# Verschlüsselung mit SSL/TLS

## Verschlüsselte Datenübertragung im Internet

Daniel Weber, 14.10.2013

# Anforderungen

- Verschlüsselung
  - Dritte sollen den Inhalt einer Nachricht nicht lesen können.
- Identität
  - Die Identität der Kommunikationspartner soll sichergestellt sein.
- Authentizität
  - Dritte sollen den Inhalt einer Nachricht nicht manipulieren können.

# symmetrische Verschlüsselung

- klassische Verschlüsselung
- beide Partner verwenden denselben Schlüssel
- Problem: sicherer Schlüsselaustausch?
- Problem: Vielzahl an geheimen Schlüsseln

# asymmetrische Verschlüsselung

- Schlüssel-Paar
  - privater Schlüssel
  - öffentlicher Schlüssel
- Schlüsselaustausch vorab nicht notwendig
- nur privater Schlüssel muss geheim bleiben
- Problem: Identität des Kommunikationspartners?
- Problem: Rechenaufwand

# Identitätsprüfung

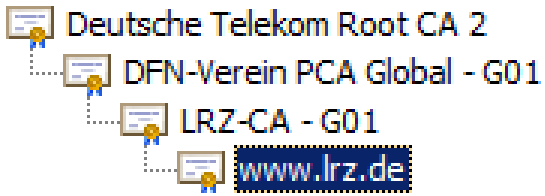
Zwei gängige Möglichkeiten:

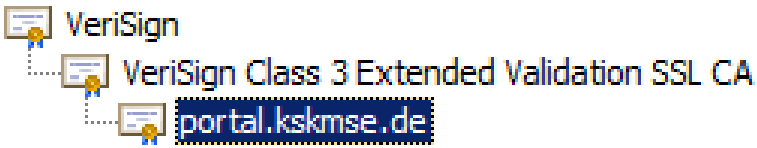
1. Vertrauensketten
   z.B. SSL/TLS

2. Vertrauensnetz
   z.B. GnuPG und PGP, manueller Aufbau

# Identitätsprüfung

- Software vertraut „ab Werk“ gängigen Zertifizierungsstellen (CAs) und dadurch deren Kunden



# Rechenaufwand

Lösung:

- Per asymmetrischer Verschlüsselung wird ein geheimer symmetrischer Schlüssel ausgehandelt

- Rechenaufwand nur beim Verbindungsaufbau

# Ablauf des Verbindungsaufbaus

| Client: | | Server: |
|---|---|---|
| 1. „Hello“ + Zufallszahl | → | |
| | ← | 2. „Hello“ + Zufallszahl |
| | ← | 3. öff. Schlüssel |
| 4. Prüfsumme, verschl. | → | |
| 5. Zufallszahl, verschl. | → | |
| 6. Verbindungsschlüssel errechnen | | 6. Verbindungsschlüssel errechnen |
| 7. Bestätigung | → | |
| | ← | 8. Bestätigung |

# Zustand woran erkennbar?

- Verschlüsselung im Internet Explorer


- Verschlüsselung im Firefox


- Identitätsprüfung gescheitert

# Anwendungsfall: Surfen

- Online-Banking
- Online-Shopping
- webbasiertes E-Mail
- Cloud-Dienste
- …

# Anwendungsfall: Mailverkehr

Was kann dabei verschlüsselt werden?

- nicht nur Inhalte sondern auch „Metadaten“
- Absender -> Server -> Server -> Empfänger

Aber:

- unverschlüsselte Speicherung auf Servern
- nicht jeder Schritt garantiert verschlüsselt

# Angriffsmöglichkeiten

- Unverschlüsselte Datenspeicherung auf den Servern (Mail, Cloud, Onlineshopping, …).
- Diebstahl und Missbrauch des privaten Schlüssels als „man in the middle“.
- Brute Force für bestimmte Mitschnitte: „Perfect Forward Privacy“ schützt davor
- Social Engineering: Täuschung des Benutzers statt der Technik.

# Gerüchteküche

„Geheimdienste können alles entschlüsseln.“ -> Falsch!

- „Brute Force“ um alles zu entschlüsseln ist zu teuer und braucht VIEL Platz und Strom
- staatlicher Zwang zur Herausgabe des privaten Schlüssels (siehe Lavabit)
- bereits genannte Angriffsmöglichkeiten

# Was tun?

- Wo immer es geht Verschlüsselung nutzen
  - Webseiten wenn möglich mit HTTPS statt HTTP aufrufen
  - Mails wenn möglich mit SSL oder TLS nutzen
    („E-Mail made in Germany“ alter Hut mit neuem Namen)

- Vorsicht bei „Cloud“-Diensten, sich bewusst sein, wem man welche Daten gibt.

- für Admins: den privaten Schlüssel schützen und regelmäßig tauschen

# Ende

Fragen?

Daniel Weber

daniel.weber@ebe-online.de