Bundesamt
für Sicherheit in der
Informationstechnik

VoIPSEC

Studie zur Sicherheit von Voice over Internet Protocol

Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189, 53175 Bonn ▪ Postfach 200363, 53133 Bonn
Tel.: +49 (0) 1888 9582-0 ▪ Fax: +49 (0) 1888 9582-400 ▪ Internet: www.bsi.bund.de

Autoren

André Adelsbach, Institut für Netz- und Datensicherheit Ruhr-Universität Bochum
Ammar Alkassar, Sirrix AG, Homburg (Editor)
Karl-Heinz Garbe, Bundesamt für Sicherheit in der Informationstechnik, Bonn
Mirko Luzaic, Hochschule für Technik und Wirtschaft, Saarbrücken
Mark Manulis, Institut für Netz- und Datensicherheit Ruhr-Universität Bochum
Edgar Scherer, Rechenzentrum der Universität des Saarlandes
Jörg Schwenk, Institut für Netz- und Datensicherheit Ruhr-Universität Bochum
Eduard Siemens, Regionales Rechenzentrum für Niedersachsen, Universität Hannover

Zur Studie beigetragen haben ferner
Rainer Jochem, Oskar Senft, Stephanie Schima, Maik Schmitt (Sirrix AG)

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 (0) 1888 95820
E-Mail: refertatI13@bsi.bund.de
Internet: http://www.bsi.bund.de

Vorwort

Sprach- und Datendienste werden in Zukunft immer stärker miteinander verzahnt sein. Auf diesen Trend stellen sich auch die traditionellen Anbieter von Telekommunikationsanlagen ein. Neue Technologien – wie Voice over IP – lassen innovative Geschäftsmodelle und neue Dienstleistungen entstehen. Von der daraus resultierenden Angebotsvielfalt profitieren die Kunden.

Mit der Verbreitung neuer Systeme erhöht sich aber immer auch das Risiko für Angriffe. Schwachstellen können von potenziellen Angreifern gefunden und unlauter ausgenutzt werden. Voice over IP (VoIP) bildet hierbei keine Ausnahme. Die vorliegende Studie beschäftigt sich daher mit der Sicherheit von VoIP-Systemen. Sie beleuchtet, was bei der Konvergenz von Sprach- und Datendiensten technisch und organisatorisch notwendig ist.

Aufgezeigt werden die Grundlagen der Echtzeitübertragung von Informationen über ein IP-Netz. Ebenfalls betrachtet werden die drei Säulen der IT-Sicherheit, Vertraulichkeit, Integrität und Verfügbarkeit, wobei der Aspekt Verfügbarkeit in vielen Fällen eine besonders wichtige Rolle spielt. Den Vorteilen der VoIP-Technik wird damit eine detaillierte Sicherheitsbetrachtung gegenübergestellt. Ob und inwieweit VoIP eine Alternative zu herkömmlichen Technologien darstellt, muss immer im Einzelfall entschieden werden. Was am Ende zählt ist die Sicherheit – ohne Ausnahme.

Bonn, im Oktober 2005

Dr. Udo Helmbrecht, Präsident des BSI

.

Inhaltsverzeichnis

1. Einführung 9

2. Grundlagen von VoIP 11

2.1 Konzeptionelle Grundlagen 11

2.2 Technische Grundlagen 13

2.3 Signalisierungsprotokolle 14

2.4 Medienübertragungsprotokolle 34

2.5 VoIP-Routing 35

2.6 Sprachdatenübertragung 40

3. Bedrohungsanalyse beim Einsatz von VoIP-Systemen 42

3.1 Definition der Sicherheitsziele 42

3.2 Angriffsklassen 46

3.3 Bedrohungen auf der Netzwerkebene 48

3.4 Bedrohungen auf Anwendungsebene 61

3.5 Spezielle Aspekte: VoIP im WLAN 65

4. Sicherheitsmaßnahmen 71

4.1 Schutzbedarfsfeststellung und Sicherheitsmaßnahmen 71

4.2 Netzdesign 71

4.3 VoIP-Middleware 98

4.4 Endgeräte 100

4.5 Protokolle 101

5. Rahmenbedingungen und gesetzliche Vorschriften 118

5.1 Fernmeldegeheimnis und Datenschutz 118

5.2 Technische Umsetzung von Überwachungsmaßnahmen 118

5.3 Notruf 119

6. Einsatzszenarien und Maßnahmenempfehlungen 120

6.1 Home-Office (Anschluss über ein öffentliches IP-Netz) 120

6.2 Mittlere Unternehmens- und Behördennetze (VoIP im Tertiärbereich) 121

6.3 Standortübergreifende Netze (VoIP im Primärbereich) 124

6.4 Campusnetze (VoIP in allen Bereichen) 126

6.5 Migration in bestehende TK-Systeme 127

6.6 Verschlusssachenkommunikation 129

7. Abschließende Sicherheitsbetrachtung 133

7.1 Fördernde und hemmende Faktoren von VoIP 133

7.2 Entwicklungsperspektiven VoIP-Sicherheit 133

7.3 Fazit 133

8. Abkürzungsverzeichnis/Glossar 135

9. Literaturverzeichnis 137

Anhang A: Tabelle Übersicht Sicherheitsmaßnahmen 142

Anhang B: Begriffserläuterungen Angriffe 144

Anhang C: Informationsstruktur 145

Abbildungsverzeichnis

Abbildung 2.1 H.323 Elemente der ITU-T-Empfehlung 14

Abbildung 2.2 Mit Routern verbundene H.323 - Zone 15

Abbildung 2.3 Registrierung von Gateways am Gatekeeper 16

Abbildung 2.4 Logischer Aufbau des Gateways 16

Abbildung 2.5 Logischer Aufbau eines Terminals 17

Abbildung 2.6 Stark vereinfachter H.323-Rufaufbau 18

Abbildung 2.7 Rufaufbau zweier Terminals über Gatekeeper 18

Abbildung 2.8 Übersicht einer SIP-Kommunikation 20

Abbildung 2.9 Vereinfachter Auf- und Abbau einer SIP-Verbindung 21

Abbildung 2.10 Aufbau von SIP-Nachrichten 22

Abbildung 2.11 Logische Elemente (Endpoint, Call, Connection) eines Media Gateways 23

Abbildung 2.12 Direkte Kopplung von klassischen Systemen mittels MGCP 24

Abbildung 2.13 Kopplung mehrerer MGCP–Systeme mit SIP oder H.323 24

Abbildung 2.14 Auf- und Abbau einer RTP–Sitzung nach MGCP 25

Abbildung 2.15 Media Gateway als logisches System 27

Abbildung 2.16 Übergang in das PSTN durch Zusammenschaltung auf Basis von SS7 28

Abbildung 2.17 Auf- und Abbau einer RTP–Sitzung nach Megaco 29

Abbildung 2.18 Fullheader 31

Abbildung 2.19 Miniheader 31

Abbildung 2.20 Registrierung 31

Abbildung 2.21 Sprachübertragung 32

Abbildung 2.22 RTP-Paket 34

Abbildung 2.23 SRV Record 36

Abbildung 2.24 Beispielhaftes RR-Paar für einen signierten SRV-RR in der ASCII-Darstellung. Für die Übertragung wird ein anderes Format verwendet. 39

Abbildung 3.1 Übergänge zwischen VoIP-Domänen und deren Kostenmodelle 55

Abbildung 4.1 Prinzipieller Aufbau einer VoIP-Netzwerkinfrastruktur mit der Trennung von Sprach- und Datennetz 74

Abbildung 4.2 Redundanzbeispiel durch zwei getrennte Service-Areas 80

Abbildung 4.3 Redundanzbeispiel mit einer Service-Area und Spanning Tree 81

Abbildung 4.4 Beispiel für ein fehlerhaftes Redundanzkonzept 81

Abbildung 4.5 Beispieldesign Firewall in VoIP-Netzen 89

Abbildung 4.6 Beispiel eines Netzwerkes mit NIDS 90

Abbildung 4.7 Full Cone NAT 92

Abbildung 4.8 Restricted Cone NAT 93

Abbildung 4.9 Symetric Cone Nat 94

Abbildung 4.10 Probleme durch NAT für VoIP 95
Abbildung 4.11 MIDCOM-Umgebung 96
Abbildung 4.12 Beispiel für einen Session Border Controller 97
Abbildung 4.13 Blockstruktur einer IPSec-Implementierung. 112
Abbildung 4.14 IPSec ESP im Tunnel-Modus. (* Pad Data besteht aus den Padding-Daten plus die Padding-Längenangabe und dem Next Header-Feld) 114
Abbildung 4.15 IKE Main Mode in 6 Nachrichten, Authentifizierung durch X.509-Zertifikat und digitale Signatur. 116
Abbildung 4.16 Der Quick Mode bei IKE. Hier werden keine Public-Key-Operationen benötigt. 116
Abbildung 6.1 Einsatzbeispiel Home-Office 120
Abbildung 6.2 Einsatzbeispiel VoIP in Telefonieanwendungen mittlerer Gröβe 123
Abbildung 6.3 Einsatzbeispiel Kopplung von Standorten 125
Abbildung 6. 2 Einsatzbeispiel Campusnetz 127
Abbildung 6. 2 Migration in bestehende TK-Systeme 128
Abbildung 6.6 Einsatzbeispiel bei hoher Vertraulichkeit 129

1. Einführung

Die Übertragung von Sprache über IP-Netze, das „Voice-over-IP“ oder kurz VoIP, ist einer der derzeit am schnellsten wachsenden Bereiche in der Telekommunikation.

Wichtigste Triebfeder ist dabei die Konvergenz der TK- und IT-Netze und die damit verbundenen Einsparpotenziale. Synergieeffekte ergeben sich durch eine gemeinsame Nutzung der Infrastruktur, beispielsweise eines firmeninternen Backbone-Netzes, durch eine einheitliche Netzwerktechnik und nicht zuletzt im personellen Bereich. Bisher separat betriebene Telekommunikation- und IT-Netzinfrastrukturbereiche können unter Kosteneinsparung zusammengefasst werden, auch bei der externen Wartung und bei der Geräte-Beschaffung werden Kostenvorteile sichtbar.

Technologisch zeichnet sich eine starke Tendenz zu einer universellen Nutzung des Internet Protokolls „IP“ ab. Unter den Stichwörtern Everything-over-IP und IP-over-Everything gewinnt IP als einheitliches Protokoll der Vermittlungsschicht, das im Wesentlichen Aufgaben der Adressierung übernimmt, überragende Bedeutung. Zunehmend werden auch echtzeitkritische Anwendungen, beispielsweise im taktischen Bereich oder bei Steuerungs- und Kontrollaufgaben auf IP migriert. Die bisherigen leitungsvermittelnden Netze, werden aufgrund ihrer geringen Flexibilität immer weiter zurückgedrängt.

Ziel dieser Studie ist es, Bedrohungspotenziale bei der Nutzung von VoIP darzustellen und geeignete Sicherheitsmaßnahmen aufzuzeigen. Diese Studie soll auch zeigen, dass die verlässliche Einführung von VoIP nicht durch einfaches Anschließen eines VoIP-Servers und von IP-Telefonen an ein bestehendes Datennetzwerk realisiert werden kann.

Wie einfach beispielsweise VoIP-Gespräche abzuhören sind, zeigen die weit verbreiteten und auch für technisch Unversierte einfach zu bedienenden Werkzeuge wie Vomit (Voice over missconfigured Internet phones, [Vomit]) mit deren Hilfe der Sprachdatenanteil eines Netzwerkdatenstroms von Unbefugten „mitgehört“ werden kann. Für den bekannten Ethernet-Sniffer Etherreal gibt es bereits Plugins zur Auswertung von SIP und H.323 Signalisierungsnachrichten mit denen sich Signalisierungsinformatinen wie Ziel und Quelladresse abhören lassen. Dabei erschweren strukturierte und geswitchte Netze den direkten Zugriff auf die Kommunikationsdaten, können aber ohne umfangreiche Sicherheitsmaßnahmen die vielfältigen Angriffe nicht unterbinden.

Weitere Gefährdungspotenziale ergeben sich durch unpräzise oder nicht sorgfältige Implementierungen bei den Geräteherstellern. Ein gefährliches Beispiel unzureichend implementierter Sicherheitsmaßnahmen zeigt der folgende Fall: Ein Hersteller bringt ein neues IP-Telefon auf den Markt, das über integrierte Verschlüsselung des Medienstroms mittels SRTP verfügt. Die Verschlüsselung ist über eine entsprechende Option einfach zu aktivieren. Unerwähnt bleibt jedoch, dass der zur Verschlüsselung des Medienstroms eingesetzte Schlüssel zu Beginn einer Verbindung im Klartext ausgetauscht wird. Die Einrichtung eines gesicherten Schlüsselaustauschs ist zwar möglich, erfordert neben tiefer technischer Fachkenntnis einen erheblichen Aufwand. So wird dem Anwender fälschlicherweise ein Gefühl der Sicherheit vermittelt. Dieses kann einen größeren Schaden anrichten, als das Wissen des Anwenders um mögliche Risiken.

Jede neue Technologie birgt neben Chancen auch neue Bedrohungen und Risiken. Die Aufgabenstellung zur Absicherung der VoIP-Technologie wird es sein, die Bedrohungen zu analysieren und zu quantifizieren, die Risiken zu bewerten und einen vertretbaren Ausgleich zwischen den erforderlichen Sicherheitsmaßnahmen und dem eingebrachten Aufwand zu halten. Einen geeigneten methodischen Ansatz hierfür liefert das vom BSI herausgegebene Grundschutzhandbuch (GSHB) und das Grundschutz-Tool (GS-TOOL).

In diesem Zusammenhang ist es Ziel dieser Studie,

- IT-Verantwortlichen einen praktischen Leitfaden an die Hand zu geben, der ihnen bei der Einführung eines VoIP-Systems Risiken aufzeigt und typische Sicherheitsmaßnahmen benennt und erläutert,

- Entscheidungsträgern denkbare Einsatzszenarien aufzuzeigen und mögliche Maßnahmen zur Gewährleistung eines verlässlichen VoIP-Systems zu skizzieren, um dadurch im Vorfeld den Aufwand zu einem verlässlichen IP-basierten Telefoniesystem besser abzuschätzen zu können,
- Hersteller und Entwickler von VoIP-Komponenten zu sensibilisieren und aufzuzeigen in welchen Bereichen Defizite in den Implentierungen der Sicherheitsmaßnahmen sind,
- der interessierten (Fach-)Öffentlichkeit einen Überblick über die technischen Grundlagen, die möglichen Einsatzszenarien sowie über die Bedrohungen, die sich im Zusammenhang mit dieser Technologie ergeben.

Die umfassende Analyse von VoIP-Sicherheit steht noch weitestgehend am Anfang. Viele VoIP-spezifische Bedrohungspotenziale werden erst nach und nach aufgearbeitet und wissenschaftlich und technisch bewertet werden.

In diesem Zusammenhang versteht sich diese Studie als erster Schritt zur Bewertung der Sicherheit im VoIP, die durch zukünftige Arbeiten fortzuschreiben ist.

Im weiteren Verlauf dieser Studie werden mit VoIP alle Anwendungen bezeichnet, bei denen Sprache über ein IP-basiertes Netz übertragen wird. Die Übertragung von Sprache über öffentliche Netze, die „Internet-Telefonie“ spielt in der vorliegenden Studie eine untergeordnete Rolle (z. B. bei der Anbindung von Heimarbeitsplätzen). Im Mittelpunkt steht die Intranet-Telefonie, die VoIP in Netzen definiert, die vollständig im Verantwortungsbereich des Betreibers stehen.

In Abgrenzung zum paketorientierten IP, wird die bisherige, leitungsvermittelnde Telefonie unter dem Begriff Time-Division Multiplexing, kurz TDM, zusammengefasst. TDM ist das übliche Verfahren zur Bereitstellung mehrerer Kanäle über eine einzelne Übertragungsleitung in leitungsvermittelnden Festnetzen.

2. Grundlagen von VoIP

2.1 Konzeptionelle Grundlagen

Sprachtelefonie über IP-basierte Netze, „Voice-over-IP“ oder kurz VoIP, unterscheidet sich von der heute vorherrschenden Sprachtelefonie in leitungsvermittelnden Netzen in Konzeption und Systematik. Dies führt auch dazu, dass sich die Sicherheitsbetrachtung von VoIP-Systemen erheblich von denen traditioneller Telekommunikation abgrenzt.

In diesem Kapitel wird zunächst die Systematik von VoIP in Abgrenzung zur traditionellen Telefonie erläutert und im Anschluss die derzeit typischen Anwendungsszenarien aufgeführt.

2.1.1 VoIP Systematik

Grundlage von VoIP ist die Übertragung von Sprache über das Internetprotokoll (IP), [RFC791]. Das IP ist ein verbindungsloses Schicht 3 (Vermittlungsschicht) Protokoll.

Im Gegensatz zur bisherigen Telefonie, bei der eine transparente Verbindung mit fester Bandbreite auf der Schicht 2 durch das Übertragungsprotokoll bereitgestellt wird, erfolgt die Vermittlung der Telefoniedaten paketorientiert. Typische Probleme wie Synchronisationsfehler und Framedrops (Verlust einzelner kurzer Datenframes), wie sie in Netzen, die auf der Synchronous Digital Hierachy (SDH) basieren, auftreten können, gibt es in IP-Netzen nicht. Hingegen tauchen neue Probleme wie Delay und Jitter sowie durch den Verlust größerer Datenpakete auf, die im TDM unbekannt sind, und die bei den Sicherheitsmaßnahmen zu berücksichtigen sind.

Die Vermittlung der Sprachdaten erfolgt in den bisherigen Telefonienetzen sitzungsorientiert und außerhalb des Sprachkanals (out-of-band). Sobald eine Verbindung beispielsweise bei ISDN über den D-Kanal signalisiert und vermittelt wurde, stellt das Telefonienetz dem Endgerät einen festen Kanal zur Sprachübertragung bereit. Bei der Übertragung von Sprache über IP, erfolgt die Gesprächssignalisierung ebenfalls out-of-band, allerdings wird dem Endgerät kein Kanal zugewiesen, sondern im Allgemeinen die Zieladresse des Gegenteilnehmers. Jedes einzelne Sprachpaket enthält daher eine Zieladresse und wird separat vermittelt.

Insgesamt ist der Protokoll-Overhead bei VoIP um ein Vielfaches höher als in TDM-Netzen. Während beispielsweise bei ISDN die kodierten Sprachdaten unmittelbar auf Schicht 1 des Übertragungskanals aufsetzen, liegen bei VoIP mehrere Protokollschichten dazwischen, die jeweils zusätzlichen Overhead erzeugen. Typischerweise durchlaufen dort die kodierten Sprachdaten das RTP (Real-Time Protocol), UDP (User Datagram Protocol), IP und Ethernet, der Protokolloverhead beträgt dabei etwa 60 Bytes, bei Verwendung eines Codecs wie G.729 liegt die Nutzdatengröße bei 20-40 Bytes.

Für die Sicherheitsbetrachtung relevant ist weiterhin, dass in bisherigen Telefonsystemen die Teilnehmerzuordnung Port-gebunden ist. Jedes Endgerät ist einem definierten Port der Vermittlungsstelle bzw. der Telekommunikationsanlage zugewiesen und physikalisch mit dieser verbunden. Eine zusätzliche Authentifikation findet nicht statt. In IP-Netzen hingegen geschieht die Teilnehmerzuordnung grundsätzlich über die IP-Adresse (bzw. MAC-Adresse), die authentische Zuordnung muss daher über zusätzliche Mechanismen explizit erfolgen.

Im Gegensatz zum ISDN, das als dienstintegrierendes Netz als Ersatz der damaligen analogen Sprachnetze entwickelt worden ist, sind die IP-basierenden Netze vorrangig zur Datenkommunikation entstanden. Daten- und Telefonienetze unterscheiden sich in der Praxis hinsichtlich der an sie gestellten expliziten und impliziten Sicherheitsanforderungen. Insbesondere die Übernahme von Telefonie-Diensten in ein bisher nach den Anforderungen der Datenkommunikation betriebenes Netz stellt daher eine große Herausforderungen dar.

Obwohl die Anforderungen im TK-Bereich in der Praxis meist höher sind als in den Datennetzen (in der gleichen Institution), wird vielfach übersehen, dass ein nicht unerheblicher Teil der

angenommenen Sicherheit nicht auf einem modernen Sicherheits-Engineering basiert, sondern auf dem Einsatz proprietärer, nicht-offener Systeme beruht. Diese Sicherheit „by obscurity“ ist kein verlässlicher Schutz, insbesondere bei höherem Schutzbedarf. Hinzu kommt, dass auch traditionelle TK-Anlagen heute aus einem ganzen Serverpark unterschiedlicher Systeme bestehen, die über IP-Netze kommunizieren und den gleichen Gefährdungen unterliegen, wie ihnen auch herkömmliche Serversysteme ausgesetzt sind, die aus dem eigentlichen Wirknetz aus Sicherheitsgründen getrennt sein sollten. Auch bei den Endgeräten findet man einen grundsätzlichen Unterschied: Im Gegensatz zu den mit wenig Intelligenz ausgestatteten analogen oder ISDN-Endgeräten, basieren heutige VoIP-Telefone auf herkömmlichen Rechnerplattformen, meist mit regulären Betriebssystemen wie Windows CE oder Linux. Dies führt zusammen mit komplexeren und vielfältigeren Protokollen zu einem höheren Bedrohungspotenzial durch fehlerhaften oder bösartigen Code. Ganz zu schweigen von einer fehlerhaften Konfiguration.

2.1.2 VoIP-Anwendungsszenarien

Für die Sprachübertragung über IP und/oder VoIP gibt es unterschiedliche Anwendungsszenarien. Das Bedrohungspotenzial und die Sicherheitsanforderungen sind dementsprechend ebenfalls unterschiedlich. Im Folgenden werden derzeit typische Anwendungsfälle dargestellt.

Einsatz von VoIP im Endgeräteanschlussbereich

Die sichere Umstellung der Sprachkommunikation auf IP in Firmen- und Behördennetzen (Local Area Network, LAN) gehört zu den wichtigsten Herausforderungen im Bereich des VoIP und bietet das derzeit interessanteste Nutzen-Potenzial dieser Technologie.

Dies umfasst – vollständig oder auch nur komponentenweise – den Einsatz von IP-Telefonen, eines LAN-basierten Telekommunikationssystems (die Vermittlungs- und Mehrwertfunktionen übernimmt sowie die Verbindung in die Außenwelt sicherstellt) und eines IP-Netzes zur Verbindung von Endgerät und TK-Anlage. Die Verbindung in das digitale Fernsprechnetz kann dabei über lokale Gateways oder über einen VoIP-Provider erfolgen. Bei so genannten „hybriden Anlagen“ werden in herkömmliche TK-Anlagen VoIP-Baugruppen integriert, die den Anschluss von IP-Telefonen, meist proprietäre Systemtelefone, ermöglichen.

Ziel dabei ist die Integration der Daten- und Telefonienetze. Den substanziellen Einsparungen in Leitungen, Netzkomponenten, Management, Administration und Wartung stehen allerdings eine Vielzahl zusätzlicher Bedrohungen gegenüber, denen Rechnung zu tragen ist. Dies relativiert einen Teil der Einsparpotenziale, insbesondere bei der Anpassung eines vorhandenen Datennetzwerkes für den VoIP-Einsatz, erscheint jedoch als zwingende Voraussetzung für den sicheren und verlässlichen Einsatz dieser Technologie.

Diese Studie konzentriert sich auf die beschriebene Anwendung von VoIP, da hier sowohl Umsetzungspotenzial als auch das Bedrohungspotenzial am größten ist.

Einsatz von VoIP im Backbone-Bereich

Die heutigen digitalen Telefonienetze („Fernsprechnetze") bestehen hauptsächlich aus einem hierarchisch angeordneten TDM (Time Division Multiplex) Netzwerk. In Deutschland kommt dabei teilnehmerseitig das Integrated Digital Services Network (ISDN) zum Einsatz, überwiegend in Form von PDH-Kanälen (Plesiochronous Digital Hierarchy, nx64 kBit/s oder 2MBit/s E1). Die Signalisierung erfolgt dabei über einen separaten Kanal (D/E-Kanal).

Das Backbone ist dabei als SDH (Synchronous Digital Hierarchy) aufgebaut, welche u.a. über ATM-Strecken betrieben wird. Die Signalisierung zwischen den Vermittlungsstellen erfolgt über das SS7-Protokoll.

Die Einführung von IP als zusätzliche Übertragungsschicht bietet Vorteile im Netzwerkmanagement und im einheitlichen Netzaufbau konvergenter Netze. In den USA haben beispielsweise bereits zahlreiche große Carrier den Transport im Backbone in ihren Telefonienetzen auf IP umgestellt.

Allerdings ist zum jetzigen Zeitpunkt noch nicht abzusehen, wie sich die zukünftigen Core-Netze im Bereich der Sprachtelefonie entwickeln werden. Alternativen Technologien wie Voice over Wavelength Divison Multiplexing (WDM) oder dem Voice over Multiprotocol Label Switching (MPLS) werden in großen Backbone-Netzen derzeit höhere Chancen eingeräumt als Technologien mit einer IP-Zwischenschicht wie VoIP over MPLS.

Einsatz von VoIP zur Anlagen-Kopplung

Eine bei mittelständischen Unternehmen zunehmend realisierte Anwendung von VoIP ist die Kopplung von lokalen Telekommunikationsanlagen (Trunking) über IP-basierte Verbindungen. Dabei werden traditionelle TK-Anlagen an verschiedenen Standorten unter Nutzung eines WAN-Datennetzes gekoppelt. Traditionell werden Anlagen überwiegend über separate Wähl- oder Standleitungen miteinander verbunden. Das WAN-Datennetz ist dabei meist über zusätzliche separate Leitungen realisiert. Die Zusammenführung von Telefonie- und Datennetz in der Standortvernetzung bietet dabei erhebliche Flexibilität, eine effizientere Bandbreitennutzung und damit auch ein Einsparpotenzial.

Alternative Protokolle zur effizienten Bandbreitenverwaltung, wie das ATM, das in diesem Fall besser auf die Bedürfnisse der Dienste eingeht, werden zunehmend zugunsten von IP verdrängt. Insbesondere die deutlich geringeren Kosten für die Netzkomponenten sind hierfür ausschlaggebend.

Einsatz von VoIP zur Internettelefonie

Die Sprachübertragung über öffentliche IP-Netze, dem „Internet“, erfreut sich im privaten Bereich immer größerer Beliebtheit. Die zunehmend größeren Bandbreiten im Backbone- und Endanschlussbereich, mit einer mittlerweile akzeptablen Sprachqualität, haben die Internet-Telefonie auch für die breite Masse der Internet-Nutzer interessant gemacht.

Dabei werden vornehmlich Smart-Phone-Clients eingesetzt, die meist – ähnlich zu Messaging-Diensten – über zentrale Verzeichnisse registriert sind. Zunehmende Verbreitung finden kompakte low-budget VoIP-Gateways, die es ermöglichen mit herkömmlichen Telefonen (analog oder ISDN) Internet-Telefonie-Dienste zu nutzen.

Für den professionellen Einsatz in Unternehmen und Behörden ist die Sprachübertragung über öffentliche, nach dem Best-Effort-Prinzip betriebene, IP-Netze derzeit jedoch nicht vertretbar, und wird in der Praxis auch nicht realisiert.

Die VoIP-Sicherheit für Anwendungen der Internettelefonie wird daher in dieser Studie nicht im Einzelnen beleuchtet.

2.2 Technische Grundlagen

Das Kapitel behandelt die grundlegende Telefonsignalisierung der wichtigsten Übertragungsprotokolle. Es beginnt mit einem Überblick über die H.323-Protokollfamilie, SIP (Session Initiation Protocol), MGCP und Megaco, sowie über einige proprietäre Protokolle wie SCCP und IAX. Der Abschnitt Medien-Übertragungsprotokolle beschreibt die Protokolle RTP und das verschlüsselte Protokoll SRTP sowie das Kontrollprotokoll RTCP. Im Anschluss daran werden Routing-Protokolle, DNS, SRV, TRIP und ENUM vorgestellt. Das Grundlagenkapitel schließt mit der Kodierungsbetrachtung ab. Für nähere Informationen zu den einzelnen Protokollen wird auf folgende Fachliteratur verwiesen [SiGe02, BaAn01, AuAn01].

2.3 Signalisierungsprotokolle

2.3.1 Übersicht und Einführung in H.323

Der H.323-Standard [ITUT03b] wurde von der ITU-T entwickelt und beschreibt die Übertragung von Echtzeitverbindungen (Video, Audio, Daten) in paketorientierten Transportnetzen. Das Protokoll wird seit 1996 kontinuierlich weiter entwickelt, so dass heute zwischen fünf H.323-Versionen unterschieden wird. Eine H.323-Verbindung unterteilt sich in Verbindungsaufbau, Verbindungsabbau und die Datenphase (Versenden der Datenpakete mit Video-, Audio- oder Faxdaten). Audio- und Videodaten werden per UDP, Faxdaten per UDP oder TCP übertragen. Vor der Übertragung von Echtzeitdaten werden so genannte logische RTP- und RTCP-Kanäle zwischen den Endpunkten (Terminals) aufgebaut. In H.323 Version 2 wurde bereits das so genannte Fast Connect eingeführt, um die Verbindungsaufbauzeit zu reduzieren. H.323 beschreibt den Rahmen der Signalisierungsprotokolle H.225.0 [ITUT03a] (basierend auf dem ISDN D-Kanal Protokoll Q.931) und H.245 [ITUT05], sowie für die Übertragung von Echtzeitinformationen mit den IETF-Protokollen RTP (Real Time Protocol) [RFC1889] und RTCP (Real Time Transport Protocol). Dabei muss das paketorientierte Transportnetz selbst kein „Qualtity of Service“ (QoS) garantieren. Um verschiedene ISDN-Dienstmerkmale in H.323 zu realisieren, werden in dem H.450-Standard [ITUT98] ergänzende Dienstmerkmale definiert.

H.323 definiert Gateways, um verschiedene Arten von Netzen für die Sprachkommunikation zu verbinden. Als Media Gateway-Protokoll (Megaco) wird H.248 bevorzugt.

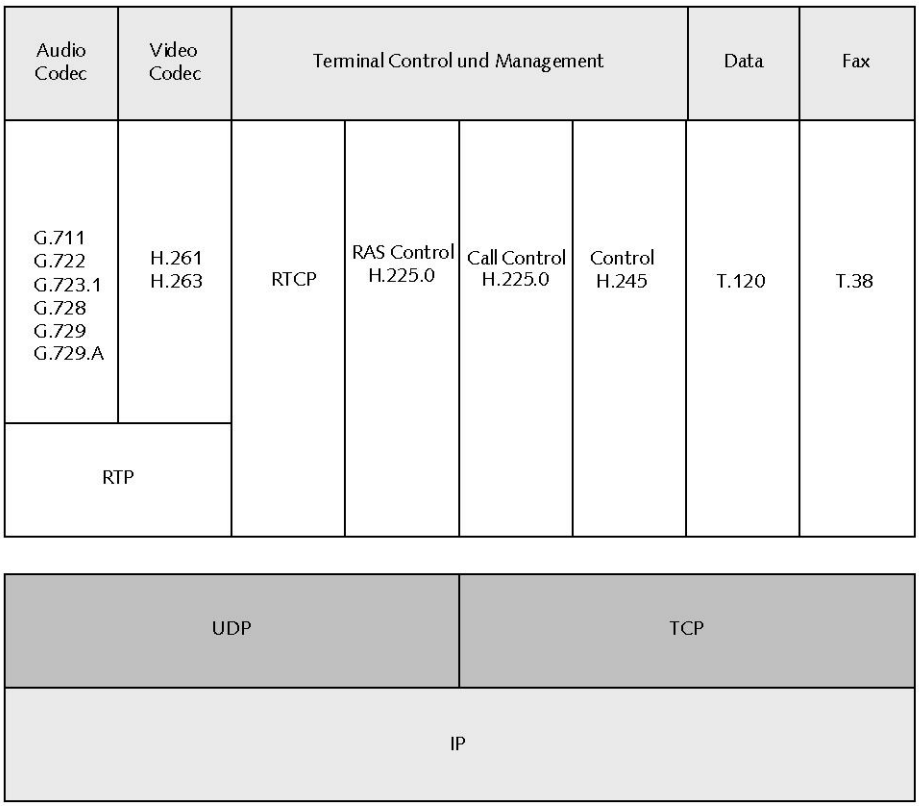

Abbildung 2.1 H.323 Elemente der ITU-T-Empfehlung

Systemarchitektur

Der H.323-Standard sieht Terminals und zu deren Unterstützung optional Gateways, Gatekeeper und MCUs (Multipoint Control Unit) vor. Terminals können direkt miteinander verbunden sein, wenn deren Adressen bekannt sind. Andernfalls wird ein Gatekeeper zur Verwaltung der zugehörigen Adressinformationen benötigt. Daneben übernimmt er die Aufgaben einzelne Zonen zu verwalten und Adressinformation (Aliases) zu übersetzen. Optional kann eine Multipoint Control Unit (MCU) eingesetzt werden. Diese unterstützt Mehrpunktverbinden. Die Gateways realisieren die Übergänge in andere Netzwerke und nehmen dabei die Anpassung der Nutzdaten und der Signalisierungsinformation vor.

Gatekeeper

Eine direkte Verbindung zwischen den Endgeräten kann nur bei bekannter IP-Adresse hergestellt werden. Da sich die Zieladressen im Netzwerk durch Umkonfigurationen ständig ändern, ist diese Art der Verbindungsaufnahme unpraktikabel. Um dem Rechnung zu tragen, ist im H.323-Standard die Funktion eines Gatekeepers vorgesehen. Seine wichtigsten Aufgaben sind:

- Registrierung und Verwaltung von Terminals, MCUs und Gateways
- Zone-Management, d.h. Zuordnung von Terminals, MCUs und Gateways zu einer Zone
- Call Authorization. Optional kann der Gatekeeper Verbindungen generell erlauben, oder unter gewissen Randbedingungen ablehnen
- Adressübersetzung für MCUs und Gateways
- Bearbeitung von „Dienstmerkmalen“
- Bandbreitensteuerung .

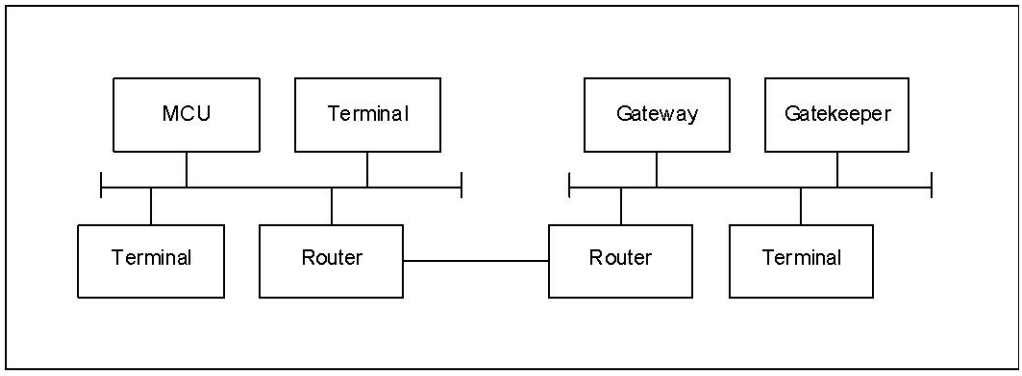

Abbildung 2.2 Mit Routern verbundene H.323 - Zone

Registrierung, Admission and Status (RAS)

- Zur Registrierung senden H.323-Endpunkte einen Register Request (RRQ) zum Gatekeeper. Der Gatekeeper sendet bei erfolgreicher Registrierung eine Register Confirmation-Nachricht (RCF) zurück. Im Fall einer Ablehnung sendet der Gatekeeper ein Registration Reject (RRJ) an den H.323-Endpunkt zurück.

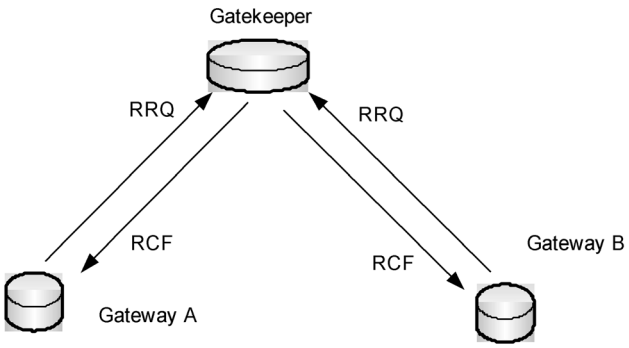

Abbildung 2.3 Registrierung von Gateways am Gatekeeper

Gateways

Gateways passen in einem H.323-System die Nutzdaten (Sprachen, Video, Daten) und die Signalisierung der jeweiligen Netze einander an. Die Gateways stellen die Übergänge in andere Netze bereit und sind gleichzeitig die Endpunkte der Kommunikation für Partnerinstanzen.

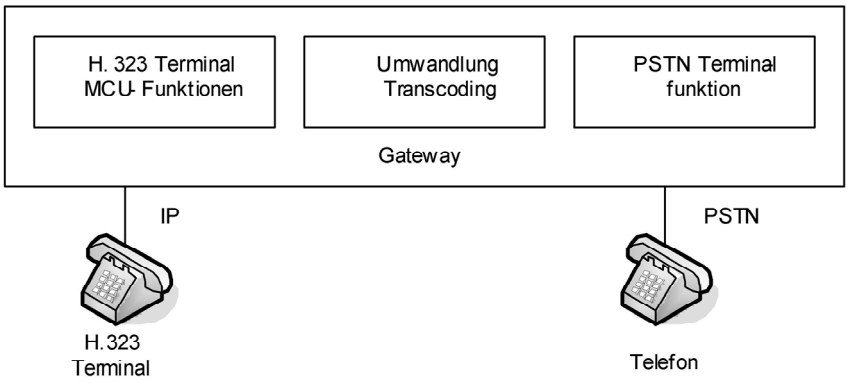

Abbildung 2.4 Logischer Aufbau des Gateways

Terminals

Die Terminals stellen die Endpunkte einer H.323-Kommunikation dar. Der H.323-Standard setzt eine minimale Konfiguration voraus; das sind die Control Unit für die Bearbeitung des H.225.0-Layer, eine Audio-Codec-Unit nach G.711-Standard mit den Codecs A-Law und u-Law und ein Netzwerkinterface.

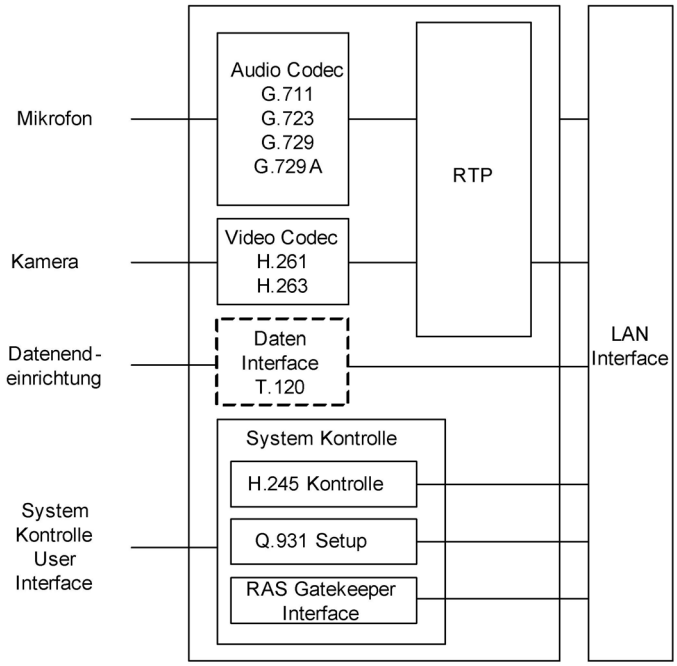

Abbildung 2.5 Logischer Aufbau eines Terminals

H.323-MCU (Multipoint Control Unit)

Um Konferenzen mit mehreren Teilnehmern führen zu können, ist eine zentrale Konferenz-Steuerungsinstanz unentbehrlich. In der MCU laufen sämtliche Medienströme von den Teilnehmern zusammen. Für die Verwaltung der Konferenzteilnehmer wird ein H.323-Gatekeeper benötigt, der die Signalisierung zwischen den H.323-Endgeräten und der MCU steuert.

Signalisierung

H.323 unterscheidet zwischen den Protokollen Call Control (H.225.0) und Bearer Control (H.245). Der H.225-Steuerungskanal entspricht in großen Teilen dem ISDN D-Kanal-Protokoll bei ISDN. Mit H.225.0 wird ein Anrufsignalisierungskanal zwischen den Instanzen über eine TCP-Verbindung hergestellt. Über den H.225.0-Signalisierungskanal werden dann die Informationen für den Aufbau des H.245-Steuerkanals zwischen den Endpunkten (Terminals) ausgetauscht. Der H.245-Kanal dient der Aushandlung der Parameter der Medienströme (RTP-Kanäle).

Beim direkten Aufbau muss dem Initiator die Netzadresse des Zielsystems bekannt sein, andernfalls wird ein Gatekeeper benötigt. Die Signalisierung nach H.323 besteht aus mehreren Einzelschritten:

- Registrierung am Gatekeeper über das RAS-Protokoll (Registration, Admission and Status). Der Nachrichtenaustausch zwischen Gatekeeper und Terminal erfolgt über UDP.
- Wie aus der untenstehenden Abbildung zu ersehen ist, wird die Verbindung von dem Terminal A mit der H.225-Signalisierung eingeleitet. Die Nachricht wird vom Terminal B mit der Nachricht Call Proceeding bestätigt. Falls die Verbindung vom Gatekeeper angenommen wird und beide Terminals sich auf gleiche Audio- und Videoformate geeinigt haben, bestätigt das Terminal B dies mit der H.225.0-Nachricht Alerting.
- Wird der Anruf von B angenommen sendet das Terminal B eine H.225.0-Nachricht Connect. Damit ist der H.245-Steuerkanal aufgebaut und Terminal A zeigt dies an.
- Anschließend werden die logischen Kanäle RTP und RTCP für die Übertragung von Mediendaten aufgebaut.

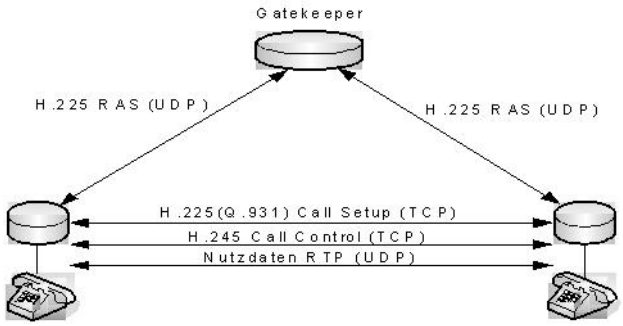

Abbildung 2.6 Stark vereinfachter H.323-Rufaufbau

Das folgende Beispiel zeigt den Signalisierungsfluss zwischen zwei Teilnehmern und einem gemeinsamen Gatekeeper. Beide Teilnehmer sind beim Gatekeeper registriert.

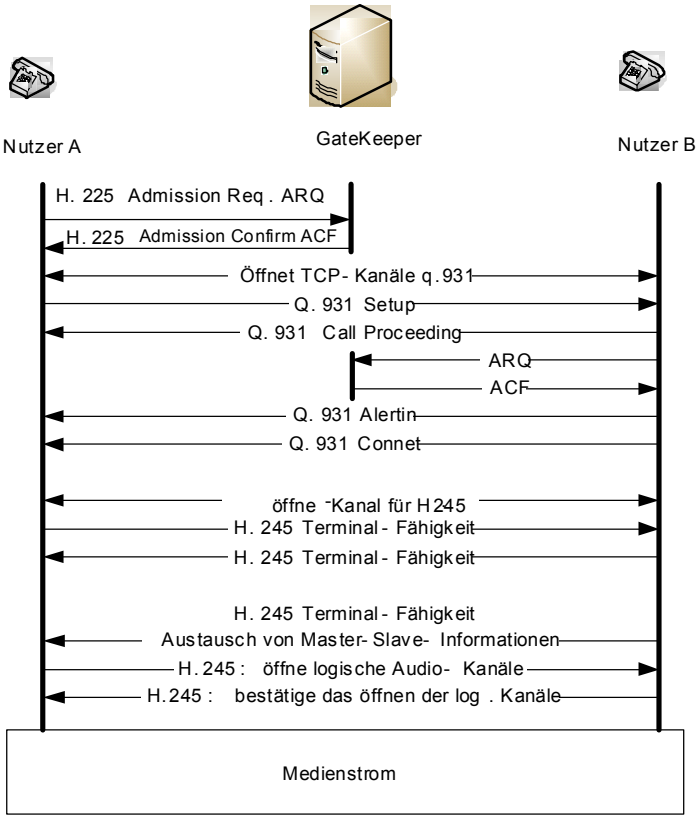

Abbildung 2.7 Rufaufbau zweier Terminals über Gatekeeper

Teilnehmer A leitet mit Admission Request ARQ über den TCP-Port 1720 den Verbindungsaufbau ein. Die Bestätigung erfolgt vom Gatekeeper mit Admission Confirmation ACF. Daraufhin wird das Call Processing (Öffnen der Q.931-Kanäle) zwischen den Teilnehmern A und B abgehandelt. Der H.225-Verbindungsaufbau wird mit dem anschließenden Q.931 Alerting und Q.931 Connect abgeschlossen. Es folgt nun der Aufbau der logischen H.245-Kanäle. Innerhalb des H.245-Aufbaus werden verschiedene Eigenschaften ausgehandelt, z. B. wie viel Frames pro RTP-Nachricht übertragen werden, Sprachpausenerkennungsinformation, welche UDP-Adressen und Port-Nummern für das Senden der RTCP-Daten benutzt werden, Übermittlungsart, wie Audio, Video oder Daten, usw.. Anschließend werden über UDP mit RTP und RTCP die Nutzdaten transportiert. Das Lösen einer Verbindung erfolgt mit der H.245-Nachricht CloseLogicalChannel.

2.3.2 Einführung in das Session Initiation Protocol (SIP)

SIP ist ein textbasierendes Client/Server-Sitzungssignalisierungsprotokoll des IETF (Internet Engineering Task Force), das zur Steuerung des Verbindungsauf- und -abbaus von Multimediadiensten verwendet wird. Aktuell liegt es in der Version 2.0 vor und wird im RFC 3261 [RFC3261] beschrieben.

Aufgrund seines im Vergleich zu H.323 einfacheren Aufbaus erfährt es immer größere Verbreitung. Es ist nicht nur für VoIP ausgelegt, sondern wird bei Videokonferenzen, Instant Messaging, verteilten Computerspielen und anderen Applikationen eingesetzt. Sein Adressierungsschema ähnelt stark dem einer E-Mail-Adresse (sip:m.mustermann@provider-name.org). In UMTS-Netzen wird künftig SIP verwendet. SIP unterstützt Punkt-zu-Punkt- und Punkt-zu-Mehrpunkt-Verbindungen.

Beim Einsatz von SIP in Firewall- bzw. NAT-Umgebungen sind einige Besonderheiten zu beachten. Wichtige Protokollinformationen (IP-Adresse, Portnummer) für den Transport des Medienstromes werden innerhalb des SIP-Bodies zwischen den Endsystemen ausgetauscht. Dadurch kann ein übertragenes SIP-Signalisierungspaket eine andere IP-Quelladresse im IP-Paket aufweisen als die im SIP-Body bekannt gegebene IP-Quelladresse.

Systemarchitektur

UA – User Agent

Die Endsysteme (Telefon, Softphone, Gateway) werden als User Agents (UA) bezeichnet. Ein User Agent kann die Rolle eines Clients bzw. eines Servers einnehmen. Der Initiator eines Gesprächs arbeitet als User Agent Server, der Gerufene als User Agent Client. Ein SIP-Endsystem beinhaltet immer beide Funktionen.

Registrar

Ein User Agent meldet sich mit einer Kennung (Benutzername, Kennwort) und seiner SIP URI (SIP-Adresse) an einem Registrar (Server) an und gibt dadurch seine Adresse (IP–Adresse) bekannt, unter der er öffentlich erreichbar ist. Aufgrund dieser Registrierung kann ein User Agent lokalisiert werden. Oftmals wird der Registration-Server zusammen mit einem Proxy-Server bzw. einem Redirect-Server auf einem Serversystem betrieben.

Proxy-Server

Ein SIP-Proxy nimmt die Rolle eines Vermittlers ein, der die Signalisierungsnachrichten bearbeitet oder weiterleitet. Ein User Agent sendet eine Anfrage an den SIP-Proxy. Der SIP-Proxy interpretiert die Anfrage und adressiert sie, nach entsprechender Bearbeitung, an den User Agent. Wenn nötig wird eine Nachricht durch den SIP-Proxy verändert.

Es können zustandslose (stateless) und sitzungsorientierte (stateful) SIP-Proxy-Server unterschieden werden. Bei zustandslosen SIP-Proxy-Servern werden keine Sitzungszustände („session states“) gespeichert. Alle REQUESTs bzw. RESPONSEs werden unabhängig voneinander bearbeitet. Sitzungsorientierte SIP-Proxy-Server speichern die Zustände einer Sitzung in so genannten Transaktions-Kontrollblöcken. Dadurch können bei der Adressierung mehrere Endpunkte – man spricht hier von Gabelung (forking) – nach einer Antwort (OK) eines Endsystems von der weiteren Bearbeitung einer Anfrage (CANCEL) ausgeschlossen werden. Die Zuständigkeit eines SIP-Proxy-Servers kann sich auf eine oder mehrere Domänen erstrecken.

Location-Server

Die Daten aus dem Registrierungsvorgang werden von dem Registrar-Server in einer Datenbank auf dem Location-Server abgelegt.
Im Proxy-Modus kontaktiert der SIP-Proxy (SIP Proxy A) des rufenden User Agents den für die Domäne des Ziel User Agents verantwortlichen SIP-Proxy (SIP Proxy B). Der SIP Proxy B ermittelt über seinen Location-Server die Zieladresse des gerufenen User Agents.

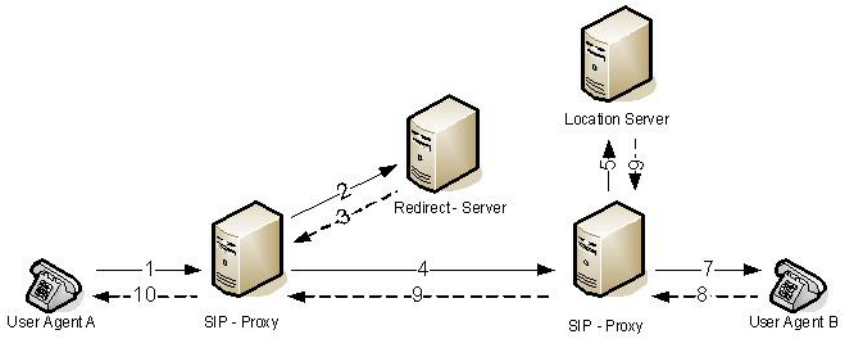

Abbildung 2.8 Übersicht einer SIP-Kommunikation

1. Der User Agent A sendet ein INVITE an den SIP-Proxy.
2. Der SIP-Proxy richtet diese Anfrage an den für die Domain der Zieladresse zuständigen Server.
3. Da der User Agent B temporär außerhalb seiner Heim-Domain erreichbar ist, erhält der SIP-Proxy eine Antwort mit der neuen URI.
4. Der Proxy richtet nun die INVITE–Nachricht an den zuständigen Ziel-Proxy.
5. Der Ziel-Proxy fragt den Location-Server nach der Lokation des User Agent B ab.
6. Der Location-Server übermittelt die benötigten Informationen an den SIP-Proxy.
7. Der SIP-Proxy sendet die Nachricht an den User Agent B.
8. Der User Agent antwortet an den SIP-Proxy.
9. Der SIP-Proxy leitet die Antwort an den ursprünglichen SIP-Proxy.
10. Über den ursprünglichen SIP–Proxy gelangt die Antwort an den User Agent A.

Signalisierung

SIP ähnelt stark dem HTTP. SIP bedient sich des UDP und TCP. Bevorzugtes Transportprotokoll ist UDP. In beiden Fällen wird zur Signalisierung standardmäßig die Port-Nummer 5060 verwendet.

Der Austausch von Nachrichten erfolgt mit Anfragen (REQUESTs) und Antworten (RESPONSEs). Anfragen werden als *Methods* bezeichnet. Nachfolgende Abbildung zeigt den vereinfachten Verlauf eines Auf- und Abbaus einer SIP-Verbindung.

Ein User Agent mit der Adresse sip:nutzer_a@standort_a.de beginnt den Verbindungsaufbau mit einem INVITE-Request an den SIP-Proxy. Der SIP-Proxy antwortet mit einem TRYING-Response. Diese Statusmeldung 100 (Trying) signalisiert dem rufenden User Agent, dass der SIP-Proxy die Anfrage bearbeitet und anstelle des User Agents die Nachricht an den Ziel-User Agent routet. Hierfür bedient sich der Proxy eines Location-Servers, der die Adresse des Nutzers sip:user_b@standort_b.de enthält.

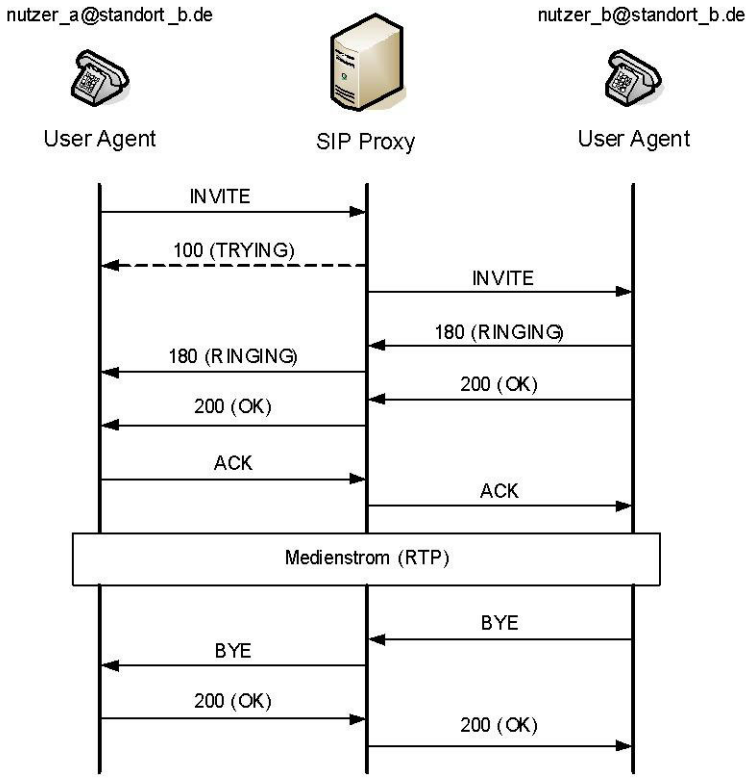

Abbildung 2.9 Vereinfachter Auf- und Abbau einer SIP-Verbindung

Der Proxy sendet die INVITE-Nachricht seinerseits an den Ziel-User Agent. Dieser antwortet mit der Statusmeldung RINGING (180). Diese Statusinformation wird durch den Proxy an den rufenden User Agent geleitet. Sobald der gerufene Nutzer das Telefon abhebt, sendet sein Telefon (User Agent) eine 200-Statusmeldung (OK), die abschließend vom rufenden Teilnehmer mit einer ACK-Nachricht bestätigt wird. Jetzt kann das Telefongespräch z. B. mit RTP übertragen werden. Nach dem Gespräch legt der gerufene Teilnehmer auf. Sein User Agent signalisiert mit BYE den Verbindungsabbau, der seitens des rufenden Teilnehmers mit der Antwort 200 (OK) bestätigt wird.

Eine SIP-Nachricht besteht aus einem Nachrichtenkopf (Header) und einem Nachrichtenkörper (Body). Der Nachrichtenkopf enthält die Anfragen (REQUESTs) bzw. Antworten (RESPONSEs) und andere für den Verbindungsauf- bzw. -abbau wichtige Parameter.

Der Nachrichtenkörper beschreibt das für den Medientransport verwendete Protokoll. Für diese Beschreibung bedient sich SIP des SDP (Session Description Protocol). Durch das SDP werden die benötigten Parameter (Codec, Übertragungsprotokoll, URI, IP-Adresse, Portnummer, Bandbreite) zur Übertragung des Medienstromes ausgehandelt bzw. bekannt gegeben.

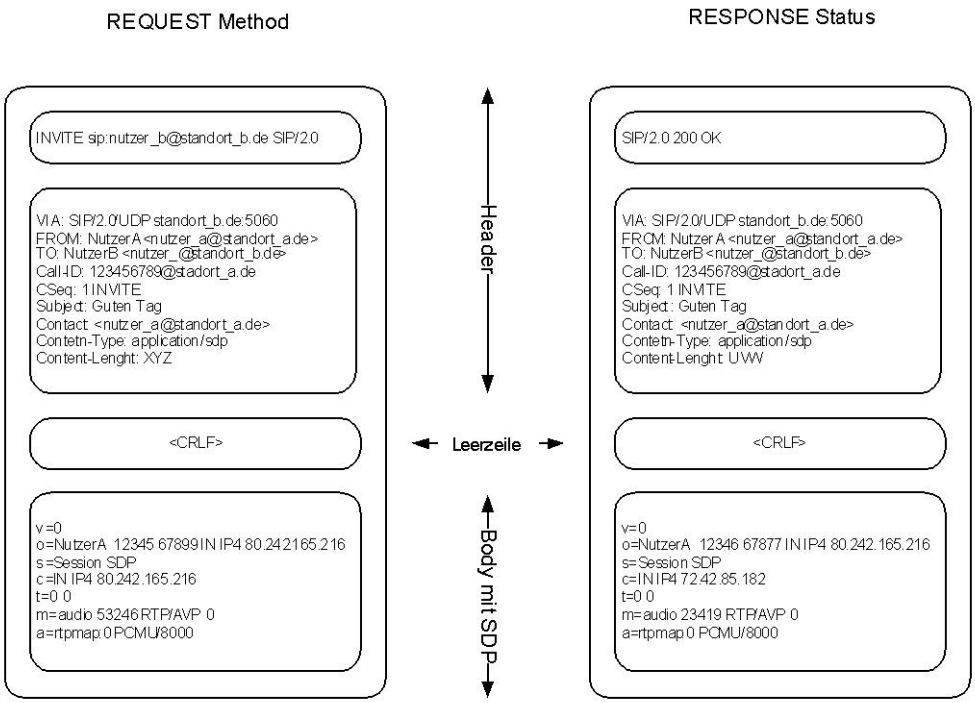

Abbildung 2.10 Aufbau von SIP-Nachrichten

2.3.3 Übersicht MGCP (Media Gateway Control Protocol)

MGCP 1.0 ist ein vom IETF im RFC 3453 [RFC3453] beschriebenes Protokoll, das zur Steuerung von verteilten Media Gateways verwendet wird. Eine MGCP-Umgebung besteht aus einem Kernsystem, dem Call Agent, in dem die Intelligenz des Systems konzentriert ist, und einem Media Gateway, das die Übersetzung der Medienströme zwischen VoIP und z. B. der klassischen Telefonie (ISDN, Analoganschluss) durchführt. Die Steuerung des Media Gateways erfolgt durch den Call Agent.

