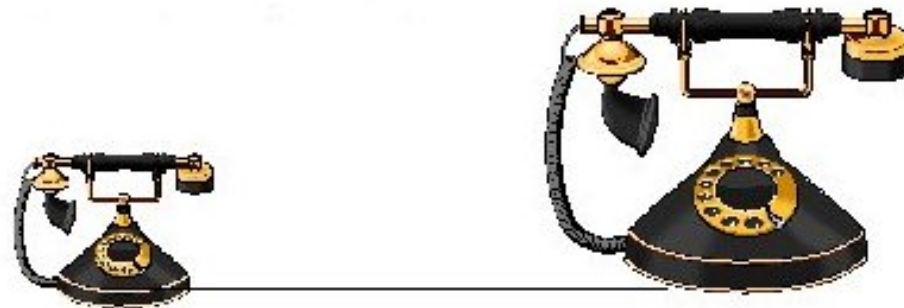


VoIP

Grundlagen und Risiken



Prof. Dr. Richard Sethmann

**Hochschule Bremen
Fakultät Elektrotechnik und Informatik**



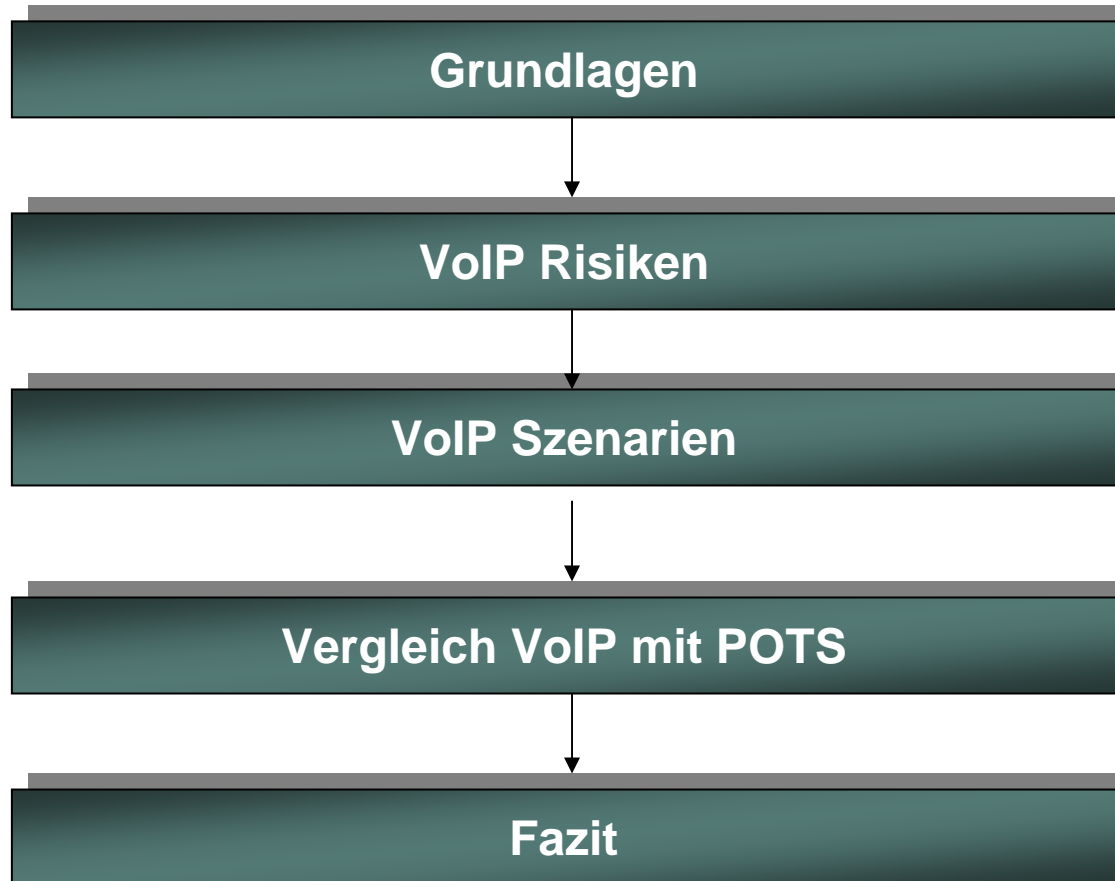
Zu meiner Person

Informatik-Professor an der Hochschule Bremen

Aktuelle Lehrgebiete: Rechnernetze
Informationssicherheit

