KAP. 5

Security für Computer Netzwerke

(Firewalls, Erkennung und Schutz von Angriffen - Intrusion Detection und Intrusion Prevention- , VPN, Daten-Verschlüsselung)

Motivation

- Anzahl der Computer Netzwerke steigt ständig
- Ca. 400 neue Arten von Viren, Würmer, Back Door-Programmen, Blended Drohungen werden jeden Tag entdeckt!!!
- Unternehmen, öffentliche Institutionen, Privatpersonen sind mehr denn je vernetzt
- Klassische Sicherheits-Schutz-Methoden:
  Firewall und Packet Filtering bieten nicht genügend Schutz gegen alle diese neuen Arten der Angriffe
  Sie bilden die so genannte erste Verteidigungs-Ebene

Arten der Angriffe:

1) Sensational Security Attacks:

- Melissa Virsus (1999)
- Code Red (2001) <Buffer Overflow in a MS-IIS>
- Slammer Worm

2) Mapping:

Vor dem Angriff auf das Netzwerk, wollen die Angreifer die IP-Adresse der Stationen wissen.
Das PING-Programm kann dazu benutzt werden, um herauszufinden, welche IP-Adressen antworten.

3) Port Scanning:

Kontaktieren sequentiell (via TCP oder UDP) die Portnummern auf einer Maschine und schauen, was als Antwort passiert. Antworten können genutzt werden, um festzustellen, welche Dienste angeboten werden.
Das NMAP-Programm kann für Auditing Zwecken verwendet werden

4) Packet Sniffer

Speichern passiv alle Daten-Link Meldungen, die am Netzwerk Controller (NIC) vorbeigehen. NIC muss in einem Promiskmodus <Empfangsmodus> arbeiten. Manager mögen es nicht, wenn das NIC des Benutzers im ***Promiskmodus*** arbeitet. (Die auf dem PC installierte Software kann bei der Managerstation Alarm auslösen).

5) IP-Spoofing

Die IP-Adresse ändern, die durch eine bestimmte Station in ein Netzwerk generiert wird.
Auf diese Art kann der Sender Meldungen verschicken, die so aussehen als ob sie auch von anderen Stationen verschickt worden sind**.**
Gleichzeitig kann er andere Parameter (Information) für die nächst höheren „Upper Layer“ des Protokoll-Stacks einbeziehen.
Der Router kann überprüfen, ob die Nachrichten von der IP-Adresse innerhalb eines bekannten Bereich kommen. Dieser Check ist bekannt unter dem Namen „***Ingress Filtering“.***

6) Denial of Service (DoS)

Der DoS Angriff schafft soviel Arbeit für das Opfer, dass die reguläre Arbeit (z. B. WEB-Service, Routing, usw.) nicht mehr richtig ausgeführt werden kann.
DoS Arten:

1. **SYN Flooding Angriff:**
   Das Flooding (das Überfluten) des Opfers mit „TCP-SYN“ Paketen, jede davon hat eine <spoofed> vorgetäuschte IP-Adresse. Der Server beendet die 2 Schritte des 3-Way-Handshakes für eine vorgetäuschte SYN, indem er Datenstrukturen reserviert und ein Zustand zuordnet**.**
   Der 3. Schritt des Handshakes wird nie beendet. Das hinterlässt eine ständig ansteigende Zahl von teilweise offenen Verbindungen. Daraus entsteht der Server Crash.

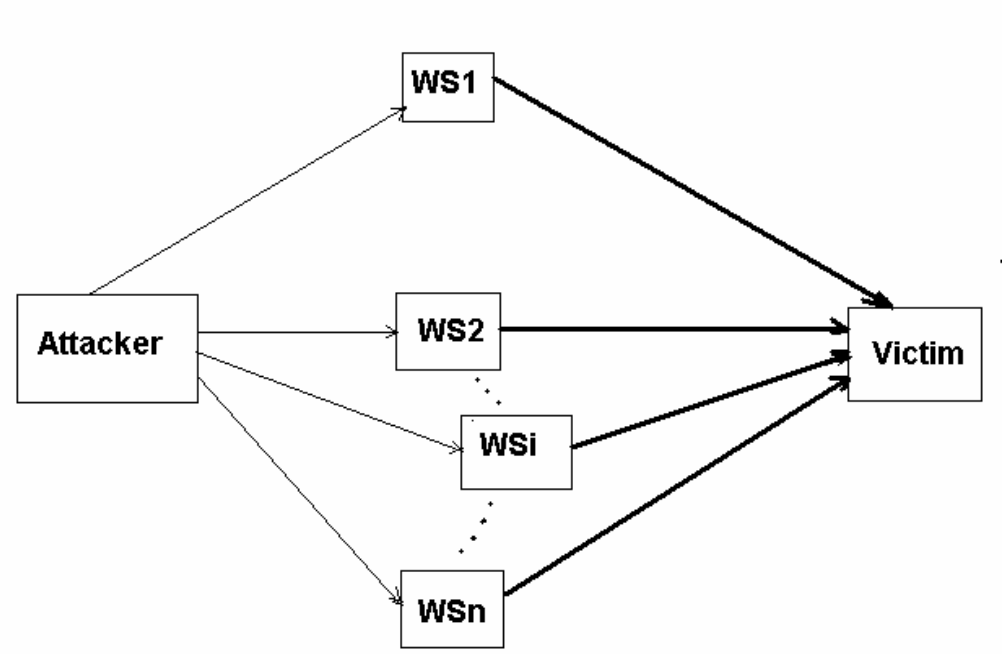
2. **IP-Fragmente Angriff:**
   Sendet IP-Fragmente zum Host, aber er sendet nie genügend Fragmente, um das Datagramm zu vervollständigen.

3. **Smurf Angriff:**
   Eine große Zahl von unschuldigen Hosts antworten auf ICMP Echo-Request Pakete, die eine vorgetäuschte <spoofed> Quell-IP-Adresse enthalten.
   Ergebnis:
   Eine große Zahl von „ICMP-Echo-Reply“ wird zur vorgetäuschten <spoofed> IP-Adresse gesendet.

4. **<u>Distributed DoS Attack (DDoS) Verteilter Dienstblockade:</u>**

   Der Angreifer erreicht zuerst Zugriff auf die Benutzerkonten auf einer großen Zahl von Hosts über das Internet (z. B. durch ***sniffing*** PW).
   Der Angreifer installiert Slave-Programme auf jeder der angegriffenen Seite. Diese Slave-Programme hören auf die Befehle vom Angreifer.

   Wenn eine große Zahl von solche Slave-Programmen laufen, dann instruiert das Master-Pgoramm die Slaves, einen DoS Angriff zu lancieren, die alle auf denselben Target-Host zielen



5. **<u>Hijacking Angriff</u>** <Entführung>
   Der Angreifer beobachtet den Austausch der Pakete auf einer Verbindung zwischen zwei Benutzern. Er kann einen von ihnen täuschen, so dass dieser glaubt, es sei der echte Benutzer. Auf diese Weise kann der Angreifer TCP-Segmente zum Opfer schicken. Diese TCP-Segmente enthalten verschiedene Informationsarten.

