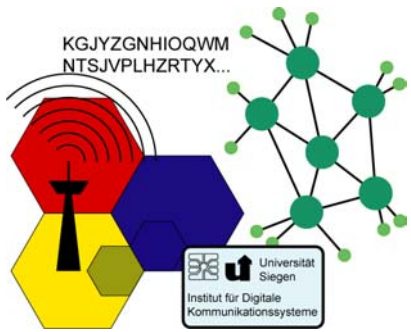
Vertrauliche Videokonferenzen im Internet



Luigi Lo Iacono, Christoph Ruland

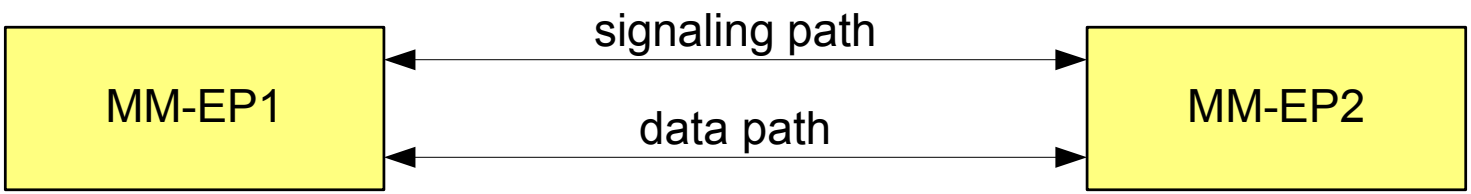
Institut für Digitale Kommunikationssysteme, Universität Siegen

Förderung

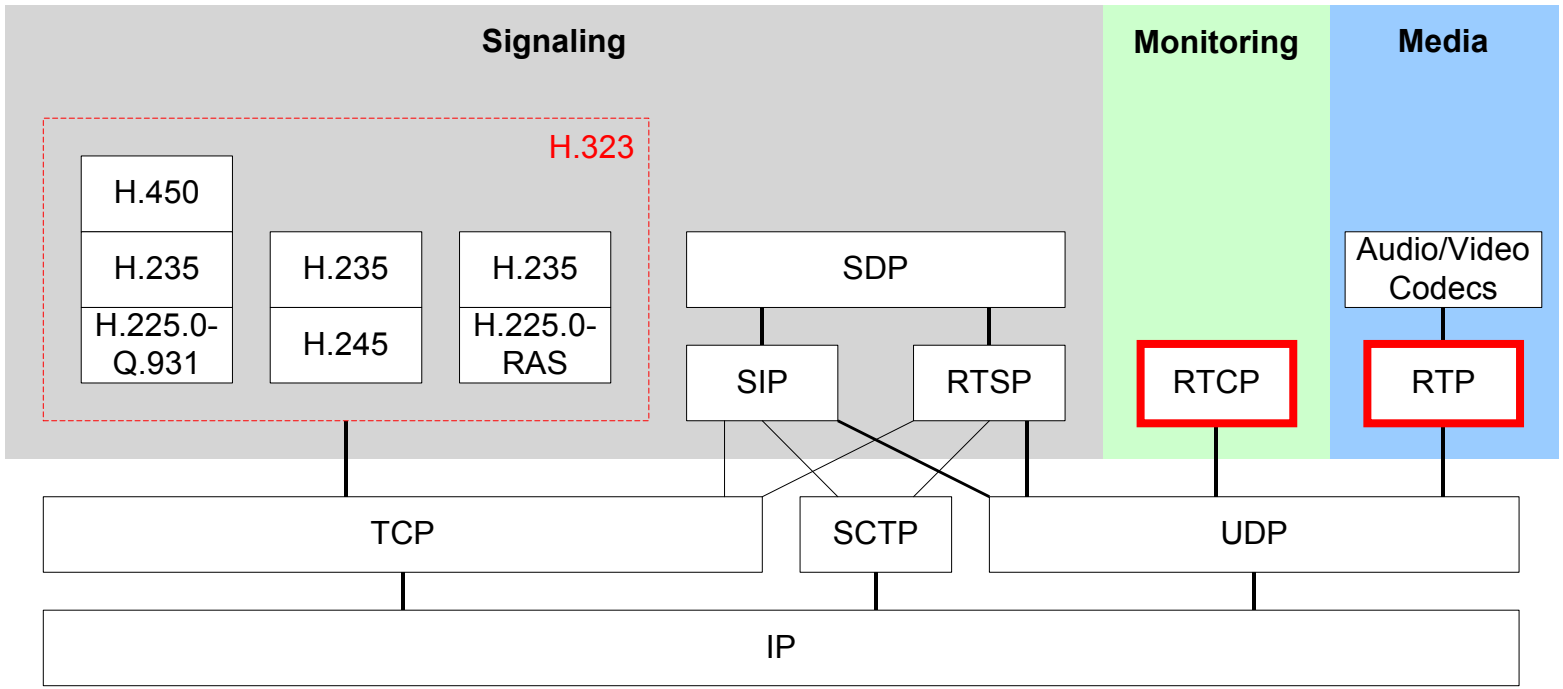
- DFG-Projekt (Ru 600/8-1)
  - Internet Security System für Voice over IP unter Berücksichtigung von Quality of Service (QoS)
  - In Zusammenarbeit mit Soongsil University Seoul (Republik Südkorea)
  - Einarbeitung in
    - Internet QoS: IntServ, RSVP, DiffServ, ToS
    - Multimedia Signalisierung: H.323, SIP, RTSP
    - Multimedia Transport: RTP/RTCP
  - Untersuchungen der verfügbaren QoS im Internet
  - Entwicklung und Implementierung eines sicheren Video-konferenzsystems auf Basis von SRTP