Aktuelle Forschung: Rechnernetze
Mobile Netze
Informationssicherheit

Funktionen: Leiter des Instituts für Informatik und Automation (IIA)
Leiter des Netzlabor
Prüfungsausschussvorsitzender Medieninformatik
Studiengangsleiter: Dualer Studiengang Informatik



VoIP

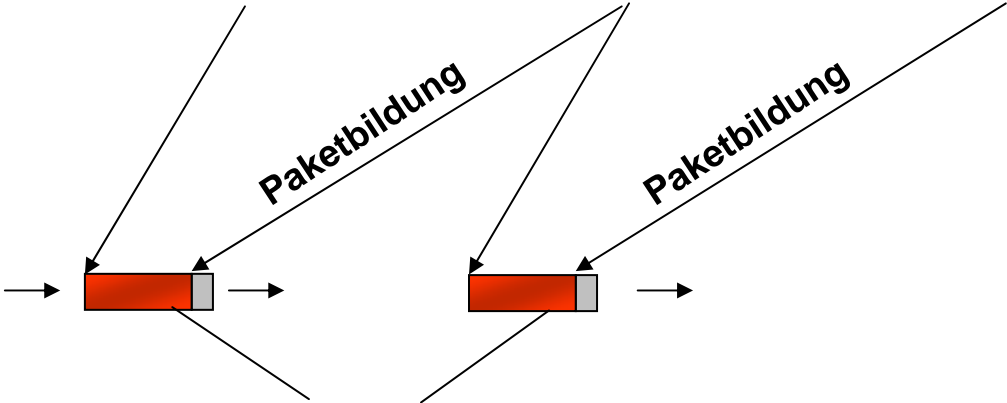
Was ist VoIP im Vergleich zu ISDN?