Das Protokoll ist textbasiert und verwendet, wie auch SIP, das SDP (Session Description Protocol) zur Beschreibung bzw. Vereinbarung des Medienstroms (z. B. RTP) zwischen zwei Media Gateways. MGCP ist nicht als konkurrierendes Protokoll zu H.323 bzw. SIP anzusehen, sondern als Ergänzung dazu. Während H.323 und SIP in erster Linie zur Verbindungssteuerug durch Endsysteme verwendet werden, ist MGCP nur für die Steuerung von Gateways konzipiert. Somit eignet sich MGCP für den lokalen Einsatz im Umfeld von TK-Anlagen bzw. zur Integration von klassischen Systemen in eine VoIP-Umgebung.

Systemarchitektur

MG - Media Gateway

Ein Media Gateway (MG) stellt den Übergang von der klassischen in die VoIP-Telefonie her. Es arbeitet als Übersetzer zwischen leitungsgebundener (circuit switched) und paketorientierter Vermittlung (packet switched). Dabei führt es die Anweisungen (Commands) des Control Agents aus und sendet Benachrichtigungen (Notifications) an den Control Agent.

Ein Media Gateway besteht aus den logischen Einheiten Endpoint, Call und Connection, wobei ein Endpoint aus mehreren Calls und ein Call aus einer oder mehreren Connections bestehen kann.

Endpoints können sowohl physikalische (analoger Anschluss, digitaler Kanal mit 64 kBit/s, …) als auch virtuelle Endpunkte (Audioquelle auf einem Server) sein, die durch einen Endpoint Identifier identifiziert werden. Ein Endpoint Identifier wird durch einen Domain-Namen sowie weitere Schnittstellenbezeichnungen aufgebaut. Als Bespiel soll hier der Endpoint Identifier *interfaceE1/12@mg.domainname.net* dienen. Er beschreibt den 12. digitalen Kanal innerhalb des Interfaces E1 des Gateways *mg* der Domain *domainname.net*. Durch die Initiierung einer Verbindung (Connection) kann ein Control Agent über einen Endpoint eines Media Gateways einen Call zu einem anderen Media Gateway aufbauen.

Die nachfolgende Abbildung verdeutlicht den Zusammenhang der logischen Einheiten eines Media Gateways.

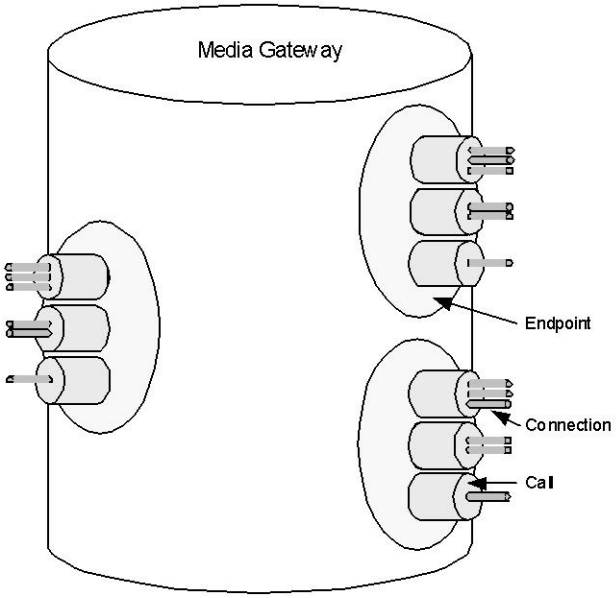

Abbildung 2.11 Logische Elemente (Endpoint, Call, Connection) eines Media Gateways

Die Signalisierung beruht auf Ereignissen (Events) an den Endpoints, die in einem Paket (Package) zusammengefasst werden. Ein MGCP-Package ist eine Gruppierung wohl definierter Erweiterungen, die je nach Typ des Endpoints verschiedene Events (Abheben des Hörers, Klingeln) zusammenfasst. Ein Endpoint kann unterschiedliche Packages unterstützen. Das Ereignis hd aus dem Package H signalisiert beispielsweise das Abheben eines Hörers (Off-hook).

Im Wesentlichen können folgende Gateways unterschieden werden:

- Residential Gateways: Ermöglichen einem oder mehreren analogen Systemen (Telefon, Modem) den Zugang zu einem VoIP-Netz.
- Access Gateways: Bieten dem VoIP-Netz sowohl analoge als auch digitale Übergänge in das klassische Telefonnetz. Ein Access Gateway kann zur Kopplung von VoIP mit einer TK–Anlage eingesetzt werden.
- Trunking Gateways: Verbinden VoIP-Netze mit klassischen Netzen (PSTN). Oftmals wird eine große Anzahl an digitalen Kanälen verwendet. Ein Anwendungsgebiet wäre ein Dienstleister, der Internettelefonkunden den Ausbruch in das PSTN ermöglicht.

Ein Media Gateway wird oftmals in Form eines speziellen Routers realisiert.

CA - Control Agent

Das MGCP-Protokoll beschreibt nur die wichtigsten Funktionen (z. B. Timer-Verwaltung) des Call Agents. Die Steuerung eines Media Gateways erfolgt durch Anweisungen (Commands) an ein entsprechendes Gateway. Die Anweisungen (Commands) werden durch Antworten (Response) des Gateways bestätigt. Der Call Agent ist verantwortlich für die Signalisierung und die Rufsteuerung. Er stellt in dem verteilten System zwischen Call Agent und Media Gateway die Steuerzentrale dar. Ein Call Agent kann als System auf einem Server betrieben werden.

Die nachfolgende Abbildung verdeutlicht den Einsatz von MGCP bei der Kopplung von klassischen Systemen.

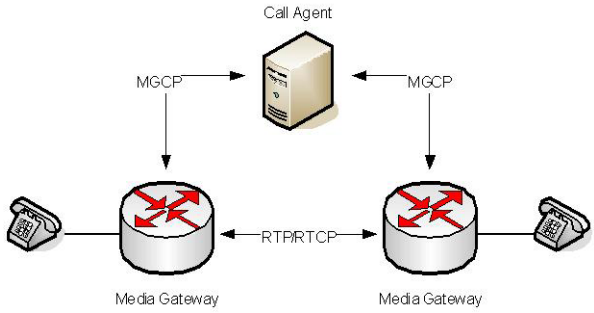

Abbildung 2.12 Direkte Kopplung von klassischen Systemen mittels MGCP

In der Abbildung ist zu sehen, dass die Signalisierung über den Call Agent erfolgt und der eigentliche Medienstrom direkt zwischen den Media Gateways ausgetauscht wird. An Media Gateways können z. B. analoge Telefone, TK-Anlagen und ähnliche Einrichtungen angeschlossen werden.

Mehrere MGCP-Systeme, die von verschiedenen Call Agents gesteuert werden, können mit SIP bzw. H.323 gekoppelt werden und erlauben so eine Vernetzung verteilter Kommunikationssysteme.

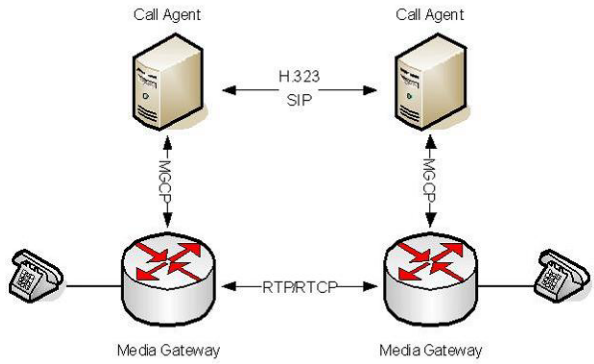

Abbildung 2.13 Kopplung mehrerer MGCP–Systeme mit SIP oder H.323###

Die Steuerung zwischen den Call Agents erfolgt durch SIP bzw. H.323. Nach dem Abheben des Hörers eines Teilnehmers werden zwischen dem Media Gateway und dem Call Agent Signalisierungsnachrichten ausgetauscht, die dann z. B. mit SIP an den Ziel-Call Agent übermittelt werden.

Signalisierung

Der Transport der Protokollnachrichten erfolgt mit UDP, wobei je nach Richtung unterschiedliche Ports verwendet werden. Protokollnachrichten vom Call Agent zum Media Gateway verwenden den UDP-Port 2427, Protokollnachrichten vom Media Gateway benutzen den UDP-Port 2727. Der Nachrichtenaustausch beruht auf Anweisungen (Commands) und Antworten (Responses). Nachfolgende Abbildung zeigt den Auf- und Abbau einer RTP-Sitzung gemäß MGCP.

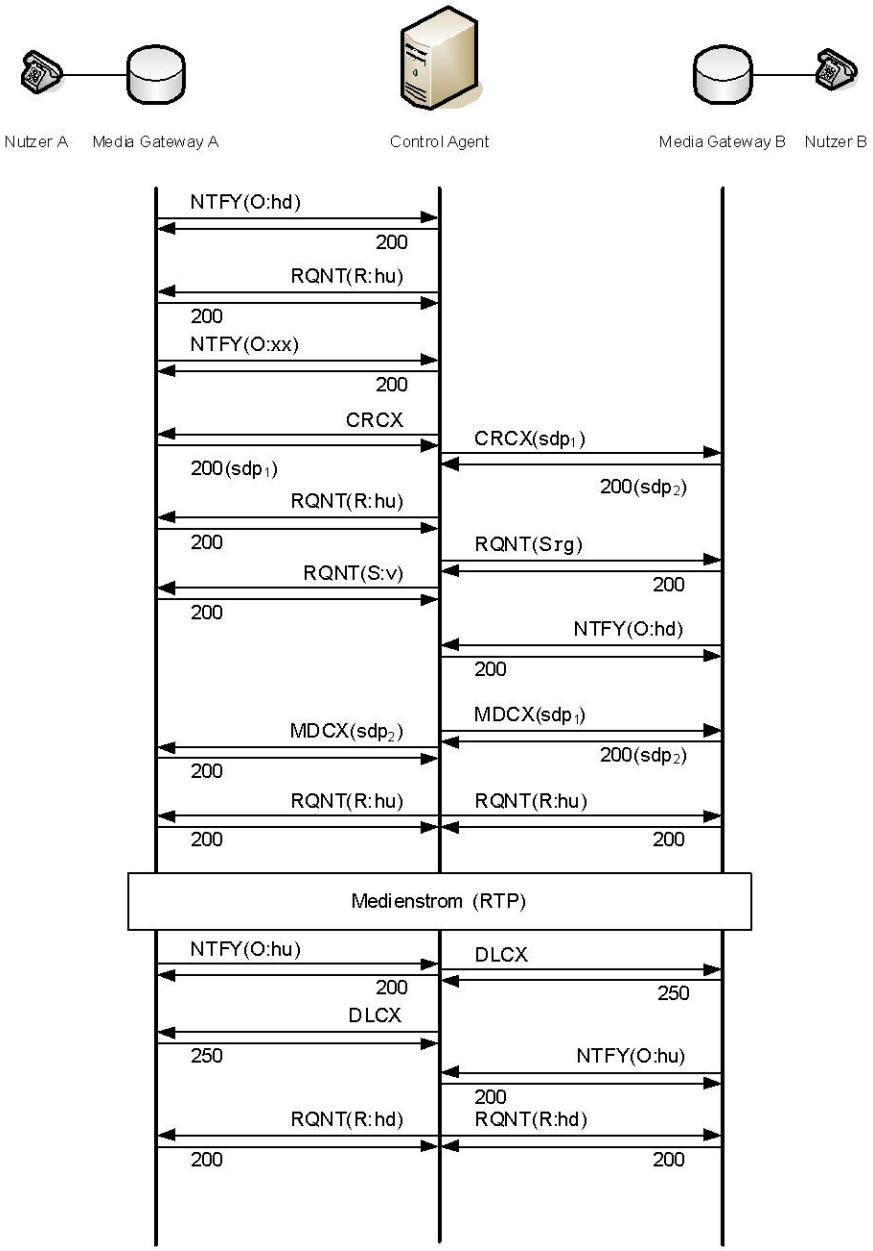

Abbildung 2.14 Auf- und Abbau einer RTP–Sitzung nach MGCP

Bevor die Steuerung eines Media Gateways durch einen Call Agent erfolgen kann, registriert sich das jeweilige Media Gateway bei dem Control Agent. Einzelheiten zum Registrierungsvorgang kann man in diverser Fachliteratur nachlesen. Nutzer A hebt im aufgeführten Beispiel den Hörer ab. Das Media Gateway signalisiert durch eine NTFY-Nachricht (Notify), das Ereignis (Event) „Abgehoben“ (Off-hook). Das O ist ein Parameter, der ein beobachtetes Ereignis (hd - Abgehoben) beschreibt. Diese Anweisung (Command) wird sofort durch eine Antwort (Response) mit dem ResponseCode 200 (200 - die angeforderte Transaktion wurde normal ausgeführt) beantwortet. Da MGCP das ungesicherte Transportprotokoll UDP zum Austausch seiner Nachrichten verwendet, werden üblicherweise alle Anweisungen durch eine Response Nachricht bestätigt. Der Call Agent fordert mit der Anweisung RQNT(R:hu) (RQTN - NotificationRequest) das Media Gateway auf, ihm das angeforderte Ereignis (R) Abheben hu - Off-hook) mitzuteilen. Durch die darauf folgende NTFY(O:xx) Anweisung wird mit dem Parameter O dem Call Agent die Zielrufnummer mitgeteilt. Der Call Agent löst die Zielrufnummer in die entsprechende IP-Adresse des Media Gateways auf, an dem der Nutzer B angeschlossen ist. Durch CRCX (CreateConnection) weist der Call Agent das Media Gateway A an eine Verbindung aufzubauen. Das Media Gateway A beantwortet diese Anweisung mit 200 und sendet

in dieser Nachricht mit SDP (Session Description Protcol, siehe SIP) die von ihm unterstützten Multimediadaten (Codec, RTP-Port). Anschließend fordert der Call Agent mit CRCX das Media Gateway B auf eine Verbindung zu initiieren. Dabei werden die vom Media Gateway A vorgeschlagenen Multimediaparameter mitgesendet. Das Media Gateway B beantwortet mit 200 und sendet seinerseits innerhalb des SDP die akzeptierten Multimediaformate an den Call Agent. Im weiteren Verlauf wird weitestgehend auf die Erwähnung der Bestätigungsnachrichten (2xx – Nachricht) verzichtet und nur bei wesentlicher Funktion ein Hinweis gegeben. Durch RQNT(R:hu) wird das Media Gateway A noch einmal aufgefordert ein Auflegen sofort an den Call Agent zu signalisieren. Mit der nächsten Nachricht RQTN (S:rg) wird das Media Gatgeway B angewiesen, einen Klingelton im Telefon des Nutzers B zu aktivieren (S ≙ SignalRequest, rg ≙ Ringing). Auch das Media Gateway A erhält eine RQTN-Anweisung, aufgrund derer ein Freizeichen im Telefon des rufenden Teilnehmers initiiert wird (v ≙ Alerting). Durch das NTFY (O:hd) signalisiert das Media Gateway B, dass der Nutzer B den Telefonhörer abgehoben hat (ObservedEvent(O) off-hoock(hd). Durch die Nachricht MDCX (ModifyConnection) wird das Media Gateway B aufgefordert den Verbindungsaufbau mit den vom Teilnehmer A unterstützten Multimediaparametern fortzusetzen. Das Media Gateway B bestätigt und übermittelt die von ihm akzeptierten Parameter, die aus den von Media Gateway A vorgeschlagenen Parametern ausgewählt wurden. Durch das anschließende RQTN (R:hu) werden beide Gateways durch den Control Agent aufgefordert, das Auflegen des Hörers (on-hook)(s.o.) zu signalisieren. Der Ruf ist aufgebaut und der Medienstrom wird zwischen den Media Gateways ausgetauscht, die ihrerseits die Informationen der Nutzdaten (Payload) in entsprechende elektrische Signale wandeln. Nach dem Auflegen (on-hook) des Teilnehmer A signalisiert das Media Gateway mit NTFY (O:du) dem Call Agent das beobachtete Ereignis (ObservedEvent). Der Call Agent fordert beide Gateways mit DLCX (DeleteConnection) auf, die Verbindung abzubauen, worauf beide Media Gateways mit 250 (connection was deleted) bestätigen. Der Nutzer B legt auf (NZFY(O:hu)), und der Call Agent weist beide Gateways mit RQTN(R:hd) an, das Auflegen des Hörers zu signalisieren.

2.3.4 Übersicht und Einführung in Megaco

Die Zusammenarbeit der IETF Megaco Working Group und der ITU-T Study Group 16 mündete in einem gemeinsamen Protokoll [RFC3015, ITUT02], das sich zum einen an den Ergebnissen des MGCP-Protokolls, und zum anderen an dem H.323-Rahmenwerk orientiert. Es wird als Signalisierungsprotokoll zwischen Media Gateways und Media Gateway Controller (bei MGCP als Call Agents bezeichnet) in VoIP–Netzen verwendet, die Zugänge in das öffentliche IP Netz bereitstellen und Signalisierungen mit dem PSTN (public switched telephone network) auf der Basis von ISDN, SS7 (Signalisierungsprotokoll zwischen öffentlichen Vermittlungsstellen) und anderen Protokollen austauschen. Bedingt durch die unterschiedlichen Organisationen werden die Namen bzw. Bezeichnungen Megaco (IETF) und H.248 (ITU) verwendet. Megaco kann als Erweiterung von MGCP mit Angleichung an die ITU-Spezifikationen angesehen werden.

Es wird sowohl textbasierte (ABFN – Augmented Backus Naur Form der Nachrichten) als auch binäre Kodierung in Anlehnung an die H.323-Protokollfamilie unterstützt. Der Nachrichtenaustausch selbst orientiert sich stark am MGCP und basiert auf Commands und Replys.

Neben den Einsatzgebieten von MGCP ist Megaco auch in großen Umgebungen zu finden, wie sie bei Breakout-VoIP-Providern auftreten.

Systemarchitektur

Media Gateway

Das Media Gateway wird als logisches System aufgefasst, das aus *Terminations* (Endpunkten) besteht, an denen entweder leitungsvermittelnde (SCN – Switched Circuit Network) oder IP-Netze angeschlossen sind, die Quellen bzw. Senken von Medien- und Signalisierungsströmen darstellen. Bei SCN spricht man von *physical Terminations*, im anderen Falle (IP/RTP) von *ephermeral*

Terminations. Verschiedene *Terminations* werden durch ihre Eigenschaften (Properties), Ereignisse (Events), Signale (Signals) und Statistiken (Statistics) innerhalb so genannter *Packages* beschrieben, durch die die Interoperabilität zwischen verschiedenartigen *Terminations* ermöglicht wird. Die Eigenschaften und Konfiguration eines Endpunktes werden durch *Descriptors* beschrieben.

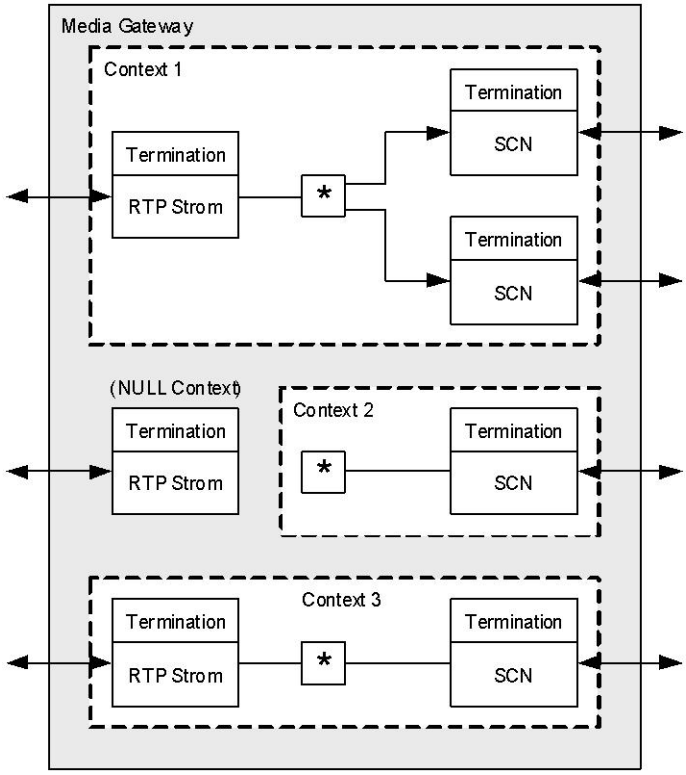

Abbildung 2.15 Media Gateway als logisches System

Die Verknüpfung der *Terminations* untereinander wird als *Context* bezeichnet. Der *Context 1* beschreibt eine Punkt-zu-Mehrpunkt-, der *Context 3* eine Punkt-zu-Punkt-Beziehung. Der *Context 2* zeigt eine geparkte SCN-Termination. Steht eine Termination nicht in einer Beziehung zu einer weiteren Termination, so wird sie automatisch dem *NULL Context* zugeordnet.

Megaco unterscheidet folgende Gateways:

- Residential Gateway: Anschluss von analogen Endgeräten. VoIP–Telefone, die mit dem Megaco Protocol arbeiten, können ebenfalls zu dieser Gruppe gezählt werden.
- SCN FAS Signalling Gateway: Terminiert Signalisierungsprotokolle aus dem PSTN auf der gleichen Schnittstelle wie die Sprachkanäle.
- SCN NFAS Signalling Gateway: Im Unterschied zum SCN FAS Signalling Gateway wird die Signalisierung nicht auf die gleiche, sondern eine getrennte Schnittstelle gekoppelt.
- Trunking Gateway: Enthält eine große Anzahl an digitalen Kanälen zum PSTN. Als Trunk wird die digitale Schnittstelle (z. B. E1) zwischen zwei Vermittlungssystemen bezeichnet.

Media Gateway Controler

Wie bei MGCP besteht die Aufgabe eines Media Gateway Controllers [RFC3525] in der Steuerung der Media Gateways, wobei nicht nur Gateways zur Übertragung des Medienstromes, sondern auch so genannte Signalling Gateways eingesetzt werden, die z. B. eine Transformation der SIP- oder H.323-Signalisierung zum Rufauf- bzw. -abbau in die entsprechende SS7–ISUP-Nachrichten (Signalisierung von ISDN Nachrichten zwischen digitalen Vermittlungsstellen des öffentlichen Fernsprechnetzes) durchführen.

Die Abbildung 2.16 zeigt eine Netzstruktur, die den Übergang in das öffentliche Telefonnetz (PSTN) durch die Zusammenschaltung mit einer Telefongesellschaft auf der Basis von SS7 ermöglicht.

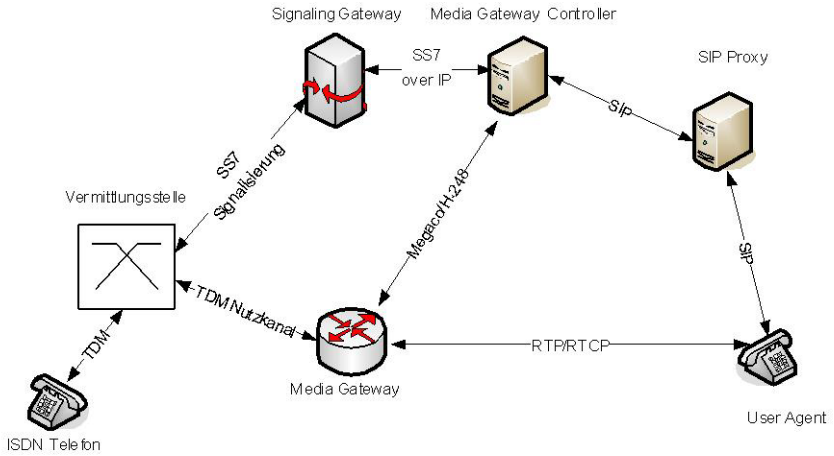

Abbildung 2.16 Übergang in das PSTN durch Zusammenschaltung auf Basis von SS7

Der User Agent verwendet SIP als Signalisierungsprotokoll, das durch den SIP-Proxy zum Media Gateway Controller geleitet wird. Der Media Gateway Controller koordiniert den Rufaufbau und die Übertragung des Medienstroms zum PSTN. Signalling Gateway und Media Gateway können sowohl physikalisch getrennt als auch in einem System abgebildet werden, wobei die Signalisierung über eigene, von der Übertragung der eigentlichen Sprache getrennte Anschlüsse (z. B. E1) oder in einem digitalen Kanal eines physikalischen Anschlusses (Interface) geführt werden kann, in dem auch Sprachdaten übertragen werden. Im ersten Fall spricht man von einem SCN NFAS Signalling Gateway und im zweiten Fall von einem SCN FAS Signalling Gateway.

Multipoint Control Unit (MCU)

Die Multipoint Control Unit unterstützt ähnlich wie bei H.323 den Aufbau und die Koordination von Mehrnutzersitzungen (Konferenzen) und kümmert sich um die Verarbeitung von Audio- und Videoinformationen sowie von Daten.

Signalisierung

Megaco unterstützt die Transportprotokolle UDP und TCP, wobei in Abhängigkeit der Kodierung die Ports gewählt werden. Port 2944 wird für textbasierte Nachrichten und Port 2945 für binär kodierte Nachrichten verwendet. Der Austausch von Nachrichten erfolgt auf der Basis von Steuernachrichten (Commands) und Antworten (Replys), die zwischen dem Media Gateway Controller und dem Media Gateway ausgetauscht werden.

Das nachfolgende Beispiel erläutert den Rufaufbau und Rufabbau mit den dazugehörigen Nachrichten. Auf den Registrierungsvorgang wurde hier verzichtet.

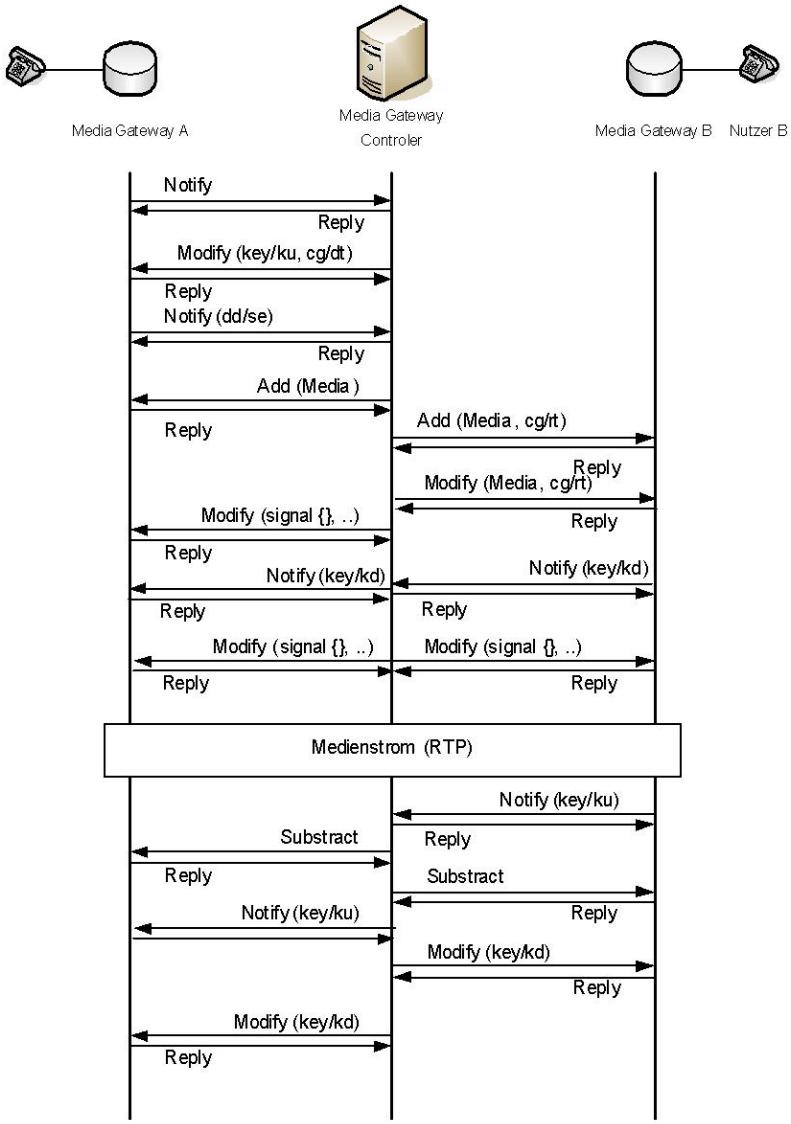

Abbildung 2.17 Auf- und Abbau einer RTP–Sitzung nach Megaco

Nach Abheben (Off-hook) des Hörers durch Nutzer A informiert das Media Gateway A mit einer Notify-Nachricht den Media Gateway Controller, der den Empfang der Nachricht mit einem Reply bestätigt. Sämtliche Commands werden im Megacoprotokoll durch Replys bestätigt. Im weiteren Verlauf wird auf die Erwähnung der Replys verzichtet. Durch das Modify wird das Media Gateway A angewiesen, ein Freizeichen (Dial Tone) auf das Telefon zu legen. Das vom Media Gateway folgende Notify übermittelt die Zielrufnummer, die vom Media Gateway Controller in eine entsprechende Ziel–IP–Adresse umgewandelt wird. Durch das Add des Media Gateway Controllers wird das Media Gateway A aufgefordert, ein Context zu erzeugen und die physikalische Terminierung (physical Termination) in diesen Context einzubinden und anschließend eine IP-Terminierung (ephermeral Termination) einzurichten und diese ebenfalls dem Context zuzuordnen. Im Reply des Media Gateways A werden dem Media Gateway Controller die akzeptablen Multimediaparameter mit SDP (Session Description Protocol) übermittelt. Eine entsprechende Add-Nachricht mit den vom Media Gateway A unterstützten Multimediaparametern wird durch den Media Gateway Controller an das Media Gateway B gesendet, das in seinem Reply seine Multimediaparameter übermittelt. Durch die nächsten Modify-Nachrichten wird das Multimedia Gateway B veranlasst, einen Klingelton am Telefon des Teilnehmers B anzulegen. Das Multimedia Gateway A erzeugt einen entsprechenden Rufton im Telefon des Nutzers A. Durch Notify informiert das Gateway B den Media Gateway Controller über das Abheben des Hörers, worüber das Gateway A durch den Media Controller in Kenntnis gesetzt wird. Die nachfolgenden Modify Messages weisen die Media Gateways an, das

Auflegen des Hörers zu signalisieren. Es beginnt die Übertragung des Medienstromes. Notify von Media Gateway B teilt dem Media Gateway Controller das Auflegen des Hörers durch Teilnehmer B mit. Die anschließende Substract-Nachricht fordert beide Media Gateways auf, ihre RTP-Sitzung einzustellen und die Terminations aus dem jeweiligen Context zu entfernen. Durch das nächste Notify teilt Media Gateway A das Auflegen des Hörers mit. Mit den abschließenden Modify-Nachrichten an beide Media Gateways werden diese aufgefordert, das Abheben des Hörers an den Media Gateway Controler zu signalisieren.

2.3.5 Übersicht IAX2 (Inter-Asterisk eXchange Protocol)

Das IAX2 steht für InterAsterisk eXchange Protocol Version 2 und wurde von der Open Source Community entwickelt. Das Protokoll eignet sich zur Vernetzung von Asterisk-Servern, sowie als Endgeräte-Kommunikationsprotokoll zur Übertragung von Audio, Video, Texten und Bildern. Die Signalisierung und die Datenübertragung werden bei IAX2 über den UDP-Port 4569 abgewickelt. Das Protokoll ist sehr schlank gehalten und eignet sich gut für die Kommunikation in privaten Netzen (NAT) sowie durch Firewalls. Die Hauptmerkmale des IAX2-Protokolls lassen sich wie folgt zusammenfassen:

- Das IAX2-Protokoll ist proprietär, aber offen gelegt.
- Signalisierungs- und Medientransport über nur einen Port (UDP 4569). Dadurch ist das Protokoll IAX2 einfach über NAT-Umgebungen zu transportieren und die Regeln in Firewalls sind überschaubar.
- Schlankes Protokoll durch binäre Codierung und geringen Protokoll-Overhead. IAX2 benötigt nur 4 Bytes Protokoll-Overhead, um Sprach- und Videopakete auszutauschen.
- Bündelung mehrerer IAX2-Verbindungen zwischen zwei Asterisk-Servern zu einem Trunk.
- Das Protokoll IAX2 unterstützt die Authentifizierung über PKI (Public-Key Infrastruktur). Das PKI-Verfahren von IAX2 ermöglicht die Authentifizierung zwischen zwei Asterisk-Servern über RSA-Schlüsselpaare.

IAX2-Signalisierung

Das IAX2-Protokoll unterscheidet zwischen einem 12 Byte großen Fullheader für die Signalisierung und einem vier Byte großen Miniheader, der ausschließlich für den Transport von Nutzdaten verwendet wird.

IAX2 benutzt nur einen UDP-Port (4569) für die Übertragung von Signalisierungsinformationen und Mediendaten. Es werden die verschiedenen Header-Typen für den Verbindungsausbau und die Sprachkommunikation vorgestellt. Detaillierte Beschreibungen findet man in der einschlägigen Literatur [AsVoEr].

Fullheader

Signalisierungsinformationen werden mit dem Type *Fullheader* ausgetauscht. Alle Übertragungen werden mit *ACK* und der entsprechenden Sequenznummer bestätigt (außer *ACK* und *HANGUP*). Die untenstehende Abbildung zeigt den Aufbau des Fullheader-Steuerpakets. Hierbei ist callnr die Identitätsnummer des Senders und dcallnr die des Empfängers. Mit ts wird ein Zeitstempel übertragen. Der Parameter seqnr ist die Sequenznummer. Mit type wird die Art des Paketes beschrieben, z. B. DTMF, VOICE, VIDEO, CONTROL, NULL, TEXT, IAX oder IMAGE. In dem Feld csub werden Steuerfunktionsparameter definiert wie NEW, PING, ACK, HANGUP usw.

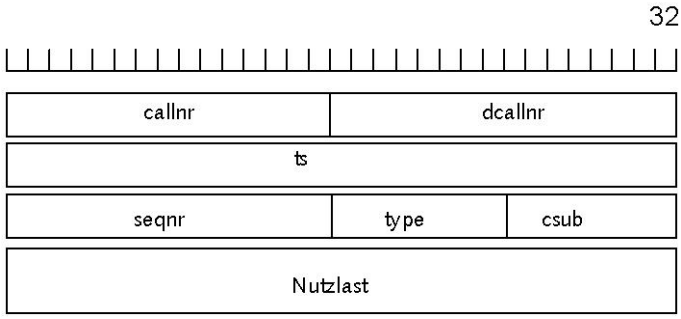

Abbildung 2.18 Fullheader

Miniheader

Um eine effiziente Nutzdatenkommunikation zwischen den Endgeräten zu erhalten, wurde ein Typ Miniheader eingeführt. Der Miniheader besteht aus vier Byte Absenderadresse, einem Zeitstempel und der Nutzlast. Die Paketgröße ist auf maximal 32 KB begrenzt. Die untenstehende Abbildung zeigt den Aufbau des Miniheader-Pakets.

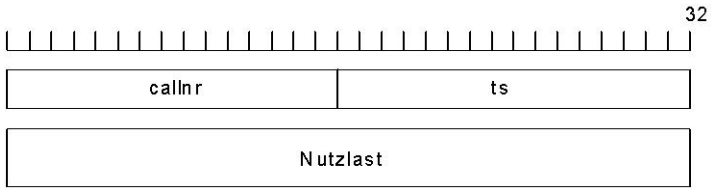

Abbildung 2.19 Miniheader

Verbindungsaufbau

Zur Registrierung des Endgeräts am Server ist eine Authentifizierung erforderlich. Das Endgerät sendet ein erstes REGREQ-Paket (Registrierungsaufforderung mit Nutzernamen und Authentifizierungsmethode), das mit ACK (Bestätigungspaket) vom Server beantwortet wird. Anschließend fordert der Server mit einem ersten REGAUTH-Paket (Übertragung des Usernamens und der Authentifizierungsmethode) das Endgerät auf, das Passwort mit einer Authentifizierungsmethode (plaintest, md5) zu übertragen. Mit dem zweiten REGREQ wird das Passwort vom Endgerät übertragen und der Server bestätigt die Richtigkeit mit REGACK. Das Endgerät quittiert die Anmeldung mit einem abschließenden ACK.

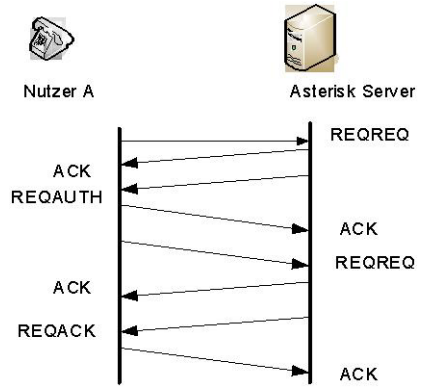

Abbildung 2.20 Registrierung

Sprachkommunikation über den Server

Der Kommunikations-Aufbauwunsch wird mit dem Paket NEW (Verbindungsanfrage mit den Informationen, wie Name des Anrufers und CallerID) vom Nutzer A eingeleitet. Der Server leitet das NEW-Paket an Nutzer B weiter und dieser beantwortet die Anfrage mit einem Bestätigungspaket ACK. Mit dem Paket AUTHREQ fordert der Server den Nutzer A auf, sich erneut zu authentifizieren (in dem Paket werden Username und die Authentifizierungsmethode angefordert). Die Authentifizierungsphase wird mit AUTHREP (Übermittelung des Passwortes) fortgesetzt, woraufhin der Server ein ACCEPT-Paket (damit wird die Authentifizierung bestätigt) an den Nutzer A zurücksendet und dieser es mit ACK bestätigt.

Anschließend sendet der Benutzer B ein RINGING-Paket, worauf Nutzer A dies mit ACK quittiert. Die Kommunikations-Aufnahmephase von Nutzer A wird mit dem ANSWER-Paket (Annahme des Anrufes) von Nutzer B bestätigt, woraufhin Nutzer A mit einem ACK antwortet. Im nächsten Schritt handelt Nutzer B mit Nutzer A über VOICE die Übertragungsart (Video, Text, Image) aus und bestätigt mit ACK.

Nachdem alle Übertragungsparameter feststehen, erfolgt die Übertragung der Nutzdaten mit dem Miniheader. In Abständen von ca. einer Minute überprüft der Server den Zustand des Dialogs mit einem Fullheader. Die Übertragung wird mit einem HANGUP (in dem Paket wird ein GoodBye übertragen) beendet.

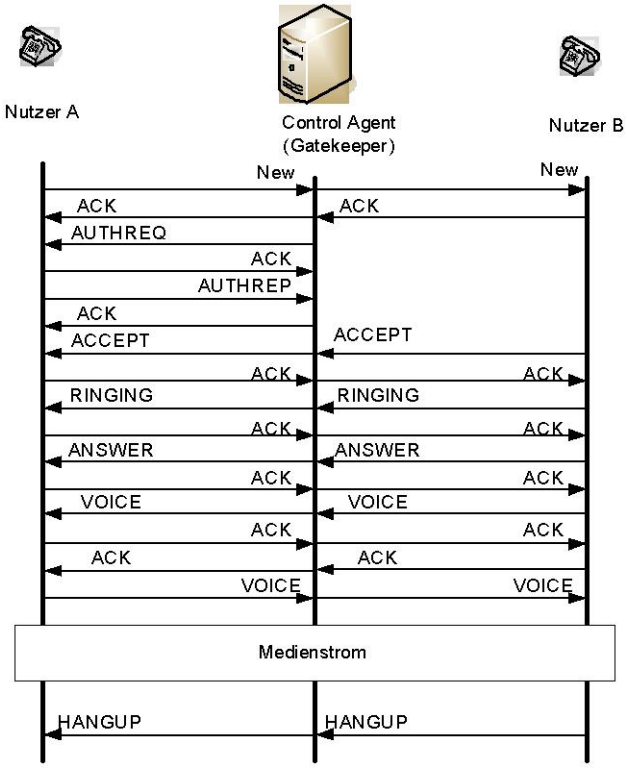

Abbildung 2.21 Sprachübertragung

2.3.6 Vergleich von H.323 und SIP

Ein unmittelbarer Vergleich der beiden Protokolle ist nur bedingt möglich, da H.323 eine architektonische Beschreibung der ITU-T ist und SIP ein Protokoll zur Verbindungssteuerung der IETF. H.323 lehnt sich stark an das ISDN-Protokoll an. Mit SIP wird nur das Protokoll zur Verbindungssteuerung beschrieben, eine Architektur wird nicht definiert. Die Architektur von H.323 orientiert sich im Prinzip an den Spezifikationen von der ITU-T und ETSI. Die untenstehende Vergleichstabelle stellt die beiden Ansätze gegenüber. Bedingt durch die verschiedenen Definitionen

der beiden Protokolle können nicht alle Eigenschaften direkt verglichen werden. Grob kann man festhalten:

- H.323
  - H.323 definiert ein komplettes und komplexes Multimedia-System für Audio und Video.
  - H.323 definiert alle Einzelheiten von der Signalisierung, Paketierung bis zur Kodierung.
  - H.323 unterstützt ein Bandbreitenmanagement
  - H.323 ist ein ist sehr komplexes Protokoll.
- SIP
  - SIP wird nur für die Signalisierung eingesetzt.
  - SIP wird benutzt um Sessions zwischen den Endteilnehmern auf- bzw. abzubauen.
  - SIP kann in einer Session beliebige Daten austauschen.
  - Der Transport der Nutzdatem liegt außerhalb des Definitionsbereichs des eigentlichen Standards.

	H.323	SIP
Standardisierungsinstanz	ITU-T	IETF
Architektur	monolithisch	modular
Anwendung	Telefonnetz	Internet
Nachrichtendefinition	ASN.1	ABNF
Teilnehmeradressierung	URL, E.164	SIP-URI
Nutzdatenübertragung	RTP/RTCP	RTP/RTCP
Nachrichtenkodierung	binär	textbasiert
Zusammenarbeit mit IP-Netzen	keine	problemlos
Zusammenarbeit mit PSTN	unmittelbar, da H.323 Protokolle des PSTN verwendet (Q.931)	keine unmittelbaren Gemeinsamkeiten
verwandte Protokolle	Q.931, Q.SIG	http
Komplexität	hoch, wegen zahlreicher Unterstandards	niedrig, nur Signalisierung spezifiziert
DTMF-Töne	ja	ja
Skalierbarkeit	eingeschränkt	ja
direkte End-to-End-Signalisierung	ja	ja
Anrufsteuerung	Gatekeeper	Endgerät
Erweiterbarkeit	aufwändig	ja
Firewall-Support	ja	ja
Forking	durch Gatekeeper	durch SIP-Proxy
Authentifizierungs-Protokoll	H.235	keine Festlegung, z. B. IPsec, TLS, SRTP, S/Mime
Mehrpunktsignalisierung	nein	ja
Konferenzart	zentriert	verteilt

Tabelle 2.1: Vergleich H.323 und SIP

H.323 ist weder ideal für das Internet noch für das klassische Fernsprechnetz, hingegen ist SIP komplett auf internettypische Anwendungen ausgerichtet. Die Nähe zwischen SIP und http ermöglicht in Zukunft eine große Anzahl von übergreifenden Diensten. Aus diesem Grund wurde SIP für UMTS von der IETF und ITU-I als Steuerungsprotokoll gewählt.

2.4 Medienübertragungsprotokolle

2.4.1 Einführung in RTP - Real-Time Transport Protocol

Das Real-Time Transport Protocol (RTP) [RFC1889] bildet die Grundlage für die Übertragung von Sprach- und Videodaten im Internet und ist Bestandteil des H.323-Protokolls. Zum Transport wird den RTP-Paketen jeweils ein RTP-Header vorangestellt und dieser zusammen mit der Payload übertragen. Das RTP-Protokoll fußt auf einer End-to-End-Verbindung. Der RTP-Header enthält Informationen über den verwendeten Codec, die Sequenznummer, den Zeitstempel, die Synchronisationsinformation und ggf. den Verschlüsselungsalgorithmus (SRTP). Sender und Empfänger tauschen ständig Zeit- und Synchronisationsinformationen aus, um Laufzeitunterschiede auszugleichen. Paketüberholungen gleicht das Protokoll durch Sequenznummern aus. Paketverluste dagegen können wegen des UDP-Transports von dem Protokoll nicht ausgeglichen werden, hier muss der Codec die Verluste ausgleichen.

Das RTP und das dazugehörige RTCP (Real-Time Control Protocol) verwenden die gleichen Adressen zur Übertragung der Nutzdaten und Steuerungsfunktionen, aber unterschiedliche Ports. RTP unterstützt die Übertragung von Echtzeitinformationen durch das Internet, aber es wird in keiner Weise ein Qualtity of Service (QoS) geboten. Die wichtigsten Grundfunktionen für den Transport von Echtzeitinformationen sind:

- PT Payload Type Identification
- Timestamp
- Sequence Number
- SSRC Synchronisation Source Identifier
- CSRC Contributing Source Identifiers

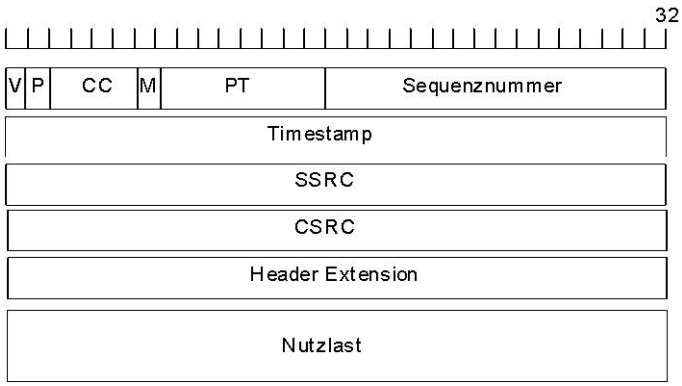

Abbildung 2.22 RTP-Paket

Das Feld V enthält die Version des RTP. P ist das Padding-Feld, das angibt ob ein Padding angehängt ist. Das Feld M ist das Marker Bit, das derzeit unspezifiziert ist. Das Feld Payload Type (PT) beinhaltet die Kodierungsart (z. B. G711, G729). Die Sequenznummer gibt eine fortlaufende Nummer für jedes Datenpaket, mit dem es möglich ist empfängerseitig die richtige Reihenfolge der Pakete zu garantieren. Das Feld mit dem Timestamp dient zur Synchronisation der Nutzdaten. Das 32-Bit Feld mit dem Synchronisation Source Identifier (SSRC) dient zur Identifikation der Datenquelle. Das

optionale 32-Bit Feld enthält bei Paketen, die aus verschiedenen Paketen gemischt werden, die Original-SSRCs.

Signalisierung von RTP

Der Transport der Sprachinformationen erfolgt mit UDP. Empfangsbestätigungen sind nicht erforderlich und eine Neuanforderung kommt aufgrund der engen Zeitfenster bei der Sprachübertragung (< 150 ms) nicht in Frage. RTP erkennt an Hand der 16-Bit-Sequenznummer falsche, fehlende oder doppelte Datenpakte und nimmt gegebenenfalls Korrekturen vor. Die Synchronisation der Datenpakete steuert das Protokoll über die jeweiligen Zeitstempel. Das Datenfeld mit dem Synchronisation Source Identifier (SSRC) ermöglicht eine eindeutige Identifizierung der Absenderquelle. Das optionale Datenfeld Content Source Identifier (CSRC) beinhaltet die Quelladresse der SSCRs.

RTP und RTPC stellen selbst keine Prozeduren zum Auf- und Abbau von Sessions bereit, wie Steuerung der Verbindung, Lokalisierung der gewünschten Benutzer oder Austausch der verwendeten Parameter (IP-Adressen, UDP-Portnummern, Codec, usw.).

2.4.2 Grundsätzliche Funktionsweise von SRTP - Secure Real-Time-Transport Protocol

Die Absicherung der VoIP-Kommunikation in WLANs, in Firmennetzen oder in öffentlich zugänglichen Hotspots wird in zunehmendem Maß diskutiert. Secure Real-Time-Transportprotokoll SRTP ist eine Alternative zur IPsec-basierten VPN-Datenkommunikation, insbesondere ist das Protokoll für Echtzeitübertragung ausgelegt. Hierbei werden die Daten mit einer symmetrischen Verschlüsselung nach AES (Advanced Encryption Standard) verschlüsselt. SRTP ist die verschlüsselte Übertragungsvariante von RTP über IP-Netze. Die Spezifikation RFC 3711 [RFC3711] beschreibt die Verschlüsselung und Authentifizierung von RTP-Daten. Damit wird z. B. das Abhören von Gesprächen oder das Lahmlegen von Komponenten unterbunden. Als End-to-End-Protokoll ist SRTP unabhängig von der Netzinfrastruktur und somit auch für öffentliche Netze geeignet.

Sicherheitsfunktionen von SRTP

SRTP stellt folgende Sicherheitsfunktionen zur Verfügung um eine vertrauliche Übertragung zu realisieren:

- Die Verschlüsselung der Sprachübertragung schützt vor unbefugtem Abhören.
- Die Authentifizierung des Absenders unterbindet Identitäts-Spoofing.
- Mit der Überprüfung der Integrität werden unberechtigte Änderungen ausgeschlossen.
- Mit dem Anti-Replay-Schutz wird ein unbefugter Zugriff auf Ziel-End-Einrichtungen verhindert.

2.5 VoIP-Routing

2.5.1 Statisches Routing

Eine Methode um die Erreichbarkeit von VoIP–Zielen zu garantieren bietet das statische Routing von VoIP-Adressen. Dabei werden beispielsweise Rufnummernprefixe durch feste Konfiguration in VoiP–Servern bzw. VoiP-Gateways zu festgelegten IP–Adressen geleitet. In kleineren Umgebungen kann das eine einfache und gute Lösung darstellen, jedoch stößt man schnell an die Grenzen der Skalierbarkeit, wenn es sich um große Unternehmensstrukturen oder gar das Internet handelt. In solchen Fällen wird gerne auf dynamische Verfahren wie z. B. DNS oder ENUM zurückgegriffen.

2.5.2 DNS und SRV Records

SRV Records sind Erweiterungen des DNS-Systems nach RFC 2782, die zum Routing von VoIP–Signalisierungsströmen verwendet werden. Ähnlich den MX Records, die das Ausliefern von E-Mails an E-Mail-Server ermöglichen, können durch SRV Records Verbindungen zu VoiP-Servern über eine Namensauflösung aufgebaut werden. Ein SRV Record zeigt auf den SIP-Server, der für die Domain zuständig ist. Werden mehrerer SIP-Proxys für eine Domain angegeben, entscheidet die Priorität zu welchem Server geroutet wird. SRV kann auch für das Routing von H.323 verwendet werden. SRV Records sind nicht ausschließlich für VoIP–Dienste geschaffen, sondern können ganz unterschiedliche Dienste adressieren.

Nachfolgende Abbildung stellt zwei SRV Records dar, die auf zwei Server (iptel1.testdomain.de und iptel2.testdomain.de) zeigen, die für die Domain testdomain zuständig sind.

_Service._Proto.Name	TTL	Class		Priority	Weight	Port	Target
_sip._udp.testdomain.de	65789	IN	SRV	20	0	5060	iptel1testdomain.de.
_sip._udp.testdomain.de	82769	IN	SRV	10	0	5060	iptel2testdomain.de

Abbildung 2.23 SRV Record

Der Dienst wird durch *_Dienst* (_sip) angegeben, gefolgt vom Transportprotokoll mit *_Pprotokoll* (_udp), der *.Domain* (testdomain) und abschließend der Top Level Domain *TLD* (de). Diese Zeichenketten werden durch Punkte voneinander getrennt. TTL entspricht dem eines DNS-Eintrags. IN stellt die DNS Class dar. Nachfolgend wird die Priorität (20 bzw. 10) angegeben. Der höchsten Priorität entspricht die niedrigste Nummer. Der Parameter „Weight (0)“ gibt die Gewichtung der Server bei gleicher Priorität an, mit der durch einen Algorithmus der zu verwendende Server bestimmt wird. Es folgt die Portnummer, unter der der Dienst erreichbar ist und schließlich der Name des zuständigen Servers. Im aufgeführten Beispiel würde grundsätzlich iptel2.testdomain.de verwendet werden und nur im Falle, dass dieser Server nicht erreichbar ist, wird iptel1.testdomain.de verwendet.

Ein Client prüft, ob für die entsprechende Domain ein SRV Record eingetragen ist. Sind mehrere vorhanden, so werden die Server in der Reihenfolge ihrer Prioritäten abgefragt. Ist kein SRV Record vorhanden, wird eine einfache DNS-Abfrage durchgeführt, um sich mit dem Server zu verbinden.

2.5.3 ENUM

Der Name ENUM leitet sich von "tElephone NUmber Mapping" ab und ist ein Internet-Standard [RFC3761], mit dem sich Telefonnummern auf Internet-Domains abbilden lassen. Diese Domains können dann zur Speicherung und Identifizierung unterschiedlichster Kommunikationsdienste herangezogen werden, darunter Fax- und Mobilfunk-Rufnummern, Voice-Mail-Systeme, E-Mail-Adressen, IP-Telefonie-Adressen, Webseiten, GPS-Koordinaten, Anrufumleitungen, Unified Messaging und vieles mehr. Mit ENUM können die Nutzer so ihre gesamte Kommunikation über eine Rufnummer abwickeln. Einmal in das Adressverzeichnis eingetragen, erfolgt die Zuordnung zu den jeweils passenden Ausgabegeräten über den ENUM-Nameserver.

ENUM nutzt dazu das Domain Name System (DNS), das eine logische Verbindung zwischen den numerischen IP-Adressen der ans Internet angeschlossenen Rechner und Domains herstellt. Das ENUM-Protokoll verwendet nun die Infrastruktur des DNS, um Informationen über die verfügbaren Dienste bereit zu halten, die einer Telefonnummer zugeordnet sind.

Man entschied sich international, für ENUM keine neue Top Level Domain einzuführen, sondern die Sub-Domain e164.arpa zu benutzen. Sie wurde ausgewählt, weil die Top Level Domain .arpa bereits für Infrastrukturzwecke konzipiert ist. E164 wiederum bezeichnet den Standard, der den internationalen Rufnummernplan der ITU beschreibt. Als internationale Registrierungsstelle für

e164.arpa fungiert RIPE NCC in Amsterdam, die Registrierungsanträgen in Abstimmung mit der jeweiligen nationalen Regierung nachkommt.

Zur Bildung der ENUM-Domain wird die betreffende Rufnummer (inklusive der Landeskennung) der Domain-Endung e164.arpa in umgekehrter Reihenfolge vorangestellt, getrennt durch Punkte zwischen den einzelnen Ziffern. Aus +49 (0)228 9582-0 wird so 0.2.8.5.9.8.2.2.9.4.e164.arpa. Über diese Domain kann ein ENUM-Client auf einen Nameserver mit so genannten NAPTR-Records (Naming Authority Pointer) zugreifen. Diese Einträge enthalten wiederum die Informationen über die verfügbaren Dienste.

Die verfügbaren Dienste können z. B. mit dem Unix-Befehl *host* abgefragt werden:

host -t naptr 0.2.8.5.9.8.2.2**.9.4.e164.arpa**

2.5.4 TRIP – Telephony Routing over IP

Die Voraussetzung für die Durchsetzung der Internet-Telefonie gegenüber der klassischen Telefonie ist die weltweite Erreichbarkeit von Telefonzielen, unabhängig von ihrer administrativen Hoheit. Hierfür ist ein Austausch von Telefonzielen (Telefonnummer, URI) zwischen den administrativen Instanzen unabdingbar. Mit dem durch das RFC 3219 beschriebenen Verfahren TRIP (Telephony Routing over IP) [RFC3219] kann weltweit die Erreichbarkeit von Telefonzielen realisiert werden. Dieses Protokoll basiert auf dem BGP-4-Protokoll (Border Gateway Protocol Version 4), das als quasi-Standard zum Austausch von Routing-Informationen zwischen den Internet Service Providern im Internet verwendet wird und als routingtechnisches Rückgrat des Internets angesehen werden kann. Der Austausch der Routinginformationen (Erreichbarkeit der Telefonziele, Routen zu den Telefonzielen, Informationen über Gateways zu Telefonzielen innerhalb des PSTN) erfolgt dynamisch zwischen Location Servern, die in diesem Zusammenhang als TRIP Peers bezeichnet werden. TRIP ist unabhängig von den verwendeten Signalisierungsprotokollen (SIP, H.323, ...). TRIP hat im Internet noch keine Verbreitung gefunden.

ITAD – IP Telephony Administrative Domain

Ähnlich dem AS (Autonomous System) definiert TRIP eine logische administrative Instanz, die ITAD (IP Telephony Administrative Domain). Unter einer ITAD wird die Ansammlung sämtlicher logischer Systemkomponenten (Gateways, Location Server, …) verstanden, die unter der Hoheit einer administrativen Verwaltung stehen. Die Voraussetzung für den Betrieb einer ITAD ist mindestens ein Location Server. Jeder ITAD wird eine ITAD-Nummer zugeordnet, die die ITAD weltweit eindeutig identifiziert. Der Bereich der möglichen ITAD-Nummern liegt zwischen 0 und 2^{32}-1. Die 0 wird vom RFC 3219 reserviert und kann nicht genutzt werden. Der Bereich von 1 bis 255 wird zur privaten Nutzung verwendet. Die übrigen ITAD-Nummern werden von der IANA (Internet Assigned Numbers Authority) auf Basis der Antragsreihenfolge vergeben.

TRIP Speaker

Ein Location Server ist eine Systemkomponente innerhalb einer VoIP–Umgebung, die Daten wie z. B. IP–Adresse, URI und ähnliche Informationen zu einem Telefonziel enthält. Tauscht ein Location Server Informationen mit einem anderen Location Server über TRIP aus, wird er als TRIP Speaker bezeichnet.

TRIP Peers

Location Server, die auf der Grundlage von TRIP eine Verbindung untereinander eingehen, werden als Peers bezeichnet. Es können *Internal* und *External* Peers unterschieden werden.

Internal Peers

Location Server, die sich innerhalb einer ITAD befinden und untereinander eine Verbindung eingehen, werden als Internal Peers bezeichnet.

External Peers

Locataion Server, die untereinander Verbindungen eingehen und sich in unterschiedlichen ITADs befinden, werden als External Peers bezeichnet.

TRIB – Telephony Routing Information Base

Die Datenbank innerhalb eines Location Servers, die die erreichbaren Telefonziele enthält, wird als Telephony Routing Information Base (TRIB) bezeichnet.