Einführung

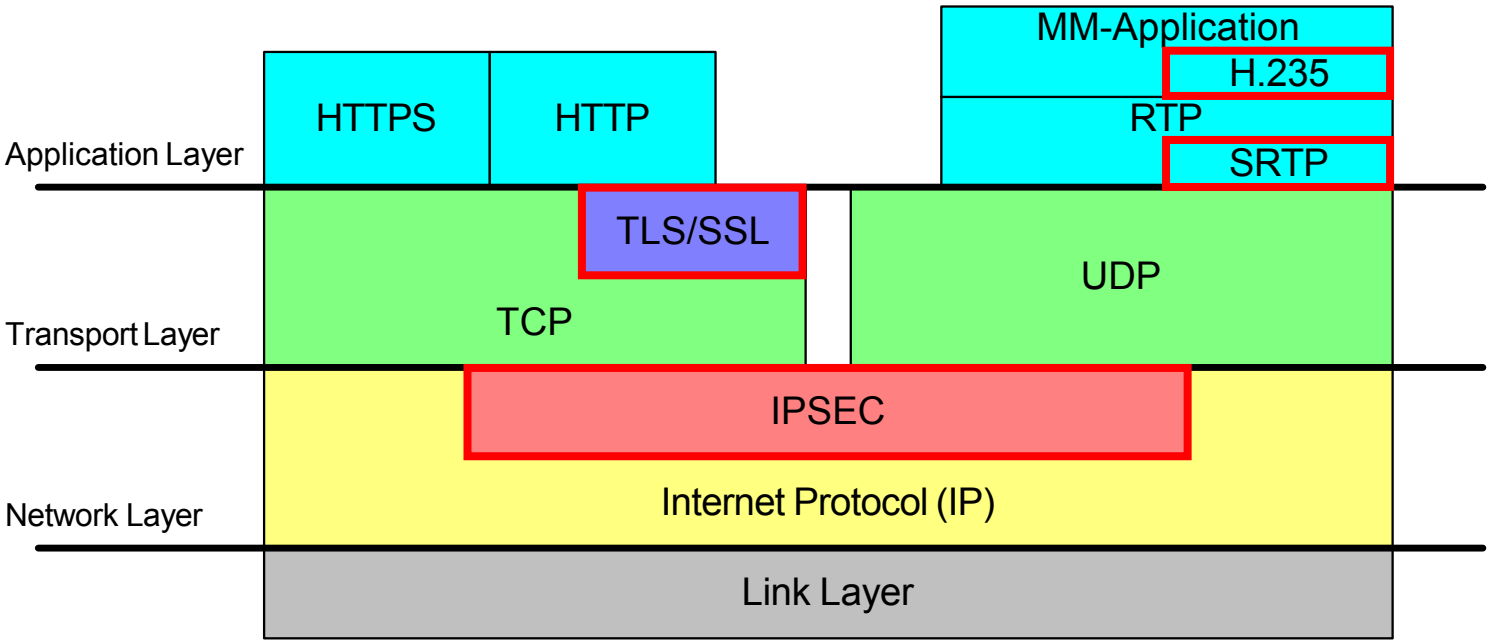
- Was versteht man unter Multimedia-Kommunikation?
  - Gleichzeitige Übertragung von Daten, Sprache und Bildern
  - Kommunikation mit Realzeit-Charakter
  - Zwei separate Übertragungspfade
    - Signalisierung
    - Transport (Synchroner-/Isochroner Übertragungsmodus)



