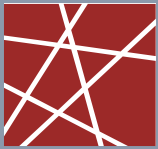




Motivierende Fragen

- ❑ Welche Kommunikation ist abhörbar?
- ❑ Wie kann man sich davon überzeugen, dass ein Kommunikationspartner der ist, der er vorgibt zu sein?
- ❑ Wie kann man sicherstellen, dass eine Nachricht vom angegebenen Sender stammt?
- ❑ Wie kann man sicherstellen, dass eine Nachricht seit dem Versenden nicht modifiziert wurde?
- ❑ Was ist ein Zertifikat? Und wie wird es eingesetzt?



Grundlagen: Rechnernetze und Verteilte Systeme

Kapitel 10: Netzsicherheit

Kryptographische Mechanismen und Dienste
IPSec, Firewalls

Prof. Dr.-Ing. Georg Carle
Lehrstuhl für Netzarchitekturen und Netzdienste
Technische Universität München
carle@net.in.tum.de
<http://www.net.in.tum.de>





1. Einführung und Motivation
 - Bedeutung, Beispiele
2. Begriffswelt und Standards
 - Dienst, Protokoll, Standardisierung
3. Direktverbindungsnetze
 - Fehlererkennung, Protokolle
 - Ethernet
4. Vermittlung
 - Vermittlungsprinzipien
 - Wegwahlverfahren
5. Internet-Protokolle
 - IP, ARP, DHCP, ICMP
 - Routing-Protokolle
6. Transportprotokolle
 - UDP, TCP
7. Verkehrssteuerung
 - Kriterien, Mechanismen
 - Verkehrssteuerung im Internet
8. Anwendungsorientierte Protokolle und Mechanismen
 - Netzmanagement
 - DNS, SMTP, HTTP
9. Verteilte Systeme
 - Middleware
 - RPC, RMI
 - Web Services
- 10. Netzsicherheit**
 - **Kryptographische Mechanismen und Dienste**
 - **Protokolle mit sicheren Diensten: IPSec etc.**
 - **Firewalls, Intrusion Detection**
11. Nachrichtentechnik
 - Daten, Signal, Medien, Physik
12. Bitübertragungsschicht
 - Codierung
 - Modems



- ❑ Sicherheitsziele und Bedrohungen
- ❑ Sicherheitsmechanismen
- ❑ Firewalls
- ❑ Virtuelle Private Netze



- ❑ Früher:
 - Öffentliche Netze: abgeschlossen, zentral verwaltet
 - Internet: reines Forschungsnetz, kein lohnendes Angriffsziel, Benutzer vertrauen einander
- ❑ Heute:
 - Dezentralisierung öffentlicher Netze nach Deregulierung der Telekommunikationsmärkte
 - Kommerzielle Nutzung des Internets
- ❑ Folge:
 - Sicherheitsmechanismen werden zum unverzichtbaren Bestandteil moderner Kommunikationssysteme



Angriffsmöglichkeiten

□ Passive Angriffe

- Ablauf der Kommunikation nicht gestört
- Aber unerlaubte Informationsbeschaffung

□ Aktive Angriffe

- Nachrichten werden verfälscht
- Betrieb des Netzes wird verändert

Abhören von
Nachrichten/
Teilnehmerkennungen

Passive Angriffe

Analyse des Verkehrsflusses

Wiederholen/Verzögern
von Nachrichten

Modifikation von
Nachrichten

Vortäuschen
fremder
Identitäten

Aktive Angriffe

Einfügen/Löschen
von Nachrichten

Blockieren von Diensten
(„Denial of Service“-
Angriffe)



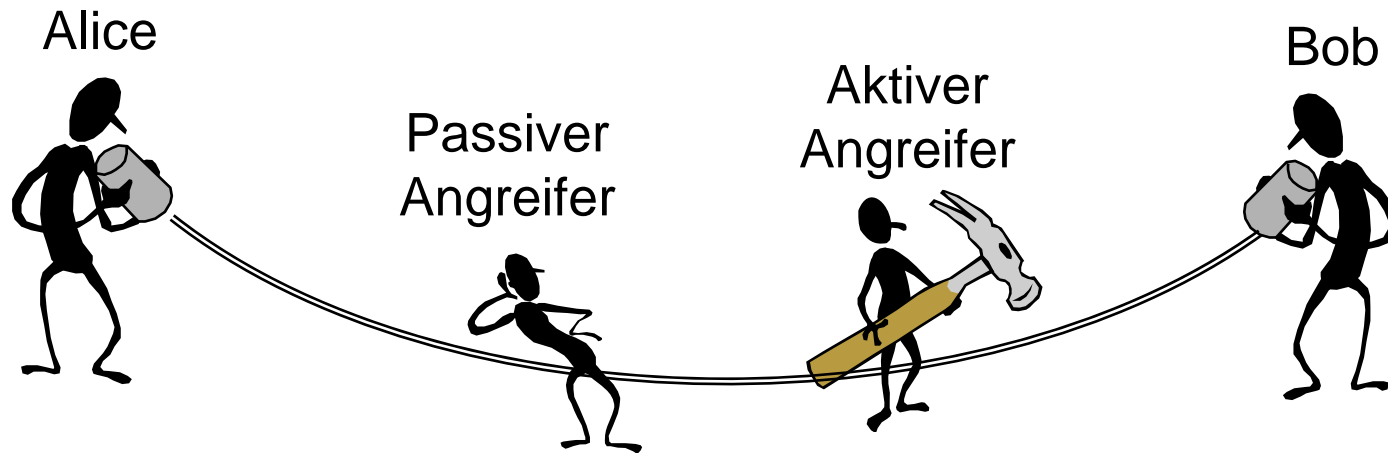
Sicherheitsanforderungen

- ❑ Authentizität
 - Angegebener Sender ist auch tatsächlicher Sender
- ❑ Vertraulichkeit
 - Ausspähen von Daten kann verhindert werden
 - ⇒ Sender verschlüsselt, und nur beabsichtigter Empfänger kann entschlüsseln
- ❑ Verbindlichkeit
 - Senden bzw. Empfangen von Daten kann nicht abgestritten werden
- ❑ Integrität
 - Empfänger kann Verfälschung von Daten erkennen
- ❑ Verfügbarkeit
 - Dienstnutzer kann Dienst auch tatsächlich nutzen



Einfaches Modell der Datenübertragung

- ❑ Passiver Angreifer: kann nur abhören, nicht manipulieren
 - Bedrohung für Vertraulichkeit
- ❑ Aktiver Angreifer: kann abhören, ändern, löschen, duplizieren
 - Bedrohung für Vertraulichkeit, Integrität, Authentizität
- ❑ Unterschied Authentizität/Verbindlichkeit:
 - Authentizität: Bob ist sicher, dass Daten von Alice kommen
 - Verbindlichkeit: Bob kann dies gegenüber Dritten beweisen





Bedrohungen

- ❑ Abhören übertragener Daten
- ❑ Modifizieren übertragener Daten
 - Ändern, Löschen, Einfügen, Umsortieren von Datenblöcken
- ❑ Maskerade
 - Vorspiegeln einer fremden Identität
 - Versenden von Nachrichten mit falscher Quelladresse
- ❑ Unerlaubter Zugriff auf Systeme
 - Stichwort „Hacking“
- ❑ Sabotage (Denial of Service)
 - gezieltes Herbeiführen einer Überlastsituation
 - „Abschießen“ von Protokollinstanzen durch illegale Pakete

