Sicherheit bei VoIP - Ein Überblick

Christian Louis
christian@kuechenserver.org

29. Dezember 2004

Überblick

- Grundlagen von IP-Telefonie
- Gefahren bei IP-Telefonie
- Standards VoIP-Sicherheit
- Status Quo
- Ausblick

... zunächst ein paar Worte in eigener Sache

- Speaker hat Diplomarbeit über Sicherheit bei VoIP geschrieben
- Dipl.-Inform. (FH) Fachrichtung Telekommunikation @ FH Bonn-Rhein-Sieg
- LUUSA-Mitgründer und dadurch im Dunstkreis des Netzladens unterwegs
- ... bald Hamburger und im IT-Security-Bereich in Lohn und Brot

Grundlagen IP-Telefonie

- Kommunikation über IP
- Nutzung von UDP und TCP für Signalisierung, UDP für Media
- darüber dann unterschiedliche Anwendungsprotokolle

Grundlagen IP-Telefonie

- Signalisierung SIP, H.323, IAX...
- Mediendaten getrennt
- Signalisierung teilweise über Proxies geleitet
- Media-Stream direkt

Gefahren bei IP-Telefonie

- Vertraulichkeit
- Integrität / Authentizität
- Anonymität (mehr dazu später)
- Verfügbarkeit hier mal nicht betrachtet...

Vertraulichkeit

- Meine Gespräche können nicht mitgehört werden
- ... auch nicht von meinem Provider oder Strafverfolgungsbehörden
- Meine Gesprächspartner können nicht ermittelt werden
- ... zumindest nicht von Dritten

Integrität

- das, was ich sage, kann nicht verändert werden
- die Authentizität des Anrufers wird übermittelt
- ... diese kann auch nicht manipuliert werden

Anonymität

- Anrufer können meine Identität nicht ermitteln
- Verbindungsdaten können nicht ermittelt werden
- Das Ziel meiner Anrufe ist nicht herauszufinden
- Randbemerkung: rein techologische Sicht, rechtliche Lage hier nicht betrachtet

Angriffe

- Pakete können fast überall mitgelesen werden
- Informationen werden im Klartext übertragen
- im LAN Angriffe über ARP, DHCP....
- Kann man dem Internet vertrauen?
- ... keine feste Wegelenkung, abschnittsweise Verantwortung

Angriffsbeispiel

- Szenario: LAN, SIP-Client, bspw. Sipgate
- per ettercap ARP-Spoofing durchführen
- Switch so auch kein Problem
- Pakete umleiten und so mitsniffen
- Verbindungsinformationen in SIP-Paketen
- Gespräch als RTP-Pakete