Multimedia Protokollstack



Vertrauliche Multimedia-Kommunikation



IPSec

- IETF Standard (RFC 2401)
- Sicherheitsdienste für IPv4 und IPv6
- Eingebunden im Betriebssystem
- IKE (RFC 2409) zur Initialisierung und Schlüsselaustausch
- Typischer Einsatz: VPNs
  - IPSec im Tunnel Mode

IPSec

- \+ Ermöglicht vertrauliche Multimedia Kommunikation
- – Hohe Datenexpansion
  - Zusätzliche IPSec-Header
  - Padding
- – Fehlerfortpflanzung
  - Abhängig von der verwendeten Betriebsart
  - Auf ein Paket bezogen/begrenzt
- – Probleme bei Ende-zu-Ende Sicherheit
  - IKE ist sehr komplex
  - IPSec und IKE Implementierung auf Small Devices
  - Firewall Filterung
- – Kein Multicast Support

SSL/TLS

- Eingeführt von Netscape Inc. (SSL)
- IETF Standard (TLS, RFC 2246)
- Sicherheitsdienste für TCP Verbindungen
- Weite Verbreitung
  - Insbesondere bei Web-Transaktionen
  - **`https://...`**

SSL/TLS

+ Schlüsselmanagement Protokoll kann verwendet werden
– Basiert auf zuverlässigem Transportprotokoll
  - TCP ungeeignet für synchrone/isochrone Übertragung
– Kein Multicast Support

H.235

Baseline security profile (Annex D)

Voice encryption profile (Annex D, optional)

Signature security profile (Annex E)

Security Services	Call Functions					
	RAS	H.225.0	H.245	RTP		
Authentication	Password HMAC-SHA1-96	Password HMAC-SHA1-96	Password HMAC-SHA1-96			
	Digital signature MD5/SHA1-RSA	Digital signature MD5/SHA1-RSA	Digital signature MD5/SHA1-RSA			
Non-Repudiation	Digital signature MD5/SHA1-RSA	Digital signature MD5/SHA1-RSA	Digital signature MD5/SHA1-RSA			
Integrity	Password HMAC-SHA1-96	Password HMAC-SHA1-96	Password HMAC-SHA1-96			
	Digital signature MD5/SHA1-RSA	Digital signature MD5/SHA1-RSA	Digital signature MD5/SHA1-RSA			
Confidentiality				RC2/CBC 56 bit	DES/CBC 56 bit	3DES/CBC 168 bit
Access Control						
Key Management	Subscription-based password assignment	Subscription-based password assignment	Integrated H.235 session key management (key distribution, key update)			
		Authenticated DH key exchange				
	Certificates	Certificates				

H.235

- \+ Ermöglicht vertrauliche Multimedia Kommunikation
- – Nur verfügbar für H.323-Terminals
  - Keine weite Verbreitung
- – Voice Encryption Profile Optional
- – Fehlende Sicherheitsdienste
  - Keine Nachrichtenauthentikation von RTP-Paketen
  - Keine Sicherheitsdienste für RTCP
- – Datenexpansion
  - Padding
- – Fehlerfortpflanzung
  - Durch Betriebsart der Chiffren (CBC)
  - Auf ein Paket bezogen/begrenzt

Secure RTP

- IETF Internet Draft
  <draft-ietf-avt-srtp-05.txt>
- Sicherheitsdienste (für RTP und RTCP)
  - Vertraulichkeit
  - Nachrichtenauthentizität/Integrität
  - Schutz vor Replay-Attacken
- Design Ziele
  - Hoher Durchsatz
  - Geringe Paket-Expansion
  - Erweiterbarkeit