TRIP verwendet TCP mit der Portnummer 6069 zum Transport der Protokollnachrichten. Zur Etablierung einer Sitzung zwischen zwei Location Servern senden beide Location Server eine OPEN-Nachricht. Eine Peering-Sitzung gilt als aufgebaut, wenn die versendeten OPEN-Nachrichten durch jeweils eine KEEPALIVE-Nachricht der Gegenseite bestätigt wurden. Nach dem Aufbau einer Sitzung können KEEPALIVE, UPDATE und NOTIFICATION Messages ausgetauscht werden.

Die Routinginformationen werden durch UPDATE-Nachrichten ausgetauscht. Anhand dieser Nachrichten kann ein Graph aufgebaut werden, der die Beziehungen zwischen den ITADs beschreibt. Werden keine neuen UPDATE-Nachrichten versendet, wird durch KEEPALIVE-Nachrichten der Fortbestand einer Sitzung gewährleistet.

Eine Route wird innerhalb von TRIP durch eine Telefon-Zieladresse, die durch einen Adressfamilienindikatior, einem Adressenprefix, sowie einem Anwendungsprotokoll (SIP, H.323,…) beschrieben. Durch das NextHopServer-Attribut der UPDATE-Nachricht kann ein Ruf geroutet werden.

2.5.5 DNSSEC

Einführung

Das Domain Name System ist ein zentraler, äußerst sicherheitskritischer Dienst des Internet. Er realisiert eine verteilte Datenbank, deren Hauptaufgabe darin besteht, zu DNS-Namen (wie bsi.bund.de) die IP-Adresse des Rechners zu liefern. Darüber hinaus wird DNS für immer mehr Aufgaben eingesetzt, z. B. zum Routing von E-Mails und zukünfig auch zur Ablage kryptographischer Schlüssel.

Die Antworten eines DNS-Servers auf Anfragen eines Clients werden kryptographisch völlig ungeschützt übertragen. Fälle, in denen diese Antworten manipuliert wurden und die Webauftritte großer Firmen lahm legten, sind gut dokumentiert [H03]. Für VoIP hätte das z. B. zu Folge, dass Anrufe bei einer bestimmten Telefonnummer (z. B. 110) bei einem kriminellen Empfänger landen können.

Um dies in Zukunft zu unterbinden, wurden in RFC 2535 die drei neuen Ressource Records SIG, KEY und NXT eingeführt:

- SIG enthält die digitale Signatur eines anderen Ressource Records,
- KEY wird zur Veröffentlichung der kryptographischen Schlüssel verwendet, und
- NXT dient dazu, auch negative Antworten signieren zu können: anstatt die Antwort „nonsene.example.com does not exists“ für jede unsinnige Anfrage „on the fly“ neu signieren zu müssen, wird auf den alphabetisch nächsten sinnvollen Eintrag verwiesen: „NXT sense.example.com“, gefolgt von dem SIG-RR für diesen NXT-Eintrag.

Leider stellte sich in ersten Experimenten heraus, dass RFC 2535 in der Praxis zu einem administrativen Albtraum geworden wäre [G04].

DNSSEC wird daher zurzeit überarbeitet. Das grundlegende Prinzip ist dabei gleich geblieben, aber die drei oben genannten Ressource Records wurden umbenannt (in der obigen Reihenfolge: RRSIG, DNSKEY und NSEC) und ein vierter (DS) hinzugefügt, der die Verkettung der einzelnen DNS-Zonen erleichtern soll [Sch05].

Bisher wurden zwei Methoden vorgeschlagen, wie DNS für VoIP eingesetzt werden soll. Diese sollen nun getrennt betrachtet werden.

DNSSEC für SRV-Ressource Records

Jeder SRV Ressource Record, der auf einen SIP Server für eine bestimmte Domäne zeigt, wird durch einen entsprechenden SIG RR ergänzt. Ein typischer Eintrag im Zonefile sieht dann wie folgt aus:

```
_sip._udp.testdomain.de     65789 IN SRV 20 0 5060 iptel1.testdomain.de.
                             65789 IN SIG SRV 1 4 65789 20050503125727 (
                                                  20050403125727 32882
                                                        testdomain.de.
                                              ah4OMhYaYvUlJBNQxIco7FzHyE6TFqHO
                                                SkP2Ji2tPaPHMW8gta1ariAtrBI= )
```

Abbildung 2.24 Beispielhaftes RR-Paar für einen signierten SRV-RR in der ASCII-Darstellung. Für die Übertragung wird ein anderes Format verwendet.

Dieser beispielhafte SIG-RR enthält folgende Daten, die natürlich auch andere Werte annehmen können:

- Die Zahl 65789 taucht im obigen Beispiel drei mal auf:
  - Im SRV-RR als „Time-to-live“ (TTL) dieses Eintrags, d.h. als Angabe in Sekunden, wie lange dieser Eintrag in einem DNS-Cache gültig bleiben soll.
  - Der SIG-RR hat den gleichen TTL-Wert, denn diese beiden Einträge müssen immer gemeinsam gecacht werden.
  - Der TTL-Wert wird als „Original TTL“ noch einmal im Datenfeld des SIG-RR wiederholt. Der Grund dafür liegt darin, dass die digitale Signatur auch über den TTL-Wert berechnet wird, dieser aber im Cache eines Servers ständig dekrementiert wird. Um die Signatur auch nach einiger Zeit noch aus den gecachten Daten heraus verifizieren zu können, muss der originale TTL-Wert wieder hergestellt werden.
- Die eigentlichen Daten des SIG-RR beginnen mit dem „type covered“-Wert SRV. Für die Codierung dieses Wertes bei der Übertragung stehen 2 Byte zur Verfügung.
- Der Wert 1 gibt den verwendeten Algorithmus an, hier ist es (laut RFC 2535) RSA/MD5.
- Die Zahl 4 gibt die Anzahl der Labels (also der durch einen „.“ getrennten Worte) im Namen (hier _sip._udp.testdomain.de) an.
- Nach dem „original TTL“ folgen die Werte 20050503125727 und 20050403125727, die den Gültigkeitszeitraum der Signatur (im genannten Beispiel vom 31.4.2005 bis zum 31.5.2005) angeben. Für die Übertragung werden diese Werte als Anzahl der Sekunden seit dem 1.1.1970 angegeben.
- Mit Hilfe des „key tags“ 32882 wird der öffentliche Schlüssel identifiziert, der zur Überprüfung der Signatur herangezogen werden muss.
- testdomain.de ist der DNS-Name des Signierers, als die Zone, zu der der öffentliche Schlüssel gehört.
- Abschließend folgt, base64-codiert, die eigentliche Signatur.

Fazit: Der Einsatz von DNSSEC für SRV-Records hilft, den für eine bestimmte Domain zuständigen Proxyserver kryptographisch sicher zu authentifizieren. Dies ist sowohl für SIP als auch für H.323 sinnvoll, und wurde hier für SIP exemplarisch dargestellt. Die SIP-Antworten eines solchen Servers

müssen dann mit anderen Methoden gesichert werden. Als Alternative bietet sich zur Authentifizierung des Proxyservers TLS an.

DNSSEC für ENUM

In ENUM werden für jede Telefonnummer ein oder mehrere NAPTR-RRs angelegt. Diese können, da sie ein RRSet bilden [G04], mit einem SIG-RR (wie im vorigen Abschnitt für SRV-RRs beschrieben) gesichert werden.

Ein Problem stellt die große Anzahl der NAPTR-RRs dar, die mit DNSSEC gesichert werden müssten: Während ein SRV-RR für einen Proxyserver und viele Telefonnummern steht, muss in ENUM für jede einzelne Telefonnummer weltweit eine Signatur erzeugt und, was wichtiger ist, nach Ablauf der Gültigkeit erneuert werden. Für solche Datenmengen stehen Erfahrungen mit DNSSEC noch aus; ein großer Feldversuch wäre sinnvoll.

2.6 Sprachdatenübertragung

2.6.1 Sprachkodierung

Die menschliche Sprache wird zum Zweck der Übertragung digitalisiert. Dabei wird ein analoges Signal zunächst abgetastet, anschließend quantisiert und zum Schluss digitalisiert. In der digitalen Form kann die Sprache z. B. über das IP–Protokoll von einer Quelle zu einer Senke transportiert werden. Um die Information auf digitalem Weg zu übertragen, bedient man sich so genannter Kodierungsverfahren, die nach bestimmten mathematischen Algorithmen die Sprachdaten in ein Codewort oder einen Bitstrom umwandeln. Die erste Sprachkodierung wurde bereits in den 30er Jahren des 20. Jahrhunderts von H.W. Dudley von den Bell Labs entwickelt. In der digitalen Welt des ISDN bedient man sich der Sprachkodierung gemäß G.711 auf der Basis von PCM (Pulse Code Modulation), bei der eine Kompandierung (kleine Amplituden werden vergrößert, große Amplituden verringert) der Sprache mittels einer nichtlinearen Kennlinie erfolgt. Es wird eine a- und eine μ-Kennlinie unterschieden, die jeweils verschiedene Quantisierungsstufen und unterschiedliche Segmenteinteilungen aufweisen. Für tiefergehende Betrachtungen wird an dieser Stelle auf die einschlägige Fachliteratur verwiesen.

In einer VoIP–Umgebung werden gerne Kodierungsverfahren eingesetzt, die eine möglichst geringe Bandbreite bei größter möglicher Sprachqualität bieten.

Name	Bitrate in kBit/s	Standardisiert durch	Kodierungsverfahren
G.711	64	ITU-T	PCM
G.723.1	5,3/6,3	ITU-T	ACELP/MP-MLQ
G.726	32	ITU-T	ADPCM
G.728	16	ITU-T	LD-CELP
G.729	8	ITU-T	CS-ACELP
G.729a	8	ITU-T	CA-ACELP
GSM	13	ETSI	RPE-LTP
iLBC	13,3/15,2	IETF	LPC

Tabelle 2.2: Kodierungsverfahren für Sprache

Die gängigsten Verfahren G.711, G.723.1 und G.729 sollten von einem VoIP-System unterstützt werden. Der Einsatz eines bestimmten Verfahrens kann je nach Ort variieren. In einer LAN-Umgebung, in der genügend Bandbreite zur Verfügung steht, kann auf G.711 zurückgegriffen werden, das eine ISDN-Sprachqualität liefert. Verbindet man verschiedene Lokationen, beispielsweise über

eine VPN-Lösung, so empfiehlt es sich bei schmalbandigen Leitungen ein Verfahren mit geringerem Bandbreitenbedarf zu wählen.

Damit beide Teilnehmer eines Gesprächs die jeweils kodierten Sprachdaten dekodieren können, müssen sie sich vorab über das verwendete Kodierungsverfahren verständigen. Dieser Vorgang wird im Rahmen der Signalisierung (z. B. unter der Zuhilfenahme von SDP) festgelegt. An Netzübergängen ist oftmals eine Umkodierung zwischen den verschiedenen Codecs notwendig, da beispielsweise der G.729-Codec im ISDN nicht üblich ist.

2.6.2 MOS – Mean Opinion Score

Der (MOS) ist in der Telekommunikation ein Verfahren zur subjektiven Beurteilung der Qualität von Sprach- und Bildübertragungen. Er ist das Ergebnis eines festgelegten Ablaufs mehrerer Tests, bei dem die empfundene Qualität der Sprache beziehungsweise der Bilder durch eine Gruppe von Versuchspersonen beurteilt wird. Das Ergebnis der Testreihe wird in eine fünfstufige Qualitätsskala (siehe untenstehende Tabelle) eingeordnet. Mit dem MOS kann die Qualität unterschiedlicher Sprachcodierungen (Codec) oder Bildkompressionsalgorithmen miteinander verglichen werden. MOS ist von der ITU-T in der Empfehlung P.800 spezifiziert (siehe auch [ITUT96a, ITUT96b]).

Wert	quality	Qualität
5	excellent	exzellent
4	good	Gut
3	fair	ordentlich
2	poor	mäßig
1	bad	mangelhaft

Tabelle 2.3 Mean Opinion Score

Für die Erlangung einer Akzeptanz von VoIP-Systemen, sollte immer ein MOS-Wert von > 3,5 angestrebt werden.

Codierungsverfahren	Delay in ms	CPU-Last in MIPS	MOS
G.711	0,75	<1	4,1
G.723.1	30	16	3,65 / 3,9
G.729	10	50	3,92
G.729a	10	10,5	4,7
GSM	20		1,8-3,5

Tabelle 2.4: Delay, CPU-Last und MOS-Werte in Abhängigkeit vom Codierungsverfahren

3. Bedrohungsanalyse beim Einsatz von VoIP-Systemen

Durch den Transport von Sprachdaten über standardisierte, offene Datennetze ergeben sich zahlreiche Bedrohungen gegen VoIP Systeme. 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.

In diesem Kapitel werden zunächst diese Bedrohungen beleuchtet und eine klare Übersicht der Bedrohungslage erstellt. Im Gegensatz zu einer „standardisierten" Bedrohungsanalyse werden die Bedrohungen hier nicht bezüglich des verursachten Schadens und ihrer Eintrittswahrscheinlichkeit bewertet, da diese vom jeweilig betrachteten Gesamtsystem abhängen. Die hier identifizierten Bedrohungen können jedoch als Grundlage bei der Erstellung einer individuellen Bedrohungs- und Risikoanalyse im Kontext seines IT-Systems dienen [ÖIT].

Die ermittelte Bedrohungslage macht die Notwendigkeit umfangreicher und ineinander greifender Sicherheitsmaßnahmen deutlich. Diese Sicherheitsmaßnahmen werden in Kapitel 4 dargestellt und anschließend in Kapitel 6 zu Maßnahmenkatalogen und Umsetzungshinweisen für einige exemplarische Fallbeispiele mit unterschiedlichen Schutzbedürftigkeiten zusammengefasst.

3.1 Definition der Sicherheitsziele

Um die Bedrohungen sinnvoll klassifizieren zu können, ist eine Bestandsaufnahme der Sicherheitsziele in VoIP-Systemen hilfreich. Obwohl die diskutierten Sicherheitsziele orthogonal zueinander sind, bestehen häufig Wechselwirkungen zwischen deren Durchsetzung bzw. zwischen den Bedrohungen auf diese Sicherheitsziele: So kann der Diebstahl eines Zugangspasswortes (Vertraulichkeitsverlust) zum Integritätsverlust eines Rechnersystems führen, wenn der Angreifer das Zugangspasswort nutzt, um unbefugten Zugriff auf das System zu erlangen und dessen Konfiguration zu ändern. Analog kann der Integritätsverlust von Konfigurationsinformationen zum Vertrauchlichkeitsverlust führen, beispielsweise indem eine Verschlüsselung deaktiviert wird oder ein schwaches Verschlüsselungssystem aktiviert wird. Daher können einzelne Sicherheitsziele in der nachfolgenden Bedrohungsanalyse kaum isoliert voneinander betrachtet werden. Die Analyse beschränkt sich daher meist auf die *unmittelbaren* Bedrohungen und geht nicht weiter auf die daraus resultierenden *mittelbaren* Bedrohungen ein.

Des Weiteren bestehen Wechselwirkungen zwischen Sicherheitszielen auf unterschiedlichen Ebenen mehrschichtiger Systeme. So kann beispielsweise die Integrität und Authentizität auf Netzwerkebene Vorraussetzung für die Vertraulichkeit auf Anwendungsebene sein und umgekehrt kann die Verletzung von Integrität und Authentizität auf Netzwerkebene (ARP- und DNS-Spoofing) einen Man-in-the-Middle Angriff ermöglichen, der wiederum die Vertraulichkeit von VoIP-Gesprächen auf Anwendungsebene verletzen kann.

Diese Wechselwirkungen erschweren eine systematische Analyse und Darstellung. Bei der Darstellung der Bedrohungslage werden die einzelnen System- und Netzwerkschichten betrachtet und zwischen den relevanten Sicherheitszielen unterschieden.

Primäre Sicherheitsziele

In allgemeinen Kommunikationssystemen unterscheidet man die drei klassischen primären Sicherheitsziele [ITSEC91]:Vertraulichkeit (engl. confidentiality), Integrität (engl. integrity) und Verfügbarkeit (engl. availability). Dabei bezeichnet „Vertraulichkeit" den Schutz vor unbefugter Preisgabe von Informationen, „Integrität" den Schutz vor unbefugter Veränderung von Informationen und Verfügbarkeit den Schutz vor unbefugter Vorenthaltung von Informationen.

Sekundäre Sicherheitsziele

Aus diesen allgemeinen primären Sicherheitszielen lassen sich weitere, die so genannten sekundären Sicherheitsziele durch Verfeinerung bzw. Spezialisierung definieren [AvLaRaLa2004]. So kann beispielsweise Authentizität als „Integrität von Nachrichteninhalt und Nachrichtenherkunft“ und Zurechenbarkeit (engl. accountability) als „Verfügbarkeit und Integrität von Identitäten (Subjekten) und der von ihnen ausgeführten Aktionen“ definiert werden, indem die primären Sicherheitsziele auf bestimmte Meta-Informationen oder System-Services (wie beispielsweise die Identität des Senders oder allgemeine Abrechnungsinformationen) angewendet werden.

Die nachfolgenden Abschnitte setzen zunächst die genannten allgemeinen klassischen Sicherheitsziele in den Kontext von VoIP-Systemen und dienen somit als Grundlage für die Analyse der Bedrohungslage. Dabei werden insbesondere auch weitere VoIP-spezifische sekundäre Sicherheitsziele beleuchtet.

3.1.1 Integrität und Authentizität

Das primäre Sicherheitsziel Integrität kann sich auf zahlreiche, teilweise systemspezifische Informationen und Meta-Information beziehen und umfasst somit eine Menge weiterer sekundärer Sicherheitsziele, die jeweils die Integrität anderer Informationen betreffen. Als Beispiel sei das Sicherheitsziel „Authentizität von Nachrichten“ genannt, das als Integrität der Nachricht und Integrität der Senderidentität definiert ist.

Im Folgenden werden die konkreten, auf Integrität basierten Sicherheitsziele im Kontext von VoIP-Systemen betrachtet, wobei insbesondere die folgenden Ziele von herausragender Bedeutung sind.

Integrität der VoIP-Systemkomponenten

Die Integrität einer Systemkomponente umfasst sowohl deren Computing Base, d.h. Betriebssystem und VoIP-Software, als auch deren Systemzustände (beispielsweise die Datenbank eines Location Servers, Accounting Daten, Wurzelzertifikate in Servern und Endgeräten oder deren Konfigurationsdateien).

Die Integrität aller VoIP-Systemkomponenten ist von zentraler Bedeutung, weil ein Angreifer das Verhalten kompromittierter Komponenten beliebig steuern kann und somit nach deren Integritätsverlust keinerlei Aussagen mehr über deren Verhalten gemacht werden kann. So kann ein Angreifer VoIP-Endgeräte derart manipulieren, dass die Sprachverschlüsselung deaktiviert wird und die unverschlüsselten Gespräche über einen Rechner des Angreifers geleitet werden. Des Weiteren kann ein Angreifer Schlüsselmaterial und Anruflisten auslesen oder Authentifizierungsinformationen des Benutzers abfangen, um Telefonate unter der Identität des Benutzers zu initiieren.

Noch weitreichender ist der Integritätsverlust zentraler VoIP-Komponenten wie Gateways, Proxies oder Redirect Servern, weil ein Angreifer dadurch Zugriff auf eine große Anzahl von Telefonaten erhält und diese abhören, umleiten oder fälschen kann. Des Weiteren können zentrale Accounting Informationen manipuliert werden, wodurch ein Angreifer Leitungsmissbräuche verschleiern kann. An dieser Stelle erkennt man die starken Wechselwirkungen zwischen den primären Sicherheitszielen, d.h. wie ein Integritätsverlust zum Verlust vertraulicher Daten führen kann. Die Integrität der Systemkomponenten wird primär durch interne Angreifer, Malware oder indirekt durch den Vertraulichkeitsverlust von Credentials wie Zugangspasswörter bedroht.

Neben der Integrität der Systemkomponenten ist die Integrität und Authentizität der übertragenen Daten ein zentrales Sicherheitsziel in VoIP-Sytemen. Dabei muss die Integrität und Authentizität getrennt nach der jeweiligen Art und Semantik der übertragenen Daten betrachtet werden.

Integrität und Authentizität der Sprachdaten

Obwohl Sprachdaten über natürliche Redundanzen und Wiedererkennungsmerkmale[1] verfügen, die deren Integrität und Authentizität in gewissem Umfang schützen, besteht ein weiteres Sicherheitsziel von VoIP-Sytemen darin, die Integrität und Authentizität der Sprachdaten zu gewährleisten. Insbesondere soll dabei auch die Meta-Information „Sendezeitpunkt der Sprachdaten" integer sein, was dem Empfänger garantiert, dass die empfangenen Sprachdaten zeitnah von seinem Gesprächspartner gesendet wurden und nicht eine Kopie (engl. replay) früherer Anrufe sind.

Integrität und Authentizität der Signalisierungsdaten

Neben der Integrität und Authentizität der Sprachdaten, können die Integrität und Authentizität folgender *Meta-Informationen* in der Praxis nicht zu unterschätzende Sicherheitsziele darstellen:

- **Identität des Anrufers und Identität des gerufenen Benutzers:** Kann ein Angreifer die Anruferidentität manipulieren, die seinem Opfer, d.h. dem gerufenen Benutzer, angezeigt wird, kann er erreichen, dass seinem Anruf eine bestimmte Bedeutung zugemessen wird oder überhaupt erst angenommen wird. So wird der Vorstandsvorsitzende einer großen Aktiengesellschaft den vermeintlichen Anruf des Aufsichtsratsvorsitzenden eher persönlich annehmen als den einer ihm unbekannten Person. Darüber hinaus kann ein Angreifer seinem Opfer durch Fälschen der Anruferidentität eine bestimmte Vertrauensbeziehung vortäuschen. So kann sich der Angreifer beispielsweise als Mitarbeiter der IT-Abteilung eines großen Unternehmens ausgeben, um Social Engineering bei den Mitarbeitern zu betreiben.
  Gelingt es einem Angreifer, seine Identität gegenüber dem VoIP-System zu fälschen, so kann er des Weiteren das Abrechnungssystem umgehen, um beispielsweise Services auf Kosten Dritter in Anspruch zu nehmen.
- **Eingangszeitpunkt von Voice Mails:** Häufig ist die Semantik einer Sprachnachricht abhängig von deren Eingangszeitpunkt. Daher sollte diese Meta-Information nicht von einem Angreifer manipuliert werden können.
- **Registrierungs- und Lokalisierungsinformationen:** So spezifiziert der SIP Standard [RFC3261] Antworten mit Status „300 Multiple Choices", die eine Auswahl von Endgeräten zurückliefert, die für eine URI registriert sind. Die Authentizität dieser Information kann in einigen Fällen von großer Bedeutung sein, weil ansonsten ein Anruf an ein unerwünschtes Endgerät geleitet werden könnte. Ein weiterer wichtiger Aspekt ist die Integrität von Registrierungsinformationen, da ein Fälschen dieser Information die Umleitung von Anrufen ermöglichen könnte (engl. registration hijacking [RFC3261]) und somit Auswirkung auf die Verfügbarkeit einzelner Teilnehmer oder ganzer Domains sowie auf die Vertraulichkeit von Gesprächs- und Metadaten haben kann. Durch Fälschen einer „Moved Permanently" Antwort kann ein Angreifer alle eingehenden Anfragen nach einem Endgerät auf sich ziehen (engl. call hijacking [RFC3261]) und als Man-in-the-Middle agieren.
- **Status von Endgeräten:** Auch der Status von Endgeräten stellt in bestimmten Situationen eine wesentliche Information dar, die vom Empfänger dieser Statusinformation interpretiert wird und bestimmte Reaktionen auslösen kann. So ist es beispielsweise möglich, dass ein gefälschtes „Besetztzeichen" (z. B. SIP Nachrichten mit Status „486 Busy Here" oder Status „600 Busy Everywhere" [RFC3261]) dem Anrufer suggeriert, dass eine Person an einem bestimmten Ort ist und ihn zu weitreichenden Fehlschlüssen verleitet.
- **Status eines Rufes:** VoIP-Systeme unterscheiden mehrere Statuszustände für Anrufe, deren Integrität ein Sicherheitsziel von VoIP-Systemen darstellt. Ein möglicher Status eines initiierten Anrufes ist, dass der Anruf abgewiesen wurde (SIP Nachricht mit Status „603 Decline" [RFC3261]). Ist die Information über eine Rufabweisung nicht authentisch, kann dies wieder zu Fehlschlüssen auf Seiten des Anrufers führen. Sendet ein Angreifer eine gefälschte SIP Nachricht

[1] Solche Wiedererkennungsmerkmale existieren natürlich nur dann, wenn die Gesprächspartner einander bereits kennen und zuvor identifiziert haben.

(Status „603 Decline“ [RFC3261]), kann er dieses Sicherheitsziel verletzen. Ein weiteres Beispiel für kritische Statusinformationen betrifft die Anzahl von Anrufern, die sich in einer Warteschleife befinden. So können gefälschte SIP Antworten mit Status „182 Queued“ [RFC3261] dem Anrufer suggerieren, dass er sich in einer Warteschlange befindet und noch eine große Anzahl anderer Anrufer vor sich hat. Solche gefälschten Nachrichten veranlassen möglicherweise den Anrufer dazu, einen wichtigen Anruf zu verschieben.

Wie in Kapitel 2 erläutert wurde, erfolgt die Steuerung von VoIP-Gesprächen (inklusive Rufaufbau und Rufabbau) und Übermittlung dieser Meta-Informationen durch den Austausch von Signalisierungsnachrichten. Dadurch kommt deren Integrität und Authentizität eine zentrale Bedeutung zu.

Bei fehlender Authentifizierung von Signalisierungsnachrichten lassen sich des Weiteren folgende Bedrohungen identifizieren. So kann sich ein Angreifer als VoIP-Server ausgeben (engl. impersonation) und Antworten auf Client Anfragen fälschen. Dadurch können weitere Sicherheitsziele (die Vertraulichkeit von Benutzer Credentials oder die Verfügbarkeit des VoIP-Dienstes, beispielsweise durch Fälschen von BYE-Nachrichten) verletzt werden.

Fehlende Authentifizierung von Signalisierungsnachrichten ermöglicht das so genannte **URI Spoofing (**analog zum URL-Spoofing heutiger Phishing Angriffe) und Fälschen der Gegenstellenidentifikation. Hierdurch können Angreifer das Opfer dazu veranlassen, VoIP-Telefonate zu einer vermeintlich vertrauten Gegenstelle zu initiieren. In Wahrheit zeigt der URI (Abk. für unique resource identifier, zu deutsch „einheitlicher Kennzeichner von (Internet-) Ressourcen“) jedoch auf ein Endgerät des Angreifers. So könnte ein Angreifer (analog zum so genannten Phishing [AGS05]) beispielsweise eine E-Mail im Namen einer Bank an sein Opfer senden, mit der Bitte die Telefonbanking Abteilung der Bank per VoIP-Anruf zu kontaktieren, indem er einfach dem enthaltenen Link auf eine VoIP URI folgt. Fehlende Authentizität von Signalisierungsnachrichten macht es dem Opfer unmöglich, die gewünschte Gegenstelle, d.h. seine Bank, zuverlässig zu identifizieren.

3.1.2 Vertraulichkeit

Wenn im Kontext von VoIP-Systemen über Vertraulichkeit gesprochen wird, liegt der Fokus dabei meist auf der Vertraulichkeit der Sprachdaten, was der Abhörsicherheit von Telefonaten entspricht [KWF05]. Des Weiteren werden dabei grundsätzlich die folgenden Unterschiede zwischen traditioneller PSTN/PBX Telefonie und VoIP Telefonie angeführt [KWF05,Klein03]:

1. **Physischer Zugang zum Transportnetz:** Traditionelle Telefonie läuft meist über separate Transportnetze, weshalb ein Angreifer sich zunächst physischen Zugang zu diesem Transportnetz verschaffen muss. Im Gegensatz dazu verwenden VoIP-Systeme ein IP-Transportnetz, das sie sich mit dem normalen Datenverkehr teilen und auf das daher zunächst auch alle angeschlossenen Rechner Zugriff haben.
2. **Proprietäre Protokolle:** Viele Protokolle in der traditionellen Telefonie sind proprietär und daher kaum öffentlich dokumentiert. Daher ist deren Analyse nicht ohne spezielle Hardware und Software möglich, was den potentiellen Täterkreis von Lauschangriffen deutlich reduziert. Dieses Argument ist nachvollziehbar, aber es sollte betont werden, dass hierdurch eine trügerische Sicherheit vermittelt wird, weil Nachrichtendienste oder sonstige Spezialisten diese Protokolle ohne weiteres analysieren und manipulieren können. Daher sollten bei entsprechender Schutzbedürftigkeit auch in der traditionellen Telefonie zusätzliche Sicherheitsmaßnahmen ergriffen werden.

Die Vertraulichkeit von Sprachdaten ist daher sicher zu Recht eine der zentralen Sicherheitsziele in VoIP-Systemen.

Neben der Vertraulichkeit der eigentlichen Sprachdaten ist die Vertraulichkeit von Credentials und Schlüsselmaterial, das zur Identifikation von Benutzern und Endgeräten dient, von zentraler Bedeutung, da deren Vertraulichkeitsverlust weitere Sicherheitsziele kompromittieren könnte. Auch sind benutzerspezifische Konfigurationsdaten, wie persönliche Ruflisten und Telefonbucheinträge, kritische Informationen, deren Vertraulichkeit in VoIP-Systemen geschützt werden sollte.

Schließlich soll an dieser Stelle die Vertraulichkeit weiterer Meta-Informationen hervorgehoben werden, die ebenfalls eine wichtige Sicherheitsanforderung darstellt und in den meisten bekannten Abhandlungen über VoIP-Sicherheit vernachlässigt wird. Beispiele kritischer Meta-Informationen von Telefongesprächen sind die Dauer von Gesprächen sowie die Identität der Gesprächsteilnehmer. Diese Informationen stellen in einigen Szenarien wertvolle, schützenswerte Informationen dar. Weitere Beispiele für vertrauliche Meta-Informationen sind Registrierungs- und Lokalisierungsinformationen von Nutzern des VoIP-Systems. So kann ein Angreifer beispielsweise nach Erhalt einer SIP Response „300 Multiple Choices“ Rückschlüsse auf mögliche Aufenthaltsorte einer Person schließen. Ähnlich schützenswert sind Informationen über die Anwesenheit bzw. Erreichbarkeit von Gesprächsteilnehmern, die bei entsprechender Konfiguration durch Statusnachrichten (Status „486 Busy Here“ oder Status „600 Busy Everywhere“) preisgegeben werden könnten.

Des Weiteren stellt die interne Netztopologie eine wertvolle Information dar, deren Vertraulichkeit trotz der Verwendung von VoIP geschützt werden sollte, da diese Interna Angriffe gegen das gesamte IT-System erleichtern können.

Kann ein Angreifer Pakete auf dem Netzwerk mitlesen, so können die darin übertragenen Signalisierungsnachrichten und Medienströme leicht mit frei verfügbaren Sniffern (z. B. Ethereal) herausgefiltert und interpretiert werden. Die in Sniffern integrierten Protokoll-Interpreter sind sehr leistungsfähig und erlauben selbst Laien die Analyse gängiger VoIP-Protokolle (inkl. H.225, H.245, SIP und RTP).

3.1.3 Verfügbarkeit

Verfügbarkeit im Kontext von VoIP-Systemen bedeutet primär die Verfügarkeit des Telefoniedienstes sowie eine hinreichende Gesprächsqualität. Für viele Wirtschaftszweige (Banken, Versicherungen, Versandhäuser) sowie Behörden und Rettungskräfte ist diese Art der Verfügbarkeit von zentraler Bedeutung und somit ebenfalls eine wesentliche Sicherheitsanforderung an das VoIP-System.

Neben der Verfügbarkeit des Telefonieservice selbst, ist darüber hinaus die Verfügbarkeit bestimmter Meta-Informationen zum sinnvollen Betrieb von VoIP-Systemen notwendig. Dabei ist insbesondere die Verfügbarkeit von (authentischen) Accounting Informationen wie Anrufer, Ziel, Zeitpunkt und Dauer von Gesprächen zum Betrieb von VoIP-Systemen von Bedeutung. Ist diese Information nicht verfügbar, können die entstandenen Kosten nicht mehr abgerechnet werden.

Schließlich kann die Verfügbarkeit (und Authentizität) der Identität des Anrufenden zur Abwehr von Spam over Internet Telephony (Spit), d.h. Spam in der IP-Telefonie, von Bedeutung sein.

Bedrohungen und Angriffe gegen diese Verfügbarkeitsziele werden in den nachfolgenden Abschnitten vertieft. Zunächst sollen aber einige zentrale Angriffsklassen definiert werden, die zur systematischen Untersuchung der Bedrohungslage in VoIP-Systemen herangezogen werden.

3.2 Angriffsklassen

Angriffe gegen IT-Systeme verfolgen immer das Ziel eine oder mehrere Sicherheitseigenschaften zu verletzen, wie beispielsweise die Erlangung vertraulicher Informationen (Verletzung der Vertraulichkeit) oder die Störung einer bestimmten Funktionalität (Verletzung der Verfügbarkeit).

Neben dem Ziel eines Angriffes lassen sich Angriffe auch anhand weiterer Merkmale klassifizieren:

- *Eigenschaften des Angreifers*, beispielsweise, ob ein Angreifer aktiv oder nur passiv beobachtend agiert, ob es sich um einen Innentäter (engl. insider) oder einen Außentäter (engl. outsider) handelt oder ob der Angreifer Kontrolle über bestimmte (zentrale) Systemkomponenten besitzt,
- dem *Angriffspunkt,* der die Systemkomponenten bezeichnet, an denen ein Angriff ansetzt (Endgeräte, zentrale Systemkomponenten oder Netzwerkverbindungen), sowie

- der *Ebene,* auf der ein Angriff ansetzt, beispielsweise Angriffe auf niedrigen Systemschichten, wie der Betriebssystemschicht oder der TCP/IP Schicht, oder Angriffe auf höheren Systemschichten wie Anwendungssoftware oder Anwendungsprotokolle.

3.2.1 Klassifizierung von Netzwerkangriffen

VoIP-Systeme sind IP-basierte Anwendungen und erben als solche alle Schwächen und Bedrohungen des zugrunde liegenden IP-Netzes. Im Folgenden wird ein kurzer Überblick über bekannte Angriffe in IP-Netzen gegeben. Man unterscheidet zwei Angriffsklassen: *passive Angriffe* bestehen im Mitlesen, Protokollieren und Auswerten (engl. sniffing) von Nachrichten, die über das Netzwerk gesendet werden.

Weitaus mächtiger sind *aktive Angriffe*, die Nachrichten (Pakete) auf dem Netzwerk manipulieren oder neue Nachrichten an das Opfersystem senden. Ein starker aktiver Angreifer ist der so genannte Man-in-the-Middle, der zwischen zwei kommunizierenden Systemen A und B sitzt und über den alle ausgetauschten Nachrichten laufen. Der Man-in-the-Middle kann somit ausgetauschte Nachrichten beliebig manipulieren oder eigene Nachrichten in fremden Namen senden. Ein Angreifer kann zum Man-in-the-Middle werden, indem er eine Netzkomponente (z. B. einen Router) unter seine Kontrolle bringt oder Pakete über ein von ihm kontrolliertes System umleitet, indem er Schwächen und fehlende Sicherheitsmaßnahmen in Protokollen des darunter liegenden Netzwerkes ausnutzt. So kann ein Angreifer in IP-Netzen beispielsweise mittels Spoofing Angriffen (siehe unten) zum Man-in-the-Middle werden.

Im Folgenden werden bekannte, für VoIP-Systeme relevante, aktive Angriffe in IP-Netzen dargestellt.

Netzwerk- und Port-Scans

Bei Netzwerk- und Port-Scans sendet der Angreifer Anfragen in ein Netzwerk oder an einen Rechner, um bestimmte Informationen (wie Rechner eines Subnetzes, installierte Dienste, installierte Betriebssysteme und deren Versionen) zu ermitteln. In der Praxis werden sie meist zum Auffinden möglicher Schwachstellen und zur Vorbereitung des eigentlichen Angriffs verwendet.

Spoofing Angriffe

Bei Spoofing Angriffen sendet der Angreifer Nachrichten oder Pakete mit gefälschten Informationen. Diese werden häufig als Baustein oder in Kombination mit weiteren Angriffstechniken verwendet. Bekannte Spoofing Angriffe umfassen das **IP Spoofing**, wobei der Angreifer Teile des IP-Headers (meist die IP-Quelladresse) fälscht, beispielsweise, um Adressen-basierendes Vertrauen in dem Opfersystem auszunutzen. Beim **ARP Spoofing** fälscht der Angreifer ARP-Antworten, wodurch das Opfersystem eine IP-Adresse mit einer falschen MAC-Adresse (engl. medium access control) assoziiert und somit IP-Pakete im Ethernet-LAN fehlgeleitet werden. Beim **DNS Spoofing** fälscht der Angreifer DNS-Antworten und kann dadurch das Opfersystem auf seine eigene IP-Adresse umleiten.

Replay Angriffe

Replay Angriffe bestehen darin, dass ein Angreifer (authentisierte) Nachrichten aufzeichnet, um sie zu einem späteren Zeitpunkt erneut zu senden.

DoS und DDoS Angriffe

DoS (engl. denial of service) Angriffe zielen auf die Verfügbarkeit von IT-Systemen, indem deren Ressourcen wie Speicher, Rechenleistung oder Netzwerkbandbreite in hohem Maße durch den Angreifer verbraucht werden. DoS Angriffe können darin bestehen, dass der Angreifer den Service des Opfersystems regulär nutzt (beispielsweise eine große Anzahl legaler Suchanfragen startet). Häufiger werden jedoch Schwachstellen in Implementierungen (z. B. des Netzwerkstacks beim Ping

of Death [Klein01]) oder in Protokollen (z. B. der TCP-Handshake beim SYN-Flooding oder der Broadcast von ICMP Echo Request beim Smurf-Angriff [Klein01]) ausgenutzt.

Unter DDoS (engl. distributed denial of service) Angriffen versteht man einen konzertierten DoS Angriff, bei dem mehrere Systeme, häufig durch den Einsatz von Malware und durch einen einzelnen Angreifer gesteuert, einen DoS Angriff gegen das Opfersystem durchführen. Durch die hohen QoS-Anforderungen von VoIP-Systemen sind diese extrem anfällig gegen DoS-Angriffe.

3.3 Bedrohungen auf der Netzwerkebene

Im Allgemeinen lässt sich feststellen, dass die Untersuchung hinsichtlich der Bedrohungen einer VoIP-Systemumgebung in großen Teilen zu ähnlichen Ergebnissen kommt, wie sie in Ethernet- bzw. IP-basierten Netzen im LAN bzw. WAN vorzufinden sind. Über die dort anzutreffenden Bedrohungen hinaus können verschiedene VoIP-spezifische Bedrohungen identifiziert werden, die ihrerseits auf Schwächen der verwendeten Signalisierungsprotokolle bzw. auf unverschlüsselte Übertragung von Sprach- und Signalisierungsdaten zurückzuführen sind. Im Vergleich zur klassischen Telekommunikation ist in einem konvergierenden Netz ein deutlich größerer Personenkreis (Netzwerkadministratoren, externe Dienstleister, Mitarbeiter, Provider) in der Lage, mit einfachen Mitteln (PC, Software) Angriffe auf das LAN auszuführen. In den folgenden Abschnitten wird ein systematischer Überblick über die verschiedenen Bedrohungen gegeben, mit dem Ziel, den Leser hinsichtlich der möglichen Schwachstellen im Netzwerk zu sensibilisieren. Die Bedrohungsanalyse wird durch den konkreten Bezug auf die VoIP–Thematik vervollständigt.

3.3.1 Netzwerkinfrastruktur

Verkabelungssystem, Datenverteiler und Serverräume

Durch einen physikalischen Zugriff auf IP-Telefonsysteme, das Netzwerk oder die Netzwerkkomponenten besteht die Möglichkeit einer totalen Kompromittierung des Systems. Ein böswilliger Angreifer, der sich den physikalischen Zutritt zu dem IT-Netzwerk oder den Netzwerkkomponenten verschafft, hat größere Manipulationsmöglichkeiten als bei einer herkömmlichen TK-Anlage. Dies ist eine unmittelbare Folge aus dem grundsätzlich anderen Aufbau des VoIP-Telefonsystems. Die physikalische Bedrohung umfasst alle IT-Komponenten vom Workgroup-Bereich über den Tertiär-Bereich bis zum Core-Bereich. Insbesondere betrifft das sämtliche Call-Server, VoiceMail-Server, Gateways, Gatekeeper, sowie alle Router, Core-Switches und Workgroup-Switches. Angriffe auf zentrale Komponenten (DHCP-Server, Call-Server, Firewall, Gatekeeper, Proxy-Server, Radius-Server) sind kritischer einzustufen als Angriffe auf die Komponenten im Tertiärbereich, weil die Schadenswirkung auf das Telefonsystem erheblich größer ist. Eine Manipulation an einem zentralen Server wie Call-Server, DHCP-Server oder Radius-Server führen zum Totalausfall der Telefonie, während von Manipulationen im Tertiärbereich lediglich einzelne Bereiche des Telefonsystems betroffen sind.

Zu den bedrohten Bereichen gehören auch alle wichtigen Kabeltrassen, Kabelverteilersysteme, Datenverteiler, USV-Räume, Leittechnikräume und Klimaräume. Falls ein Angreifer physikalischen Zugriff erlangt, können Eingriffe wie Trennung der Komponenten vom Stromnetz, Kurzschluss in der Stromversorgung, Durchtrennung der Kabel, Änderungen an Verkabelungsinfrastruktur oder Manipulation der Klima-Einstellung zu Störungen oder zum Totalausfall der IP-Systeme und damit auch des Telefonsystems führen.

Server und Netzwerkkomponenten stehen oftmals in unverschlossenen und unüberwachten Räumen und eröffnen dem Angreifer einen direkten Zugang zur Konsolenschnittstelle der Systeme. Der Angreifer kann die Integrität des Systems verändern und dadurch das Telefonsystem außer Betrieb setzten, sich einen unberechtigten Telefonanschluss einrichten, eine Rufumleitung einrichten, einen 0190-Rufzugang konfigurieren, Systemeinstellungen löschen oder eigene Software aufspielen wie z. B. eine Backdoor-Software, Protokolldaten verändern, Zugangskennungen einrichten oder

verändern; er hat die Möglichkeit, Datenträger mit sensitiven Informationen zu entwenden und andere Manipulationen vorzunehmen.

Bedrohungen auf der Ebene Layer 2

In den meisten Fällen kann davon ausgegangen werden, dass in einem heutigen Unternehmen die Netzwerkinfrastruktur auf der Basis von Ethernet-Switches und Routern aufgebaut ist. War man lange Zeit der Meinung, dass geswitchte Netze gegenüber Netzen auf Hub–Basis für mehr Sicherheit sorgen, so weiß man heute, dass dies keineswegs der Fall ist.

Die Adressierung von Frames innerhalb einer Broadcastdomäne erfolgt mit MAC-Adressen, die jeweils an eine Netzwerkkarte gebunden sind. Wird ein System neu in ein Netzwerk integriert, so flutet er einen eingehenden Ethernet-Frame auf alle Ports, außer dem Port, von dem er den Frame empfangen hat. Durch den Empfang dieses Frames hat der Switch gelernt, dass sich die MAC-Adresse des Frames auf diesem Port befindet. Antwortet ein Zielsystem und sendet einen Frame an die ursprüngliche MAC–Adresse, lernt der Switch die MAC–Adresse des Zielsystems und bindet dessen MAC-Adresse an den entsprechenden Port. In der weiteren Kommunikation werden die Frames zwischen den beiden Kommunikationspartnern nicht mehr auf allen Ports ausgegeben, sondern nur noch auf den Ports, an die die jeweilige MAC-Adresse gebunden ist. Andere Systeme, die auch an dem Switch angeschlossen sind, können den Verkehr zwischen den Beteiligten nicht sehen. Die Zuordnung von MAC-Adresse zu Port wird in einer Tabelle gepflegt, der so genannten MAC-Table, die eine speicherabhängige maximale Größe annehmen kann. Die Einträge in dieser MAC-Table unterliegen einer bestimmten endlichen Lebensdauer, nach deren Ablauf die MAC-Table neu aufgebaut wird.

MAC Spoofing

Sendet ein Angreifer Frames mit der (gefälschten) MAC-Adresse eines anzugreifenden Endsystems an einen Switch, so trägt dieser den Port, an dem der Angreifer angeschlossen ist mit der MAC-Adresse des Endsystems in seine Tabelle ein und sendet alle Ethernetrahmen, die für das Endsystem bestimmt sind, an den Angreifer. Der ursprüngliche Eintrag in der MAC-Table ist überschrieben, und das angegriffene System erhält solange keine Datenübermittlung vom Switch, bis es selbst einen Frame aussendet und der Switch den Eintrag in der Tabelle wieder überschreibt. Sendet der Angreifer ständig Frames mit gefälschter MAC-Adresse aus, führt er einen DoS–Angriff gegen das Endsystem aus.

Durch das MAC Spoofing können alle VoIP-spezifischen Systeme (Telefone, VoiP–Server, Gateways, Gatekeeper, MCU) angegriffen und ihre Funktion innerhalb des Netzwerkes gestört werden.

Wird der Angriff auf MAC-Adressen von IP–Telefonen ausgeführt bzw. Softphones, die auf Rechnern laufen, sind die jeweiligen Teilnehmer nicht mehr erreichbar. Von den angegriffenen Geräten können keine Gespräche aufgebaut bzw. geführt werden.

Angriffe auf zentrale VoIP-Server können die Telefonie innerhalb einer ganzen VoIP–Domäne ausschalten. Betroffene Gateways können nicht erreicht werden, und die Kommunikation vom und zum PSTN ist in Folge dessen nicht mehr möglich.

MAC Flooding

Durch die Aussendung einer erheblichen Anzahl von Frames mit unterschiedlichen gefälschten MAC-Adressen kann die MAC-Table eines Switches derart aufgefüllt werden, dass die Grenze des zur Verfügung stehenden Speichers überschritten wird. In diesem Fall flutet der Switch empfangene Rahmen an alle Ports (auch auf den des Angreifers), und ein Angreifer kann beispielsweise die Signalisierung eines Rufaufbaues mitlesen bzw. ein bestehendes Gespräch abhören oder gar die Registrierungsinformationen (Benutzername, Kennwort) zwischen IP-Telefonen und einem VoIP–Server bzw. die Authentisierung zwischen VoIP-Server und Gateway oder IP-Telefon und Gateway abfangen. Basierend auf den gesammelten Informationen können Identitätsbetrug (Anmeldung an VoIP-Servern bzw. Gateways mit den erspähten Benutzerdaten) und Gebührenbetrug (Toll Fraud)

betrieben werden. Die übermittelten Informationen können als Grundlage für die Übernahme von Gesprächen bzw. Signalisierungsströmen verwendet werden.

ARP Spoofing

Das ARP-Protokoll ist ein Hilfsprotokoll, das einem System die dynamische Zuordnung zwischen einer IP-Adresse und der MAC-Adresse erlaubt und so die Kommunikation innerhalb eines Netzwerksegmentes ermöglicht.

Die Zuordnung von IP–Adresse zur MAC-Adresse wird in einem so genannten ARP-Cache in jedem Endsystem gespeichert und kann durch entsprechende ARP-Pakete (ARP Reply) verändert werden. Durch gezielt eingesetzte ARP–Pakete, die beispielsweise an ein IP–Telefon und an einen Router gesandt werden, kann der Netzwerkverkehr zum Angreifer umgeleitet werden. Das angegriffene Endsystem verwendet die MAC-Adresse des Angreifers fälschlicherweise als die des Routers, und der Router verwendet sie als die MAC-Adresse des IP-Telefons. So kann ein Angreifer sämtlichen Verkehr mitlesen und ggf. verändern bzw. eine Sitzung oder einen Rufaufbau übernehmen und so beispielsweise eine Identität vortäuschen und möglicherweise unberechtigt kostenpflichtige Anrufe absetzen (Toll Fraud). Sämtliche Kommunikationsbeziehungen innerhalb einer Broadcastdomäne können mit dieser Art von Angriffen kompromittiert werden. Telefongespräche können auf andere Systeme (Gateway, VoIP-Server) des Angreifers umgeleitet und dadurch vollständig kontrolliert und manipuliert werden. Gleiches gilt für die Kommunikation zwischen einem Gateway und einem VoIP–Server.

STP-Attacken

Mit STP (Spanning Tree Protocol) können redundante Layer 2-Strukturen aufgebaut werden, die ausgehend von einer Wurzel (Root-Bridge) einen nach dem Spanning Tree-Algorithmus aufgebauten, schleifenfreien Pfad zu allen beteiligten Switches (Bridges) bilden. Durch Versenden falscher Protokollinformationen (BPDU – Bridge Protocol Data Unit) können DoS-Angriffe durchgeführt werden, die eine erneute Berechnung des Spanning Trees in angegriffenen Switches provozieren und diese dadurch einige Sekunden von der aktiven Teilnahme an der Kommunikation ausschließen. Die Folge hiervon können je nach betroffenem Switch Unterbrechungen der Kommunikationsverbindung zwischen IP-Telefon und VoIP-Server bzw. Gateway sein. Insbesondere können Angriffe auf Switches, an denen zentrale Komponenten angeschlossen sind, den kompletten Telefonverkehr lahm legen.

Ein weiterer STP-basierender Angriffstyp beruht auf der Anbindung eines Angreifers an zwei Switches. Ein Angreifer, der beispielsweise zwei Netzwerkkarten in seinem System im Bridge-Mode betreibt und am STP teilnimmt, kann Parameter (Kosten, Bridge-ID) derart verändern, dass sämtlicher Verkehr über seinen PC läuft. Das ermöglicht ihm den VoiP-Verkehr zu manipulieren bzw. die Kommunikation zu stören (DoS). Man in The Middle-Angriffe wie Abhören der RTP–Ströme zwischen den VoIP–Komponenten, Übernahme (Highjacking) von Anrufen bzw. Rufaufbau sowie Identitäts- und Gebührenbetrug (Toll Fraud) können die Folge sein. Es sind Umleitungen des Telefonie- und Signalisierungsverkehrs auf Systeme des Angereifers (VoIP-Server, Gateway) möglich, die zum Ausspähen von Benutzerdaten (Registrierung an einem VoIP–Server) oder zum Abhören des Gesprächs missbraucht werden können.

VLAN-Angriffe

VLANs basieren auf einer logischen Trennung auf Layer 2, bei der eine Gruppe von Ports durch Markierung (Coloring) innerhalb des Switches zu einem logischen Netzwerk (Broadcastdomäne) zusammengefasst werden können. Eine Kommunikation zwischen diesen logischen Netzen ist nur über Router (Layer 3) möglich. Werden logische Netze über mehrere Switches aufgebaut, werden die Frames, die zu einem VLAN gehören, durch eine Protokollmarkierung zwischen den Switches über den so genannten Trunk-Port ausgetauscht. Jedes VLAN hat eine eigene ID, die der VLAN-Markierung entspricht. Baut der Angreifer eine Trunk–Verbindung zu einem Switch auf, so kann er Zugriff auf alle logischen Netze erhalten und sämtliche in diesem Kapitel aufgeführten Angriffe

ausführen. Die möglichen Angriffe auf VoIP-Systeme entsprechen den unter ARP-Spoofing bzw. STP-Attacken beschriebenen Angriffstypen.

Ein weiterer Angriffspunkt ist das VLAN–Hopping, bei dem der Angreifer einen Frame gleich zweifach markiert und dadurch Ethernet-Frames von einem Switch zu einem anderen Switch in ein anderes VLAN leiten kann. Die erste Markierung entspricht dem Native VLAN und die zweite Markierung dem des anzugreifenden VLANs. Der Switch entfernt beim Empfang die erste Markierung und leitet den Frame über einen Trunk-Port zum nächsten Switch. Die zweite Markierung wird entfernt und der Ethernetframe an das entsprechende Endsystem weitergeleitet. Es sind DoS-Attacken auf alle VoIP-Systemkomponenten (VoIP–Server, IP-Telefone, Gateways) möglich, die zum Ausfall der jeweiligen Einheit führen und dadurch zur Einschränkung der Kommunikation bis hin zum Totalausfall führen können.

Bedrohungen auf der Layer 3-Ebene

IP Spoofing

Verwendet ein Angreifer unberechtigt eine IP-Adresse, die einen anderen Ursprung vortäuscht, so spricht man von IP-Spoofing. Denkbare Bedrohungen sind die Überlistung von Paketfiltern auf Routern oder Firewalls, die den Netzzugang zu schützenswerten Ressourcen, beispielsweise einem VoIP–Server oder einem VoIP-Gateway, sicherstellen sollen, sowie DoS- und dDoS-Attacken (verteilter Angriff auf die Verfügbarkeit eines Dienstes). Daraus resultieren weitere mögliche Attacken, wie Toll Fraud (Gebührenbetrug), unberechtigtes Einloggen auf den VoIP-Systemkomponenten oder illegales Anmelden eines IP-Telefons an einem VoIP–Server bzw. Gateway.

ICMP Redirect

ICMP-Nachrichten werden zur Steuerung bzw. Fehlerbenachrichtigung in IP-Netzen verwendet. ICMP-Nachrichten werden von nahezu allen heutzutage eingesetzten Netzteilnehmern (Rechner, Router) auf Layer 3 verarbeitet. Eine ICMP Redirect-Nachricht wird durch einen Router an ein Endsystem versendet, um dieses über eine bessere Route zu informieren. Bei einem Angriff versendet ein Angreifer eine ICMP Redirect-Nachricht mit einem fingierten Gateway an das anzugreifende Endsystem, um so entweder die Pakete für bestimmte Ziele umzuleiten oder auf nicht erreichbare Ziele umzulenken und so einen DoS zu provozieren. Umleitungen des VoIP-Verkehrs können hier zum Abhören der Kommunikationsströme (Sprach- und Signalisierungsdaten) und deren Manipulation führen. Das Ausspähen von Benutzerdaten kann zum Identitäts- und somit zum Gebührenbetrug verwendet werden.

IRDP Spoofing

Mit IRDP (ICMP Router Discovery Protocol) werden Endsysteme über die IP–Adresse des im Netz zuständigen Gateways informiert. Ein Angreifer kann mit gefälschten IRDP-Paketen den Default Gateway-Eintrag eines Endystems überschreiben, so den Paketstrom umleiten und dadurch einen DoS einleiten oder die Paketinhalte manipulieren, sie mitschneiden oder eine Sitzung komplett übernehmen. Durch einen IRDP-Angriff können alle VoiP-Systemkomponenten kompromittiert werden.

Route Injection

In größeren Campus- bzw. Unternehmensnetzen werden oftmals dynamische Routingprotokolle eingesetzt, die bei Fehlkonfiguration (z. B. kein MD 5-Passwort bei RIP2 oder OSPF-Nachbarn gesetzt) das Einschleusen falscher Routen ermöglichen und so eine Umleitung von IP–Paketen für bestimmte Ziele ermöglichen.

VoIP-relevante Datenströme (RTP, Signalisierung, Registrierung) können umgeleitet werden, und ein Angreifer kann dann sämtliche Daten mithören bzw. manipulieren. Die Folge können Identitätsbetrug, Gebührenbetrug sowie die Verletzung der Vertraulichkeit sein.

HSRP- und VRRP -Angriffe

HSRP (Hot Standby Router Protocol) und VRRP (Virtual Router Redundancy Protocol) sind Protokolle zwischen Routern bzw. Gateways, die einem lokalen Netzwerk ein redundantes Gateway in Form eines virtuellen Systems zur Verfügung stellen, wobei mindestens zwei oder mehrere Gateways bzw. Router zu einem virtuellen System zusammengefasst werden. Durch Injektion gefälschter HSRP- oder VRRP-Nachrichten kann das System des Angreifers zum aktiven Gateway werden und so sämtlichen Verkehr kontrollieren, der über das Gateway geführt wird.

DHCP Starvation

Durch Vortäuschung von DHCP-Paketen kann ein Angreifer mit einer beliebigen Anzahl von gefälschten MAC-Adressen sämtliche vom DHCP-Server zu vergebenden IP-Adressen an sich binden und berechtigten Clients die IP-Adressen absaugen. Dadurch wird den Clients die Möglichkeit genommen, am Netzwerk teilzunehmen, was bei IP-Telefonen, die Ihre IP-Adresse und weitere Informationen über DHCP zugewiesen bekommen, bedeutet, dass sie nicht nutzbar sind. Bei diesem Angriff handelt es sich um einen DoS-Angriff.

DHCP Rogue Server

Wird in ein bestehendes Netzwerk, das unter anderem auch einen DHCP-Server zur Vergabe von Netzwerkkonfigurationen (IP–Adresse, Standard-Gateway, TFTP-Server) verwendet, unberechtigterweise ein weiterer DHCP-Server angeschlossen, so spricht man von einem DHCP Rouge Server. Über einen Rouge Server können sämtliche vergebenen Parameter manipuliert werden und so DoS- oder auch Man-In-The-Middle-Attacken ausgeführt werden.

Durch die Verbreitung eines falschen TFTP-Servers mittels DHCP können IP–Telefone, die nach dem Einschalten ihre Konfiguration bzw. ihr Betriebssystem von einem TFTP-System beziehen, manipulierte Daten bzw. Dateien von einem Angreifersystem laden und so vollständig unter die Kontrolle des Angreifers geraten. In den Konfigurationsdateien können falsche Gateway-Adressen bzw. VoIP-Server eingetragen sein, an denen sich ein kompromittiertes Endgerät anmeldet, bzw. über die es seine Kommunikatikonsströme führt. Dadurch sind das Abhören und die Manipulation der Kommunikationsströme (Sprache, Signalisierung, Anmeldung) mit den schon aufgezeigten Folgen möglich.

Die Verbreitung eines falschen Gateways ermöglicht dem Angreifer sämtliche Kommunikationsdaten auf ein von ihm kontrolliertes System umzuleiten, um so die Kommunikation abzuhören, Signalisierungsströme zu verfälschen, oder eine Kommunikation gänzlich zu unterbinden.

Die Zuweisung eines unter der Kontrolle des Angreifers liegenden DNS-Servers ermöglicht DNS Spoofing-Angriffe, die zur Umleitung von Kommunikationsströmen mit den schon aufgezeigten Folgen führt.

Ping Flood

Das Opfersystem wird mit größtmöglicher Geschwindigkeit mit echo request-Paketen - also ping-belastet. Das Opfersystem ist fast ausschließlich damit beschäftigt, darauf zu antworten und kommt seinen eigentlichen Aufgaben nicht mehr nach. Werden diese Attacken auf VoIP-Komponenten ausgeführt, so kann es zu erheblichen Betriebsstörungen bzw. zum Totalausfall der Kommunikation kommen.

Bedrohungen auf der Layer 4-Ebene

SYN Flood

Diese Angriffe basieren auf einer großen Menge von Verbindungsanfragen, die den Protokollstack eines Systems so stark belasten, dass das betroffene Endsystem nur noch mit der Bearbeitung bzw. der Verwaltung dieser halboffenen Verbindungen beschäftigt ist. Sämtliche VoIP-Systeme können durch solch eine Attacke angegriffen werden; die gesamte Kommunikationsfähigkeit des betroffenen Systems wird dadurch eingeschränkt oder sogar ausgeschaltet.

