HTTP
- POP/SMTP
- TCP/IP
- Offene, unverschlüsselte Übertragung

# The Man in the Middle



- Verlust der Privatsphäre
  - Bankgeheimnis
  - Datenschutz



- Verlust der Nachrichtenintegrität
- Autentizitätsverlust

# Gliederung

- 1 Einführung
  - Motivation
  - **Kryptographie**
  - Zertifikate
  
- 2 Secure Sockets Layer
  - Definition
  - Handshake-Protokoll
  - Record-Protokoll

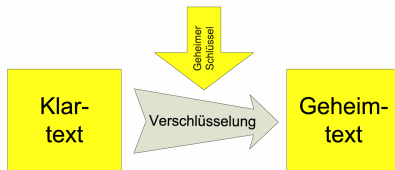
# Begrifflichkeit

- Vom griechischen *kryptós*, „verborgen“, und *gráphein*, „schreiben“
- Wissenschaft der Verschlüsselung von Informationen
- Caesar Verschlüsselung, Enigma

# Moderne Kryptographie

- Mathematische Algorithmen
  - Faktorisierung großer Zahlen (Zerlegung in Primzahlfaktoren)
- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung

# Symmetrische Verschlüsselung



- Geheimer Schlüssel zur Ver- und Entschlüsselung
- Schnelle Ver- und Entschlüsselung
- Problematisch: Schlüsselaustausch

# Symmetrische Verfahren

- Advanced Encryption Standard (Rijndael)
- Data Encryption Standard
- Blowfish/Twofish
- IDEA

# Asymmetrische Kryptosysteme

- Verwendung von Schlüsselpaaren
  - Public Key
  - Private Key

# Authentizität



# Privatsphäre

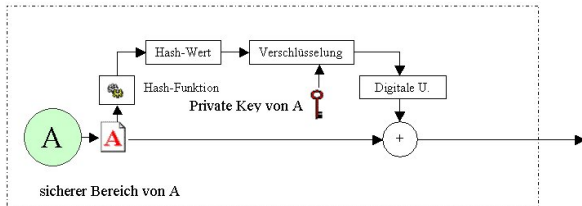


- + Schlüsselaustausch unproblematisch
- - Hohe Rechnerlast  $\Rightarrow$  Hybride Verfahren

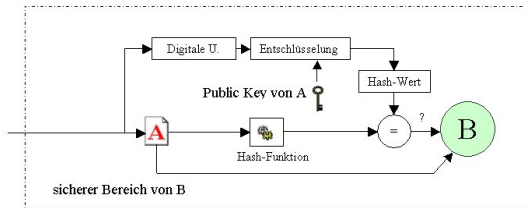
# Verfahren

- RSA
- Rabin
- Elgamal

# Digitale Unterschrift



- Hashwert als eindeutiger Fingerabdruck
- Veränderung bei Bitveränderungen
- One-Way-Hash  $\Rightarrow$  Keine Datenrekonstruktion



- Nachrichtenintegrität
- Authentizität

# Schlüsselerstellung

- Freie Schlüsselerstellung
- Keine Überprüfung
- Identitätsüberprüfung?  $\Rightarrow$  Zertifikate

# Gliederung

- 1 Einführung
  - Motivation
  - Kryptographie
  - Zertifikate
  
- 2 Secure Sockets Layer
  - Definition
  - Handshake-Protokoll
  - Record-Protokoll

# Digitale Ausweise

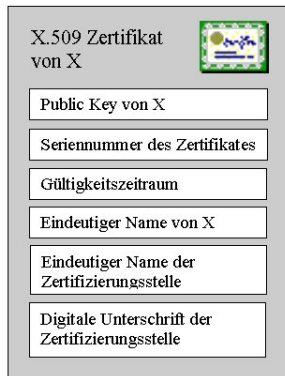
- Keine Identitätsüberprüfung bei Schlüsselerstellung
- Authentizität
- Zertifikate als digitale Ausweise

# Certificate Authorities

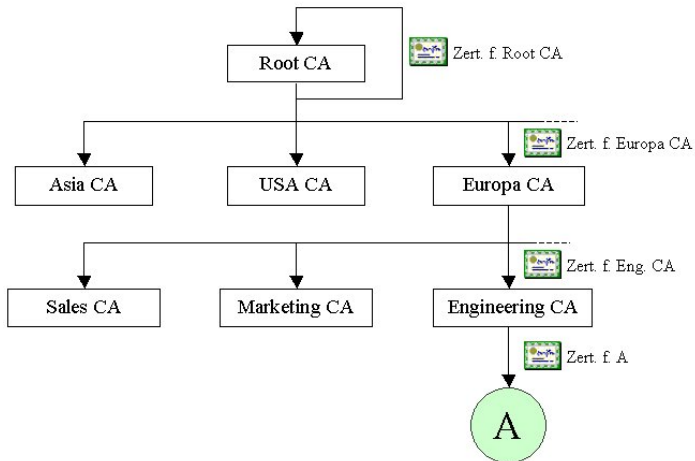
- Zertifizierungsstellen
- Identitätsüberprüfung
- Personalausweis/Führerschein