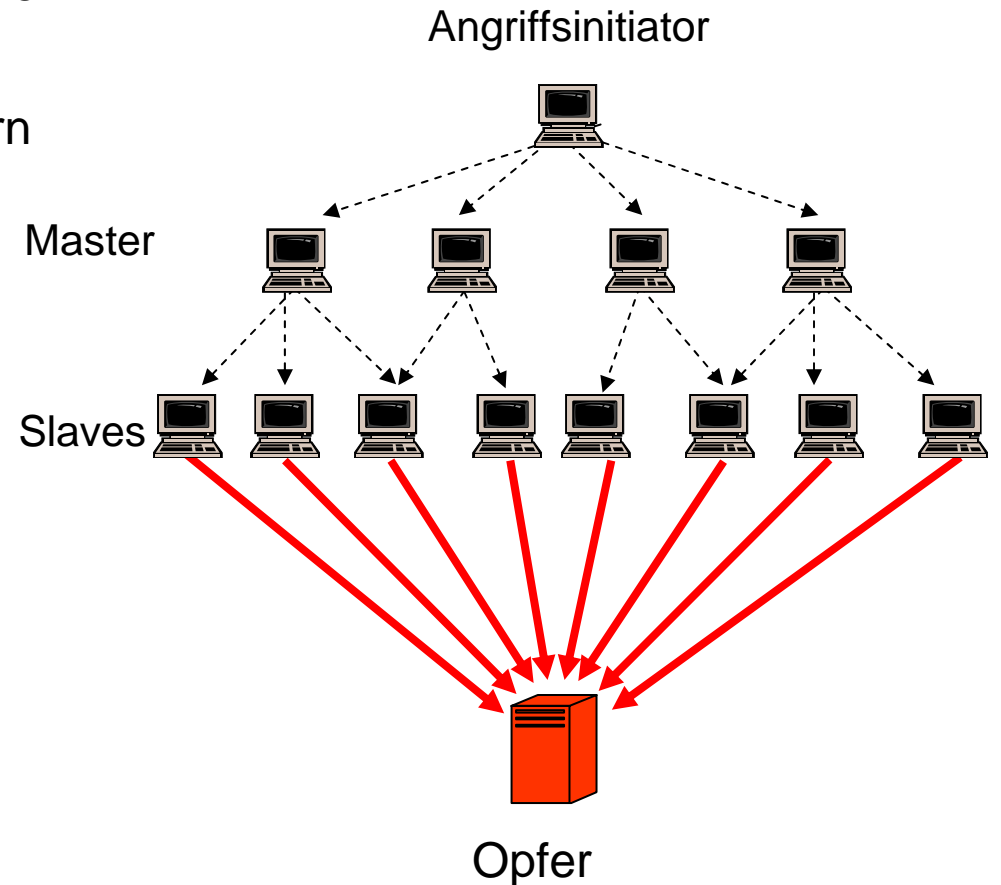


- ❑ Anzapfen von Leitungen oder Funkstrecken
- ❑ Zwischenschalten (man-in-the-middle attack)
- ❑ Wiedereinspielen abgefangener Nachrichten (replay attack)
(z.B. von Login-Nachrichten zwecks unerlaubtem Zugriff)
- ❑ gezieltes Verändern/Vertauschen von Bits oder Bitfolgen
(ohne die Nachricht selbst entschlüsseln zu können)
- ❑ Brechen kryptographischer Algorithmen
Gegenmaßnahmen:
 - Keine selbst entwickelten Algorithmen verwenden,
sondern nur bewährte und als sicher geltende Algorithmen!
 - Auf ausreichende Schlüssellänge achten
 - Möglichkeiten zum Auswechseln von Algorithmen vorsehen



Angriffsbeispiel: Verteilte Denial-of-Service-Angriffe

- Zahlreiche kompromitierte Systeme
 - Mehrere 1000 "Bot-Netze" mit mehreren 10.000 Rechnern
- Master-Systeme
 - Erhalten Befehle vom Initiator
 - Kontrollieren Slave-Systeme
- Slave-Systeme
 - Führen Angriff durch



-----> Kontrollverkehr —————> Angriffsverkehr



Sicherheitsdienste

- ❑ Authentisierung
 - Authentisierung der Kommunikationspartner (Entity Authentication)
 - Authentisierung des Datenursprungs (Data Origin Authentication)
- ❑ Zugriffskontrolle
 - Schutz einer Ressource vor unberechtigtem Zugriff
- ❑ Abhörsicherheit
 - kein Fremder soll Daten mitlesen können
- ❑ Verbindlichkeit bzw. Nicht-Zurückweisbarkeit (Non-Repudiation)
 - Sender bzw. Empfänger kann nachgewiesen werden
- ❑ Datenintegrität (Fälschungssicherheit)
 - Echtheit der Daten soll garantiert sein

- ❑ Verfügbarkeit
 - Schutz eines Dienstes vor Blockierung
- ❑ Privatheit
 - Anonymisierung bzw. Pseudonymisierung ist möglich
- ❑ Autorisierung
 - darf jemand mit der vorgegebenen Kennung einen Dienst nutzen?
- ❑ Vertraulichkeit
 - Schutz der Daten vor unberechtigter Offenlegung



Sicherheitsmechanismen: Begriffe

- ❑ Verschlüsselung
 - Kodierung der Daten mit Hilfe eines Schlüssels
 - Dekodierung nur mit zugehörigem Schlüssel möglich
 - Oder durch gezielten, sehr hohen Rechenaufwand
 - Verfahren:
 - Symmetrische Verschlüsselung: DES, Triple-DES, AES, RC4, RC5, IDEA
 - Asymmetrische Verschlüsselung: RSA
- ❑ Schlüsselaustausch und Schlüsselverwaltung
 - Diffie-Hellman-Schlüsselaustausch: Protokoll, mit dem zwei Kommunikationspartner einen geheimen Schlüssel erzeugen können
 - Standard: X.509 - Standard für Public-Key-Infrastruktur ⇨ Zertifikate
- ❑ Firewall
 - Filterfunktion zwischen verschiedenen Netzwerken
 - Erlaubt Abschottung zum Internet
 - Auch intern wichtig: über 50% aller Angriffe kommen von eigenen Mitarbeitern!



Erbringung von Sicherheitsdiensten

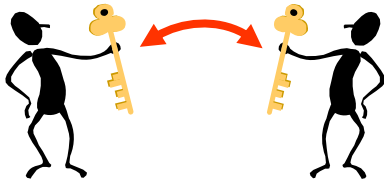
- Überwiegend mit kryptographischen Mechanismen:
 - Authentisierung
 - von Datenpaketen (data origin authentication)
 - von Systemen/Benutzern (entity authentication)
 - Integritätssicherung (integrity protection)
 - häufig kombiniert mit Daten-Authentisierung
 - Verschlüsselung (encryption)
 - Schlüsselaustausch (key exchange)

- Überwiegend Ohne kryptographische Mechanismen:
 - Zugriffskontrolle (access control)
 - Einbruchserkennung (intrusion detection)



(A)symmetrische Kryptographie

□ Symmetrische Kryptographie



□ Instanzen besitzen gemeinsamen geheimen Schlüssel

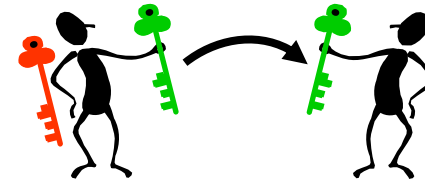
▪ Vorteile:

- geringer Rechenaufwand
- kurze Schlüssel

▪ Nachteile:

- Schlüsselaustausch schwierig
- keine Verbindlichkeit

□ Asymmetrische Kryptographie (Public-Key-Kryptographie)



□ Schlüsselpaar aus privatem und öffentlichem Schlüssel

▪ Vorteile:

- öffentliche Schlüssel sind relativ leicht verteilbar
- Verbindlichkeit möglich

▪ Nachteile:

- hoher Rechenaufwand
- längere Schlüssel

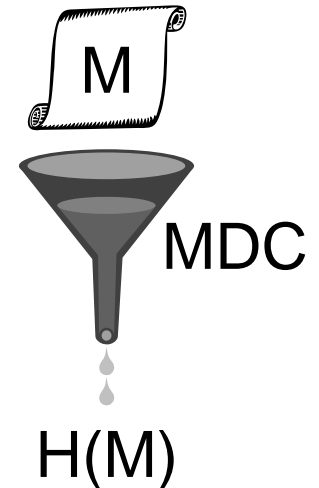


Authentisierung (1)

❑ Kryptographische Hash-Funktion

(Modification Detection Code bzw. Message Digest Code, MDC):