Erste Ebene der Verteidigung

A) Paket-Filtering

Prinzip: Öffnet zwei Ports für jeden Kommunikationskanal
- einen Port für eingehenden Datenverkehr
- einen Port für ausgehenden Datenverkehr

Probleme: Die Ports sind nicht mit dem Inhalt und der Verbindung des ein- und ausgehenden Datenverkehrs verbunden.

Ergebnis: Unzulässige Pakete können als Teil der existierenden Session erscheinen. Diese Pakete können geschützten Ressourcen schaden.

B) Firewall Methode:

Prinzip: Entscheiden, welcher Datenverkehr erlaubt ist und welcher Verkehr verboten ist basierend auf so genannten Policy Regeln**:**

Implementierung: Um Anwendungen zu unterstützen, die für Unternehmen wichtig sind, muss eine Firewall Datenverkehr erlauben, der von typischen Internet-Protokollen unterstützt wird, z. B.: HTTP, FTP, SMTP.

Ergebnis: **Firewall erlaubt Datenverkehr, von dem er annimmt, dass er keine Gefahr für das Organisations-Netzwerk bedeutet. Dieser genehmigte Verkehr könnte verschiedene Arten von versteckten Angriffen enthalten.**

Lösung: Den Sicherheits-Schutz erweitern, und zwar durch so-genannte 2. Verteidigungs-Ebene**.**

Zweite Ebene der Verteidigung

Die Methoden, die für die Installierung dieser Ebene bekannt sind, basieren auf sorgfältigen Echtzeit-Analysen der Anwendungen als auch des Inhalts der transferierten Dateien.

A) IDS-Intrusion Detection System

- Echtzeit-Analysen der Anwendungen innerhalb des Datenverkehrs
- ***Entdeckt so genannten „unerwünschten Datenverkehr“,*** *d.h. signaturbasierte Einbruchserkennung und die Erkennung von Anomalien des Netzwerkverkehrs.*
- Löst „positiven Alarm“ aus im Falle vom Erkennen von unverwünschtem Datenverkehr.

B) IPS-Intrusion Detection und Prevention System

- Echtzeit-Analysen der Anwendungen innerhalb des Datenverkehrs
- **Entdeckt so genannten „unerwünschten Datenverkehr“,** d.h. signaturbasierte Einbruchserkennung und die Erkennung von Anomalien des Netzwerkverkehrs.
- ***Enfernt die Nachrichten und blockiert die Verbindung***, die unerwünschten Datenverkehr transportiert
- Löst „positiven Alarm“ aus im Falle vom Erkennen von unverwünschtem Datenverkehr

C) Steganographie

<Verborgenen Speicherung oder Übermittlung von Informationen>

Methode, um unsichtbare Informationen <verborgene> zu transportieren. Die verborgene Botschaft können digitale Daten sein und sie kann in fast allen Arten von digitalen Daten verborgen sein.

Prinzip: - Die Existenz der eigentlichen Botschaft ist unbekannt
- Das Hauptziel ist, die eigentliche Botschaft zusammen mit anderen Informationen zu verstecken.

Ergebnis: ist dann erreicht, wenn kein Verdacht auftritt, dass eine versteckte Information transportiert wird.

Security Solution: **=> *Steganalysis:***

Methoden, um den Transport von Daten herauszufinden.

Sie hat zwei Ziele:

1. die Existenz von verborgenen Botschaften entdecken / beweisen
2. Zerstörung dieser Botschaften

Aktuelle Stand der Steganographie

Die jüngsten Forschungs- und Entwicklungsaktivitäten konzentrieren sich auf:

- *das Schaffen von neuer Steganographie-Werkzeuge und*
- *Algorithmen hauptsächlich zum Verstecken Text von oder Bildern in Texten, Bildern oder Audio-Daten.*

Vergleich verschiedener Methoden der Netzwerk-Sicherheit

File Level	→	**Steganography, Steganalysis** *Examine files inside application traffic*
Application Level	→	**Intrusion Detection Prevention IDS/ IPS** *Examine application fields within the traffic*
Session + Transport Level	→	**Firewall statefull inspection** *Examine packet header and control fields; usage of state behavior*
Network Level	→	**Packet Filtering** (Access Control Lists: ACL-CISCO or IPChains-Linux) *Examine few fields within the packet header*
Data Link Level		-----
Physical Level		-----

Firewall: Allgemeine Aspekte

Wozu brauchen wir Firewalls?

- Datensicherheit
  - Integrität
  - Verfügbarkeit
- Ressourcen-Schutz
- Image-Schutz des Unternehmens

Gegen wen müssen wir uns schützen?

- Soziale Angriffe: Manipulationen des Benutzers
- Angriffe gegen Dienste:
  - E-Mail-Überschwemmungen
  - Deaktivieren eines Dienstes

- Rauben von Informationen
  - Sniffen des Netzwerks, um das PW, Daten, etc. heraus zu bekommen

Arten der Angreifer

- Joyrider: Leute, die aus Spaß angreifen
- Vandalen: Leute, die Interesse an Zerstörung haben
- Point Hunters**:** Punkte-Jäger
- Industriespione

Was ist ein internet-Firewall?

- Schutz eines internen Netzes vor Internet-Angriffen
- Gewährleistet, dass die richtigen, erwünschten Daten Zugang haben
  - vom Internet zum internen Netzwerk
  - vom internen Netzwerk zum Internet
- Analysiert und limitiert den Datenverkehr
  Vergleich: Wassergräben um eine mittelalterliche Festung

Was kann eine Firewall?

- Implementiert Zentren von Sicherheits-Mechanismen
- Implementiert eine Sicherheits-Policy der entsprechenden Filialen des Unternehmens
- Loggt (Protokolliert) die Internet-Aktivitäten
- Reduziert die Angriffs-Risiken

