VoIP-Security – Standards, Evaluierung und Konzeptbeispiele anhand von Asterisk

Dr. Kai-Oliver Detken[1], Prof. Dr. Evren Eren[2]

[1]DECOIT GmbH, Fahrenheitstraße 9, D-28359 Bremen
detken@decoit.de

[2]FH Dortmund, FB Informatik, Emil-Figge-Straße 42, D-44227 Dortmund
eren@fh-dortmund.de

Zusammenfassung

Mit Einführung der VoIP-Technologie lassen sich die Arbeitsprozesse schneller und effektiver umsetzen, was zu erheblichen Kosteneinsparungen führen kann. Allerdings werden die Sicherheitsaspekte angesichts dieser Kostenvorteile oft vernachlässigt. Durch die Integration der Sprachdatenübertragung in das IP-Netz ergeben sich aber unbestritten neue Herausforderungen an die IT-Sicherheit. VoIP-Pakete werden über ein so genanntes „Shared Medium" übertragen, also über ein Netz, welches sich mehrere Teilnehmer und unterschiedliche Dienste teilen. Unter gewissen Voraussetzungen kann es Angreifern möglich sein, die Daten auf dem Übertragungsweg abzugreifen und das Gespräch aufzuzeichnen. Es existieren beispielsweise Programme, mit deren Hilfe der Datenstrom auch aus geswitchten Umgebungen mittels „ARP-Spoofing" abgegriffen und daraus wieder eine Audiodatei erzeugt werden kann. Dieser Beitrag hat das Ziel, bestehende Risiken bei der Verwendung der VoIP-Technologie und mögliche Lösungsansätze für eine sichere Verbindung aufzuzeigen. Dabei werden die Standards und ihre Sicherheitsmechanismen einer kritischen Betrachtung unterzogen sowie Szenarien aufgezeigt. Als Realisierungsbeispiel wird die Open-Source-Lösung Asterisk näher untersucht und für die Sicherheitsanforderungen evaluiert.

1 Stand der Technik

Das Telefonieren mittels IP kann sich für den Teilnehmer genauso darstellen wie in der klassischen Telefonie. Wie bei der herkömmlichen Telefonie teilt sich das Telefongespräch hierbei in drei grundsätzliche Vorgänge auf. Diese Vorgänge sind der Verbindungsaufbau, die Gesprächsübertragung und der Verbindungsabbau. Im Unterschied zur klassischen Telefonie werden bei VoIP aber keine „Leitungen" durchgeschaltet, sondern Sprache wird in kleinen IP-Paketen transportiert.

Der Auf- und Abbau von Rufen (Rufsteuerung) erfolgt über ein von der Sprachkommunikation getrenntes Protokoll. Auch die Aushandlung und der Austausch von Parametern für die Sprachübertragung erfolgt über andere Protokolle als die der Rufsteuerung. Um in einem IP-basierten Netz eine Verbindung zu einem Gesprächspartner herzustellen, muss die aktuelle IP-Adresse des gerufenen Teilnehmers innerhalb des Netzes bekannt sein, jedoch nicht not-

wendigerweise auf der Seite des Anrufers. Feststehende Anschlüsse wie im herkömmlichen Festnetz (Public Switched Telephone Network – PSTN) gibt es in rein IP-basierten Netzen nicht. Die Erreichbarkeit des Angerufenen wird, ähnlich wie in Mobilfunknetzen, durch eine vorangegangene Authentifizierung des Gerufenen und einer damit verbundenen Bekanntmachung seiner momentanen Adresse, ermöglicht.

Aufgrund z. B. von Ortswechsel des Teilnehmers, Wechsel des Teilnehmers am gleichen PC oder die dynamische Adressvergabe beim Aufbau einer Netzwerkverbindung ist eine feste Zuordnung von Telefonnummern zu IP-Adressen nicht möglich. Die allgemein angewandte Lösung besteht darin, dass die IP-Telefonie-Teilnehmer bzw. dessen Endgeräte ihre aktuelle IP-Adresse bei einem Dienstrechner (Registrar-Server) unter einem Benutzernamen hinterlegen. Der Verbindungsrechner für die Rufsteuerung, oder manchmal sogar das Endgerät des Anrufers selbst, kann dann bei diesem Server die aktuelle IP-Adresse des gewünschten Gesprächspartners über den angewählten Benutzernamen erfragen und damit die Verbindung aufbauen.

Durch Nutzung des gleichen Netzes und der damit verbundenen Teilung mit anderen Teilnehmern wird die Sprache ungeschützt übertragen. Zwar besteht die Möglichkeit, die Übertragung zu verschlüsseln, jedoch wird dies häufig von den Anwendern nicht genutzt oder von den Herstellern bzw. Anbietern nicht angeboten. Einerseits liegt dies an fehlenden Implementierungen oder an der Unkenntnis über diese Möglichkeit, andererseits kann eine Verschlüsselung auch die Sprachqualität beeinträchtigen, weshalb sich häufig Anwender zu Gunsten der Sprachqualität entscheiden.

Ein VoIP-System lässt sich auf verschiedene Arten realisieren. Es gibt einige konkurrierende Protokolle mit spezifischen Vor- und Nachteilen. Insbesondere der Verbindungsaufbau muss gesichert werden, um die Authentizität der Teilnehmer zu gewährleisten und ein Umleiten bzw. Abhören des Datenstromes zu verhindern. Auch der Schlüsselaustausch zur Absicherung der nachfolgenden Nutzdaten muss auf sicherem Wege erfolgen. Zusätzlich soll der Datenstrom ebenfalls verschlüsselt gesendet werden, um ein Abhören bzw. Manipulieren der gesendeten Daten zu unterbinden.