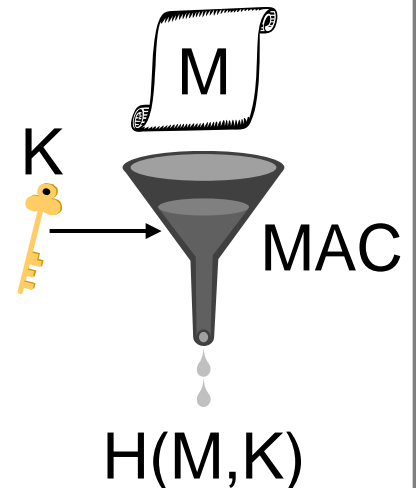
- Nachricht M (beliebig lang) \rightarrow Hash-Wert $H(M)$
- Wichtig: „Einweg“-Eigenschaft:
keine Kollisionen effizient erzeugbar
Kollision: M, M' mit $H(M)=H(M')$
- Beispiele: MD5, SHA-1, RIPEMD-160



❑ Schlüsselabhängige Hash-Funktion

(Message Authentication Code, MAC):

- Nachricht M , Schlüssel $K \rightarrow$ Hash-Wert $H(M,K)$
- kann aus MDC konstruiert werden:
HMAC (RFC 2104), z.B. HMAC-MD5
 $H(K \text{ xor pad}_1, H(K \text{ xor pad}_2, M))$

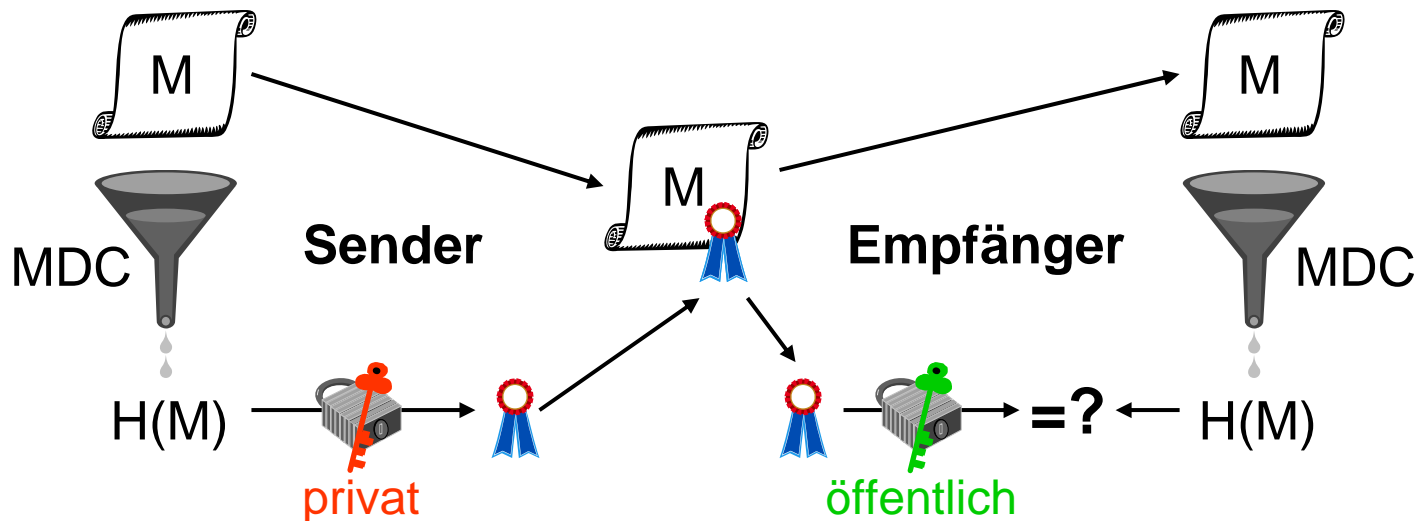




Authentisierung (2)

□ Digitale Signatur

- Hash-Wert $H(M)$ wird mit privatem Schlüssel signiert
- Empfänger überprüft Signatur mit öffentlichem Schlüssel
- kann auch Verbindlichkeit garantieren
- wichtigste Algorithmen: RSA, DSA, ElGamal
- min. Schlüssellänge: 1024 bit
(160 bit bei DSA-Variante mit elliptischen Kurven)





Authentisierung (3)

- **Authentisierung/Integritätssicherung von Datenpaketen**
 - Anhängen einer Sequenznummer zur Reihenfolgesicherung (falls nicht ohnehin vorhanden)
 - Anhängen von MAC oder Signatur, berechnet aus Daten, Sequenznummer und Schlüssel

- **Authentisierung von Systemen/Benutzern**
 - **nicht-kryptographisch:**
Benutzername/Passwort (unsicher!), Einmalpassworte, biometrische Verfahren (z.B. Fingerabdruck)
 - **kryptographisch:** Login-Nachrichten mit MAC oder Signatur
 - Sicherung gegen **Wiedereinspielen** alter Login-Nachrichten:
 - Zeitstempel (synchrone Uhren nötig)
 - Zufallszahlen (Challenge/Response-Verfahren)



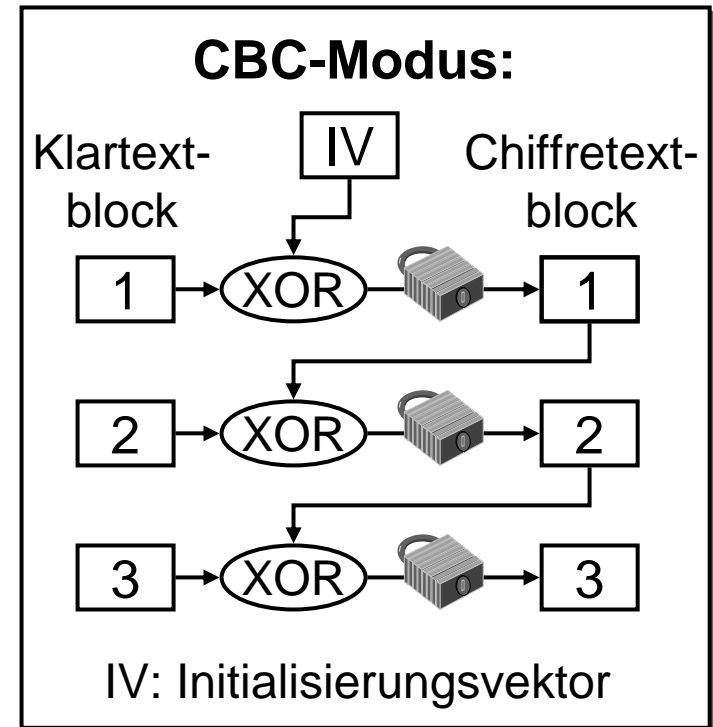
Verschlüsselung (symmetrisch)

□ Symmetrische Verschlüsselungsalgorithmen

- minimale derzeit sichere Schlüssellänge: 80 bit
- als sicher geltende Algorithmen: AES sowie Triple-DES

□ Betriebsarten

- Gängige Algorithmen (Blockchiffren) arbeiten blockweise (meist 64 bit)
- **Electronic Codebook (ECB)**
 - blockweise Verschlüsselung
 - Nachteil: Gleiche Klartextblöcke werden auf gleiche Chiffretextblöcke abgebildet
- **Cipher Block Chaining (CBC)**
 - sicherer, da jeder Block vom Vorgänger abhängt
- Weitere Betriebsarten z.B. zur byteweisen Verschlüsselung sowie zur Vorratsberechnung der kryptografischen Algorithmen





Verschlüsselung (asymmetrisch)

- ❑ Asymmetrische (Public-Key-) Verschlüsselungsalgorithmen
 - minimale derzeit sichere Schlüssellänge: 1024 bit
 - als sicher geltender Algorithmus: RSA
 - relativ langsam

- ❑ In der Praxis: Hybride Systeme
 - Zunächst: Benutzer-Authentisierung und Austausch eines Sitzungsschlüssels (symmetrisch oder Public-Key)
 - Danach: Authentisierung/Verschlüsselung der Nutzdaten mit Sitzungsschlüssel (symmetrisch)
 - Bei langen Sitzungen sollte Sitzungsschlüssel gelegentlich ausgewechselt werden (z.B. stündlich)



Schlüsselaustausch

- ❑ Symmetrisch: mit Hilfe eines Key Distribution Center (KDC)
 - KDC hat geheimen Schlüssel mit jedem Benutzer/Dienst
 - KDC authentisiert Benutzer und verteilt Sitzungsschlüssel
 - Beispiel: Kerberos (RFC 1510)

- ❑ Asymmetrisch: 2 Möglichkeiten:
 - Verschlüsseln/Signieren des Sitzungsschlüssels mit beliebigem Public-Key-Algorithmus
 - Diffie-Hellman-Schlüsselaustausch
 - Diffie-Hellman-Schlüsselaustausch allein ist bei Man-In-The-Middle-Angriff nicht sicher
 - Zusätzliche Authentisierung nötig!