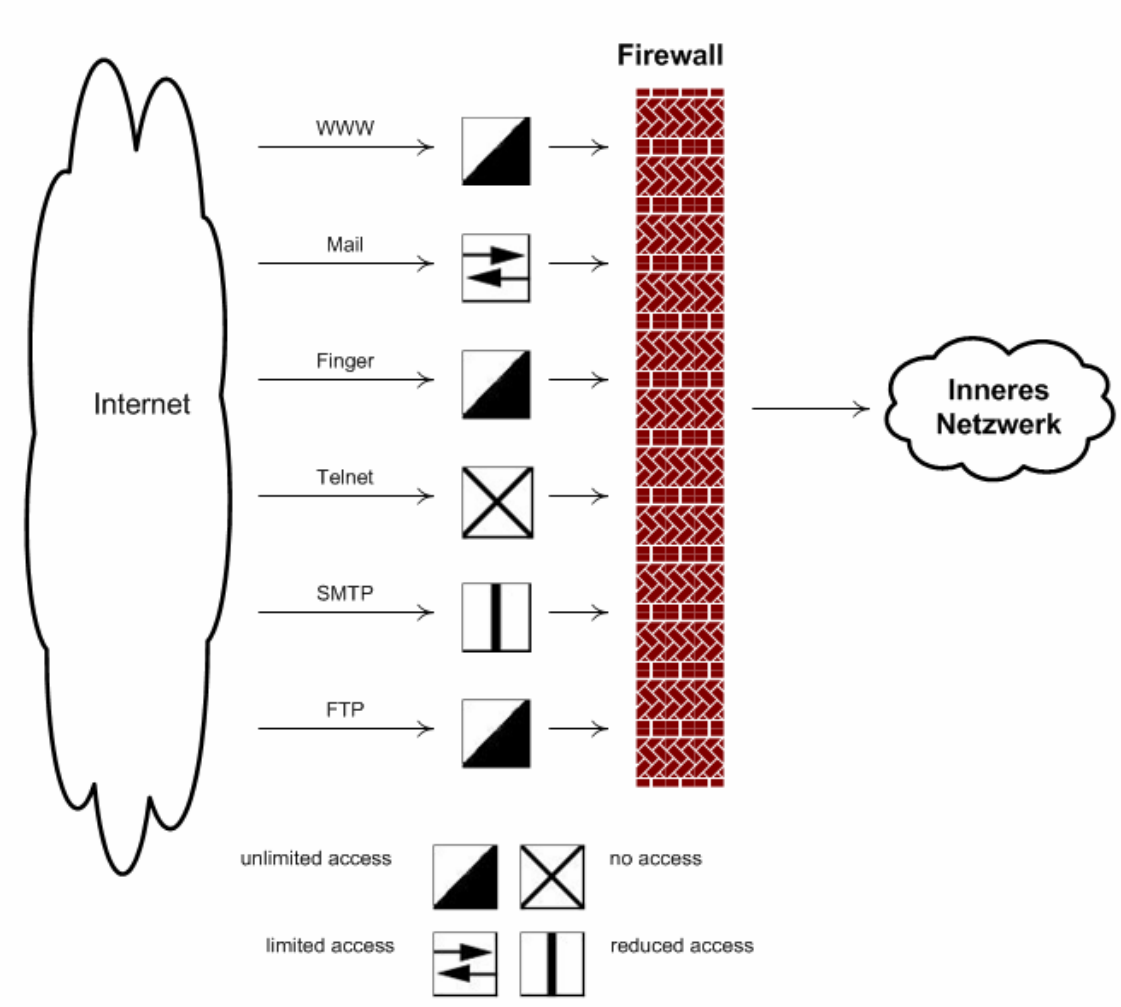
Was kann eine Firewall nicht?

- Schutz gegen böswillige Insider
- Schutz von Verbindungen, die nicht durch die Firewall gehen
- Schutz vor ganz neuen, unbekannten Angriffen
- Schutz gegen alle existierenden Viren

Planen des Gebrauchs und der Integration von Firewall

- Man braucht Internet-Know-how
- Analysieren Sie das Unternehmens-Netzwerk
    - die Hardware-Architektur
    - Art der Anwendungen
- Etablieren Sie eine Sicherheits-Policy: welcher Dienst ist erlaubt und welcher nicht?
- Legen Sie die Firewall-Konfiguration fest
- Entscheiden Sie, welche Plattform genutzt werden soll:
    - Public Domain Software-Paket
    - Lizensiertes Software-Paket
- Implementieren Sie eine Pilot-Konfiguration, um die Sicherheits-Policy zu testen
- Legen Sie fest, wer das Firewall-System verwalten soll
- Zertifizieren Sie die Installation durch den Gebrauch von speziellen Check-Werkzeugen (oder indem Sie zertifizierte Unternehmen bitten, dies zu tun)

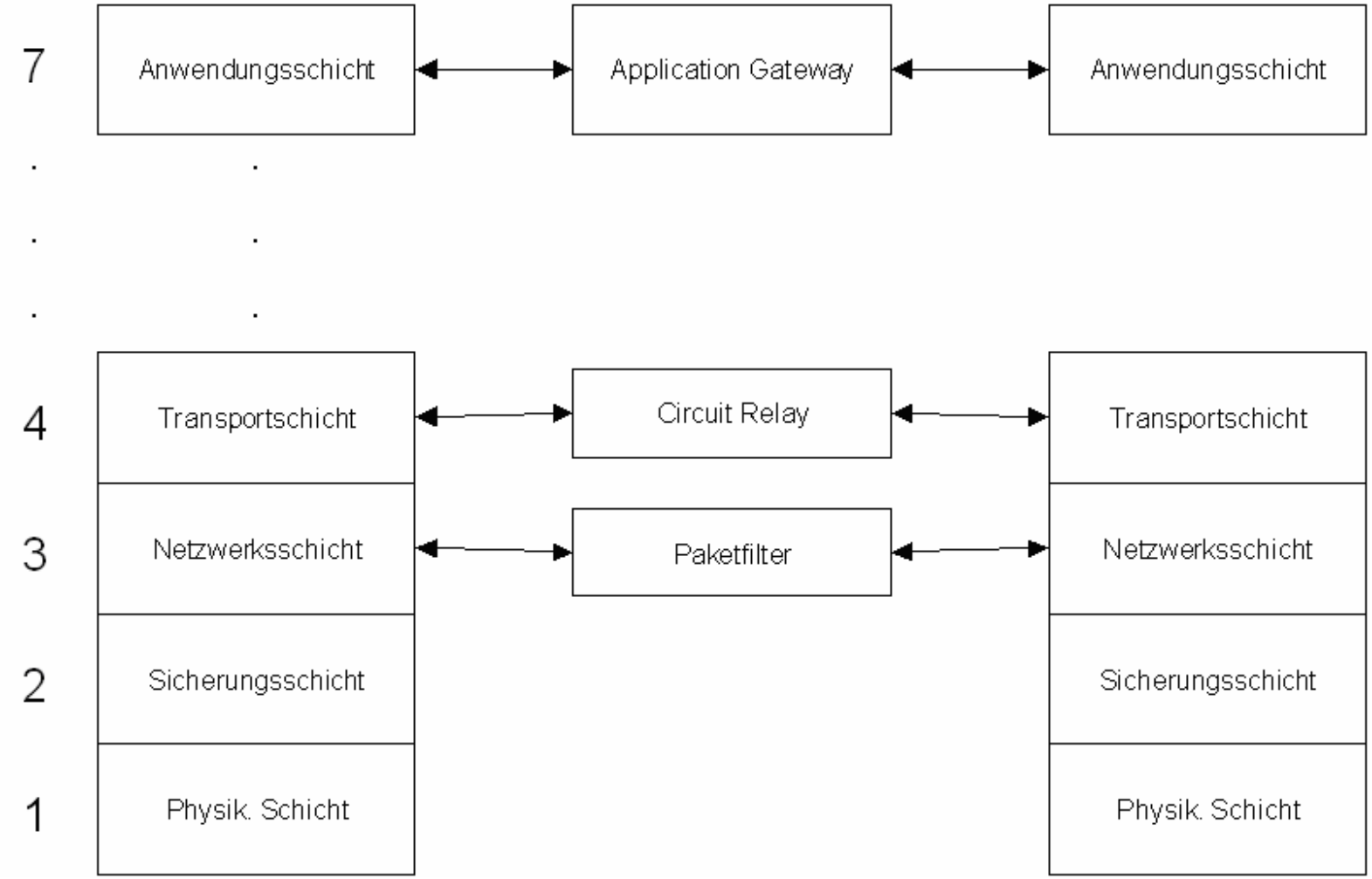
Firewallkonzept und Konfigurationsprinzip



