Sicherheit im Internet

Technische
Universität
Darmstadt

Seminar: Ausgewählte Kapitel der Rechts- und Wirtschaftsinformatik

Wintersemester 1998/99

Fachgebiet BWL V - Betriebliche Kommunikationssysteme

Prof. Dr. H. J. Petzold

Thomas Schmitz & Michael Hurler

Gliederung

- Motivation
- Anforderungen an ein Sicherheitskonzept
- Kryptographie
- Protokolle und ihre Sicherheitsprobleme
- Schutz offener Systeme: Firewalls
- Dienste und ihre Sicherheitsprobleme am Beispiel des WWW
- Ausblick

Motivation

- Internet gewinnt zunehmend an Bedeutung für Unternehmen und Privatpersonen
- Kommunikation i.d.R. unverschlüsselt
- Bedrohung:
  - Zugriff auf übertragene Daten durch staatliche und private Organisationen
  - Angriffe auf Unternehmensrechner aus dem Internet
  - Technisch relativ leicht realisierbar
  - Ziel: Kopieren, Ändern und Löschen von Daten
- Gefahr wird meist unterschätzt

Sicherheit im Internet

- Sicherheit im Internet ≈ Kommunikationssicherheit
- Nicht Gegenstand der Arbeit
  - Vergabe von Zugriffsrechten
  - Physischer Schutz der Kommunikationsinfrastruktur
  - Rechtliche Rahmenbedingungen, wie
    - Datenschutz
    - Vertragsschluß
    - Zahlungsverkehr

Kriterien für Kommunikationssicherheit

- Vertraulichkeit
- Datenintegrität
- Verfügbarkeit
- Berechtigung
  - Authentifikation
  - Zugriffskontrolle
  - Sicherstellung der Zustellung
- Wahrung der Anonymität

Sicherheitsanforderungen

- Zu erfüllende Kriterien
  - Einschränkung von Risiken
  - Benutzbarkeit der Lösung
  - Realisierbarkeit
    - technische Durchführbarkeit
    - ökonomische Vertretbarkeit
- Ausarbeitung unter Einbeziehung und Mitarbeit der Unternehmensleitung
- Mittel zur Bestimmung der Sicherheitsanforderungen: Durchführung einer detaillierten Risikoanalyse

Risikoanalyse

- Bestandsaufnahme
- Bedrohungsanalyse
- Bestimmung von Eintrittswahrscheinlichkeit und möglicher Schadenshöhe
  - Risiko = Schadenshöhe $\times$ Eintrittswahrscheinlichkeit
- Risikobewertung
  - tragbare Risiken
  - nicht tragbare Risiken