Secure Shell (SSH)

- ❑ Aufgabe: sichere entfernte Rechnernutzung (remote login)
 - rsh/rlogin haben keine Authentisierung
 - telnet überträgt Passworte ungeschützt

- ❑ Funktionsweise:
 1. Austausch eines Sitzungsschlüssels (Diffie-Hellman) und Server-Authentisierung (digitale Signatur)
danach: symm. Verschlüsselung + MAC für alle Pakete
 2. Benutzer-Authentisierung (dig. Signatur oder Passwort)

- ❑ Zusätzliche Funktionalität:
 - Verschlüsselte Dateiübertragung mit scp
 - Verschlüsselte Tunnel für einzelne TCP-Ports
 - automatische Einrichtung eines X11-Tunnels

- ❑ Versionen: 1.0, 2.0 zueinander inkompatibel (Infos: www.ssh.fi)



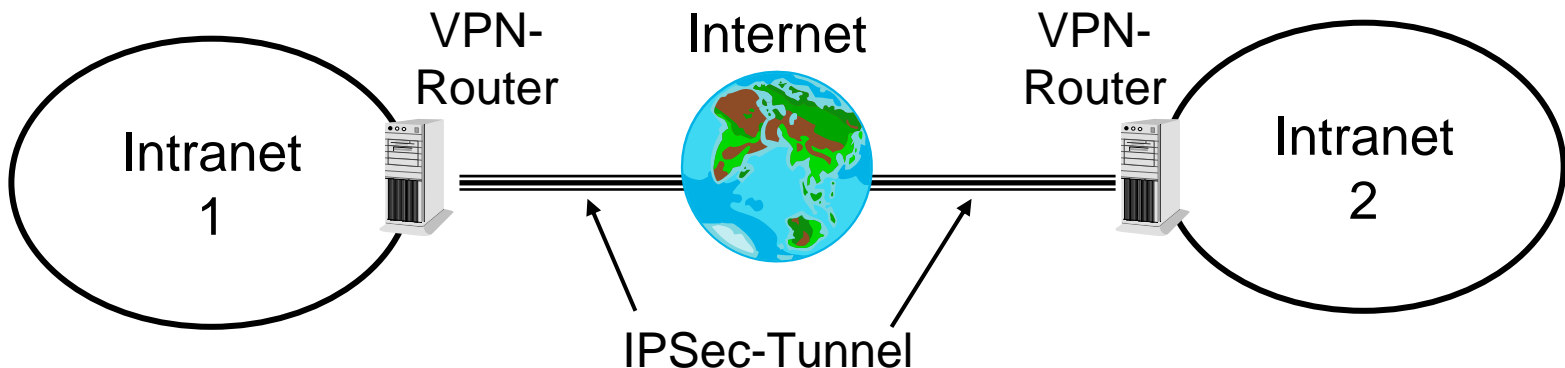
Secure Socket Layer (SSL)

- ❑ Aufgabe: Verschlüsselung/Datenintegrität für einzelne Sockets
 - Haupteinsatzgebiet: verschlüsselte HTTP-Verbindungen (https)
- ❑ Funktionsweise:
 - Austausch eines Sitzungsschlüssels (Diffie-Hellman)
 - optional Server-/Benutzer-Authentisierung (digitale Signatur)
 - danach: Verschlüsselung + MAC für alle Pakete
- ❑ Versionen:
 - von Netscape: SSL 1.0 bis SSL 3.0
 - TLS - Transport Layer Security (RFC 2246) basierend auf SSL 3.0



IP Security (IPSec)

- Aufgabe: sicheres Tunneln von IP-Paketen
 - Verschlüsselung am Tunneleingang, Entschlüsselung am Ausgang
 - kann z.B. für das gesamte VPN automatisch durchgeführt werden oder nur für bestimmte Anwendungen
- Beispiel: IP Security
 - Funktionsweise:
 - MAC und/oder symm. Verschlüsselung
 - 2 Paketformate: AH (RFC 2402), ESP (RFC 2406)
 - Produkte:
 - FreeS/WAN (www.freeswan.org)
 - Cisco VPN-Produkte
 - Windows VPN-Funktionen





IPSec: Authentication Header und Encapsulating Security Payload

□ Authentication Header

Authentifizierung, Datenintegrität durch MAC

▪ Transportmodus

- Keine Veränderung der Adressen, falls direkte Kommunikation

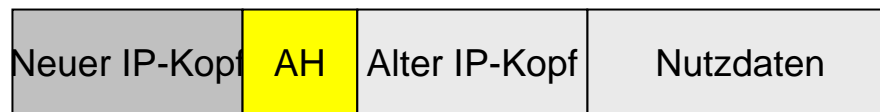
Transportmodus



▪ Tunnelmodus

- Neue IP-Adressen, zwischen beliebigen Partnern

Tunnelmodus

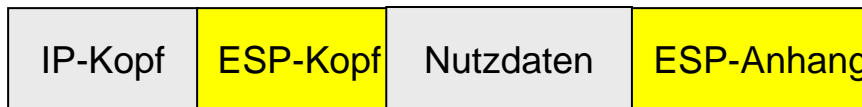


□ Encapsulating Security Payload

- Authentifizierung, Datenintegrität, Privatheit durch Verschlüsselung und/oder MAC

▪ Transportmodus

Transportmodus



▪ Tunnelmodus

Tunnelmodus





- ❑ X.509 - Standard für Public-Key-Infrastruktur
- ❑ hierarchisches System von vertrauenswürdigen Zertifizierungsstellen (engl. certificate authority, kurz CA)
- ❑ Webbrowser beinhalten eine vorkonfigurierte Liste vertrauenswürdiger Zertifizierungsstellen, deren ausgestellten SSL-Zertifikaten der Browser vertraut.
- ❑ Zertifizierungsstelle kann ungültige Zertifikate in Zertifikatsperrlisten (certificate revocation list, kurz CRL) führen

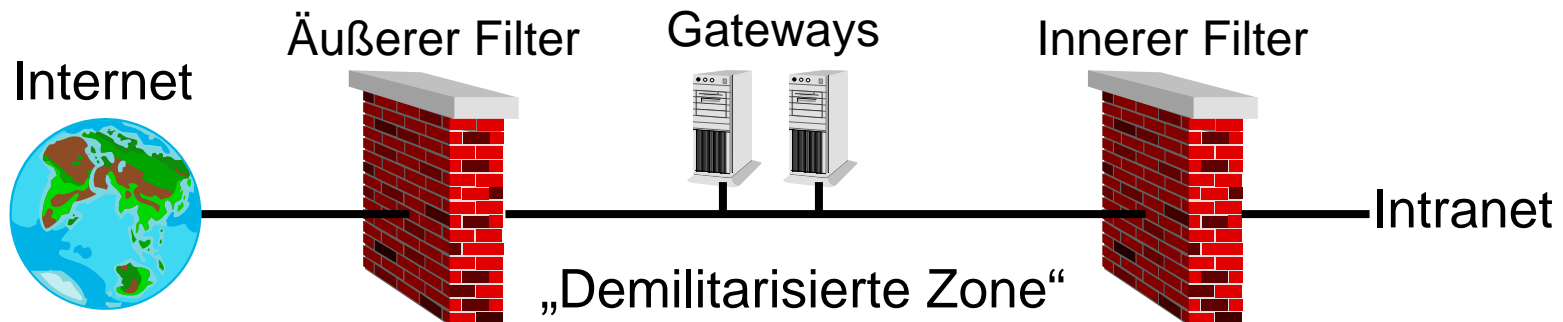
Struktur eines X-509-v3-Zertifikats

- ❑ Zertifikat
 - Version
 - Seriennummer
 - Algorithmen-ID
 - Aussteller
 - Gültigkeit
 - von
 - bis
 - Subject
 - Subject Public Key Info
 - Public-Key-Algorithmus
 - Subject Public Key
 - Eindeutige ID des Ausstellers (optional)
 - Eindeutige ID des Inhabers (optional)
 - Erweiterungen
 - ...
- ❑ Zertifikat-Signaturalgorithmus
- ❑ Zertifikat-Signatur



