# Sicherheit geht vor

## Herausforderungen der Sprachdatenübertragung im IP-Netz

Kai-Oliver Detken

**Im Gegensatz zum herkömmlichen, quasi geschlossenen, Telefonnetz werden Datenströme für Voice over Internet Protocol (VoIP) über das nicht abgesicherte Internet oder über die Datennetze der Unternehmen übertragen. Dies erfolgt im Normalfall völlig ohne Sicherheitsmechanismen, so dass ein Mitschneiden von Gesprächen selbst für Laien relativ einfach möglich sein kann.**

**Hatten die Hersteller von VoIP-Lösungen in der Vergangenheit Sicherheitsaspekte zumeist der allgemeinen Netzsicherheit überlassen, müssen heutige Lösungen eigene Sicherheitsmechanismen bieten, um am Markt bestehen zu können. In dem Artikel werden deshalb exemplarisch drei Anbieter auch daraufhin untersucht.**

*Prof. Dr.-Ing. Kai-Oliver Detken ist Dozent an der Hochschule Bremen im Fachbereich Informatik sowie Geschäftsführer der Decoit GmbH*

Mit der Vielzahl von „Knoten" in einem Netz für die paketorientierte Übertragung von Sprachdaten eröffnen sich für Angreifer potenziell mehr Angriffspunkte als in klassischen Datennetzen. Die Komplexität von VoIP-Infrastrukturen verlangt ein besonderes Vorgehen. Ein VoIP-Netz besteht aus einer Vielfalt von Komponenten und Anwendungen wie Telefone, Konferenzeinheiten, mobile Endgeräte, Call Manager, Gateways, Router, Firewalls und evtl. spezielle Software. Somit ist ein Vorgehen auf Systemebene erforderlich, wo Sicherheit in allen Schichten abgebildet wird und von einer zentralen Stelle aus koordiniert werden kann. Ein allumfassendes Sicherheitskonzept muss sowohl Anteile von Standardnetz- als auch VoIP-spezifischer Sicherheit umfassen.

### Spezielle VoIP-Anforderungen

Der Natur von IP-Netzen entsprechend müssen von einer VoIP-Komponente zusätzliche Anforderungen erfüllt werden – beispielsweise

- Benutzerauthentifizierung, da Telefone nicht mehr physisch verbunden sind;
- Adressenumsetzung von Telefonnummern nach IP-Adressen und umgekehrt;
- Routing zur Lokalisierung des richtigen Gateways, um das Zieltelefon zu erreichen;
- Erzeugen, Verarbeiten und Übertragen der Caller-ID über das Internet Protocol;
- Erzeugen, Verarbeiten und Übertragen der Billing-Daten für PSTN- und VoIP-Dienste;
- Notrufdienste;
- Abhörmöglichkeiten zur gesetzlichen Überwachung (Legal Interception).

Komponenten wie Router, Switche, Gateways und Server bilden Netzgrenzen und Schnittstellen zu anderen Netzen, die gegen Angriffe und nichtautorisierten Zugang abgesichert werden müssen. Für ein einwandfreies Funktionieren sind geeignete Hardware, Betriebssysteme, unterstützende Basisdienste wie DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), AAA-Mechanismen (Authentifizierung, Autorisierung und Accounting) als integrale Bestandteile zu sehen. Dabei sind in der Regel IP, TCP (Transmission Control Protocol), UDP (User Datagram Protocol), VoIP-spezifische Protokolle wie H.323, SIP (Session Initiation Protocol) und RTP (Real-Time Transport Protocol) vonnöten.

Die speziellen VoIP-Protokolle wurden, ähnlich wie IP-Protokolle im Allgemeinen, zunächst ohne jegliche Sicherheitsmechanismen ausgestattet. Dies hat sich inzwischen aber geändert; so wurden für H.323, SIP und RTP Erweiterungen implementiert, die eine aktuelle VoIP-Lösung auch unterstützen sollte (siehe *Bild*).

Ein weiteres Differenzierungsmerkmal ist das sehr ausgeprägte Wechselspiel zwischen Dienstgüte und Sicherheit. Dies abzuwägen, gestaltet manche Konzeption schwierig. Besonders die VoIP-Provider ignorieren geflissentlich jegliche Sicherheitsmechanismen und haben mitunter aufgrund der eigenen Netzstruktur auch Probleme in der Qualitätssicherung.