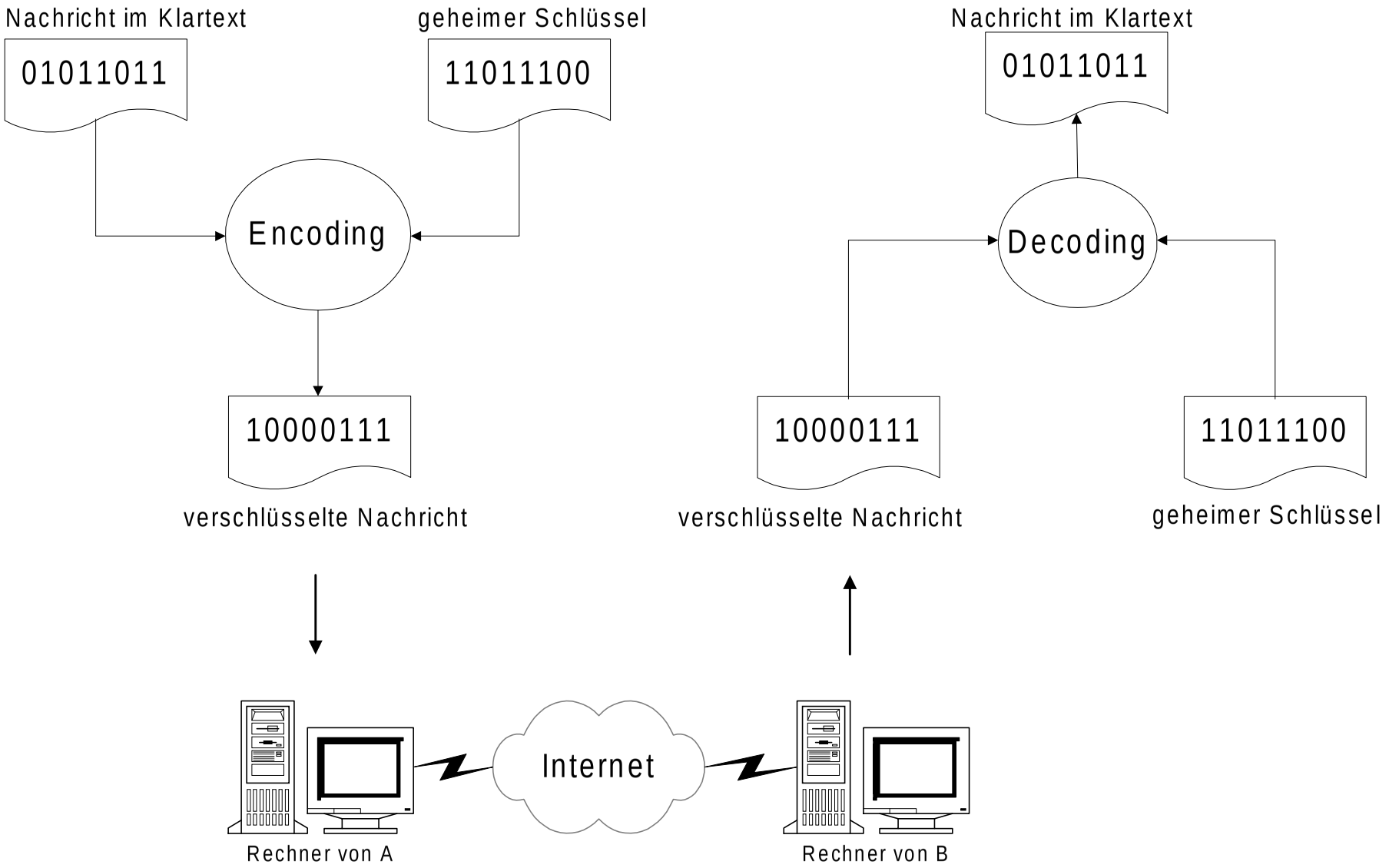
Sicherheitskonzept

- **Ziel:** Schließung der Sicherheitslücken, die den Sicherheitsanforderungen zuwiderlaufen
- Maßnahmen
  - präventive
  - überwachende
  - reaktive
- Maßnahmenbündel zur Aufrechterhaltung der Systemsicherheit jetzt und in der Zukunft
  - Anpassung der Anforderungen
  - Überarbeitung der Maßnahmen

