Online Banking

de Lorenzo, Hopfgartner, Leupold

February 13, 2011

Übersicht

- Geschichte
- Bedenken
- Verschlüsselungsarten
- Netzwerkarchitektur und Sicherheit
- Zusammenfassung und Fazit

Entwicklung

- Erste Systeme Anfang der 80er Jahre
- 1981 boten bereits vier große Banken einen Online-Service via "videotex" an
- 1983 boten die ersten europäischen Banken eine solche Dienstleistung an
- Die "Stanford Federal Credit Union" war die erste Bank die all ihren Mitgliedern einen Online-Banking-Service gewährte
- 2010 nutzen bereits 55 Millionen amerikanische Familien Online-Banking

Bedenken - Teil 1

Regierungen

- Kartellrechtliche Bedenken
- Konsumentenschutz
- Verwendung von hochqualitativen Verschlüsslungsalgorithmen

Unternehmen

- Sicherheit im Zahlungsverkehr
- Kundenverlust aufgrund fehlender Zahlungsmethoden

Bedenken - Teil 2

Banken

- Abhängig von Transaktionsgebühren
- Sicherheit der Computersysteme

Kunden

- Sicherheit der Systeme
- Sicherheit persönlicher Daten
  - 82% aller Amerikaner haben Bedenken im Bezug auf die Sicherheit ihrer persönlichen Daten