Dazu gehört neben der Nutzung von geeigneten starken Verschlüsselungstechniken auch ein gutes und sicheres Schlüsselmanagement. Konfigurationsschnittstellen der einzelnen Komponenten sind ebenfalls mit einem verschlüsselten Zugang (z.B. https) zu schützen. Zusätzlich muss sichergestellt werden, dass die anfallenden Gebühren (bei Telefonaten zwischen einem VoIP-Netz und einem klassischen Telefonnetz wie z.B. ISDN) korrekt erfasst werden können und nicht manipulierbar sind (etwa durch das Verhindern des Abbaus der Verbindung).

Ebenso muss das Netzwerk gegen Angriffe Dritter (Hacker) sowie Viren, Würmer, Trojanische Pferde und andere bösartige Software geschützt werden. Dies lässt sich am besten mit geeigneten Firewall-, Intrusion-Detection-Systemen und Virenscannern realisieren. Außerdem ist darauf zu achten, etwaige Designfehler bei der Implementierung der VoIP-Software zu vermeiden, durch die Sicherheitslücken entstehen können.

Verbreitete Signalisierungsprotokolle sind:

- Session Initiation Protocol (SIP), IETF RFC-3261
- Session Description Protocol (SDP), IETF RFC-4566
- H.323 – Packet-based multimedia communications systems, ITU-T-Standard
- Inter-Asterisk eXchange Protocol (IAX)

- 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

Im Normalfall schickt jedes Endgerät die codierten Sprachdaten direkt über das Netzwerk an die IP-Adresse der Gegenstelle. Die Gesprächsdaten fließen also nicht über den Server eines VoIP-Providers, sondern werden direkt zwischen den Endgeräten der Teilnehmer ausgetauscht.

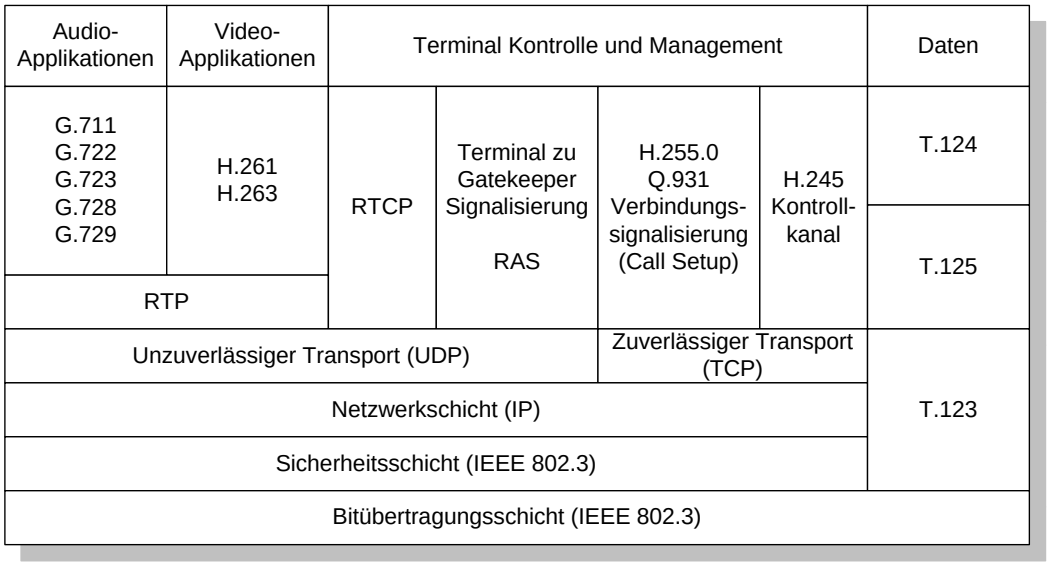

Abb. 1: Protokollstack bei VoIP

Der eigentliche Transport der Daten erfolgt über das Real-Time Transport Protocol (RTP), gesteuert durch das Real-Time Control Protocol (RTCP). RTP verwendet zur Übertragung in der Regel das User Datagram Protocol (UDP). UDP kommt zum Einsatz, da es ein minimales, verbindungsloses Netzwerkprotokoll ist, das nicht auf Zuverlässigkeit ausgelegt wurde wie beispielsweise das Transmission Control Protocol (TCP). Dies bedeutet, dass der Empfang der Sprachpakete nicht bestätigt wird, also keine Übertragungsgarantie besteht. Der Vorteil von UDP ist aber dessen geringere Latenzzeit gegenüber der von TCP, da nicht auf eine Bestätigung gewartet und fehlerhafte Pakete nicht erneut gesendet werden und sich somit der Datenfluss insgesamt nicht verzögert. Eine vollkommen fehlerfreie Übertragung ist ohnehin nicht nötig, da die gesprochene Sprache eine hohe Redundanz aufweist und heutige Codecs in der Lage sind, Fehler bis zu einer bestimmten Anzahl zu korrigieren. Für ein kontinuierliches Gespräch ist eine geringe Antwortverzögerung wesentlich wichtiger.

Die Anforderungen an das Netz für Datenübertragung und IP-Telefonie unterscheiden sich erheblich. Neben der erforderlichen Übertragungskapazität (ca. 64 kbit/s für ein unkomprimiertes Gespräch) haben insbesondere Qualitätsmerkmale wie Latenz, Jitter und Paketverlustrate erheblichen Einfluss auf die erreichbare Sprachqualität. Durch Priorisierung und entsprechende Auslegung der Netze ist es möglich, eine entsprechende Steuerung vorzunehmen, um unabhängig von der sonstigen Netznutzung zuverlässig eine gleich bleibende Sprachqualität zu erreichen.