LAND FLood

Bei einer LAND-Attacke ist in dem TCP-Verbindungsaufbaupaket das SYN-Flag gesetzt und wird an das Zielsystem versendet, wobei Quell-IP und Quell-Port sowie Ziel-IP und Ziel-Port identisch sind. Das Zielsystem sendet die Antwort an sich selbst, infolgedessen steigt die CPU-Last enorm es können keine weiteren Anfragen bearbeitet werden. Für die betroffenen VoIP-Systeme kommt es zu den gleichen Folgen wie bei SYN-Flood-Attacken.

Bedrohung beim Einsatz von Firewalls und Intrusion Detection Systemen

Eine Firewall ist ein zusammengesetztes System aus Einzelkomponenten (z. B. Portfilter, Proxy, IDS, IPS), die in ihrem Zusammenwirken die Umsetzung der Sicherheitsrichtlinie (Security Policy) einer Organisation (Behörde, Verwaltung, Unternehmen) ermöglicht. Das Zusammenspiel von Intrusion Detection Systemen und Paketfiltern kann Ziel von DoS-Attacken sein. Wird beispielsweise ein VoIP–Server hinter einem dynamischen Portfilter betrieben, der mit einem IDS-System gekoppelt ist, kann durch gezielte SYN-Flood-Attacken auf die VoIP-spezifischen Ports das IDS-System dazu gebracht werden, den Portfilter zu veranlassen, keine weiteren Anfragen auf den entsprechenden Ports mehr anzunehmen, wodurch die Kommunikation zum VoIP–Server verhindert wird. Die Folge hiervon wäre der Stillstand der Kommunikation einer gesamten VoIP-Domäne. Alle automatischen Gegenmaßnahmen eines Firewallsystems können für ähnliche DoS-Angriffe ausgenützt werden und auf Telefon und Gateways ausgeweitet werden. Betreibt eine Organisation Internettelefonie, so kann durch solch einen Angriff die Erreichbarkeit der gesamten Organisation verhindert werden.

Die nachfolgende Tabelle fasst die aufgeführten Angriffsmöglichkeiten zusammen und gibt an, welche Sicherheitsziele sie bedrohen.

Angriffe	Integrität		Vertraulichkeit	Verfügbarkeit
	Dateni-ntegrität	Authentizität		
MAC Spoofing		ja	ja	
MAC Flooding				ja
ARP Spoofing	ja	ja	ja	ja
STP BPDU-Attacke				ja
STP-Umleitung	ja	ja	ja	ja
VLAN rouge Trunk	ja	ja	ja	ja
VLAN Hopping		ja	ja	
IP Spoofing		ja	ja	ja
ICMP Redirect	ja	ja	ja	ja
IRDP Spoofing	ja	ja	ja	ja
Route Injection	ja	ja	ja	ja
HSRP-Angriffe	ja	ja	ja	ja
VRRP-Angriffe	ja	ja	ja	ja
DHCP Starvation				ja
DHCP rouge Server	ja	ja	ja	ja
SYN Flood				ja
Land Flood				ja
Ping Flood				ja
Fragmentierungs Attacken				ja

Tabelle 3.1: Angriffsmöglichkeiten und bedrohte Sicherheitsziele

Die folgende Übersicht verdeutlicht die Auswirkungen auf definierte Angriffspunkte für VoIP–Systeme. Die entsprechenden Angriffsmethoden wurden in den vorgehenden Abschnitten aufgezeigt.

Unterbindung der Kommunikation:

- Störung der Betriebsabläufe (Verfügbarkeit)
- Nichterreichbarkeit der Teilnehmer (Verfügbarkeit)

Umleitung von Datenströmen:

- Abhören der Sprachdaten (Integrität, Vertraulichkeit)
- Auslesen von Registrierungsvorgängen an VoIP-Servern bzw. Gateways (Integrität, Authentizität, Vertraulichkeit)
- Manipulation bzw. Modifikation der übertragenen Daten (Integrität, Authentizität, Vertraulichkeit)
- Übernahme von Verbindungen bzw. Sitzungen (Authentizität, Integrität)
- Identitätsbetrug (Authentizität, Integrität)
- Verhinderung der Kommunikation (Verfügbarkeit)
- Gebührenbetrug (Authentizität)

Beeinträchtigung der Dienstgüte:

- Verzerrung der Sprachkommunikation (schlechte Sprachverständlichkeit) (Verfügbarkeit)
- Verlangsamung von Verbindungsauf- und -abbau (Verfügbarkeit)
- Fehlerhafte Gebührenerfassung (Integrität)
- Ausfall einzelner Endgeräte oder Gruppen von Geräten (Verfügbarkeit)

Übergang zwischen dem herkömmlichen Telefonnetz und der VoIP-Umgebung

Die aktuellen VoIP-Installationen werden häufig als unternehmensweite Domänen realisiert. Dabei bildet die Installation innerhalb des Unternehmens eine logisch abgeschlossene Einheit mit einem in sich konsistenten Rufnummernplan, eigenem Telefonie-Routing und eigener Gebührenabrechnung. Außerdem findet gegenwärtig das so genannte IP Telephony Service Providing (IPTSP) eine zunehmende Verbreitung. Dabei werden die zentralen Server zu einem Service Provider ausgelagert. Die Nutzer bekommen bei dem IPTSP einen IP-Telefonie-Account - ähnlich einem E-Mail-Account - mit einer diesem Account zugeordneten Telefonnummer. In beiden Szenarien werden für eine weltweite telefonische Erreichbarkeit der Teilnehmer Gateways zu anderen VoIP-Inseln sowie zum ISDN-Netz aufgestellt (siehe Bild Übergänge zwischen VoIP-Domänen und deren Kostenmodelle). Solche Gateways bilden aus zwei Gründen sicherheitsrelevante Stellen einer VoIP-Installation.

1. VoIP-Gateways stellen einen Übergang zwischen zwei Domänen mit unterschiedlichen Protokollen und in der Regel mit unterschiedlicher administrativer Zuständigkeit dar. Gateways stehen als ein „Tor“ für unbekannte (externe) Nutzer da. Eine vollständige Abschottung der VoIP-Gateways von der Außenwelt ist somit nicht möglich. Dient ein Gateway der Zusammenschaltung mehrerer IP-Telefonie-Domänen, so müssen mindestens die Transportadressen für die Signalisierung von VoIP-Verbindungen freigegeben werden. Damit erhöht sich vor allem die Gefahr der Ausnutzung von Schwachstellen der konkreten Implementierungen von Protokollstacks auf Gateways wesentlich. Hinsichtlich der möglichen Attacken treffen auf Gateways die Betrachtungen unter 5.4.2 und 5.5.2 zu mit der Nebenbedingung, dass potentielle Attacken aus fremden Netzen kommen können.
2. Zwischen IP-Carriern werden IP-Daten üblicherweise volumenabhängig tarifiert. Da Sprachverbindungen in Relation zu anderen Anwendungen in IP-Netzen ein geringes Datenaufkommen produzieren, entstehen den Netzbetreibern durch IP-Telefonate kaum Mehrkosten. Häufig werden für die Datenübertragung Flatrates genutzt. Verbindungen in das öffentliche Telefonnetz werden hingegen zeitabhängig tarifiert. Diese zeitabhängigen Kosten entstehen in der Regel an den Punkten, wo die Gateways an das öffentliche Netz angeschlossen

sind. Durch eine unberechtigte Nutzung eines Gateways zum öffentlichen Telefonnetz kann somit Gebührenbetrug begangen werden.

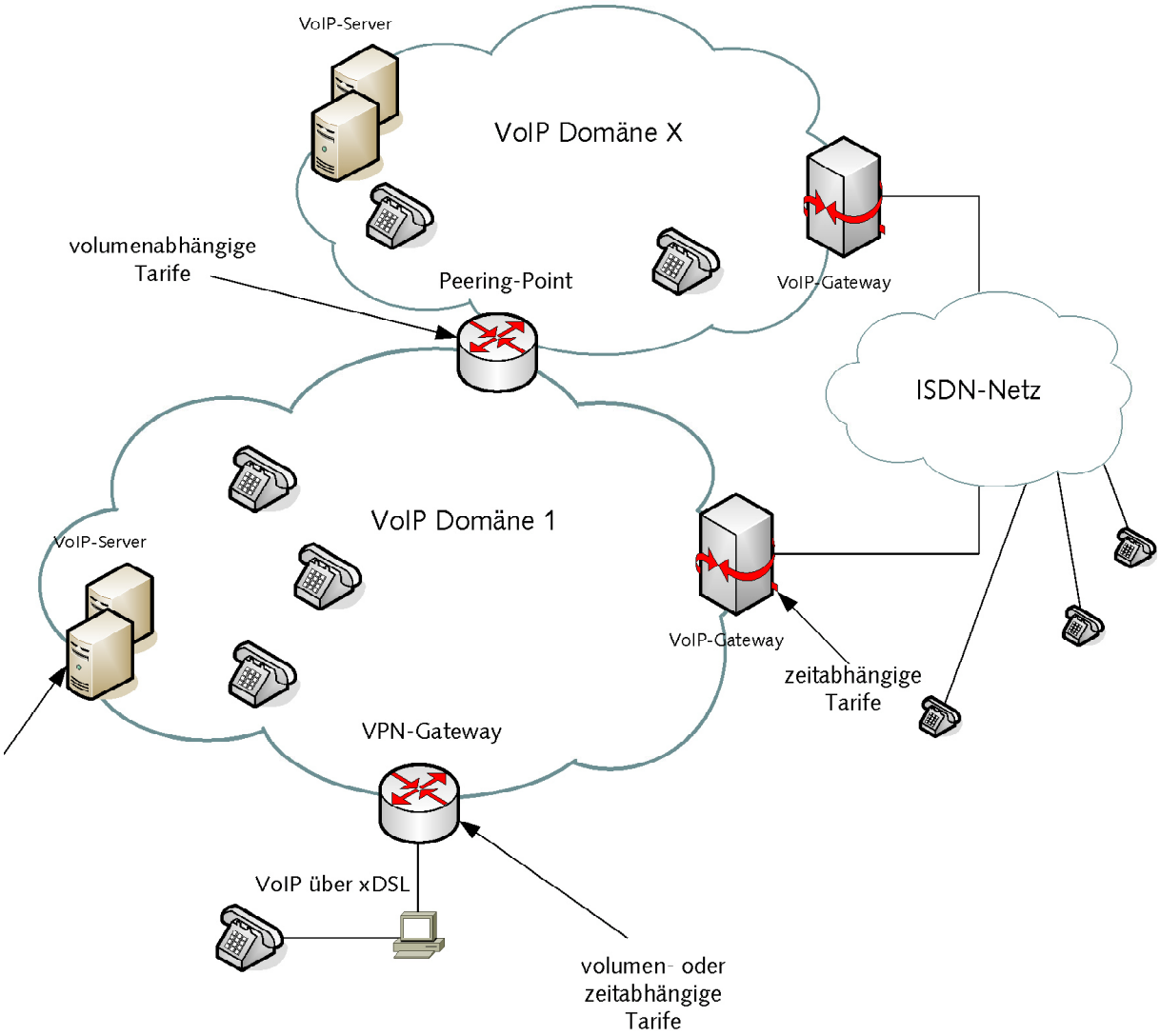

Abbildung 3.1 Übergänge zwischen VoIP-Domänen und deren Kostenmodelle

Das Ausmaß der Bedrohungen bei den Übergängen zwischen Netzen hängt von den dabei verwendeten Protokollen ab. Für die Medienströme wird fast ausschließlich RTP oder SRTP verwendet. Für die Signalisierung werden die Protokolle H.323, SIP, MGCP und MEGACO verwendet. Dazu kommen fallweise proprietäre Protokolle zum Einsatz. Nachfolgend werden die Bedrohungspotentiale bei Verwendung oben genannter Protokolle vorgestellt.

RTP

Das Real-time Transport Protocol 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 die Sequenznummer, der Zeitstempel des Datenpakets, die Art des Medienstroms (Audio/Video) und die Länge des RTP-

Headers. Mit diesen Informationen kann eine Menge von Datenpaketen einer Verbindung in einer korrekten Reihenfolge mit dem passenden Codec dekodiert und auf einem Ausgabegerät abgespielt werden, ohne auf die Signalisierung dieser Verbindung zurückgreifen zu müssen. Diese einfache Dekodierung des Medienstroms versetzt einen Angreifer in die Lage die Datenpakete eines Sprachstromes abzuh ören und zu manipulieren, sobald er auf sie zugreifen kann. Dabei ist sogar die Reihenfolge der empfangenen Datenpakete unerheblich. Beim Fehlen bestimmter Datenpakete entstehen zwar Lücken bei der Dekodierung, dies ist aber nicht mit einem Synchronisationsverlust des Kanals verbunden.

SRTP

Wegen der Verwundbarkeit des RTP wurde eine Erweiterung des Protokolls um eine symmetrische Verschlüsselung der Medienströme vorgenommen, wodurch ein Abhören des Medienstroms ohne Kenntnis des verwendeten Schlüssels nicht möglich ist. Der Schlüssel wird im Signalisierungsprotokoll ausgetauscht. Das Protokoll gilt zurzeit als sicher.

H.323

Die wesentlichen Angriffspunkte der Protokolle der H.323-Familie sind die Täuschung der Identität seitens des anrufenden Teilnehmers, sowie die 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 sonstigen kriminellen Handlungen unter falscher Identität offen.

Die Identifikation des Anrufers 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 - in Verbindung mit einem Passwort für die Authentifizierung 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 kann mit einem beliebigen ASN.1-Parser - z. B. mit dem Packetsniffer Ethereal – dekodiert und im Klartext dargestellt werden.

Des Weiteren können die Transportadressen der Sprachströme bei dem Verbindungsaufbau verändert werden, wodurch diese an eine beliebige IP-Adresse umgeleitet werden und dort abgehört, aufgezeichnet oder verändert weitergeleitet werden können. Diese Bedrohungen betreffen Endgeräte ebenso wie Gateways.

SIP

Im SIP wird eine Sicherung der Nachrichten unter Verwendung kryptographischer Hashes eingesetzt. Dadurch kann eine zuverlässige Methode zur Authentifizierung und zur Absicherung gegen Veränderungen der Signalisierungsnachrichten verwendet werden.

Es werden aber nicht alle Header durch die Hashes abgedeckt, wodurch die 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 – dafür reicht ein kurzes Script, das bestimmte Header der Nachricht umschreibt und weiterleitet. Diese Bedrohungen betreffen Endgeräte ebenso wie Gateways.

MGCP und MEGACO

Sicherheitsmechanismen sind in diesen Protokollen nicht direkt vorgesehen. Gelingt es die Datenströme abzuhören und zu manipulieren, so können die Nachrichten dekodiert und beliebig verändert werden. Die Daten können mit ASN.1 oder in ASCII kodiert sein. Somit ist ggf. für die Dekodierung und Manipulation ein ASN.1-Parser notwendig. Diese Protokolle werden nur zwischen VoIP-Servern und Gateways bzw. zwischen Gateways eingesetzt. Somit sind von den Manipulationen der Protokoll-Nachrichten nur Gateways betroffen.

Skinny Client Control Protocol (SCCP)

SCCP ist ein proprietäres Kommunikationsprotokoll, das für die Kommunikationssteuerung zwischen IP-Telefonen und dem Gatekeeper verwendet Wird. Das Protokoll ist nicht öffentlich dokumentiert und kann vom Hersteller jederzeit verändert werden. Die Protokollabläufe sind aber sehr simpel. Die ganze Verbindungssteuerung läuft in einer einzigen TCP-Verbindung ab, in der parametrisierte Befehle binär kodiert übertragen werden. In den älteren Versionen des Protokolls, das immer noch von sehr vielen Endgeräten verwendet wird, wird lediglich die MAC-Adresse zur Authentifizierung im Protokoll übertragen. Diese Kommunikation kann sehr einfach nachgebildet werden (ca. 300 Zeilen Perl-Code) und somit kann dem Gatekeeper ein fremdes IP-Telefon vorgetäuscht werden. Auf diese Weise kann auf fremde Kosten telefoniert werden, die Identität gegenüber Dritten vorgetäuscht werden, aber auch eine Denial-of-Service-Attacke auf die CallManager durchgeführt werden.

Neuere Versionen der Telefone verwenden X.509-Zertifikate für die Authentifizierung der Telefone und verschlüsseln den TCP-Signalisierungsstrom mit Hilfe von TLS. Damit ist eine Vortäuschung fremder Identität sowie das Decodieren der Kommunikation zwischen IP-Telefonen und dem Gatekeeper nicht mehr möglich.

Für die Steuerung unterschiedlicher Leistungsmerkmale der Telefone wird intensiv das HTTP-Protokoll verwendet. Diese Vorgänge laufen bislang ebenfalls ohne Verschlüsselung ab. Damit kann auch hier die Kommunikation abgehört und die Nachrichten manipuliert werden.

3.3.2 VoIP-Middleware

Der Bedrohungskatalog für VoIP-Middleware (Call-Server und Dienste-Server) reicht vom Abhören über Manipulation von Konfigurationsdateien (z. B. Rufumleitungen, Gebührenbetrug) bis hin zum Ausfall des gesamten VoIP-Systems. Eine Bedrohung verfolgt unterschiedliche Ziele. Zum einen will man die Systeme stören, oder gar zerstören, zum anderen die Administrationsrechte über die Systeme erlangen, um diese für eigene Zwecke zu missbrauchen. Der Anwender registriert einen erfolgreichen Angriff auf die VoIP-Infrastruktur oder die IT-Struktur als Ausfall des VoIP-Dienstes.

Call-Server werden meist auf „gängigen“ Betriebssystemen – speziell Windows und Unix-Betriebssysteme - installiert. Diese Betriebssysteme sind nicht speziell für VoIP entworfen worden und dadurch für viele Angriffe anfällig. Nur wenige VoIP-Systemanbieter „härten“ ihr Betriebssystem und unterbinden dadurch eine große Zahl von Angriffsmöglichkeiten. Oftmals fehlen aktuelle Virenwächterprogramme oder HIDS (Host-Based Intrusion Detection System) auf den Call-Servern und deren angeschlossenen Dienste-Servern (UMS-, FAX-, Mail-Server, usw.) um Angriffe zu erkennen. Fehlendes Softwareupdate-Management für die einzelnen Komponenten ist eine weitere Gefahrenquelle.

Dieser Abschnitt beschäftigt sich unter anderem mit den Fragen verschiedener Netzbedrohungen bzw. systemspezifischen Sicherheitslücken, denen VoIP-Middleware-Komponenten wie Call-Server, Proxy-Server, Gatekeeper, Gateways und deren Basisdienste wie DNS-Server, TFTP-Server, Datenbank-Server (LDAP) ausgesetzt sind. Die Server laufen in der Regel unter Unix- oder Windows-Betriebssystemen, wie z. B. Linux oder Windows 2000 Server. So können, beispielsweise durch Ausnutzung von Sicherheitslücken in den Betriebssystemen der Maschinen, auf diesen Software für Netzattacken installiert und ausgeführt werden. In Netzwerksystemen (Gatekeeper, Gateways, Router) hingegen findet man häufig auch proprietäre Betriebsysteme. Proprietäre Systeme benutzen eigene Protokoll-Stack-Implementierungen und sind damit nicht sicherer; im Gegenteil, durch die geringere Verbreitung sind diese Systeme häufig weniger getestet, und die Sicherheitslücken werden nur verzögert aufgedeckt. VoIP-Systeme sind für die Entwickler von Malware oder Angreifer aus dem Netzwerk nur weitere, wenn auch lohnende Objekte um z. B. Gebührenbetrug (Fraud) zu begehen. Ein Angreifer versucht zunächst über passives Monitoring (Ethernet Sniffing, Eavesdropping) Informationen über das Netzwerk zu bekommen, um diese dann gezielt gegen die Middleware-Systeme einzusetzen. Kapitel 3.4.1 beschreibt allgemein die Angriffsarten, wobei in diesem Kapitel die Frage nach den Auswirkungen auf die Vertraulichkeit, Integrität und Verfügbarkeit der VoIP-Middleware gestellt wird.

Physikalische Angriffe

Durch einen physikalischen Zugriff auf IP-Telefonsysteme besteht das Potential einer totalen Kompromittierung des Systems. In Kapitel 4.4.1wird eingehend auf physikalische Angriffe eingegangen.

Malware Angriffe (*malicious* = boshaft und *Software),* die durch Viren, Spyware, Adware oder Key Logger-Programme ausgelöst werden, werden in Kapitel 4.4.2 beschrieben.

Password Sniffing

Beim Password Sniffing-Angriff leitet der Angreifer über ARP-Spoofing oder DNS-Spoofing (siehe Kapitel 4.4.1) den kompletten Datenstrom über seinen Rechner zum Default Gateway. Der Angreifer ist in der Lage, Benutzername und Passwort aus dem Datenstrom herauszufiltern und kann somit den VoIP-Middleware-Server bei unverschlüsseltem Passwort übernehmen. Besitzt der Angreifer das Root-Passwort, so kann er die Integrität des Systems angreifen und Daten verändern. Die Vertraulichkeit des Systems wird verletzt, indem er Passwörter mitliest und in Protokolldateien einsieht, und schließlich kann er die Verfügbarkeit des Systems empfindlich stören oder gar das System selbst zerstören durch Veränderungen von Systemdateien.

DNS-Spoofing, Rouge DHCP

Vorausgesetzt der Angreifer sieht die DNS-Anfragen des Zielsystems, so kann er mit ARP-Spoofing die Gateway-Adresse des Zielsystems verändern (siehe Kapitel 4.4.1). Dieser Angriff ermöglicht dem Angreifer, ausgewählte VoIP-Middleware-Systeme vom Netzwerk abzuhängen und die Verfügbarkeit der VoIP-Middleware-Systeme partiell oder vollkommen zu stören. Diese Angriffsarten sind auch auf VoIP-Endgeräte übertragbar.

DHCP Starvation

Ein DHCP Starvation-Angriff (starvation = verhungern) erschöpft den IP-Adressbereich des DHCP-Servers (siehe Kapitel 3.5.1). VoIP-Endgeräte werden in der Regel von einem DHCP-Server mit einer IP-Adresse, Gateway-Adresse, DNS-Server-Adresse und TFTP-Adresse (um Profileinstellungen anzufordern) versorgt. Ein wiederholtes Nachfordern von Netzwerkadressen führt zur Ausschöpfung der vom DHCP-Server zu vergebenden Adressen, und der Server kann keine neuen Adressen mehr zuweisen. Das führt dazu, dass sich keine neuen VoIP-Endgeräte anmelden können. Da bereits konfigurierte Endgeräte ihre Konfiguration in regelmäßigen Abständen erneuern, verlieren sie nach einer gewissen Zeit ihre Konfiguration und gehen nacheinander außer Betrieb.

ICMP Redirect

Der Router informiert mit ICMP Redirect das Endsystem über eine „bessere“ Route zum Zielsystem. Mit gefälschten ICMP Redirects ist ein Angreifer in der Lage, den Datenverkehr eines Middleware-Servers über seinen Rechner zum Zielsystem zu leiten und ihn zu manipulieren. Der Angreifer kann den Datenverkehr mitlesen, somit die Vertraulichkeit des Datenverkehrs verletzen oder die Integrität der Datenverbindung durch Einspeisung zusätzlicher Pakete oder durch gezieltes Entfernen beeinträchtigen. Die Angriffe können sich sowohl auf die Steuerinformationen als auch auf den Nutzdatentransport beziehen. Der Angreifer kann durch Manipulation der Steuerinformation ein eigenes VoIP-Endgerät einbinden und Toll Fraud (Gebührenbetrug) begehen oder einzelne Funktionen wie einen http-Service vorspiegeln. Beim Abhöhren der Datenströme können Telefonate abgehört und ggf. verfälscht oder gestört werden.

SYN Flood, LAND Flood, PING Flood

Ein Angreifer versendet ausschließlich TCP-Verbindungspakete (SYN-Pakete) und erreicht damit, dass das Zielsystem in Pufferengpässe kommt (siehe Kapitel 4.4.1). Die drei Netzwerk-Angriffsarten führen bei den Zielsystemen (VoIP-Middleware, VoIP-Endsysteme) dazu, dass die Verfügbarkeit gemindert oder gänzlich beeinträchtigt wird. Durch gezielte Manipulation (ID des Netzes, Quelladresse) des PING-Pakets kann eine komplette Broadcast-Domäne – in der Regel das gesamte LAN - auf einmal geflutet werden. Dies führt zur Beeinträchtigung oder vollkommenen Störung der Verfügbarkeit (z. B. Störung der Betriebsabläufe, Nichterreichbarkeit des Gateways und des Authentifizierungsservers, Nichterreichbarkeit der Teilnehmer, Verzerrung der Sprachkommunikation, Verhinderung eines Verbindungsaufbaus, verzögerter Verbindungsauf- und -abbau, Ausfall einzelner

Geräte oder Gruppen) und der Integrität (z. B. fehlerhafte Gebührenabrechnung) von VoIP-Middleware und VoIP-Endgeräten.

ARP Spoofing, MAC Spoofing

Mit ARP Spoofing und MAC Spoofing leitet der Angreifer alle Pakete zu seinem Rechner um (siehe Kapitel 4.4.1). Diese Angriffe werden genutzt, um weitere Manipulationen einzuleiten, beispielsweise um die Vertraulichkeit (z. B. Password sniffing, Abhören von Verbindungen) zu verletzten, oder um die Integrität der Verbindungen durch Einspeisen zusätzlicher oder Entfernen bestehender Pakete (Signalisierungsdaten, Gebührenbetrug, RTP-Medienstöme) und die Verfügbarkeit selektiv zu beinträchtigen. Die Angriffe betreffen sowohl die VoIP-Middleware als auch die VoIP-Endgeräte.

3.3.3 VoIP-Endgeräte

VoIP-Endgeräte kommunizieren mit den VoIP- oder anderen Servern über das IP-Protokoll. Die VoIP-spezifischen Protokolle setzen ausschließlich oberhalb von IP auf. Aus diesem Grunde kann ein VoIP-Endgerät auch auf jedem IP-Stack abgesetzt werden. Reine Softwareimplementierungen nennt man Softphones.

Die VoIP-Endgeräte –außer Softphones- verfügen über einen eigenen IP-Stack, auf dem die Anwendungssoftware aufsetzt, die ihrerseits unterschiedliche Signalisierungs- und Medienübertragungsprotokolle unterstützen kann. Für die VoIP-Endgeräte (Hardphone, Softphone, Konferenzsystem, PDA) gelten im Prinzip die gleichen Aussagen wie für die Middelware [Kapitel 4.4.2]. VoIP-Endgeräte laufen größtenteils mit gängigen Betriebssystemen (Linux, Microsoft Windows) oder mit einer eigener Firmware. Die Angriffe lassen sich fast 1:1 auf die Endgeräte übertragen. In der oben stehenden Auflistung wird bei den einzelnen Protokollen auf die Bedrohung für die VoIP-Endgeräte hingewiesen.

3.3.4 Qualitiy of Service und Class of Service

Damit die VoIP-Anwendung mit einer akzeptablen Qualität angeboten werden kann, muss ein Mindestmaß an Dienstgüte in den betroffenen Netzen bereitgestellt werden. Die Dienstgüte kann durch andere über die Netze übertragene Datenströme beeinflusst werden. Quality of Service (QoS) bezeichnet dabei Maßnahmen mit denen eine bestimmte Dienstgüte garantiert werden kann, während Maßnahmen zur Zuordnung einer bestimmten Dienstgütenkategorie (ohne individuelle Garantie) als Class of Service (CoS) bezeichnet wird.

Die Verringerung der Dienstgüte im Netz stellt ebenfalls eine Bedrohung der Anwendung VoIP dar, weil damit der Dienst gezielt oder nicht gezielt beeinträchtigt wird und im Extremfall gänzlich zum Erliegen gebracht werden kann.

Folgende Dienstgüteparameter beeinflussen im Wesentlichen die Qualität von VoIP-Anwendungen:

- Einweg-Paketverlust (Packet Loss). Paketverluste sind besonders in Signalisierungsströmen kritisch, da sie den Verbindungsauf- oder -abbau stark beeinträchtigen. Die Datenströme der Sprachübertragung sind deutlich robuster hinsichtlich Paketverlusten. Je nach verwendeter Kodierung der Sprache kann trotz Paketverlustraten von 2-10 % eine Sprachverbindung in akzeptabler Qualität zustande kommen [TUT96a, Goeh01].
- Einweg-Verzögerung (Delay). Eine zu starke Verzögerung der Laufzeit der Datenpakete führt zur Reduktion der Wahrnehmung der Sprachqualität. Der ITU-T Standard G.114 [ITUT96b] nennt eine Grenze für Einwegverzögerungen der Sprachdaten vom Mikrofon zum Hörer von 150 ms als akzeptabel. Hierbei ist zu berücksichtigen, dass die Sprachdaten in den Endgeräten durch die Verwendung von Jitter-Buffern bereits eine Verzögerung von 30-50 ms bekommen. Somit kann die Qualität der Sprache beeinflusst werden, wenn zwischen Endsystemen Einweg-Verzögerungen der Datenpakete von mehr als 100 ms auftreten.
- Schwankung der Einwegverzögerungen (Jitter). Geringfügige Schwankungen der Paketlaufzeiten werden durch Jitter-Buffer aufgefangen. Überschreiten Jitter die zeitliche Kapazität der

verwendeten Jitter-Buffer (10-30 ms), so kommt es zur deutlichen Störung der wahrgenommenen Sprachqualität.

Paketverluste, Delay und Jitter können beispielsweise in Überlastsituationen entstehen, in fehlerhaft Konfigurierten Netzen oder durch gezielte Eingriffe in das Netz gezielt verursacht werden. So können in Netzen mit einer geringen Datenrate (<100 Mbit/s) starke Jitter mit sehr geringem Aufwand erzeugt werden. Um die Sprachqualität deutlich zu beeinträchtigen genügt es beispielsweise, einen oder einige wenige wiederkehrende UDP-Datenströme mit einer möglichst hohen Datenrate im Netz zu erzeugen, die zu einer kurzzeitigen Überlastsituationen in den Warteschlangen der Router und Switches führen.

Zur Gewährleistung bestimmter Dienstgüten können verschiedene QoS und CoS-Maßnahmen eingestetzt, die im Kapitel 4.2.1 näher erläutert werden. Allerdings können QoS-Maßnahmen ihrerseits Ziele von böswilligen Angriffen werden.

3.3.5 Energieversorgung

Der Ausfall der Energieversorgung stellt eine zentrale Bedrohung bezüglich der Verfügbarkeit dar, da dadurch der gesamte Telefoniedienst zum Erliegen gebracht werden kann. In diesem Zusammenhang kann ein möglicher Ausfall in drei Kategorien betrachtet werden:

Ausfall der Energieversorgung der Endgeräte. Während bisherige analoge und ISDN-Endgeräte über die Kommunikationsleitung mit Energie versorgt werden und nur selten eine eigene Stromversorgung benötigen, werden heutige IP-Endgeräte üblicherweise externe mit Strom versorgt. Ein wesentliches Problem stellt dabei der hohe Stromverbrauch von IP-Telefonen dar, während herkömmliche Telefone aufgrund der meist einfachen Systemarchitektur mit wenigen Watt auskommen (der ISDN Standard sieht max. 1 bis 4 W zur Speisung vor [ETSI EN 300 012-1]). Bei VoIP-Systemen wird im Standard IEEE 802.3af, „Power over Ethernet, PoE“ eine ähnliche Funktionalität angeboten, auf die in Kapitel 4.2 näher eingegangen wird. Eine in diesem Zusammenhang stehende Frage ist die Notstromfähigkeit von IP-Telefonen: Kein ein (jedes) Telefon, das im Normalbetrieb über eine externe Stromversorgung betrieben wird im Notfall und mit Grundfunktionen mittels PoE betrieben werden?

Ausfall der Energieversorgung der Middleware. Vergleichbar mit dem Ausfall der zentralen Telekommunikationsanlage ist der Ausfall der Middleware-Komponenten in VoIP-Systemen. Ist nur die Middleware von einem Ausfall betroffen, so kann allerdings im Gegensatz zur traditonellen Telekommunikationtechnik, durch Wahl alternativer Middleware der Telefoniedienst aufrecht erhalten werden. Bei nicht vorhandener USV ist bei VoIP-Middleware die ungeordnete Abschaltung der Systeme durch Energieausfall ebenfalls problematisch. Weiterhin ist meist das automatische Hochfahren der Systeme nach einem Energieausfall und Wechsel in einen gesicherten Grundmodus wenn nicht die Übernahme des letzten Betriebsmodus nicht gegeben.

Ausfall der Energieversorgung des Übertragungsnetzes. Die unterbrechungsfreie Energieversorgung aller Komponenten (Router, Switche, Filter) des Übertragungsnetzwerkes ist besonders kritisch einzustufen. Der Ausfall führt zwangsläufig zu einer völligen Unterbrechung der gesamten Sprachkommunikation. Die Bedrohungslage ist dabei größer als bei der traditionellen Telekommunikationstechnik, da dort üblicherweise passive Komponenten auf dem Übertragungswege liegen (Kupferleitungen etc.) und nur wenige aktive (Splitter, NTBA, Repeater etc.).

3.3.6 Diskussion der Sicherheit auf Netzebene

Die Darstellungen in den vorangehenden Abschnitten zeigen, dass die Gefahren, denen eine VoIP-Installation ausgesetzt wird, vom verwendeten Betriebssystem der Endgeräte und der zentralen Server und deren Schwachstellen abhängen. Es ist beim Betrieb von VoIP-Systemen darauf zu achten, dass der Anbieter oder Betreiber der Systeme mit dem Bekanntwerden von Sicherheitslücken im zugrunde liegenden Betriebssystem rechtzeitig Updates und Patches zur Verfügung stellt. Hier spielt auch die Wartbarkeit des Systems eine wesentliche Rolle. Ist das Aufspielen sicherheitsrelevante Updates mit einem hohen Arbeitsaufwand verbunden, so steigt die Wahrscheinlichkeit dafür, dass solche

Maßnahmen vom Betreiber nicht rechtzeitig getroffen werden. Zu beachten ist ebenfalls, dass die in der VoIP-Umgebung verwendete Hard- und Software in der Regel sehr leistungsfähig ist. Gelingt es Angreifern die Kontrolle über ein derartiges System zu erlangen, kann es für weitere Attacken oder für illegale Aktivitäten missbraucht werden (z. B. durch Installation von Peer-o-Peer- oder Trojaner-Software auf dem System).

Ein wesentlicher Punkt sind die Sicherheitsregeln in Firewalls. Die Administratoren sind angehalten, sie ständig zu verifizieren, um Einbrüche auszuschließen.

Einen weiteren sicherheitskritischen Aspekt des Betriebs von Voice over IP-Umgebungen stellen Maßnahmen zum Schutz der Serverräume, der zentralen Komponenten der VoIP-Umgebung sowie der Netzkomponenten (Router und Switches) gegen den Zutritt Unbefugter dar.

Ein sicherer Betrieb von VoIP-Umgebungen bedarf einer ganzheitlichen und lückenlosen Planung und Umsetzung von Security- Verfügbarkeits- und QoS-Konzepten.

3.4 Bedrohungen auf Anwendungsebene

3.4.1 Programme mit Schadensfunktionen

Unterschiedliche Programme mit Schadensfunktionen (Malware), wie Viren, Würmer und Trojanische Pferde, sowie Fehler in der Implementierung (Bugs) stellen ein Risiko für die Funktionalität und Sicherheit von Anwendungen der IP-Telefonie dar.

Viren

Computer-Viren sind *nichtselbstständige* Programme, die sich selbst reproduzieren, indem sie sich an andere Programme oder Bereiche des Betriebssystems anhängen und, einmal aktiviert, vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornehmen. Als nicht selbstständiges Programm benötigt ein Virus zur Aktivierung das so genannte Wirtsprogramm.

Würmer

Computer-Würmer sind *selbstständige* Programme, die sich selbst reproduzieren, indem sie über ein Netzwerk an Programmen oder Betriebssystemen anderer Computer Manipulationen vornehmen. Die Abgrenzung zu Viren besteht darin, dass ein Wurm versucht eine Zahl von Computern in einem Netzwerk zu infizieren, während ein Virus versucht, Dateien auf einem Computersystem zu infizieren. Würmer beanspruchen Systemressourcen und können die Leistung des infizierten Systems beeinträchtigen und somit DoS-Angriffe verursachen. Zudem können Würmer genauso wie Viren spezielle Schadensroutine enthalten.

Trojanische Pferde

Trojanische Pferde sind Programme, die neben scheinbar nützlichen auch verborgene, schädliche Funktionen enthalten und diese unabhängig vom Benutzer und ohne dessen Wissen ausführen. Im Gegensatz zu Würmern können Trojanische Pferde sich jedoch nicht selbständig verbreiten. Trojanische Pferde werden zur Manipulation, oder Ausspähung und Weiterleitung von vertraulichen Daten, sowie zwecks eines vom Benutzer unkontrollierten Fernzugriffs auf das System eingesetzt.

Implementierungsfehler

Entwicklung von sicherheitskritischen Anwendungen erfordert einen hohen Qualitätsstandard in der Softwareentwicklung (z. B. Verwendung von Vorgehensmodellen wie dem V-Modell). Durch Fehler in der Implementierung können unbeabsichtigt Sicherheitslücken geöffnet und das Schadensrisiko unnötig gesteigert werden.

Die am häufigsten ausgenutzten Implementierungsfehler führen zu so genannten Pufferüberlauf-Angriffen (Buffer-Overflow). Durch Fehler im Programm werden dabei zu große Datenmengen in einen unterdimensionierten Speicherbereich geschrieben, wodurch es zur Überschreibung nachfolgender Informationen im Speicher kommen kann. Mit Pufferüberlauf-Angriffen kann der Angreifer Zugangspasswörter, verdeckte IP-Adressen von sicherheitskritischen Netzkomponenten und weitere geheime Informationen herausfinden, sowie unter Umständen einen eigenen schädlichen Programmcode in das System hineinschleusen, der auch zur Übernahme der Kontrolle über das System führen kann.

Bei Implementierung von Netzwerkprotokollen können kritische Fehler aufgrund von inkorrekter Verarbeitung von Daten aus den Paket-Headern entstehen. Wird z. B. keine Überprüfung des Wertebereichs und -typs durchgeführt, so kann der Angreifer mit speziell präparierten Paket-Headern im Rahmen einer DoS-Attacke einen Systemabsturz herbeiführen.

3.4.2 VoIP – Endgeräte

Gerätearten

Bei VoIP-Endgeräten unterscheidet man zwischen zwei Arten: IP-Telefone und Softphones.

IP-Telefone sind eigenständige Geräte mit eigenen Hardwarekomponenten und meistens proprietären Betriebssystemen, die direkt an das IP-Netzwerk angeschlossen werden. IP-Telefone laden meistens Ihre aktuelle Konfiguration von dem Call-Control-Center (siehe Kapitel 4.5.3) über das TFTP-Protokoll.

Softphones sind auf dem Computer installierte Anwendungsprogramme, deren Funktionalität der eines IP-Telefons entspricht. Für den Zugang zum IP-Netz benutzen Softphones die Schnittstelle des Computers, die sie mit anderen installierten Anwendungen teilen.

Funktionen und Risiken

Alle VoIP-Endgeräte bieten im Wesentlichen ähnliche Funktionen an, die von Programmen mit Schadensfunktionen beeinträchtigt werden können. Das Bedrohungsspektrum erstreckt sich dabei von partieller Beeinträchtigung des Normalbetriebs bis zu einer vollständigen Übernahme der Kontrolle über das Gerät durch den Angreifer.

Im Bereitschaftsmodus warten Geräte auf Benutzereingaben oder auf die ankommenden Anrufe. Dabei kann Malware versuchen verdeckte Anrufe ohne Wissen des Anwenders zu initiieren, oder Informationen über die geführten Telefonate, sowie privaten Telefonnummern aus dem Adressbuch zu ermitteln und weiterzuleiten.

Wird ein Anruf vom Anwender initiiert, so bauen Geräte die Verbindung gemäß eingestellter Konfiguration und gewählter Telefonnummer auf. Manipulationen an der Konfiguration oder Firmware des Geräts können zur Störung des Anwahlprozesses oder sogar zur Umleitung des Gesprächs über die Angreiferinfrastruktur führen. Damit kann der Angreifer das darauf folgende Gespräch abhören.

Selbst wenn der Anruf korrekt durchgestellt wird, kann es im Laufe eines Gesprächs zur Ausbreitung von Würmern, sowie Aktivierung und Steuerung von Trojanischen Pferden kommen. Trojanische Pferde können benutzt werden, um private Informationen eines Teilnehmers oder Gesprächsinhalt während des Gesprächs an einen Angreifer zu übermitteln. Ausserdem können Sprachdaten aus dem Gespräch gespeichert und weitergeleitet werden.

Beendet der Anrufer das Gespräch, so kann das infizierte Gerät die Signalisierung des Gesprächsendes vortäuschen, während die Verbindung im Hintergrund aufrecht erhalten wird, und dem Anrufer zusätzliche Kosten verursacht werden. Ist ein Gerät von einem Virus befallen, so kann dieses die Signalisierung von ankommenden Anrufen unterdrücken, ohne dass der Angerufene es merkt, und damit eine DoS-Attacke verursachen.

Viele VoIP-Endgeräte bieten die Möglichkeit an, ankommende Anrufe weiterzuleiten. Infizierte Geräte können diese Weiterleitung stören oder manipulieren, und einem Angreifer unter gewissen Umständen das Abhören ermöglichen.

Eine weitere potentielle Angriffsvariante durch Malware besteht darin, das Mikrofon eines VoIP-Endgerätes unbemerkt zu aktivieren, um es zu einer Wanze zu machen, die Gespräche im Raum aufzeichnet und per VoIP an den Angreifer übermittelt. Der Aufwand zur Programmierung einer entsprechenden Malware mit Wanzenfunktionalität ist dabei relativ gering, weil die benötigte VoIP-Funktionalität (Codec, VoIP-Protokolle) bereits auf den Endgeräte implementiert ist und von der Malware genutzt werden kann.

Diskussion

In welchem Maße die beschriebenen Risiken tatsächlich bei einem Gerät auftreten, hängt von mehreren Faktoren ab, wie z. B., Art und Einstellungen des Betriebssystems, Verwendung von gemeinsamen Ressourcen mit anderen Anwendungen (z. B., bei Softphones), und implementierten Schutzmechanismen.

Generell lässt sich sagen, dass Softphones besonders stark für die Angriffe von Programmen mit Schadensfunktionen (z. B., Code-Red und Nimda) anfällig sind, weil sie meistens auf den weit verbreiteten Betriebssystemen, wie Windows, Unix, oder Linux basieren und Ressourcen mit anderen installierten Anwendungen teilen, die eigene Sicherheitslücken haben können. Dagegen haben IP-Telefone eine eigene Netzschnittstelle und basieren meistens auf proprietären Betriebssystemen, deren Einstellungen auf die geforderte Funktionalität zugeschnitten sind. Somit können sie nur den Angriffen von schädlichen Programmen ausgesetzt werden, die speziell für solche Betriebssysteme entwickelt worden sind. Der Anteil solcher speziell entwickelten Programme mit Schadensfunktionen ist aber deutlich geringer.

3.4.3 VoIP-Middleware

Gatekeeper

Gatekeeper, auch Callmanager oder Call-Server genannt, sind server-basierte Softwarelösungen zur Kontrolle von IP-Telefonie, die auf einer zum IP-Netz angeschlossenen Hardwareplattform (IP-PBX) installiert werden. Gatekeeper sind zuständig für Signalisierung und Durchführung von ankommenden und abgehenden Anrufen, dienen zur Konfiguration von abhängigen VoIP-Endgeräten, ermöglichen Pflege von angeschlossenen Benutzerdatenbanken, überwachen die Zugriffskontrolle auf die IP-Telefonieund können zur Protokollierung von Anrufen, sowie zur Verwaltung von Sprachnachrichten (Voice-Mails) benutzt werden. Einige Gatekeeper erlauben eine Fernsteuerung über eine Webschnittstelle. Es existieren Gatekeeper, die zudem eine Verschlüsselung von Anrufsignalen und übertragenen Mediendaten unterstützen.

Einige Gatekeeper basieren auf weit verbreiteten Betriebssystemen und sind demnach auch den systemspezifischen Angriffen durch Malware und Implementierungsfehler ausgesetzt. Da Gatekeeper auf einer Hardwarekomponente des IP-Netzwerks installiert werden, können Viren und Würmer von anderen infizierten Netzwerkkomponenten (wie VoIP-Endgeräte oder Komponenten, die nicht für IP-Telefonie benutzt werden) auf das System gelangen. Auch ist es umgekehrt möglich, dass schädliche Programme sich von einem infizierten Gatekeeper auf andere Teile des IP-Netzwerks ausbreiten und ihre Funktionalität beeinträchtigen. Wird die Konfiguration des Gatekeepers über die Webschnittstelle vorgenommen, so kann der Angreifer versuchen die Authentifizierungsdaten auszuspähen, wenn diese im Klartext mit HTTP-Protokoll übertragen werden.

Enthält der Angreifer Zugriff auf Gatekeeper, so kann er unter Umständen weitere VoIP-Endgeräte an das System anschließen oder Konfigurationen von angeschlossenen IP-Telefonen mittels manipulierten TFTP-Antworten verändern (mit allen daraus resultierenden Risiken aus dem Kapitel 4.5.2), Benutzerdaten ausspähen und Benutzerrechte verändern, vertrauliche Voice-Mails abhören und manipulieren, sowie Anrufe in Echtzeit abhören und umleiten. Auch zahlreiche DoS-Angriffe sind

denkbar. Die Funktionen von Gatekeeper können zudem durch Angriffe auf seine Untersysteme, wie Benutzerdatenbanken (z. B., mit SQL Slammer Wurm oder Voice-Mail Spam) beeinträchtigt werden.

VoIP-Router

Die Funktionalität von VoIP-Routern ist ähnlich der von Routern in übrigen IP-Netzwerken. Neben einer Weiterleitung von IP-Paketen in verschiedene IP-Subnetze, erlauben VoIP-Router IP-Telefonie für Geräte mit analogen Telefonanschlüssen. Die meisten VoIP-Router können über eine Webschnittstelle konfiguriert werden.

Infizierte VoIP-Router können demnach DoS-Angriffe verursachen. Auch Manipulationen an weitergeleiteten VoIP-Paketen sind denkbar. Mit Hilfe von installierten Trojanischen Pferden können die über das HTTP-Protokoll während einer Fernsteuerung übertragenen Authentifizierungsdaten ausgespäht werden. Die Webschnittstelle stellt auch ein Risiko zur Ausbreitung von Würmern dar.

VoIP-Gateways

VoIP-Gateways bestehen aus zwei Komponenten: Media-Gateways und Media-Gateway-Controllern.

Media-Gateways (MGs) sind Netzwerkkomponenten der VoIP-Infrastruktur, die eine Konvertierung von zeitmultiplexen Sprachsignalen in die IP-basierte RTP-Pakete ermöglichen, und als Schnittstelle zwischen den VoIP- und PSTN-Netzwerken eingesetzt werden. MGs können lokal über mitgelieferte Software oder ferngesteuert von Media-Gateway-Controllern (MGC) über Megaco/H.248 Protokoll konfiguriert und verwaltet werden. Dabei kann ein MGC gleichzeitig mehrere MGs verwalten, die auch miteinander über IP-Netz verbunden sind. Ein MGC kann sowohl einzelne Anrufe als auch Konferenzanrufe kontrollieren. Einige MGs können selbst keine Anrufe initiieren, sondern befolgen Anweisungen des MGC.

Die Übernahme eines MGCs ermöglicht dem Angreifer nicht nur eigene Anrufe in das PSTN-Netzwerk zu initiieren und geführte Telefonate zu stören, abzuhören, zu manipulieren oder umzuleiten (z. B. über teuere 0190-Nummern), sondern öffnet auch Türen zur Verwaltung und Konfiguration aller davon abhängigen MGs, und schafft somit ein größeres Risiko als das der Übernahme eines einzelnen MGs.

Folgende Sicherheitsrisiken sind denkbar, wenn ein Angreifer die Kontrolle über einen MG übernimmt. Neben verschiedenen DoS-Attacken auf der Seite des IP-Netzwerks, können Anrufe in und aus PSTN-Netzwerk abgehört werden. Obwohl es keine Gefahr zur Ausbreitung von Viren und Würmern bei Telefonaten in oder aus einem PSTN-Netzwerk besteht, können diese auf andere, damit über ein IP-Netz verbundene, MGs übertragen werden.

VoIP-Firewalls

Firewalls werden in IP-Netzwerken eingesetzt, um diese vor Angriffen und unerlaubtem Zugriff zu schützen. Pakete werden von Firewalls zwischen externen und internen IP-Netzen gemäß implementierten Filterregeln weitergeleitet, die verschiedene Netzwerkprotokolle und zugehörige Ports umfassen. Eine Übertragung der zu einer Verbindung gehörenden Pakete kann blockiert werden, wenn diese nicht den implementierten Regeln entsprechen. Somit können Sicherheitsrichtlinien zentral mit einer Firewall durchgesetzt werden, statt an Endpunkten von Verbindungen. Zudem können Firewalls Protokollierung von eingehenden und ausgehenden Paketen vornehmen. Firewalls können sowohl auf proprietären als auch auf weit verbreiteten Betriebssystemen basieren und eine Webschnittstelle zur Fernsteuerung enthalten.

In VoIP-Netzwerken werden Firewalls zur Filterung von IP-Telefonie benutzt. Anhand der Überprüfung von Paketheadern können Firewalls zwischen verschiedenen Gesprächsverbindungen, sowie ihren Zuständen (z. B. zwischen Einwahl- und Gesprächsphasen) unterscheiden. Erlangt ein Angreifer Kontrollrechte über eine VoIP-Firewall, so kann er nicht nur eigene Filterregeln implementieren und damit vorgeschriebene Sicherheitsrichtlinien verändern, sondern auch die Durchstellung von Anrufen oder selbst Gesprächsvorgänge beeinflussen (z. B. stören, umleiten, abhören).

Einige VoIP-Firewalls realisieren zusätzlich die Schnittstelle zwischen den Sprach- und Datensegmenten eines VoIP-Netzwerks, um bestimmte Funktionalität zu erfüllen, wie z. B. Übertragung von gespeicherten Voice-Mails aus dem Datensegment zu dem sich in einem Sprachsegment befindlichen Gatekeeper oder Zugriff von Softphones (Datensegment) auf den Gatekeeper zwecks Konfigurationseinstellungen. In diesem Kontext ist das Risiko denkbar, dass ein Virus als Anhang einer Voice-Mail in das Sprachsegment übertragen wird, oder eine DoS-Attacke sich aus dem Datensegment in das Sprachsegment ausbreitet.

Diskussion

Bei Angriffen auf VoIP-Middleware können alle dadurch geleiteten IP-Telefonate gestört, abgehört, umgeleitet und manipuliert werden, wenn keine Sicherheitsmechanismen vorhanden sind. Einige Komponenten sind zudem Schnittstellen zu anderen Netzen (z. B. PSTN), und öffnen somit zusätzliche Risiken für die IP-Telefonie. Demnach haben Angriffe auf VoIP-Middleware-Komponenten ein weitaus größeres Risiko verglichen mit den Angriffen auf einzelne VoIP-Endgeräte, die in erster Linie IP-Telefonate des Geräts beeinflussen. Demnach ist die Absicherung von VoIP-Middleware-Komponenten ein wichtiger Aspekt für die Sicherheit des VoIP-Netzwerks.

Die auf proprietären, gehärteten Betriebssystemen basierten VoIP-Middleware-Anwendungen haben statistisch gesehen, eine bessere Resistenz gegen Malware. Durch eine logische Trennung des IP-Netzwerks in ein Sprach- und ein Datensegment kann für IP-Telefonie eine bessere Sicherheit erreicht werden, wenn proprietäre Betriebssysteme im Sprachsegment eingesetzt werden. Dennoch ist diese Sicherheit nur so groß wie das schwächste Glied der Kette. Im Falle einer Segmentierung ergeben sich die größten Risiken an VoIP-Firewalls, die als Schnittstelle zwischen den Sprach- und Datensegmenten dienen.

Fernsteuerung von VoIP-Middleware-Komponenten über implementierte Webschnittstellen ist ein potentielles Risiko für die Ausspähung von Authentifizierungsdaten mit Hilfe von installierten Trojanischen Pferden, und für die Ausbreitung von Würmern. Demnach sollte überlegt werden, ob eine Fernsteuerung unbedingt notwendig sei, und ob man dafür eine verschlüsselte Verbindung (z. B., HTTPS) einsetzt.

3.5 Spezielle Aspekte: VoIP im WLAN

3.5.1 Einführung WLAN

WLANs (engl. wireless local area networks) basieren heute meist auf den IEEE 802.11 Standards. Der erste 1999 offiziell verabschiedete Standard 802.11b arbeitet im 2.4 GHz Frequenzband und erreicht eine maximale Datenrate von 11 MBit/s, was einer effektiven Datenrate von 5,9 MBit/s (TCP) und 7,1 MBit/s (UDP) entspricht. Darauf folgte der 802.11a Standard, der im 5 GHz Frequenzband arbeitet und mit 54 MBit/s eine deutlich höhere Datenrate ermöglicht. Heute ist Hardware auf Basis des 802.11g Standards weit verbreitet, der ebenfalls eine Datenrate von 54 MBit/s besitzt, jedoch im 2.4 GHz Frequenzbereich arbeitet und kompatibel zum 802.11b Standard ist.

WLANs setzen sich zunehmend in Heimnetzwerken, aber auch innerhalb von Organisationen durch, da sie eine Vielzahl an Vorteilen bieten. So können WLANs sehr leicht aufgebaut werden, weil sie keine aufwändige Verkabelung voraussetzen und dem Nutzer flexiblen, positionsunabhängigen Netzzugang innerhalb der Reichweite der Basisstation (engl. access point) bieten. Des Weiteren können WLANs vergleichsweise kostengünstig redundant ausgelegt werden, so dass Clients bei Ausfall einer Basisstation von einer anderen übernommen werden, wodurch die Verfügbarkeit im Falle von Hardwareausfällen erhöht wird.

Aus diesen Gründen wird in den nächsten Jahren mit einer weiteren, stark zunehmenden Verbreitung von WLANs zum Aufbau geschlossener Netzwerke gerechnet. Gleichzeitig geht man von einer

starken Verbreitung so genannter öffentlicher *Hotspots* aus, die drahtlosen Internetzugang in Ballungsgebieten und öffentlichen Orten wie Bahnhöfen und Flughäfen bieten werden.

Gerade auch der kostengünstige kabellose Aufbau von WLANs könnte Anwender, insbesondere kleine bis mittelgroße Unternehmen, dazu bewegen ein separates VoIP-Netzwerk auf WLAN-Basis aufzubauen. In VoIP-Telefonanlagen ist es darüber hinaus geradezu natürlich Mobilteile über WLAN anzubinden, weil dies keinen Übergang bei der Signalisierung oder bei der Sprachübertragung erfordert, wie er beispielsweise bei der Nutzung von DECT anfallen würde. Erste Anbieter haben bereits entsprechende VoIP-Mobiltelefone auf WLAN-Basis auf den Markt gebracht und darüber hinaus sind auch hybride Mobiltelefone denkbar, die sowohl GSM/UMTS, als auch VoIP über WLAN oder Wimax (802.16) unterstützen.

Daher ist es absehbar, dass VoIP über WLAN, und somit auch den spezifischen Sicherheitsbedrohungen, mittelfristig eine große Bedeutung zukommen wird. Diese Sicherheitsbedrohungen werden im Kapitel 3.5.3 betrachtet. Zunächst soll jedoch ein kurzer Überblick über existierende WLAN Standards gegeben werden.

3.5.2 802.11 Sicherheitsmechanismen

WLANs nutzen Funkwellen als Broadcast Medium, so dass gesendete Nachrichten a-priori von jedem Gerät innerhalb der Reichweite empfangen und mitgelesen werden oder aber auch Nachrichten an jedes Gerät gesendet werden können. Aus diesem Grund hat das 802.11 Standardisierungsgremium Sicherheitsfeatures auf der Netzzugangsschicht spezifiziert, um einen Schutz, vergleichbar mit dem von kabelgebundenen Netzwerken, zu bieten. Damit war WEP (engl. wired equivalent privacy) geboren.

WPA und WPA2

Aufgrund der Sicherheitsschwächen von WEP wurde eine Arbeitsgruppe (TG i) ins Leben gerufen, die deutlich stärkere Sicherheitsmechanismen erarbeiten sollte. Um jedoch kurzfristig ein marktreifes sicheres WLAN anbieten zu können, spezifizierte das Wi-Fi Konsortium einen WPA (Wi-Fi Protected Access) genannten Interimstandard, der das unsichere WEP kurzfristig ablösen sollte. Bei der Entwicklung von WPA wurde, neben verbesserten Sicherheitseigenschaften, insbesondere auf eine weitgehende Hardwarekompatibilität zum 802.11g Standard geachtet, so dass er kurzfristig und kostengünstig auf existierender Hardware implementierbar war. Die wesentlichsten Neuerungen in WPA sind:

- Das TK*IP* (engl. temporal key integrity protocol) generiert stärkere RC4-Schlüssel aus den symmetrischen Master-Schlüsseln, wodurch ein effektiver 128-Bit RC4-Schlüssel zur Verschlüsselung verwendet wird und mit schwachen Schlüsseln verschlüsselte Pakete nicht mehr identifiziert werden können.
- Zur Authentifizierung von Paketen wird ein *MIC* (engl. message integrity code) verwendet, der als Keyed-Hashfuntion berechnet wird und eine stärkere Authentifizierung von Paketen darstellt.
- WPA spezifiziert die Verwendung der *802.1x* (standard for port based network access control). Dieser Standard ermöglicht eine starke Authentisierung auf Basis von EAP (engl. extensible authentication protocol) und löst gleichzeitig das Problem des Schlüsselmanagements, da der Authentisierungsserver einen gemeinsamen symmetrischen Schlüssel zwischen WLAN-Clients und Access-Points etablieren und in regelmäßigen Abständen erneuern kann.

Im Juni 2004 wurde der 802.11i Standard (auch als WPA2 bekannt) verabschiedet. Dieser umfasst alle Sicherheitsmechanismen von WPA und bietet darüber hinaus eine starke Verschlüsselung nach dem Advanced Encryption Standard (AES) im CCM Betriebsmodus, der gleichzeitig als Message Authentication Code fungiert [Wong05]. Leider kann das Feature AES Verschlüsselung meist nicht Hardware-kompatibel zu WEP implementiert werden, so dass der Standard 802.11i neue Hardware voraussetzt und nicht nachträglich per Software- oder Firmware-Update nachrüstbar ist.