Anforderungen an die Technik

Anforderungen

1. Sicherheit
2. Anonymität (Datenschutz)
3. Authentifizierung

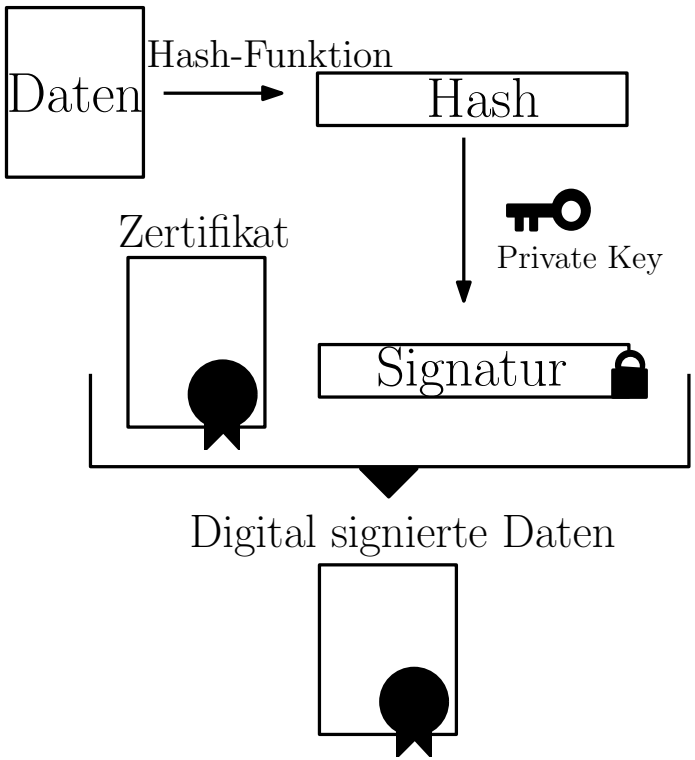
Software basierende Systeme

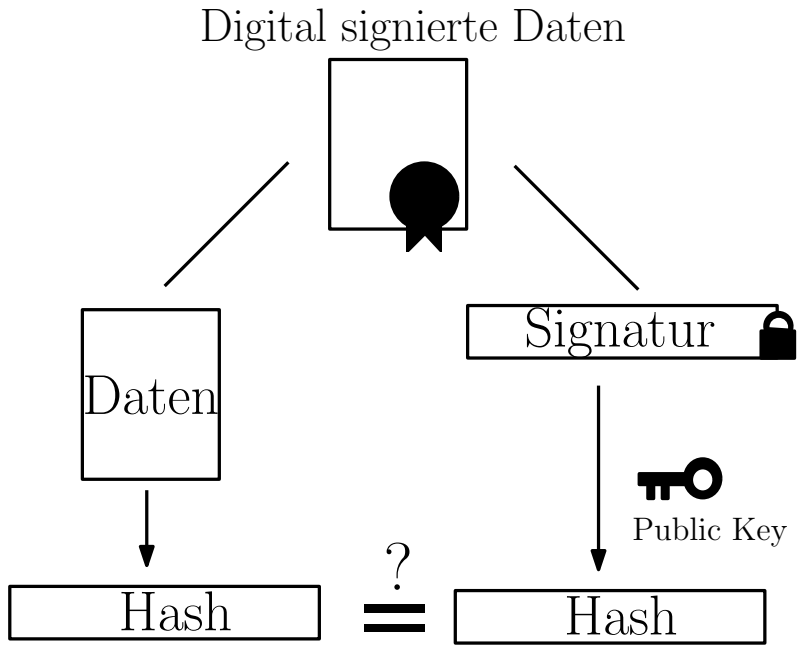
- En- und Dekodierung erfolgt rein über Sicherheits-Software
- Zwei grundlegende Methoden der Verschlüsselung
  1. Symmetrisches Kryptosystem
  2. Asymmetrisches Kryptosystem
- Beispiele für Software basierende Verschlüsselungsarten: RSA, Secure Electronic Transaction, Pretty Good Privacy ...

Digital Signature - Teil 1

- 1976 - Whitfield Diffie, Martin Hellman - Stanford University
- Bestätigt die Echtheit juristischer und finanzieller Dokumente
- Asymmetrisches Kryptosystem
- Kollisionsarm

Digital Signature - Teil 2





RSA - Teil 1

- Rivest, Shamir, Adleman
- Vierteljahrhundert ohne aufgebrochen zu werden
- Asymmetrisches Kryptosystem
- Verwendet für Verschlüsselung und digitale Signatur
- Nachteil: relativ langsam

RSA - Teil 2

Ablauf

1. Wähle zwei Primzahlen p und q, die größer sein als 1.024.
2. Berechne $n = p \times q$ und $z = (p - 1) \times (q - 1)$.
3. Wähle eine Zahl, die teilerfremd zu z ist, und nenne sie d.
4. Finde e so, dass $e \times d = 1 \ mod \ z$.

Beispiel

Wir wählen $p = 3$ und $q = 11$.

Klartext (P) | Chiffretext (C) | Nach der Entschlüsselung

Symb.	Num.	P^3	$P^3(mod 33)$	C^7	$C^7(mod 33)$	Symb.
S	19	6859	28	13492928512	19	S
U	21	92	21	1801088541	21	U
Z	26	17576	20	1280000000	26	Z
A	01	1	1	1	01	A
N	14	2744	5	78125	14	N
N	14	2744	5	781256	14	N
E	05	125	26	8031810176	05	E