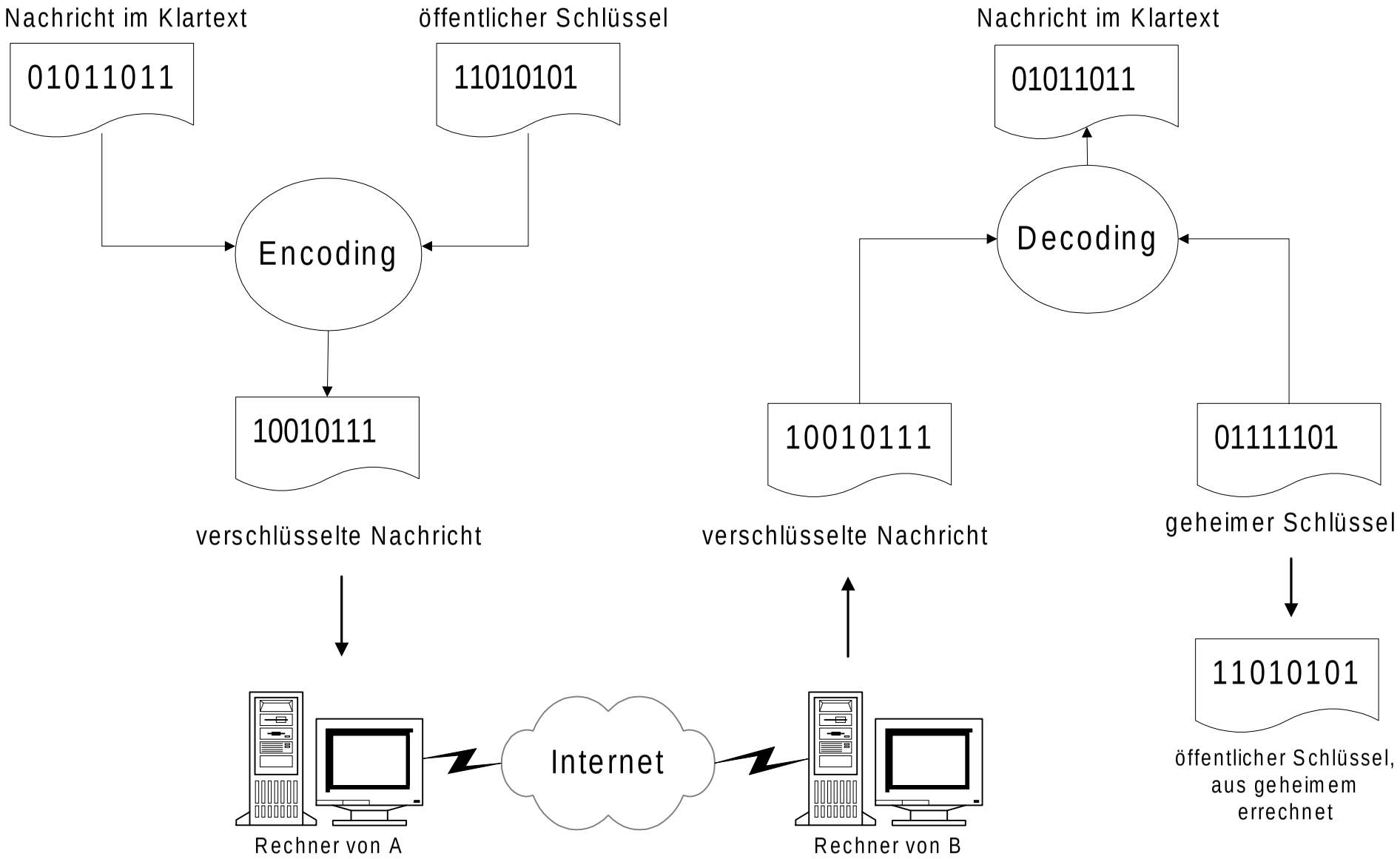
Kryptographie

- Verschlüsselung
  - Schutz vor unberechtigter Einsichtnahme
  - Verfahren
    - symmetrische
      - Bekannte Verfahren: DES, IDEA, CAST
    - asymmetrische
      - Bekannte Verfahren: RSA, ElGamal
- Message Digest / Signaturen
  - Berechnung eines „Fingerabdrucks“ einer Nachricht
  - In Verbindung mit Verschlüsselung Schutz vor unberechtigter Veränderung
  - Bekannte Verfahren: MD5, SHA

Symmetrische Verschlüsselung (Beispiel)



Asymmetrische Verschlüsselung (Beispiel)



Bedeutung der Schlüssellänge

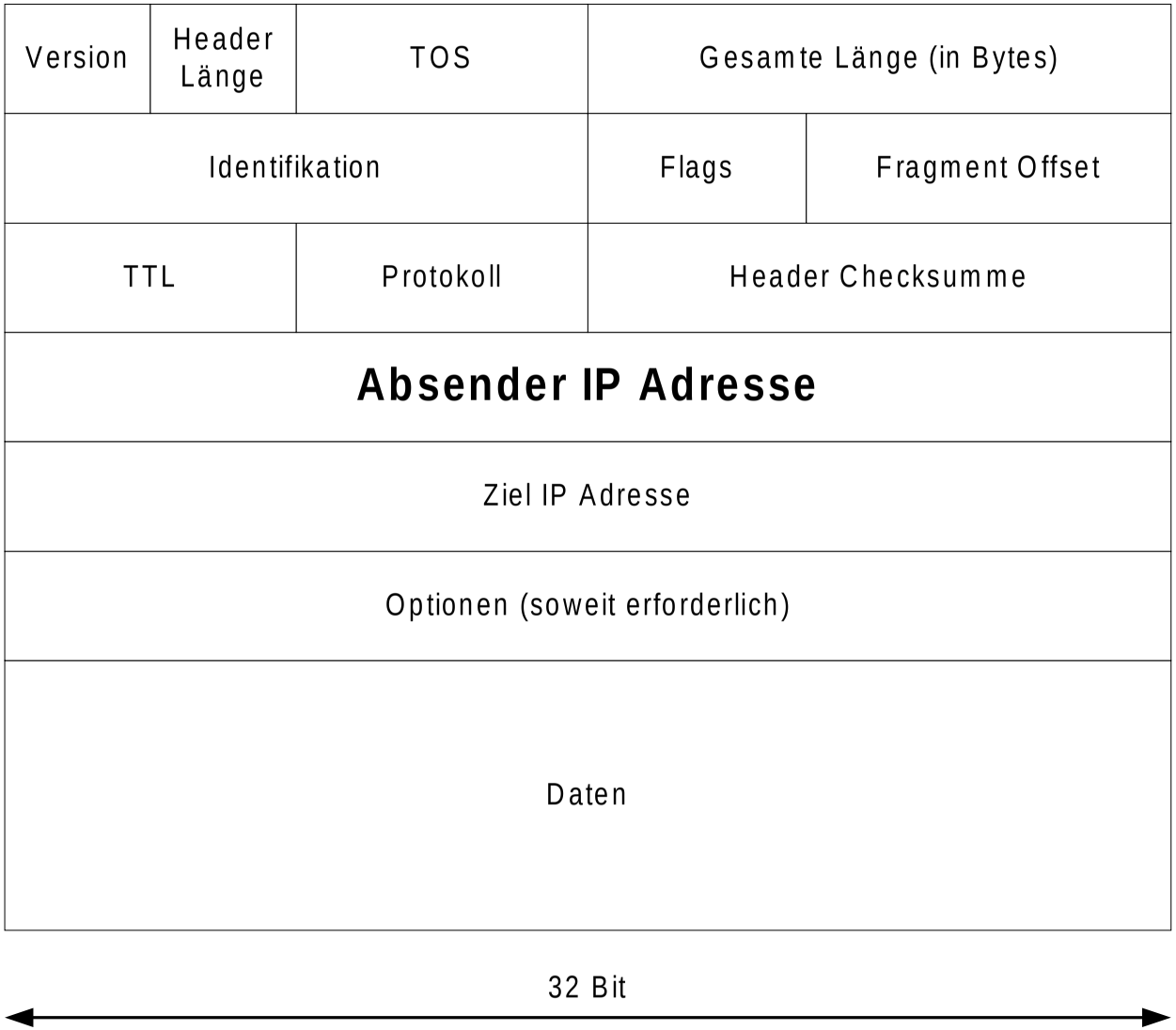
Kosten/Schlüssellänge in Bit	40	56	64	80	112	128
$ 100.000	2 s	35 h	1 a	70.000 a	10^{14} a	10^{19} a
$ 1.000.000	0,2 s	3,5 h	37 d	7.000 a	10^{13} a	10^{18} a
$ 10.000.000	0,02 s	21 min	4 d	700 a	10^{12} a	10^{17} a
$ 100.000.000	2 ms	2 min	9 h	70 a	10^{11} a	10^{16} a
$ 1.000.000.000	0,2 ms	13 s	1 h	7 a	10^{10} a	10^{15} a
$ 10.000.000.000	0,02 ms	1 s	5,4 min	245 d	10^{9} a	10^{14} a
$ 100.000.000.000	2 µs	0,1 s	32 s	24 d	10^{8} a	10^{13} a
$ 1.000.000.000.000	0,2 µs	0,01 s	3 s	2,4 d	10^{7} a	10^{12} a
$ 10.000.000.000.000	0,02 µs	1 ms	0,3 s	6 h	10^{6} a	10^{11} a