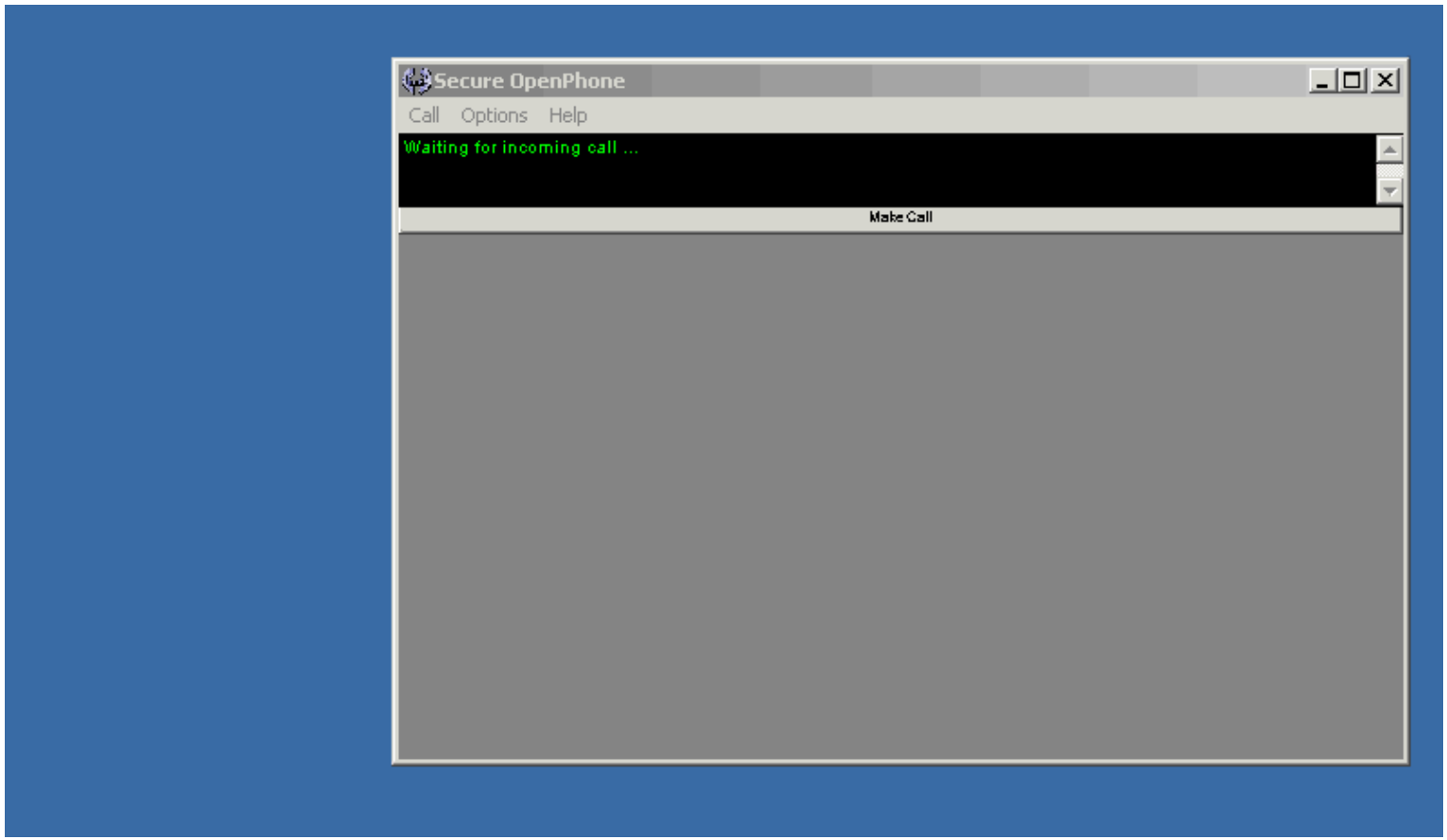
Secure RTP - Vertraulichkeit

- Verschlüsselungsalgorithmen
  - AES 128 Bit Blocksize (Default)
  - Weitere möglich
- Betriebsarten
  - Segmented Integer Counter Mode (SIC) (Default)
  - F8 Mode
  - Weitere möglich