Berechnung des Senders

Berechnung des Empfängers

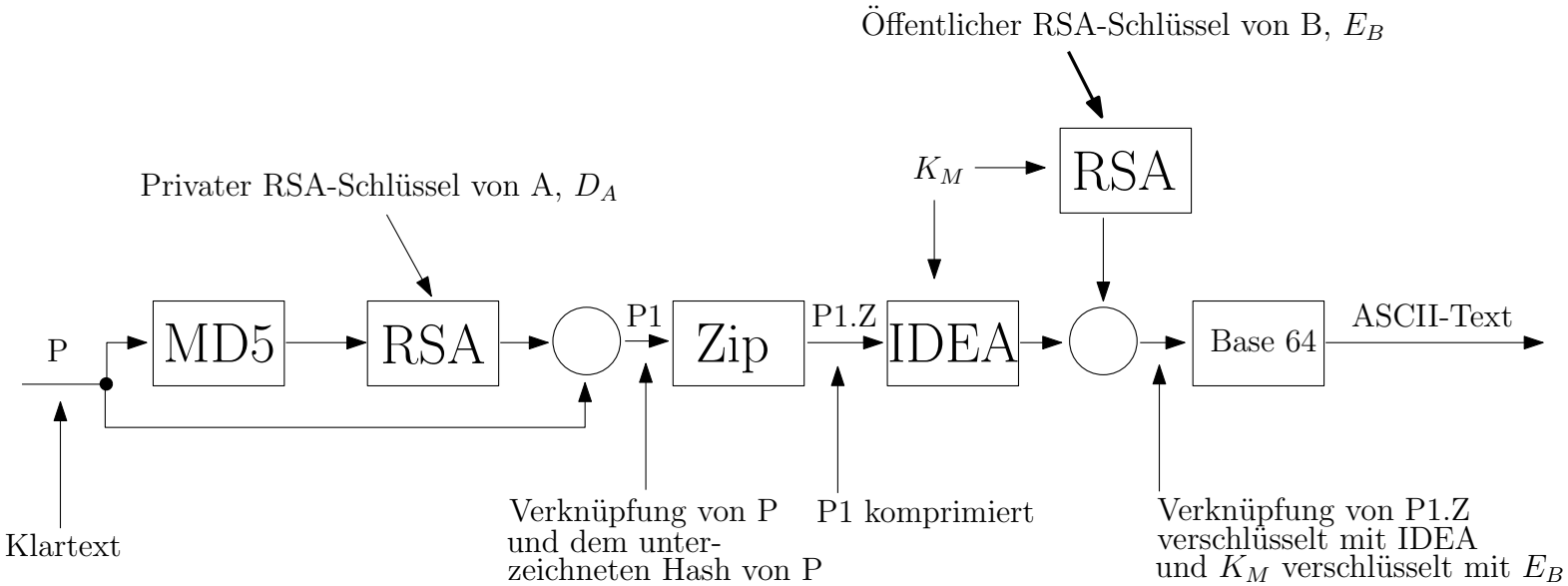
Pretty Good Privacy (PGP) - Teil 1

- Phil Zimmermann
- "If privacy is outlawed, only outlaws will have privacy."
- Quellcode kostenlos verfügbar
- Datenschutz, Authentifizierung, digitale Unterschrift und Komprimierung
- IDEA zur Verschlüsselung
- RSA zur Schlüsselverwaltung
- MD5 für die Datenintegrität

Pretty Good Privacy (PGP) - Teil 2

- Verfahren aufgrund angeblicher Verstöße gegen US Gesetze zum Export von Rüstungsgütern
- Breite Palette an verschiedenen Versionen
- Verwendet bewusst bestehende Algorithmen

Pretty Good Privacy (PGP) - Teil 3



Hardware basierende Systeme

Vorteile

- Daten sind geschützt auch wenn BS nicht aktiv
- Verschlüsselung ist transparent zum BS

Nachteile

- Wegen der geringen Grösse, kann das System dem "brute force attack" ausgesetzt werden.
- Hersteller verraten nicht wie die Verschlüsselung genau funktioniert. - führt zu "vendor lock-in"
- Hohe Kosten für Installation und Wartung