Sowohl WPA als auch WPA2 (802.11i) können nach heutigem Kenntnisstand als hinreichend sicher betrachtet werden. Es verbleiben jedoch inhärente Bedrohungen gegen die Vertraulichkeit und Verfügbarkeit durch die Verwendung eines Funkmediums, welche zusammen mit WEP Risiken betrachtet werden.

3.5.3 802.11 Schwächen und VoWLAN Bedrohungen

Im Allgemeinen sind drahtlose Netzwerke anfälliger gegen jegliche Art von Angriffen, gleich ob aktiv oder passiv, da ein Angreifer sehr viel einfacher Zugang zum Netzwerk, sogar außerhalb der physischen Grenzen der betreibenden Organisation, erhalten kann und somit die erste Hürde, der Zugang zum Netzwerk, leicht zu nehmen ist. Somit können Angreifer aus sicherer Entfernung und vergleichsweise anonym operieren.

Daher implementieren heutige WLAN Komponenten einige Sicherheitsmechanismen, die diese Angriffe weitestgehend verhindern sollen. Leider sind viele der heute verbreiteten Sicherheitsmechanismen unzureichend und bergen daher weitreichende Risiken, sofern man sich ausschließlich auf sie verlässt und keine Sicherheitsmechanismen auf höheren Schichten verwendet.

MAC ACL (engl. access control list):

Access Points implementieren einen sehr rudimentären Zugangsschutz zum Drahtlosnetzwerk, indem sie nur solche Clients bedienen, deren MAC Adressen in einer Liste, der so genannten MAC ACL (engl. access control list), aufgeführt sind. Die Sicherheit dieser Maßnahme beruht darauf, dass Endgeräte eine eindeutige, unveränderbare MAC Adresse besitzen. Diese Annahme ist jedoch falsch, weil bei vielen verfügbaren WLAN Karten die MAC Adresse durch manipulierte Gerätetreiber [Wong05] geändert werden kann (MAC Spoofing), wodurch es möglich wird diese Maßnahme zu umgehen und ein Angreifer auf MAC-Ebene Zugang zum VoIP-Netzwerk erlangen kann.

Würde diese Maßnahme alleine zum Schutz eines VoIP WLAN-Netzwerkes eingesetzt, so könnte ein Angreifer beispielsweise ein Softphone auf einem Laptop betreiben, die MAC-Adresse eines VoIP-Telefons im WLAN verwenden und so beispielsweise auf Kosten seines Opfers telefonieren. Des Weiteren können Netzwerkdienste wie DHCP-Server oder ARP-Antworten manipuliert werden, um die Konfiguration von WLAN-VoIP-Telefonen zu manipulieren (siehe auch Kapitel 3.4.2).

WEP (engl. wired equivalent privacy)

WEP war der erste Sicherheitsmechanismus zum Schutz von 802.11 Drahtlosnetzwerken. Neben dem Schutz der Authentizität und Vertraulichkeit der WLAN-Daten bietet WEP einen expliziten Challenge-Response Zugangsschutz auf Basis der Verschlüsselung, weil Access Points mit aktivierter WEP-Verschlüsselung weder *Klartext*pakete annehmen noch versenden.

Als kryptographischer Algorithmus kommt die RC4-Stromchiffre mit 64- oder 128-Bit Schlüssel zum Einsatz. Der Schlüsseltext ergibt sich als XOR zwischen RC4-Strom und Klartext, dem zum Schutz der Authentizität und Integrität zuvor eine CRC (engl. cyclic redundancy check) Prüfsumme angehangen wird. Der eigentliche RC4 Schlüssel wird aus einem *dynamischen Teil* und einem s*tatischen Teil,* dem WEP-Passwort*,* das dem Access-Point und dem Client bekannt sein muss, generiert. Der dynamische Teil besteht aus einem 24-Bit Initialisierungswert (IV), der nach jedem Paket erhöht und als Klartext zusammen mit dem verschlüsselten Paket übertragen wird.

Erste Sicherheitsanalysen förderten schon kurz nach der Veröffentlichung des WLAN Standards 802.11b Schwächen in WEP zu Tage, die sich im Laufe weiterer Untersuchungen als erhebliche Sicherheitslücken erwiesen, welche im Folgenden beschrieben werden. Die resultierenden Bedrohungen auf VoIP-Systeme werden ebenfalls in Abschnitt betrachtet.

Eine wesentliche Schwäche von WEP ist die Tatsache, dass der Initialisierungswert als Klartext in jedem Paket mitgesendet wird. Dies vermindert zum einen die effektive Schlüssellänge deutlich auf 40 Bit bzw. 104 Bit und zum anderen entstehen subtile, ausnutzbare Schwächen in der RC4-basierten Stromchiffre:

WEP Key-Recovery: Fluhrer, Mantin und Shamir [FMS01] identifizierten wiederkehrende schwache RC4-Schlüssel in WEP und entwickelten einen Angriff, der den WEP-Schlüssel durch passives Lauschen rekonstruieren kann, sofern genügend Pakete mitgehört wurden. Mit einer ersten Implementierung dieses Angriffes wiesen Stubblefield, Ioannidis und Rubin [SIR02] die Praktikabilität dieses Angriffs nach. Mittlerweile existieren mehrere Open-Source Implementierungen dieses Angriffs, die 5 bis 10 Millionen WEP-Pakete zur Rekonstruktion des Schlüssels benötigen. Verbesserte Versionen des Angriffs können den Schlüssel mit deutlich weniger Paketen (unter 1 Million) rekonstruieren [Schmidt05]. Selbst in WLANs mit niedriger Auslastung kann dieser Angriff zum Erfolg führen, wenn er mit einem aktiven Angriff kombiniert wird, der dafür sorgt, dass die notwendigen Pakete von Clients im WLAN gesendet werden (z. B. Replay von ARP-Requests) [Schmidt05].

Hat ein Angreifer erst den Schlüssel eines VoIP-Endgerätes rekonstruiert, so hat er vollen Zugriff auf das WLAN und kann somit auch alle zuvor (siehe Kapitel 3.3.1) beschriebenen Angriffe ausführen. Ein wichtiger Unterschied besteht darin, dass sich der Angreifer dazu keinen physischen Zugang zur Netzwerkinfrastruktur verschaffen muss, sondern unauffällig und aus sicherer Entfernung agieren kann.

IV-Kollisionen: Unter IV-Kollisionen versteht man die Verschlüsselung unterschiedlicher Pakete unter Verwendung des gleichen IV-Wertes und des gleichen statischen Schlüssels. In diesem Fall ist der abgeleitete RC4 Schlüssel und somit der zur Verschlüsselung verwendete RC4 Schlüsselstrom identisch, wodurch die XOR-Verknüpfung der beiden Schlüsseltexte der XOR-Verknüpfung der *Klartexte* entspricht. Mittels statistischer Methoden können daraus unter Umständen Teile der beiden Klartexte rekonstruiert werden [BGW01]. Da die WEP Spezifikation die Erzeugung der Initialisierungswerte offen lässt, kann es relativ häufig zu IV Kollisionen kommen. So berichten Borisov, Goldberg und Wagner [BGW01] von Implementierungen, die die IV-Werte nach jeder Initialisierung auf Null setzen, wodurch zahlreiche IV-Kollisionen vorprogrammiert sind.

Schwache Authentisierung: Die Authentisierung von WEP-Paketen ist ebenfalls angreifbar, weil die CRC-Prüfsumme nur zur Erkennung von zufälligen, nicht-böswilliger Fehler dient und sowohl die CRC-Prüfsumme als auch die Stromchiffre linear sind [BGW01]. Dadurch bewirkt das Kippen eines Bits im Schlüsseltext ein Kippen des entsprechenden Klartextbits und ein Angreifer kann den CRC-basierten MAC (engl. message authentication code) entsprechend anpassen. Borisov, Goldberg und Wagner [BGW01] deckten zudem Schwächen auf, die es erlauben neue authentische WEP-Frames ohne Kenntnis des Schlüssels zu generieren, wodurch sich die WEP-basierte Zugangskontrolle umgehen lässt. Auch sind Replays ganzer verschlüsselter Pakete möglich, da der Standard keine Überprüfung des WEP Initialisierungswertes vorschreibt. Diese Schwachstellen ermöglichen aktive Angriffe, beispielsweise mit dem Ziel, die Verfügbarkeit zu stören oder das Senden vieler verschlüsselter Pakete auszulösen, um einen WEP-Key Recovery Angriff zu beschleunigen (siehe unten).

Angreifer gegen WLAN-basierende VoIP-Systeme können die schwache Authentisierung nutzen, um Angriffe auf Netzwerkebene durchzuführen, Rufe zu initiieren oder falsche einkommende Rufe zu signalisieren.

Ein weiteres schwerwiegendes Problem liegt darin, dass die WEP-Management Frames *nicht* authentifiziert werden. Dies kann insbesondere für DoS-Angriffe ausgenutzt werden (siehe oben).

WEP-Gruppenschlüssel: Der WEP-Standard spezifiziert 4 WEP-Schlüssel pro WLAN, wodurch sich mehrere Clients eines WLANs dieselben Schlüssel teilen müssen. Selbst von den 4 möglichen WEP-Schlüsseln wird häufig nur ein einziger im ganzen WLAN verwendet. Dadurch können Clients den Datenverkehr anderer Clients im WLAN mitlesen und deren Authentisierung fälschen, wodurch ein Insider unerkannt neue Pakete unter falscher Identität senden kann.

Wird in einem solchen WLAN VoIP-Telefonie betrieben, kann ein Insider die Datenströme (Medienströme und Signalisierung) anderer VoIP-Telefone abhören und Anrufe unter fremder Identität initiieren, sofern auf den höheren Schichten keine Sicherheitsmechanismen verwendet werden.

Solche Insiderangriffe sind nicht mehr möglich, wenn individuelle WEP-Schlüssel zwischen Client und Access Point vereinbart werden, so dass die Kommunikation anderer Clients nicht mehr ohne weiteres entschlüsselt werden kann. Dieses Feature wird jedoch nicht von allen WLAN Access Points implementiert, so dass häufig weiterhin nur ein symmetrischer Schlüssel für das gesamte WLAN genutzt wird.

Selbst wenn ein Access Point individuelle Schlüssel unterstützt, stellt sich das Problem des Schlüsselmanagements in (mobilen) VoIP Endgeräten. Auch übliche Mechanismen wie 802.1X dürften erst mittelfristig in VoIP Endgeräten verfügbar sein, was zudem auch die Anfälligkeit gegen WEP-Key-Recovery Angriffe deutlich erhöht.

Access Points: Sollen VoIP Endgeräte über WLAN angebunden werden, so muß zwangsläufig ein Access Point betrieben werden. Da die Zugangskontrolle WEP-basierter Access Points sehr schwach ist, können diese das gesamte interne Netzwerk gefährden. Über einen schlecht gesicherten Access Point können Angreifer möglicherweise Zugang zum internen Netzwerk erlangen und existierende Schutzmaßnahmen wie Firewalls umgehen.

Weitere Bedrohungen können durch die Konfigurationsschnittstelle von Access-Points entstehen, da sie potentielle Sicherheitslücken, wie Standardpasswörter oder Buffer Overflows in der Systemsoftware, besitzen können.

Vertraulichkeit von Meta-Information: Ein inhärentes Problem ist die Vertraulichkeit von Meta-Information. Diese lässt sich in einem drahtlosen Netzwerk selbst durch aktivierte starke Verschlüsselung kaum schützen. Dies liegt daran, dass nur die eigentlichen Nutzdaten (engl. payload) der WLAN-Frames verschlüsselt werden. Die Adressinformation (insbesondere die MAC-Adresse des Empfängers) muss unter praktischen Gesichtspunkten als Klartext übertragen werden.[2]

Damit lässt sich das Kommunikationverhalten von drahtlosen Endgeräten überwachen, wodurch ein Angreifer Rückschlüsse auf Metainformationen wie eingehende und abgehende Anrufe, aktive Endgeräte sowie auf die Dauer von Gesprächen ziehen kann.

Diese Problematik stellt jedoch keine VoWLAN-spezifische Bedrohung dar, sondern tritt in allen kabellosen Endgeräten, also auch in DECT Mobilteilen auf. Lediglich die verbreitete Basis an potentiellen Sniffern ist im Falle von WLANs größer, weil jeder Laptop mit WLAN-Modul per Software zum Sniffer umfunktioniert werden kann.

Denial-of-Service: Durch die folgenden DoS-Angriffe kann die Verfügbarkeit des ganzen WLANs oder einzelner Stationen gestört werden. Für VoIP Endgeräte, die über WLAN angebunden sind, bedeutet dies, dass ein Angreifer die Signalisierung von eintreffenden Anrufen sowie die Initiierung von Anrufen unterbinden kann. Es können aber auch laufende Telefonate abgebrochen werden. Diese Angriffe funktionieren größtenteils auch gegen WPA-geschützte 802.11 Drahtlosnetzwerke [GN04]. Bei Verwendung von 802.1X können darüber hinaus EAP-spezifische DoS-Angriffe (z. B. durch gefälschte EAPoL-Failure Nachrichten oder Flooding mit EAPoL-Start Nachrichten) die Verfügbarkeit des WLAN stören [GN04].

Der offensichtlichste DoS-Angriff besteht in der Verwendung eines Störsenders, der im entsprechenden Frequenzbereich (2.4 GHz für 802.11b/g und 5 GHz für 802.11a/h) arbeitet.[3]

Weitaus trickreicher sind DoS-Angriffe, die Protokollschwächen ausnutzen. Diese sind ähnlich effektiv wie Störsender, können jedoch wesentlich gezielter eingesetzt werden und sind außerdem auch schwieriger zu erkennen. Zudem können sie mit standard-konformer WLAN-Hardware und frei verfügbarer Software durchgeführt werden, weil manipulierte Gerätetreiber über die Firmware einiger 802.11-konformer Hardware direkten Zugriff auf die Protokolle der Netzzugangsschicht erlangen können.

---

[2] Sonst müsste jeder Client versuchen, jedes Datenpaket zu entschlüsseln, um zu erkennen, ob es an ihn adressiert ist.

[3] Das 2.4 GHz Band ist sehr anfällig für Störungen durch elektrische Geräte wie Mikrowellen und es kann zu Wechselwirkungen zwischen mehreren WLANs kommen, weil nur eine geringe Anzahl an Kanälen zur Verfügung steht.

Angriffspunkte können der zentrale WLAN-Access-Point sein, so dass das gesamte WLAN gestört wird, oder aber bestimmte Endgeräte oder Verbindungen, die gezielt gestört werden:

- Beim so genannten *„Association Flooding“* und *„Authentication Flooding“* sendet ein Angreifer eine große Anzahl entsprechender Management-Frames mit gefälschten Absender MAC-Adressen an den Access Point, um dessen verfügbare Ressourcen aufzubrauchen und dessen korrekte Funktion zu stören. Neuere Access Points sollen gegen diese Angriffe weitestgehend immun sein [KS04].
- Beim *Deauthentication-Angriff* sendet der Angreifer ein Deauthentication-Paket mit gefälschter MAC-Adresse des Opfers, woraufhin der Access-Point die Verbindung zum Opfer auflöst. Dieser Angriff lässt sich sogar effizient auf das ganze WLAN ausdehnen, indem der Angreifer Deauthentication-Pakete unter der Adresse des Access Points per Broadcast versendet. Dieser Angriff ist sogar bei aktivierter WEP-Verschlüsselung möglich, weil die Deauthentication-Pakete nicht authentifiziert werden. Ein ähnlicher Angriff ist der *„Disassociation-Angriff“*, bei dem der Angreifer Disassociation-Pakete mit falscher MAC-Adresse an den Access Point sendet.
- Eine weitere Quelle für DoS-Angriffe ist der Mechanismus zur Vermeidung von Kollisionen auf dem Funkmedium. Durch gezielte Störung bestimmter Frames (beispielsweise des CTS Frames) können Stationen am Senden gehindert werden. Des Weiteren kann ein Angreifer seine WLAN-Komponente per Software dazu veranlassen, die im 802.11 Standard vorgeschriebenen Parameter zu verändern, um dadurch das WLAN zu monopolisieren. So kann ein Angreifer vorgeschriebene Wartezeiten (SIFS oder DIFS) vor dem Zugriff auf das Medium ignorieren, um konformen Stationen immer zuvorzukommen. Des Weiteren kann ein Angreifer den NAV-Parameter in RTS-Frames vergrößern, mit dem ein Angreifer das WLAN exklusiv reservieren kann, wodurch konforme Stationen vom Zugriff auf das WLAN abgehalten werden.
  Raya, Hubaux und Aad [RHA2004] beschreiben mehrere Ansätze, wie Angreifer Ihre eigene Durchsetzung auf Kosten anderer Teilnehmer im gleichen WLAN erhöhen können. Diese Angreifer verfolgen somit nicht direkt das Ziel die Verfügbarkeit des Netzwerkes für andere Teilnehmer zu reduzieren, es folgt jedoch indirekt, weil die Bandbreite beschränkt ist und der Angreifer seinen Anteil maximiert. Des Weiteren lassen sich diese Angriffe dahingehend optimieren, dass die Verfügbarkeit des Netzwerkes möglichst stark gestört wird.

4. Sicherheitsmaßnahmen

4.1 Schutzbedarfsfeststellung und Sicherheitsmaßnahmen

Voraussetzung für die Auswahl geeigneter Schutzmaßnahmen ist eine Schutzbedarfsfeststellung, deren Ziel es ist zu entscheiden, welchen Schutzbedarf ein Telekommunikationssystem bezüglich der Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit besitzt.

Daher ist die genaue Einordnung der Telefonie und ihrer Bedeutung in den Ablaufprozessen des Unternehmens/Behörde essentielle Voraussetzung zur Ermittlung des Schutzbedarfs. So hat ein Call-Center eine andere Anforderung an die Verfügbarkeit der Telefonie als ein Konstruktionsbüro, eine Ermittlungs- bzw. Jusitzbehörde andere Anforderungen an die Vertraulichkeit der ausgetauschten Informationen als die Tourismuszentrale eines Landkreises.

Der Schutzbedarf wird laut BSI Grundschutzhandbuch [GHSB04] qualitativ in den drei Kategorien „niedrig-mittel“, „hoch“ und „sehr hoch“ eingestuft und orientiert sich an den Schäden, die mit einer Beeinträchtigung des betroffenen TK-Systems verbunden sind. Zu den Schutzbedarfskategorien zählen Verstöße gegen Gesetze/Vorschriften/Verträge, die Beeinträchtigung des informationellen Selbstbestimmungsrechtes, die Beeinträchtigung der persönlichen Unversehrtheit, die Beeinträchtigung der Aufgabenerfüllung, eine mögliche negative Außenwirkung, sowie mögliche finanzielle Auswirkungen.

Bei der Schutzbedarfsbestimmung werden zunächst die Schadensszenarien mit den möglichen maximalen Schäden bei Verletzung der Sicherheitsziele aus Sicht des Anwenders beschrieben. Davon ausgehend wird für jede Komponente des Systems und für jedes Sicherheitsziel ein Schutzbedarf festgestellt.

Eine ausführliche Beschreibung der Vorgehensweise ist im GSHB, Kapitel 2.2 zu finden. Im Kapitel 6 werden Einsatzszenarien, Schutzbedarf und Maßnahmenempfehlungen beispielhaft aufgezeigt.

In diesem Kapitel werden Maßnahmen zur Bereitstellung eines sicheren Betriebs von VoIP-Umgebungen vorgestellt. Dabei ist zu beachten, dass die jeweiligen Maßnahmen unabhängig von einem konkreten Schutzbedarf dargestellt werden. Welche Schutzmaßnahmen im Einzelnen benötigt werden kann erst nach erfolgter Schutzbedarfsfeststellung erfolgen.

Insgesamt ist zu beachten, dass heutige VoIP-Systeme – sowohl die zentralen Komponenten als auch die Endgeräte – üblicherweise auf Standardhard- und -software aufsetzen und die gleichen IP-basierte Netzwerktechnologie verwenden wie die jetzigen Datennetze. Somit gelten die allgemein auf IP- und Ethernet-Netze zutreffenden Maßnahmen auch für VoIP-Umgebungen. Eine grundlegende Übersicht der Sicherheitsmaßnahmen sowie der Design-Aspekte zum Aufbau solcher Netze wird im vom Bundesamt für Sicherheit in der Informationstechnik veröffentlichten IT-Grundschutzhandbuch [GSHB04] gegeben.

4.2 Netzdesign

Die hohe Verfügbarkeit von VoIP stellt eine besondere Herausforderung an die Netzinfrastruktur dar. Das IP-Netzwerk verbindet alle Anwendungen, Middleware und Endgeräte (Server, PCs, IP-Telefone). Die Nutzer der herkömmlichen Telefonie sind einen nahezu störungsfreien Telefonbetrieb gewohnt. Die hohe Verfügbarkeit bei der herkömmlichen Telefonie wird durch TDM–Technik (TDM – Time Division Multiplex-Zeitmultiplex) erreicht, die bei einer Verbindung einen dedizierten Kanal mit einer festen Bandbreite zur Verfügung stellt und so die Übertragung der Sprache in sehr guter Qualität ermöglicht. Der Zugang zu diesen Kanälen bleibt in der Regel nur Fachpersonal des Telekommunikationsanbieters (Telefongesellschaft) vorbehalten. Die Komponenten der VoIP-Technik arbeiten paketorientiert und sind von Hause aus gegen Überlast und Kompromittierung (z. B. DoS, illegales Abhören) anfälliger. Bislang haben sich die Netzwerkdesigner darauf konzentriert, die

Anforderungen an das Netzwerk mit speziellen Produkten und Komponenten zu lösen. Dies führt zwangsläufig zu einem hohen Managementaufwand und macht Betrieb, Verwaltung und Wartung komplexer und teurer. Das heutige Netzwerkdesign strebt ein konvergentes und universelles Netzwerk für Sprachen und Daten an, in dem alle Einzelfähigkeiten - wie Sicherheitseinstellungen, Durchsatz und Verfügbarkeit - in einem Gesamtsystem integriert sind. Gegenüber einem klassischen Telekommunikationssystem (Leitung zum öffentlichen Netz, TK-Anlage, Telefon) hängt die Verfügbarkeit eines VoIP-Systems von deutlich mehr Komponenten (Anbindung an das öffentliche Netz, VoIP-Server, Switches, Router, Firewall, VoIP-Telefone) ab, deren Ausfall die Funktion teilweise oder ganz verhindern kann. Für die Sicherheit bedeutet das die Aufstellung netzwerkweiter Sicherheitsrichtlinien statt Einzellösungen und ebenso das netzwerkweite Management der Systemkomponenten. Dies schließt auch weiterführende Technologien wie Wireless LAN und IP-Sprachverkehr mit ein. Kerngedanke ist die Integration von Sicherheitsrichtlinien in alle Netzwerkkomponenten und Endgeräte.

Die Sicherheitsmaßnahmen [1]…[19] werden im Einzelnen diskutiert und im Folgenden wird auf sie verwiesen. Die einzelnen Maßnahmen sind für sich nicht ausreichend, um einen Schutz gegen Angriffe zu erreichen, sondern bilden nur einzelne Bausteine [GHSB04] in den Sicherungsmaßnahmen. Erst durch das Zusammenwirken der verschiedenen Sicherheitsmaßnahmen verringern sich die Angriffsmöglichkeiten.

[1] Sicherungsmaßnahmen für einen physikalischer Schutz

Zur Vermeidung von Manipulationen von VoIP-Komponenten insbesondere im zentralen Bereich – hierzu zählen VoIP-Server, UMS-Server, Gateways zum PSTN, Core Switches, Workgroup Switches, Router, Firewall und IDS-Systeme - sollten diese in getrennten, verschließbaren und überwachten Räumlichkeiten untergebracht werden. Der physikalische Zutritt zu den zentralen Servern und Komponenten des Netzwerkes sollte nur autorisierten Personen erlaubt sein. Die Zutrittskontrolleinrichtung selbst sollte über Smartcarts und Einmal-Passwörter für die starke Authentisierung eines Benutzers und eine Videoüberwachung verfügen. Eine regelmäßige Überprüfung gehört ebenso zu den Sicherungsmaßnahmen. Zur Erhöhung der Verfügbarkeit sind diese Räume durch weitere Sicherungsmaßnahmen gegen Stromausfall, Wasserschaden oder Feuer zu ergänzen.

Wichtige Kabeltrassen innerhalb von Gebäuden sollten vor physikalischem Zugriff durch eine Verkleidung oder Unterputzverlegung abgesichert werden. Die Verkleidung ist feuerfest auszulegen, damit auch im Brandfall die Funktionsfähigkeit der Netzwerkinfrastruktur - zumindest zeitweise - erhalten bleibt. Nichtzentrale Komponenten (z. B. Tertiärkomponenten wie Workgroup Switches) dürfen ebenso wenig frei zugänglich sein und sind in abschließbaren Netzschränken gegen unbefugten Zugriff zu schützen.

[2] Sicherungsmaßnahmen für eine Stromversorgung

Um das Telefoniesystem auch bei einem partiellen oder vollständigen Ausfall der Stromversorgung verfügbar zu halten, sind Maßnahmen zur Sicherung der Stromversorgung zu ergreifen.

Power-over-Ethernet (PoE): Die Stromversorgung der Endgeräte kann mittels PoE physikalisch über die gleichen Netzwerkleitungen gewährleistet werden, die auch für die Sprach- und Datenkommunikation genutzt werden, so dass keine zusätzlichen Netzteile für die VoIP-Telefone verwendet werden müssen. PoE ist im IEEE-Standard 802.3af [I802.3af] standardisiert. Der Standard definiert den Modus A (Inline-Power, Phantom-Power über die Pins 1&2 und 3&6) und Modus B (Midspan-Power, Pins 4&5 und 7&8)). Bei der Midspan-Energieversorgung sind aus heutiger Sicht drei nachteilige Begebenheiten zu erwähnen:

a) In den Verteilerschränken sind zusätzliche Verteilerelemente einzubauen, was zu Platzproblemen führen kann.
b) Die Anzahl der Patchkabel verdoppelt sich in den Datenverteilern.

c) Wegen der Belegung der Pins 4&5 und 7&8 des Ethernetkabels ist eine 8-adrige Anschlusstechnik notwendig, die kein „Cable Sharing“ zulässt, d.h. eine doppelte Anwendung über ein Ethernetkabel ist nicht mehr möglich.

Das VoIP-Endgerät sollte sich die Adernpaare selbstständig aussuchen, auf welchem die Speisespannung anliegt und sollte auch gegen eine Verpolung unempfindlich sein. Moderne speisende Endgeräte (Switch) können die Leistungsabgabe über eine Signatur der Endgeräte (VoIP-Telefon) in den Klassen 0 bis 3 optimieren und eine bestmögliche Auslastung der Switch-Ports gewährleisten. Die maximale Speisespannung beträgt 57 Volt bei 0,4 Ampére. Die Klasse 0 ist die vordefinierte Einstellung und erlaubt eine Leistungsabgabe von 0,44 Watt bis 12,95 Watt.

Aus Gründen einer erhöhten Brandgefahr sollte auf eine externe Energieversorgung der VoIP-Telefone über Steckernetzteile verzichtet werden. Die Energieversorgung mittels PoE ermöglicht eine zentrale Energiepufferung mit USV-Anlagen, um Stromausfälle zu überbrücken.

Unterbrechungsfreie Stromversorgung (USV): Die Stromversorgung der Middleware und der Übertragungswege (Switche, Router) sollte durch geeignete USV-Systeme abgesichert werden. Bei erhöhtem Schutzbedarf (Verfügbarkeit) sind diese so auszulegen, dass nicht ein geregeltes Abschalten der Systeme durchgeführt wird, sondern der Betrieb für eine durch die Verfügbarkeitsanforderung festgelegte Zeit aufrechterhalten bleibt. In bestimmten Fällen sind für längere Stromausfälle Dieselaggregaten zur Energiegewinnung vorzusehen.

Zu den Sicherungsmaßnahmen der Energieversorgung gehört eine regelmäßige Wartung und Überprüfung der USV- und Notstromversorgungsanlage durch Fachpersonal, um einen weitgehend störungsfreien und hochverfügbaren Betrieb zu gewährleisten. Eine automatische Überwachung und Meldesysteme (E-Mail, SMS) über den Zustand der Energieversorgungsanlagen, sowie ein Entstörungsmanagement sollten in einem VoIP-Betriebskonzept integriert werden.

[3] Sicherungsmaßnahme Trennung von Sprach- und Datennetz

IP-basierende Telefonie ermöglicht das Telefonieren über das existierende Datennetz. Jedoch sollten zur Erhöhung von Skalierbarkeit, QoS, Managebarkeit und Sicherheit die Datennetze von den Sprachnetzen logisch getrennt werden. In besonders kritischen Fällen (beispielsweise Polizei) kann eine komplette physikalische Trennung des Sprachnetzes vom Datennetz sinnvoll sein. Die Trennung von Daten- und Sprachnetzen verringert im ersten Ansatz deutlich die Angriffsmöglichkeiten. Eine logische Trennung kann mit VLAN-Technologie auf der Ebene 2 mit VLAN-fähigen Switches aufgebaut werden. VLANs alleine bieten jedoch keinen Schutz vor Angreifern, die sich mit ihrem System (PC, Laptop oder Server) physikalisch in ein VLAN einklinken. Da der VLAN-Port des Telefons jedem unmittelbar zugänglich ist, kann der Angreifer direkt die Telefone im VLAN angreifen, indem er z. B. anstatt eines Telefons seinen PC mit dem VLAN-Netz verbindet. Aus diesem Grunde sollten weitere, über die Netztrennung hinausgehende Maßnahmen getroffen werden, um derartigen Angriffe zu begegnen. Je nach Schutzbedarf sollten zusätzliche Maßnahmen wie Authentisierung nach 802.1x [IEEE01], dynamische oder statische Zuordnung der MAC-Adresse zu Port und VLAN-Zugriffslisten eingesetzt werden, um einen sichereren Betrieb zu gewährleisten.

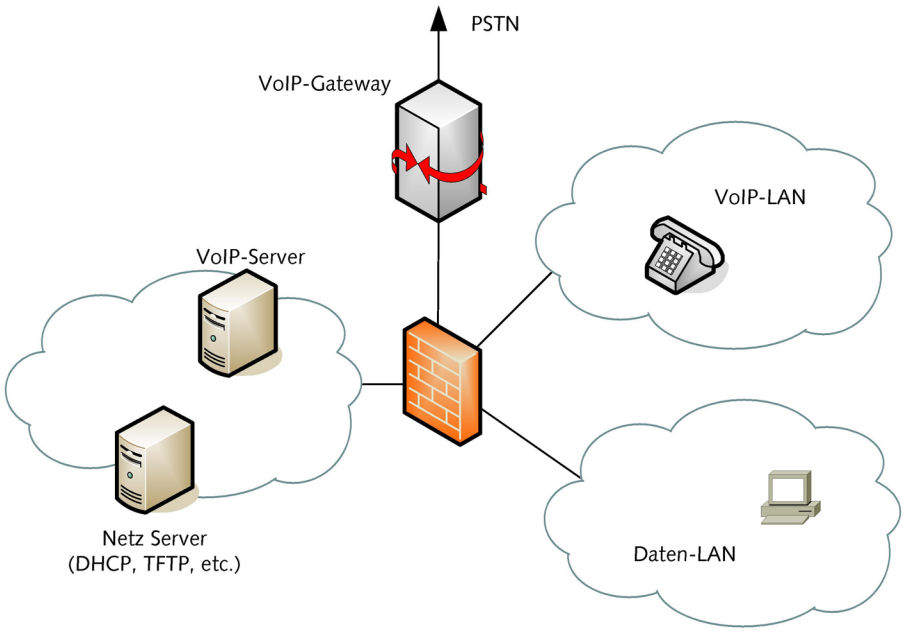

Abbildung 4.1 Prinzipieller Aufbau einer VoIP-Netzwerkinfrastruktur mit der Trennung von Sprach- und Datennetz

[4] Sicherungsmaßnahme Authentifizierung Endgeräte

Wann immer es möglich ist, sollte das IP-Telefon einer Authentifizierung unterzogen werden. Die einfachste Methode ist die Authentifizierung über die MAC-Adresse. Versucht ein Endgerät, über das Netzwerk Daten auszutauschen, sollte die MAC-Adresse automatisch von dem Netzwerk-Switch geblockt werden, falls die MAC-Adresse dem Switch unbekannt ist bzw. am falschen Port erkannt wird, denn es könnte sich um einen Angreifer handeln. Neuere Switches haben die Fähigkeit neben den statischen MAC-Einstellungen auch eine dynamische Verbindungstabelle aller gültigen angeschlossenen Endgeräte aufzubauen und damit neue Anschlussversuche von Geräten zu blocken. Die dynamischen MAC-Tabellen werden nach dem Anschalten des Switches aufgebaut und im Switch gespeichert. Kennt ein Angreifer eine gültige MAC-Adresse, kann er in seinem System die gültige MAC-Adresse setzen und so diesen Mechanismus umgehen. Wie man erkennen kann, greift diese Maßnahme nur teilweise gegen das Eindringen ins VLAN, weil der Transientzustand beim Einschalten nicht abgedeckt wird und auch das Vortäuschen einer korrekten MAC-Adresse nicht verhindert werden kann. Nur eine starke Authentifizierung nach 802.1x am Switch-Port kann das Eindringen ins VLAN verhindern.

Endgeräte verfügen oftmals über einen eingebauten Switch, um in VLANs geführte Frames weiterzureichen bzw. fehlende Ports am Switch oder den Anschlussdosen in Büros zu kompensieren. Diese in die Telefone integrierten Switches stellen wegen ihrer im Vergleich zu einem Etagenswitch (Backbone) nicht vorhandenen Konfigurationsmöglichkeiten eine Sicherheitslücke dar, die durch Abschaltung der zusätzlichen Ports am Telefon geschlossen werden sollte. Trunking zum Endgerät eröffnet bewusst oder unbewusst die Möglichkeit LAN-Kurzschlüsse zu erzeugen. Aus diesem Grund sollte kein Trunking zum Telefon verwendet werden.

Externe Nutzer (beispielsweise Heimarbeitsplätze) sollten nur über einen gesicherten VPN-Zugang an das Telefon-VLAN angeschlossen werden, wobei die Pakete der externen Nutzer über eine Firewall geführt werden sollten, bevor sie in das Telefon-VLAN gelangen.

[5] Sicherungsmaßnahmen gegen MAC Spoofing

MAC Spoofing und MAC Flooding-Angriffe können in modernen Switches über Porteinstellungen unterbunden werden. In der Konfiguration sollte die Gesamtanzahl der MAC-Adressen an dem Switch limitiert werden, und es sollte festgelegt werden, um welche MAC-Adressen es sich dabei handeln darf. Mit der Überwachung der Quelladressen bieten einige Switches einen weiteren Schutzmechanismus gegen MAC Spoofing an. Daneben gibt es die Möglichkeit über SNMP-Traps Verstöße mitzuprotokollieren, um gegebenenfalls Gegenmaßnahmen, wie z. B. VLAN-Zugriffslisten auf dem Switch, dem Router oder der Firewall einzuleiten.

Statischer MAC-Eintrag

MAC-Adressen werden dynamisch vom Switch erfasst, sobald ein Frame auf dem Port eintrifft. Die Quelladresse wird aus dem Frame ausgelesen, mit dem Port verknüpft und in der MAC-Tabelle abgelegt. MAC-Adressen, die mit keinem Port verknüpft werden können, werden an alle Ports des relevanten VLANs weitergegeben. Um an dieser Stelle Manipulationen der MAC-Tabelle im Switch durch einen Angreifer zu unterbinden, sollte eine feste Zuordnung der wichtigsten VoIP-Systeme durch eine statische Verknüpfung von MAC-Adresse und Port herbeigeführt werden. Der Versuch den statischen Eintrag in der MAC-Tabelle zu manipulieren wird damit verhindert. Für alle kritischen Systeme wie VoIP-Server, Gateways und Gatekeeper sollten feste MAC-Zuordnungen vorgenommen werden.

Aktivierungszeiten am Switch-Port festlegen.

Bei häufig wechselnden Anbindungen (z. B. Laptops) ist es sinnvoll, eine aktive Zeit sowie eine inaktive Zeit für die Switch-Ports zu definieren. Eine aktive Zeit oder Lebensdauer der MAC-Adresse kann auch zum Schutz vor wiederholten MAC-Adressenänderungen (Spoofing) benutzt werden, d.h. eine neue MAC-Adresse wird erst nach dem Ablauf der Lebensdauer in die MAC-Tabelle des Switches übernommen. Durch diese Maßnahme wird MAC Spoofing eingedämmt. Die Einstellung der aktiven Zeit sollte dabei immer kleiner als die inaktive Zeit sein, denn damit wird gewährleistet, dass alle Adressen sicher aus der MAC-Tabelle entfernt werden.

Verletzungslimitierung einschalten

Mit der Begrenzung der Anmeldeversuche am Switch-Port soll verhindert werden, dass sich eine bereits gültige MAC-Adresse erneut in die MAC-Tabelle des Switches einträgt oder ein Angreifer mit einer gefälschten MAC-Adresse sich wiederholt am Switch-Port anmeldet und dadurch gültige MAC-Adressen aus der MAC-Tabelle entfernt. Einige Switches sperren daraufhin den Port und geben ihn erst wieder nach dem Ablauf eines Timers oder manuell wieder frei und setzen eine Meldung an den Syslog-Server ab.

802.1x Authentifizierung

Die statische Zuordnung von MAC-Adressen zu Ports in den Switches schränkt die Flexibilität der Netzwerkinfrastruktur stark ein. Der IEEE-802.1x-Standard [ReJö04] ist ein wichtiger Eckstein im Sicherheitskonzept für den Netzwerkzugang und bietet die Möglichkeit, schon am Netzwerkzugangsport des Switches eine Benutzerauthentifizierung durchzuführen. Dabei erfolgt die Authentifizierung mittels des Extensible Authentication-Protokolls (EAP). EAP beschreibt den Austausch der Authentifizierung zwischen Benutzer und Authentifizierungsserver (Radiusserver), wobei die eigentliche Authentifizierung des Benutzers zum Beispiel mit den Verfahren MD5 oder TLS erfolgt. Bei erfolgreicher Authentifizierung wird der Port für den Datenverkehr freigegeben. Mit der 802.1x-Funktion Single-Sign-On kann sich der Benutzer mit einer einzigen Authentifizierung an verschiedenen Systemen anmelden, z. B. bei NAS, Firewalls, VPNs oder Wireless LANs. Der zentrale Authentifizierungsansatz 802.1x ist deutlich flexibler, sicherer und nur mit einem einmaligen Administrationsaufwand verbunden. Insbesondere kann in vielen Fällen auf bestehende Benutzerdatenstrukturen zurückgegriffen werden und neben der Zugangskontrolle eine Bandbreitenzuweisung und eine Abrechnung vorgenommen werden.

[6] Sicherungsmaßnahmen gegen ARP Spoofing

ARP-Attacken, die oft auch als ARP Spoofing oder ARP Cache Poisoning bezeichnet werden, erlauben eine Vielzahl verschiedener Attacken, wie zum Beispiel DoS, Umleiten des VoIP–Verkehrs oder Abhören und Manipulation des Medienstroms. Im Folgenden werden die verschiedenen Sicherungsmaßnahmen vorgestellt.

Gratuitous ARP abschalten

Die Empfänger überprüfen in der Regel nicht das Feld mit der Zieladresse, sondern übernehmen die ARP-Adresse ungeprüft in ihre ARP-Tabelle. Mit einem einzigen Ethernet-Broadcast kann auf allen Rechnern innerhalb der Broadcast-Domäne ein vorhandener Eintrag manipuliert werden, um z. B. den Endsystemen eine neue Gateway-Adresse mitzuteilen. Deshalb sollte Gratuitous ARP [RFC3220] in jedem Fall an allen Endgeräten und Servern abgeschaltet werden.

Statische ARP-Einstellungen

Statische ARP-Einträge bieten in der Regel keinen Schutz gegen ARP Spoofing, weil in den meisten IP-Implementierungen die statischen Einträge mit ARP Replay- oder ARP Request-Paketen überschrieben werden können.

Proxy ARP abschalten

Proxy ARP-Angriffe [RFC 1027] in Netzwerken können recht einfach unterbunden werden, indem auf den Router-Schnittstellen der Mechanismus Proxy ARP abschaltet wird. Damit kann der Angreifer auf dem Zielsystem (z. B. VoIP-Server, Telefon) keinen falschen ARP-Eintrag generieren.

[7] Maßnahmen gegen DHCP-Attacken

Das DHCP-Protokoll wird zur Vergabe von IP-Adresse, sowie zur Festlegung von DNS-Server und des Default Gateways eingesetzt. Das Protokoll bietet dem Angreifer einige Möglichkeiten die IP-Infrastruktur, wie z. B. Server und Endgeräte, zu stören. RFC 3118 [RFC3118] beschreibt mit der DHCP-Authentifizierung (Identifiers für Clients und Server) eine allgemeine Lösung, um die Schwachstellen zu beheben; jedoch ist in den wenigsten Endsystemen dieser Standard implementiert. Daher müssen auf Layer 2 in den Switches Port die hier beschriebenen Security-Maßnahmen 3, 4, 5, 6 und 7, sowie weitere Maßnahmen wie z. B. DHCP Snooping und VLAN ACLs (Zugriffslisten in den Switches) ergriffen werden, um einen hinreichenden Schutz zu erzielen.

DHCP Starvation

Als Schutzmaßnahme gegen DHCP Starvation (to starve [engl.] = verhungern) bietet sich nur eine explizite Konfiguration aller Clients auf dem DHCP-Server an oder eine Limitierung der DHCP-Anfragen am Switch-Port. Ist das Limit überschritten, schaltet der Switch den Port ab. Einige Switch-Hersteller unterscheiden in ihren Switches zwischen vertrauenswürdigen und nicht vertrauenswürdigen Ports und erlauben nur auf den vertrauenswürdigen Ports DHCP-Verkehr (DHCP Snooping).

Rogue Server abwehren

Neuere Switches ermöglichen es, Port-basierende Zugriffslisten zur Abwehr von DHCP-Angriffen gegen Rogue Server einzusetzen. Man kann mit Zugriffslisten eine Zugriffkontrolle definieren. Eingehende Zugriffslisten filtern alle Pakete vom DHCP-Server zum Client, und mit ausgehenden Zugriffslisten werden alle Pakete vom DHCP-Client zum Server gefiltert.

[8] Maßnahmen gegen STP-Attacken

VLANs und Port Security (siehe Maßnahmen 1bis 9) schützen nur vor Man-in-the-Middle-Attacken, jedoch nicht vor STP-basierten DoS-Angriffen. Gegen diese Art von Angriffen bieten manche Switches weitere Schutzmaßnahmen an wie die Überwachung der Herkunft von Datenpaketen oder die Überwachung der Weiterleitung der Datenpakete.

[9] Anti Spoofing-Filter

Mit Anti-Spoofing-Filtern (ACL Access Listen) wird verhindert, dass ein externer Angreifer IP-Adressen aus dem inneren Netzwerk (Quelladressen) verwenden kann. Der ausgehende Datenverkehr ist ebenso auf gültige Quelladressen hin zu überprüfen, um DoS-Angriffe von innen zu unterbinden. Anti Spoofing-Filterregeln sollten immer allen anderen internen und externen Netzfilterregeln vorangestellt werden.

[10] Maßnahmen gegen VLAN-Angriffe

Native Tunnel gegen VLAN Hopping

Bei VLAN Hopping werden zweifach markierte Ethernet-Frames von einem Switch zu einem anderen Switch in ein anderes VLAN geleitet. *VLAN Hopping* lässt sich unterbinden, indem man ein unabhängiges *Native* VLAN als Tunnelverbindung zwischen den VLANs konfiguriert. Dadurch, dass die *Native* VLAN-Tunnel-ID keine Übereinstimmung mit dem VLAN-ID des Switch-Ports hat, wird das Paket des Angreifers unverändert (d.h. der Header wird nicht entfernt) über die Trunkverbindung weitergeben und kann somit nicht an das Zielsystem gelangen.

Untersuchung der Ethernet-Frames mit VLAN ACLs in Switches

Mit VACLs *(VLAN Access-Listen)* kann in modernen Switches der gesamte Datenfluss innerhalb (Host-zu-Host) des VLANs, sowie von und zu einem VLAN kontrolliert werden. Ein Ethernet-Frame wird dabei bis zur Ebene Layer 3 untersucht. Die Überprüfung der Ethernet-Frames erfolgt hierbei bereits auf Layer 2, wenn das Paket zum ersten Mal am Switch-Port gesehen wird. VLAN-Angriffe können mit entsprechenden Filterregeln schon sehr früh abgefangen werden.

Untersuchung der Ethernet-Frames mit ACLs in Routern

Um Host-zu-Host-Verbindungen zu schützen, die sich im gleichen privaten VLAN (privaten VLAN = PVLAN) befinden, müssen auf dem Router am Promiscuous Port entsprechende ACLs konfiguriert werden. Mit den ACLs am Promiscuous Port kann der Intra-Subnetz-Verkehr geregelt werden. Es lassen sich damit Regeln gegen VLAN Hopping definieren.

Port-basierende ACLs auf dem Promiscous Port der Switches

VLAN-Zugriffslisten (ACLs) beziehen sich immer auf das gesamte VLAN. Möchte man nur einzelne Ports kontrollieren, so gibt es die Möglichkeit Port-basierende Zugriffsregeln zu definieren. Es können unterschiedliche Regeln definiert werden (z. B. Zugriffsregeln bezogen auf die Quelladresse; Zugriffsregeln mit der Angabe von Quell-, Ziel- und Protokolladresse; MAC-Zugriffsregeln mit Quell- und Zieladresse und Protokolltyp).

[11] Struktur von LANs und Zugang der VLANs

Durch eine Aufteilung des Netzwerks in mehrere Broadcast-Domänen (VLANs) für die unterschiedlichen Aufgaben können die meisten Layer 2-Angriffe verhindert werden. Innerhalb der VLANs gibt es zunächst keinen erhöhten Schutz vor Angriffen wie sie in Kapitel 4.4.1 beschrieben werden. Eine weitergehende Strukturierung der VLANs nach den Aufgaben der Systeme innerhalb des VLANs (PC, Workstations, Telefone, Server) führt zu der Unterteilung in ein „producing VLAN“, in dem sich alle Server befinden, und in ein „consuming VLAN“, in dem alle PCs und Workstations untergebracht werden. Die Weiterleitung zwischen den einzelnen VLANs übernimmt dann ein Router oder eine Firewall. Die Zugriffslisten in dem Router bzw. der Firewall legen die Verkehrsbeziehungen von Server-VLAN und Client-VLAN innerhalb der Arbeitsgruppe fest. Layer 2-Angriffe können dann nur noch innerhalb des jeweiligen VLANs verübt werden.

Moderne Switches haben die Fähigkeit, Zugriffslisten auf VLAN-Ebene zu definieren, mit denen der Datenfluss bis in die Layer 3-Ebene innerhalb und zwischen den Broadcast-Domänen kontrolliert werden kann. Lässt sich eine Trennung von Sprach- und Datennetzen nicht realisieren, können durch VLAN-Zugriffslisten viele Angriffe auf die VoIP-Systemkomponenten verhindert bzw. abgewehrt werden.

[12] Netzzugang aus dem öffentlichen Netz ins LAN

Netzzugänge in lokale LANs aus öffentlichen Netzen sollten einem strengen Regelwerk unterzogen werden. VPN-Verbindungen mit einer Authentifizierung und Verschlüsselung sind die Voraussetzung eines gesicherten Zugangs. Darüber hinaus sollten für jeden Zugang eigene Regeln (Firewall) definiert werden, in denen genau festgelegt wird, mit welchen Diensten und zu welchen Servern ein Kontakt hergestellt werden darf. Die Verbindungen sollten generell mitgeloggt werden (syslog), um Aufschluss über die Aktivitäten zu erlangen.

Layer 3-Angriffe

[13] Maßnahmen gegen IP Spoofing

Bei Spoofing-Angriffen verwendet der Angreifer vertrauenswürdige Quelladressen, um Zugrifflisten in Routern, Firewalls oder in Switches zu umgehen. Zur Überwachung sowohl des externen als auch des internen Datenverkehrs auf gültige Quelladressen eignen sich Anti Spoofing-Filter in den Routern. Switch-basierende ACLs eignen sich, um den lokalen Datenverkehr auf gültige Quelladressen zu prüfen. Da die Regeln schnell sehr groß und unübersichtlich werden, empfiehlt es sich, diese auf dem LAN-Routerinterface zu definieren.

[14] Maßnahmen gegen ICMP Redirect

ICMP Redirect wird normalerweise vom Router dazu benutzt, um die Endsysteme über eine bessere Route zu informieren. Daraus leiten sich verschiedene Angriffe (Kapitel 4.4.1) ab. Durch Abschaltung der Verarbeitung von Redirect-Nachrichten auf den Zielsystemen (Gateway, Netzwerkservern und Endsystemen) kann der Angriff abgewehrt werden. Mit ICMP Redirect-Filtern in den Routern kann ebenso ein wirksamer Schutz aufgebaut werden. Eine weitere Möglichkeit ist die Verwendung von privaten VLANs, um den direkten Verkehr zwischen den Systemen zu unterbinden. Der Router übernimmt das Routing zwischen den Systemen und definiert mit Zugrifflisten den Verkehr untereinander.

[15] Maßnahmen gegen IRDP Spoofing

IRDP (ICMP Router Discovery Protocol, RFC 1256 [RFC1256]) sollte man nicht in einem Netzwerk einsetzen. Weil keine Authentifizierung der Pakete durchgeführt wird, kann der Angreifer problemlos die Gateway-Adressen auf allen Systemen verändern. IRDP-basierende Angriffe zwischen den Hosts lassen sich durch private VLANs mit Zugriffsfiltern (ICMP-Typ 9 auf Layer 3) auf dem Routerinterface verhindern.

[16] Maßnahmen gegen Route Injection

Um das Einschleusen von falschen Routing-Paketen zu unterbinden, dürfen keine Protokollinformationen (z. B. RIP2 oder OSPF) von Endsystemen bzw. hierfür nicht autorisierten Routern in das Netzwerk gelangen. Route Injection kann mit Zugriffslisten, die die Quell- und Zieladressen von Routingprotokollnachrichten prüfen bzw. filtern, sowie durch Passwörter bzw. Hashes geschützte Nachbarschaftsbeziehungen zwischen den Routern abgewehrt werden können. Es empfiehlt sich, Zugriffslisten auf allen Ports bzw. Netzübergängen zu konfigurieren, über die keine Routingprotokollnachrichten gesendet werden dürfen.

[17] Maßnahmen gegen HSRP- und VRRP-Angriffe

Eine einfache Möglichkeit, sich gegen HSRP- und VRRP-Angriffe zu wehren, ist der Gebrauch von ACL-Listen auf den Routern, d.h. die Router nehmen nur noch Pakete von vorher festgelegten Adressen an. Eine weitere Maßnahme ist die Authentisierung der HSRP- oder VRRP–Pakete, um gefälschte Pakete zu erkennen. VRRP-Angriffen begegnet man am besten durch eine feste IP-Adressenzuordnung von Master- zu Backup-Router. Entfernte HSRP-Angriffe können mit

entsprechenden Anti Spoofing-Filtern abgewehrt werden. VACLs in Switches ermöglichen bei diesen prinzipiell den gleichen Schutz wie auf den Routern. Zum Schutz gegen Angriffe kann man auf den Switches private VLANs oder VLAN ACLs verwenden, und mit entsprechenden Kontrolllisten lassen sich HSRP- oder VRRP-Angriffe abwehren.

[18] Maßnahmen gegen DHCP Starvation und DHCP Rogue Server

Die Maßnahmen werden unter Layer 2 in Paragraph [6] in diesem Abschnitt beschrieben.

[19] Maßnahmen gegen Ping Flood, SYN Flood und LAND Flood

Durch Massenanfragen werden Schwachstellen im IP-Stack ausgenutzt, oder das Betriebssystem wird damit beschäftigt, diese Anfragen zu beantworten. Zu solchen Attacken zählen:

IP-Fragmentangriff (teardrop, newtear, bonk)

IP-Bombing (DDOS-Attacke)

SYN Flood-Attacken (massenhafte Verbindungsanfragen)

Mit Paketfilter-Systemen (Firewall) lassen sich die Schwachstellen nur bedingt beseitigen, da diese selbst Opfer eines solchen Angriffes sein können; es sei denn, sie besitzen ein IDS-System und erkennen die Attacken und verwerfen die Angriffe schon am Porteingang.

Redundante Netzkomponenten und Server

Zu den wichtigsten Konzepten der Absicherung gegen den Ausfall von Hardware gehören Redundanz-Konzepte. Eine der herkömmlichen Telefonie gleichende Verfügbarkeit des Voice over IP-Dienstes ist nur durch den Aufbau von redundanten Strukturen möglich. Bei den zentralen Servern und Diensten ist darauf zu achten, dass diese nach dem Hot-Standby-Prinzip realisiert sind. Je nach Aufgaben unterscheiden sich die Anforderungen an die Umschaltzeiten der Systeme. Gemeinsam ist allen Systemen die Anforderung, den Betrieb ohne aktives Eingreifen von Administratoren zu übernehmen. Nachfolgend werden einzelne Komponenten einer VoIP-Umgebung in der Reihenfolge steigender Anforderungen an die Geschwindigkeit der Umschaltung beim Ausfall einer Komponente aufgelistet.

DHCP-Server, TFTP-Server, FTP-Server. Die Telefone erneuern ihre Konfiguration in der Regel einmal in 3-6 Stunden bzw. beim Bootvorgang. Fällt ein DHCP-Server aus, so kann ein neues Telefon seine Konfiguration nicht bekommen. Wird die Konfiguration vom Endgerät lediglich erneuert, so wird beim Ausbleiben einer Antwort vom DHCP-Server die aktuelle Konfiguration nicht sofort gelöscht, sondern es wird wiederholt versucht, den Service zu erreichen. Somit sind bei diesen Services Ausfälle bis in den Minuten-Bereich nicht kritisch.

Registrars oder Gatekeeper - in proprietären Lösungen auch als Call Manager bezeichnet - verwalten die Telefonie-Teilnehmer und überprüfen die Berechtigungen der Nutzer zum jeweiligen Anruf. Das wichtigste Feature ist eine verteilte Datenbank der Nutzer mit ihren Zuständen. Die Konsistenz des Datenbestands ist hierbei kritischer als eine schnelle Umschaltung auf den Backup-Server. In der Zeit der Umschaltung sind lediglich keine Anfragen an diese Server und somit keine neuen Anrufe möglich. Bestehende Sprachverbindungen bleiben aber erhalten, da die Medienströme direkt zwischen den Endgeräten ausgetauscht werden. Umschaltzeiten im Bereich von Sekunden sind akzeptabel.

Provisioning-Server. Häufig werden für die Gebührenabrechnung ein oder mehrere separate Server bereitgestellt. Diese werden dann als Provisioning-Server bezeichnet. Die Anforderungen an die Umschaltzeiten sind hier vergleichbar mit denen an die Registrars, so lange die Datenkonsistenz erhalten bleibt. Häufig werden Verluste von einigen wenigen Call Detail Records toleriert.

Firewall. Häufig werden nicht nur die Signalisierungsströme, sondern auch Medienströme durch die Firewall geleitet, um Attacken auf die Server und Endgeräte zu erkennen und zu verhindern. Folglich muss die Umschaltung zwischen Firewalls so schnell erfolgen, dass

bestehende Sprachverbindungen nicht unterbrochen werden. Es wird somit eine Umschaltzeit im Bereich von unter einer Sekunde benötigt.

Switches und Router. Aus Kostengründen werden nur die zentralen Komponenten redundant an das IP-Netz angebunden. Dabei gibt es zwei Strategien der Anbindung. Diese sind in Abbildung 4.2 und Abbildung 4.3 dargestellt. Im ersten Fall werden keine speziellen Vorkehrungen für die Umschaltung zwischen den Switches benötigt. Im zweiten Fall kann Spanning Tree oder Fast Spanning Tree zur Umschaltung im Störungsfall eingesetzt werden. Hierbei sind die Anforderungen hinsichtlich der Umschaltzeiten dieselben wie bei den Firewalls, da hier ebenfalls bestehende Gespräche nicht unterbrochen werden dürfen. Ein häufig gemachter Fehler besteht darin, dass die redundanten Stränge von den Servern bzw. Gateways im Netz auf einem einzelnen Switch zusammenlaufen, wodurch dieser einen Single Point of Failure darstellt (siehe Abbildungen unten).