Länge symmetrischer Schlüssel	Länge asymmetrischer Schlüssel
56 Bit	384 Bit
64 Bit	512 Bit
80 Bit	768 Bit
112 Bit	1792 Bit
128 Bit	2304 Bit

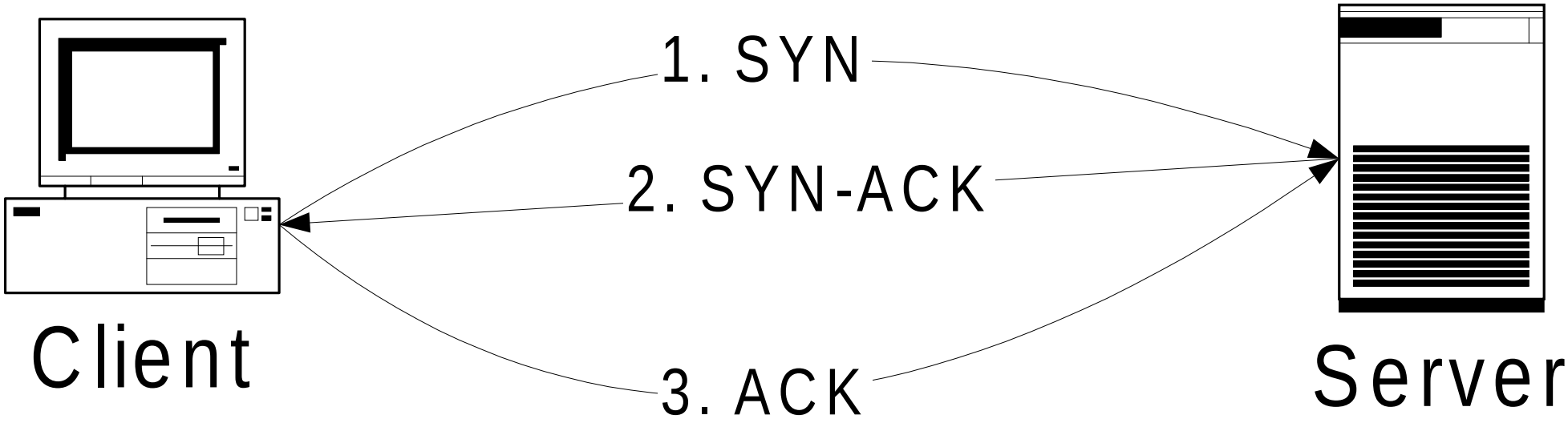
Protokolle und ihre Sicherheitsprobleme

- Ziele von Angriffen
  - IP
  - TCP
  - (ICMP, ARP, UDP)
- Angriff auf IP
  - **IP-Spoofing** - Fälschung der Absenderadresse
- Angriffe auf TCP
  - **SYN-Flooding** - Denial-of-Service-Angriff
  - ...