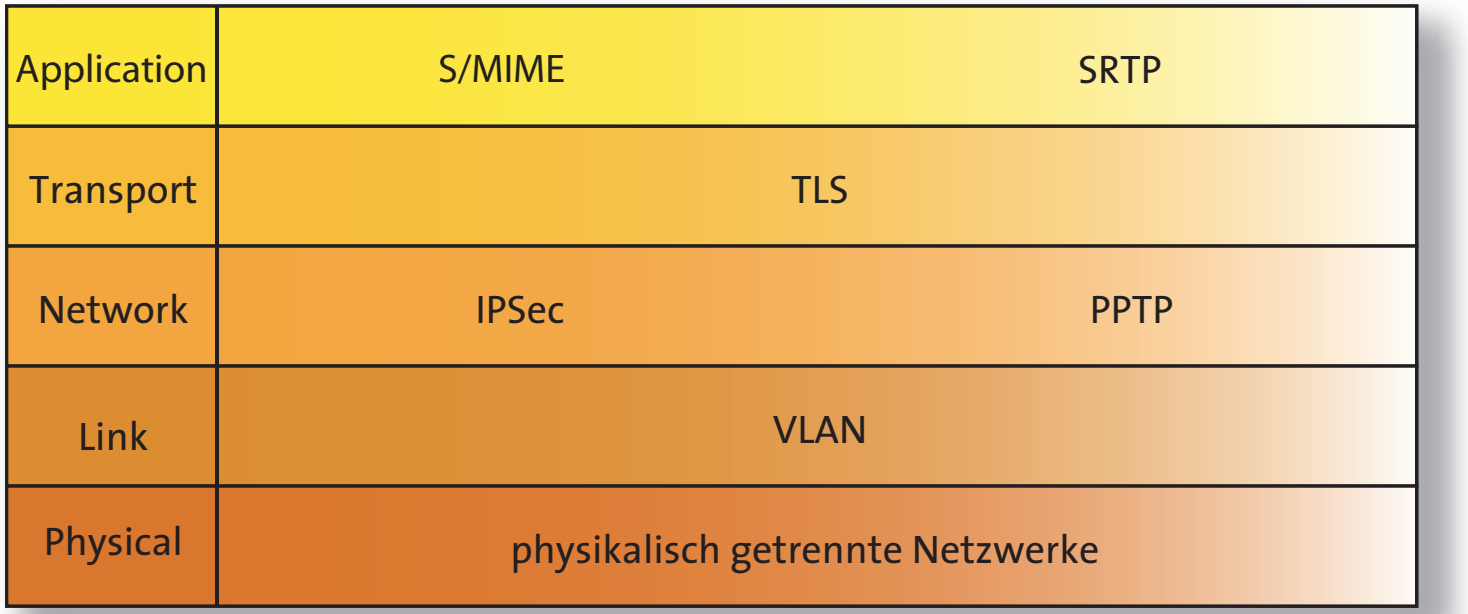
Angriffsbeispiel

- Wir haben nun die Pakete
- Ethereal macht die Auswertung automatisch
- erkennt RTP-Streams aus Signalisierung
- kann Payload .au-kodiert direkt exportieren
- ... war das nun schwierig?

Standards VoIP-Sicherheit

- Bewährtes: IPSec, VPN allgemein, TLS
- Spezielles: SRTP, H.235, Secure SIP
- Exotisches: SCCP, Skype

Sicherheitsmaßnahmen im Überblick



Maßnahmen nach Nerzwerkschichten

VPN

- sternförmige Struktur
- Vorab-Konfiguration
- daher im Bereich Internet-Telefonie nicht ideal
- Ad-Hoc-Aufbau der Verbindung ohne Konfiguration noch nicht Realität

TLS, H.235, Secure SIP

- bewährter Standard
- bei Zertifikaten und Prüfung relativ sicher
- Problem: schafft nur Hop-to-Hop - Verschlüsselung
- Ziel: Ende-zu-Ende

SRTP

- Verschlüsselung des Media Stream
- symmetrisches Verfahren auf Basis von z.B. AES
- Austausch des Sitzungsschlüssels
- bietet auch Authentizität

S/MIME

- SIP spezifiziert Verschlüsselung der Verbindungsinformationen auf Anwendungsebene per S/MIME
- Schlüsselaustausch Ende-zu-Ende möglich
- In Kombination mit SRTP der Weg der Wahl
- PKI - später

SCCP, Skype

- Kein Standard
- Skype nicht einmal offengelegt
- Daher nicht zu akzeptieren, auch wenn Skype fast wie Apple ist
- ... „es funktioniert einfach“

Status Quo

- Hard-/Softphones
- Provider
- IP-TK-Anlagen

Hard-/Softphones

- bei Hardphones nur wenige Produkte: snom, Cisco, Avaya
- Softphones: inige freie und kommerzielle Implementationen für SIP, H.323, IAX, SCCP....
- mir nur eine freie Implementation mit Sicherheitsfunktionen bekannt: minisip
- Skype unterstützt Verschlüsselung - aber closed source und keine Standards

Provider

- alle mir bekannten Provider unterstützen noch keine Sicherheitsfunktionen
- TLS und SRTP sollten ASAP implementiert werden
- jedoch eigener Entwicklungsaufwand, da Open Source Produkte diese Funktionalität noch nicht bieten

IP-TK-Anlagen

- Cisco (Entwickler von SRTP) haben Lösungen im Programm, jedoch eigenen Standard
- Asterisk bietet noch keine Unterstützung für SRTP und Co.
- Siemens hat H.235 entwickelt
- Avaya bietet Support und Standards

Ausblick

- PKI im Bereich VoIP
- SPIT
- Mobilität der Nutzer
- Anonymität

PKI bei VoIP

- Wer zertifiziert was?
- Web of Trust vs. CAs
- ggf. Recycling von S/MIME - E-Mail-Zertifikaten
- Schlüsselverteilung
- ggf. in Verbindung mit ENUM im DNS sinnvoll

Anonymität

- Media-Stream meist direkt
- daher IP-Adresse des Anrufers herauszufinden
- Anonymous Remailer übernehmen?
- Echtzeitproblematik
- neue Entwicklungen mit Media-Proxies notwendig

Fazit

- Es exisiteren brauchbare Lösungen in der Theorie
- sowohl Produkte als auch Provider müssen diese nur noch umsetzen
- PKI größtes Problem bei der Implementierung
- Anonymität noch Forschungsgebiet

Vielen Dank

Fragen?