Zugriffskontrolle

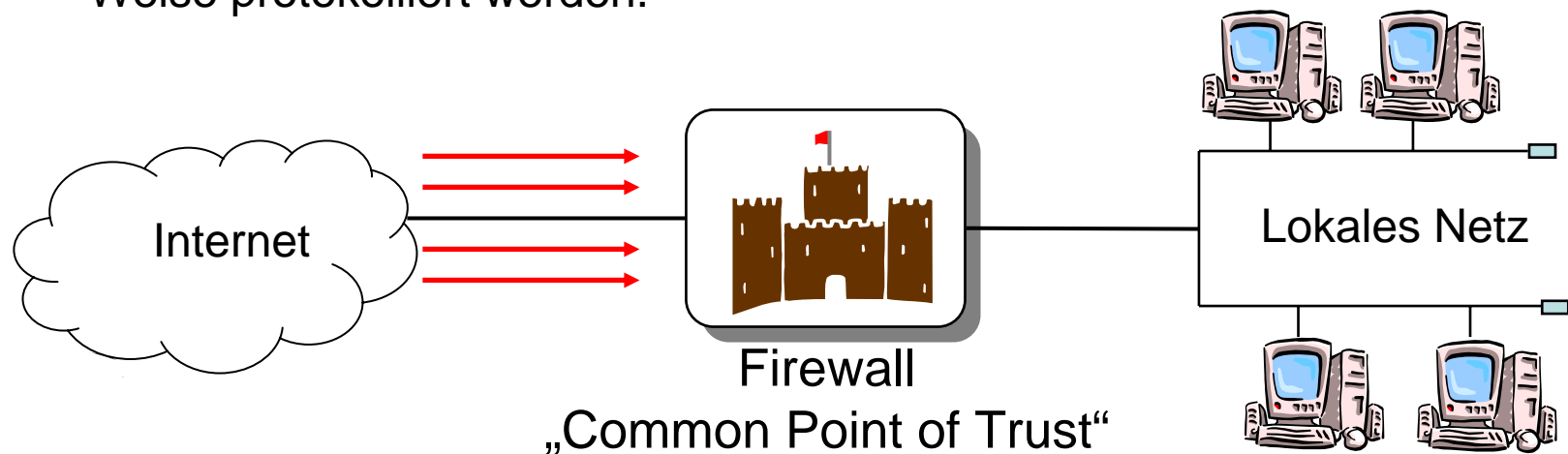
- Auf Anwendungsebene: System von Zugriffsrechten
 - Beispiele: Unix/NT-Dateirechte, SNMP-Objektrechte
- Auf Netzwerk-/Transportebene: Firewalls
 - Paketfilter filtern nach Quell/Zieladresse + Ports (TCP/UDP)
 - Unterscheidung: ingress/egress filtering (inbound / outbound packets)
 - Anwendungs-Gateways (Zugriffskontrolle, Protokollierung)
 - Kann mit privaten Adressen und Adressumsetzung (NAT) kombiniert werden
 - Probleme mit manchen Protokollen (z.B. FTP, H.323)





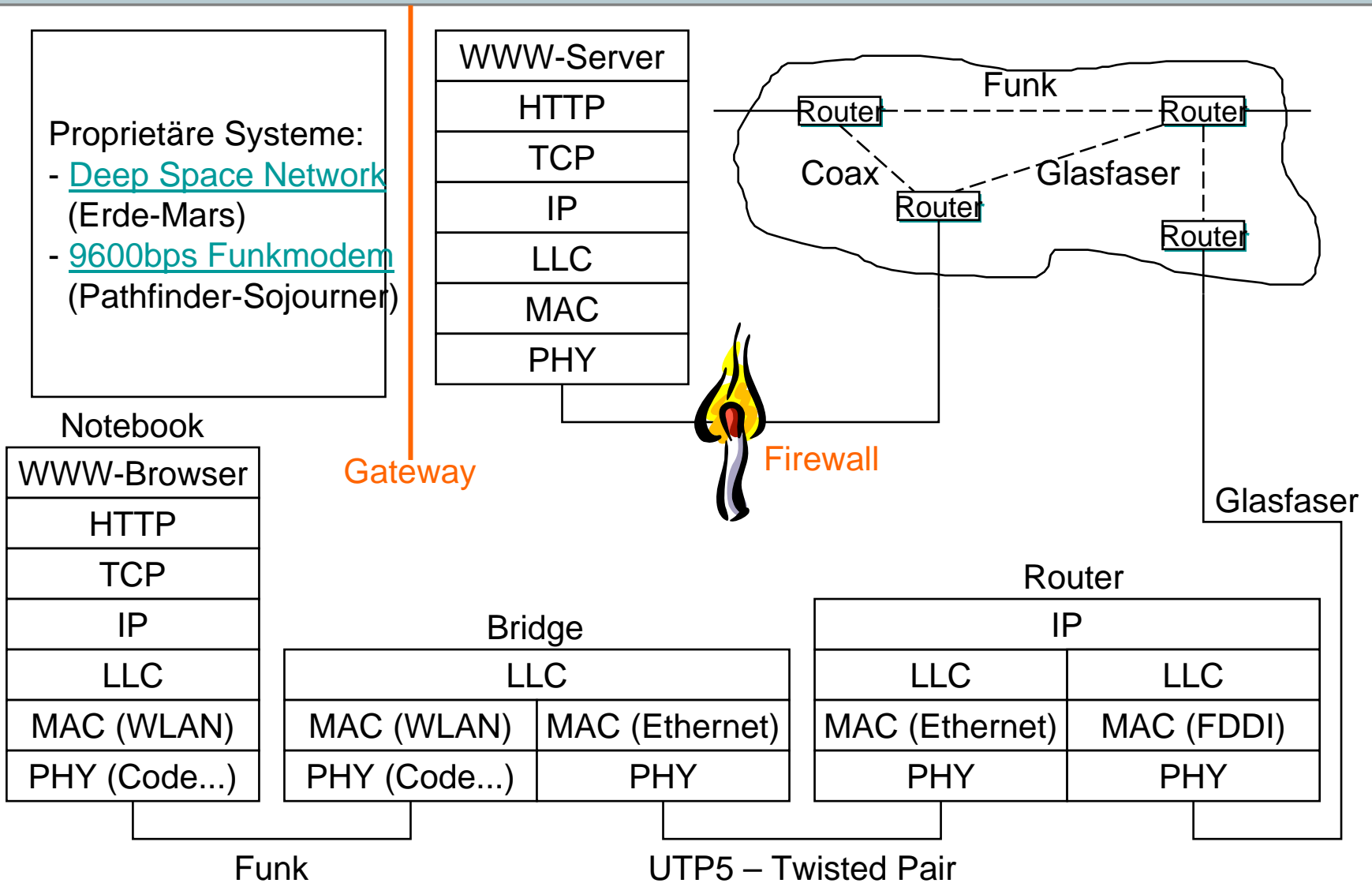
Firewall

- ❑ Ziel: Schutz des lokalen Netzes hauptsächlich gegenüber externen (aktiven/passiven) Angriffen („keep the good bits in and the bad bits out“)
- ❑ Vorteile:
 - Kosten: Die zentrale Realisierung von Sicherheitsmechanismen ist wesentlich kostengünstiger als die Absicherung jedes einzelnen Rechners.
 - Wirkung: Die Sicherheitspolitik eines Unternehmens kann sehr einfach durchgesetzt bzw. angepasst werden.
 - Sicherheit: Es existieren nur wenige Angriffspunkte im Netz (im Idealfall nur das Firewall-System selbst).
 - Überprüfbarkeit: Sämtliche Kommunikationsvorgänge können auf einfache Weise protokolliert werden.