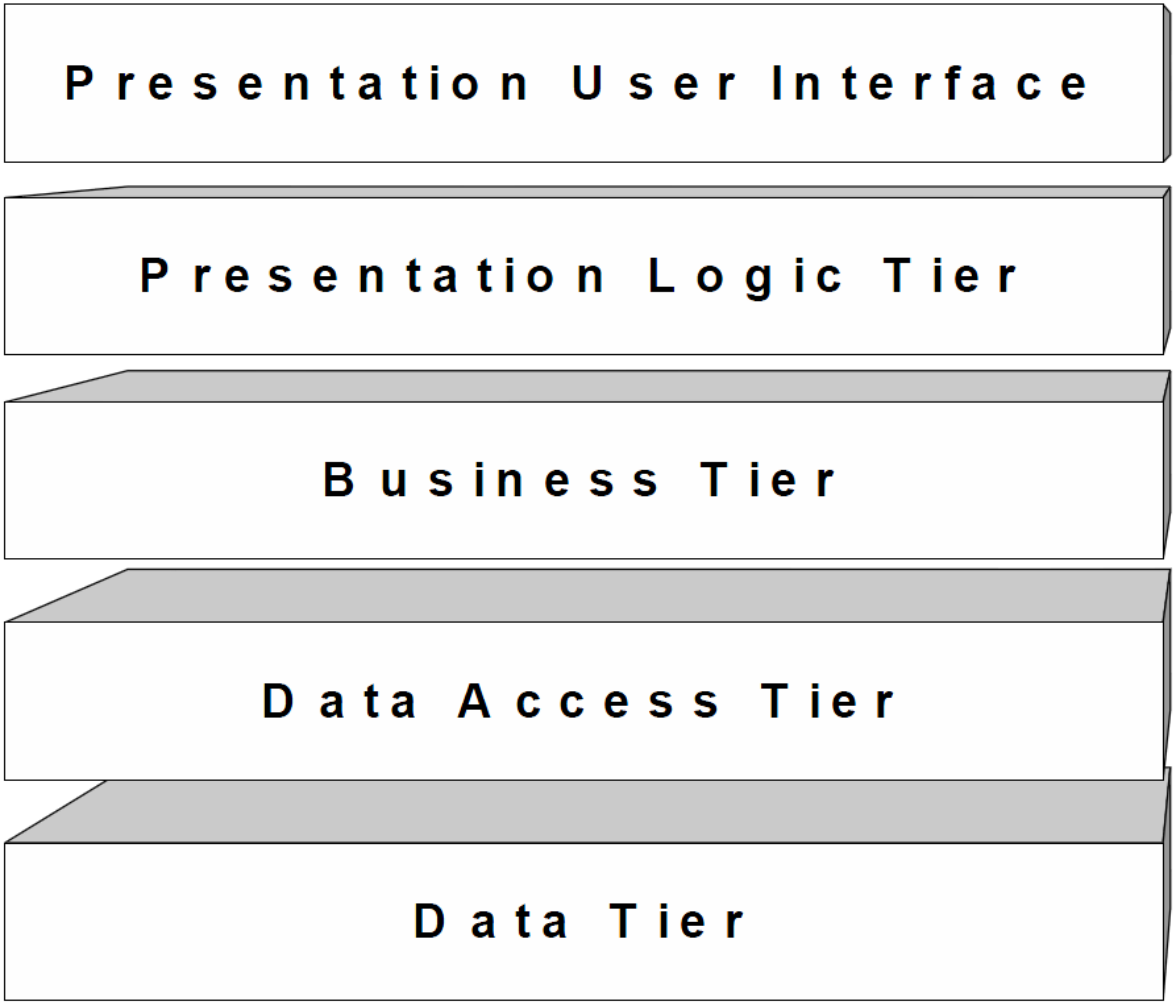
Smartcard System

- Ist ein mechanisches Gerät. Codiert die Informationen auf einem Chip auf der Karte.
- Identifikation erfolgt über einen Algorithmus, der auf asymmetrischer Sequenz basiert.
- Praktische Limits:
  1. große Mengen an Informationen, die dekodiert werden müssen können nicht verarbeitet werden
  2. Sichert nur die private Identifikation des Users aber nicht die Übertragung