2 Asterisk

Asterisk [ASTE07] ist eine Open-Source-Software, die alle Funktionalitäten einer herkömmlichen Telefonanlage abdeckt. Asterisk unterstützt VoIP mit unterschiedlichen Protokollen und kann mittels relativ günstiger Hardware mit Anschlüssen wie POTS (analoger Telefonanschluss), ISDN-Basisanschluss (BRI) oder -Primärmultiplexanschluss (PRI, E1 oder T1) verbunden werden. Asterisk wurde ursprünglich von Mark Spencer der Fa. Digium (http://www.digium.com) entwickelt. Wichtige Erweiterungen und Applikationen stammen aber auch von anderen Entwicklern. Veröffentlicht wurde die Software unter der GNU General Public License. Aufgrund dieser Tatsache schreitet die Weiterentwicklung rasch voran.

Die folgenden Funktionen stellen einen Auszug dar:

- Wählregeln, die sich individuell anpassen und sich durch zusätzliche Applikationen erweitern lassen, so dass exakt entschieden werden kann, was mit einem eingehenden Anruf passiert.
- Interaktives Sprachmenü zur Führung des Anrufers durch die Menüs, um z.B. das richtige Zielsystem zu erreichen.
- Zeit- und Kostenabrechnung für jeden Teilnehmer bzw. jede Nummer.
- Voicemail bietet ein komplettes Anrufbeantwortersystem mit passwortgeschütztem Zugangssystem, Weiterleitung der Aufzeichnungen per E-Mail sowie zwischen den verschiedenen Teilnehmern.
- Warteschlange mit Musikunterstützung für z.B. Call Center, um Kunden eine Möglichkeit zu geben, einen Teilnehmer zu erreichen.
- Konferenzraum, um eine einfache Möglichkeit zu bieten, mit mehreren Teilnehmern gleichzeitig zu sprechen.
- Anrufweiterleitung bei „nicht erreichbar“ oder „besetzt“.
- Blacklists zum Blocken unerwünschter Teilnehmer (vorausgesetzt, die Rufnummer wird übermittelt).

Des Weiteren unterstützt Asterisk viele paketbasierte Protokolle wie z.B. IAX/IAX2, H.323, SIP, MGCP und SCCP.

Da jedoch nicht nur paketbasierte Systeme angebunden werden sollen, werden auch diverse Protokolle der traditionellen Telefonie unterstützt wie z.B. E-DSS1 (Euro-ISDN), National ISDN2, DMS100, BRI (ISDN4Linux) und 4ESS. Aufgrund der Vielfalt von Asterisk, müssen auch die unterstützten paketbasierten Protokolle einer Sicherheitsuntersuchung unterzogen werden. [KESS06]

3 Risiken

Durch den Transport von Sprachdaten über standardisierte, offene Datennetze ergeben sich zahlreiche Bedrohungen. Verschärft wird die Bedrohungslage dadurch, dass VoIP-Systeme aus vielen Einzelkomponenten bestehen und jede dieser Einzelkomponenten für sich genommen bereits ein komplexes, vielschichtiges System mit möglichen Schwachstellen darstellt.

3.1 Protokolle

Das Ausmaß der Bedrohungen bei den Übergängen zwischen Netzen hängt von den dabei verwendeten Protokollen ab. Für die Medienströme wird fast ausschließlich RTP und für die Signalisierung H.323, SIP, MGCP und MEGACO verwendet. Dazu kommen fallweise proprietäre Protokolle zum Einsatz.

3.1.1 H.323

Die wesentlichen Angriffspunkte der Protokolle der H.323-Familie sind Täuschung der Identität seitens des anrufenden Teilnehmers, sowie Manipulation der Nachrichten mit Hilfe von Man-in-the-Middle-Attacken. Gelingt es einem Teilnehmer mit falscher Identität Sprachverbindungen über ein Gateway zu führen, so ist der Weg zum Gebührenbetrug oder anderen kriminellen Handlungen unter falscher Identität möglich.

Die Anruferidentifikation kann dabei anhand der IP-Adresse, der H.323-Identifikation oder der Absender-Rufnummer durchgeführt werden. Häufig wird aber nur eines dieser Kriterien – nämlich die H.323-Identifikation – für die Authentifizierung in Verbindung mit einem Passwort verwendet. Dabei werden die Daten unverschlüsselt über das Netz übertragen. Um an diese Daten zu gelangen, genügt es dem Angreifer, den Signalisierungsstrom im Netz mit Hilfe einer der oben beschriebenen Attacken abzugreifen. Der binäre Datenstrom lässt sich dann mit einem beliebigen ASN.1-Parser – z. B. mit dem Packet Sniffer Wireshark (ehemals Ethereal) – decodieren und im Klartext darstellen.

Des Weiteren ist es möglich, beim Verbindungsaufbau die Transportadressen der Sprachströme zu verändern, wodurch diese an eine beliebige IP-Adresse umgeleitet, und dort abgehört, aufgezeichnet oder gar verändert weitergeleitet werden können. Diese Bedrohungen betreffen Endgeräte ebenso wie Gateways.

3.1.2 Session Initiation Protocol (SIP)

Das Session Initiation Protocol (SIP) bietet eine Sicherung der Nachrichten unter Verwendung kryptographischer Hashes und Verschlüsselungsmechanismen an. Dies erlaubt eine zuverlässige Authentifizierung und Absicherung gegen Veränderungen der Signalisierungsnachrichten. Allerdings sind nicht alle Header durch Hashing abgedeckt, wodurch eine Manipulation der Absenderkennung möglich ist. Wird keine Absicherung der SIP-Nachrichten mit Hashes vorgesehen, so können die im Bereich H.323 beschriebenen Angriffe sogar mit noch einfacheren Mitteln realisiert werden, da die Nachrichten im ASCII-Text kodiert werden. Hierzu reicht ein kurzes Skript, das bestimmte Header der Nachricht umschreibt und weiterleitet. Auch hier sind Endgeräte und Gateways betroffen.