Beispiel: Firewall zum Schutz eines WWW-Servers





Firewalls im Internet

□ Firmen, Behörden, Privatpersonen, Universitäten sind von den Protokollen TCP/IP her gleichberechtigt an das Internet angebunden

⇒ Das *interne* Netz von unerwünschten Zugriffen von außen schützen:

- am sichersten ist nur die physikalische Trennung zwischen Rechnern am Internet und firmeninternen Rechnern
- Firewalls sind meist Router, die Pakete anhand der IP-Adresse und Port-Nummer herausfiltern können (zusätzliche Vermerke in einer Log-Datei möglich)
 - *Beispiel:* Ausfiltern von Paketen mit dem Port 80 verhindert den Zugriff auf normale WWW-Server; werden z.B. 129.13.x.y Adressen gefiltert, kann kein Rechner aus diesem Subnetz auf etwas zugreifen!
- Außer Paketfilter sind oft noch Anwendungsgateways und Adressübersetzung integriert
 - Umsetzung zwischen verschiedenen mail-Systemen
 - dynamische Abbildung einer IP-Adresse auf viele verschiedene interne Endsysteme



- ❑ Kann auf verschiedenen Protokollschichten arbeiten, viele unterschiedliche Funktionen anbieten
- ❑ Schicht 2
 - Filtern nach MAC-Adressen
 - lässt z.B. nur Adapter zu, die in der Firewall bekannt sind
- ❑ Schicht 3
 - Filtern nach IP-Adressen
 - kann z.B. Verkehr nach Herkunft und Ziel filtern
- ❑ Schicht 4
 - Filtern nach Ports
 - kann z.B. Pakete je nach Anwendung filtern
- ❑ Anwendungsschicht - Proxy
 - Virenschanner, Inhaltsüberprüfung (Text, Bilder), WWW-Adressen, ...



Firewall Beispiel

- ❑ Gezielte Aktionen in Abhängigkeit von Adressen und Anwendungen
- ❑ Spezielle Firewall-Lösungen mit hoher Leistungsfähigkeit erhältlich
- ❑ Sicherheit aber nur so gut wie die Wartung!

Quelladresse	Zieladresse	Dienst	Aktion	Protokoll
beliebig	Web-Server	http	akzeptieren	kurz
Intranet	Intranet	smtp	verschlüsseln	normal
Intranet	alle	http	akzeptieren	kurz
Extranet	Intranet	smtp, http	akzeptieren, Viren-Scan	normal
alle	alle	alle	verwerfen	Alarm, lang



Firewall-Mechanismen

- Analyse der ein-/ausgehenden Datenpakete (Packet Filtering)
 - Kontrolle der Felder des Paketkopfes, z.B. Flags, IP-Adresse und Portnummer
 - Erlaubter/nicht erlaubter Datenverkehr ist in Access-Liste vermerkt
 - eingehend: deny *.*.*, 23 blockiert telnet
 - ausgehend: permit 129.13.*.*, 80 erlaubt http nur für Rechner mit IP=129.13.x.y

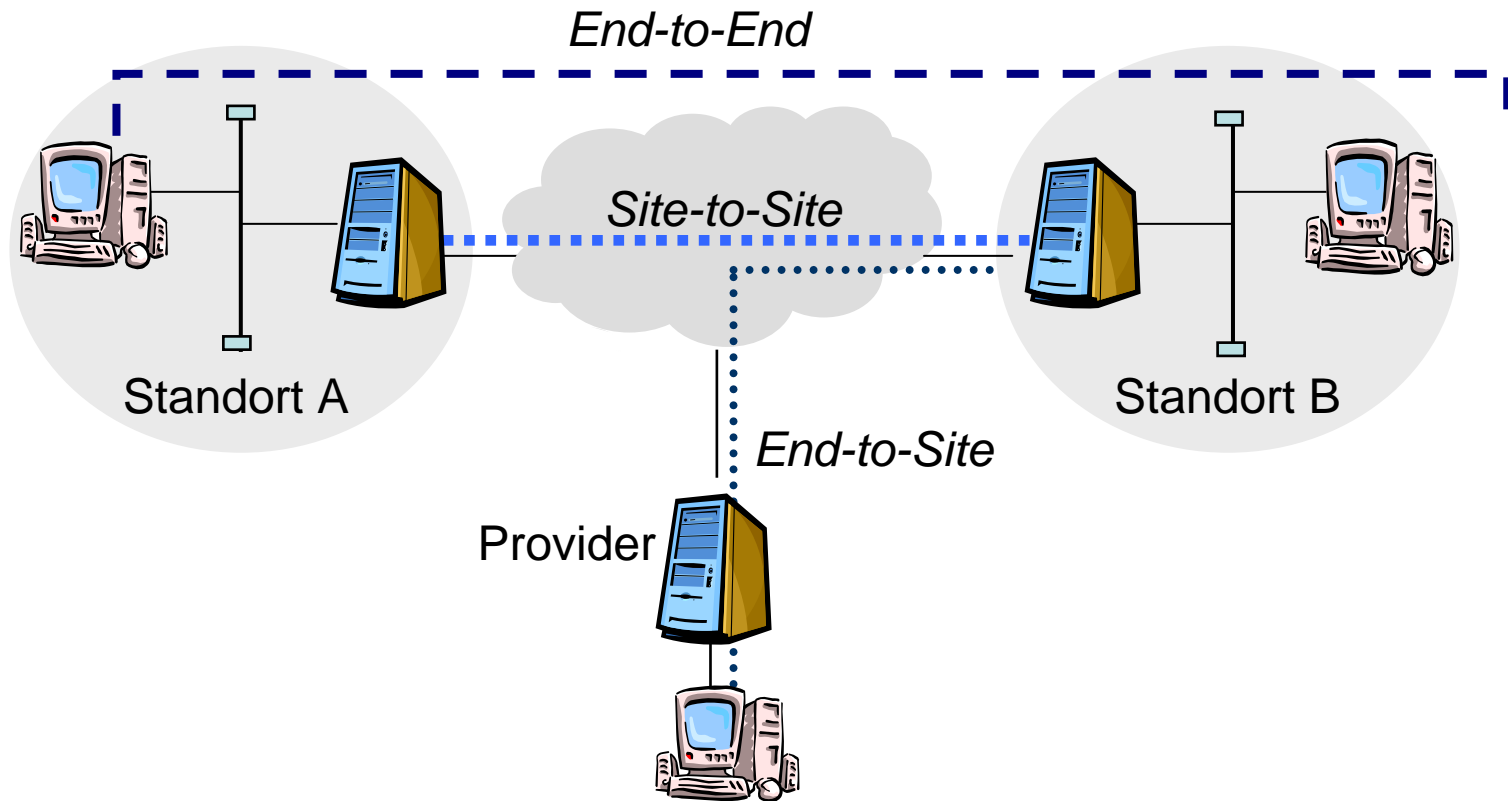
- Adressumsetzung (Network Address Translation, NAT)
 - Rechner im lokalen Netz von außen nicht erreichbar (z.B. 192.168.x.y)
 - Firewall/Gateway nimmt Abbildung auf gültige Adressen vor

- Proxy-Dienste (Proxy Services)
 - Endsysteme im geschützten Netz nur über (Application-)Gateway erreichbar
 - Für jede zulässige Anwendung fungiert Gateway als Proxy
 - Verbindungsaufbau zu Zielrechner nur nach Authentifikation
 - Filterung auf Anwendungsebene (z.B. nur ftp-get aber kein ftp-put)
 - Detaillierte Rechteverwaltung und Protokollierung