# Inhalte

- Implementierung in SSL
- Zusätzliche Liste aller Zertifizierungsstellen



# CA-Hierarchie

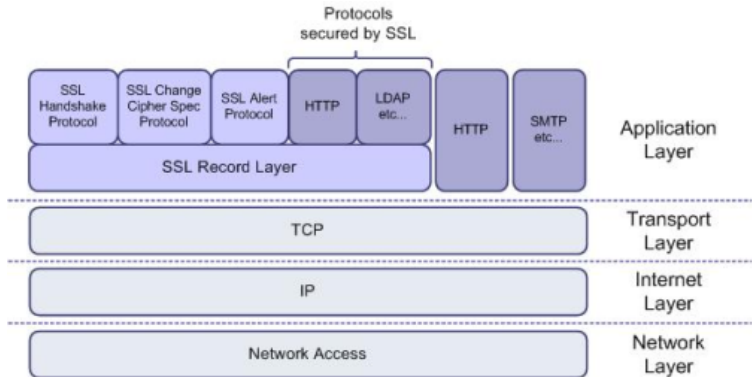


# Gliederung

- 1 Einführung
  - Motivation
  - Kryptographie
  - Zertifikate
- 2 Secure Sockets Layer
  - Definition
  - Handshake-Protokoll
  - Record-Protokoll

- Verschlüsselungsprotokoll für Datenübertragungen im Internet
- Sicherheitsmechanismen für Anwendungsprotokolle
- Transparente Implementation
- Versionen
  - SSL 3.0 (1996)
  - TLS/SSL 3.1 (1999)

# SSL im OSI-Modell



# Gliederung

- 1 Einführung
  - Motivation
  - Kryptographie
  - Zertifikate
- 2 Secure Sockets Layer
  - Definition
  - **Handshake-Protokoll**
  - Record-Protokoll

# Aufgabe

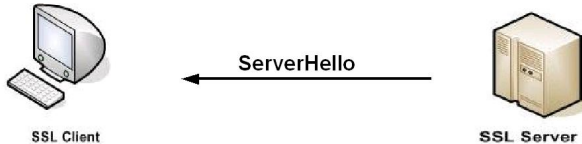
- Erstellung einer Session
  - Definition / Initialisierung der Sicherheitsparameter
  - Authentifizierung
  - Fehlermeldungen

# ClientHello



- Client Zeit im Unixformat
- 28 Random Bytes
- Session ID
- Vom Client unterstützte kryptographische Algorithmen
- Kompressionsverfahren
- SSL Version

# ServerHello



- Ausgewählte SessionID
- Verschlüsselungsalgorithmus
- Kompressionsmethode
- SSL Version

# ServerCertificate



SSL Client

Certificate

A horizontal arrow pointing from the server icon on the right towards the client icon on the left.

SSL Server

# CertificateRequest



SSL Client

← CertificateRequest →



SSL Server

# Server Hello Done



SSL Client

← ServerHelloDone →



SSL Server

# ClientCertificate



SSL Client

ClientCertificate →



SSL Server

# Client Key Exchange



- Generierung d. Premaster-Secrets
  - 48 zufällige Bytes
- Verschlüsselung mittels Public Key des Servers
  - s. Hybrides Verfahren

# Certificate Verify



- Authentifizierung des Clients durch Digitale Unterschrift

# Change Cipher Spec u. Finished Message



- Finished Message symmetrisch Verschlüsselt
  - Geheimer Schlüssel abgeleitet v. Master-Secret
- Beinhaltet HASH-Werte über
  - Alle gesendeten Nachrichten
  - Master-Secret

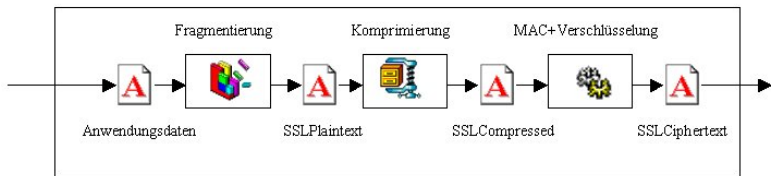
# Gliederung

- 1 Einführung
  - Motivation
  - Kryptographie
  - Zertifikate
- 2 Secure Sockets Layer
  - Definition
  - Handshake-Protokoll
  - Record-Protokoll

# SSL Low-Level

- Unterste Ebene im SSL Protokoll
- Verarbeitung der Nutzdaten
- Generierung einer MAC

# Arbeitsschritte



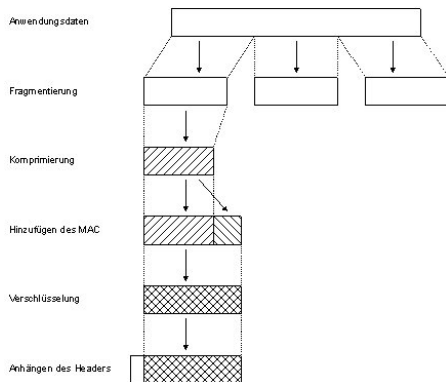
- SSLPlaintext Größe  $\leq 2^{14}$  Bytes
- Komprimierungsverfahren
  - NULL
  - GZIP

# MAC - Message Authentication Code

- Erkennung von Nachrichtenmodifizierungen
- HASH-Wert aus
  - SSLCompressed
  - Geheimer Schlüssel
  - ipad und opad
  - paketspezifische Sequenznummer
  - Protokoll Typ
  - Länge des SSLCompressed

# Verschlüsselung

- Verschlüsselung von
  - Datenblock
  - MAC



# SSL Record Header



- Content Type (8 Bit): Verarbeitungsprotokoll
- Major Version (8 Bit): SSL Hauptversion
- Minor Version (8 Bit): SSL Unterversion
- Compressed Length (16 Bit): Länge der Daten in Byte

# Ende

## Fragen?

Jetzt oder an [info@eren-elci.net](mailto:info@eren-elci.net)