ISDN Datenstrom

kontinuierlicher Datenstrom auf separater Leitung

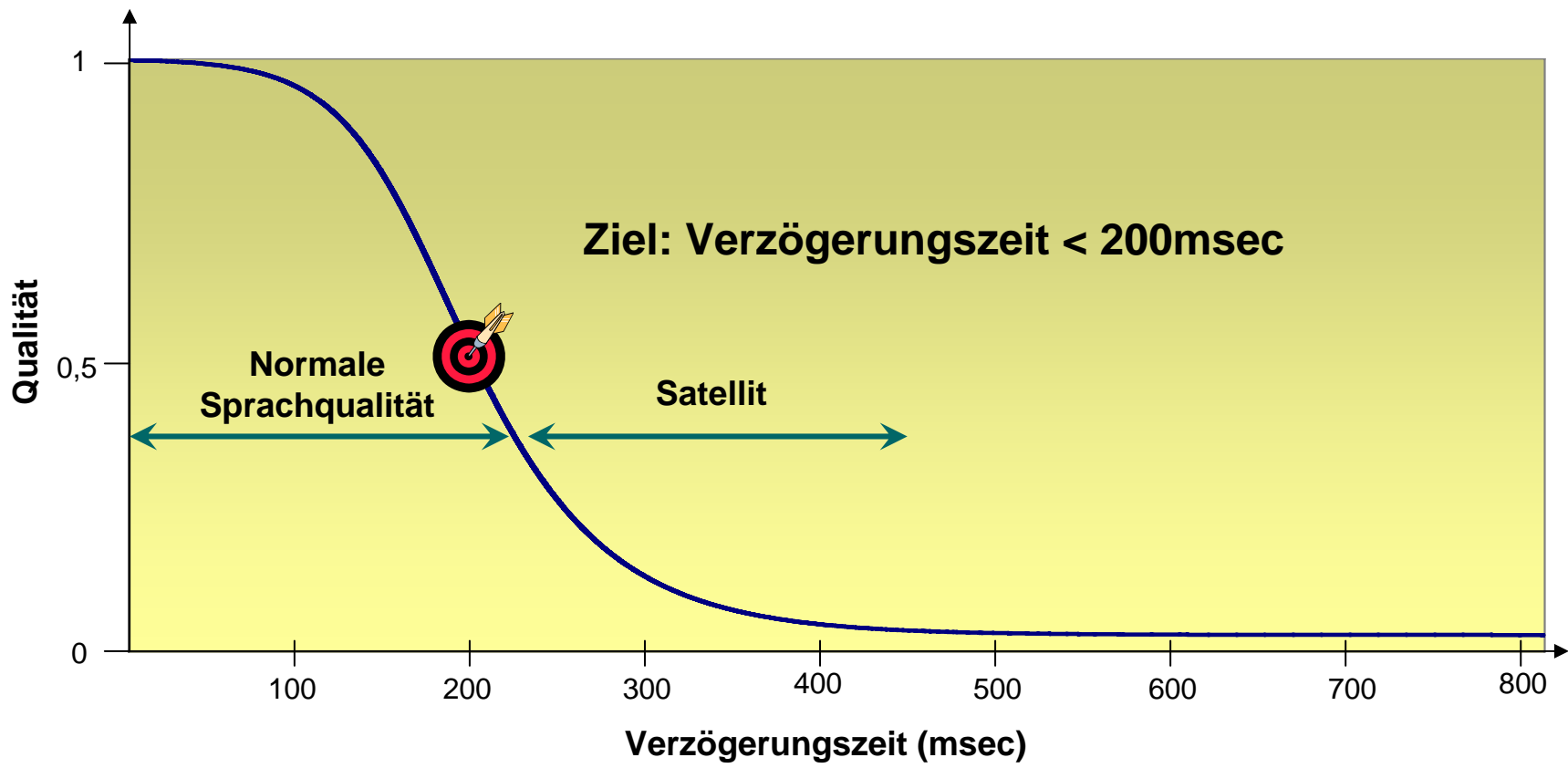
011 110 111 011 100 110 111 010 101 100 011 110 111 →

VoIP Pakete



IP Pakete, die sich mit anderen IP Paketen die Leitung teilen

Qualität der Sprachverbindung in Abhängigkeit der Verzögerungszeit





Eigenschaften von VoIP Paketen

- **Zeitverzögerung**
 - bedingt durch Paketbildung
 - bedingt durch unterschiedliche Wege im Netz
 - bedingt durch begrenzte Datenraten (Datenstau im Router oder Switch)

Abhilfe:

- garantierte und definierte Verzögerungszeit, realisierbar über QoS Mechanismen (Prioritäten gesteuert)
- garantierte Bandbreite für jeden VoIP Sprachkanal (QoS)