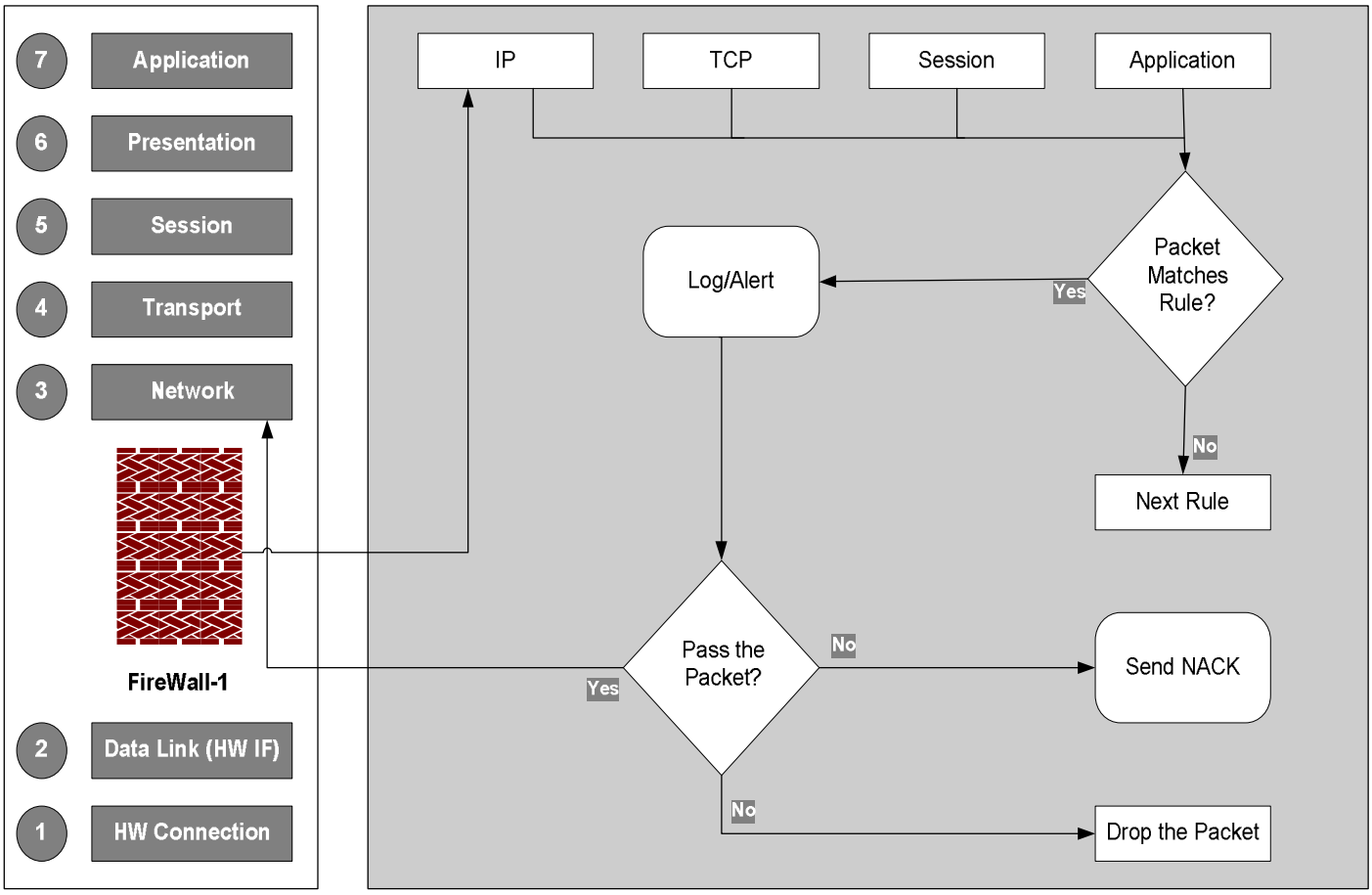
Methods:

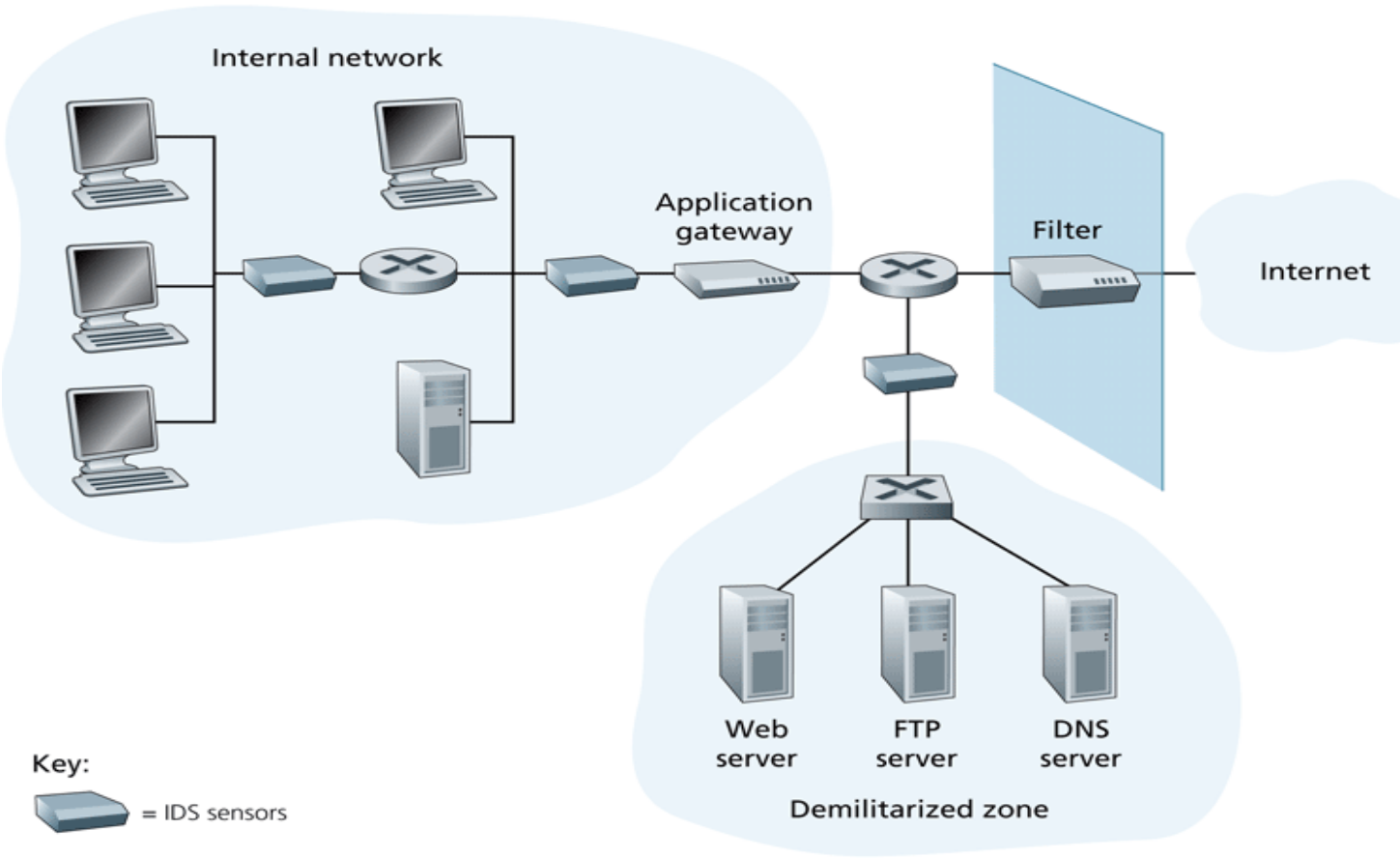
1. **Packet Filtering**
2. **Applikation-Level Gateway**
3. **Circuit-Level Gateway**

