Hochschule Bremen Workshop 06

VoIP- Sicherheit:

State-of-the-art, Sicherheitsstandards und Lösungen

Dr.-Ing. Kai-Oliver Detken
Private URL: http://www.detken.net
Business URL: http://www.decoit.de

Consultancy & Internet Technologies

Portfolio der DECOIT GmbH

- **Consulting** zur Identifizierung der Probleme und Angebot einer Lösung aus einem Lastenheft für die effektive Umsetzung des Projekts (z.B. im Bereich Security, VoIP)
- **Systemmanagement** zur Umsetzung und Betreuung der erarbeiteten Lösung
- Kundenorientierte **Workshops, Coaching, Schulungen** zur Projektvorbereitung und -begleitung
- Nationale und internationale **Förderprojekte** auf Basis neuer Technologien, um neues Know-how aufzubauen oder Fördermöglichkeiten aufzuzeigen
- **Technologie- und Markttrends**, um strategische Entscheidungen für und mit dem Kunden vor einer Projektrealisierung treffen zu können
- **Software-Entwicklung** zur Anpassung von Schnittstellen und Internet-Projekten
- Schaffung innovativer **Produkte**

Consultancy & Internet Technologies

Inhalte

- Einführung
- Technische Randbedingungen
- Welche Sicherheitsstandards gibt es?
- Welche gesetzlichen Einschränkungen gibt es?
- Herstellerlösungen
- Offene Probleme

Historie

- 1963: Halbautomatischer Telefondienst zwischen Deutschland und den USA
- 1980: Beschreibung des Internet Protocol (IP) in RFC 791
- 1989: Einführung von ISDN
- 1992: Einführung des Mobilfunknetzes GSM
- 1995: Ein MS-Windows-Programm von dem israelischen Unternehmen Vocaltec ermöglicht Internet-Telefonie im Halbduplexbetrieb
- 1996: Beschreibung des RTP-Protokolls
- 1998: Erstmalige Verabschiedung des Standards H.323
- 1999: Beschreibung des SIP-Protokolls
- 2002: SIP-Erweiterungen und Interoperabilität ISDN-SIP

Voice-over-IP (VoIP)

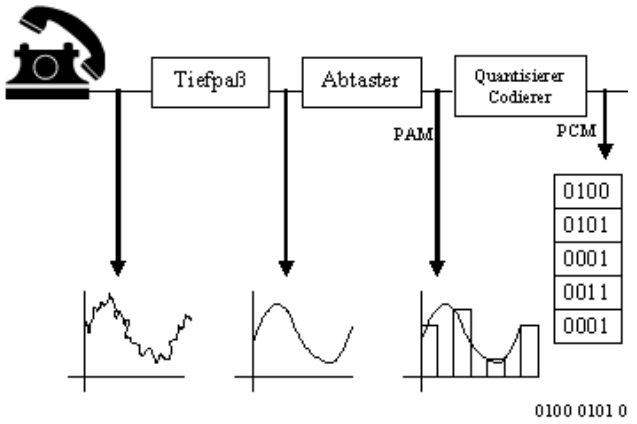
- Sprachdaten, die über ein IP-basiertes Datennetz transportiert werden
- Dabei sind Echtzeitdaten im Weitverkehrsumfeld gemeint
- VoIP hängt in seiner Qualität stark von den Begebenheiten der Internet-Protokolle ab
- VoIP kann dabei sehr unterschiedlich, stark anhängig vom Hersteller, realisiert werden

IP-Telefonie (IPT)

- IP-Telefonie beschränkt sich auf den lokalen Bereich und meint vornehmlich den Einsatz von IP-Endgeräten zur VoIP-Kommunikation
- Mittels VoIP ist die Anbindung an bestehende TK-Netze möglich
- Endgeräte für IP-Telephonie sind mannigfaltig am Markt vorhanden
- Software-basierte Lösungen sind neben Hardware-Geräten verfügbar (u.a. über die TAPI-Schnittstelle)

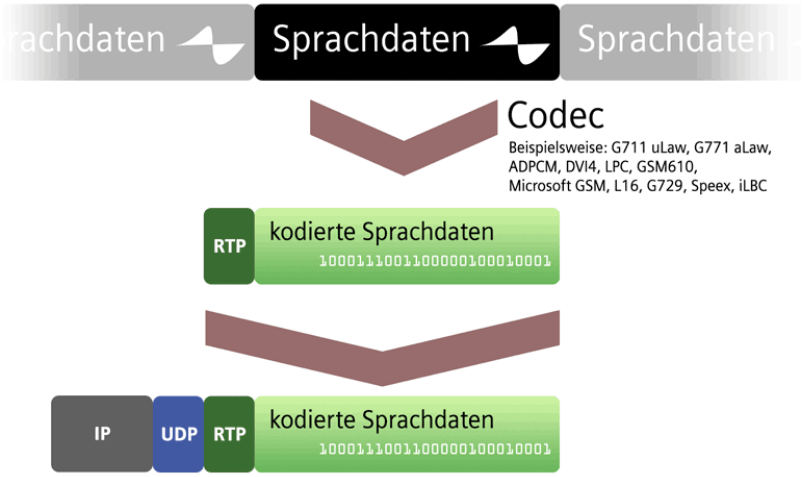
Technische Daten (1)