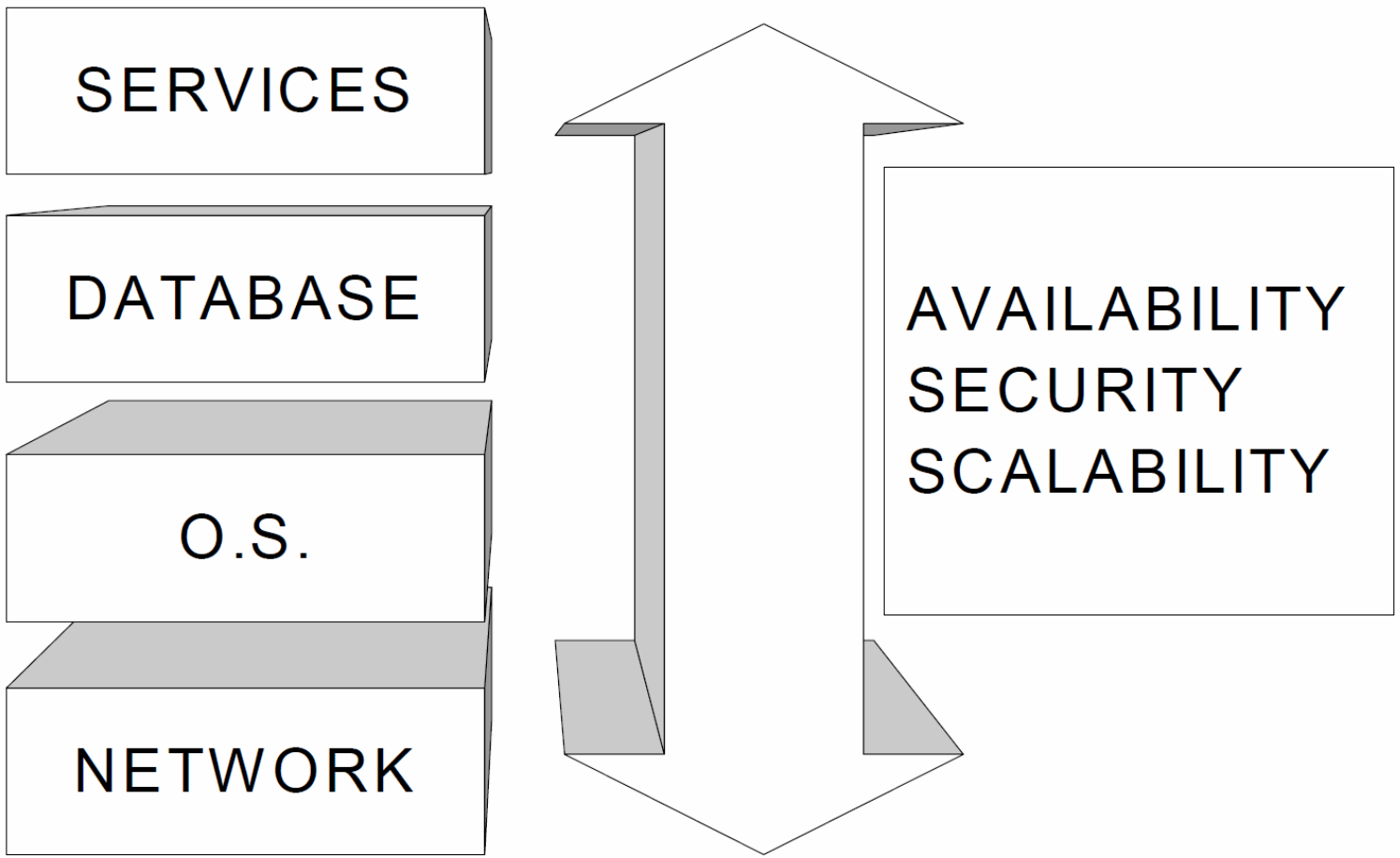
MeChip

- Entwickelt von ESD (European Association for the Promotion of Sustainable Development)
- Information, die gesichert werden muss, wird direkt zum MeChip gesendet
- Unterzeichnet und codiert an Bank übertragen
- Protokolliert und bestätigt