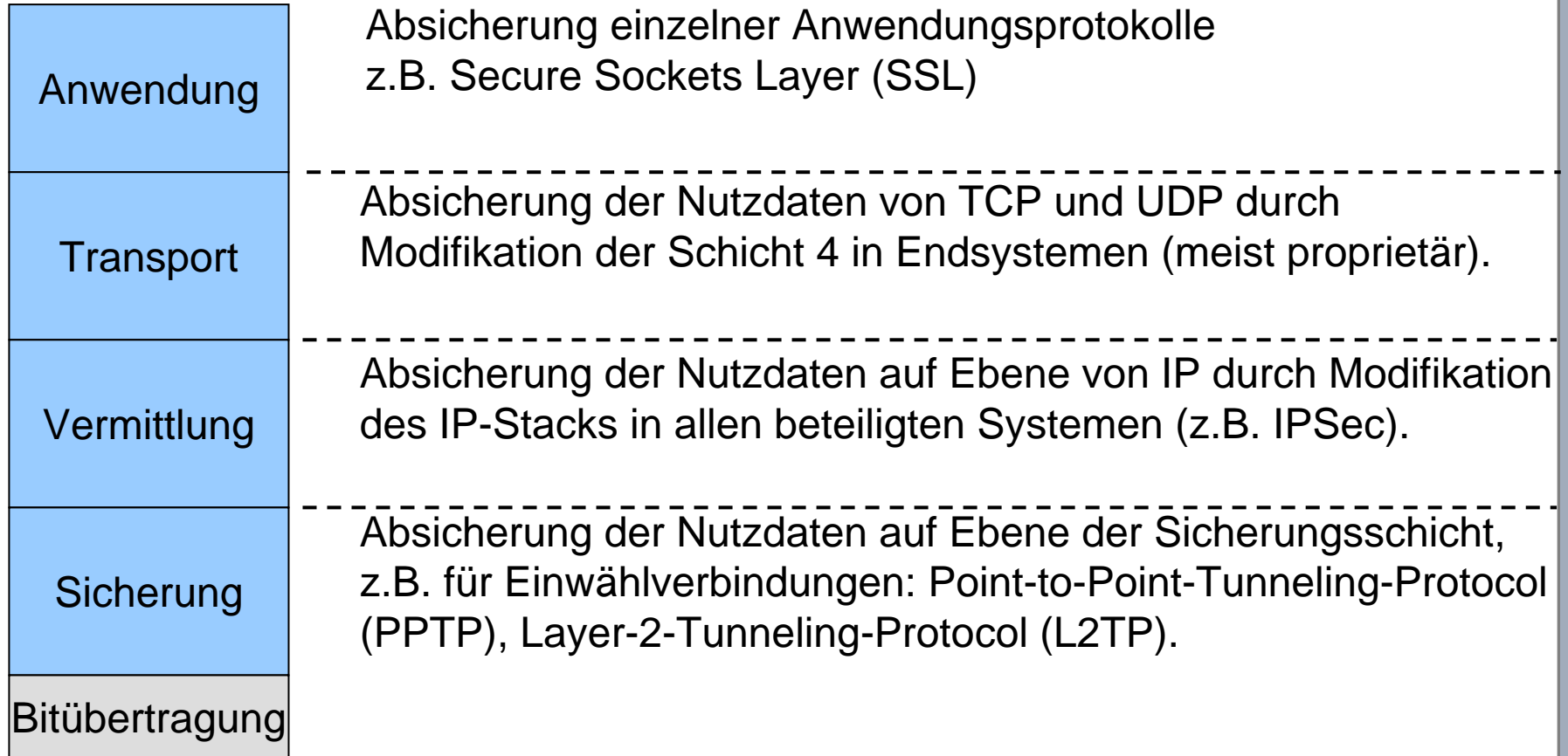
Virtuelle private Netze (VPNs)

- **Ziel:** Gewährleistung eines gesicherten Datenaustauschs zwischen entfernten Kommunikationspartnern/Standorten über (ungesicherte) Transit-Netze (z.B. das Internet) durch Authentifizierung und Verschlüsselung.





VPNs im Internet

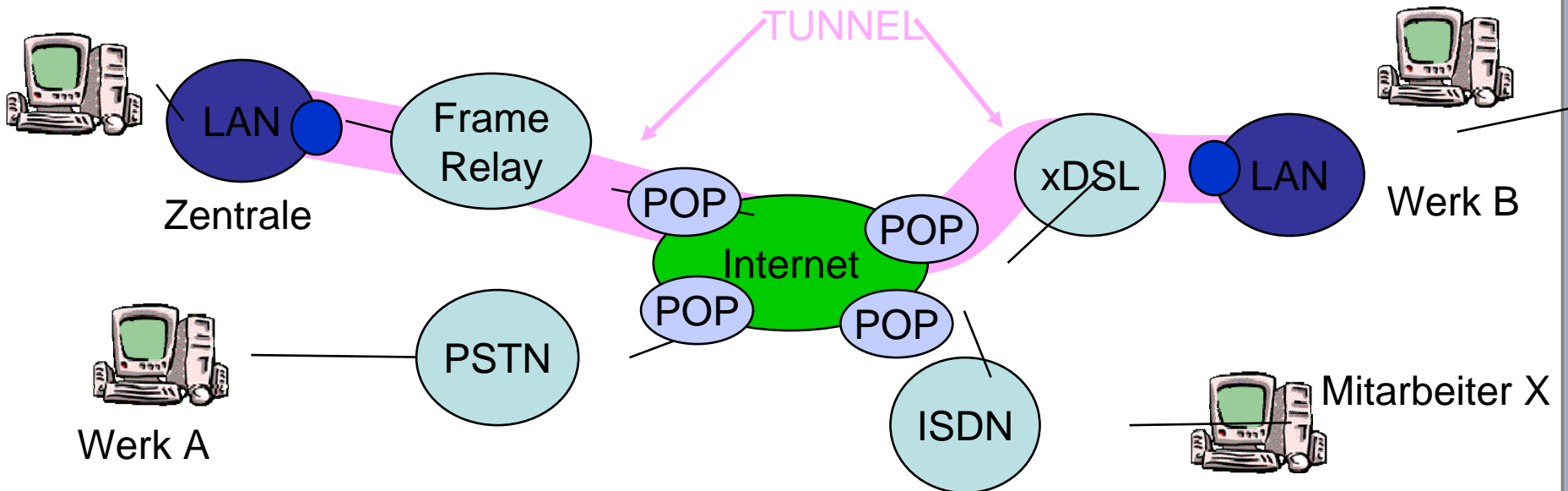




Virtuelle Private Netze

□ Lösung: Virtuelle Private Netze (VPN)

- VPN als logisches Netz
- VPNs können auf verschiedenen Techniken basieren
 - Schicht-2-Tunneling: LAN-Pakete werden transparent über ein externes Netz transportiert
 - Schicht-3-Tunneling: IP-Pakete werden transparent über ein externes Netz transportiert