- Anlog-Digitalwandlung
  - Die analogen Signale werden durch einen A/D-Wandler in ein digitales Format überführt und über Codecs in entsprechende Audio-Binärformate gewandelt
  - Je nach verwendetem Codec können die Daten dabei unterschiedlich stark komprimiert werden
  - Die meisten Codecs benutzen dabei ein Verfahren bei dem für das menschliche Gehör unwichtige Informationen weggelassen werden
  - Das verkleinert die Datenmenge und verringert so die zur Übertragung benötigte Bandbreite
  - Werden allerdings zu viele Informationen weggelassen, leidet auch die Sprachqualität!



Technische Daten (2)

- Datentransport
  - Findet über das Real-Time Transport Protocol (RTP) statt
  - Gesteuert wird der Datenstrom durch das Real-Time Transport Control Protocol (RTCP)
  - UDP kommt über RTP zum Einsatz da es ein minimales, verbindungsloses Netzwerkprotokoll ist, das nicht auf Zuverlässigkeit ausgelegt wurde
  - Ein gewisser Verlust an Daten auf dem Verbindungsweg wird deshalb akzeptiert, da die Geschwindigkeit ein entscheidender Funktionsfaktor bei der VoIP ist



Technische Daten (2)

- Übertragungsqualität
  - Da das Internet in seiner heutigen Form keine gesicherte Übertragungsqualität zwischen Teilnehmern garantiert, kann es durchaus zu Übertragungsverlusten und Aussetzern kommen, sodass die Sprachqualität nicht der von herkömmlichen Telefonnetzen entspricht
  - Eine Priorisierung der Sprachpakete ist sinnvoll. Das heute im Internet verwendete Protokoll IPv4 bietet die Priorisierung zwar, jedoch wird sie von den Routern im Internet in der Regel nicht beachtet
  - Sorgfältig geplante und konfigurierte IP-Netze können heute eine gewisse Quality-of-Service (QoS) gewährleisten

Technische Daten (3)

- Übertragungsprobleme
  - **Laufzeit:** grundsätzliche Verzögerungszeit (150 ms sind noch tolerierbar)
  - **Jitter:** Als Jitter bezeichnet man die zeitliche Schwankung zwischen dem Empfang von zwei Datenpaketen. Um große zeitliche Schwankungen zu kompensieren werden sog. Jitter-Buffer eingesetzt
  - **Paketverlust:** Von Paketverlust spricht man, wenn gesendete Datenpakete den Empfänger nicht oder nicht in der richtigen Reihenfolge erreichen und verworfen werden
  - **Ausfallsicherheit:** Die Ausfallsicherheit ist im Internet derzeit so hoch wie bei herkömmlichen Telefonnetzen

Signalisierungsprotokolle

- SIP – Session Initiation Protocol, IETF RFC 3261
- H.323 – Packet-based multimedia communications systems, ein ITU-T-Standard
- IAX – Inter-Asterisk eXchange protocol
- ISDN over IP – ISDN/CAPI-basierendes Protokoll
- MGCP und MeGaCo – Media Gateway Control Protocol H.248, gemeinsame Spezifikation von ITU-T und IETF
- MiNET – von Mitel
- Skinny Client Control Protocol – von Cisco

Rahmenbedingungen und gesetzliche Vorschriften

- Die gesetzlichen und regulatorischen Rahmenbestimmungen in der Telekommunikation in Deutschland werden maßgeblich durch das Telekommunikationsgesetz (TKG96) vorgegeben
- Nicht abschließend geklärt ist, inwieweit VoIP-Dienste als öffentlich zugängliche Telefondienste aufzufassen sind
- In einem Eckpunktepapier vom 09.09.2005 hat die Bundesnetzagentur festgelegt, dass VoIP-Dienste mittelfristig die selben Kriterien erfüllen müssen wie traditionelle Dienste
- Dies hat unmittelbare Auswirkungen auf die Anwendbarkeit vieler Regelungen aus dem TKG

Fernmeldegeheimnis und Datenschutz

- Der Anbieter von Telekommunikationsdiensten darf personenbezogene Daten seiner Kunden (Bestands- und Verkehrsdaten) nur in den vorgegebenen Grenzen erheben, verarbeiten und nutzen
- Der Anbieter hat auch sicherzustellen, dass die erhobenen Daten entsprechend gesichert und Dritten nicht zugänglich sind
- Wenn der Arbeitgeber die private Telefon-Nutzung am Arbeitsplatz erlaubt, ist er insoweit auch Anbieter und hat die Regelungen des TKG einzuhalten!