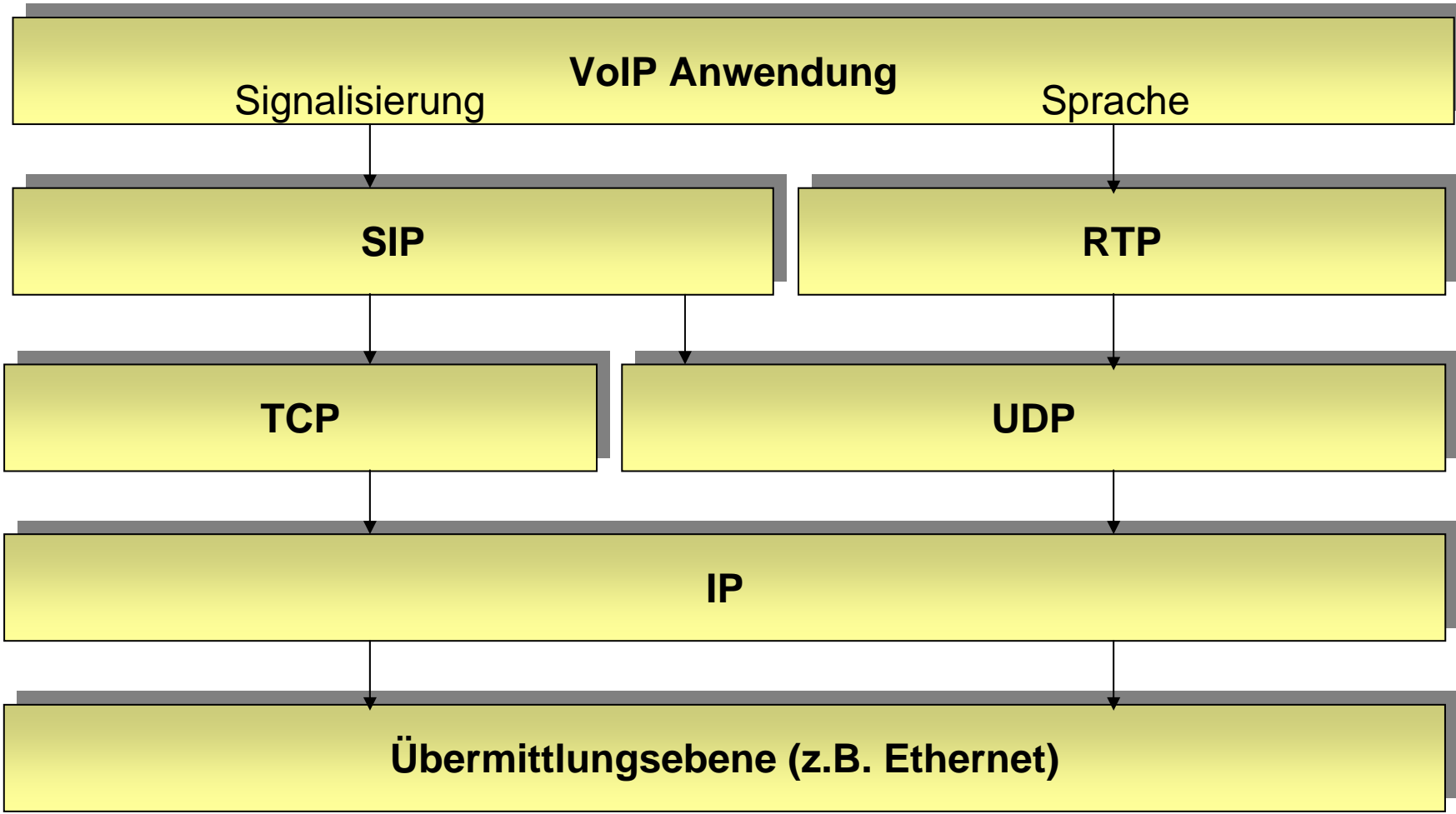
Audio Codecs (Codierer und Decodierer)

Datentransferraten der gängigsten Audio-Codecs:

G.711	64	kbit/s (keine Komprimierung)
G.722	56	kbit/s
G.726	32	kbit/s
G.728	16	kbit/s
G.729	8	kbit/s
G.723.1.a	6,4	kbit/s
G.723.1.b	5,3	kbit/s



VoIP Protokollstack



- Signalisierung
 - SIP (Session Initiation Protocol)
 - Stellt die Verbindung her (wählen)
 - H.323 (auslaufendes Protokoll)
- Datentransport
 - IP / UDP (Internet Protocol / User Datagram Protocol)
 - IP: Adressierung der Teilnehmer über IP-Adressen
 - UDP: Auswahl der Anwendung auf dem Endgerät über Port-Nummern
 - RTP (Real Time Transport Protocol)
 - Transport der VoIP-Pakete
 - Versieht jedes Paket mit einem Zeitstempel