IP-Datagramm



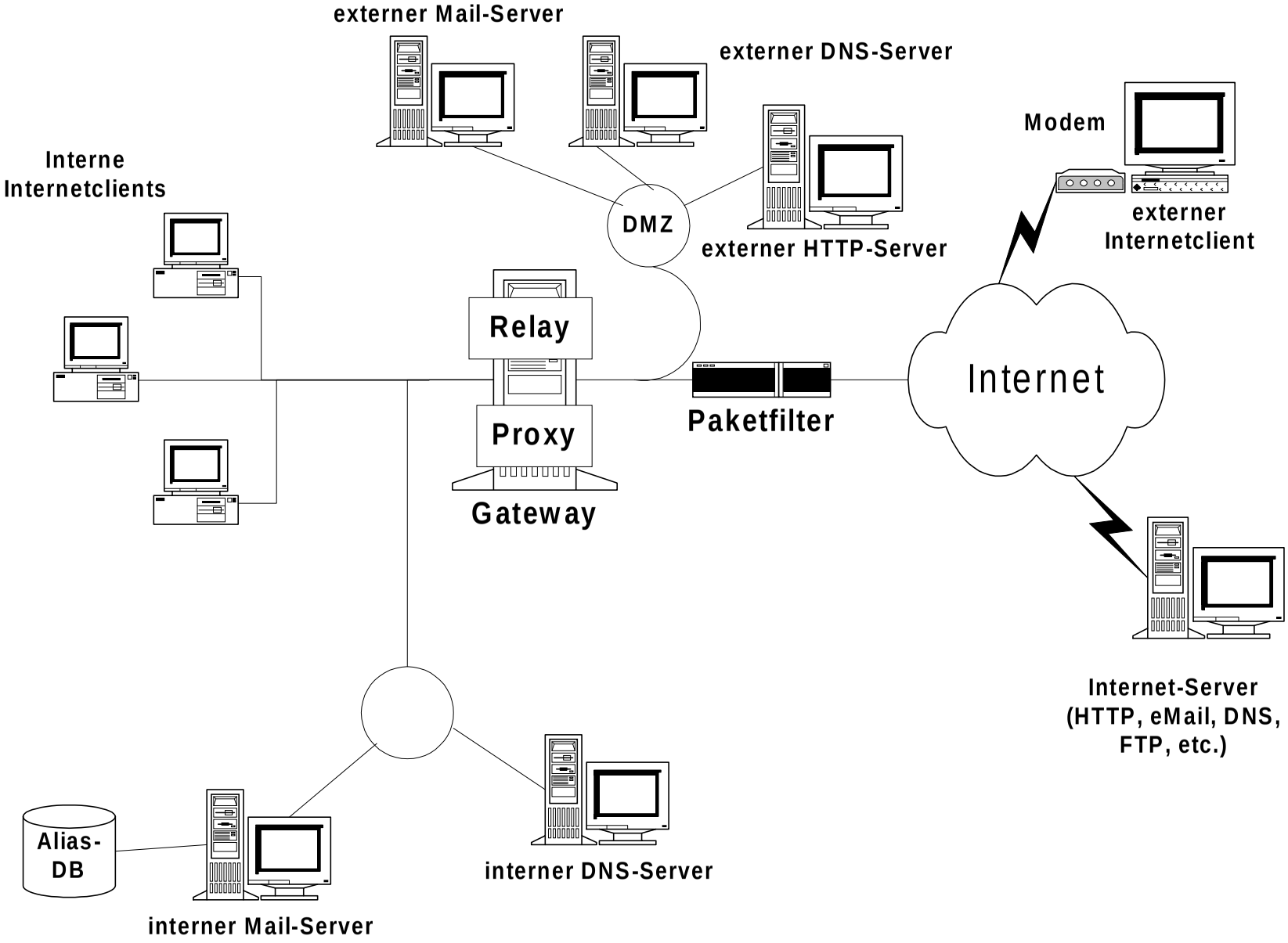
SYN-Flooding / TCP-Verbindungsaufbau



Schutz offener Systeme: Firewalls

- Schutz des Unternehmensnetzes vor Angriffen aus dem Internet
- Zwei verschiedene Konzepte
  - Paketfilter
    - performant
    - in vielen Routern bereits integriert
    - nur beschränkter Schutz
  - Proxy Gateways
    - potentieller Flaschenhals
    - Beschaffung neuer Soft- und Hardware notwendig
    - weitreichender Schutz
- System darf von außen nur über Firewall zugänglich sein

Schutz mit Firewalls - ein Beispiel



Dienste und ihre Sicherheitsprobleme

- Dienste
  - DNS
  - Remote Access
  - Terminalbetrieb
  - eMail
  - FTP
  - **WWW**
  - ...
- **Häufigstes Problem:** Übertragung von vertraulichen Daten im Klartext