3.1.3 Real-time Transport Protocol (RTP)

Das Real-time Transport Protocol (RTP) dient der Übertragung der Medienströme von Echtzeit-Anwendungen. Dabei werden in jedem Datenpaket die notwendigen Informationen zur Rekonstruktion der Daten mit übertragen. Dazu gehören insbesondere Sequenznummer, Zeitstempel des Datenpakets, Art des Medienstroms (Audio/Video) und Länge des RTP-Headers. Mit diesen Informationen kann eine Menge von Datenpaketen einer Verbindung in einer korrekten Reihenfolge mit dem passenden Codec decodiert und auf einem Ausgabegerät abgespielt werden, ohne auf die Signalisierung dieser Verbindung zurückgreifen zu müssen. Diese einfache Decodierung des Medienstroms versetzt einen Angreifer in die Lage, die Datenpake-

te eines Sprachstromes abzuhören und zu manipulieren, sobald er auf diese zugreifen kann. Dabei ist sogar die Reihenfolge der empfangenen Datenpakete unerheblich. Zwar entstehen Lücken bei der Decodierung, wenn bestimmte Datenpakete fehlen, jedoch ist dies nicht mit einem Synchronisationsverlust des Kanals verbunden.

3.1.4 MGCP und MEGACO

Bei den Protokollen MGCP und MEGACO sind Sicherheitsmechanismen ebenfalls nicht direkt vorgesehen. Gelingt es einem Angreifer, Datenströme abzuhören und zu manipulieren, so können diese decodiert und beliebig verändert werden. Falls die Daten mit ASN.1 oder in ASCII codiert sein sollten, ist für die Offenlegung ein ASN.1-Parser notwendig.

Die oben genannten Protokolle werden nur zwischen VoIP-Servern und Gateways bzw. zwischen Gateways selbst eingesetzt. Somit sind von den Manipulationen der Protokoll-Nachrichten nur Gateways betroffen.

3.1.5 Skinny Client Control Protocol (SCCP)

Das Skinny Client Control Protocol (SCCP) ist ein proprietäres Kommunikationsprotokoll, das für die Kommunikationssteuerung zwischen IP-Telefonen und dem Gatekeeper (bei Cisco der Call Manager) verwendet wird. Es ist nicht öffentlich dokumentiert und kann vom Hersteller jederzeit verändert werden.

Die Abläufe des Protokolls sind einfach gehalten. Die gesamte Verbindungssteuerung läuft in einer einzigen TCP-Verbindung ab, in der parametrisierte Befehle binär-codiert übertragen werden. In älteren Protokollversionen, die immer noch in sehr vielen Endgeräten verwendet werden, wird lediglich die MAC-Adresse zur Authentifizierung übertragen. Diese Kommunikation lässt sich relativ einfach nachbilden (ca. 300 Zeilen Perl-Code sind hierzu notwendig) und somit dem Gatekeeper ein fremdes IP-Telefon vortäuschen. Auf diese Weise kann auf fremde Kosten telefoniert, die Identität gegenüber Dritten vorgetäuscht, aber auch eine Denial-of-Service-Attacke auf VoIP-Server durchgeführt werden.

Neuere Versionen von SCCP-basierten IP-Telefonen verwenden SCCPS für die Authentifizierung X.509-Zertifikate und verschlüsseln den TCP-Signalisierungsstrom mit Hilfe von TLS.[1] Damit ist Identity-Spoofing sowie das Dekodieren der Kommunikationsdaten zwischen IP-Telefonen und dem Gatekeeper nicht mehr möglich. Für die Steuerung unterschiedlicher Leistungsmerkmale der Telefone wird verstärkt HTTP verwendet. Auch dies läuft bislang ohne Verschlüsselung ab. Damit kann auch hier die Kommunikation abgehört und die Nachrichten manipuliert werden.

3.1.6 InterAsterisk eXchange Protocol (IAX)

Das InterAsterisk eXchange Protocol (IAX) ist eine Entwicklung der Open Source Community. Es eignet sich zur Vernetzung von Asterisk-Servern sowie als Endgeräte-Kommunikationsprotokoll zur Übertragung von Medien (Audio, Video, Texten und Bilder). Signalisierung und Datenübertragung werden über UDP-Port 4569 abgewickelt. Das IAX-Protokoll ist sehr schlank gehalten und eignet sich gut für die Kommunikation in privaten Netzen (NAT) sowie durch Firewalls.

---

[1] Hinweis: Analog zu HTTPS (Port 443) wird standardmäßig der TCP-Port 2443 verwendet, für SCCP wird der TCP-Port 2000 genutzt.

Die Hauptmerkmale des IAX-Protokolls lassen sich wie folgt zusammenfassen:

- Proprietär, jedoch offen.
- Signalisierungs- und Medientransport werden über einen einzigen Port (UDP 4569) abgewickelt. Dadurch ist das Protokoll IAX2 einfach über NAT-Umgebungen zu transportieren und die Regeln in Firewalls sind überschaubar.
- Schlank durch binäre Codierung und geringen Protokoll-Overhead. IAX weist ein Protokoll-Overhead von nur vier Bytes auf, um Sprach- und Videopakete auszutauschen.
- Die Bündelung mehrerer IAX-Verbindungen zwischen zwei Asterisk-Servern zu einem Trunk ist möglich.