- SIP
 - Signalisierungsdaten werden im Klartext übertragen
 - Abhilfe: Verschlüsselung z.B. über TLS, IPSec mit IKE und S/MIME
- RTP
 - Sprachdaten werden unverschlüsselt übertragen
 - Abhilfe: Verschlüsselung z.B. über Secure- RTP (SRTP)

- Angriffe auf Netzebene leichter möglich als bei ISDN
 - Denial-of-Service (DoS)
 - ARP, IP, UDP Spoofing
 - Man-In-The-Middle Angriffe
 - Syn- oder PING- Flooding
 - Sniffing
 - Replay
 - Etc.
- Angriffe auf Applikationsebene
 - Nichtautorisierte Nutzung (Phreaking)
 - Spam over IP-Telephonie (SPIT)
 - Etc.

- ARP-Spoofing
vortäuschen einer falschen IP- Adresse, um einen Man-In-The-Middle Angriff vorzubereiten
- Man-In-The-Middle Angriff
Angreifer setzt sich zwischen (mindestens) zwei VoIP-Telefonen, um den Sprachverkehr abzuhören
- Werkzeuge
 - Ettercap
 - Cain&Abel
 - Etc.



Maßnahmen gegen Risiken

ISO / OSI Ebene	Gefahren	Gegenmaßnahmen
Anwendung (Layer 5-7)	SPIT, Malware	Digitale Zertifikate, Schlüsselaustausch, STUN, SPIT-Filter, aktuelle Patches, Antivirus, u.w.
Netzebene (Layer 3-4, IP, TCP, UDP)	DoS, Lauschangriffe, Spoofing	Verschlüsselung, starke Authentisierung und Autorisierung, u.w.
Übermittlungsebene (Layer 1-2, z.B. Ethernet)	DoS, Lauschangriffe, Spoofing	Zugangssteuerung (802.1x), VLAN, VPN, MAC-Filterung,

Quelle: VoIP Security, Evren Eren, Kai-Oliver Detken

- **Campus VoIP**
 - Nebenstellenanlage auf IP-Basis
 - IP-Telefone und / oder Softphones
 - Verbindung ins öffentliche Telefonnetz über Gateways
 - Schwer von außen angreifbar, da keine direkte Verbindung zum Internet
- **IP Centrex / Hosted IP**
 - Virtuelle und IP basierte Nebenstellenanlage wird vom Provider über das Internet bereitgestellt
 - IP-Telefone und / oder Softphones im Unternehmen
 - Angriffe können über das Intranet und / oder Internet erfolgen



Vergleich

Herkömmliche Telefonie	VoIP
Oftmals nicht ins CRM integriert	Lässt sich leichter ins CRM integrieren
Telefon-Admin oftmals vom externen Dienstleister	VoIP - Administration wird oftmals vom Netz-Administrator übernommen
Wartung der Telefonanlage oftmals nur selten notwendig	Wartung des Netzes sollte regelmäßig durchgeführt werden
Hohe Verfügbarkeit und Verlässlichkeit	Verfügbarkeit und Verlässlichkeit muss sichergestellt sein durch entsprechende Auslegung des IP Netzes
Angriffe eher selten	Angriffe leichter möglich (Abhören, DoS, SPIT, etc.)

- Sprachqualität sicherstellen über Priorisierung (QoS) und geeigneten Audio Codec (z.B. G.711)
- Hochverfügbarkeit des Netzes sicherstellen
- Zusätzlichen Administrationsaufwand abschätzen
- Geeignete Maßnahmen gegen VoIP Risiken ergreifen, z.B.
 - LAN: Maßnahmen gegen ARP-Spoofing ergreifen
 - LAN und WAN: SIP und RTP-Daten verschlüsseln
- Kostenvergleich durchführen

- Voice over IP - Die Technik, Anatol Badach, 4., überarb. und erw. Aufl. 2009, Hanser-Verlag
- VoIP Security – Konzepte und Lösungen für sichere VoIP-Kommunikation, Evren Eren, Kai-Oliver Detken, 2007, Hanser-Verlag



**Schönen Dank
für die
Aufmerksamkeit!**