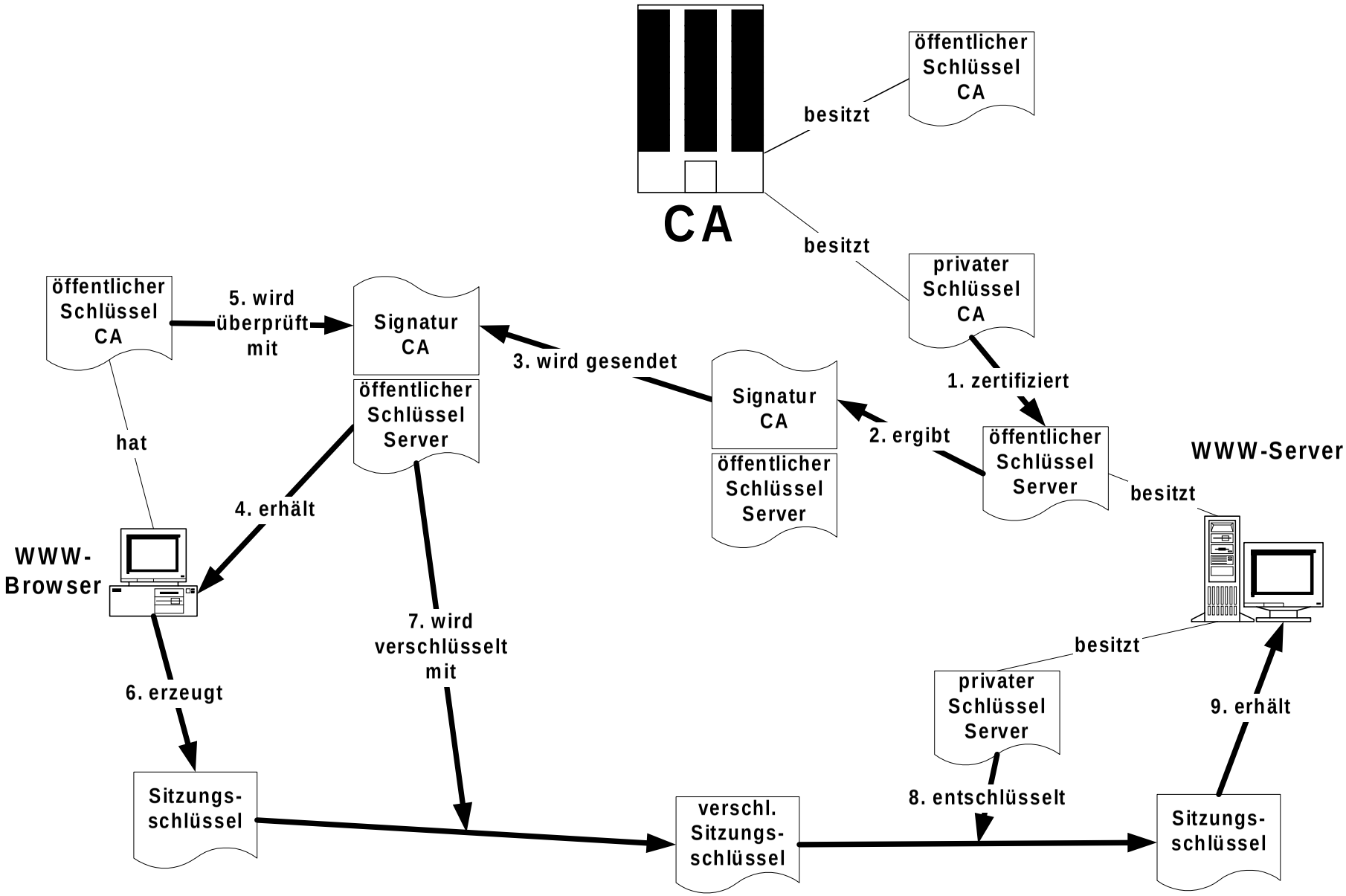
WWW

- Probleme
  1. Übermittlung vertraulicher Daten im Klartext
  2. Erstellung detaillierter Kundenprofile
  3. Aktive Inhalte (z.B. Java)
- Gegenmaßnahmen
  1. Verwendung kryptographischer Protokolle
  2. Gesetzliche Regelungen / Deaktivierung von „Cookies“
  3. Implementierung von Sicherheitskonzepten / Deaktivierung aktiver Inhalte

SSL - Secure Socket Layer

- Verschlüsselte Übertragung von Daten über das Internet
- Verwendung zertifizierter asymm. Schlüssel (= Schlüssel mit einer Signatur) zur Authentifizierung und zur Vereinbarung eines symm. Sitzungsschlüssels
- Bei ausreichender Schlüssellänge sicheres Verfahren
- Sehr häufig im WWW verwendet
- Prinzipiell für jede Übertragung über TCP/IP geeignet
- Ähnliches Verfahren: S-HTTP