Firewall Methods



Architecture of Stateful Inspection Method





Konfiguration mit: Firewall, Router (Packet Filtering), Application Gateway IDS (Intrusion Detection System)

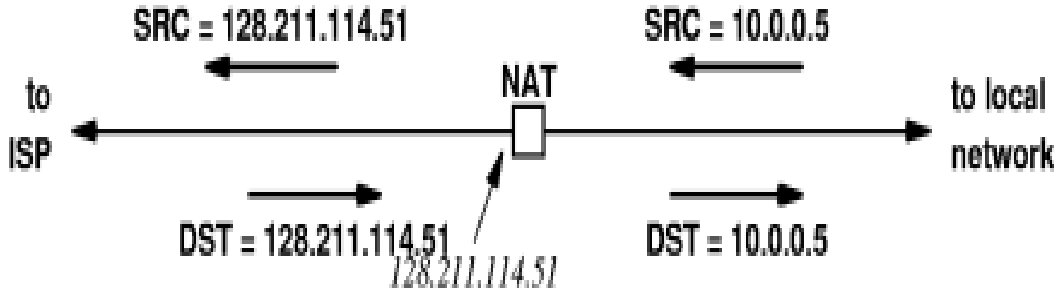
Policy	Firewall Setting
No outside Web access.	Drop all outgoing packets to any IP address, port 80
No incoming TCP connections, except those for organization's public Web server only.	Drop all incoming TCP SYN packets to any IP except 130.207.244.203, port 80
Prevent Web-radios from eating up the available bandwidth.	Drop all incoming UDP packets—except DNS packets.
Prevent your network from being used for a smurf DoS attack.	Drop all ICMP ping packets going to a "broadcast" address (eg 130.207.255.255).
Prevent your network from being tracerouted	Drop all outgoing ICMP TTL expired traffic

Policies and Filtering Rules for Subnet.: 130.207.0.0/16 with WEB Server 130.207.244.203

Packet Filtering (Access Control List)

action	source address	dest address	protocol	source port	dest port	flag bit	check conxion
allow	222.22/16	outside of 222.22/16	TCP	>1023	80	any	
allow	outside of 222.22/16	222.22/16	TCP	80	>1023	ACK	X
allow	222.22/16	outside of 222.22/16	UDP	>1023	53	—	
allow	outside of 222.22/16	222.22/16	UDP	53	>1023	—	X
deny	all	all	all	all	all	all	

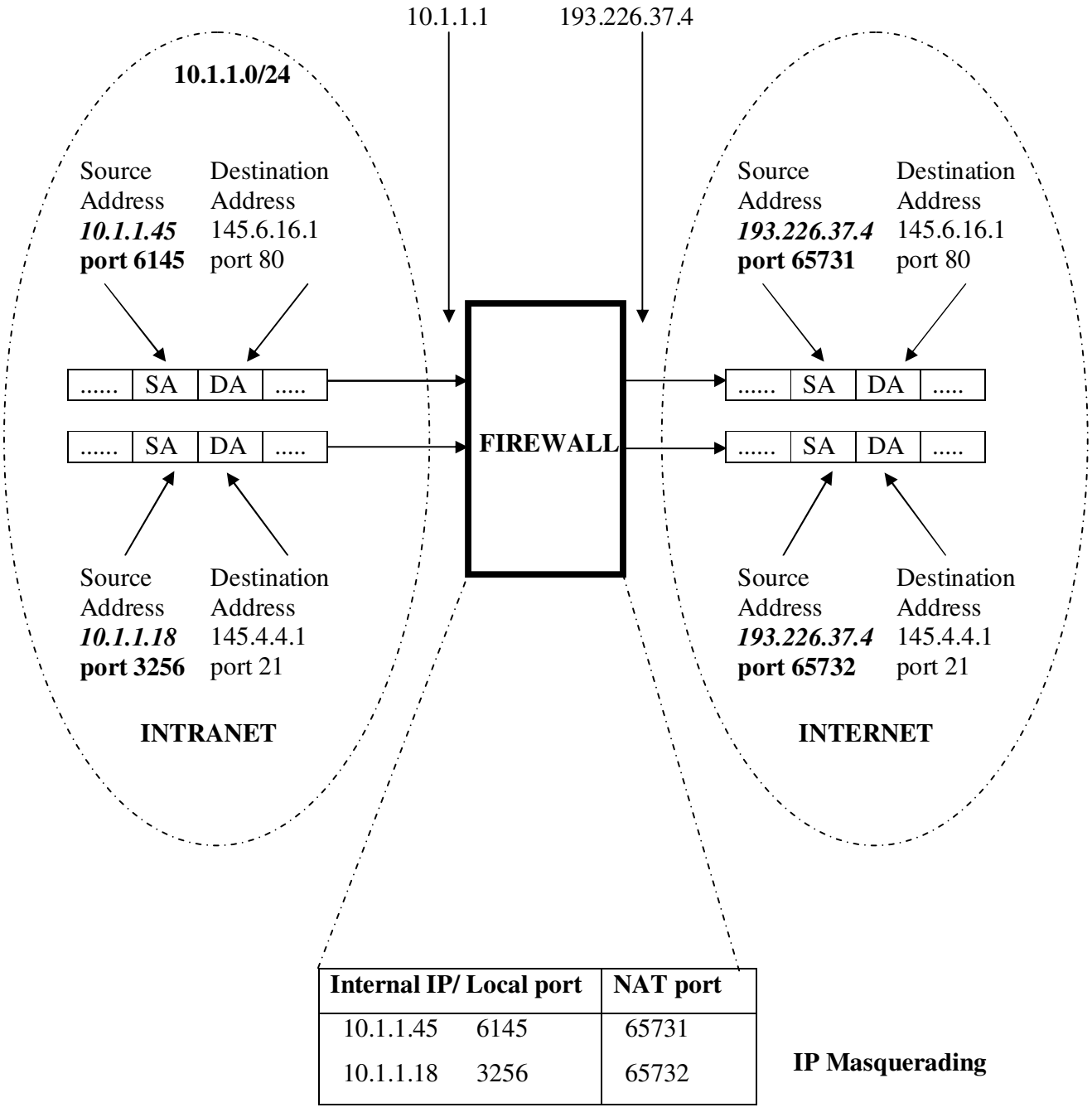
Network Address Translation (NAT)



Prinzip:

- Die lokalen Netzwerk angeschlossenen Computer benutzen beliebige Adressen; in der Regel ungültige Internet-Adressen
- Nat übersetzt Internet-Adressen:
  a) Einkommende Nachrichten
    - NAT übersetzt eine gültige Adresse (die Adresse des Firewalls oder des Routers) in eine ungültige Adresse (die Adresse eines Rechnres innerhalb des Privaten Netzwerks)
      Bp: Destination Adr: 128.211.114.51 0 => 10.0.0.5