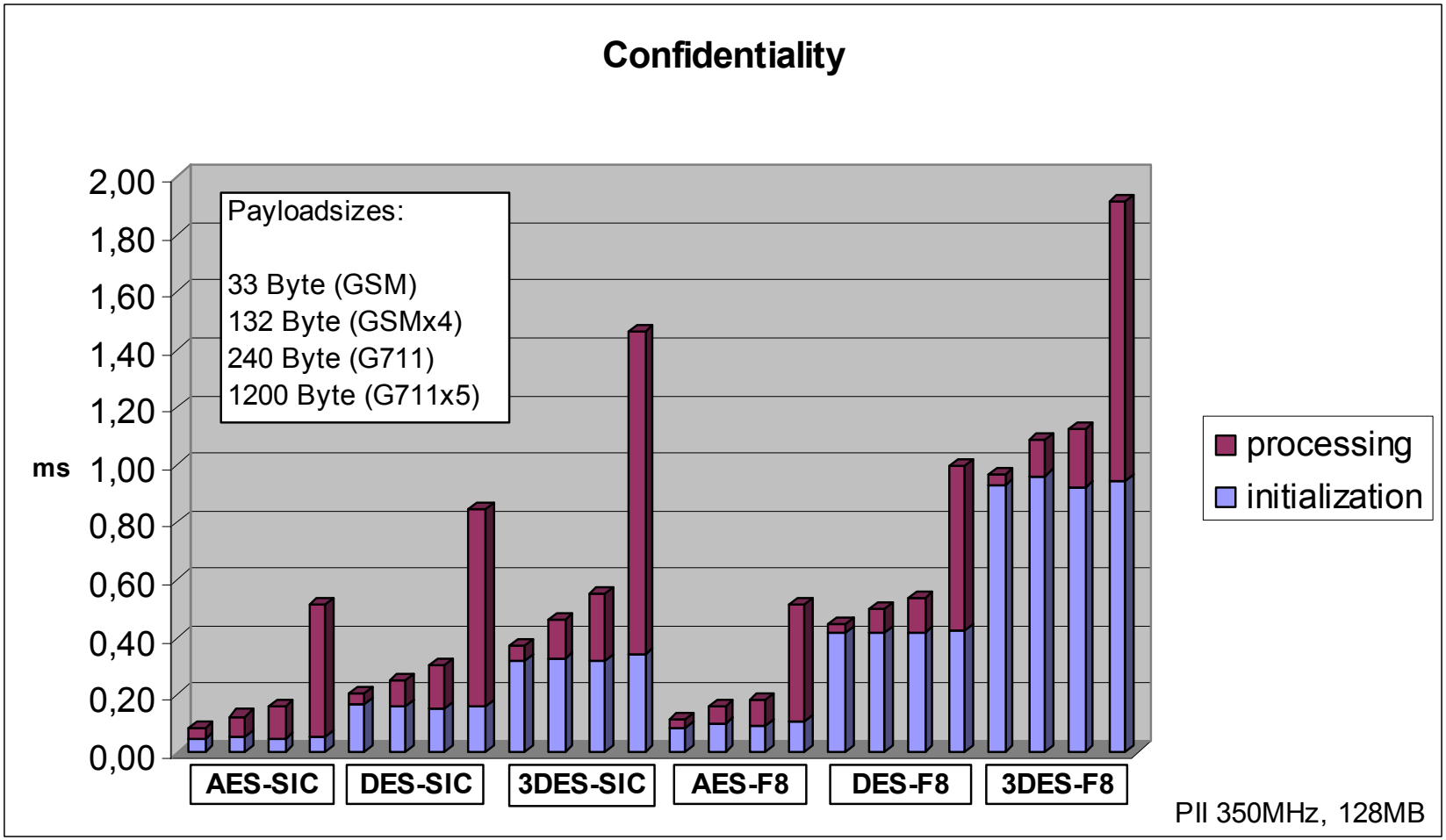
Secure RTP

- \+ Ermöglicht vertrauliche Multimedia Kommunikation
- \+ Geeignet zur Implementierung auf Small Devices
- \+ Kein Schlüsselmanagement spezifiziert
  - Kann abhängig von Applikation gewählt werden
- \+ Multicast Support
- \+ Keine Fehlerfortpflanzung
- – Datenexpansion
  - Nachrichtenauthentikation (MACs)
- – Noch nicht als Standard verabschiedet

Secure OpenPhone



Secure RTP - Messergebnisse



Zusammenfassung

- QoS ist zwingend erforderlich für Internet Multimedia Kommunikation
- IPSec, H.235 und SRTP ermöglichen Vertraulichkeit
- SRTP-Implementierung hat keinen zusätzlichen Einfluss auf die QoS
  - Keine zusätzlichen Ressourcen für Vertraulichkeit
- SRTP vielfältig einsetzbar
  - SIP, RTSP, H.323

Fragen