Im eigentlichen IAX-Protokoll wurden keine Sicherheitsmechanismen verankert. Dies wurde in der Version IAX2 nachgeholt. Hinzu kommt, dass IAX-Endgeräte relativ selten am Markt vorkommen, so dass dieses Protokoll nur in Szenarien mit Asterisk-Servern relevant ist. [ERDE07]

3.2 Bedrohungen und Attacken

Attacken können bei VoIP auch von Nichtexperten ausgeführt werden, da es eine ausreichende Anzahl von Tools frei im Internet gibt. Neben den typischen Attacken gegen Netzwerk- und IT-Systeme kommen dabei auch spezielle VoIP-Angriffe zum Tragen. Diese Attacken betreffen alle Netzwerkschichten. Die Verfügbarkeit des VoIP-Dienstes hängt direkt mit der Verfügbarkeit der Netzwerkinfrastruktur zusammen. Dadurch können Angriffe wie Denial-of-Service (DoS) den VoIP-Dienst genauso negativ beeinflussen wie andere IT-Dienste.

Dadurch, dass VoIP UDP und TCP nutzt, sind folgende Netzwerkattacken relevant:

- Denial-of-Service (DoS)
- ARP, MAC, IP, UDP, IRDP Spoofing
- SYN-, PING- oder MAC-Flooding
- TCP-Session-Hijacking
- RST-Attack
- Data Injection through ISN-Guessing
- Sniffing
- Replay

Diese Attacken lassen sich noch einfacher ausnutzen, wenn Netzwerkbereiche den gleichen Trust-Level ohne Benutzerauthentifizierung teilen. Auf der anderen Seite müssen folgende Angriffe gegen die Applikationsschicht einbezogen werden:

- Abfangen der Anschlussgebühren
- Rufmanipulation
- Nichtautorisierte Nutzung (Phreaking)
- Dialer
- Verletzung der Privatsphäre
- Spam over IP Telephony (SPIT)

Weitere Sicherheitsrisiken wie z.B. dynamische Portnutzung, Konfiguration von Netzwerkequipment (Standardports, Passwörter, Administration), fehlerhafte Implementierung in VoIP-Protokollen, Angriffe gegen IP-PBX und Betriebssysteme von VoIP-Systemen sind möglich.

3.3 Angriffstools

Es existieren außerdem viele Angriffstools, mit denen VoIP-Systeme direkt attackiert werden können. Die hier aufgelisteten Tools adressieren die Anfälligkeit der SIP- und RTP-Protokolle:

- **Cain & Abel:** bedient sich dem ARP-Spoofing, d.h. es werden 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, die 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 in einem Datenstrom heraus. Es legt eine Kopie eines G.711-Gesprächs an und konvertiert dieses in ein WAV-File. Unterstützt werden die Protokolle SIP, H.323, SCCP, RTP und RCTP.
- **SIP Vulnerability Scanner (SiVuS):** untersucht VoIP-Installationen auf Fehler. Dies wird durch das Initiieren von Attacken vorgenommen. Es können auch eigene SIP-Nachrichten generiert werden.
- **SIPcrack:** als Protokoll-Login-Cracker enthält es zwei Programme: SIPdump, um die eingelogten SIP-User zu finden und SIPcrack, um die Passwörter der gefundenen SIP-User mittels Bruteforce-Attacks zu ermitteln.
- **RingAll:** ermöglicht DoS-Attacken auf ungeschützte SIP-Clients.

Weitere Tools, die auf Netzwerkebene VoIP zu schaffen machen könnten, sind Wireshark (ehemals Ethereal), Sipsak, Nmap und THC-Hydra. Eine größere Auswahl kann auf den Webseiten der VOIP Security Alliance (http://www.voipsa.org) abgefragt werden.

3.4 Bewertung und Auswirkungen

VoIP bietet grundsätzlich eine größere Angriffsfläche als die traditionelle Telefonie. Dies liegt zum einen an der Nutzung offener Netzprotokolle, die meistens ungesichert betrieben werden und zum anderen an der gemeinsamen Kommunikationsplattform (Sprache und Daten über ein gemeinsames Netz). Allerdings muss man die Schwächen auch klar von den VoIP-Szenarien abhängig machen, um eine Bewertung vornehmen zu können:

- **Campus VoIP:** In einer Campus-VoIP-Umgebung wird eine Nebenstellenanlage auf IP-Basis verwendet, die auch als IP-PBX (Private Branch eXchange) bezeichnet wird. IP-Telefone und/oder Softphones sind mit dieser Nebenstellenanlage verbunden. Der Verbindungsaufbau in das öffentliche Telefonnetz wird über Gateways ermöglicht. Realisiert werden kann dieses System Hardware-basiert (aufgerüstete Nebenstellenanlage mit VoIP-Interface) oder Software-basiert (Serversystem mit VoIP-Software). Beide Varianten sind schwer von außen zu attackieren, da die Telefongespräche nicht über das

Internet oder andere unsichere Netze geführt werden. Potenzielle Attacken müssen daher hauptsächlich aus dem Intranet kommen oder von außerhalb über die Firewall.

- **IP Centrex / Hosted IP:** Diese VoIP-Variante beinhaltet eine virtuelle, IP-basierte Nebenstellenanlage, die von einem Provider zur Verfügung gestellt wird. Der Provider ist hierdurch in der Lage, eigene Sprachdienste anzubieten, ohne dass ein Unternehmen eigene Gateways oder PBX-Systeme anschaffen muss. Aus Sicht des Unternehmens muss nur eine ausreichende Internet-Anbindung vorhanden sein und IP-Telefone und/oder Softphones müssen angeschafft werden. Attacken auf das VoIP-System können über das Intranet oder über das Internet (aus dem Providernetz) erfolgen.
- **VoIP-Trunks:** VoIP-Trunkverbindungen lösen zunehmend herkömmliche verbindungsorientierte Telefonverbindungen ab. Dies liegt an der zunehmenden Konvergenz der Netze und den sich daraus resultierenden Kosteneinsparungen. Auch erhöht sich die Flexibilität, wenn keine T1- oder PRI-Interfaces mehr verwendet werden müssen. Allerdings kann es hierbei auch zu einem höheren Angriffspotenzial kommen, wenn die Übertragung über unsichere Netze realisiert wird. Speziell die Attacken aus dem Internet führen dazu, dass Unternehmensnetze verletzlicher werden.