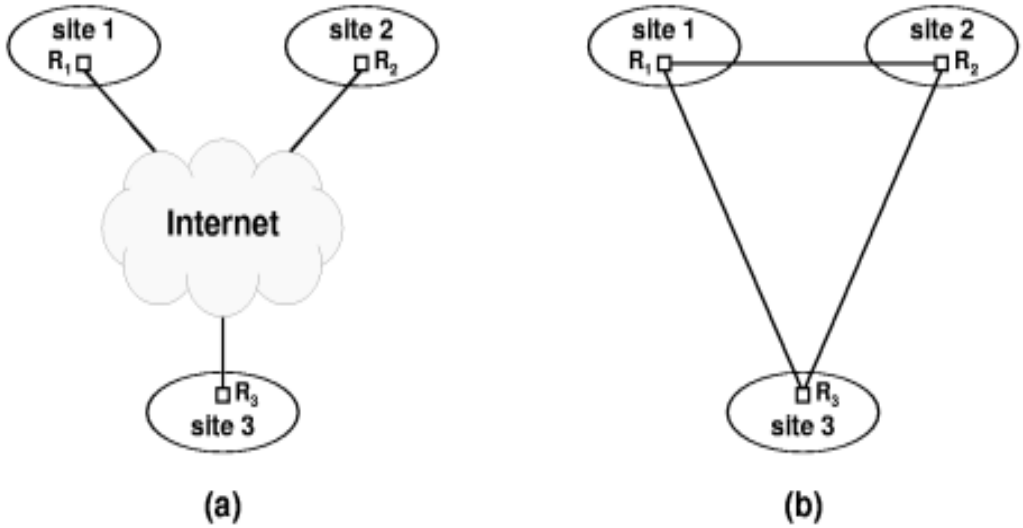
  b) Ausgehnden Nachrichten.
    - NAT übersetzt eine ungültige Quelle-Adresse (die Adresse des intern platzierte Station) in eine gültige Adresse (die Adresse des Firewalls oder des Routers)
      Bp: Destination Adr: 128.211.114.51 0 => 10.0.0.5
- NAT Funktionen sind in der Regel von Firewalls oder von Router Durchgeführt; Ausnahmen: Rechner unter Windows od. UNIX/LINUX können NAT Funktionen auch durchführen (etwas langsamer!)



Internal IP/ Local port		NAT port
10.1.1.45	6145	65731
10.1.1.18	3256	65732

IP Masquerading

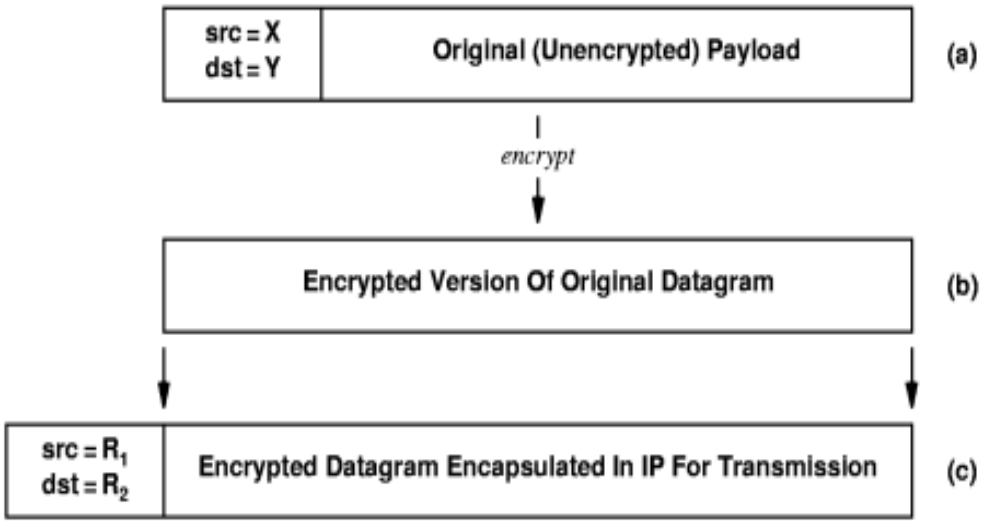
Virtuelle Private Network (VPN)



Die Internet Verbindungen zwischen Netzwerke an verschiedene Standorten:

a) mittels öffentliche Internet Verbindingen via IS-Provider
   Nachteil: Ungesicherte Verbindung: Daten können abgehört od. verfälscht

b) mittels öffentliche Internet aber unter Verwendung einer Technologie die die "private Verbindung" unterstützt: ***VPN***
   - Die Router an allen Standorte erhalten VPN Software:
   - VPN Software verschüsselt alle Übertragungen so dass keine Daten auf Netz abgelesen bzw. Gefälscht warden können.



VPN - Tunneling - Prinzip: IP-in IP Kapselung in einem VPN

a) Unverschlüsseltes Datagramm

b) Verschlüssltes Datagramm

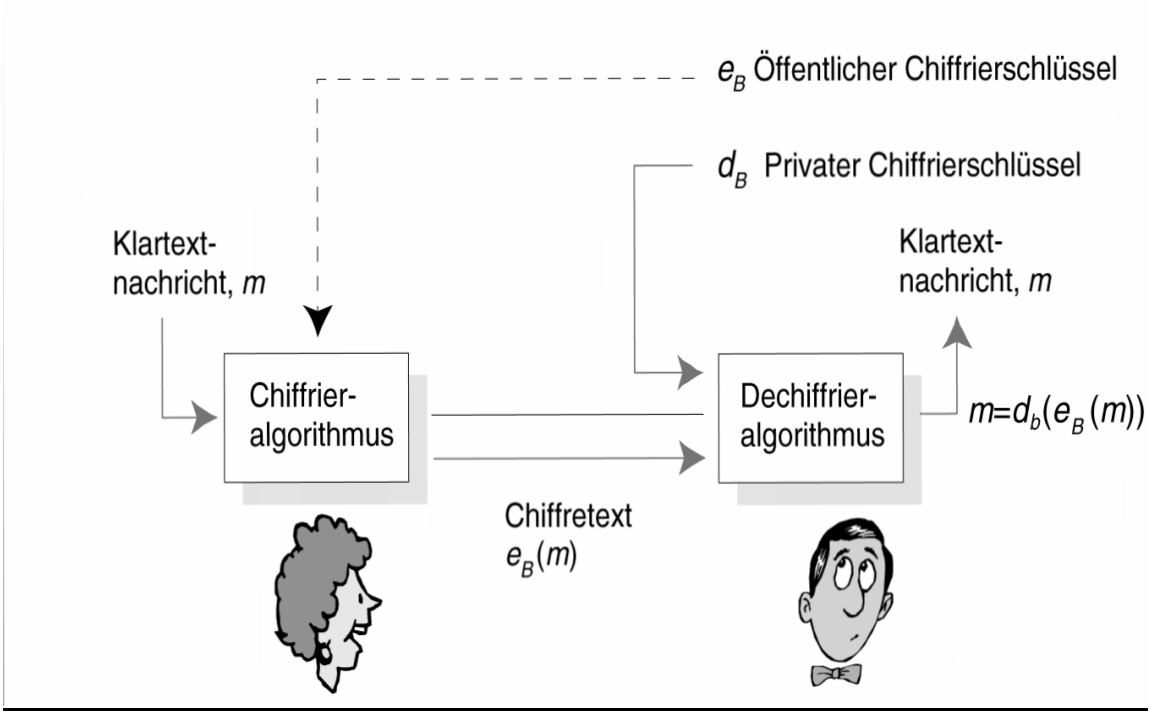
c) Verschlüsseltes und in einem weiteren Datagramm für Die Übertragung im Internet gekapseltes Datagramm

Bemerkung:
Das für die VPN-Verbindung notwendige ***VPN-Protokoll PPTP*** (Point to Point Tunneling Protocol) wird bei Windows XP direkt mit installiert.