N-Tier Architektur



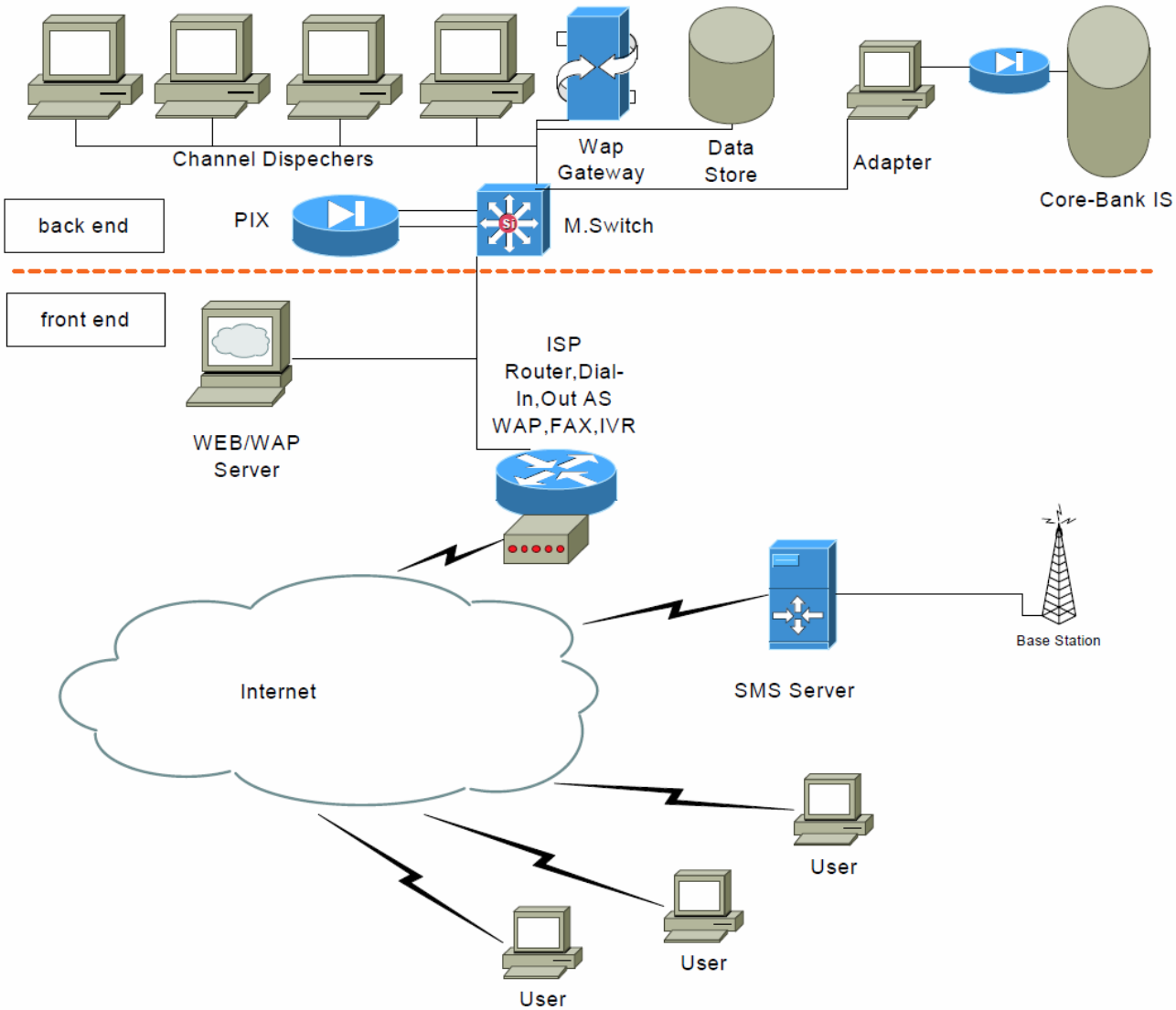
Anforderung an das Netzwerk



Netzwerkaufbau

- Der Aufbau des Netzwerkes ist unterteilt in Sektionen:
  - Edge Router
  - Access Server
  - Stateful Firewalls
  - Multilayer - Switch
  - Server

Netzwerkaufbau



Edge Router

- Edge Router empfangen:
  - Internetanfragen
  - Dial-In Verbindungen
  - WAP Services
- Sie bilden den Ein- und Ausgang zum Onlinebanking Netzwerk und haben eine exklusive Verbindung zum Access Server

Edge Router

- Sicherheitsschichten im Edge Router:
  - Extened Access Control Lists (ACL)
  - IOS Firewall Feature Set (FFS)
  - Stateful Firewalls

Webserver

- Sichere Verbindung zum Webserver gewährleistet durch:
  - Secure Socket Layer (SSL)
  - Public Key Infrastructure (PKI)
  - Identity Authentication

SSL - Secure Socket Layer

- Sichere Webserver benutzen SSL für den Netzwerkverkehr
- SSL Protokoll schafft verschlüsselte Kommunikationskanäle für Client/Server
- Algorithmen werden zur Chiffrierung des Datenverkehrs erstellt und Server authentifiziert sich gegenüber dem Client (Handshake)
- Sicher für Client-Server Kommunikation. Bei mehreren Schichten (z.B. Applikationsschicht) nicht sinnvoll ohne weitere Zusatzlösungen

Zusammenfassung und Fazit

- Viele verschiedene Sicherheitsmaßnahmen auf den unterschiedlichen Ebenen sichern das System maximal
- Dezentrale Architektur in allen Bereichen machen Angriffe von außen aussichtslos
- Das System wird dann anfällig, wenn der Mensch, der es benutzt, fahrlässig mit seinen Daten umgeht
- Eine Transaktion am Geldautomaten ist unter Umständen unsicherer (öffentlicher Ort, nur Karte/Pin Abfrage)

Vielen Dank für eure Aufmerksamkeit

Referenzen

- Andrew S. Tanenbaum
  Computer Networks
  Pearson Education, 978-0130661029, 2003
- Yi-Jen Yang
  The Security of Electronic Banking, 1997
- Lj. Antovski, M. Gusev
  E-BANKING-DEVELOPING FUTURE WITH ADVANCED TECHNOLOGIES, 2002
- M. Szydlowski, C. Kruegel, E. Kirda
  Secure input for web applications, 2007