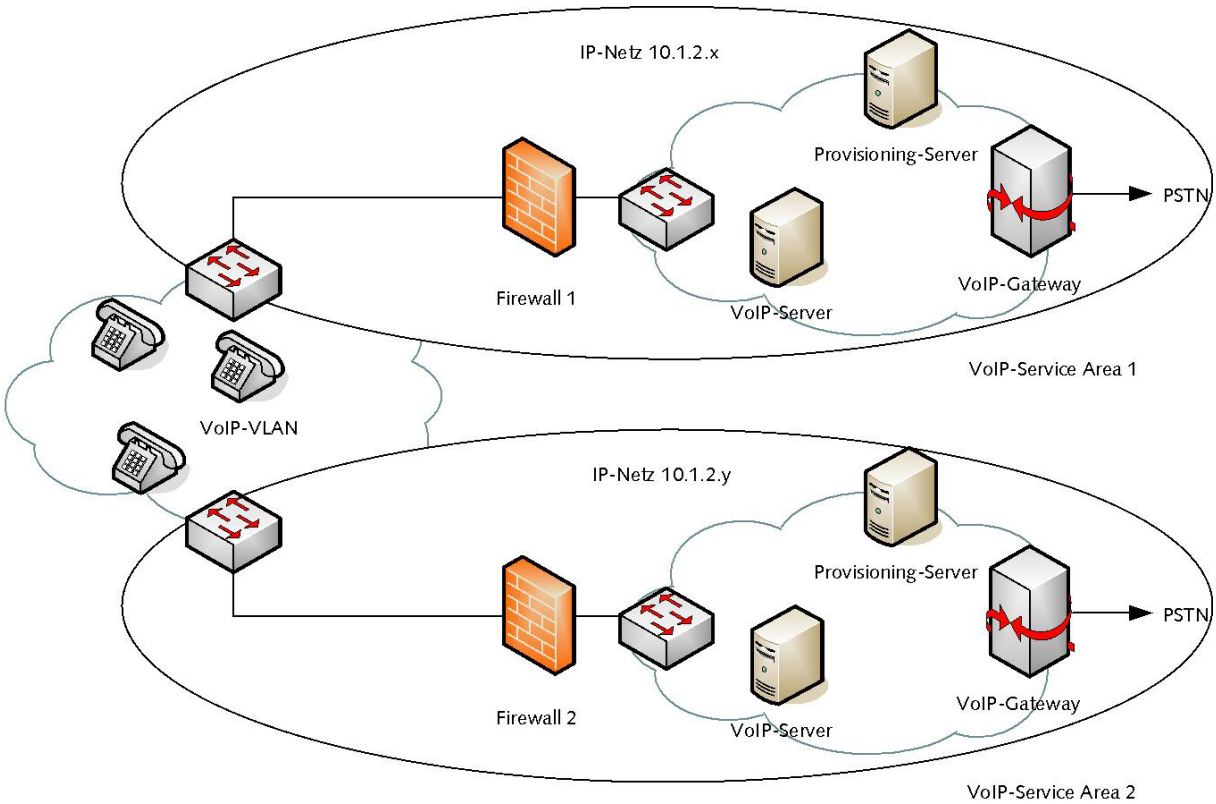

Abbildung 4.2 Redundanzbeispiel durch zwei getrennte Service-Areas

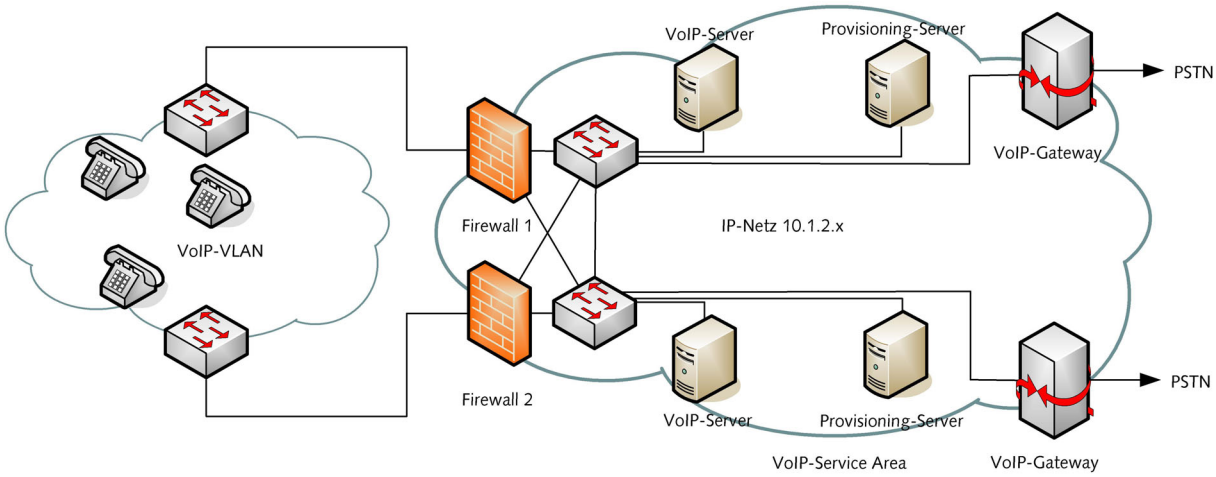

Abbildung 4.3 Redundanzbeispiel mit einer Service-Area und Spanning Tree

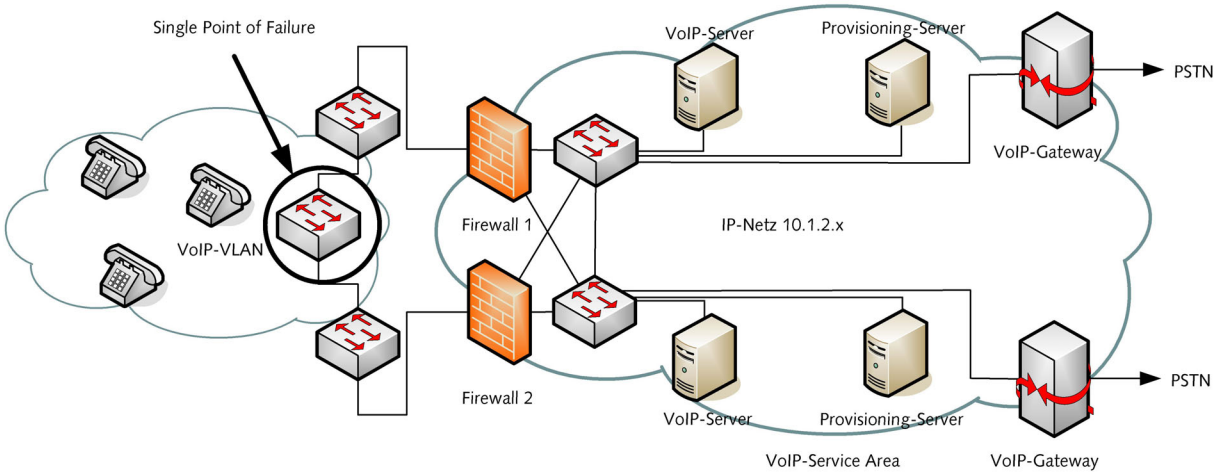

Abbildung 4.4 Beispiel für ein fehlerhaftes Redundanzkonzept

VoIP-Gateway. Jedes VoIP-Gateway ist an einen ISDN-Anschluss eines öffentlichen oder privaten Telefonie-Providers angeschlossen. Durch den Anschluss einer VoIP-Installation über mehrere Gateways wird das Aufrechterhalten einer Kopplung zum ISDN-Netz nicht nur beim Ausfall eines Gateways, sondern auch beim Ausfall einer ISDN-Strecke bzw. einer ISDN-Baugruppe sichergestellt. Da bei ISDN keinerlei Mechanismen zur Übernahme einer bestehenden ISDN-Verbindung auf einen anderen Anschluss vorgesehen sind, ist hier eine Hot-Standby-Realisierung nicht möglich. Vielmehr wird in den zentralen Komponenten – Gatekeeper, SIP-Proxy oder Call Manager - eine Präferenz der Auswahl eines bestimmten Gateways festgelegt. Beim Ausfall eines VoIP-Gateways oder einer Baugruppe werden alle bestehenden ISDN-Verbindungen unterbrochen. Aus diesem Grund ist es ratsam, nicht nur den Überlaufverkehr auf einen weiteren Gateway zu leiten, sondern eine gleichmäßige Lastverteilung über alle verfügbaren Gateways zu realisieren.

4.2.1 Dienstgüte und Netzmanagement

Das Netzmanagement bildet ein wichtiges Glied in der Kette der Sicherung eines VoIP-Dienstes. Neben den Aspekten des Schutzes vor Angriffen beeinflussen geeignete Maßnahmen des Netzmanagements im Wesentlichen die Verfügbarkeit und die Güte des Dienstes.

DiffServ sowie Class-of-Service nach IEEE 802.1p

Ein wichtiger Ansatz für die Sicherstellung der Dienstgüte in IP-Netzen sind die so genannten Differentiated Services (DiffServ). Eine komplette CoS-Architektur für DiffServ-Netze wird in RFC 2475 [RFC2475] vorgestellt. Beim DiffServ-Ansatz werden einzelne Datenströme nach ihren Anforderungen an die Dienstgüte klassifiziert. Einzelnen Klassen werden bestimmte Werte des TOS-Feldes im IP-Header zugeordnet [RFC2474]. Entsprechend dem Wert des TOS-Feldes wird das Datenpaket in den Netzknoten priorisiert behandelt.

Damit die benötigte Dienstgüte in der Sicherungsschicht sichergestellt werden kann, wird die Markierung gemäß DiffServ auf ein Class of Service-Feld (CoS) im Ethernet-Rahmen abgebildet. Die Verwendung der Class of Service-Bits ist im IEEE-Standard 802.1p [IEEE98] festgelegt.

Zu den wesentlichen Maßnahmen in Verbindung mit DiffServ sowie CoS gehört die Sicherstellung, dass keine Datenpakete unberechtigt mit einer hohen Priorität markiert werden, sowie dass Datenströme mit markierten Datenpaketen die zugelassenen Verkehrscharakteristiken nicht überschreiten. Dies kann nur durch ein lückenloses QoS-Management z. B. nach RFC 2475 erreicht werden. Dabei gehört zum QoS-Management vor allem das Policing – die Überprüfung der Berechtigungen zur Allokation von bevorzugten Ressourcen und der Übereinstimmung der gesendeten und vereinbarten Verkehrsprofile.

Unterstützen die VoIP-Netze das Modell der Differentiated Services, so muss dies lückenlos, z. B. nach RFC 2475 [RFC2475], implementiert werden. Fehlt beispielsweise das Policing im DiffServ-Netz, können datenhungrige Anwendungen ihre Datenpakete mit hoher Priorität markieren, wodurch die Sprachströme massive Paketverluste erfahren und Sprachverbindungen nicht mehr möglich sind. Speziell Peer-to-Peer-Anwendungen versuchen häufig, die Datenströme mit einer hohen Priorität in das Netz zu injizieren.

Voice over IP-Dienste sind in einem DiffServ-Netzwerk aber nicht nur durch mutwillige Eingriffe gefährdet. Eine falsche Dimensionierung der Netzkomponenten kann zur punktuellen Überlastung von Verbindungen oder Netzwerk-Ressourcen (Prozessoren der Router, Firewalls) führen und damit ebenfalls den Dienst zum Erliegen bringen

Overprovisioning

Häufig wird beim Einsatz von IP-Telefonie keine unterschiedliche Behandlung der Datenströme je nach Markierung vorgenommen. Es wird davon ausgegangen, dass moderne lokale Netze sowie WANs ausreichend überdimensioniert sind, um Stauungen in Warteschlangen zu vermeiden. Eine solche QoS-Policy wird als Overprovisioning bezeichnet. Im Fall von Overprovisioning ist ein permanentes Monitoring potentieller Engpässe im Netz notwendig. Dabei bildet nicht zwangsläufig die Datenrate einer Strecke den Flaschenhals einer Verbindung. Es kann genauso die CPU-Performance eines Routers, die Backplane eines Switches oder die Durchsatzrate einer Firewall sein. Eine systematische Untersuchung der notwendigen Überdimensionierung der Netze ist zurzeit nicht bekannt. Empirische Untersuchungen im Breitband-Wissenschaftsnetz des DFN vor einigen Jahren haben einen Faktor 4 bis 6 zwischen den 5-Minuten-Mittelwerten des Durchsatzes und der vollen Link-Datenrate als akzeptablen Richtwert für die Überdimensionierung für multimediale Anwendungen ergeben [Lix98]. Des Weiteren zeigen praktische Erfahrungen des Betriebs der Router und Switches an den Hochschulen, dass Paketverzögerungen und –verluste bei Prozessorlasten von 50-80 % rapide steigen. Folglich gehört auch die CPU-Auslastung aktiver Komponenten zum Monitoring des Netzes. Entscheidend ist ein lückenloses Monitoring der CPU-Last und der Auslastung einzelner Verbindungen in den Netzen sowie periodische Analysen beispielsweise mit Hilfe von aktiven Messungen der Einweg-Verzögerungen.

Bei der Verwendung des Overprovisioning muss beachtet werden, dass keine festen Garantien der Qualität von Sprachanwendungen gegeben werden können. Vielmehr bauen die Aussagen und Abschätzungen auf Erfahrungswerten aus der Vergangenheit. Das Verhalten der Netze kann sich durch Einführung neuer Anwendungen wie beispielsweise Videoconferencing oder Grid-Computing gänzlich ändern. Speziell beim Einsatz von Overprovisioning können VoIP-Anwendungen durch gezielte Injektion von Datenströmen in die Netze stark beeinträchtigt werden. Es ist also eine genaue Beobachtung der Auslastung einzelner Strecken und Netzkomponenten erforderlich.

MPLS

MPLS kann in Weitverkehrsnetzen verwendet werden, um Kanäle mit garantierter Bandbreite für Sprachverbindungen vom restlichen Verkehr zu isolieren. Damit kann das Prinzip des Overprovisioning auf einzelne MPLS-Tunnel angewendet werden. Da VoIP-Verkehr eine geringere Burstiness als sonstiger IP-Verkehr hat, ist davon auszugehen, dass VoIP-Tunnel stärker gefüllt werden können als Strecken, auf denen VoIP-Verkehr mit dem restlichen Datenverkehr übertragen wird.

Es ist zu beachten, dass MPLS lediglich Vorteile hinsichtlich der Dienstgüte, aber nicht hinsichtlich der Sicherheit der Datenübertragung bringen kann. Die Datenpakete der MPLS-Tunnel werden ähnlich einem VLAN-Tagging mit einem zusätzlichen Header versehen und unverschlüsselt mit dem restlichen Verkehr übertragen. Somit können solche Tunnel ähnlich wie Ethernet-Verkehr mit einem geeigneten Sniffer abgehört und manipuliert werden.

Traffic Shaping

Traffic Shaping wird in Gateways zwischen lokalen und Fernverkehrsnetzen eingesetzt, um die Datenrate bestimmter, in der Regel unerwünschter, Verkehrsarten zu drosseln. Besonders häufig wird Traffic Shaping von Peer-to-Peer-Anwendungen auf Datenströme mit Transportadressen angewendet. Die Erfahrungen aus dem Netzbetrieb der Hochschulrechenzentren zeigen aber, dass solche Maßnahmen schnell umgangen werden können, indem z. B. andere Port-Adressen verwendet werden. Traffic Shaping gehört somit zu den Maßnahmen eines Quality of Service-Konzepts und hat nur eine geringe Sicherheitsrelevanz.

Resource Reservation Protocol (RSVP)

Das Resource Reservation Protocol (RSVP) ist in RFC 2205 [RFC2205] spezifiziert und dient einer Ende-zu-Ende-Signalisierung der Dienstgüte für einzelne Datenströme. Ursprünglich wurde RSVP für die Realisierung von so genannten Integrated Services (IntServ) in IP-Netzen konzipiert [RFC1633], das im Gegensatz zu Diffserv eine „echte“ QoS-Dienstgüte garantieren kann. Für den Einsatz von RSVP in der ursprünglichen Form müssen alle Vermittlungsknoten, Betriebssysteme sowie Anwendungen das Protokoll beherrschen. Zurzeit ist sowohl die Unterstützung in den Betriebssystemen als auch in den Anwendungen mangelhaft oder gar nicht gegeben. Somit muss RSVP, sowie das Integrated Services QoS-Modell, in Verbindung mit Voice over IP nicht weiter betrachtet werden.

Ein mögliches weiteres Einsatzszenario für RSVP ist das Management von MPLS-Verbindungen – das so genannte Traffic Engineering (MPLS-TE) [RFC3209]. Das Protokoll findet aber zurzeit ebenfalls kaum Anwendung bei Netzbetreibern. Außerdem werden bei Verwendung des MPLS-TE die RSVP-Nachrichten nicht Ende-zu-Ende, sondern nur zwischen MPLS-Routern ausgetauscht. Damit ist eine Manipulation der Nachrichten seitens der Endsysteme nicht möglich. Folglich ist auch im Zusammenhang mit MPLS die Betrachtung des RSVP aus Security-Gesichtspunkten nicht erforderlich.

Störungsmanagement und Eskalationsprozesse

Des Weiteren gehört zu den unentbehrlichen Management-Maßnahmen bei einem Betrieb von Voice over IP eine lückenlose Dokumentation der Konfiguration von Netzkomponenten, sowie die Definition von Eskalationsprozessen im Störungsfall, damit ein Ausfall bestimmter Netzbereiche in einer vertretbaren Zeit behoben wird.

Zu den Eskalationsprozessen gehört die Absicherung der VoIP- sowie Netzwerk-Dienste durch Unterstützungs- und Wartungsverträge. Zu solchen Verträgen können an dieser Stelle keine pauschalen Aussagen getroffen werden. Die Ausgestaltung solcher Verträge hängt von der Anzahl und dem Ausbildungsstand des beim Netzbetreiber und der VoIP-Umgebung verfügbaren Personals ab. Die Ausfallzeit des Dienstes infolge von Hardwareausfällen kann durch Garantieverlängerungen mit Hardwareaustausch oder aber durch das Vorhalten identischer Hardware als Notreserve abgedämpft

werden. Speziell für zentrale Server sind schnelle Reaktionszeiten bei Hardwareausfällen sowie bei Support-Leistungen zu vereinbaren.

Security Management

Zu einem reibungslosen Betrieb eines VoIP-Systems gehört ein ganzheitliches Security Management-Konzept. Dieses beschreibt den Katalog an Maßnahmen, die zur Absicherung des Netzes sowie des Dienstes gegen Angriffe von Dritten getroffen werden sollen. Außerdem beinhaltet ein solches Konzept die personellen Zuständigkeiten für einzelne Security-Maßnahmen wie die Verwaltung von Passwörtern der Netzkomponenten sowie der Server-Systeme, Vertretungspläne und die Zuständigkeiten für die Überprüfung der Einhaltung der Security Policies. Die Zugriffskontrollen sowie Filterung im Netz dürfen nur an definierten und dokumentierten Stellen im Netz erfolgen, damit im Störungsfall eine schnelle Fehlerlokalisierung möglich wird. Durch die Dokumentation der Maßnahmen zur Einschränkung des Verkehrs wird sichergestellt, dass mögliche Fehlerursachen auch bei Personalausfall oder bei Bedarf der Störungsbeseitigung durch Dritte nachvollzogen werden können.

4.2.2 Aspekte im Zusammenhang mit Protokollen

Maßnahmen gegen Störungen der Anwendung (DoS) und der Basisdienste

Durch die Störung des Netzes oder der Basisdienste der Netze kann zum einen die wahrgenommene Qualität der Anwendung VoIP beeinträchtigt werden, zum anderem eine oder mehrere Komponenten der Anwendung so kompromittiert werden, dass die Datenströme zum Angreifer umgeleitet werden.

Die Maßnahmen zum Schutz der Anwendungen sind vielschichtig. Zum einen ist eine große Sorgfalt bei dem Betrieb der Router und Switches zu tragen, damit diese nicht kompromittiert werden. Zum anderen sind die Rechner, auf denen die Basisdienste laufen, gegen Missbrauch zu schützen. Außerdem sind die Endgeräte – Hard- und Softphones - gegen Kompromittierung und Angriffe zu schützen.

Zu den Sicherheitsmaßnahmen auf Netzwerkschicht gehören in erster Linie die in Kapitel 4.2.1 behandelten Aspekte des Netzdesigns Eine der wichtigsten Maßnahmen ist hierbei das systematische Einspielen neuer Sicherheits-Patches für das verwendete Betriebssystem der Netzkomponenten und der Rechner, welche die Basisdienste hosten. Diese Maßnahme betrifft ebenso die IP-Telefone. Einige Hersteller verwerfen zum Beispiel zu häufig ankommende Ping-Nachrichten und bewahren somit, dass das Telefon vor einem PING Flooding.

Zur Absicherung der Betriebssysteme für die Basisdienste gehört die Abschaltung aller nicht zwingend erforderlichen Dienste. Ein Fernzugriff für die Konfiguration der Netzkomponenten und der Server hat ausschließlich verschlüsselt zu erfolgen. So soll SSH statt Telnet und FTP verwendet werden; ebenso sollen Web-Konfigurationen über das Protokoll HTTPS erfolgen, damit die Passwörter für die Administration nicht abgehört werden sowie die Datenströme nicht manipuliert werden können. Leider gibt es eine Vielzahl von VoIP-Systemen auf dem Markt, welche keinen verschlüsselten Remote-Zugang zu Administrationszwecken bieten. Folglich ist auf die Möglichkeit der Administration über verschlüsselte Kanäle schon bei der Produktauswahl zu achten.
Die Gefahr von DHCP Starvation und DHCP Rogue auf Server und Endsysteme kann z. B. durch die Implementierung eines geeigneten Netzdesigns reduziert werden. So sollte die Broadcast-Domäne ausschließlich auf die Ports beschränkt werden, an welchen die IP-Telefone angeschlossen sind. Mit der Bildung von VLANs wird ein Ethernet-Port für die IP-Telefone und ein natives VLAN für die angeschlossenen PCs realisiert. Werden verdächtige DHCP-Nachrichten oder IP-Pakete mit einer falschen Absenderadresse auf einem Port festgestellt, so kann dieser gesperrt werden, oder es wird eine Meldung an den Systemadministrator gegeben.

Aspekte einer statischen oder dynamischen Einschränkung des IP-Verkehrs in bestimmten Teilbereichen des Netzes werden im Kapitel 5.1 behandelt.

Maßnahmen gegen das Abhören und die Manipulation von Medienströmen

Die Sprachdaten werden in RTP-Protokollrahmen verpackt und diese wiederum über UDP übertragen. In Kapitel 3.3.1 (Paragraph über RTP) wurde bereits dargestellt, dass Medienströme direkt dekodiert und mit geringem Aufwand ausgegeben werden können – vorausgesetzt man bekommt Zugang zu den Datenpaketen der Medienströme. Die einzige effektive Maßnahme gegen das Dekodieren der Medienströme ist eine Verschlüsselung der Daten. Die Verschlüsselung kann wahlweise durch Schaltung von Tunneln oder durch die Verschlüsselung der RTP-Datenströme erfolgen.

Die Schaltung von Tunneln – z. B. mit IPSec oder PPTP - hat den Vorteil, dass diese zwischen zwei Netzen statisch oder dynamisch aufgebaut werden und damit sowohl die Sprachdaten als auch Signalisierungsdaten verschlüsselt übertragen werden. Zu beachten ist, dass in der Vergangenheit einige Schwachstellen zum PPTP bekannt geworden sind. Folglich soll möglichst IPSec-Tunneln der Vorzug gegeben werden.

Des Weiteren ist zu beachten, dass VPN-Tunnel lediglich zur Verbindung zwischen Netzen bzw. zur Anbindung von mobilen Teilnehmern an ihr Heimatnetz eingesetzt werden. Somit bleibt die Kommunikation innerhalb des LAN unverschlüsselt.

Mit SRTP steht ein Verschlüsselungsmechanismus zur Verfügung, welcher lediglich für die Verschlüsselung der Sprachinformationen verwendet wird. SRTP muss von den beteiligten Endgeräten unterstützt werden. Zu den Vorteilen der Verwendung von SRTP gehört die Möglichkeit zur Verschlüsselung innerhalb von LANs sowie ein deutlich geringerer Protokoll-Overhead der Protokoll-Header als bei IPSec. Die Unterstützung des SRTP muss von jedem an der Kommunikation beteiligten Endgerät gegeben sein.

Die Daten im SRTP werden mit einem symmetrischen Schlüssel verschlüsselt. Somit muss am Anfang einer verschlüsselten Sprachübertragung ein Schlüsselaustausch erfolgen. Dies erfolgt in der Regel während des Verbindungsaufbaus im Signalisierungsprotokoll. Die Protokolle H.323, SIP und SCCP unterstützen bereits Methoden zum Schlüsselaustausch für SRTP.

Maßnahmen gegen Manipulation der Signalisierung und Gebührenbetrug

Weitaus wichtiger als die Verschlüsselung der Medienströme ist die Verschlüsselung oder die Sicherstellung der Integrität der Signalisierungsströme. Eine Möglichkeit hierfür ist wieder die Schaltung von verschlüsselten VPN-Kanälen. Auf die Vor- und Nachteile dieses Verfahrens treffen die bei der Betrachtung der Medienströme gemachten Aussagen zu. Für die Protokolle MGCP und MEGACO ist dies die einzige Möglichkeit einer verschlüsselten Kommunikation.

Der Standard H.235 sieht die Möglichkeit zur Integritätsüberprüfung sowie der Verschlüsselung der Signalisierung nach H.323 vor. Ebenso wie bei den Medienströmen müssen alle beteiligten Endsysteme die Kommunikation nach H.235 unterstützen. Ein kritischer Punkt bleibt noch die Schlüsselverwaltung für die gesicherte Kommunikation. Hier wird in der Regel auf X509-Zertifikate zurückgegriffen.

Wird die Kommunikation nach H.235 von den VoIP-Gateways nicht unterstützt, so ist dringend zu empfehlen den Zugriff auf das Gateway auf Basis von IP-Adressen und H.323-Identitäten so weit wie möglich einzuschränken. Dafür empfiehlt sich der Einsatz eines Gatekeepers und die Einschränkung des Zugriffs auf das VoIP-Gateway nur im Gatekeeper-routed Mode. Dadurch kann die Anzahl potentieller Angreifer auf das Gateway stark reduziert werden.

Das Session Initiation Protocol sieht eine gesicherte Übertragung der Passwörter zur Authentifizierung vor. Darüber hinaus können einige wenige Header-Felder gegen Veränderungen geschützt werden. Im Allgemeinen wird aber der Header einer SIP-Nachricht in jedem Proxy auf dem Weg vom Client zum Server verändert, wodurch ein gesamter Integritätstest der Nachricht nicht möglich ist. Prinzipiell ist die gesicherte Übertragung des Passwortes ausreichend, beispielsweise für eine Authentifizierung eines Endgerätes bei einem Registrar oder einem ISDN-Gateway. Es kann aber ein Identitätsbetrug in das ISDN-Netz begangen werden, weil die Absender-Kennung im Protokoll weiterhin frei manipulierbar ist.

Für eine gesicherte Datenübertragung im SIP hat sich die Verwendung von TLS etabliert. Damit wird die gesamte Signalisierung zwischen einzelnen SIP-Instanzen verschlüsselt. Dafür müssen SIP-Systeme eine Signalisierung über TCP und TLS unterstützen, obwohl der Standard eine Kommunikation über UDP präferiert. Bei Verwendung von TLS wird zwischen jeweils zwei SIP-Instanzen auf dem Weg zwischen dem Client und Server eine TCP/TLS-Verbindung aufgebaut. Voraussetzung für eine derartige Kommunikation ist das Vertrauen der Nutzer in die Betreiber von SIP-Proxies.

4.2.3 Firewalls und NIDS

Anforderungen an eine Firewall in einer VoIP-Systemumgebung

Grundsätzlich sollte der Sicherheit von VoIP–Systemkomponenten mindestens genauso viel Aufmerksamkeit geschenkt werden wie es bereits bei Serversystemen in Datennetzen der Fall ist. Der Anforderungskatalog ist, bedingt durch die Verzahnung der Systeme (VoIP-Server, VoIP-Gateway, VoIP-Telefone, Softphones, UMS–Server, CTI-Systeme) sowie protokollspezifischer Gegebenheiten, bei weitem größer und komplexer als im reinen Datennetz. Oftmals ist die strikte Trennung von Sprach- und Datennetzen gar nicht möglich, da beispielsweise Softphones von Arbeitsplatzrechnern aus dem Datennetz auf den VoIP-Server im Sprachnetz zugreifen, Groupware-Clients das direkte Wählen von Rufnummern gespeicherter Kontakte aus der Applikation ermöglichen oder VoIP–Server mit Verzeichnisdiensten (LDAP, ADS) gekoppelt werden. Hinzu kommt die Vernetzung von geografisch getrennten Unternehmens- bzw. Organisationsniederlassungen, die beispielsweise einen zentralen VoIP-Server für die unternehmensweite Kommunikation verwenden und gleichzeitig diese Verbindung für den Austausch von Daten nutzen.

Eine Firewall soll ein internes, sicheres System vor unberechtigten Zugriffen aus einem unsicheren Netz schützen und gleichzeitig berechtigte Zugriffe zu den geschützten Bereichen zulassen. Was als sicheres bzw. unsicheres Netz gilt, welche Ressourcen schützenswert sind und wie sie zu schützen sind, wird in den Sicherheitsrichtlinien (Security Policy) einer Organisation festgelegt.

Den höchsten Schutzbedarf im Zusammenhang mit der IP-Telefonie haben die zentralen VoIP-Systemkomponenten, da deren Kompromittierung die gesamte Kommunikation eines Unternehmens bzw. einer Organisation betreffen. Zu den zentralen VoIP-Systemen sind in erster Linie VoIP-Server und VoIP-Gateways zu zählen.

Zugriffe auf VoIP-Systemkomponenten durch berechtigte Nutzer bzw. Administratoren sollten erst nach erfolgreicher zentraler Authentisierung möglich sein, wobei die Authentifizierungs-Instanz ihrerseits mit den schützenden Firewallsystemen verbunden ist. Die Firewallsysteme können dann für den spezifischen, berechtigen Zugriff dynamisch einen zeitlich begrenzten Zugriff auf die Systeme erlauben (Öffnen eines Ports für eine bestimmte Quell- und Ziel-IP- Adresse).

Werden Signalisierungs- und Sprachdaten über Firewallgrenzen hinaus geleitet, sollte eine so genannte VoIP-fähige Firewall verwendet werden, die in der Lage ist, die verwendeten Signalisierungsprotokolle mit dem gesamten Rufauf- und -abbau zu analysieren und die jeweiligen Zustände zu speichern. Anhand der Protokollanalyse (z. B. die zu verwendenden UDP-Ports für die mit RTP übertragenen Sprachdaten) werden die benötigten Ports für die Dauer der Kommunikation geöffnet.

Die Leistungsfähigkeit des eingesetzten Firewallsystems beeinflusst nicht nur den Schutz, sondern auch die Qualität der übertragenen Sprache. Durch die Verarbeitung vieler kleiner Datenpakete, wie sie bei VoIP üblich sind, wird die CPU einer Firewall stark belastet, was direkte Auswirkungen auf Delay und Jitter der übertragenen Sprachsignale haben kann. Eingebaute IDS-Mechanismen in der Firewall dürfen die große Anzahl an UDP-Paketen nicht fälschlicherweise als DoS-Attacken (UDP Flooding) interpretieren und dadurch die Kommunikation verhindern.

Die bereits üblichen Abwehrmechanismen zeitgemäßer Firewallsysteme gegen DoS-Attacken wie ICMP Flooding, SYN Flooding, Fragmentierungsangriffe und andere bösartige, auf manipulierten Paketen basierende, Angriffe gehören zu den Grundfunktionalitäten wie sie bereits in Firewalls bei

Datennetzen eingesetzt werden. Die Systeme erkennen solche Angriffe mit einem integrierten IDS-System und wehren sie durch Verwerfen der Pakete ab, wobei Schwellenwerte konfiguriert werden können, die je nach Netzgröße variieren. Beim Einsatz solcher Mechanismen ist zu beachten, dass gerade diese Automatismen, die eigentlich der Erhöhung der Sicherheit der Systeme dienen sollen, auch als Ansatzpunkt für neue DoS-Attacken dienen können.

Die NAT-Problematik stellt sich in der Regel bei Übergängen zwischen privaten und öffentlichen Netzen und wird im Abschnitt NAT (Kapitel 4.2.4) behandelt.

Die Auswahl des richtigen Systems hängt in der praktischen Umsetzung von verschiedenen Faktoren ab:

- Wie ist die Größe des Netzes? Hier kann zwischen den verschiedenen Größen von Unternehmen bzw. Organisationen wie SOHO, SMB und Enterprise unterschieden werden.
- Welche Systemkomponenten stehen zur Verfügung? Ermöglichen bestehende Switches eine VLAN – Trennung von Sprach- und Datennetzen? Unterstützen bestehende Router Zugriffslisten (ACLs) oder Firewallfunktionalitäten?
- Welche Firewallsysteme werden bereits im Datennetz eingesetzt?
- Ist nur eine auf das LAN begrenzte IP-Telefonie oder auch die Internet-Telefonie geplant?
- Wie umfassend sind die Kenntnisse des betreuenden IT-Personals?
- Welche VoIP-Systemkomponenten werden eingesetzt?
- Welcher Kompromiss kann zwischen einer idealen Lösung und einer praktikablen Lösung gefunden werden?
- Wie ist der finanzielle Rahmen, der für die Umsetzung der Sicherheitsziele zur Verfügung steht?

Paketfilter auf Layer 3 und Layer 4 (Stateless Packet Filter)

Einfache Paketfilter können auf Routern, Layer 3-Switches bzw. Firewalls zur Trennung von Daten- und Sprachnetz eingesetzt werden, wobei Ihre Filterfunktionalität gegenüber zustandsbasierenden Filtern bzw. Application Level Gateways deutlich eingeschränkt ist.

Zustandsbasierende Portfilter auf Layer 3 und Layer 4 (stateful packet inspection)

Zustandsbasierende Portfilter können die für eine Kommunikation benötigten Rückpakete dynamisch durchlassen und so ein erhöhtes Maß an Sicherheit für ein Netzwerk bereitstellen. Sie speichern Zustände einer Verbindung ab und können so Rückpakete, die zu einer bestehenden Verbindung gehören, durchlassen, ohne das dafür explizite Zugriffslisten konfiguriert werden müssen.

Wenn möglich, sollte eine zustandsbasierende Firewall einem einfachen Paketfilter vorgezogen werden. Ihr Einsatzgebiet ist ebenfalls die Trennung von Sprach- und Datennetzen.

Applicaion Level Gateway (ALG)

Ein Application Level Gateway kann im Gegensatz zu den vorgenannten Systemen nicht nur auf IP–Adressen und Ports, sondern auch auf der Applikationsebene filtern. Es handelt sich in der Regel um eingebettete Software, die so genannte Parser für ASN.1 (H.323 ist in ASN.1 kodiert), SIP, MGCP und SDP enthält, und die verschiedenen Zustände der Signalisierungsprotokolle zwischenspeichert und auf Grundlage eines Sitzungszustandes Ports dynamisch öffnet und schließt. Der Vorteil eines Application Level Gateway macht sich gerade bei der Übertragung von RTP-Paketen bemerkbar. Die für die RTP-Übertragung zu verwendenden UDP-Ports werden im Rahmen der Signalisierung (mittels SDP) zwischen den Endpunkten ausgetauscht. Diese Ports variieren in der Regel bei jedem neuen Gespräch und müssen von der Firewall freigegeben werden. Da das ALG den Austausch der Protokollnachrichten verfolgt, in denen die IP-Adressen und die zu verwendenden UDP-Ports vereinbart werden, kann es dynamisch Filter setzen, die den betreffenden RTP-Strom passieren lassen. Beim Einsatz von NAT werden IP-Pakete, die beispielsweise SIP-Nachrichten mit SDP-Informationen enthalten, ausgepackt und die SDP-Informationen (IP-Adresse, UDP-Port) neu gesetzt. Diese SIP-

Nachricht wird dann wieder in ein IP-Paket verpackt. Das ALG unterhält eine entsprechende Tabelle, um in den eingehenden RTP-Paketen die Ziel-IP-Adresse und den Zielport umzuschreiben. Vergleicht man zustandslose, zustandsorientierte und ALG–Firewalls miteinander, so empfiehlt es sich aufgrund der Vorteile möglichst ein ALG einzusetzen. Um eingehenden RTP–Verkehr zu ermöglichen, müssen zustandslose und zustandsorientierte Firewalls große UDP-Portbereiche (z. B. von 16384 – 32767) dauerhaft öffnen, damit RTP-Pakete mit Sprachdaten durchgelassen werden können. Solche Konfigurationen stellen ein erhebliches Sicherheitsrisiko dar, da sie eine große Angriffsfläche für DoS- (UDP Flooding) und andere Attacken bieten. Applicaton Level Gateways hingegen öffnen nur die tatsächlich benötigten UDP-Ports für die Dauer der Kommunikation und bieten daher weniger potentielle Angriffsmöglichkeiten.

Überblick der verschiedenen Zugriffe zwischen den VoIP-Systemkomponenten

Die Kenntnis über die Kommunikationsbeziehungen zwischen den einzelnen Komponenten ist die Voraussetzung für die sinnvolle und sichere Konfiguration eines Firewallsystems. In der nachfolgenden Tabelle sind die gängigsten Teilsysteme und Ihre Kommunikationsbeziehung dargestellt.

	CTI-Applikationen	Groupware	Softphones	UMS-Server	Verzeichnisdienste	VoIP–Gateway	VoIP–Server	VoIP–Telefone	Webbrowser
CTI-Applikationen		X	X	X	X	X	X	X	
Groupware	X	X	X	X	X		X	X	
Softphones			X	X	X	X	X	X	
UMS-Server		X	X	X	X	X	X	X	
Verzeichnisdienste									
VoIP–Gateway			X	X		X	X	X	
VoIP–Server			X	X	X	X	X	X	
VoIP–Telefone			X	X	X	X	X	X	
Webbrowser	X	X		X		X	X	X	
XML–Pushservice			X					X	

Tabelle 4.1: VoIP-Systemkomponenten und ihre Kommunikationsbeziehung

Vertikal sind die Systemkomponenten aufgetragen, von denen aus eine Kommunikationsbeziehung auf die horizontal aufgetragenen Systemkomponenten erfolgt. Auf den Webbrowser als reine Client-Komponente ist kein Zugriff erforderlich.

Befinden sich die betreffenden Systeme in getrennten Netzen, werden die entsprechenden Ports (UDP/TCP) in den Firewallsystemen frei geschaltet, durch die der IP-Verkehr durchgeleitet werden muss.

Beispieldesign

Für die grundsätzliche Firewallkonfiguration und das Firewalldesign zur Umsetzung der Sicherheitsrichtlinie einer Organisation sei an dieser Stelle auf entsprechende Fachliteratur verwiesen. In der nachfolgenden Abbildung soll ein Designbeispiel gezeigt werden, das die besprochene Forderung der Trennung von Sprach- und Datennetz erfüllt, jedoch durch Übergänge der einzelnen Netzsegmente auch Verkehr zwischen den Netzsegmenten ermöglicht. Die Netzübergänge werden in diesem Beispiel mit ALG-Firewallsystemen umgesetzt.

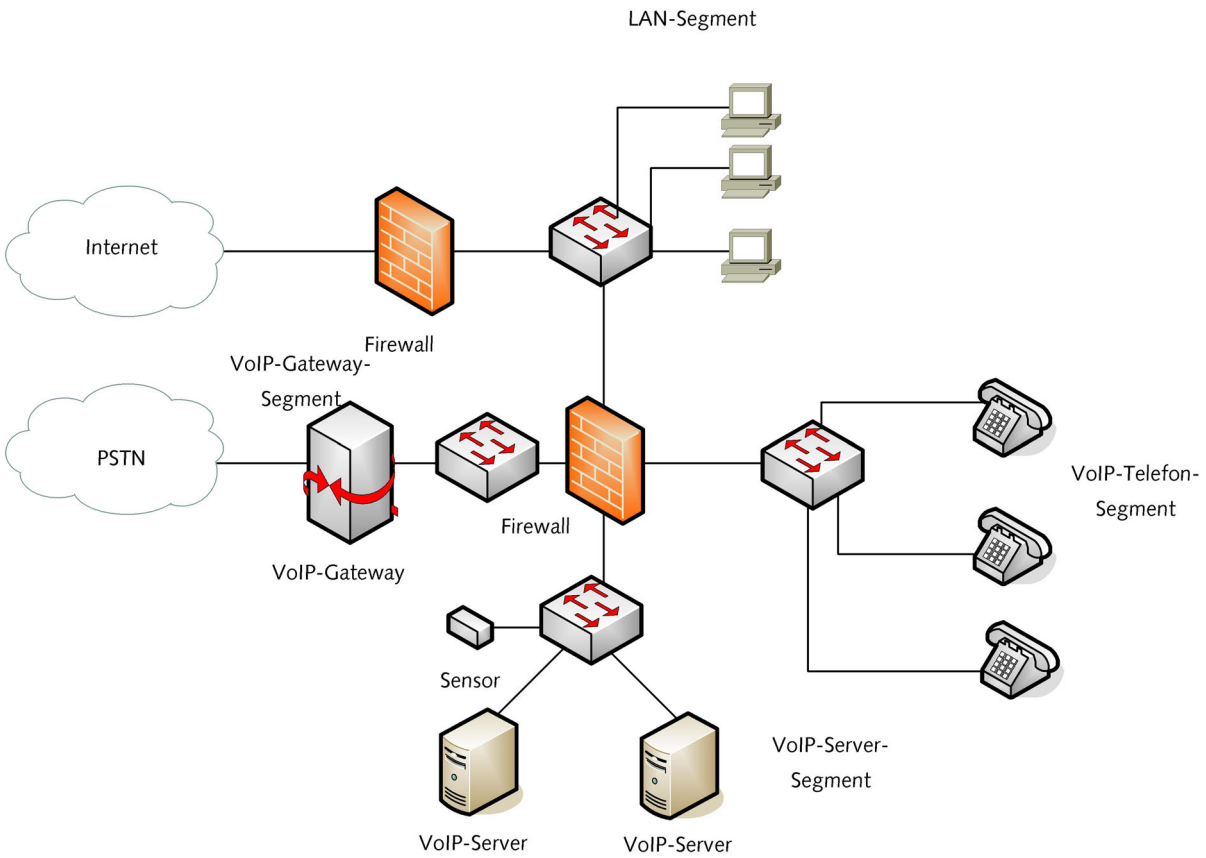

Abbildung 4.5 Beispieldesign Firewall in VoIP-Netzen

Zwischen Internet und dem internen Netzwerk sitzt ein Firewallsystem, das Pakete vom Internet in das interne Netz nur dann zulässt, wenn sie zu einer vom internen Netz initiierten Sitzung gehören. Das zweite Firewallsystem trennt die Netzsegmente LAN, Telefon, VoIP-Server und VoIP-Gateway, und kontrolliert den Verkehr zwischen diesen Segmenten. Jeder Übergang zwischen den Netzen kann jeweils eigenen Firewallregeln unterworfen werden, die die Umsetzung der Sicherheitsrichtlinie garantieren.

Anforderung an ein NIDS

Ein NIDS – Network Intrusion Detection System – ist eine Netzwerksicherheitskomponente, die als Server oder Appliance aufgebaut sein kann und in einem Netzwerk den Verkehr hinsichtlich Anomalien untersucht, die Rückschlüsse über etwaige Angriffe liefern. Die Erkennung von Angriffen basiert auf dem Vergleich des Netzwerkverkehrs mit so genannten Angriffsmustern (Patterns), die zuvor im NIDS abgelegt werden. Eine weitere Methode ist die heuristische Analyse des Netzverkehrs, bei der durch statistische Methoden auch neue Angriffe erkannt werde können. Wird ein Angriff erkannt, können verschiedene Reaktionen wie Alarmmeldungen, E-Mail oder SMS erfolgen.

Bevor eine Anomalie als Angriff erkannt werden kann, muss zunächst der Netzwerkverkehr durch so genannte Sensoren abgegriffen werden. In einem aus Hubs aufgebautem Netzwerk ist der Netzwerkverkehr auf allen Ports sichtbar, so dass er einfach von einem Sensor in der entsprechenden Kollisionsdomäne gelesen werden kann. In einem geswitchten Netzwerk wird der Netzwerkverkehr einer Broadcastdomäne auf einen Switchport gespiegelt, an dem der Sensor des NIDS angeschlossen ist. Die Sensoren können den Netzwerktraffic filtern, um zu verhindern, dass erlaubter und bekannter Netzwerkverkehr durch das NIDS bearbeitet und dadurch die Leistungsfähigkeit des Systems beeinträchtigt wird. Es kann sowohl eingehender als auch ausgehender Verkehr untersucht werden.

Wird ein NIDS in Betrieb genommen, so ist es unumgänglich, zunächst eine Testphase zu durchlaufen und das System durch iterative Überarbeitung der Konfiguration (Tuning) anzupassen, um so Meldungen auszusortieren, die keine tatsächliche Bedrohung darstellen (false positive). Dabei ergibt

sich allerdings eine weitere Herausforderung: Falsch optimierte Systeme können einen tatsächlichen Angriff übersehen (false negative). Werden mehrere Sensoren bzw. IDS-Systeme in einem Netz eingesetzt, so sollten die Ergebnisse der Analyse korreliert werden, um durch die Einzelproben ein Gesamtbild der Bedrohungslage zu erhalten.

Regelmäßige Updates der Signaturen stellen sicher, dass der musterbasierte Erkennungsmechanismus aktuell bleibt und auch bei neu bekannt gewordenen Netzwerkangriffsarten Alarm schlägt.

Neben den Anforderungen, die an ein NIDS in einer üblichen Netzwerkumgebung ohne VoIP gestellt werden, muss in einer VoiP-Umgebung sichergestellt werden, dass die große Anzahl kleiner UDP-Pakete (RTP) nicht fälschlicherweise als Angriff (UDP flood) interpretiert wird und womöglich einen Schutzmechanismus einer Firewall (IPS) auslöst, durch den der Transport der Medienströme unterbunden und damit eine Sprachkommunikation unmöglich gemacht wird. Andererseits muss das NIDS-System schnell updatebar sein, um auch künftige, heute noch nicht bekannte Angriffe zu erkennen, die auf VoIP–Systeme und VoIP-Applikationen abzielen. Wie gut ein System ist, hängt demnach auch davon ab, wie schnell neue Patterns zur Verfügung stehen.

Wo sollte ein NIDS-System positioniert werden

Heutzutage kann man davon ausgehen, dass aufgrund des relativ geringen Anschaffungspreises für einen Switch die meisten Netzwerke geswitcht sind. Das bedeutet für ein NIDS, dass der Switchport, an dem es angeschlossen ist, den Netzwerkverkehr spiegelt. Moderne Switches können diese Funktionalität durch SPAN (Switched Port Analyzer) zur Verfügung stellen. Die nachfolgende Abbildung zeigt ein Beispiel für eine Implementierung eines NIDS in einem Netzwerk mit VoIP.

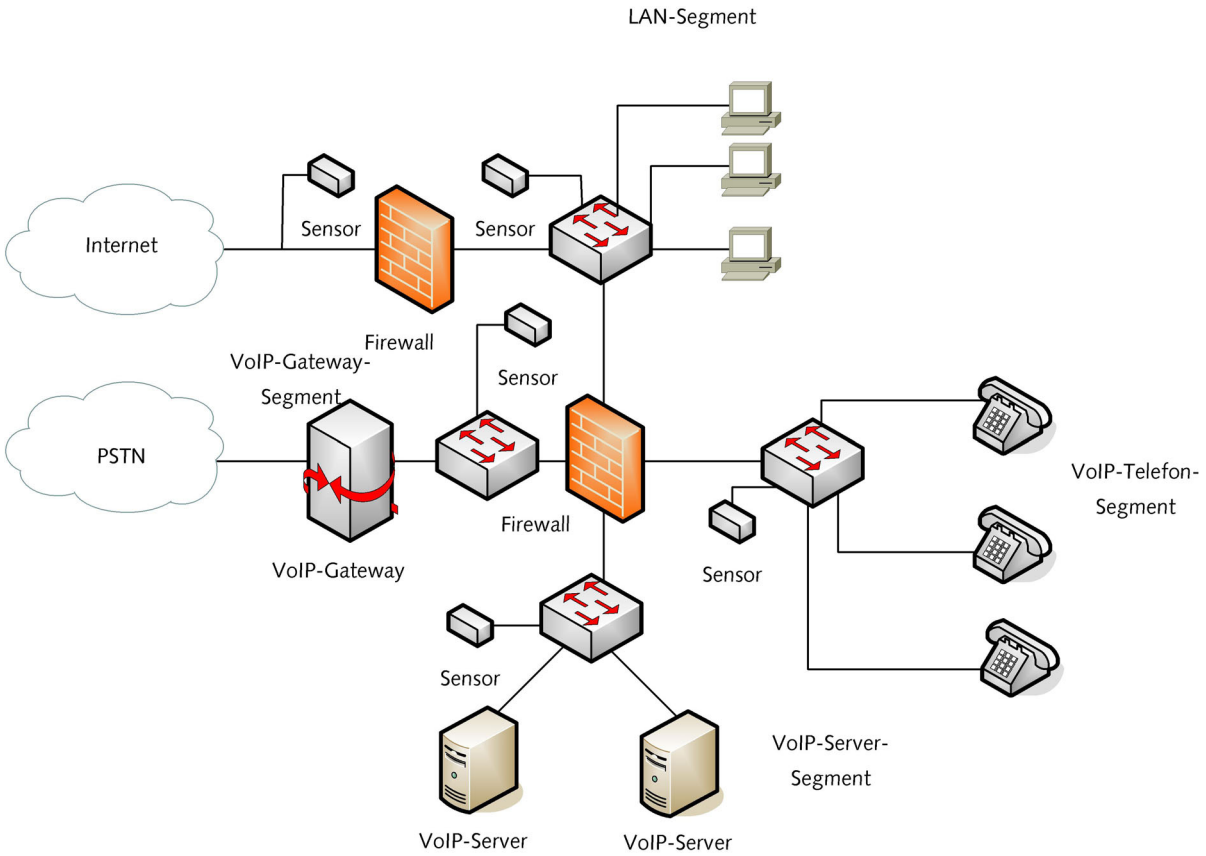

Abbildung 4.6 Beispiel eines Netzwerkes mit NIDS

Die Internetanbindung des gezeigten Netzwerkes wird durch eine Firewall gesichert, die die internen Netzsegmente vor unautorisierten Zugriffen aus dem Internet schützt. Vor und hinter der Firewall wird jeweils ein NIDS–Sensor gesetzt, der den gesamten Netzwerkverkehr des entsprechenden Segments analysiert. Der Sensor vor der Firewall zum Internet hin kann mit einem Hub oder Switch angebunden

werden. Aus Gründen der Übersicht wurde solch ein Netzelement an dieser Stelle in der Abbildung nicht aufgeführt, jedoch entspricht es im Wesentlichen der Anbindung der übrigen Sensoren im Netz hinter der Firewall. Die einzelnen internen Netzsegmente (LAN, VoIP-Telefone, VoIP-Server und VoIP-Gateway) werden jeweils durch einen Sensor überwacht.

4.2.4 NAT und VoIP

Einführung in NAT

NAT – Network Address Translation [RFC1631] – ermöglicht das Übersetzen einer IP-Adresse in eine andere IP-Adresse und wird meistens zum Übersetzen von privaten IP-Adressen in öffentlich geroutete IP-Adressen verwendet. Bei dieser Adressumwandlung werden durch ein entsprechendes NAT-Gateway (Router oder Firewall) Quell-IP-Adressen und die dazugehörigen Quellports in öffentliche Quell-IP-Adressen mit öffentlichen Ports übersetzt. Damit das NAT-Gateway Rückpakete bzw. eingehende Pakete, die an die öffentliche IP adressiert sind, an den richtigen internen Host weiterleiten kann, unterhält es eine Tabelle, die die Zuordnung von der öffentlichen IP-Adresse/Port zur privaten IP-Adresse/Port ermöglicht.

Statisches NAT

Bei statischem NAT wird durch Konfiguration im NAT-Gateway eine dauerhafte feste Beziehung zwischen einer externen und einer internen IP-Adresse geschaffen, was beispielsweise den Betrieb von öffentlich erreichbaren Servern (WWW-Server, DNS-Server, E-mail-Server) hinter einer NAT-Umgebung ermöglicht. Dabei kann je Dienst eine öffentliche IP-Adresse/Port auf je eine interne IP-Adresse/Port oder eine öffentliche IP-Adresse mit verschiedenen Portbindungen auf verschiedene interne IP-Adressen mit den dazugehörigen Ports abgebildet werden. Die nachfolgenden Tabellen verdeutlichen den Zusammenhang.

Dienst	öffentlich		privat	
	IP	Port	IP	Port
www	217.1.2.1	80	192.168.1.1	80
DNS	217.1.2.2	53	192.168.1.2	53
SMTP	217.1.2.3	25	192.168.1.3	25

Dienst	öffentlich		privat	
	IP	Port	IP	Port
www	217.1.2.1	80	192.168.1.1	80
DNS	217.1.2.2	53	192.168.1.2	53
SMTP	217.1.2.3	25	192.168.1.3	25

Tabelle 4.2: Statisches NAT-Mapping für öffentlich erreichbare Dienste

Dynamisches NAT

Dieses Verfahren übersetzt interne IP-Adressen dynamisch auf externe IP-Adressen, die zuvor in einem so genannten Adresspool festgelegt wurden. Die Zuordnung erfolgt nach dem Round Robin-Verfahren. Es können sowohl die IP-Adresse als auch die Ports übersetzt werden.

PAT – Port Adress Translation

Mittels PAT teilen sich mehrere interne IP-Adressen eine öffentliche IP-Adresse. Das NAT-Gateway übersetzt jeweils eine interne IP-Adress-Portkombination in dieselbe externe IP-Adresse. Durch die Vergabe eines jeweils neuen Ports kann eine Unterscheidung getroffen und sichergestellt werden, dass eine Zuordnung für Rückpakete möglich ist.

In der nachfolgenden Tabelle werden Pakete vor und nach der PAT-Übersetzung gezeigt.

Paket intern vor PAT			
Quell IP-Adresse /Port		Ziel IP-Adresse /Port	
IP	Port	IP	Port
192.168.1.1	62123	217.1.2.1	80
192.168.1.1	62124	217.1.2.2	80
192.168.1.1	62126	217.1.2.3	25
192.168.1.7	39146	217.1.2.3	445
192.168.1.9	42126	217.1.2.3	25

Paket extern nach PAT			
Quell IP-Adresse /Port		Ziel IP-Adresse /Port	
IP	Port	IP	Port
194.1.2.3	63768	217.1.2.1	80
194.1.2.3	64001	217.1.2.2	80
194.1.2.3	63816	217.1.2.3	25
194.1.2.3	63526	217.1.2.3	445
194.1.2.3	61126	217.1.2.3	25

Tabelle 4.3: Pakete vor und nach PAT

Full Cone NAT

Alle Anfragen von der gleichen internen IP-Adresse und Port werden auf die gleiche externe IP-Adresse und Port abgebildet. Jede externe Quelle (Host) kann Pakete zu einem internen System (Host) senden, indem sie die Pakete an die externe IP–Adresse und den externen Port adressiert, auf denen die interne IP–Adresse und Port abgebildet sind. Es findet ein statisches Mapping statt.

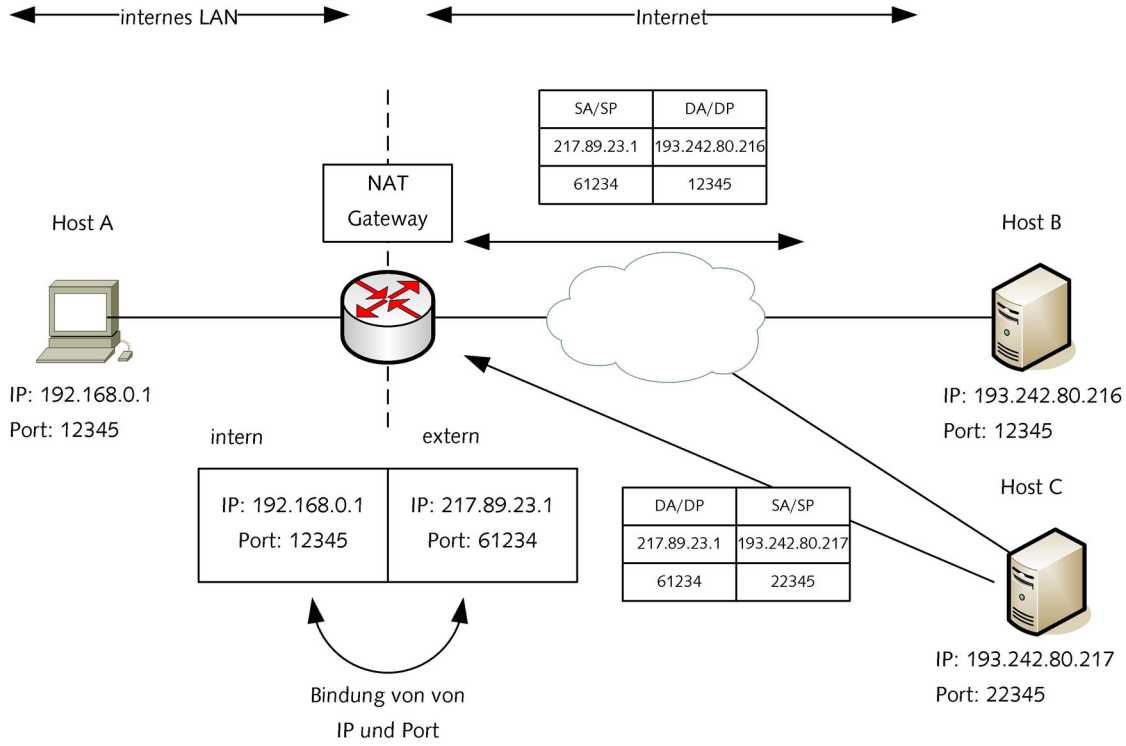

Abbildung 4.7 Full Cone NAT

Die Abbildung „Full Cone NAT“ zeigt den internen Host A, der auf Host B zugreift. Host C kann auf Host A über dessen öffentliche IP Adresse 217.89.23.1 mit dem Port 61234 zugreifen.

Restricted Cone NAT

Alle Anfragen von der gleichen internen IP-Adresse und Port werden auf die gleiche externe IP-Adresse und Port abgebildet. Jede externe Quelle (Host B) kann nur dann Pakete zu einem internen System senden, wenn der interne Host A zuvor Pakete an den externen Host B gesendet hat.

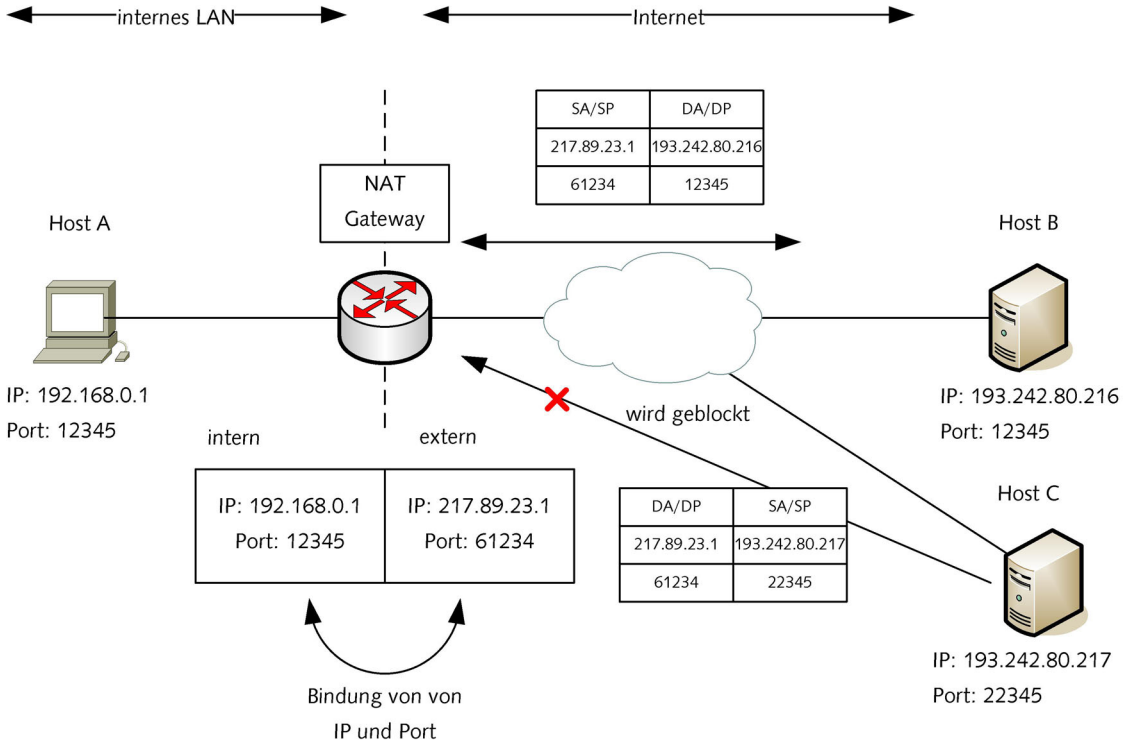

Abbildung 4.8 Restricted Cone NAT

Da Host A zuvor auf Host B zugegriffen hat, kann Host B auf Host A zugreifen. Der Kommunikationsaufbau durch Host C wird geblockt, da Host A noch keine Verbindung zu Host C aufgebaut hat.