Traditionelle Telefonsicherheit

- **Vertraulichkeit:** Das gesprochene Wort und die Identität des Kommunikationspartners sind nicht zu erkennen
- **Integrität und Authentizität:** Niemand kann sich als der gewünschte Partner ausgeben (+Nummernanzeige)
- **Zurechenbarkeit:** Verfolgung krimineller Anrufe und Kostenkontrolle sind möglich
- **Verfügbarkeit** ist sehr hoch
- **Benutzungssicherheit** ist gegeben, da jede Person ein Telefon ohne Anleitung bedienen kann (Notfall)

Vertraulichkeit der Identität

- Bei Telekommunikation ohnehin beeinträchtigt:
  - Routinemäßige Aufzeichnung (Einzelverbindungsnachweise)
  - Rufnummernanzeige (abschaltbar)
- Abhören
  - Analoge Telefone: absolut trivial
  - ISDN: mehr Aufwand
  - GSM: auf der Luftschnittstelle schwierig, da verschlüsselt
  - Fazit: es ist immer räumliche Nähe erforderlich
  - Ausnahme: staatliche Stellen

Integrität und Authentizität

- Angriffe sind schwierig durchzuführen und relativ leicht aufzudecken
- Praktisch unmöglich bei Menschen, die sich kennen
- Problematischer:
  - Telefon-Banking u.ä.
  - Fax
  - Dial-up-Connections, Fernkonfiguration, Fernabfrage

Zurechenbarkeit

- Publizierte Fälle von 0190/0900-Angriffen
  - Keine Kostenkontrolle
- Identifizierung der „Leitung“
- Anonyme Anrufe möglich (Leistungsmerkmal!)
  - Gegenmittel: Fangschaltung
  - Allerdings: nur das Gerät ist ermittelbar (z.B. Telefonzelle)
- Abwägung mit dem Datenschutz

Verfügbarkeit und Benutungssicherheit

- Ausfallwahrscheinlichkeit $p_{down} < 10^{-5}$ gilt als selbstverständlich
  - Erhöht Kosten signifikant
  - Komplexität reduziert allerdings die Verfügbarkeit
- Unabhängigkeit vom Stromnetz
- Plug&Play (Technik und Benutzerwissen)
  - Einschränkung: Nebenstellenanlagen!
- Wenn es funktioniert, sind kaum Fehlfunktionen zu beklagen

Was ist anders bei VoIP?

- Hier wird Ende-zu-Ende statt zentralisiert eine Verbindung aufgebaut
  - Endgeräte können auch direkt miteinander kommunizieren
  - keine Telekom oder PBX im herkömmlichen Sinne
- Es existiert keine Leitungsidentifikation mehr
- Achtung: Die standardisierte Infrastruktur stellt allerdings ein Sprungbrett für Angreifer dar!

IP-Telefonie

- Nutzung von Internet-Technologien
  - Inhärent abhörgefährdete Umgebung
  - Kein Verlass auf vertrauenswürdige Instanzen
- Einsatz kryptographischer Verfahren
  - Digitale Signaturen, Zertifikate; Cookies
  - Verschlüsselung von Sprache, Signalisierung, ...
- Echte Sicherheit wird ermöglicht Ende-zu-Ende

Vertraulichkeit des Wortes

- Wessen und welche Netze werden durchquert?
  - Weniger Kontrolle über ISPs
  - Illusion des sicheren Intranet
- Ende-zu-Ende Verschlüsselung
  - Austausch von Sitzungsschlüsseln pro Telefonat
  - Sichere Signalisierung notwendig
- Konsequenz: Das Abhören auch für Behörden ist nahezu nicht möglich!

Vertraulichkeit der Identität

- Signalisierungsinformationen schützen
  - H.235
  - SIP Security
- Anonymität
  - Wie CLIR (Calling Line Identification Restriction) über „Gentlement's Agreement"
  - Allerdings gibt es keine klare öffentlich/private Schnittstelle mehr
  - Anonymizer: spezieller Dienst

Integrität, Authentizität

- Denial-of-Service Angriffe
- Anruferauthentisierung
  - H.235: „Shopping-list“ von Mechanismen
  - SIP: End-to-end (S/MIME) versus hop-by-hop
- Telefon-Banking: SSL-ähnliches Szenario (Prüfen des Adresseigentümers)

Zurechenbarkeit

- Fangschaltung
  - Rückverfolgung über IP-Adressen
  - Zukünftig der Einsatz von Cookies o.ä.
- Kostenkontrolle
  - Sicherung der Signalisierung
  - Authentisierung, Autorisierung, Accounting (AAA)