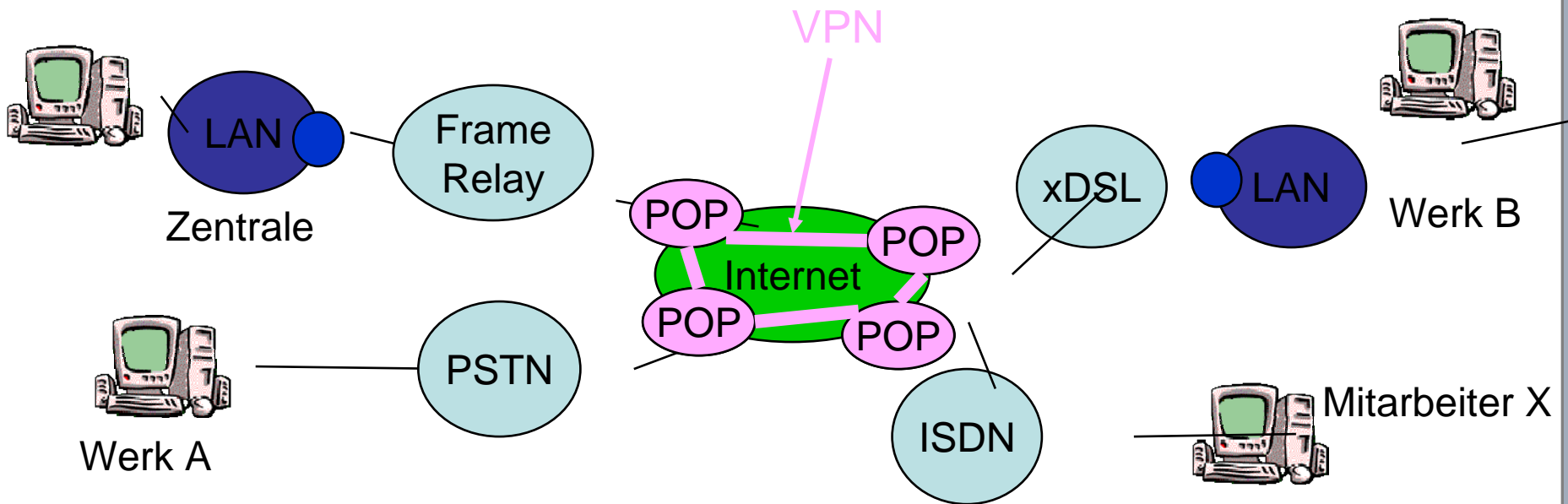




Ort eines VPN

□ Outsourcing

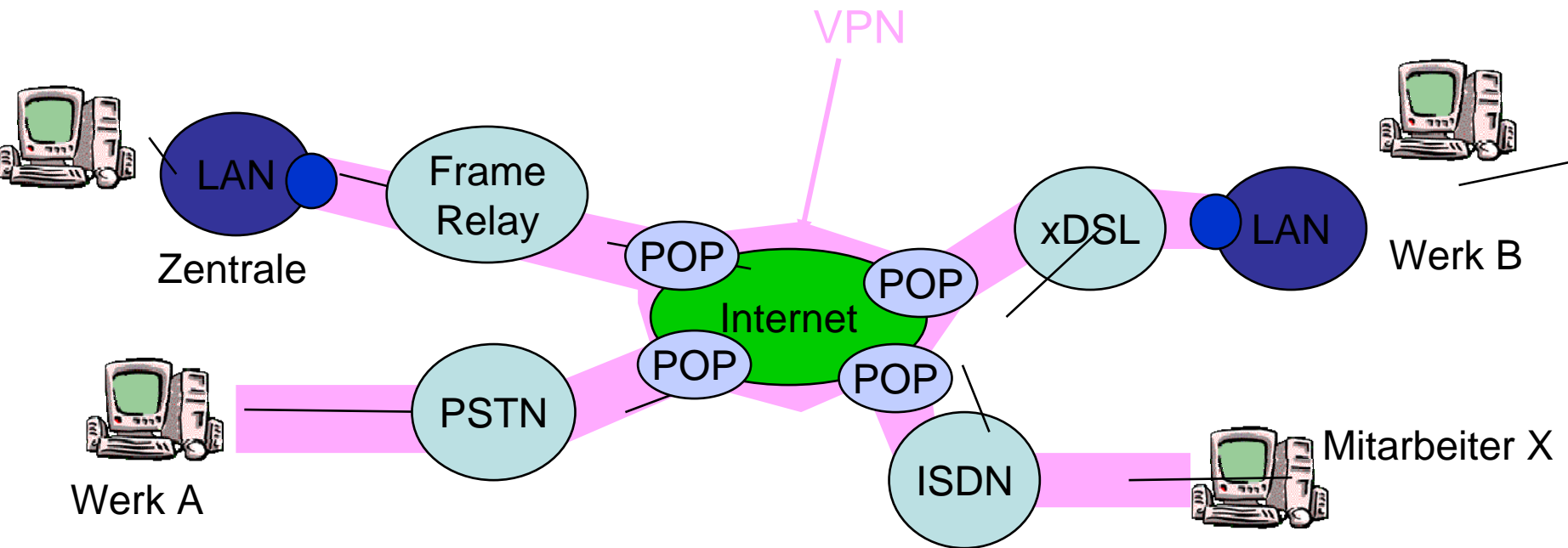
- VPN wird vom Netz-Provider zur Verfügung gestellt
- Provider bietet Einwahlpunkte, zwischen diesen besteht ein VPN
- kaum Hard-/Software auf Kundenseite nötig





Ort eines VPN

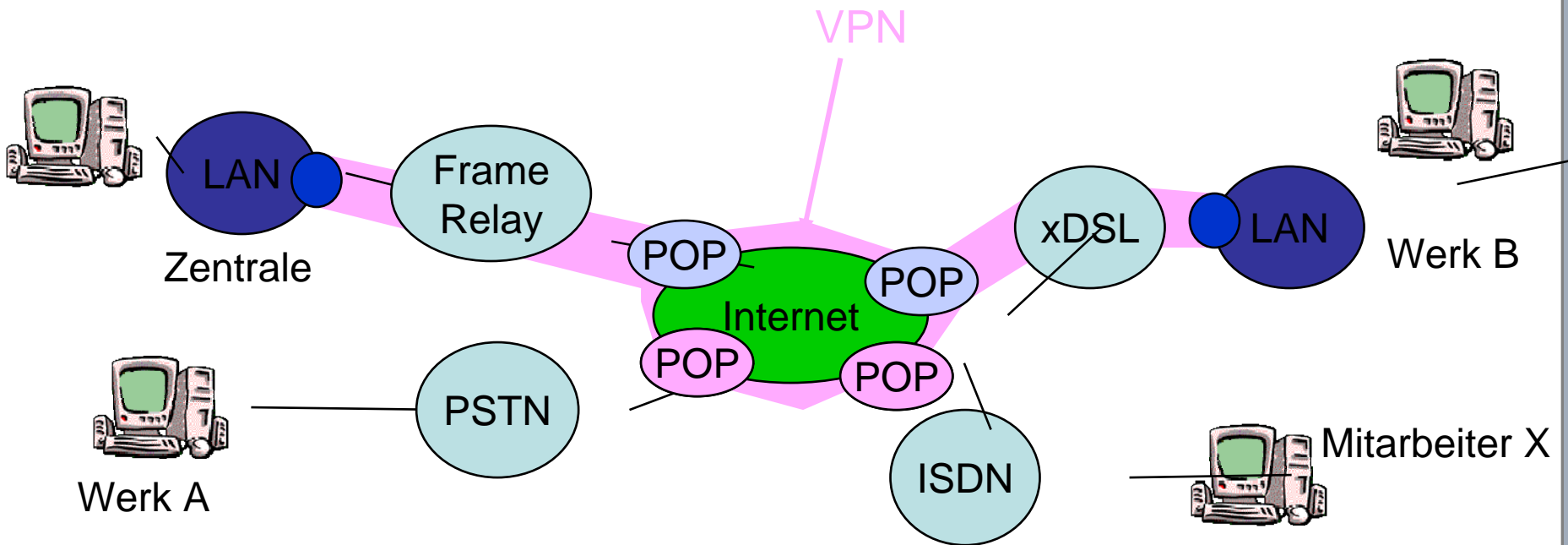
- In-house VPN, VPN zwischen den Standorten
 - Tunnels werden z.B. zwischen den firmeneigenen Routern aufgebaut
 - Netz-Provider hat keinen Einblick in das VPN
 - Firma legt selbständig Sicherheit, Protokolle etc. fest
 - Software für Sicherheit, Tunneling, Verschlüsselung notwendig





Ort eines VPN

- Mischformen möglich
 - oftmals werden Tunnels zwischen Routern eingerichtet, nicht jedoch für den entfernten Zugriff
 - VPN endet am POP des Providers





Entfernter Zugriff auf das Intranet

- ❑ Außenanbindung
 - Außendienstmitarbeiter
 - Kunden, Lieferanten etc.
 - Informationen für alle
- ❑ Firewall zur Zugangsbeschränkung
 - Anbindung des Intranet an das Internet
 - Zugang von jedem beliebigen Rechner weltweit
 - Schutz durch eine Firewall, d.h. Filter für unerlaubte Daten
 - Software für Firewall benötigt, Rechenleistung auf Router wichtig
- ❑ Einwahlmöglichkeiten für den Außendienst
 - Erweiterung des VPN dynamisch bis hin zum Ort des Mitarbeiters
 - Einwahl via Modem (ISDN/analog)
 - Sicherheit durch Passwort, gesicherte Verbindung
 - Modem plus Software benötigt



Weitere Sicherheits-Themen

- ❑ E-Mail Sicherheitsproblem: SPAM
 - Webmail: Mit Bots lassen sich zahlreiche Benutzer-Konten erzeugen
 - Capatcha: Completely Automated Public Turing test to tell Computers and Humans Apart
 - DNS blacklisting
 - Spamer Virus

- ❑ Voice-over-IP Sicherheitsprobleme
 - SPIT Spam over IP-Telephony
 - DoS
 - Abhören und Modifikation
 - Missbrauch der Dienste (Fraud)
 - Nicht-Autorisierte oder Nicht-abrechenbare Ressourcen Nutzung
 - Impersonifizierung, gefälschte Identitäten