VPN unter Windows XP nutzt per Default ***PPTP*** als Protokoll. Dieses bietet in der neuesten Version eine Verschlüsselung von 128 Bit und ist ausreichend sicher. Das modernere ***Protokoll IPsec*** bietet zwar eine höhere Sicherheit, wird aber nicht von allen Betriebssystemen unterstützt.

Verschlüsselung und Vertraulichkeit

Motivation: Inhalt einer Nachricht muss vertraulich bleiben
Lösung: Verschlüsselung (Encryption)

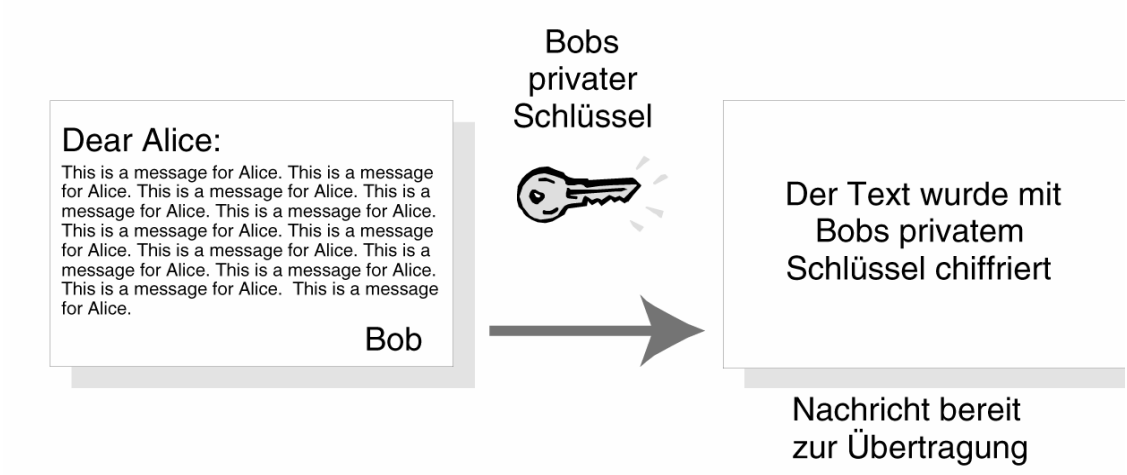


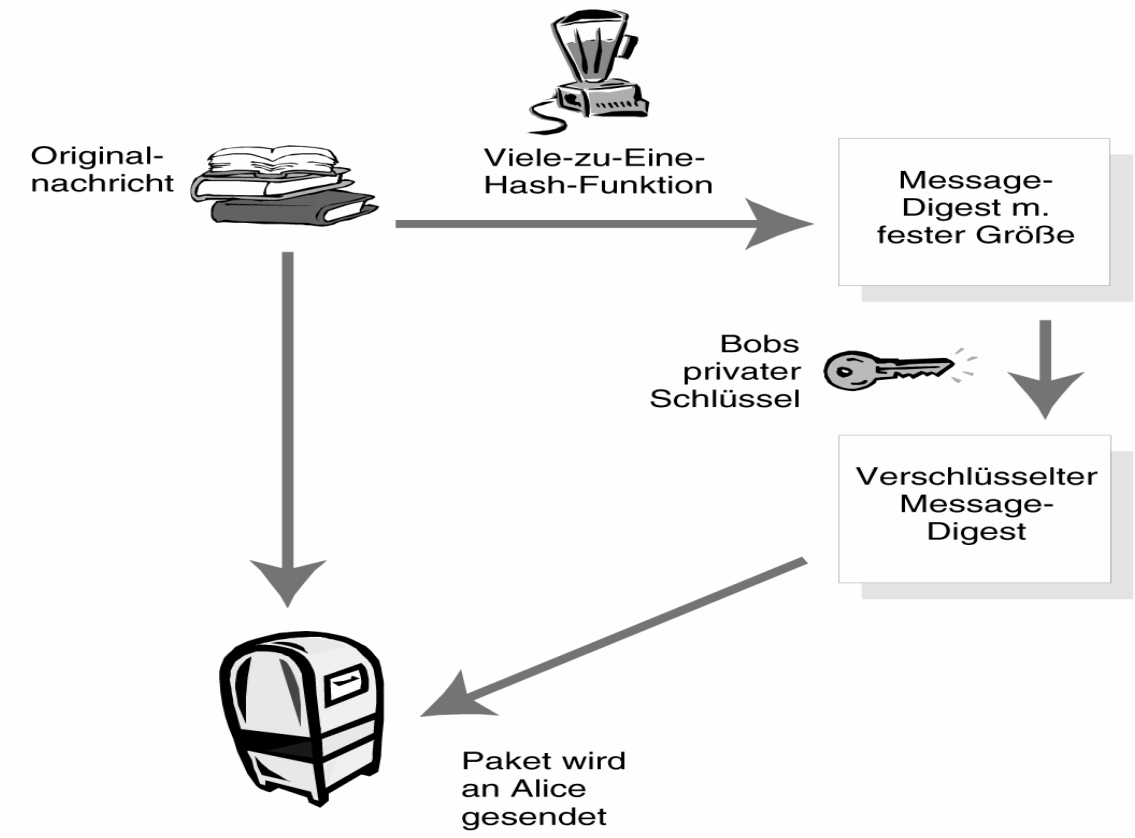
Lösungs-Prinzip:
- Die Bits einer Nachricht warden durch “Chiffrieralgorithmus umgestellt
- Sender und Empfänger erhalten jeweils eine Kopie des Chiffrierschlüssle(encryption key)
  Die Schlüssel müssen geheim gehalten werden

Lösungen für Geheimhaltung:
- *Symetrische (private) SchlüsselPprinzip*: (per Post zugesandt)
- *Asymetrische od public Schlüssel* -Prinzip: es gibt 2 keys:
  eine public key und eine geheim key
  Sender benutzt der public key des Empfängers zum versclüsseln der Nachricht
  Der Empfänger muss eigene private key verwenden um die Nachricht lessen zu können.

Digitale Signatur

Eine Nachricht kann auch “unterschrieben” warden





Prinzip:

- Der Sender chiffriert die Nachricht mit einem Schlüssel der nur ihm bekannt ist

- Schlüssel wird auf der Basis eines Centers verteilt: Bei der Verteilung wird auf eine vertrauenswürdige dritte Partei zurückgegriffen. Diese Organisationen sind als Certification Authrity (CA) bekannt.