### Attacken auf VoIP-Systeme

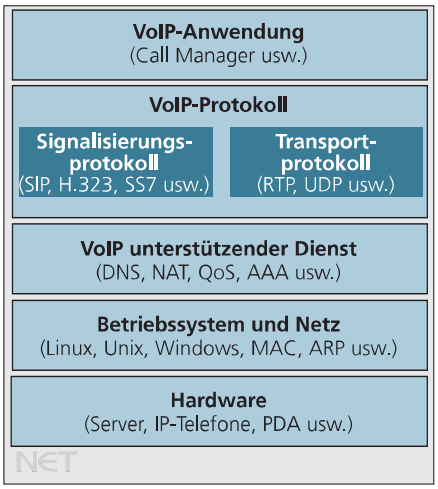
Attacken können bei VoIP auch von Nichtexperten ausgeführt werden, da es eine große Anzahl von Tools frei im Internet gibt. Neben den typischen Attacken gegen Netz- und IT-Systeme sind auch spezielle VoIP-Angriffe gängig, die alle Netzschichten betreffen. Die Verfügbarkeit des VoIP-Dienstes hängt direkt mit der Verfügbarkeit der Netzinfrastruktur zusammen. Dadurch können Angriffe wie Denial of

Service (DoS) den VoIP-Dienst genauso negativ beeinflussen wie andere IT-Dienste.
Dadurch, dass VoIP die Protokolle UDP und TCP nutzt, sind auch allgemeine Netzattacken relevant, zum Beispiel DoS, Spoofing, Flooding oder Sniffing. Die Attacken lassen sich noch leichter ausführen, wenn Netzbereiche den gleichen Trust-Level ohne Benutzerauthentifizierung teilen.
Auf der anderen Seite müssen folgende Angriffe gegen die Applikationsschicht einbezogen werden:

- Abfangen der Anschlussentgelte;
- Rufmanipulation;
- nichtautorisierte Nutzung (Phreaking);
- Dialer;
- Verletzung der Privatsphäre;
- Spam over IP Telephony (SPIT).

Weitere Sicherheitsrisiken wie dynamische Portnutzung, Konfiguration von Netzequipment (Standardports, Passwörter, Administration), fehlerhafte Implementierung in VoIP-Protokollen, Angriffe gegen Betriebssysteme von VoIP-Systemen sind ebenfalls möglich.
Für solche Attacken gibt es fertige Tools, mit denen man VoIP-Systeme direkt angreifen kann. Die nachfolgenden nutzen die Anfälligkeit der SIP- und RTP-Protokolle aus:

- *Cain & Abel* bedient sich des ARP-Spoofings, es werden also ARP-Abfragen vorgetäuscht und MAC-Adressen gefälscht, wodurch der Sprachverkehr umgeleitet und abgehört werden kann.
- *Vomit* wandelt ein Cisco-basiertes IP-Telefongespräch in ein WAV-File um, das mit jedem Audio-Player abgespielt werden kann. Vomit erfordert eine tcpdump-Ausgabedatei. Es arbeitet nur mit dem G.711-Codierungsstandard zusammen.
- *VoIPong* erkennt und filtert VoIP-Calls aus einem Datenstrom. Es legt eine Kopie eines G.711-Gesprächs an und konvertiert es in ein WAV-File. Unterstützt werden die Protokolle SIP, H.323, SCCP (Skinny Client Control Protocol), RTP und RTCP (Real-Time Control Protocol).
- *IP Vulnerability Scanner (SiVuS)* untersucht VoIP-Installationen auf Fehler mittels Initiieren von Attacken. Es können auch eigene SIP-Nachrichten generiert werden.
- *SIPcrack* als Protokoll-Login-Cracker enthält zwei Programme: SIPdump, um die eingeloggten SIP-User zu finden und SIPcrack, um die Passwörter der gefundenen SIP-User mittels Bruteforce-Attacken zu ermitteln.
- *RingAll* ermöglicht DoS-Attacken auf ungeschützte SIP-Clients.



*Die für VoIP relevanten Schichten*

Weitere Tools, die auf Netzebene VoIP zu schaffen machen könnten, sind Wireshark (ehemals Ethereal), Sipsak, Nmap und THC-Hydra. Eine noch größere Auswahl findet sich auf der Website der VoIP Security Alliance (www.voipsa.org).

## Sicherheitsimplementierungen

Der Schutz von VoIP-Netzen beginnt zunächst mit grundsätzlichen Maßnahmen zur Absicherung von Datennetzen. Vorhandene datenzentrierte Sicherheitstechniken können als Basis und verstärkend eingesetzt werden. Wegen der besonderen Risiken bei der VoIP-Kommunikation sind zusätzlich neue Techniken erforderlich. Diese beinhalten das Absichern von Sprachpaketen (Anwendungsebene) und von IP (Transport- oder Netzebene). Aufgrund der Spezifika in der VoIP-Kommunikation müssen darüber hinaus spezielle VoIP-Sicherheitskomponenten wirken, die mit den VoIP-Protokollen angeboten werden.
Dementsprechend ist eine gründliche Planung Voraussetzung, um einen verlässlichen Betrieb des VoIP-Dienstes mit einer zufriedenstellenden Dienstgüte (Quality of Services – QoS) gewährleisten zu können. Prinzipiell kann VoIP-Sicherheit die Bereiche Konfiguration, Anrufsteuerung, Sprachstrom und Datenstrom betreffen:

- Konfigurationssicherheit: TLS, SHHTTP usw.;
- Signalisierungssicherheit: TLS, IPsec usw.;
- Sprachpaketsicherheit: SRTP, SIP, IAX2 usw.;
- Datenpaketsicherheit: IPsec, SSH, VPN usw.