Verfügbarkeit und Benutzersicherheit

- Stromausfall
  - Problem wird gemildert durch Mobiltelefone
  - Fernspeisung von IP-Telefonen durch Ethernet-Technologie möglich (Notstromversorgung für Switches notwendig)
- Software-Bugs durch Einsatz neuer Technologien
- Verfügbarkeit des IP-Netzes ist abhängig von der temporären Netzauslastung

Bedrohungsszenarien VoIP (1)

- **Pharming:** manipulieren laufender Dienste auf anderen Servern. Umleiten von IP-Calls zu anderen Zielen (z.B. Kundengespräche). Dadurch lassen sich Daten sammeln und gezielt Falschinformationen streuen.
- **Phreaking:** Aneignung von Authentifizierungsdaten für den Verbindungsaufbau und die Gebührenberechnung (kostenloses Telefonieren). Der Besitzer des VoIP-Anschlusses bezahlt die Rechnung.
- **Phishing:** es fehlt noch an einem einheitlichen Verfahren zur Identifizierung des Anrufers. Rufnummern können daher gefälscht werden (Vortäuschen von anderen Teilnehmern). Dadurch können vertrauliche Informationen erlangt werden.

Bedrohungsszenarien VoIP (2)

- SPIT: Werbeanrufer können über das Internet kostenlos realisiert werden. Spam-of-IPT (SPIT) ermöglicht automatisches Anrufen mit aufgezeichneten Werbebotschaften. Die Nachricht wird einmal aufgezeichnet und an beliebige Nummern gesendet.
- Clipping: Durch die Anzahl der Datenpakete, die ein Angreifer an einen IP-Anschluss sendet, kann die Sprachqualität stark beeinträchtigt werden (Aussetzer).
- Denial-of-Service (DoS): Ein Angreifer stört den IP-Anschluss so stark, dass kein VoIP mehr möglich ist.
- Voice Bombing: Eine oder mehrere Sprachboxen werden mit einer Vielzahl aufgezeichneter Sprachnachrichten (Voice-Mails) überflutet.

Sicherheitsstandards (1)

- H.235-Standard
  - Sicherheit und Verschlüsselung für H.323 und H.245 basierende Terminals
  - Authentifizierung mittels verschiedener Algorithmen sowie Datenschutz, welcher durch Verschlüsselung, erreicht wird
  - SSL/TLS wird zur Sicherung der H.245- und H.225.0-Kontrollkanäle verwendet
  - Ein H.235-basierter Gatekeeper kann sicherstellen, dass nur vertrauenswürdige Endpunkte Zugang zu den Diensten des Gatekeepers gewährt bekommen
  - Wird langsam in Herstellerlösungen implementiert

Sicherheitsstandards (2)

- SIP Security
  - SIP-over-SSL (SIPS): Verschlüsselung der SIP-Kommunikation
  - Kann teilweise auf bestehende Internet-Security zurückgreifen (IPsec, Proxy-Authentification, SSL/TLS)
  - Secure RTP (SRTP): verschlüsselte Version von RTP zur Chiffrierung der Audiodaten → kompressionsfreundlich!
  - Vorbeugen gegen
    - Fälschen der Rufnummer (Phishing Anrufer)
    - Erschleichen kostenloser Telefonate (Phreaking)
  - Bisher kaum in den Herstellerlösungen implementiert

Sicherheitsstandards (3)

- SIPS-Verschlüsselungsnachteile
  - Zusätzlich erforderliche Rechenleistung
  - Verschlechterung des Overhead-/Payload-Verhältnisses
  - Aushebeln vorhandener IDS-Systeme
- SRTP-Verschlüsselungsvorteile
  - Nur die Gesprächsdaten werden verschlüsselt
  - Header-Informationen bleiben so in ihrem Ursprung erhalten
  - Echtzeitverschlüsslung kann dadurch in Hardware realisiert werden

Zusammenfassung

Consultancy & Internet Technologies

Fazit

- VoIP-Lösungen der Hersteller wurden anfangs komplett ohne Sicherheitsmechanismen ausgestattet
- IP-Telefonielösungen schützen sich durch Firewalls & Co. durch externen Zugriff; deshalb wurden hier auch keine Sicherheitsmechanismen implementiert
- VoIP wird langsam der herkömmlichen Telefonie rechtlich gleichgestellt!
- Dadurch sind alle Hersteller im Zugzwang
- Internet-Telefonie wird heute völlig offen und unverschlüsselt betrieben
- SIP Security muss mehr eingesetzt werden; befindet sich aber noch in der Standardisierung

DECOIT

Vielen Dank für die Aufmerksamkeit

DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
http://www.decoit.de
info@decoit.de

Consultancy & Internet Technologies