- Schlüsselverteilung auf der Basis von Zertifikaten: Hier werden zwei Klassen von Verteilungstechniken unterschieden: Schlüsseltransfer (Verschlüsselung lokal erzeugter Schlüssel mittels öffentlichem Schlüssel) und Schlüsselaustausch (Schlüssel wird sowohl lokal als auch beim entfernten Schlüsselmanagementsystem kooperativ erzeugt)

- Um die Integrität der übertragene Meldung zu sichern es wird auch ein sog. „ Message Digest“ Wert ausgerechnet und an die Empfänger geschickt. Message Digest ist eine Art „Checksum“ und wird auch als „Hash Funktion“ gennant

Hash Funktion => Man nimmt ein Wert „m“ und berechnet einen „Fixed Sized“ string . Message Digest schützt die zu übetragene Meldung

Bekannten Message Digest Algorithmen:

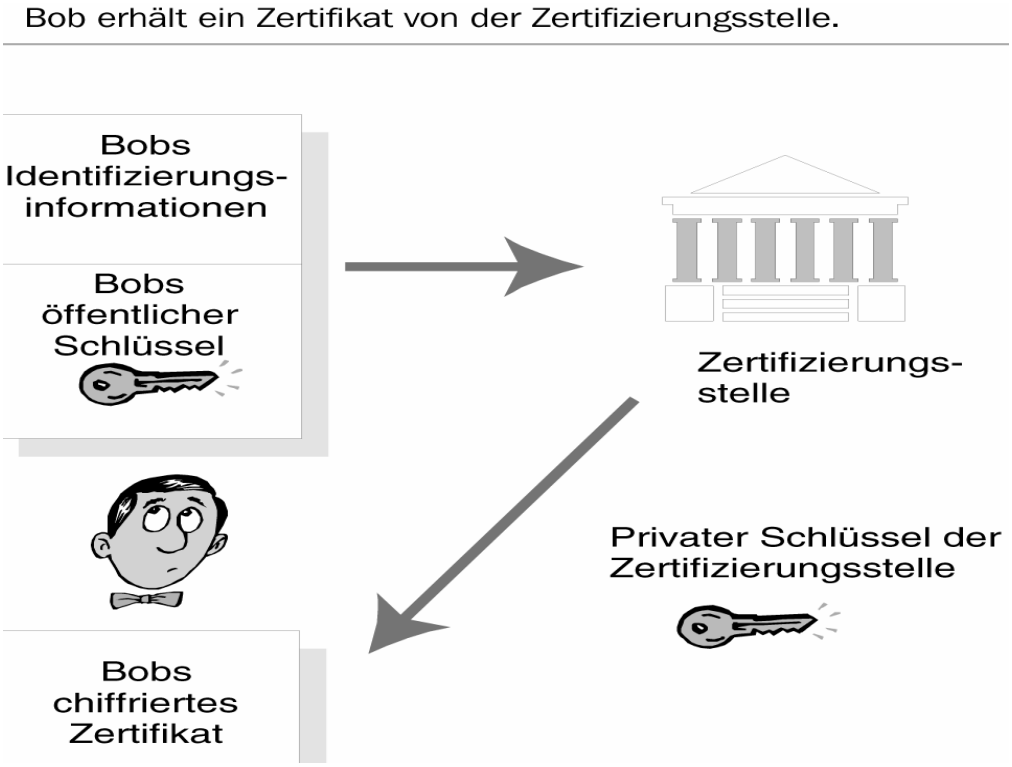
- MD5 : Message Digest 5 verwendet 128 Bit message digest
- SHA-1 : Secure Hash Algorithm: verwendet 160 Bit message digest

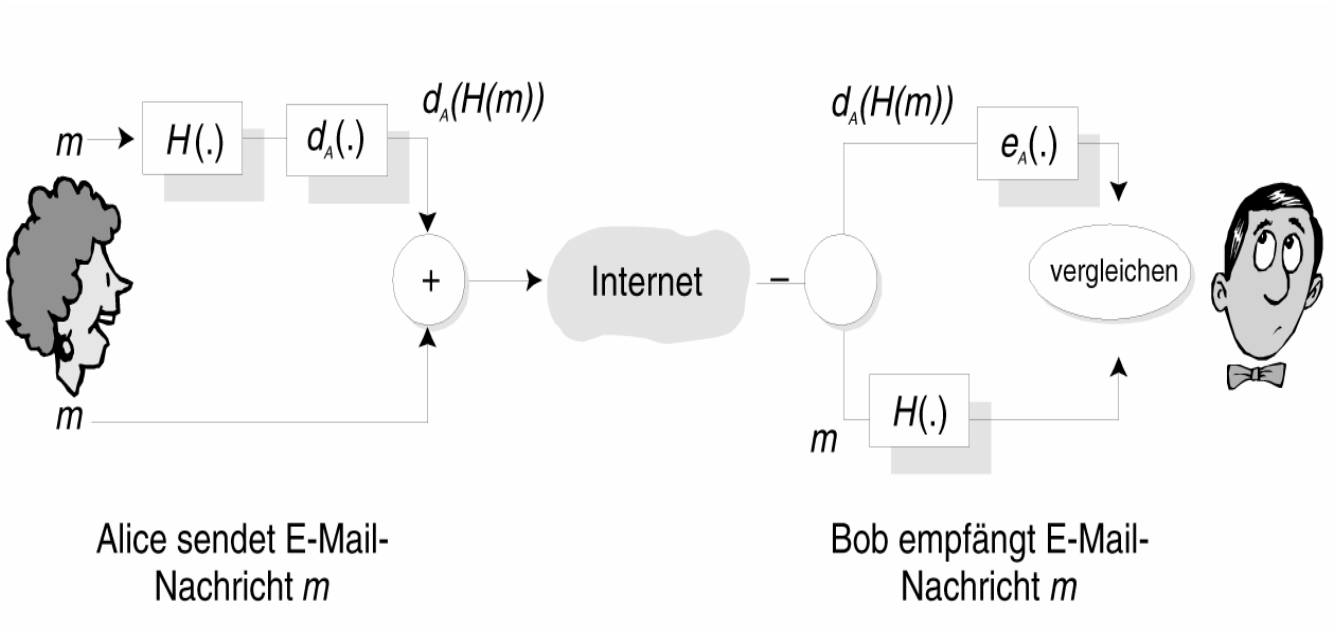
Bemerkung:

Die Bundesnetzagentur veröffentlicht jedes Jahr eine Empfehlung für kryptographische Algorithmen für die Erzeugung qualifizierter elektronischer Signaturen. In der Empfehlung von 2006 werden als geeignete digitale Signaturverfahren RSA, DSA und DSA-Varianten. Zu jedem dieser Verfahren werden die Mindestlängen für die Schlüssel sowie weitere Anforderungen an die Parameter angegeben.

Internet Zertifikate und die damit verbundene Zertifizierung ermöglichen einen Identitätsnachweis sowie die Verschlüsselung von Informationen, z.B. bei:

- Sicherung Ihrer Onlinegeschäfte
- Problemlose Unterzeichnung elektronischer Dokumente
- Garantie der Integrität von Dokumenten
- Verschlüsselung von Nachrichten - nur vom befugtem Empfänger lesbar
- Gewährleistung der Vertraulichkeit von Informationen





Verwendung von Hash-Funktionen und digitalen Signaturen, um Senderauthentifikation und Nachrichtenintegrität zu unterstützen