Obwohl die Bereiche unterschiedliche Sicherheitsmechanismen beinhalten, unterscheiden sich die grundlegenden Sicherheitskomponenten nicht voneinander. Um die wesentlichen Sicherheitsziele Autorisierung, Authentifizierung, Integrität, Vertraulichkeit und Nachweisbarkeit abbilden zu können, kommen Konfiguration, Authentifizierung, Schlüsselmanagement und Verschlüsselung zum Tragen.
Alle VoIP-Protokolle sind so erweitert worden, dass sie die Verschlüsselung von Sprach- und Signalisierungsdaten ermöglichen können. Die Erweiterungen müssen von den entsprechenden Implementierungen aber auch angeboten werden, um sie nutzen zu können.
Nachfolgend werden drei unterschiedliche Systeme miteinander bez. der Sicherheitsprotokollmechanismen verglichen, die auf reiner Software (Asterisk) und einer Hardware-Software-Kombination (Cisco und Siemens) basieren (*Tabelle*).

*Asterisk*
Das Open-Source-Projekt Asterisk unterstützt alle gängigen VoIP-Protokolle. Es wurde für die Absicherung von RTP sogar ein eigener Entwicklungszweig „securertp“ ins Leben gerufen. Allerdings wird die RTP-Verschlüsselung nur optional ermöglicht, was bedeutet, dass auch eine unverschlüsselte Verbindung hergestellt wird, wenn Endgeräte keine Verschlüsselung unterstützen sollten. Eine wirkliche Implementierung von SRTP wird bei Asterisk erst ab der Version 1.6.3 (1.8) Ende dieses Jahres erwartet. Bei der Implementierung des SIP-Protokolls in Asterisk wird lediglich UDP unter-

stützt. Somit bleibt zur Absicherung der SIP-Signalisierung lediglich die Nutzung einer Digest-Authentifizierung über einen MD5-Hash-Wert. Da immer wieder Sicherheitslücken in der SIP-Channel-Version von Asterisk gefunden wurden, kann hier auch nicht von einer sicheren Kommunikation ausgegangen werden. Zusätzlich bietet das IAX-Protokoll die Verschlüsselung mittels asymmetrischer RSA-Verschlüsselung an. Dies ermöglicht es, einen Benutzer, der einen Anruf über Asterisk durchführt, oder Asterisk gegenüber einem anderen Knoten zu authentifizieren. Leider wird das IAX2-Protokoll hauptsächlich für die Server-Server-Kommunikation verwendet, da viele Endgeräte es nicht unterstützen. Aufgrund der Implementierungslücken ist Asterisk momentan nicht mit Verschlüsselung zu empfehlen.

| VoIP-Systeme | SRTP | SIPS | IAX2 | H.323 | SCCPS | MGCP |
|---|---|---|---|---|---|---|
| Asterisk | o | o | + | o | o | o |
| Cisco Unified Communications Manager | + | + | - | + | + | + |
| Siemens HiPath-Serie | + | + | - | + | - | o |

*Tabelle: Sicherheitsimplementierungen bei verschiedenen VoIP-Systemen*
***–** = nicht implementiert; **+** = implementiert; **o** = noch unzureichend implementiert;*
*SRTP – Secure RTP; SIPS – SIP Secure; IAX – InterAsterisk eXchange; SCCPS – SCCP Secure; MGCP – Media Gateway Control Protocol*

*Unified Communications Manager*

Der Cisco Unified Communications Manager besitzt seit der Version 4 Sicherheitsmerkmale. Davor versuchte der Hersteller durch das Erhöhen der allgemeinen Netzsicherheit die Sicherheitsproblematik in den Griff zu bekommen. Inzwischen sind Sicherheitsprotokolle von VoIP und zur Netzkommunikation ausreichend implementiert. Früher einfach zu nutzende Dienste wie DHCP, DNS, Ping, Logdatei-Zugang usw. sind heute nur noch über die grafische Benutzeroberfläche über HTTPS oder per Kommandozeile über SSH zugänglich. Auch sind die Schnittstellen bis auf wenige Ausnahmen durch eine Verschlüsselung über HTTPS, SLDAP, SSH, SFTP und SNMPv3 gesichert.