SSL: Vereinbarung des Sitzungsschlüssels

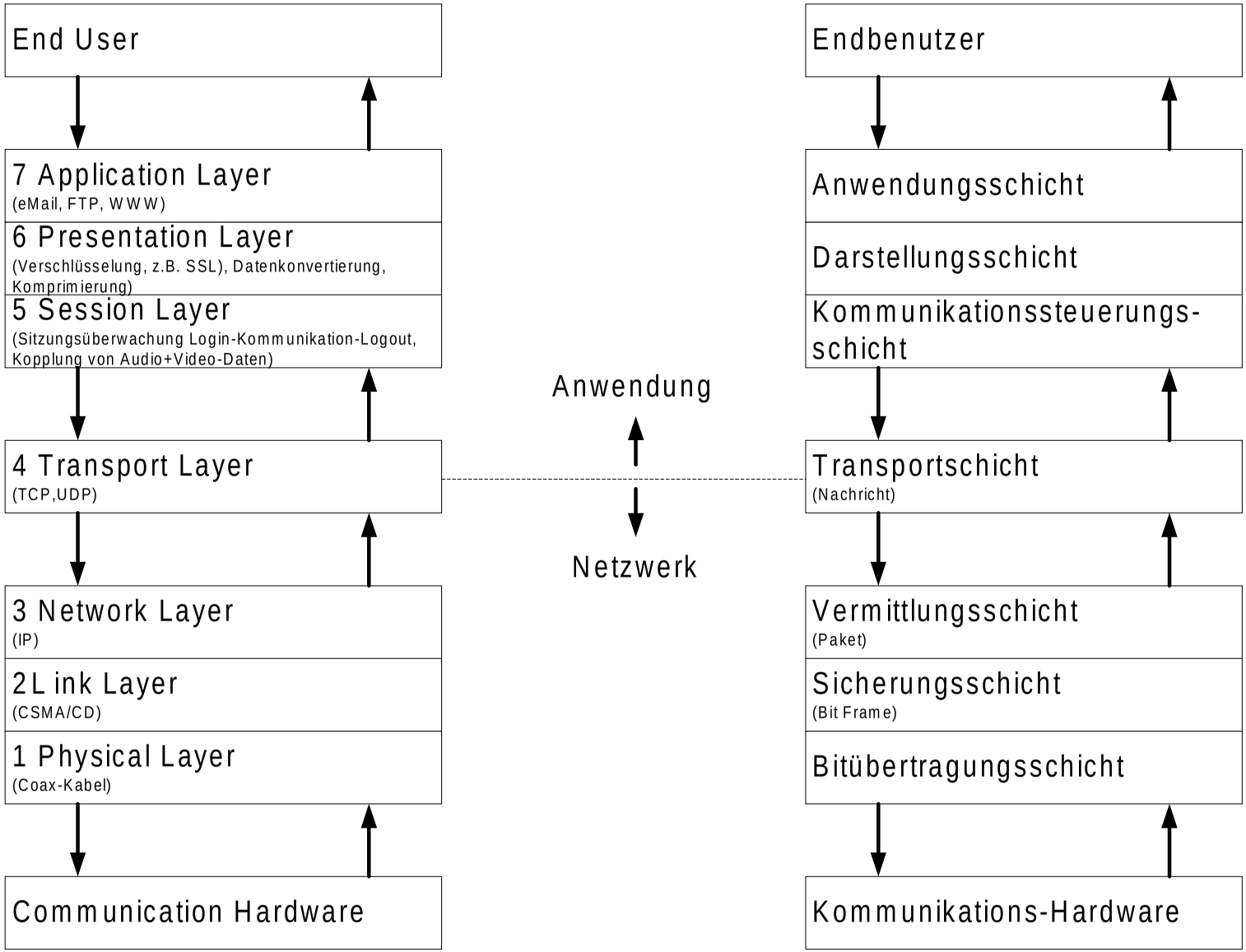


Zusammenfassung & Ausblick

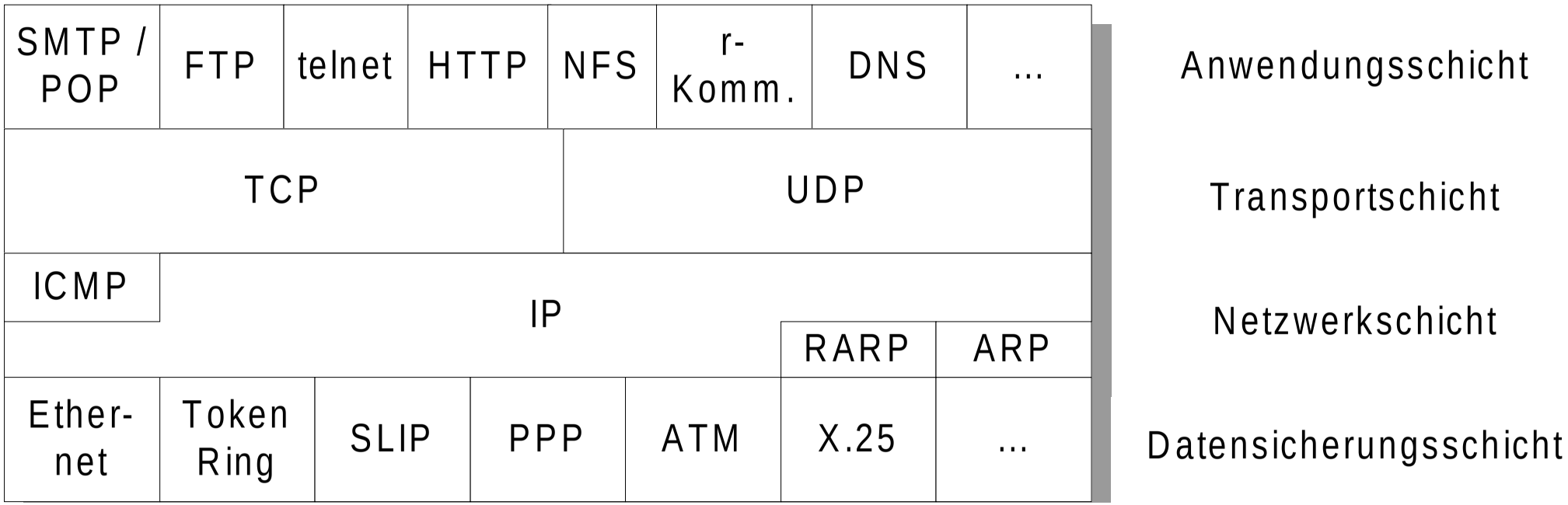
- Vorstellung organisatorischer Konzepte
- Grober Überblick über kryptographische Verfahren
- Probleme mit Internetprotokollen
- Firewalls als Schutz von Netzwerken
- Sicherheitsprobleme von Diensten am Beispiel des WWW