Port Restricted Cone NAT

Alle Anfragen von der gleichen internen IP-Adresse und Port werden auf die gleiche externe IP-Adresse und Port abgebildet. Ein externer Host B mit der IP-Adresse = Z kann nur dann Pakete mit dem Quellport=c an einen internen Host A senden, wenn Host A zuvor ein Paket an Host B mit der Zieladresse IP = Z und Zielport = c gesendet hat. Port Restricted NAT funktioniert im Prinzip wie Restricted Cone NAT, wobei neben der IP auch der Port berücksichtigt wird.

Symmetric Cone NAT

Alle Anfragen von der gleichen internen IP-Adresse und Port des Host A an den externen Host B werden auf die gleiche externe IP-Adresse und Port abgebildet. Werden Anfragen an einen anderen externen Host C mit der gleichen internen IP-Quelladresse und Quellport gesendet, so wird eine andere externe IP-Adresse/Port–Abbildung verwendet.

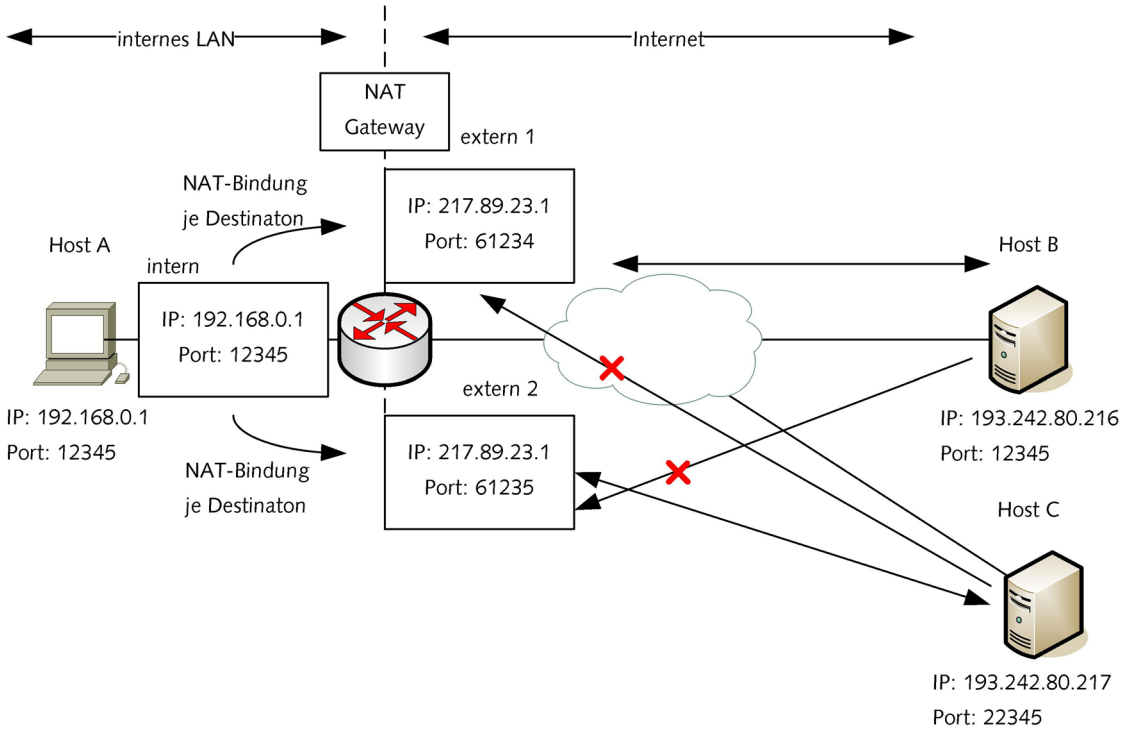

Abbildung 4.9 Symetric Cone Nat

Host B kann keine Kommunikation über die NAT-Bindung, die für Host C unterhalten wird, aufbauen. In umgekehrter Weise kann Host C keine Verbindung über die NAT-Bindung, die für Host C gilt, aufbauen.

Probleme durch NAT für VoIP

Die für den RTP- bzw. RTCP-Strom verwendeten Ports werden dynamisch im Bereich von 1024 bis 65534 vergeben und bei den meisten VoIP-Protokollen innerhalb des SDP (Session Description Protocol) in den Signalisierungsnachrichten übertragen. Durch NAT werden die Quell-IP-Adresse im IP-Header und der Quellport im UDP- bzw. TCP-Header modifiziert. Die Angaben über die Quell-IP-Adresse und den UDP-Port im Nachrichtenteil bleiben unverändert. In Folge können keine Medienströme an das VoIP-Telefon, das sich hinter einem NAT-Gateway befindet, gesendet werden. VoIP-Geräte, die sich im Internet befinden, können keinen Rufaufbau zu einem hinter einem NAT-Gateway befindlichen VoIP-Telefon aufbauen, da die private IP-Adresse nicht im Internet geroutet wird und dem rufenden System weder die NAT-Bindung und der NAT-Typ innerhalb des NAT-Gateways bekannt ist, noch klar ist, ob eine NAT-Bindung offen ist. In der nachfolgenden Abbildung wird die Problematik anhand eines Beispiels aufgezeigt, bei dem ein VoIP-Telefon hinter einem NAT-Gateway ein VoIP-Telefon im Internet anruft.

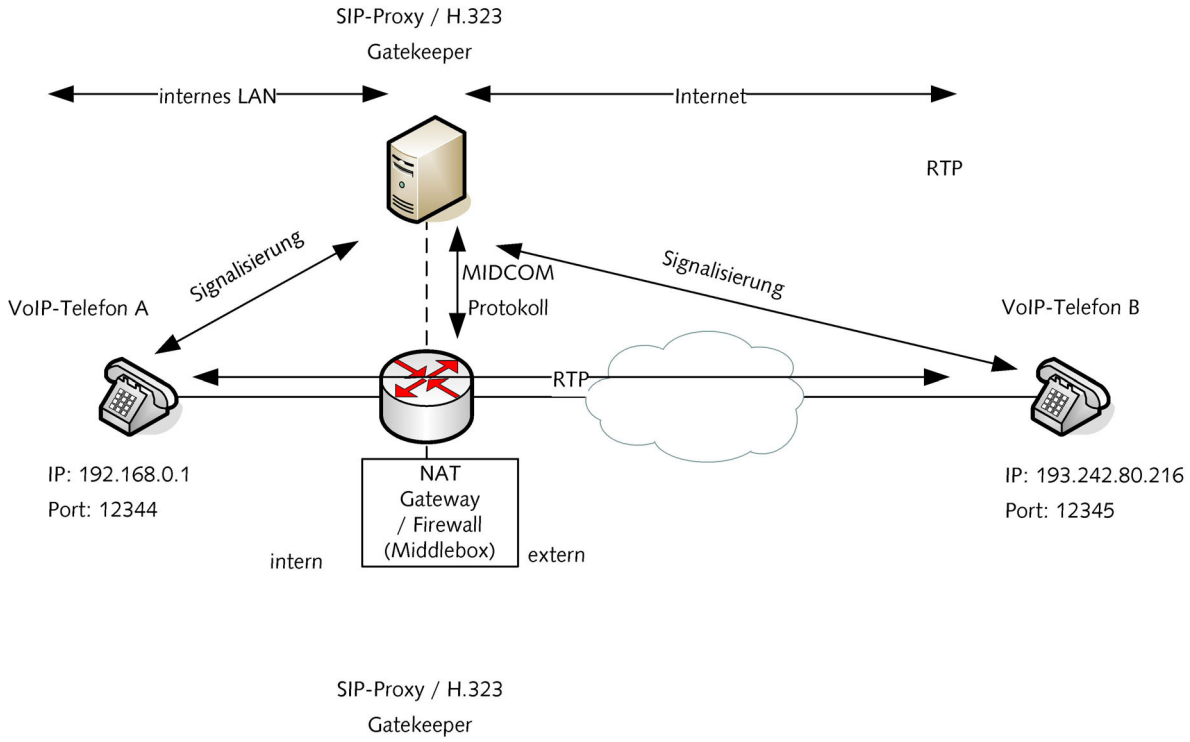

Abbildung 4.10 Probleme durch NAT für VoIP

In dem gezeigten Beispiel wird angenommen, dass das VoIP-Telefon A die NAT-Adresse kennt (Konfiguration im Telefon). Dadurch kann der SIP-Signalisierungsaufbau auch durch NAT hindurch erfolgen, da die Software des VoIP-Telefons die öffentliche IP-Adresse in den SIP-Header einsetzt. Nach dem die Sitzung aufgebaut ist, beginnt der Teilnehmer am VoIP-Telefon A das Gespräch. Die Audio-Daten werden mit RTP an das VoIP-Telefon B gesendet. Der Teilnehmer am VoIP-Telefon B beginnt nun ebenfalls zu sprechen. Seine Sprachdaten werden mit RTP an die öffentliche IP-Adresse gesendet, jedoch an den UDP-Port, der im SDP von VoIP-Telefon A stand. Da das NAT-Gateway jedoch keine Bindung für diesen Port eingetragen hat, werden diese RTP-Pakete nicht durch das NAT-Gateway an das VoIP-Telefon B weitergeleitet. Die Sprache wird nur in eine Richtung übertragen. Eine Kommunikation ist nicht möglich.

Hätte das VoIP-Telefon A die öffentliche NAT-Adresse nicht in den SIP-Header eingetragen, wäre weder der SIP-Sitzungsaufbau erfolgt noch die Einwegeübertragung von RTP-Paketen erfolgt.

In den nachfolgenden Abschnitten werden Möglichkeiten aufgezeigt, die einen VoIP-Betrieb in einer NAT-Umgebung ermöglichen.

ALG und NAT

Die Funktionsweise eines ALG (Application Level Gateway) wird im Kapitel Firewalls und NIDS beschrieben.

MIDCOM

MIDCOM steht für Middlebox Commmunications und ist ein Draft der IETF, der eine Lösung für die NAT- und Firewallproblematik im Zusammenhang mit VoIP bietet. Ein MIDCOM-System besteht aus einer Middlebox und einem Serversystem, dass die Middlebox steuert bzw. konfiguriert. Der Steuerungsserver ist ein VoIP-Server (H.323-Gatekeeper, SIP-Proxy), der sich im Signalisierungspfad befindet und den Austausch der SDP-Daten verfolgt, und anhand dieser Daten über das MIDCOM-Protokoll die Middlebox (NAT-Gateway, Firewall) steuert, die die NAT–Bindungen in die NAT-Tabelle einträgt und die entsprechenden Ports öffnet. In der nachfolgenden Abbildung ist die MIDCOM-Architektur skizziert.

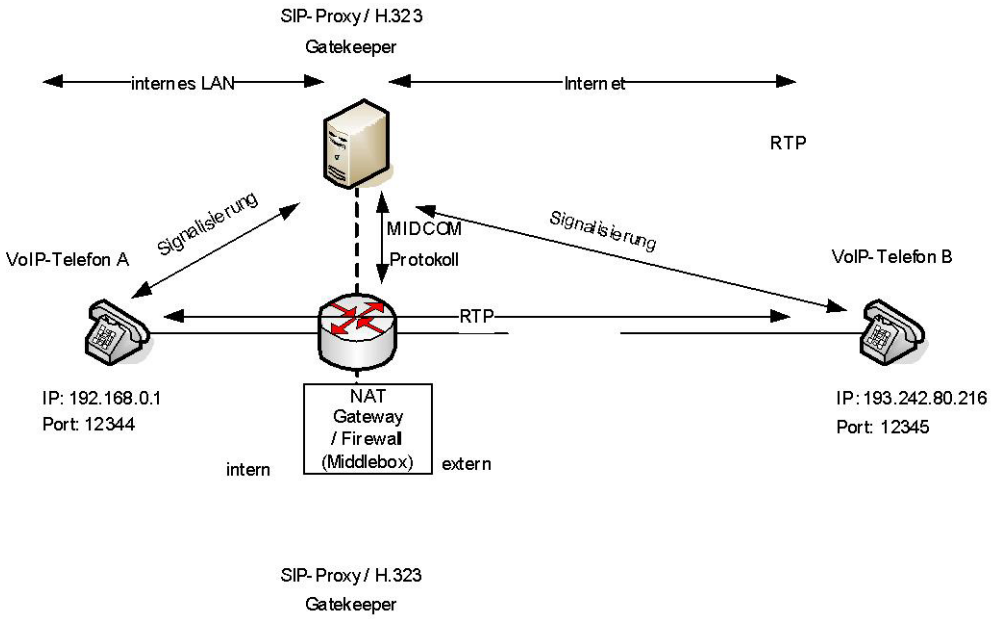

Abbildung 4.11 MIDCOM-Umgebung

Da der VoIP-Server selbst offen im Internet steht, empfiehlt es sich, den VoIP-Server ebenfalls durch eine Firewall zu schützen, da ein erfolgreicher unauthorisierter Zugriff auf solch einen Server durch einen Angreifer auch die von ihm kontrollierte Middlebox (Nat-Gateway, Firewall) kompromittiert und so Tür und Tor für weitere Angriffe öffnet. Bisher ist MIDCOM noch nicht abschließend durch das IETF festgelegt worden.

Session Border Controller

Die bisherigen Arbeiten der Midcom Working Group der IETF wurden bisweilen noch nicht in einsatzfähige Produkte umgesetzt. Hersteller haben begonnen, proprietäre Lösungen auf den Markt zu bringen, die die NAT- und Firewallproblematik lösen und meist Providernetze adressieren. Unter anderem werden neben der Unterstützung für den Firewall- bzw. NAT-Durchgang je nach Implementierung eines Session Border Controllers SLA Monitoring, Rufannahmesteuerung (Call Admission Control), Billing und das gesetzliche Abhören für Bedarfsträger ermöglicht. Session Border Controller werden als Appliances oder Serversysteme angeboten. Die nachfolgende Abbildung zeigt ein Beispiel einer Session Border Controller-Implementierung, die aus einem Signalisierungs- und einem RTP-Proxy besteht. Sämtlicher Verkehr (Signalisierung und Medienstrom) läuft über diesen Session Border Controller. Dem VoIP-Telefon ist die tatsächliche IP-Adresse von VoIP-Telefon A nicht bekannt.

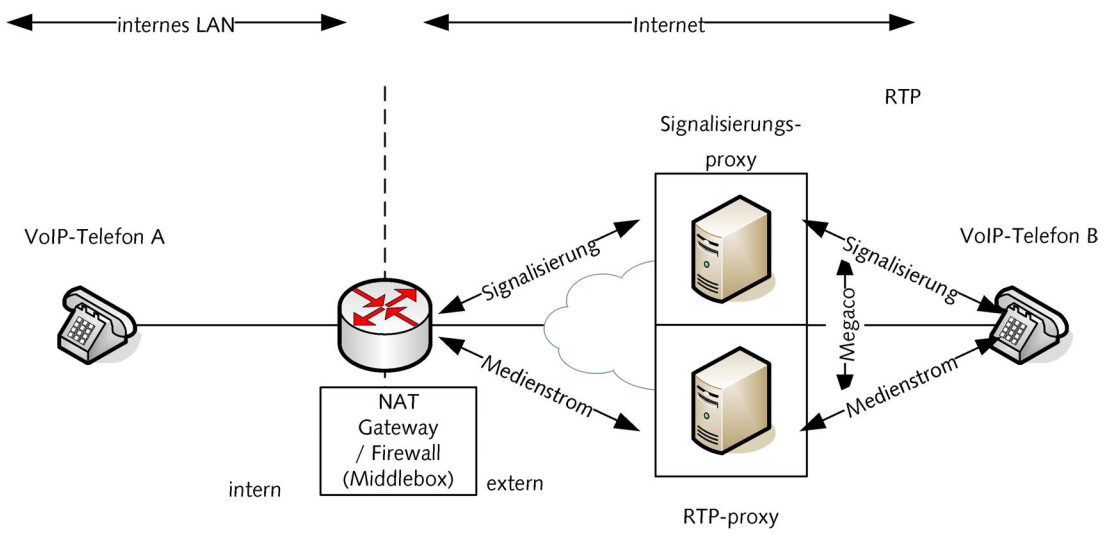

Abbildung 4.12 Beispiel für einen Session Border Controller

UPnP – Universal Plug and Play

UPnP ist ein Industriestandard, der vor allem im Heimbereich immer größere Verbreitung findet. Mit der UPnP-Architektur soll die Vernetzung von PCs und intelligenten Endgeräten (beispielsweise Drucker, Scanner, WLAN Access Points) vereinfacht werden. Durch UPnP können Applikationen die öffentliche IP-Adresse des NAT-Gateways lernen, die zu verwendenden Bindungen vorgeben und nach der Beendigung einer Sitzung wieder entfernen. Es kann auch eine so genannte Lease Time vorgegeben werden, die die Dauer der Gültigkeit einer NAT-Bindung festlegt. Werden mehrere NAT-Gateways hintereinander geschaltet, kann mit UPnP kein NAT-Durchgang erzielt werden.

STUN – Simple Traversal of User Datagram Protocol (UDP) Through NATs

Mit Hilfe von STUN [RFC3489] wird Endsystemen, die sich hinter einem NAT-Gateway befinden, ermöglicht, ihre öffentliche IP-Adresse zu ermitteln und die NAT-Bindung des Gateways zu lernen. Dabei sendet der STUN–Client (beispielsweise ein VoIP-Telefon) eine Anfrage (STUN Shared Request) zum STUN-Server, der seinerseits dem Client einen Benutzernamen und eine Kennung zuweist. Mit diesen Benutzerdaten sendet der STUN-Client eine zweite Anfrage (STUN Binding Request) an den STUN-Server um die NAT-Bindung des letzten NAT-Gateways vor dem STUN-Server zu erfahren. Der STUN-Server entnimmt dem letzten Request die Quell-IP-Adresse und den Quell-IP-Port und sendet diese Informationen in seiner Antwort (STUN Binding Response) an den STUN-Client. Durch weitere Abfragen kann der Client den NAT-Typ herausfinden. Symmetric NAT wird von STUN nicht unterstützt. Die NAT-Bindings werden bei VoIP im Signalisierungsprotokoll übertragen, so dass eingehende RTP-Ströme an das NAT-Binding adressiert werden und so das sich hinter dem NAT-Gateway befindliche VoIP-Telefon zu erreichen. Die im RFC 3489 beschriebene STUN-Technologie wird bereits von vielen VoIP-Telefonen unterstützt und wird von den meisten VoIP-Providern angeboten.

TURN – Traversal Using Relay NAT

TURN erlaubt Systemen hinter einem NAT-Gateway bzw. einer Firewall eingehende TCP- und UDP-Verbindungen zu empfangen und verhindert gleichzeitig, dass diese Möglichkeit für den Betrieb von öffentlich erreichbaren Servern, wie Webserver oder Mailserver, genutzt werden kann, indem je IP-Adresse-Portkombination nur eine Sitzung zu einem Peer erlaubt ist. Im Gegensatz zu STUN können mit TURN auch Systeme hinter symmetrischen NAT-Gateways eingehende Verbindungen empfangen. TURN ist ein einfaches Client/Server-Protokoll, das auf der gleichen Syntax und den generellen Operationen von STUN aufbaut. Ein TURN-Client (z. B.: VoIP-Telefon) sendet eine Anfrage (TURN Allocate request) an der TURN-Server. Eine Authentisierung erfolgt auf der Basis von so genannten „Shared Secrets“, d.h. auf Passwörtern, die sowohl Client und Server bekannt sind.

Der TURN-Server merkt sich die IP-Adresse und den Port von dem die Anfrage kam als SA (Source Adress - Quelladresse) und sendet in seiner Antwort (TURN response) eine öffentliche Transportadresse PA (Public Address – öffentliche Adresse) an den TURN-Client. Der TURN-Server nimmt eine eingehende Verbindung auf der öffentlichen Adresse PA an und leitet die Pakete an die SA Adresse des Clients. Empfängt er Daten von SA, leitet er sie weiter an PA. Der TURN-Server fungiert als Relay. Ein TURN-Client kann bei dem TURN-Server gerade bzw. ungerade Ports anfordern und die nächst höheren Ports reservieren lassen, was bei Verwendung des RTP sinnvoll ist. TURN ist ein Internet-Draft des IETF, der jedoch noch nicht als RFC veröffentlicht wurde.

ICE – Interactive Connectivity Establishment

Da bei TURN sämtliche Medienströme über den TURN-Server geführt werden, ist es sinnvoll, einen TURN-Server nur dann einzusetzen, wenn mit STUN der Empfang eingehender Verbindungen nicht möglich ist. ICE stellt eine Methode für SIP dar, um einen NAT-Durchgang auf Grundlage mehrerer über SDP bekannt gegebener Adressen zu ermöglichen, wobei auf die Protokolle STUN, TURN, RSIP und MIDCOM zurückgegriffen wird. Es wird davon ausgegangen, dass einem Client mehrere Adressen (beispielsweise von STUN oder TURN gelernte Adressen) zur Verfügung stehen, über die er Medienströme empfangen kann. Da zwei Endsysteme nicht wissen, welche Adresse funktioniert, werden die Adressen nacheinander nach ihrer Priorität geprüft, wobei die Adresse mit der höchsten Priorität als erstes getestet wird. Die Prioritäten werden anhand der geringsten Kosten und dem Maximum an QoS festgelegt und dann nacheinander innerhalb des SDP aufgeführt. ICE ist für SIP konzipiert, funktioniert jedoch auch mit RTSP und H.323 und ermöglicht, dass ein Endgerät unabhängig von der NAT-Umgebung betrieben werden kann. ICE ist ein Internet-Draft des IETF, der jedoch noch nicht als RFC veröffentlicht wurde.

4.3 VoIP-Middleware

Bei der VoIP-Middelware handelt es sich grundsätzlich Serversysteme, die mit den gleichen Sicherheitsmaßnahmen zu schützen sind, wie sie auch für andere Serversysteme eingesetzt werden (siehe auch GSHB). Darüber hinaus sind weitere Sicherheitsmaßnahmen anzuwenden, die den besonderen Bedrohungen bei VoIP-Systemen gerecht werden.

4.3.1 Leistungsmerkmale

Wie bei traditionellen TK-Systemen bieten VoIP-Systeme ebenfalls eine große Vielfalt verschiedener Leistungsmerkmale. Es sollte vor Betrieb eines VoIP TK-Systemes geklärt sein, welche Leistungsmerkmale und Funktionalitäten vorhanden sind, welche benötigt werden. Die nicht benötigten Leistungsmerkmale sollten deaktiviert werden. Zu den sicherheitskritischen Leistungsmerkmalen gehören beispielsweise das Aufschalten auf ein bestehendes Gespräch, Raumüberwachungsfunktionen und Wechselsprechen.

4.3.2 Administration und Zugänge

Administration und Konfiguration der Middleware ist immer an der Konsole oder über gesicherte Verbindungen durchzuführen. Die Administration kann beispielsweise über eine SSH Secure Shell oder eine IPSec-gesicherte VPN-Verbindung erfolgen.

Viele VoIP-Systeme ermöglichen eine Konfiguration über ein Webinterface. Der dabei installierte Web-Server kann ein zusätzliches Sicherheitsrisiko darstellen. Daher ist es empfehlenswert, ein mögliches Web-basiertes Konfigurationsinterface physikalisch von kritischer Middleware, wie Gateways und Gatekeeper zu trennen. Eine Web-basierte Konfiguration sollte immer gesichert erfolgen, beispielsweise durch den Einsatz von https und TLS.

Bei der Planung des Administrierkonzeptes sollte ein Rollenkonzept vorgesehen sein, in dem verschiedenen Berechtigungsstufen eingerichtet werden (vergl. GSHB). Ein zweiter Zugang sollte zu

Vertretungszwecken eingerichtet sein. Veränderungen sollten durch das System nicht-manipulierbar protokolliert werden. Dies ist insbesondere auf dem Hintergrund zu sehen, dass der Administratorzugang sowohl Zugriff auf möglicherweise personenbezogene Daten wie private Verbindungsdaten hat als auch in der Lage ist, mit geringem Aufwand alle Gespräche, die über das System geführt werden aufzuzeichnen.

4.3.3 Datenbackup

Ein umfassendes Datensicherungskonzept ist eine zentrale Anforderung zur Sicherstellung bzw. zur raschen Wiederherstellung der Verfügbarkeit. Dabei ist darauf zu achten, dass bei der Sicherung personenbezogener Daten – wie beispielsweise privater Verbindungsdaten – diese in verschlüsselter Form abgelegt werden.

4.3.4 Softwaresicherheit

Es ist darauf zu achten, dass die eingesetzte Software immer auf dem aktuellesten Stand ist und etwaige Sicherheitspatches unverzüglich aufgespielt werden. Dies gilt insbesondere auch für das eingesetzte Betriebssystem.

Für die Verlässlichkeit des Gesamtsystems ist eine korrekt implementierte Software von großer Bedeutung. Insbesondere die vitalen Funktionen des Telefoniesystems, wie die einfache Vermittlung von Gesprächen und die Gatewayfunktion in das digitale Fernsprechnetz sollten daher einem besonderen Evaluierungsprozess unterzogen werden.

Daher ist es empfehlenswert auf Systeme zurückzugreifen, die in einem bewährten Modell entwickelt (beispielsweise nach dem V-Modell) und nach anerkannten Kriterien bewertet und geprüft wurden. Maßgeblich für die Evaluierung der Sicherheit von Systemen in der Informationstechnik sind heute die Common Criteria [CC2000, ISO/IEC15408]. Ein für die VoIP-Anwendung zugeschnittenes Schutzprofil existiert allerdings derzeit noch nicht,

4.3.5 Betriebssystemsicherheit

Die VoIP-Komponenten sollten so als Minimal-System (siehe auch GSHB M4.97) konzipiert werden, dass verschiedene Dienste auf verschiedenen Servern betrieben werden. Allerdings ist insbesondere bei kompakten stand-alone Systemen, die meist nur aus einer Hardware bestehen, die vollständige Trennung von Diensten nicht ohne weiteres möglich.

Das eingesetzte Betriebsystem sollte mindestens als minimales Betriebssystem (siehe GSHB M4.95) ausgelegt sein und die Anzahl der auf der Middleware ausgeführten Applikationen so klein wie möglich gehalten werden. Jede zusätzliche Applikation kann das Riskio von fehlerhafter oder böswilliger Software erhöhen. Daher ist genau zu prüfen, welche Applikationen benötigt werden und nicht benötigte Anwendungen sind zu deinstallieren Software, die zur Installation benötigt wird, ist im Anschluss zu löschen (beispielsweise Compiler). Nicht benötigte Netzdienste sind zu deaktivieren und den Zugriff durch lokale Paketfilter/Firewall zu beschränken.

Eine zusätzliche Maßnahme ist der Einsatz gehärteter Betriebssystemversionen, die bereits bzgl. ihrer Sicherheitseigenschaften optimiert sind (z. B. SINA-Linux, SE-Linux).

Ein umfassender Schutz wird allerdings erst durch eine vollständige Abkapselung der Prozesse auf niedrigster Ebene möglich. Dies ermöglicht eine verlässliche, von einem Angreifer nicht zu umgehende, Trennung der Dienste. Entsprechende sichere Betriebssystemplattformen werden bereits in verschiedenen Anwendungen eingesetzt (z. B. µ-Sina [HWS03], Perseus/EMSCB [PRS+01, ASSS05]).

4.4 Endgeräte

Für die Endgeräte, die meist als vollständiges Serversystem aufgebaut sind, gelten ähnliche Sicherheitsmaßnahmen wie bei der Middleware. Zusätzliche Sicherheitsmaßnahmen betreffen insbesondere ihre sichere Konfiguraton und Firmware-Update.

4.4.1 Software

Vertreuenswürdige Firmware-Update

Viele IP-Endgeräte bieten die Möglichkeit zum automatischen Update ihrer Firmware.

Es sollte sichergestellt werden, dass neue Firmware nur nach erfolgter Authentifizierung des Codes auf das Endgerät aufgespielt werden kann. Ein nicht-kryptographischer CRC-Check ist nicht ausreichend, vielmehr sollte die Authentizität des Codes Überprüfung einer Digitalen Signatur vorgesehen sein.

Vertrauenswürdiges Konfigurieren und Digitale Zertifikate

Viele IP-Endgeräte bieten verschiedene Möglichkeiten zur Konfiguration. Hierzu gehören die lokale Konfiguration am Endgerät, die Web-basierte Konfiguration durch Zugriff auf einen im Endgerät integrierten Webserver sowie die automatische Konfiguration durch „Ziehen“ (Pull) der Konfiguration von einem http(s)- oder TFTP-Server.

Die lokale Konfiguration wird selten eingesetzt. Sie sollte Passwort-geschützt sein oder falls nicht erforderlich deaktiviert werden. Der Zugang zur Web-basierten Konfiguration sollte Passwort-geschützt sein und über eine gesicherte Verbindung, beispielsweise https, erfolgen. Ein zusätzlicher Schutz wird erreicht durch die Verwendung eines Client-Zertifikats zur Authentifizierung autorisierter Clients.

Die automatische Konfiguration über einen TFTP-Server sollte nicht gewählt und deaktiviert werden. Insbesondere die automatische TFTP-Serverwahl innerhalb des DHCP-Bootvorganges bietet zahlreiche Angriffsmöglichkeiten.

Eine automatische Konfiguration sollte über einen https-Server erfolgen. Der https-Server sollte sich mit einem Zertifikat authentisieren, das vom Endgerät vor dem Laden der Konfiguration validiert werden kann. Üblicherweise wird das Server-Zertifikat bei der Erstinberiebnahme auf die Endgeräte manuell installiert.

4.4.2 Sicherheitsfunktionalität

IP-Telefone sollten die Möglichkeit zur Passworten-basierten ein- oder mehrstufigen Zugangskontrolle (z. B. personen-bezogenes Login oder Passwort für Amtsberechtigung), bieten. Bei aktiviertem Passwort-Schutz sollten dann nur Notruf-Dienste zur Verfügung stehen.

Viele IP-Telefone haben noch mit vielfältigen „Kinderkrankheiten“ zu kämpfen. Daher ist unbedingt darauf zu achten, dass die angebenen Sicherheitsfunktionalitäten auch implementiert sind. Ggf. ist ein Evaluierungs-/Zertifizierungsnachweis zu verlangen.

Aufgrund der bisherigen Erfahrungen und den in IP-Telefonen weit verbreiteten Sicherheitslücken, erscheint es empfehlenswert, in sensiblen Bereichen nur Endgeräte zuzulassen, die nach formalen Methoden wie den Common Criteria evaluiert sind. Dabei erscheint auch hier der Einsatz eines sicheren Betriebssystems mit der strikten Trennung der verschienden Dienste eine essentielle Voraussetzung für den verlässlichen Einsatz dieser Technologie zu sein.

4.5 Protokolle

Die in Kapitel 2.2 eingeführten Protokolle zur Signalisierung und zum Medientransport bieten teilweise eigene Sicherheitsmechanismen oder Erweiterungen zur Abwehr einiger der vorgestellten Bedrohungen. In diesem Abschnitt werden diese Sicherheitsmechanismen betrachtet, die erreichten Sicherheitsziele beleuchtet und verbleibende Bedrohungen diskutiert. Dabei werden zunächst die Sicherheitsmaßnahmen zum Schutz der Signalisierung fokusiert und mögliche Sicherheitsmaßnahmen zum Schutz des Medienstroms beschrieben. Abschließend werden allgemeine Sicherheitsmaßnahmen auf der Netzwerkschicht (IPSec und DNSSec) diskutiert, die ebenfalls zur Absicherung von VoIP-Systemen herangezogen werden können.

4.5.1 Sichere Signalisierung

Die beiden wichtigsten Standards zur VoIP-Signalisierung sind SIP 2.0 [RFC3261] und H.225 (Setup-Signalisierung) sowie H.245 (Aufbau der logischen Kanäle) innerhalb des H.323 Frameworks (siehe Kapitel 2.3.1). Neben diesen Standards gibt es weitere proprietäre Signalisierungsprotokolle wie IAX2, das in der aktuellen Draft-Version [IAX2] über keine eigenen Sicherheitsmechanismen verfügt. Aus diesem Grund beschränkt sich der Abschnitt auf Sicherheitsmechanismen der SIP und H.323 Protokolle. Daneben existieren spezielle Signalisierungsprotokolle (MGCP und Megaco) zur Steuerung von Media Gateways, die ebenfalls keine Sicherheitsmechanismen bieten. Die Absicherung dieser Protokolle muss daher im Allgemeinen durch geeignete Sicherheitsmaßnahmen auf der Netzwerkschicht (siehe Kapitel 4.2) erfolgen.

Die H.235 Sicherheitsarchitektur

Der H.235 Standard definiert Sicherheitsmechanismen für H.323. Seit Version 1 (verabschiedet im Juni 1998) wurden bis zur aktuellen 3. Version (verabschiedet im August 2003) umfangreiche Sicherheitsmechanismen zum Schutz von H.323-basierter VoIP Telefonie definiert. Die spezifizierten Mechanismen umfassen insbesondere den Schutz der Anrufsignalisierung (H.225/Q.931), des Steuerungskanals (H.245) sowie die Sicherheit des Medienstroms.

H.235v2 (verabschiedet im November 2000) erweiterte H.235v1 um effiziente EC (elliptic curve) Kryptographie und AES Unterstützung. Des Weiteren wurden Sicherheitsprofile (engl. security profiles) eingeführt (Annex D – Annex F), die jeweils gängige Anwendungsszenarien und Anforderung adressieren und eine entsprechende Auswahl kryptographischer Algorithmen und Protokolle spezifizieren. Ziel dieser Sicherheitsprofile war unter anderem die Verbesserung der Interoperabilität zwischen H.235 Produkten [KWF05].

Darüber hinaus wurden in H.235v3 nützliche Features, wie verschlüsselte DTMF (engl. dual tone multi-frequency) Signale, NAT-fähige authentisierte Signalisierung, verbessertes Sitzungsschlüsselmanagement, erweiterte Sicherheitsmechanismen für direkte Anrufsignalisierung sowie einen neuen Betriebsmodus EOFB (engl. extended output feedback), zur Verschlüsselung von Medienströmen eingeführt.

Im Folgenden wird ein Überblick über die wichtigsten Sicherheitsmechanismen der aktuellsten Spezifikation H.235v3 gegeben, sowie über die darin spezifizierten Sicherheitsprofile. Alle verwendeten Algorithmen und Protokolle entstammen ISO oder IETF Standards.

Vertrauenswürdige Systemkomponenten: H.235 betrachtet alle Systemkomponenten, die Endpunkte eines verschlüsselten H.245 Kontrollkanals oder eines verschlüsselten logischen Kanals sind, als *vertrauenswürdige Komponenten*, die entsprechend authentifiziert werden müssen. Beispiele für vertrauenswürdige und zu authentifizierende Systemkomponenten sind MCUs und Gateways.

Sicherheitsmechanismen auf Netzwerk- oder Verbindungsschicht: Grundsätzlich kann die Vertraulichkeit und Authentizität der H.323 Signalisierung durch Sicherheitsmechanismen auf der Netzwerk- oder Verbindungsschicht (beispielsweise IPSEC oder TLS) geschützt werden. Da dem H.225 Protokoll keine Vereinbarung des Sicherheitsmechanismus vorangeht, muss die Verwendung

implizit, beispielsweise durch Verwendung eines definierten Ports, vereinbart werden. Die Verwendung von IPSEC oder TLS zur Sicherung des H.245 Protokolls kann innerhalb des H.225 Protokolls zwischen den Parteien vereinbart werden. Darüber hinaus spezifiziert H.235 eigene Sicherheitsmechanismen, speziell zur Authentifizierung von Signalisierungsnachrichten.

Authentifizierung: H.235 definiert folgende Arten der Authentifizierung:

a) Subskriptionsbasierte Authentifizierung (engl.: subscription-based authentication) mittels symmetrischer Kryptographie und eines gemeinsamen, zuvor ausgetauschten Geheimnisses (beispielsweise eines Passwortes). Als kryptographische Verfahren können entweder symmetrische Verschlüsselungsverfahren oder Keyed-Hash-Funktionen dienen, wobei das gemeinsame Geheimnis jeweils als symmetrischer kryptographischer Schlüssel verwendet oder kryptographisch sicher daraus abgeleitet wird.

b) Authentifizierung basierend auf zertifizierten öffentlichen Schlüsseln und signierten Nachrichten.

Jedes dieser Verfahren kann jeweils mit 2 Nachrichten unter Verwendung von Zeitstempeln oder mit 3 Nachrichten mit zufälligen Challenges als Challenge-Response Protokoll implementiert werden.

c) Diffie-Hellman (DH) Schlüsselvereinbarungsprotokoll mit optionaler Authentifizierung: In einer ersten Phase führen beide Kommunikationsparteien ein DH Schlüsselvereinbarungsprotokoll basierend auf zertifizierten öffentlichen Schlüsseln durch. Der dabei erzeugte gemeinsame symmetrische Schlüssel wird in der optionalen zweiten Authentifizierungsphase zur eigentlichen Authentifizierung, basierend auf symmetrischer Verschlüsselung, verwendet.

Diese Authentifizierungen können für alle Signalisierungsnachrichten verwendet werden.

Media Anti-Spam: H.235 spezifiziert einen Mechanismus, genannt Media Anti-Spam, der den Empfänger von RTP Paketen effizient überprüfen lässt, ob ein RTP Paket authentisch ist und von einem autorisierten Sender stammt. Dazu wird ein kurzer MAC (engl. message authentication code) über ausgewählte Felder des RTP-Paketes berechnet, den der Empfänger prüft, bevor er mit der eigentlichen Verarbeitung des RTP-Paketes beginnt. Der MAC kann entweder durch einen Verschlüsselungsalgorithmus (DES oder 3DES im MAC-Betriebsmodus) oder durch eine Keyed-Hash-Funktion (HMAC-SHA1-96)[4] berechnet werden. Dieser Mechanismus ist primär zur Abwehr von DoS-Angriffen durch RTP Flooding und Spit auf bekannt gewordenen RTP-Ports gedacht.

H.235v3 Annex D – Baseline Security Profile: Das Baseline Sicherheitsprofil umfasst Mechanismen zur Hop-by-Hop Benutzerauthentifizierung und zur Hop-by-Hop Authentifizierung von Signalisierungsnachrichten (RAS, H.225.0 und H.245) durch beliebige Komponenten auf dem Signalisierungspfad. Die spezifizierte Authentifizierung basiert auf HMAC-SHA1-96 und ist optional auf eine gegenseitige Authentifizierung erweiterbar. Der HMAC wird an jedem Endpunkt eines Kanals verifiziert und dieser wird ggf. vor der Weiterleitung der Nachricht zum nächsten Hop der Signalisierungskette mit dem entsprechenden Passwort des nächsten Kanals neu berechnet.

Das Baseline Sicherheitsprofil umfasst des Weiteren zwei optionale Erweiterung, das „Authentication-Only Profile“ sowie das „Voice Encryption Profile“

Das „Authentication-Only Profile“ ist eine Abschwächung des Baseline Security Profils in dem nur Teile der Signalisierungsnachrichten authentifiziert werden, so dass die restlichen Teile zur Überwindung von NAT Gateways und Firewalls modizifiert werden können, ohne die Authentifizierung zu beschädigen.

Das „Voice Encryption Profile“ ist eine Option zur Verschlüsselung von Sprachdaten in RTP Pakten, die in Verbindung mit dem Baseline Sicherheitsprofil sowie den unten beschriebenen Sicherheitsprofilen verwendet werden kann. Als Verschlüsselungsalgorithmus ist die Unterstützung

[4] HMAC-SHA1-96 bezeichnet einen auf 96 Bit gekürzten HMAC auf Basis der SHA1-Hashfunktion. Vor dem Hintergrund der aktuellen Angriffe gegen SHA1 sollte die Sicherheit dieses verkürzten MAC neu überdacht werden.

von DES vorgeschrieben und optional werden 128-Bit AES, 3DES und 56-Bit RC2 spezifiziert. Als Operationsmodi sind CBC und EOFB spezifiziert.

Des Weiteren umfasst das Voice Encryption Profile eine Schlüsselvereinbarung zwischen den Kommunikationsendgeräten innerhalb der H.225.0 Ruf-Signalisierung und auf Basis des Diffie-Hellman Protokolls. Der dabei vereinbarte gemeinsame Master-Key wird zum sicheren Austausch von Session Keys innerhalb des H.245 Protokolls verwendet. Diese wiederum werden zur eigentlichen Verschlüsselung des Medienstroms verwendet und in regelmäßigen Abständen durch entsprechende H.245 Nachrichten erneuert. Die Verwendung von SRTP wird zurzeit als Annex G zum H.235 Standard spezifiziert – dessen Verabschiedung steht jedoch noch aus.

Das Baseline Sicherheitsprofil beinhaltet keine expliziten Mechanismen zum Schutz der Vertraulichkeit von Signalisierungsnachrichten. Diese muss gegebenenfalls auf niedrigeren Schichten beispielsweise durch IPSEC oder TLS geschützt werden.

Das Baseline Sicherheitsprofil selbst basiert ausschließlich auf symmetrischer Kryptographie und setzt voraus, dass die dazu benötigten symmetrischen Schlüssel in Form eines Passwortes bereits ausgetauscht wurden.

Es ist somit vergleichsweise einfach zu implementieren, weil das Schlüsselmanagement ausgeklammert wird und verteilte symmetrische Schlüssel bzw. Passwörter vorausgesetzt werden. Damit ist es primär in Gatekeeper-basierter Signalisierung zur Hop-by-Hop Sicherung von Terminal-Gatekeeper, Gatekeeper-Gatekeeper und Gateway-Gatekeeper Verbindungen in administrativen/organisatorischen Einheiten verwendbar. Eine Erweiterung auf direkte Rufsignalisierung ist mittlerweile in Annex I spezifiziert (siehe unten).

H.235v3 Annex E – Signature Security Profile: Wie der Name bereits vermuten lässt, basiert dieses Sicherheitsprofil auf asymmetrischer Kryptographie, insbesondere digitalen Signaturen, welche ausschließlich zur Authentisierung von Nachrichten zum Einsatz kommen. Durch den Einsatz eines Public-Key Schlüsselmanagements skaliert dieses Profil deutlich besser, insbesondere wenn die Kommunikationspartner oder die einzelnen Hops der Signalisierungskette zuvor keine Vertrauensbeziehung in Form gemeinsamer Geheimnisse besitzen.

Wie das Baseline Security Profile bietet das Signature Security Profile Hop-by-Hop Benutzerauthentifizierung sowie die Hop-by-Hop Authentifizierung von Signalisierungsnachrichten (RAS, H.225.0 und H.245) durch beliebige Komponenten auf dem Signalisierungspfad. Des Weiteren bietet das Signature Security Profile Nicht-Abstreitbarkeit (engl.: non-repudiation), was die Beweislage für Streitigkeiten bzgl. Abrechnungsinformationen deutlich verbessert. Zudem ermöglicht das verbesserte Schlüsselmanagement eine *Ende-zu-Ende* Authentifizierung und die Signierung von Signalisierungsnachrichten bietet zudem Nicht-Abstreitbarkeit dieser Nachrichten.

H.235v3 schreibt die Verwendung von RSA-SHA1[5] oder RSA-MD5 Signaturen vor. Aufgrund der erfolgreichen Kollisionsangriffe gegen MD5 sollte von der Verwendung dieser Hashfunktion für digitale Signaturen, speziell in Zertifikaten, abgesehen werden [Ba2005]. Dies scheint im hybriden Sicherheitsprofil bereits berücksichtigt worden zu sein, da es MD5 zur Erstellung von RSA Zertifikaten explizit ausschließt.

Ein Nachteil dieses Profils liegt darin, dass das Signieren jeder Nachricht einen relativ großen Rechenaufwand erfordert. Damit führt der Einsatz dieses Profils auf leistungsschwachen Endgeräten oder auf zentrale Komponenten der H.323 Infrastruktur, die zahlreiche Signalisierungsnachrichten authentifizieren müssen, möglicherweise zu Problemen.

Zum Schutz der Vertraulichkeit der Sprachdaten kann das Signature Security Profil wiederum mit der Voice Encryption Option kombiniert werden. Zum Passieren von NAT-Gateways und Firewalls steht ebenfalls die Authentication-Only Option zur eingeschränkten Authentifizierung von Nachrichten zur Verfügung.

---

5 Kürzlich wurden Angriffe gegen Hash-Funktionen (MD5, SHA-1) bekannt (z.B. [WaLi05]), die die Berechnung von Kollisionen ermöglichen bzw. die benötigte Komplexität deutlich verringern.

H.235v3 Annex F – Hybrid Security Profile: Das hybride Sicherheitsprofil basiert auf hybrider Kryptographie und vereint die Vorteile des „Baseline Security“ und des „Signature Security“ Profils.

Digitale Signaturen werden zur Authentifizierung der ersten Handshake-Nachrichten verwendet. Während des Handshakes wird ein symmetrischer Schlüssel vereinbart, der anschließend wie im Baseline Sicherheitsprofil zur Authentifizierung nachfolgender Nachrichten verwendet wird. Damit erreicht das hybride Sicherheitsprofil annähernd die gleichen Sicherheitseigenschaften wie das Signatur Sicherheitsprofil. Lediglich die Nicht-Abstreitbarkeit späterer Nachrichten wird nicht erreicht, da diese wiederum auf symmetrischen MACs beruht. Auch wird kein Ende-zu-Ende Sicherheitsmechanismus spezifiziert.

Durch die Verwendung symmetrischer Kryptographie ist das hybride Sicherheitsprofil jedoch deutlich effizienter, wodurch es wiederum besser skaliert und auch auf schwächeren Endgeräten verwendet werden kann. Auch dieses Profil ist mit der Voice Encryption Option und der Authentication-Only Option kombinierbar.

H.235v3 Annex I - Direkte Ruf-Signalisierung: Die vorherigen Sicherheitsprofile zielten ausschließlich auf Gatekeeper-signalisierte Rufe und sind somit nicht zur Sicherung direkt-signalisierter Rufe verwendbar. Problematisch ist dabei die Schlüsselvereinbarung zwischen den beiden Endgeräten.

Annex I definiert einen Sicherheitsmechanismus für direkte Signalisierung für den Fall, dass beide Endgeräte eine etablierte Vertrauensbeziehung zu demselben Gatekeeper haben. In diesem speziellen Fall kann der Gatekeeper die Rolle eines Key-Distribution Centers wie im Kerberos Protokoll übernehmen: Möchte ein Endpunkt A einen Ruf zu Endpunkt B aufbauen, so sendet A zunächst eine Admission-Nachricht an den Gatekeeper. Dieser generiert daraufhin einen symmetrischen Sitzungsschlüssel und verschlüsselt diese einmal für A und einmal für B. Beide Schlüsseltexte werden als ClearToken innerhalb der ACF Nachricht an A gesendet. Beim eigentlichen Rufaufbau sendet Endpunkt A den für Endpunkt B verschlüsselten Sitzungsschlüssel an B. Anschließend besitzen sowohl A als auch B einen gemeinsamen Sitzungsschlüssel und können die bekannten Sicherheitsmechanismen aus Annex D und F verwenden.

H.235v3 Annex G – SRTP und MIKEY: Zurzeit steht ein neuer Annex zu H.235 vor der Verabschiedung, der die Einbindung des MIKEY Schlüsselmanagementprotokolls und die Verwendung von SRTP (siehe Kapitel 4.5.2) zur Sicherung des Medienstroms spezifiziert. Die Einbindung des MIKEY Protokolls ist dabei ähnlich zu dessen Einbindung in das SIP Protokoll, wo es in SDP Nachrichten getunnelt wird.

SIP

Ein grundlegendes Problem in der Absicherung von Signalisierungsprotokollen wie dem SIP Protokoll besteht darin, dass bei der Signalisierung häufig mehrere Komponenten (Endgeräte und Server) involviert sind, die jeweils Teile der Signalisierungsnachrichten lesen oder sogar verändern müssen. Aus diesem Grund ist eine naive Anwendung von Ende-zu-Ende Sicherheitsmechanismen nicht möglich, sondern erfordert anwendungsspezifische Anpassungen.[6]

Aus diesem Grund befürwortet der SIP Standard explizit die Verwendung von Sicherheitsmechanismen auf Schichten unterhalb der Anwendungsschicht einzusetzen und nur jeweils die Kommunikation zwischen den einzelnen SIP-Komponenten (UA, Proxy-, Registrar-, Redirect- und Location-Server) abzusichern, was häufig als „Hop-to-Hop“ Sicherheit bezeichnet wird.

Als weiteres Argument für „Hop-to-Hop“ Sicherheitsmechanismen wird im SIP 2.0 Standard darauf hingewiesen, dass den Servern ohnehin in gewissem Umfang vertraut werden muss. Hier sollte jedoch deutlich Vertrauen bezüglich Signalisierung gegenüber Vertrauen bezüglich des Medientransports,

[6] Als Beispiel sei an dieser Stelle auf die URI von SIP-Anfragen oder die Route Header-Felder genannt, die von SIP-Proxies interpretiert werden müssen. Darüber hinaus müssen SIP-Proxies in der Lage sein, bestimmte Header-Felder, wie beispielsweise das „Via“ Header-Feld anzupassen, damit Rufe den gewünschten Teilnehmer erreichen können.

d.h. der Sprachdaten, unterschieden werden. Daher sollten in sicherheitskritischen Umgebungen zusätzlich geeignete Ende-zu-Ende Maßnahmen eingesetzt werden, die die Vertraulichkeit und Authentizität des Medientransports (z. B. auch den Schlüsselaustausch für SRTP) auch gegen solche Angreifer gewährleisten, die einen SIP-Server kontrollieren.

Die aktuelle SIP 2.0 Spezifikation RFC 3261 definiert unterschiedliche Sicherheitsmechanismen, die sich sowohl bezüglich Sicherheitsziel, Sicherheit und möglichen Einsatzszenarien unterscheiden. Die Autoren der SIP Spezifikation versuchten dabei, existierende Sicherheitsmechanismen wie HTTP Digest Authentisierung, S/MIME, TLS und IPSec wieder zu verwenden und, sofern nötig, an SIP anzupassen.

Authentisierung von SIP Anfrage-Nachrichten (Requests):

Erhält eine SIP Komponente eine Anfrage-Nachricht, so kann diese eine Authentisierung durch den Initiator der Anfrage verlangen. Dazu spezifiziert SIP einen zustandslosen Challenge-Response Authentisierungsmechanismus, der auf der HTTP Digest Authentisierung (RFC 2617) aufbaut und leicht an die Erfordernisse von SIP angepasst wurde.[7] Dieser Authentisierungsmechanismus verhindert Replays von Anfragen und bietet Einweg-Authentisierung.

Die Funktionsweise des HTTP Digest Authentisierungsmechanismus ist sehr einfach: erhält eine Komponente eine SIP Anfrage-Nachricht (engl. request), so kann diese eine Authentisierung der Anfrage durch den Sender anfordern. Dazu sendet sie eine SIP Antwort-Nachricht (engl. response) vom Typ Code 401"Unauthorized" oder Code 407 „Proxy Authentication Required" an den Sender der Anfrage. Diese Antwort-Nachricht enthält ein „WWW-Authenticate" bzw. „Proxy-Authenticate" Header-Feld, worin die Realm und ein Zufallswert (engl. nonce), die so genannte „Challenge" des Authentisierungsverfahrens, enthalten ist.
Der Initiator, der diese Antwortnachricht empfängt, sucht nun nach passenden Credentials (Username und Passwort) für diese Realm und berechnet daraus die passende Response als Hashwert, auch „digest" genannt, aus Challenge, Anfrage-Nachricht (Methode, URI sowie Nachrichtenkörper), Realm und Credential. Diese wird schließlich in Form eines „WWW-Authorization" bzw. „Proxy-Authorization" Header-Feldes in die ursprüngliche Anfrage-Nachricht eingebettet. Die authentisierte Anfrage wird nun erneut gesendet und vom Empfänger durch einfaches Nachrechnen verifiziert.

Der SIP 2.0 Standard schreibt vor, dass die Digest Authentisierung von allen SIP Komponenten (UAs, Registrar-, Proxy-, Redirect- und Location-Server) implementiert wird. Somit kann er zur gegenseitigen Authentifizierung zwischen beliebigen Komponenten verwendet werden.

Abschließend sei auch an dieser Stelle nochmals betont, dass der SIP Digest Mechanismus nicht die Integrität und Authentizität der Gesamtnachricht gewährleistet, sondern nur die Authentizität der Methode, des URI sowie des Nachrichtenkörpers schützt (siehe dazu auch Abschnitt 26.4.1 des RFC 3261). Somit sollten zusätzliche Maßnahmen zum Schutz der Authentizität der übrigen SIP Header gegen aktive Angreifer ergriffen werden (vgl. Abschnitt 22 des RFC 3261). Aus diesem Grund wird die HTTP Digest Authentisierung hauptsächlich als komplementäre Maßnahme zur nachträglichen UA Authentifizierung über TLS-geschützte Verbindungen angesehen. Dies dürfte, analog zu WWW-Szenarien, immer dann notwendig sein, wenn ein UA über kein eigenes TLS-Zertifikat verfügt und somit keine UA Authentisierung über TLS möglich ist.

S/MIME

Der Standard Secure/MIME erweitert die MIME-Datentypen um Konstrukte für signierte und verschlüsselte Nachrichten. Diese Sicherheitsmechanismen werden somit vollständig in das MIME-Konzept integriert, wodurch S/MIME letztlich zum Nachfolger von PEM und zum Konkurrenten von OpenPGP wurde. Er ist im Wesentlichen in den RFCs 2311-2315 (Version 2), 2630, 2632 und 2633 (Version 3) sowie RFC 3851 (Version 3.1) beschrieben. Der Wechsel von Version 2 zu Version 3 ist weniger durch technische Notwendigkeiten begründet, als vielmehr mit der Geschäftspolitik rund um

[7] Die Version 1.0 der SIP Spezifikation (RFC 2543) sah noch die Verwendung des HTTP „Basic" Authentisierungsmechanismus vor, welche jedoch in der aktuellen SIP 2.0 Spezifikation (RFC 3261) aufgrund der Klartextübertragung von Passwörtern und den daraus resultierenden Sicherheitsproblemen explizit verboten wird.

das RSA-Patent. In S/MIME Version 2, die unter maßgeblicher Beteiligung der Firma RSA Inc. entstand, spielt der RSA-Algorithmus, als einziger zwingend vorgeschriebener Public-Key-Algorithmus, eine Schlüsselrolle, und die Public Key Cryptography Standards (PKCS) 1, 7 und 10 dieser Firma werden in den RFCs namentlich erwähnt. Warum dies von der IETF nicht weiter unterstützt wurde, ist unbekannt. In Version 3 wurde der RSA-Algorithmus zur Option degradiert, und die PKCS-Standards zu einem „Cryptographic Message Syntax (CMS)"-Dokument [RFC 2630] zusammengefasst.

Die wesentlichen Unterschiede zwischen den beiden Versionen betreffen die verwendeten kryptographischen Algorithmen. Abgesehen von diesen Unterschieden basieren Version 2 und 3 auf der gleichen Technologie.

Eine Beschreibung neuer Sicherheitsfunktionalitäten, die mit Hilfe des S/MIME-Standards implementiert werden können, findet man im Dokument "Enhanced Security Services for S/MIME" [RFC 2634]. Dort ist beschrieben, wie man signierte Empfangsbestätigungen und Sicherheitslabel erzeugen kann, wie die Verschlüsselung einer Nachricht an eine große Mailingliste in sicherer Art und Weise einem Mail Agent überlassen werden kann, und wie Informationen zum Zertifikat in die Signatur mit eingebunden werden können.

Anwendung in SIP

Der Aufbau einer SIP-Nachricht ähnelt sehr stark einer E-Mail: Auf einen Header, der aus verschiedenen Zeilen besteht, folgt, getrennt durch eine Leerzeile, der Body. Während der Body einer E-Mail den eigentlichen Text (oder auch andere Daten) enthält, ist der Body einer SIP-Nachricht entweder leer (100 Ringing, 180 Trying) oder enthält eine Beschreibung der zu etablierenden Session in SDP. Für letzteres wird der MIME-Content-Type application/sdp verwendet. Es liegt daher nahe, den S/MIME-Sicherheitsstandard für E-Mails auch auf SIP zu übertragen.

S/MIME tritt an die Stelle von PGP (Pretty Good Privacy) wie es in SIP 1.0 (RFC 2543) spezifiziert wurde und ist im Kontext von SIP als Ende-zu-Ende Sicherheitsmechanismus prinzipiell auf vielfältige Art und Weise einsetzbar. Der SIP 2.0 Standard spezifiziert zwei Arten, S/MIME auf SIP-Nachrichten anzuwenden (vgl. Abschnitt 23, RFC 3261)

In der einfachsten Form wird zunächst nur der SDP Body einer SIP Nachricht mittels S/MIME geschützt, so dass die Authentizität und Vertraulichkeit der darin enthaltenen Parameter geschützt wird. Auf diese Weise lassen sich zum Beispiel Session-Keys vertraulich und authentisch austauschen, die wiederum zur Sicherung des Medienstroms verwendet werden können (siehe unten). Da der Session-Key nicht von Signalisierungsservern gelesen werden kann, bleibt die Sprachübertragung selbst dann sicher, wenn ein Angreifer einen SIP-Server kompromittiert hat.

Die Verarbeitung der S/MIME-Nachrichten findet auch hier in den Endgeräten statt. Es treten dabei aber in der Praxis die gleichen Probleme auf wie bei E-Mail:

- INVITE-Nachrichten des „application/pkcs7-mime"-Datentyps können von nicht S/MIME-fähigen Endgeräten nicht verarbeitet werden, auch wenn die INVITE-Nachricht nicht verschlüsselt, sondern nur signiert ist.
- Bei Verwendung von „multipart/signed"-Nachrichten ist es um die Interoperabilität besser bestellt, aber auch dies funktioniert nur, wenn zwei Bedingungen erfüllt sind:
  - Auch für nicht S/MIME-fähige Endgeräte muss eine (teilweise oder volle) Unterstützung des MIME-Standards zwingend („mandatory") vorgeschrieben werden, sonst können diese die Multipart-Nachricht nicht interpretieren.
  - Es muss sichergestellt werden, dass SIP-Gateways den Body von SIP-Nachrichten nicht verändern. (Eine typische Veränderung, die eine vorhandene Signatur ungültig machen würde, ist z. B. die Umwandlung von Tab-Zeichen in ein oder mehrere Leerzeichen.)

Der Header der SIP Nachrichten bleibt dabei jedoch zunächst ungeschützt. Da dieser Informationen enthält, die SIP Proxies zum Routing benötigen, ist eine Ende-zu-Ende Verschlüsselung ganzer SIP Nachrichten auch nicht ohne weiteres möglich.