Um die Sicherheit und Verfügbarkeit weiter zu erhöhen, wird seit der Version 5 die Linux-Distribution Red Hat Enterprise verwendet und nicht mehr wie vorher eine Servervariante von Windows. Um Server-Server-Protokolle wie MGCP und H.323 abzusichern, wird eine Verbindung mit IPsec zwischen zwei Gateways aufgebaut. Cisco benutzt ein bidirektionales Austauschen der X.509v3-Zertifikate als Basis der beiderseitigen Vertrauensbeziehung. Einmal authentifiziert und autorisiert, wird ein „Preshared Master Secret" erzeugt. Von da an ist eine Vertrauensbeziehung für alle Geräte etabliert. Verschiedene Modi für den Zertifikatsaustausch sind wählbar, wie auch verschiedene Kombinationen bei der Authentifizierung. Dadurch ist es möglich, einen Mischbetrieb zu konfigurieren.

Für die Kommunikation kann auch das Cisco-eigene Protokoll SCCP verwendet werden. Heutige Versionen von SCCP-basierten IP-Telefonen nutzen das SCCPS für die Authentifizierung der X.509-Zertifikate und verschlüsseln den TCP-Signalisierungsstrom mit TLS. So ist Identity-Spoofing oder das Decodieren der Kommunikationsdaten zwischen IP-Telefonen und dem Gatekeeper nicht mehr möglich. Cisco hat damit seine Hausaufgaben gemacht und bietet speziell mit der IPsec-Kommunikation die Absicherung unsicherer Protokolle wie MGCP an.

*HiPath-Serie*

Die HiPath-Serie von Siemens ist inzwischen eine auf internationalen Sicherheitsstandards basierende Lösung. Auch hier waren anfangs keinerlei Sicherheitsprotokolle implementiert. Die Gesprächsdaten werden von SRTP zwischen den Endgeräten mit einem als abhörsicher geltenden Verschlüsselungsalgorithmus gesichert. Dazu wird keine zusätzliche Soft- oder Hardware benötigt, da sie bereits in der Betriebssystemsoftware des Endgerätes enthalten ist. Das SRTP-Protokoll verschlüsselt nur den Nutzinhalt eines Datenpaketes mit dem Advanced-Encryption-Standard (AES). Der Paketkopf, der Absender und Adressat enthält, bleibt von der Verschlüsselung unberührt. Durch TLS wird zusätzlich eine Verschlüsselung der Signalisierung ermöglicht. Bei entsprechenden Siemens-Endgeräten sollte dabei kein Unterschied zur unverschlüsselten Kommunikation feststellbar sein.

Zusätzlich verschlüsselt das HiPath-System das eigene Systemprotokoll „CorNet IP" mit AES. Auch standortübergreifende Absicherungen können so betrieben werden. Die Sicherheitslösung lässt sich mit einem HiPath-Management-Tool zentral verwalten. Das größte System der HiPath-Familie, die HiPath8000, läuft ebenfalls auf Basis eines Linux-Betriebssystems (SuSE Enterprise Server) und setzt auf SIP bzw. das proprietäre SIP-Q als zentrale IP-Signalisierung. Erweiterte SIP-Sicherheitsmechanismen sind ebenfalls in den Implementierungen enthalten. Siemens bietet damit ebenfalls eine Absicherung von gängigem VoIP an, setzt aber weiterhin auf proprietäre Erweiterungen, um mehr Leistungsmerkmale zu ermöglichen.

## Fazit

Über Protokollerweiterungen besteht die Möglichkeit, die Sprach- und Signalisierungsdaten zu verschlüsseln. Hierbei besitzen kommerzielle Hersteller wie Siemens und Cisco gegenüber Asterisk leichte Vorteile, was den Implementierungsgrad betrifft (siehe *Tabelle*). Auch kann die Kombination von Hard- und Software eine zusätzliche Performance ermöglichen, die für die Verschlüsselung notwendig sein kann. So wurde in eigenen Tests mit Asterisk z.B. ein starker Anstieg der CPU-Auslastung durch die Verschlüsselung registriert. Das bedeutet, dass die VoIP-Systeme und Endgeräte erhöhten Leistungsanforderungen gerecht werden müssen. Zudem sollten auch die Endgeräte in der Lage sein, Verschlüsselung zu unterstützen. Eine alleinige Unterstützung der Telefonanlage reicht hier nicht mehr aus, da die Kommunikation von VoIP abhängig vom Hersteller direkt zwischen den Endgeräten erfolgt.

Unabhängig von der Herstellerimplementierung sollte man Sprach- und Datennetze auf der logischen Ebene mittels Virtual LANs voneinander trennen und separat absichern. (*we*)