Auf Asterisk bezogen sollte eine Campus-VoIP-Lösung zum Einsatz kommen, die keine unsichere Kommunikation über das Internet ermöglicht. Durch die bereits vorhandene Absicherung des Firmennetzes gegenüber äußeren Angreifern, wird auch das VoIP-System geschützt. Hinzu kommt, dass ein Quality-of-Service (QoS) konsequent umgesetzt werden kann, um die Sprachqualität auf einem höchstmöglichen Niveau zu halten. VoIP wird in diesem Szenario einfach als ein weiterer IP-Dienst begriffen, der sehr hohe Anforderungen an das Netz und die Sicherheit stellt.

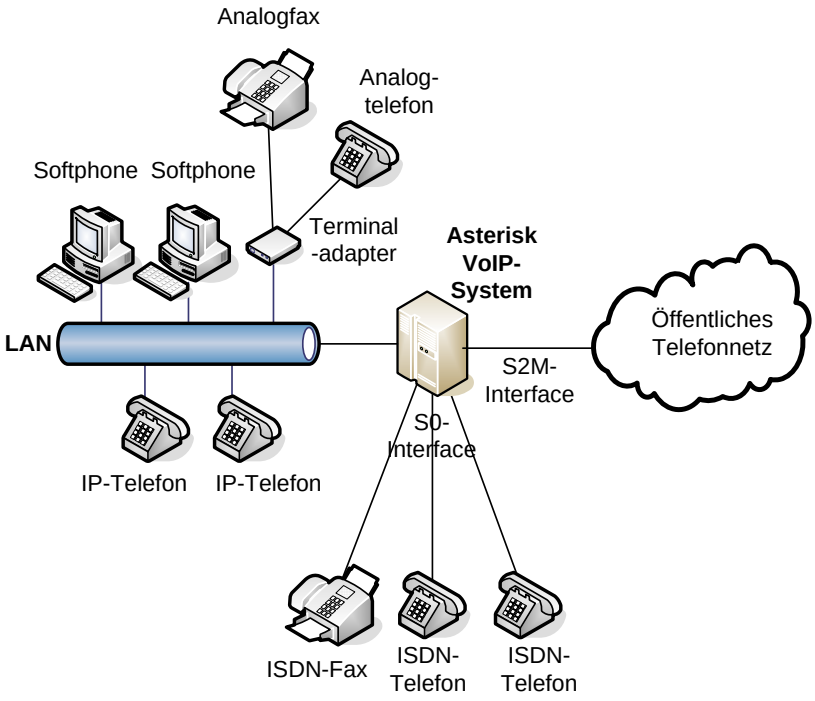

Abb. 2: Asterisk VoIP-Szenario

VoIP-Netzwerke beinhalten viele unterschiedliche Komponenten wie IP-Telefone, Gateways, Server (Gatekeeper bzw. SIP Proxy), Router, etc., die spezielle Anforderungen an die Sicherheit besitzen. Dabei muss bei VoIP sowohl die Netzwerk- als auch die Applikationsseite mit betrachtet werden. Dies beinhaltet auf der Netzwerkseite die Bereiche Netzwerksicherheit, Virtual LANs (VLAN), Verschlüsselung, Authentisierung, Firewalls, IDS/IPS, NAT und STUN, Soft- und Hardphones, Netzwerkequipment, Betriebssysteme, QoS, Remote Management und Patchmanagement. Die Netzwerksicherheit wird hier nicht weiter betrachtet, da hier die grundsätzlichen Sicherheitsanforderungen umgesetzt werden müssen.

Dies verhält sich bei den verwendeten Signalisierungsprotokollen, die ein VoIP-System verwendet, etwas anders. Da hier Asterisk als VoIP-System angesehen werden soll, kommen für die Betrachtung unseres Szenarios die sicherheitstechnisch erweiterten Protokolle SRTP, IAX2 und Sicherheitsmechanismen für SIP in Frage:

- **SRTP:** Es wird eine Verschlüsselung der Medienströme vorgenommen. Um eine Verschlüsselung zu gewährleisten, muss zunächst ein Schlüsselaustausch erfolgen. Aufgrund der AES-Verschlüsselung ist sichergestellt, dass der Inhalt eines Gespräches nicht aufgezeichnet werden kann. Durch die Verwendung von SHA-1 werden die Gesprächsteilnehmer authentifiziert. Der Schlüssel, welcher genutzt wird, um die Nutzdaten zu verschlüsseln, wird allerdings über SIP übertragen. Somit kann der Schlüssel ausgespäht werden, wenn SIP nicht ausreichend abgesichert ist[2].
- **SIP:** SIP wurde um diverse Sicherheitsmechanismen wie TLS, HTTP Digest, IPsec mit IKE und S/MIME erweitert. Es wird Ende-zu-Ende-Sicherheit und Hop-by-Hop-Kommunikation angeboten[3]. SIP wird bei Asterisk jedoch nur über UDP realisiert. Das schließt die Absicherung über TLS aus, da dies TCP voraussetzt. Obwohl es schon einige Bemühungen gab, andere Sicherheitsmechanismen für SIP zu realisieren, wird bei Asterisk nur SIP Digest Authentication mit MD5 eingesetzt. Hierbei kann der Message Digest in der Konsole generiert und in der Konfiguration eingetragen werden. Die fehlenden Sicherheitsmechanismen für SIP sollen über die nächste Generation des SIP-Channels (Version 3[4]) nachgeholt werden, die jedoch noch über das Projekt „Pineapple“ in der Entwicklung sind. [PINE07] Da hier ein stärkerer Eingriff in der Architektur von Asterisk notwendig ist, wird es hier auch keine Rückwärtskompatibilität geben. Die Entwicklung hängt vom Sponsoring und der Beteiligung an der Entwicklung ab.
- **IAX2:** Es handelt sich bei IAX2 (im Gegensatz zu SIP) nicht um ein textbasiertes, sondern Binärprotokoll. Ursprünglich wurde das IAX-Protokoll entwickelt, um eine Kommunikation zwischen Asterisk-Servern zu realisieren. Allerdings beherrscht IAX auch die Möglichkeit, Gespräche zu initialisieren und Sprachdaten zu übertragen. Dafür werden einige Sicherheitsmechanismen zur Verfügung gestellt. Asterisk-Server können sich gegenseitig über eine PKI authentifizieren. Dazu findet ein RSA- oder alternativ ein Diffie-Hellman-Schlüsselaustausch statt. Zur Verschlüsselung der Nachrichten wird hier AES mit 128 Bit verwendet. Da IAX2 für den Verbindungsaufbau nur einen UDP Port (4569) benötigt, muss auch nur dieser Port in der Firewall geöffnet werden.

---

[2] der Schlüssel wird im SIP-Body über die SDP-Parameter übertragen

[3] Zur Hop-by-Hop-Absicherung gehören TLS und IPsec und zur Ende-zu-Ende-Absicherung zählen SIP-Digest-Authentication und S/MIME. S/MIME ist im RFC-3261 allerdings nur optional definiert.

[4] Aktuell wird Version 1 eingesetzt. Version 2 hatte nur Patch-Level-Status und wird nicht mehr weiter entwickelt

Da die IP-Endgeräte heute bis auf Ausnahmen kein IAX2 unterstützen, muss auf die Sicherheitsmechanismen in der SIP-Spezifikation und SRTP ebenfalls zurückgegriffen werden. IAX2 sollte zur Kopplung von Asterisk-Servern zwischen verschiedenen Standorten zum Einsatz kommen. Neben der erhöhten Sicherheit kann auch ein Sprachqualitätszuwachs dabei registriert werden sowie eine verbesserte Ausnutzung der vorhandenen Bandbreite.

Eine weitere Methode der Absicherung von Asterisk (für das Szenario „VoIP-Trunks“) ist die Absicherung über das SIMCO[5]-Protokoll. Das SIMCO-Protokoll ist dabei vollständig konform zum MIDCOM Protokoll[6]. Digium Partner Ranch Networks hat hierfür (Ende Januar 2006[7]) auf Wunsch von Digium selbst seinen Programmcode der Community bereitgestellt. Dieser steht in einem getrennten Entwicklungszweig „Asterisk-Netsec“ zur Verfügung. Durch die Implementierung dieses Protokolls in Asterisk, werden über „Policy Rule Control Messages“ Firewall Ports (insbesondere für RTP) dynamisch[8] frei geschaltet. Die Kommunikation vom Asterisk-Server zum Middlebox-Gerät[9] verläuft dabei abgesichert über OpenSSL. Obwohl diese Methode bewusst sehr generisch entwickelt wurde, ist zurzeit der Einsatz nur über Geräte von Ranch Networks bekannt.

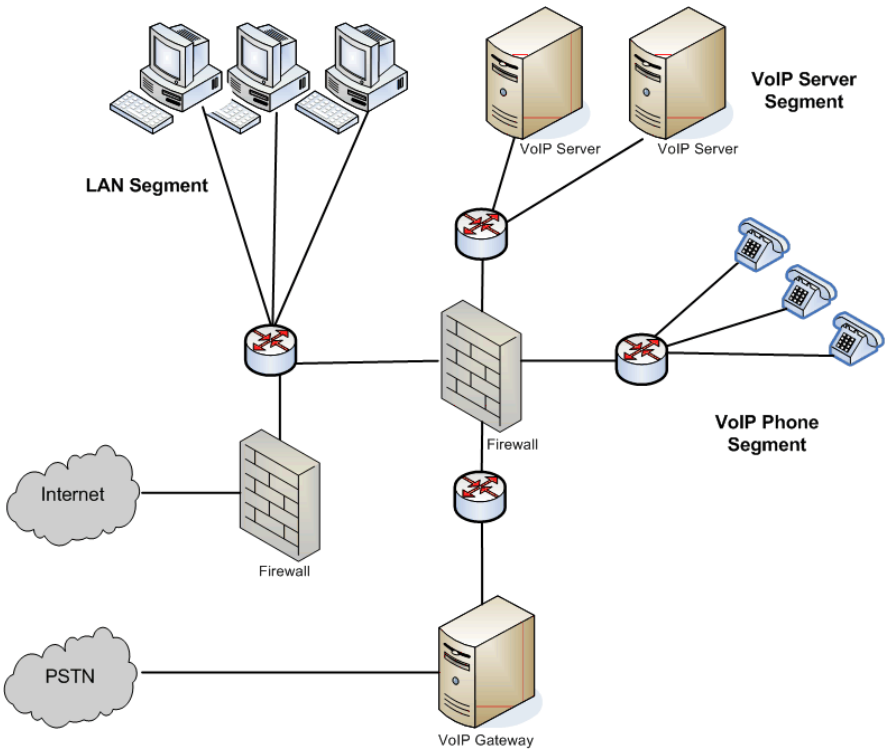

Abb. 3: Einsatz von Firewalls und VLANs zur Absicherung des VoIP-Systems

Des Weiteren sollte eine Separation der Daten- und des VoIP-Bereichs erfolgen, um Kollisionen und Engpässe zu vermeiden. Zum einen sollte der VoIP-Bereich separat durch Firewalls