- Notwendigkeit, für die Sicherheitsproblematik des Internets ein breites Bewußtsein zu schaffen
- Neue Protokolle müssen schon unter Sicherheitsaspekten entworfen werden (IPv6)

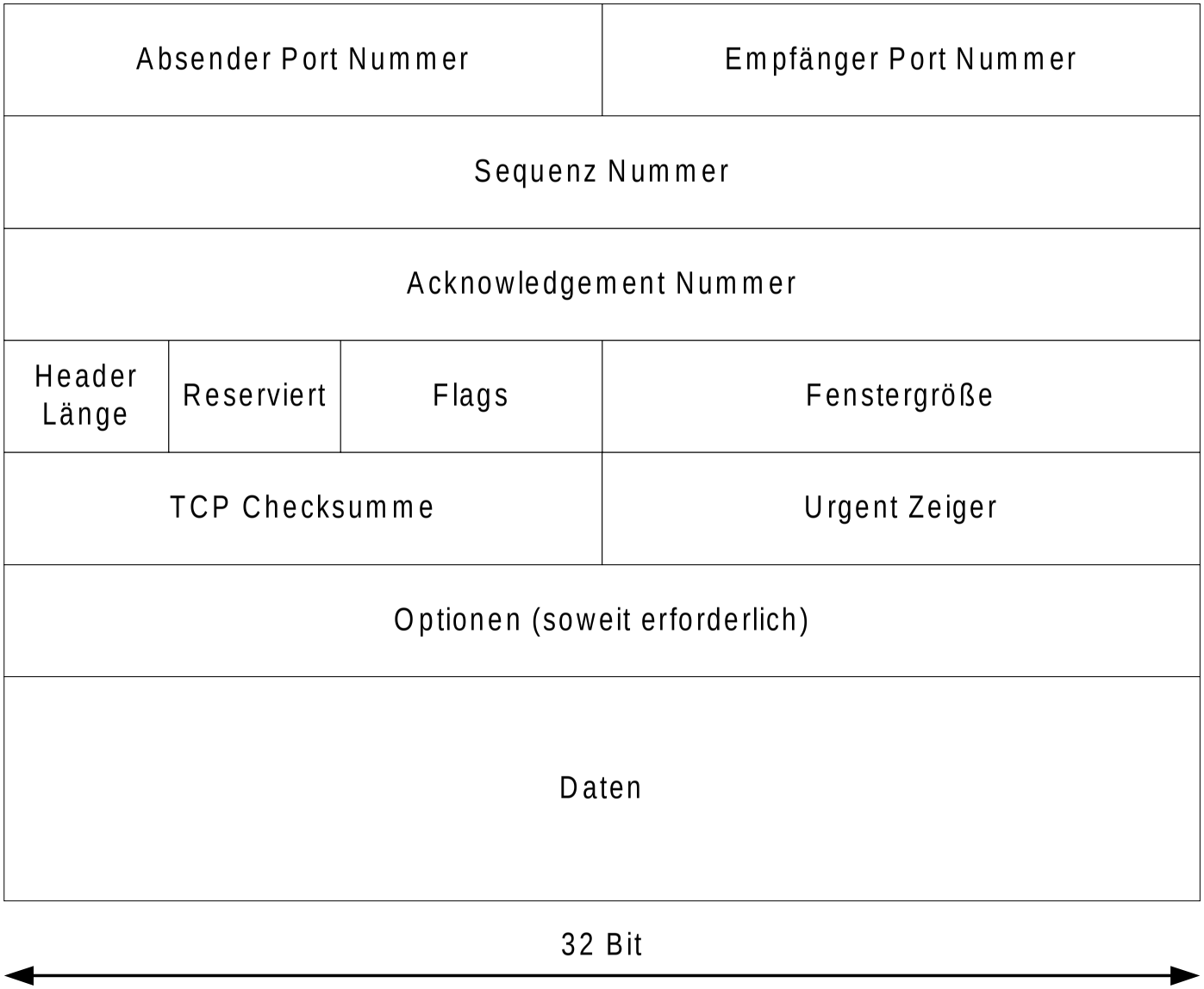
ISO-OSI-Referenzmodell



Funktionale Schichten und Protokolle des Internet



TCP-Paket


Absender Port Nummer
Empfänger Port Nummer
Sequenz Nummer
Acknowledgement Nummer
Header Länge
Reserviert
Flags
Fenstergröße
TCP Checksumme
Urgent Zeiger
Optionen (soweit erforderlich)
Daten
32 Bit