[5] SIMCO: SImple Middlebox COnfiguration, RFC-4540

[6] MIDCOM: MIDdlebox COMmunication, RFC-3303 und RFC-3304

[7] http://tinyurl.com/2nfujr oder http://tinyurl.com/2tq9wz

[8] nur, wenn gerade ein Anruf durchgeführt wird

[9] z.B. NAT Device, Firewall, Ranch Network Device oder Kombinationen aus diesen

abgetrennt werden, um einen zusätzlichen Schutz zu ermöglichen. Zum anderen sollten auch die IP-Telefone in einem anderen Subnetz bzw. anderem Netzsegment enthalten sein. Dies ermöglicht eine bessere Aufteilung der Netze und die effiziente Einführung von Priorisierungsmechanismen (Q-Tag, DiffServ). Über VLANs kann auch auf Schicht 2 eine Teilung der Netze erfolgen, so dass auf logischer Ebene Sprache und Daten getrennt werden, während man beide Verkehrstypen über die gleiche Infrastruktur nutzen kann. [ERDE07]

Tab. 1: Übersicht über Risiken und Kompensationsverfahren

Risiken	Praxisansätze
Application Level Attacken	• Application Level Gateways, Firewalls und ISD/IPS
DoS/DDoS	• IDS/IPS • Aktuelle Patch-Levels • Anti-Virus-System • Policy-basierte Sicherheitszonen • VLAN
Abhören	• VPN zum isolieren von VoIP-Datenverkehr • Verschiedene Verschlüsselungen
Attacken gegen die Protokolle	• Application Level Gateways und IDS/IPS
SPIT	• Starke Authentifizierung, Autorisierung und IPsec
Nicht autorisiertes SIP-Monitoring und Spoofing	• Starke Authentifizierung, Autorisierung und IPsec

4 Ausblick

Das oftmals eingesetzte SIP-Protokoll kann ebenso nicht in allen in der Praxis anzutreffenden Formen als hinreichend sicher betrachtet werden. Es verfügt zwar über Sicherheitsmechanismen (bspw. Call-IDs auf der Basis von Hashes), bietet jedoch Angriffsmöglichkeiten für DoS-Attacken. Außerdem könnte das Phreaking mit VoIP sozusagen ein Revival erleben. Das Szenario beruht darauf, dass bei der VoIP-Kommunikation die Signalisierung (beispielsweise via SIP) von den Sprachdaten (Payload, bspw. RTP) entkoppelt ist. Zwei speziell präparierte Clients bauen über den SIP-Proxy ein Gespräch auf und verhalten sich absolut standardkonform. Nach dem Gesprächsaufbau wird dem SIP-Proxy ein Gesprächsabbau signalisiert. Dieser sieht die Sitzung als beendet an und verbucht das Gespräch. Einzig der RTP-Datenstrom wird von den Clients aufrechterhalten. Die Gesprächspartner telefonieren anschließend kostenlos weiter. Ein anderer sicherheitsrelevanter Bereich ist zwar nicht ausschließlich auf diese Technik begrenzt, wird jedoch durch die geringen Kosten, die für die Gespräche anfallen, begünstigt. So besteht die Möglichkeit einer Art von „VoIP-Spam“, auch SPIT („Spam over Internet Telephony“) genannt.

Für sicheres VoIP muss daher momentan ein Campus-Szenario betrieben werden, aus dem heraus über ISDN kommuniziert wird. VoIP sollte hier als zusätzlicher IP-Dienst begriffen werden, der vom restlichen Netz separiert operiert. Zukünftig kann dann eine Anbindung an öffentliche VoIP-Provider vorgenommen werden, wenn die Signalisierungsstandards ein ho-

hes Sicherheitsniveau übergreifend erreicht haben sowie Authentifizierung und Verschlüsselung auch von Providern angeboten werden.

Literatur

[ASTE07] http://www.asterisk.org

[ERDE07] Evren Eren, Kai-Oliver Detken: Voice-over-IP Security Mechanisms - State-of-the-art, risks assessment, concepts and recommendations. 8th International Symposium on Communications Interworking, Santiago de Chile 2007

[HJP06] Handley, Jacobson, Perkins: SDP – Session Description Protocol. RFC-4566. Network Working Group. Category: Standards Track. IETF 2006

[KESS06] Lars Kessner: VoIP-Standards und Migration verschiedener Unternehmensszenarien. Diplomarbeit, Hochschule Bremen, Studiengang: Technische Informatik, Bremen Januar 2006

[PINE07] Pineapple-Projekt: http://www.codename-pineapple.org/start.shtml

[RSC+02] Rosenberg, Schulzrinne, Camarillo, Johnston, Peterson, Sparks, Handley, Schooler: SIP – Session Initiation Protocol. RFC-3261. Network Working Group. Category: Standards Track. IETF 2002

[SKR+02] Srisuresh, Kuthan, Rosenberg, Molitor, Rayhan: Middlebox communication architecture and framework. RFC-3303. Network Working Group. Category: Informational. IETF 2002

[SMS+02] Swale, Mart, Sijben, Brim, Shore: Middlebox Communications (midcom) Protocol Requirements. RFC-3304. Network Working Group. Category: Informational. IETF 2002

[SQC06] Stiemerling, Quittek, Cadar: NEC's Simple Middlebox Configuration (SIMCO) Protocol Version 3.0. RFC-4540. Network Working Group. Category: Experimental. IETF 2006