Zum Schutz ganzer SIP Nachrichten (inklusive Header) spezifiziert der RFC 3261 das so genannte *„SIP Tunneling“*, wobei eine vollständige SIP Nachricht in S/MIME getunnelt wird. Die Funktionsweise ist dabei ähnlich dem S/MIME-geschützen Weitersenden einer E-Mail: eine vollständige, zu schützende SIP-Nachricht (innere Nachricht) wird, nachdem ihr ein „Content-Type: message/sip“ vorangestellt wurde, als Body einer SIP-Nachricht (äußere Nachricht) behandelt, signiert oder verschlüsselt, und mit einem identischen SIP-Header versehen an den SIP-Proxy gesendet.

Der SIP Standard spezifizert das weitere Vorgehen des Empfängers, sofern auf der Empfängerseite Unterschiede zwischen Header-Feldern der inneren und äußeren Nachricht bestehen.

Die SIP Spezifikation fordert dabei, dass S/MIME Implementierungen zumindest SHA1 Signaturen und 3DES Verschlüsselung unterstützen. RFC 3853 fordert die Unterstützung von AES, der von NIST als Nachfolgestandard für DES propagiert wird, da er sicherer als DES/3DES ist und gleichzeitig eine geringere Rechen- und Speicherkomplexität besitzt [RFC3853]. Insbesondere die geringere Komplexität ist für den Einsatz in VoIP-Endgeräten ein wesentlicher Faktor, der zur schnelleren Verfügbarkeit in VoIP-Endgeräten führen könnte.

S/MIME ist der einizige von SIP spezifizierte Ende-zu-Ende Sicherheitsmechanismus zwischen dem rufenden und dem gerufenen UA. S/MIME ist aber leider nur als „optional“ spezifiziert, so dass es fraglich ist, ob und wann S/MIME auf dem VoIP-Markt Einzug hält.

S/MIME zum Setup des Medienstroms

SIP nutzt das SDP (Session Description Protokoll [RFC2327]), um beim Aufbau einer Session Informationen über die Art der Session (beispielsweise Telefonie oder Instant Messaging) sowie die zu verwendenden Ports und Codecs auszutauschen. Im Falle von VoIP werden somit alle notwendigen Informationen über die zu initiierenden Medienkanäle ausgetauscht. Insbesondere kann dieser Mechanismus auch verwendet werden, um temporäre Schlüssel für den nachfolgenden Medienstrom, die so genannten Session-Keys, auszutauschen. Auf Basis dieser Session-Keys können die Telefonate mittels RTP Verschlüsselung (Vertraulichkeit) oder SRTP (Vertraulichkeit und Authentizität) gesichert werden (siehe Kapitel 4.5.2). In Verbindung mit weiteren SIP Sicherheitsmechanismen können und müssen die ausgetauschten Session-Keys authentisch und vertraulich ausgetauscht werden, um aktive (z. B. Man-in-the-Middle Angriffe) bzw. passive Angriffe abzuwehren.

S/MIME Schlüsselverwaltung in SIP

Auch sieben Jahre nach Einführung von S/MIME ist das Schlüsselmanagement in den E-Mail-Clients noch sehr kompliziert und nicht einheitlich geregelt. Dies hat mit zur mangelnden Akzeptanz von S/MIME beigetragen. Hier bemüht sich der SIP-Standard um klarere Regelungen [RFC 3261, 23.2 S/MIME Key Exchange], aber ihre Wirkung können diese Regelungen wohl nur entfalten, wenn regelmäßige Interoperabilitätstests durchgeführt werden.

Die eingesetzten Zertifikate müssen die SIP-URI des Teilnehmers enthalten. Diese soll, analog zu E-Mail-Zertifikaten, im SujectAltName-Feld des X.509-Zertifikats aufgeführt werden.

Ein Schlüsselmanagement über zentrale Verzeichnisdienste (LDAP, http) wird im SIP-Standard klar als optional gekennzeichnet: „Similarily, UACs SHOULD support a mechanism for importing ... certificates discovered in public directories ...“

Dagegen wird das Schlüsselmanagement über SIP zwingend vorgeschrieben: „Whenever the CMS SignedData message is used in S/MIME for SIP, it MUST contain the certificate bearing the public key necessary to verify the signature.“

Dies entspricht der Standard-Vorgehensweise bei E-Mail, und minimiert den Implementierungsaufwand in Endgeräten.

Sicherheit auf der Transportschicht: SIP über TLS (Transport Layer Security)

TLS ist ein in [RFC2246] spezifiziertes Protokoll, das auf SSL (engl. secure sockets layer) Version 3.0 basiert und einen sicheren, d.h. authentischen und vertraulichen, Kanal auf der Transportschicht implementiert.

Die SIP Spezifikation RFC 3261 schreibt vor, dass alle konformen SIP Server (Proxy-Server, Redirect-Server, Location-Server und Registrar-Server) das TLS Protokoll mit gegenseitiger

Authentifizierung sowie Einweg-Authentifizierung unterstützen müssen. Des Weiteren sollte zumindest die Cipher-Suite `TLS_RSA_WITH_AES_128_CBC_SHA` von allen TLS unterstützenden SIP Anwendungen implementiert werden.

Durch die Verwendung eines SIPS Request-URI wird die Verwendung von TLS mit gegenseitiger Authentifizierung und `TLS_RSA_WITH_AES_128_CBC_SHA` Cipher-Suite angefordert und der SIP Standard fordert, dass konforme Implementierungen dieser Aufforderung nachkommen sollten. UAs sollten TLS verwenden, um ihre Kommunikation mit Proxy-, Redirect- sowie Registrar-Servern zu schützen.

Die Verwendung eines SIPS URI bedeutet, dass jeder Hop bis zur *Ziel-Domain* durch die Verwendung von TLS geschützt werden sollte. Der letzte Hop vom Proxy der Zieldomain zum UA muss ebenfalls gesichert werden, wobei der dabei eingesetzte Sicherheitsmechanismus durch die Sicherheitspolitik innerhalb der Ziel-Domain bestimmt wird.

Bewertung von TLS: TLS 1.0 gilt als sicheres, etabliertes Protokoll mit vielen, teilweise frei verfügbaren Implementierungen, was eine schnelle Verbreitung auf dem VoIP Markt verspricht. Da es auf Zertifikaten basiert, kann es zwischen Systemen zum Einsatz kommen, die zuvor keine Vertrauensbeziehung (beispielsweise in Form gemeinsamer symmetrischer Schlüssel) besitzen.

TLS bietet im Kontext von SIP Systemen nur Hop-to-Hop Sicherheit zwischen je 2 benachbarten Hops. Dies hat auf der einen Seite Vorteile, weil einzelne Hops ohnehin Zugriff auf Teile der Klartextnachrichten haben müssen, beispielsweise um diese an die richtigen Domains weiterleiten zu können.

Auf der anderen Seite muss man sich aber auch der Tatsache bewusst sein, dass dadurch keine echte Ende-zu-Ende Sicherheit erreicht werden kann. Auch mangelt es an einer Art sicherem „Feedback"-Mechanismus, der insbesondere den beteiligten Endgeräten bestätigt, dass alle Hops gesichert sind. Hier müssen die Endgeräte momentan allen Proxy-Servern entlang des Signalisierungspfades vertrauen: zum einen kann der rufende UA nicht sicher sein, dass zwischen allen Hops TLS verwendet wird, weil ein kompromittierter Proxy einen *SIPS* Request in einen *SIP* Request umwandeln kann, so dass nachfolgende Hops keine TLS-Verschlüsselung mehr verwenden. Zum anderen kann ein gerufener UA, der einen SIPS Request empfängt nicht sicher sein, dass alle Hops gesichert sind, weil ein Angreifer einen SIP Request zu einem SIPS Request umwandeln kann, um der gerufenen UA eine „sichere Verbindung" vorzutäuschen.

Um diesen Bedrohungen entgegenzuwirken, enthält die SIP Spezifikation einige heuristische Überprüfungen, die aber letztendlich keine wirkliche Sicherheit bieten.

Ein weiteres Problem besteht darin, dass TLS eine zuverlässige Transportschicht voraussetzt. Somit können durch SIPS initiierte TLS-geschützte Sessions nicht über UDP initiiert werden, was den Overhead durch TCP-basierte Signalisierung erhöht. Zusätzlich limitiert die Komplexität von TLS die Skalierbarkeit auf zentralen Komponenten wie Proxy- oder Registrar-Server, die eine Vielzahl an (TLS)-Verbindungen offen halten müssen. Vor diesem Hintergrund sollte auf die Verwendungen effizienter kryptographischer Algorithmen geachtet werden oder gegebenenfalls spezielle Beschleunigerhardware für TLS zum Einsatz kommen.

Sicherheit auf der Netzwerkschicht: SIP über IPSec

IPSec ist ein weit verbreiteter Sicherheitsmechanismus, der sichere (authentische und vertrauliche) Kanäle auf der Netzwerkschicht implementiert (siehe Kapitel 4.5.3). Somit kann IPSec alle oberhalb, d.h. auf Transportschicht (TCP, SCTP und UDP) und Anwendungsschicht (SIP), operierenden Protokolle absichern.

Der Hauptanwendungsbereich für SIP ist insbesondere die authentische und vertrauliche Kommunikation zwischen UAs und SIP-Servern (End-to-Middle und Middle-to-End [KWF05]) bzw. die sichere Kommunikation zwischen einzelnen SIP Domänen, sofern der Aufwand für SIP-spezifische Sicherheitsmaßnahmen zu groß ist.

Der SIP Standard scheint jedoch TLS gegenüber IPSec zu bevorzugen und sieht die Unterstützung von IPSec daher nur als optional vor und lässt notwendige Details offen. Voraussetzung für den breiten Einsatz von IPSec in SIP Systemen wäre somit die Spezifikation eines entsprechenden IPSec Profils, was derzeit jedoch nicht existiert.

Anmerkung zu kryptographischen Algorithmen und Standards:

Kürzlich wurden Angriffe gegen Hash-Funktionen (MD5, SHA-1) bekannt (z. B. [WaLi05]), die die Berechnung von Kollisionen ermöglichen bzw. die benötigte Komplexität deutlich verringern. Daraus resultieren Sicherheitsbedrohungen gegen darauf aufbauende Sicherheitsmechanismen, wie beispielsweise Digest Authentication, MACs und digitale Signaturen, die zur Zeit noch nicht völlig überblickt werden können. Es zeichnet sich jedoch ab, dass viele Standards nun kurzfristig angepasst werden müssen, so dass sie die Verwendung als sicher geltender Hashfunktionen vorschreiben. Wie schnell diese neuen Spezifikationen in Implementierungen übernommen werden bleibt abzuwarten, aber man sollte bei der konkreten Produktauswahl auf die Verwendung von als sicher geltenden Hashfunktionen achten [Klima05,RiOs05].

4.5.2 Sicherer Medientransport mit SRTP

Das RTP Protokoll wird zur Übertragung von Datenpaketen der IP-Telefonie und das RTCP Protokoll zu deren Kontrolle eingesetzt. Beide Protokolle bieten keine eigenen Schutzmechanismen gegen das Abhören und Manipulationen von IP-Telefonaten an. SRTP Protokoll [RFC 3711] spezifiziert eine Erweiterung von RTP/RTCP, die solche Schutzmechanismen für die Übertragung gewährleisten.

Überblick

SRTP kann in VoIP eingesetzt werden, um die Vertraulichkeit, Authentifikation und Schutz gegen Replay-Angriffe für die Medienübertragung auf Basis von RTP zu erreichen. Das zugehörige SRTCP Protokoll bietet gleiche Eigenschaften für RTCP Nachrichten an.

SRTP präzisiert passende kryptographischen Mechanismen für die Verschlüsselung und Authentifikation von RTP-Nachrichten, und ermöglicht eine sichere Unicast- und Broadcastübertragung. Zum Transport werden die RTP/RTCP-Pakete in SRTP/SRTCP-Pakete eingekapselt.

Schlüsselmanagement

Neben dem kryptographischen Kontext, der verschiedene Sicherheitsparameter umfasst, definiert SRTP zwei Schlüsselarten: den Masterschlüssel k_m, und Sitzungsschlüssel k_e für Verschlüsselung und k_a für Authentifikation.

SRTP enthält keinen eigenen Mechanismus zur Erzeugung und Verwaltung von mindestens 128 Bits langen Masterschlüsseln. Dieser kann mit Standards, wie z. B. Multimedia Internet Keying (MIKEY) realisiert werden.

Sitzungsschlüssel k_e (min. 128 Bits) und k_a (min. 160 Bits) werden aus dem Masterschlüssel mit Hilfe einer kryptografisch sicheren pseudo-zufälligen Funktion abgeleitet. Diese Schlüssel werden in Verschlüsselungs- und Authentifikationsmechanismen eingesetzt.

SRTP verringert die Gefahr einer Kryptoanalyse, indem es eine zeitliche Aktualisierung von Master- und Sitzungsschlüsseln ermöglicht.

Verschlüsselung

SRTP definiert zwei symmetrische Verschlüsselungstransformationen auf Basis von Advanced Encryption Standard (AES): AES-CTR und AES-f8, die aus dem jeweiligen SRTP Paketindex und dem Sitzungsschlüssel k_e eine pseudo-zufällige Bitfolge erzeugen. Diese Bitfolge wird mit der RTP-Nutzlast durch XOR-Summe vermischt und damit eine sichere One-Time-Pad-Verschlüsselung erzeugt.

Im AES-CTR Modus wird die pseudo-zufällige Bitfolge durch die Konkatenation der mit AES unter Verwendung des Sitzungsschlüssels k_e verschlüsselten 128-Bit Blöcke, der Summe des Initialisierungvektors IV und der Blocknummer gebildet.

Im AES-f8 Modus ergibt sich die pseudo-zufällige Bitfolge aus der Konkatenation der mit AES unter Verwendung des Sitzungsschlüssels k_e verschlüsselten 128-Bit Blöcken der XOR-Summe des maskierten Initialisierungsvektors IV', der Blocknummer und der Verschlüsselung des Vorgängerblocks. AES-f8 Modus ist in SRTP optional und für UMTS-Übertragung vorgesehen. Für VoIP ist demnach AES-CTR Modus von Interesse.

Symmetrische Verschlüsselungsverfahren, wie AES sind deutlich effizienter als die asymmetrischen Verfahren und somit besonders gut für latenzkritische Anwendungen geeignet, zu denen auch IP-Telefonie gehört. Demnach kann SRTP für End-to-End und Hop-by-Hop Verschlüsselung von IP-Telefonaten eingesetzt werden.

Mathematische Berechnungen in AES sowie Berechnungen der XOR-Summen können besonders effizient in Hardwarekomponenten realisiert werden. IP-Telefone und mobile IP-Telefone, die generell weniger Rechenleistung als die auf einem Computer installierten Softphones haben, können von SRTP zusätzlich profitieren, wenn ihre Hardwarekomponenten die mathematischen Berechnungen übernehmen werden.

Die RTP-Header werden in SRTP Nachrichten unverschlüsselt versendet und können somit verlustfrei komprimiert werden. Damit kann die Bandbreite für die sichere IP-Telefonie reduziert werden.

Authentifikation und Integrität

Authentifikation und Intergrität von RTP-Nachrichten wird in SRTP mittels der HMAC-SHA1-Transformation mit dem Sitzungsschlüssel k_a realisiert. Dabei beträgt die empfohlene Länge des übertragenen Fingerabdrucks 80 Bits. Demnach muss der 160-Bits lange Fingerabdruck aus HMAC-SHA1 auf 80 Bits reduziert werden. Diese Anpassung verringert zwar die Übertragungsgröße von SRTP-Paketen, steigert aber das Kollisionsrisiko von Fingerabdrücken und schwächt somit den Intergritätsschutz der Nachrichten. Zudem ist der zukünftige Einsatz von HMAC-SHA1 bedenklich, seitdem die Schwächen der Hashfunktion SHA1 bekannt geworden sind [WYY05]. Es gibt zwar andere Hashfunktionen (z. B., SHA-256), die SHA1 nach zusätzlicher Anpassung der Schlüsselgröße in HMAC-SHA1 ersetzen können, aber sie sind noch nicht standardisiert.

Durch Kombination mit der Verschlüsselung kann SRTP eine gleichzeitige Vertraulichkeit, Authentifikation und Intergrität von RTP-Nachrichten gewährleisten. Laut [BeNa00] ist dabei die sicherste und auch effizienteste Methode die RTP-Nutzlast zunächst zu verschlüsseln und dann den Fingerabdruck von den verschlüsselten Daten zu erstellen.

SRTP erlaubt eine schwächere Authentifikation (z. B., 32 Bits) bzw. gar keine Authentifikation von Nachrichten für Anwendungen, bei denen es unwahrscheinlich ist, dass der Angreifer eine verschlüsselte Nachricht so manipulieren kann, dass eine spätere Entschlüsselung eine sinnvolle Nachricht liefern wird. Die bei einem VoIP-Telefongespräch übertragenen RTP-Pakete können ohne Authentifikation und Integritätsschutz auskommen, wenn die Stimme des Gesprächspartners und der Gesprächsinhalt über die Richtigkeit der übertragenen Daten Aufschluss geben können. Dennoch ist die Authentifikation von RTCP-Nachrichten notwendig, weil damit die laufende RTP-Verbindung koordiniert wird. Aufgrund der symmetrischen Verschlüsselungstechnik ist keine Authentifikation des Senders und damit auch keine Nicht-Abstreitbarkeit gewährleistet. Die Nicht-Abstreitbarkeit kann in IP-Telefonie zwar mittels Sprachanalyse nachgewiesen werden, doch die fehlende Senderauthentifikation kann besonders in IP-Telefonie mit mehreren Teilnehmern Probleme bereiten. Der Einsatz von digitalen Signaturen zur Gewährleistung von Senderauthentifikation und Nicht-Abstreitbarkeit wird in SRTP-Spezifikation wegen Effizienzverlust verworfen.

Schutz gegen „Replay"-Angriffe

SRTP bietet Schutz gegen „Replay"-Angriffe, bei denen ein Angreifer abgefangene RTP- oder RTCP-Pakete speichert und diese später wieder verschickt. „Replay"-Angriffe können unter anderem DoS-Attacken verursachen. Voraussetzung für den Schutz gegen „Replay"-Angriffe ist ein vorhandener Integritätsschutz und Nachrichten-Authentifikation. Der Empfänger von SRTP-Paketen führt eine so genannte „Replay"-Liste, die Indices von vorher empfangenen authentischen Paketen enthält. Die maximal mögliche Anzahl der gespeicherten Indices muss vorher festgelegt werden. Beim Empfang

eines neuen Pakets wird diese Liste auf Kollisionen untersucht und die wiederholten Pakete werden verworfen. Bei IP-Telefonen, die einen geringeren Speicher besitzen, ist die Länge der „Replay"-Liste ein Sicherheitsparameter, der mit Hinblick auf die gewünschte Sicherheit optimal gewählt werden soll.

SRTP-Schlüsselmanagement mit MIKEY

MIKEY, standardisiert in [RFC3830] von der Arbeitsgruppe IETF MSEC, beschreibt das Schlüsselmanagement für die Echtzeit-Multimedia-Kommunikation und ermöglicht den Austausch von Schlüsseln, genannt Transport Encryption Key (TEK) und Transport Generation Key (TGK), sowie weiteren Sicherheitsparametern (Data Security Association) zwischen den Teilnehmern. Der Einsatz von MIKEY umfasst Peer-to-Peer, One-to-Many und kleinere Many-to-Many Kommunikationsszenarien. Der Austausch läuft in zwei Kommunikationsrunden ab und ist daher für Echtzeit-Anwendungen, wie IP-Telefonie besonders geeignet. Der Schlüsselaustausch in MIKEY kann, in Hinblick auf VoIP, auf folgende drei Arten vollzogen werden:

- Teilnehmer verfügen über ein vorher festgelegtes gemeinsames Geheimnis, mit dem sie unabhängig von einander Schlüssel für Geheimhaltung und Authentifikation mittels einer pseudo-zufälligen Funktion ableiten können. Der Anrufer übermittelt den gewählten TGK verschlüsselt und authentisch an den Angerufenen, der mit einer authentischen Bestätigung antwortet. Beide Teilnehmer leiten den TEK aus dem TGK ab.
- Der Anrufer wählt ein Envelope-Key k_env und leitet daraus Schlüsse, mit denen er die TGK an den Angerufenen verschlüsselt und authentisch übermittelt, ab. k_env wird an den Angerufenen ebenfalls authentisch und mit dessen öffentlichem Schlüssel verschlüsselt übertragen. Der Angerufene sendet eine authentische Bestätigung. Beide Teilnehmer leiten den TEK aus dem TGK.
- Teilnehmer führen das Diffie-Hellman Schlüsselaustausch-Protokoll und bestimmen den TGK. Die notwendigen Parameter (z. B. mathematische Gruppenbeschreibungen) werden von dem Anrufer zuvor an den Angerufenen übermittelt. Beide Teilnehmer leiten den TEK aus dem TGK ab.

Prinzipiell gibt es eine vierte Möglichkeit den TEK zu vereinbaren. Sie basiert auf einem vereinfachten Diffie-Hellman Schlüsselaustausch-Protokoll unter Verwendung eines vorher festgelegten gemeinsamen Geheimnisses zusammen mit einer pseudo-zufälligen Funktion (MIKEY-DHHMAC). MIKEY-DHHMAC befindet sich aber noch im Entwicklungsstadium und ist nicht standardisiert.

Nachdem Teilnehmer den TEK vereinbart haben, können sie mit symmetrischer Verschlüsselung weitere Sicherheitsparameter für den Kommunikationsprotokoll (z. B., SRTP) austauschen. In VoIP kann MIKEY somit für den Austausch des Masterschlüssels k_m und weiteren Sicherheitsparametern benutzt werden, um eine sichere SRTP-Übertragung zwischen den Endgeräten zu ermöglichen. Dabei ist der TEK aus dem MIKEY-Paket der Masterschlüssel k_m. Durch die zeitliche Aktualisierung von TEKs ermöglicht MIKEY auch die zeitliche Aktualisierung von Masterschlüsseln in SRTP.

MIKEY ist unabhängig von dem darunterliegenden Signalisierungsprotokoll, wie H.323 oder SIP. Somit kann eine sichere Verbindung auch zwischen den Geräten realisiert werden, die nur einen von diesen Protokollen unterstützen. Zudem untersützt MIKEY einen parallelen Austausch von Schlüsseln und Sicherheitsparametern für unterschiedliche Kommunikationssitzungen und Kommunikationsprotokolle. Demnach ist es möglich RTP- und RTCP-Verbindungen getrennt von einander abzusichern. Mit dem Bündelungskonzept von Kommunikationssitzungen erlaubt MIKEY einen gemeinsamen TEK für mehrere parallellaufende Sitzungen zu benutzen. Somit können, z. B., VoIP-Konferenzen effizienter abgesichert werden.

4.5.3 IPSec

Einführung

„IPSec“ ist die Abkürzung für eine Reihe von Standards, die von der IP Security (IPSec) Working Group [IPSec] der IETF erarbeitet wurden [Sch05]. Diesen RFCs liegt ein wohldurchdachter Ansatz zugrunde, mit dem das komplexe Problem der Absicherung eines Netzwerkes (das viel schwieriger ist als die Absicherung einer Client-Server-Verbindung) überzeugend gelöst wurde. IPSec hat noch Ecken und Kanten, z. B. was den Umgang mit Zertifikaten und das Zusammenspiel mit Network Address Translation (NAT) Gateways betrifft, wird aber heute von allen Herstellern von Netzwerkequipment angeboten.

IPSec beschreibt Datenformate zur Verschlüsselung (ESP) und Authentisierung (AH, ESP) von IP-Paketen, und das Schlüsselmanagement.

Die wichtigste Idee in den IPSec-Standards [IPSec] ist, im Header nur die minimal notwendige Information unterzubringen, die eine Entschlüsselung und ggf. die Überprüfung eines MAC erlaubt.

Diese minimale Information ist einfach ein *Verweis* auf einen Datei- oder Datenbankeintrag, der alle benötigten Informationen enthält. Dieser Verweis ist 32 Bit lang und wird „*Security Parameters Index (SPI)*“ genannt. Ansonsten enthalten die IPSec-Header keinerlei kryptographischen Informationen (ausgenommen natürlich eines evtl. vorhandenen MAC). Zusammen mit der IP-Zieladresse und dem Sicherheitsprotokoll (ESP oder AH) ist er eine eindeutige Referenz auf eine Menge von kryptographischen Parameter und Algorithmen, die zur Verarbeitung des Pakets benötigt werden.

Jede solche Menge wird als „Security Association (SA)“ bezeichnet. Die SAs werden bei IPSec in einer „Security Association Database (SAD)“ verwaltet, die während des Betriebs meist im Hauptspeicher abgelegt ist.

Eine typische IPSec-Implementierung besteht aus einer Reihe von Software-Modulen, die in Abbildung 4.13 wiedergegeben sind. Die Funktionsweise dieser Module wird in den nachfolgenden Abschnitten näher erläutert. Hier soll zunächst einmal ein grober Überblick über die Funktionsweise gegeben werden.

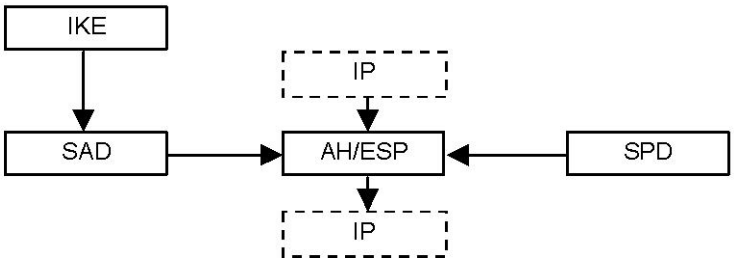

Abbildung 4.13 Blockstruktur einer IPSec-Implementierung.

Am schwierigsten zu implementieren ist das AH/ESP-Modul, da es sich in die Verarbeitung von IP-Paketen durch die Netzwerksoftware des Betriebssystems zwischenschalten muss. Aufgaben dieses Moduls sind:

- eingehende IPSec-geschützte Pakete zu entschlüsseln, zu überprüfen und als „normale“ IP-Pakete wieder an die Netzwerksoftware zu übergeben, und
- ausgehende IP-Pakete nach den Vorgaben des Netzwerkadministrators
  - unverändert durchzulassen,
  - zu verschlüsseln,
  - zu authentisieren oder
  - zu verwerfen.

Die zur Durchführung dieser Aufgaben benötigten Angaben zu kryptographischen Algorithmen und Parametern holt dieses Modul sich aus dem SAD-Modul, wobei IP-Zieladresse, IPSec-Protokoll und SPI als Referenzen dienen.

Die Einträge in der SAD werden bei IPSec mit dem Schlüsselaustauschprotokoll IKE („Internet Key Exchange“) ausgehandelt, wobei IKE in verschiedenen Public-Key-Varianten oder im „preshared secret“-Modus betrieben werden kann.

Was mit ausgehenden IP-Paketen geschehen soll, ist in der „Security Policy Database (SPD)“ beschrieben. Auch hier ist nicht unbedingt eine Datenbank gefordert, sondern die Regeln können z. B. auch in Form einer Routing-Tabelle realisiert werden, bei denen die zu verschlüsselnden IP-Pakete auf das Netzwerk-Interface des AH/ESP-Moduls geroutet werden. Bei einfachen IPSec-Implementierungen mit einer überschaubaren Zahl von Regeln wird die SPD meist in einer Konfigurationsdatei gespeichert.

Die einfachste Möglichkeit, IPSec einzusetzen, besteht darin, lokale Netzwerke durch IPSec geschützt über das Internet zu verbinden. Viele Firmen haben von dieser Möglichkeit schon Gebrauch gemacht, um die Netze an den verschiedenen Standorten kostengünstig zu verbinden. Dabei blieb die Struktur des Gesamtnetzes weitgehend erhalten, denn auch vorher mussten die verschiedenen Standorte über Datenleitungen miteinander verbunden werden.

Ein privates Netz, das aus lokalen Netzwerken an den verschiedenen Standorten und gemieteten (privaten) Standleitungen (ATM, Frame Relay) bestand, wurde zu einem virtuellen privaten Netz (VPN), indem die privaten Standleitungen durch virtuelle Datenkanäle im Internet ersetzt wurden: Die mit IPSec geschützten Pakete passieren hier das öffentlich zugängliche Internet, aber niemand im Internet kann sie lesen oder fälschen.

VPN-Lösungen werden vor allen Dingen wegen der damit verbundenen Kostenersparnisse und der größeren Flexibilität eingesetzt: Benötigt man bei einem privaten Netz zur Verbindung von n Standorten n(n-1)/2 Standleitungen (wenn man nicht den gesamten Datenverkehr über zentrale Knoten führen will), so braucht man bei einem VPN nur n Zugänge zum Internet.

Unter dem Schlagwort „VPN“ werden die verschiedensten Techniken zum Ersatz von Standleitungen durch das Internet angeboten. Eine dieser Möglichkeiten ist der IPSec Tunnelmodus, der als positiven Nebeneffekt die Daten noch kryptographisch absichert. Man kann IPSec auch dazu benutzen die Pakete anderer Tunnelprotokolle kryptographisch zu sichern, z. B. IPSec over L2TP [RFC 2888]. IPSec wird zum kryptographischen Schutz von VPN-Verbindungen gerne benutzt, weil es im Gegensatz zu anderen Techniken öffentlich diskutiert und akzeptiert ist.

Die zweite Möglichkeit besticht ebenfalls durch Kostenersparnis im geschäftlichen Umfeld: Musste ein Außendienstmitarbeiter sich bislang direkt über eine Telefonverbindung (im Extremfall eine internationale Verbindung) in das Firmennetz einwählen, um auf seine Ressourcen (E-Mail, Terminkalender, Software) zuzugreifen, so kann er sich mit IPSec einfach lokal bei einem Internet Service Provider einwählen, und die IP-Kommunikation mit dem Firmennetz wird mit IPSec geschützt.

Weniger häufig, weil in großem Stil schwerer zu realisieren, ist die direkte Verbindung zweier Hosts über IPSec. Sie ist nichtsdestotrotz möglich und kann z. B. im privaten Bereich mit den unten beschriebenen Softwarelösungen realisiert werden.

IPSec-Datenformate (AH vs. ESP, Transport- vs. Tunnelmodus)

Eine eindeutige Formatierungsvorschrift, wie aus einem gegebenen ungeschützten Datenformat ein geschütztes gebildet und später wieder zurück transformiert wird, ist das Kernstück jedes Sicherheitsstandards. Für IPSec wurden zwei Formate spezifiziert:

- der Authentication Header (AH) zum Schutz der Integrität eines IP-Pakets, und
- das Encapsulation Security Payload (ESP) zum Schutz der Vertraulichkeit und Integrität.

Darüber hinaus wird unterschieden, welche Daten geschützt werden sollen:

- Transport Mode: Nur die Nutzlast des IP-Pakets, z. B. der TCP-Header und die Daten, werden geschützt. Dieser Modus kann nur bei der dritten Einsatzmöglichkeit, der direkten Host-Host-Kopplung eingesetzt werden.
- Tunnel Mode: Hier wird das gesamte IP-Paket als Datum betrachtet, geschützt und als Nutzlast in ein neues IP-Paket eingefügt.

Somit ergeben sich insgesamt vier verschiedene Datenformate, von denen ESP im Tunnelmodus zweifellos das wichtigste ist.

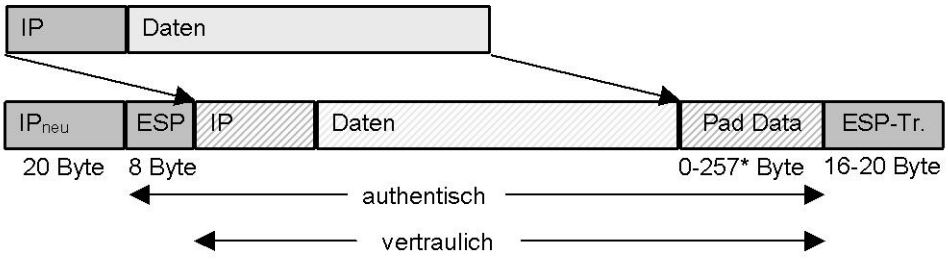

Abbildung 4.14 IPSec ESP im Tunnel-Modus. (* Pad Data besteht aus den Padding-Daten plus die Padding-Längenangabe und dem Next Header-Feld)

Schlüsselmanagement

Das Schlüsselmanagement ist in der IPSec-Architektur eine völlig unabhängige Anwendung, die in der Regel eine nicht IPSec-geschützte TCP/IP oder UDP/IP-Verbindung nutzt. Sie wird normalerweise vom AH- oder ESP-Modul gestartet, wenn eine benötigte SA noch nicht zur Verfügung steht.

In den aktuellen IPSec-Implementierungen ist das Internet Key Exchange Protocol (IKE) [RFC 2409] für das Schlüsselmanagement zuständig. IKE hat eine lange Geschichte, und sie ist noch nicht abgeschlossen. Ein Nachfolger ist unter der Bezeichnung IKEv2 „Approved as a Proposed Standard“ zu finden [IKEv2].

Um das Schlüsselmanagement für IPSec implementieren zu können, muss man folgende Standards berücksichtigen:

- RFC 2412 OAKLEY Key Determination Protocol: Hier wird, in unzähligen Varianten, beschrieben, wie man auf Basis des Diffie-Hellman-Schlüsselaustauschs authentisch einen gemeinsamen Schlüssel vereinbaren kann.
- RFC 2407 Internet IP Security Domain of Interpretation for ISAKMP Proposed standard und RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP): Hier werden Datenformate für den Schlüsselaustausch vorgegeben. Dies ist der bei weitem umfangreichste und komplizierteste Standard, weil hier ursprünglich ein Rahmen für alle möglichen Schlüsselaustauschverfahren im Internet (also auch z. B. SSL und S/MIME) geschaffen werden sollte.
- RFC 2409 Internet Key Exchange (IKE): Hier wird beschrieben, welche Teile der vorangegangenen RFCs denn jetzt zu Standard gehören.

Der Internet Key Exchange (IKE) [RFC 2409] füllt also das von ISAKMP vorgegebene Gerüst mit Leben, indem die Protokolle aus OAKLEY den verschiedenen Phasen von ISAKMP zugeordnet und um Konstrukte aus SKEME ergänzt werden.

Um eine implementierbare Spezifikation zu erhalten, macht IKE außerdem zahlreiche Einschränkungen, die die vielen unübersichtlichen Möglichkeiten von ISAKMP und OAKLEY deutlich einschränken:

- In ISAKMP Phase 1, in der eine SA für das ISAKMP-Protokoll selbst ausgehandelt wird, dürfen IKE Main Mode (sechs Nachrichten) oder Aggressive Mode (drei Nachrichten) verwendet werden. Main Mode muss dabei von jeder IKE-Implementierung unterstützt werden, Aggressive Mode kann auch entfallen.

- Es gibt vier Paare von Main Mode/Aggressive Mode-Protokollen, die sich durch die Art der Authentisierung unterscheiden: Hier können digitale Signaturen, Public Key-Verschlüsselung (in zwei Varianten) oder vorher ausgetauschte symmetrische Schlüssel („Preshared Keys“) zum Einsatz kommen.
- Um auch im Aggressive Mode die Identität von Initiator und Responder schützen zu können, wurde die Methode der Public-Key-Verschlüsselung zur Authentikation von SKEME übernommen.
- In ISAKMP Phase 2, in der die SAs für IPSec AH oder ESP ausgehandelt werden, darf nur Quick Mode zum Einsatz kommen. Phase 2 ist bereits durch die ISAKMP SA geschützt, daher kann hier auf Main und Aggressive Mode verzichtet werden.
- Die schnelle Schlüsselerneuerungsmethode durch Austausch von Zufallswerten wurde ebenfalls von SKEME übernommen.

IKE wird nun an einem Beispiel erläutert, in dem digitale Signaturen zur Authentisierung verwendet werden. Für dieses Beispiel werden die folgenden Festlegungen getroffen:

- In Phase 1 wird der Main Mode benutzt, bei dem sechs Nachrichten ausgetauscht werden. Die beiden Parteien werden dabei durch Nutzer-basierte X.509-Zertifikate identifiziert, die keine IP-Adresse enthalten. Dadurch kann auch der Fall dynamisch zugewiesener IP-Adressen mit behandelt werden.
- In Phase 2 sollen Security Associations für IPSec ESP mit Verschlüsselung und Authentifikation ausgehandelt werden. Dafür wird der Quick Mode verwendet.

Phase 1: Aushandeln der ISAKMP-SA

Die sechs Nachrichten des IKE Main Mode können in drei Gruppen unterteilt werden:

- Nachrichten 1 und 2 handeln die Rahmenbedingungen für die SAs aus. Dazu gehört der Zweck der SA (für ISAKMP oder IPSec) und die kryptographischen Algorithmen. Außerdem verhindert der Einsatz von Cookies Denial-of-Service-Attacken. Diese beiden Nachrichten sind unverschlüsselt und nicht authentisiert.
- Mit Nachrichten 3 und 4 werden Zufallszahlen und Diffie-Hellman-Werte zwischen den beiden Partnern ausgetauscht. Mit diesen Werten kann der Schlüssel SKEYID berechnet werden. Diese beiden Nachrichten sind unverschlüsselt und nicht authentisiert.
- In den Nachrichten 5 und 6 werden mit digitalen Signaturen die Inhalte der früheren Nachrichten authentisiert. Sie enthalten in diesem Fall auch die (optionalen) Zertifikate zur Überprüfung dieser Signaturen. Diese Nachrichten sind durch die Algorithmen und den Schlüssel SKEYID geschützt.

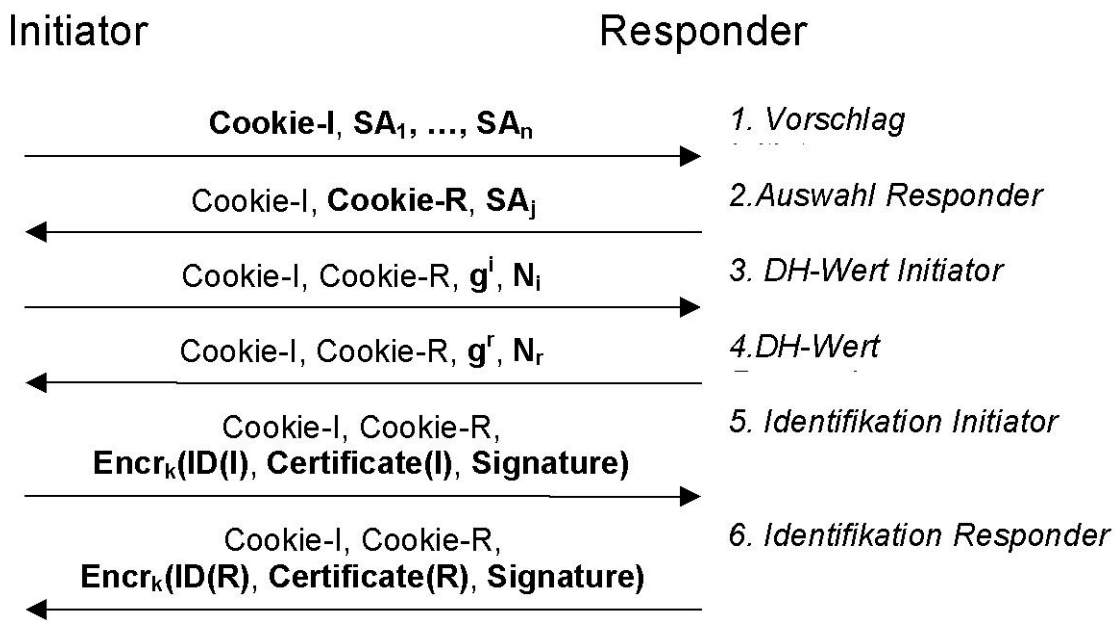

Abbildung 4.15 IKE Main Mode in 6 Nachrichten, Authentifizierung durch X.509-Zertifikat und digitale Signatur.

Phase 2: Aushandeln der SAs für IPSec ESP

In Phase 2 wird OAKLEY Quick Mode benutzt. In Abbildung 4.16 ist die Variante ohne Perfect Forward Secrecy angegeben. Man kann PFS erreichen, wenn in den Nachrichten 1 und 2 neue Diffie-Hellman-Werte in einem Key Exchange (KE)-Feld mit übertragen werden.

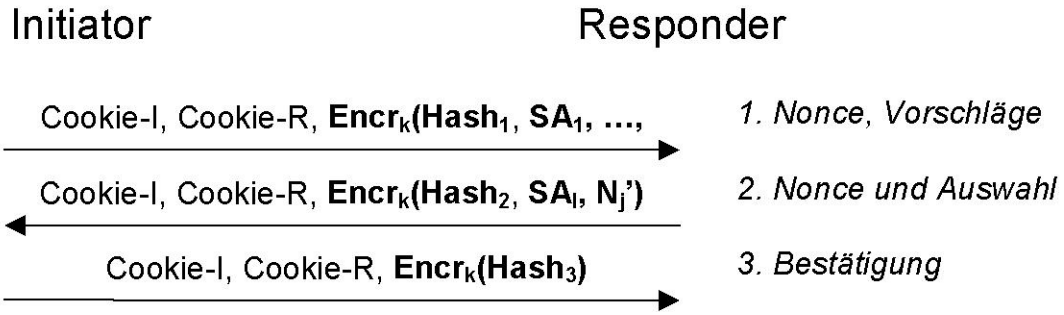

Abbildung 4.16 Der Quick Mode bei IKE. Hier werden keine Public-Key-Operationen benötigt.

Fazit

Das große Problem von IPSec ist das Schlüsselmanagement zur Authentisierung der Partner in IKE. Viele Anwender setzen zunächst sogenannte „Preshared Keys“ ein, d.h. in beide Endpunkte der IPSec-Verbindung muss jeweils der gleiche geheime Wert eingegeben werden. Dieser Wert wird nicht zur Verschlüsselung der Daten, sondern zur Authentisierung der beiden IKE-Peers genutzt. Dieser Ansatz beinhaltet jedoch einen erheblichen Administrationsaufwand sowie, beim Einsatz von schwachen Passwörtern als Preshared Keys, ein Sicherheitsrisiko und sollte daher vermieden werden.

Möchte man Zertifikate nach dem X.509-Standard einsetzen, so stößt man schnell an seine Grenzen: Unter werden gerade einmal vier Produkte genannt, die dies (interoperabel) unterstützen. Das VPN Consortium macht sich nicht einmal die Mühe, diese Interoperabilität zu testen (http://www.vpnc.org/testing.html).

IPSec in Call-Setup-Protokollen (H.323, SIP)

Da in Call-Setup-Protokollen in der Regel mindestens zwei Endgeräte und zwei Proxyserver über IPSec kommunizieren müssen, und da die Proxyserver in verschiedenen Domains und somit in unterschiedlicher administrativer Verantwortung liegen, kann IKE nur mit zertifikatsbasierter Authentifikation zum Einsatz kommen.

Gegen einen solchen Einsatz sprechen die seit langem bestehenden Interoperabilitätsprobleme auf diesem Gebiet.

IPSec wird in SIP wie folgt erwähnt: „Any deployment of IPSec for SIP would require an IPSec profile describing the protocol tools that would be required to secure SIP. No such profile is given in this document.“. Um einen wirkungsvollen Einsatz von IPSec mit SIP zu gewährleisten, wäre hier ein eigener Draft erforderlich. Auf der Webseite der SIP-WG ist aber kein solcher Draft zu finden.

IPSec zur Absicherung der Sprachdaten

Auch beim Einsatz von IPSec zur Absicherung der Übertragung der Sprachdaten treten Probleme auf. Eine exemplarische Untersuchung dazu findet man in [BBR02].

Folgende Randbedingungen müssen berücksichtigt werden:

- VoIP-Datenverkehr muss in Routern bevorzugt behandelt werden. Da bei IPSec der TCP bzw. UDP-Header immer verschlüsselt ist, muss diese Bevorzugung allein aus dem IP-Header ersichtlich sein. IPv4 hat hier gewisse Mängel, IPv6 sollte diese beheben.
- Das jetzige IKE benötigt 7 Handshake-Nachrichten, um einen Schlüssel zwischen zwei Hosts auszutauschen. Dies entspricht 3,5 Round-Tip-Times, IKEv2 liefert hier bessere Ergebnisse. Wird IKE erst duchgeführt, wenn die Verbindung etabliert ist und der Empfänger des Anrufs den Hörer abgenommen hat, so kann hier eine irritierende Wartezeit entstehen. Dies könnte durch einen IKE-Schlüsselaustausch während der RINGING-Phase vermieden werden.
- In Firmennetzen mit proprietärer Infrastruktur stellt das Interoperabilitätsproblem der IKE-Implementierungen im Bereich X.509-Zertifikate kein Problem dar, wohl aber bei Internet-weiten Lösungen. Eine Lösung mit Preshared Secrets kommt wegen der geringen Skalierbarkeit im Internet sowieso nicht in Betracht. Dieses Problem besteht sowohl für Gateway-basierte Lösungen (Tunnel Modus) als auch für Endgeräte-basierte Lösungen (Transport Modus).
- Da VoIP-Datenpackete nur zwischen 10 und 40 Byte Nutzlast enthalten, ist der Datenoverhead, der durch die 44-48 zusätzlichen Byte von ESP im Tunnelmodus erzeugt wird, signifikant [BBR02].
- Die Ver- und Entschlüsselung der Daten kann zur Erhöhung der Latenzzeit führen. In [BBR02] wurde eine Gateway-basierte Verschlüsselung mit DES und 3DES getestet.

Fazit

Zur Absicherung von SIP sind TLS oder S/MIME die bessere Wahl, IPSec sollte höchstens zur Absicherung der Sprachdaten eingesetzt werden. Da hierbei aber durch Verschlüsselung der UDP-Header QoS-Probleme auftreten können, ist SRTP die bessere Wahl.

5. Rahmenbedingungen und gesetzliche Vorschriften

Die gesetzlichen und regulatorischen Rahmenbestimmungen in der Telekommunikation in Deutschland werden maßgeblich durch das Telekommunikationsgesetz [TKG96], durch das Bundesdatenschutzgesetz [BDSG90] und bei Behörden meist durch weitere Dienstanweisungen vorgegeben. Nicht abschließend geklärt ist, in wie weit VoIP-Dienste als öffentlich zugängliche Telefondienste aufzufassen sind. In einem Eckpunktepapier vom 09.09.2005 hat die Bundesnetzagentur (www.bundesnetzagentur.de) 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.

5.1 Fernmeldegeheimnis und Datenschutz

Die wichtigsten Anforderungen für öffentlich zugängliche Telefondienste und für geschlossene Benutzergruppen öffentlicher Stellen sind in den §§ 88-107 TKG aufgeführt.

Danach darf der Anbieter von Telekommunikationsdiensten 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.

Die Sicherheitsmaßnahmen müssen in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen und werden üblicherweise in drei Schutzbereiche unterteilt (siehe Anhang Informationstruktur). Zu berücksichtigen ist dabei, dass die Verkehrsdaten und Inhalte der Gespräche dem Fernmeldegeheimnis unterliegen und daher besonders schützenswert sind.

Private Verkehrs- und Gesprächsdaten fallen unter den Schutzbereich 2, entsprechende Maßnahmen zur Gewährleistung der Vertraulichkeit sind daher unbedingt zu ergreifen.

Da die Verpflichtung zur Wahrung des Fernmeldegeheimnisses nicht nur für private, sondern auch für dienstliche Gespräche gilt, ist für einen Mitschnitt solcher Telefonate die Einwilligung der Teilnehmer erforderlich.. Das unbefugte Aufzeichnen von Gesprächen stellt bei VoIP-Systemen ein größeres Problem dar als bei herkömmlichen TK-System. Während beispielsweise die meisten TK-Systeme aus proprietärer Technik bestehen, ist die Installation von fremder Software zum Mitschnitt nicht ohne weiteres möglich, bzw. erfordert ein außerordentlich hohes Maß an Know-How. In der Betriebssoftware vorgesehene Mitschnittoptionen lassen sich dort üblicherweise abschalten bzw. überprüfen.

Daher ist sicher zu stellen, dass keine Aufzeichnungsmöglichkeiten auf den Middleware-Servern gegeben ist. Dies ist regelmäßig durch die IT-Sicherheitsbeauftragen zu überprüfen.

5.2 Technische Umsetzung von Überwachungsmaßnahmen

Die Überwachung von Telekommunikationssystemen nach den Anforderungen der Strafprozessordnung (§100a, §100b), dem Artikel-10 Gesetz (§3, §5, §8) sowie dem Zollfahndungsdienstgesetzes (§23a-23f, §45-46) wird in der Telekommuniktaionsüberwachungsverordnung [TKÜV97] geregelt.

Eine umfängliche Überwachung von VoIP-Verbindungen existiert derzeit nicht, und die technischen Möglichkeiten hierfür sind noch nicht abschließend bewertet. Die Bundesnetzagentur (früher Regulierungsbehörde für Post und Telekommikation (RegTP)) hat in ihrer im Frühjahr 2005 bei VoIP-Anbietern durchgeführten Umfrage hierauf Bezug genommen.

5.3 Notruf

Eine wichtige Anforderung bei der Bereitstellung öffentliche zugänglicher Telefoniedienste ist die Einrichtung von jederzeit zugänglichen Notrufnummern. Schwierigkeiten bestehen in der Lokalisierung und Identifizierung eingehender Notrufe, so dass derzeit keine zufriedenstellende Lösung existiert.

6. Einsatzszenarien und Maßnahmenempfehlungen

In diesem Kapitel werden beispielhaft typische Einsatzszenarien von VoIP beschrieben. Diese Beispiele spiegeln weder eine generische Vorgehensweise wieder, noch können sie als umfassende oder abschließende Sicherheitsbetrachtung aufgefasst werden. Sie können aber hilfreiche Anhaltspunke liefern, den eigenen Schutzbedarf zu ermitteln und damit geeignete Sicherheitsmaßnahmen umzusetzen.

6.1 Home-Office (Anschluss über ein öffentliches IP-Netz)

Einsatzszenario

Betrachtet wird folgendes Einsatzszenario: Ein Heimarbeitsplatz soll über ein öffentliches IP-Netz an das Telefoniesystem eines Unternehmens oder einer Behörde angeschlossen werden. Der Heimarbeitsplatz ist dabei über einen Internetanschluss mittlerer Bandbreite (z. B. ADSL) mit dem öffentlichen IP-Netz verbunden. Der Internetanschluss wird auch für den Datenaustausch am Heimarbeitsplatz genutzt. Der Internetanschluss und der Heimarbeitsplatz werden nur von einem Mitarbeiter genutzt (keine Mehrfachnutzung).

Anforderungsprofil

Verfügbarkeit: Ein kurzzeitiger Ausfall (Größenordnung: Stunden) der telefonischen Erreichbarkeit des Mitarbeiters am Heimarbeitsplatz wird als hinnehmbar eingestuft. Die Sprachqualität der Verbindung muss eine problemlose, verständliche Sprachkommunikation ermöglichen; dabei muss allerdings die Qualität einer ISDN-Verbindung nicht zwingend erreicht werden (mindestens GSM-Qualität).

Vertraulichkeit: Inhalt und Verbindungsdaten sind gegenüber Außenstehenden vertraulich zu halten. Private Gespräche werden nicht über den VoIP-Anschluss des Heimarbeitsplatzes abgewickelt.

Integrität/Authentizität: Sowohl der missbräuchliche Zugang zum firmeninternen Telefonienetz als auch die Nutzung der externen Leitungen (Gebührenmissbrauch, Imageschaden) ist auszuschließen.

Damit kann in diesem Einsatzszenario von einem Sicherheitsbedarf der Schutzklasse 1 gering/mittel ausgegangen werden.

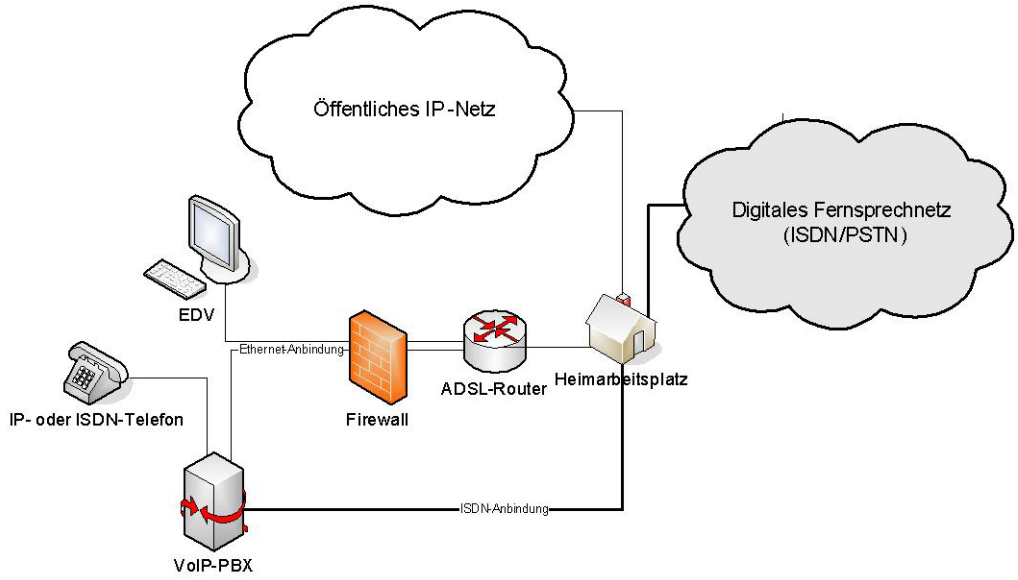

Abbildung 6.1 Einsatzbeispiel Home-Office

Maßnahmen

Komponente	Grundwert	Schutzbedarf	Maßnahme
IP-Telefone/VoIP-PBX	Vertraulichkeit	hoch	Verschlüsselung mittels SRTP
IP-Telefone/VoIP-PBX	Vertraulichkeit	hoch	Schlüsselaustausch mittels MIKEY oder durch Verschlüsselung der Signalisierung
IP-Telefone/VoIP-PBX	Integrität	hoch	Starke Authentikation zur Anmeldung des Heimarbeitsplatzes am zentralen VoIP-System des Unternehmens/Behörde. (z. B. Zertifikat-basiert mittels TLS/https)
Außenanbindung	Verfügbarkeit	mittel	Redundante Außenanbindung; z. B. durch VoIP-Gateway mit Anschluss an das PSTN-Netz. Diese soll die Erreichbarkeit auch bei Ausfall/Überlastung des IP-Anschlusses gewährleisten.
Firewall	Verfügbarkeit/ Integrität/ Vertraulichkeit	Mittel	Einrichtung einer Firewall zwischen Router und IP-Telefon/IP-PBX. Diese soll direkte Angriffe aus dem öffentlichen IP-Netz erschweren.
Firewall	Verfügbarkeit	hoch	Beachtung der Problematik von NAT-Firewalls (siehe Kapitel 4.2.4).
ADSL-Router	Verfügbarkeit	Niedrig	Ggf. ist ein Router mit Traffic-Shaping einzusetzen, um Sprachverbindungen zu priorisieren. Damit kann verhindern werden, dass durch kurzzeitige Bursts (z. B. durch einen Download verursacht), laufende Sprachverbindungen gestört oder unterbrochen werden.

Tabelle 6.1: Maßnahmenkatalog Home-Office

Anmerkungen

Grundsätzlich ist die direkte Anbindung eines IP-Telefons an den Heimarbeitsplatz-Router möglich. Empfehlenswert ist der Einsatz einer entsprechenden VoIP-PBX, durch die die Sicherheit und Verlässlichkeit des Gesamtsystems erhöht werden kann.

Geeignete VoIP-PBX Kompakt-Systeme unterstützen beispielsweise meist ein breiteres Spektrum an Sicherheitsprotokollen, können an das ISDN-Netz angebunden werden und ermöglichen beispielsweise eine automatische Umschaltung auf eine ISDN-Verbindung bei schlechter Qualität der IP-Verbindung. Auch die Auswahl der Endgeräte ist deutlich breiter, es können meist beliebige ISDN-, analog als auch IP-Endgeräte betrieben werden, ohne dass diese bestimmte Sicherheitsfunktionalitäten anbieten müssen.

Der Einsatz eines Routers mit integrierter VPN-Funktionalität ist möglich, aufgrund der Auswirkungen auf das QoS jedoch nicht zu empfehlen. Bisherige Erfahrungswerte mit VPN-Gateways zeigen, dass insbesondere bei Verbindungen über mittelbandige Zugänge (z. B. ADSL) im Allgemeinen keine dauerhaften Verbindungen mit akzeptabler Qualität erreicht werden können.

6.2 Mittlere Unternehmens- und Behördennetze (VoIP im Tertiärbereich)

Einsatzszenario

Wir betrachten folgendes Einsatzszenario: Eine mittlere Behörde oder ein mittelständisches Unternehmen mit rund 200 Mitarbeitern will seine Telefonie vollständig auf IP migrieren. Der

Anschluss an das öffentliche Fernsprechnetz soll weiterhin über konventionelle ISDN-Anschlüsse (S_0 und S_2M) erfolgen. Der Standort verfügt über eine dauerhafte symmetrische Internetbreitbandanbindung. Im Endgeräte-Bereich kommen IP-Telefone zum Einsatz, die Anbindung der Telefax-Geräte erfolgt über entsprechende Analog-Adapter.

Neben den Standard-Telefoniefunktionen soll das Telekommunikationssystem mit einem Unified-Messaging System ausgestattet werden.

Anforderungen

Verfügbarkeit: Für die Verfügbarkeit des Telefoniesystems werden die Anforderungen zugrunde gelegt, die in der Schutzbedarfsfeststellung für das bisherige TK-System verankert worden sind. D.h. eine maximale Ausfalldauer der Zentraletechnik von <0,5h pro Jahr bei maximal 3 Vorfällen kann geduldet werden. Für die Endgeräte gilt eine maximale Ausfalldauer von <1h bei 10 Vorfällen im Jahr. Notrufmöglichkeiten sind einzurichten und deren Verfügbarkeit zu gewährleisten.

Interne Angriffe auf die Verfügbarkeit des Telefoniesystems, die mit einfachen Mitteln durchgeführt werden sowie externe Angriffe, die mit qualifizierten Mitteln durchgeführt werden, sollen ausgeschlossen werden.

Die Sprachqualität soll gegenüber den bisherigen ISDN-Verbindungen keine wesentlichen Qualitätsnachteile mit sich bringen. Die Sprachqualität ist unabhängig von einem möglichen Aufkommen im Datennetz zu gewährleisten.

Vertraulichkeit: Das Telefoniesystem darf von den Mitarbeitern zu privaten Zwecken genutzt werden, die anfallenden privaten Verbindungsdaten sind auch gegenüber internen Vorgesetzten vertraulich zu halten. Die Vertraulichkeit der Gesprächsinhalte ist vor Angreifern, die über qualifizierte Mittel verfügen, zu gewährleisten.

Integrität/Authentizität: Manipulationsangriffe, die mit qualifizierten Mitteln durchgeführt werden, sind auszuschließen. Dies umfasst Manipulationen mit dem Ziel des Gebührenbetruges und des Imageschadens durch gefälschte Absenderrufnummern.

Damit kann in diesem Einsatzszenario von einem Sicherheitsbedarf der Schutzklasse 2 hoch ausgegangen werden.

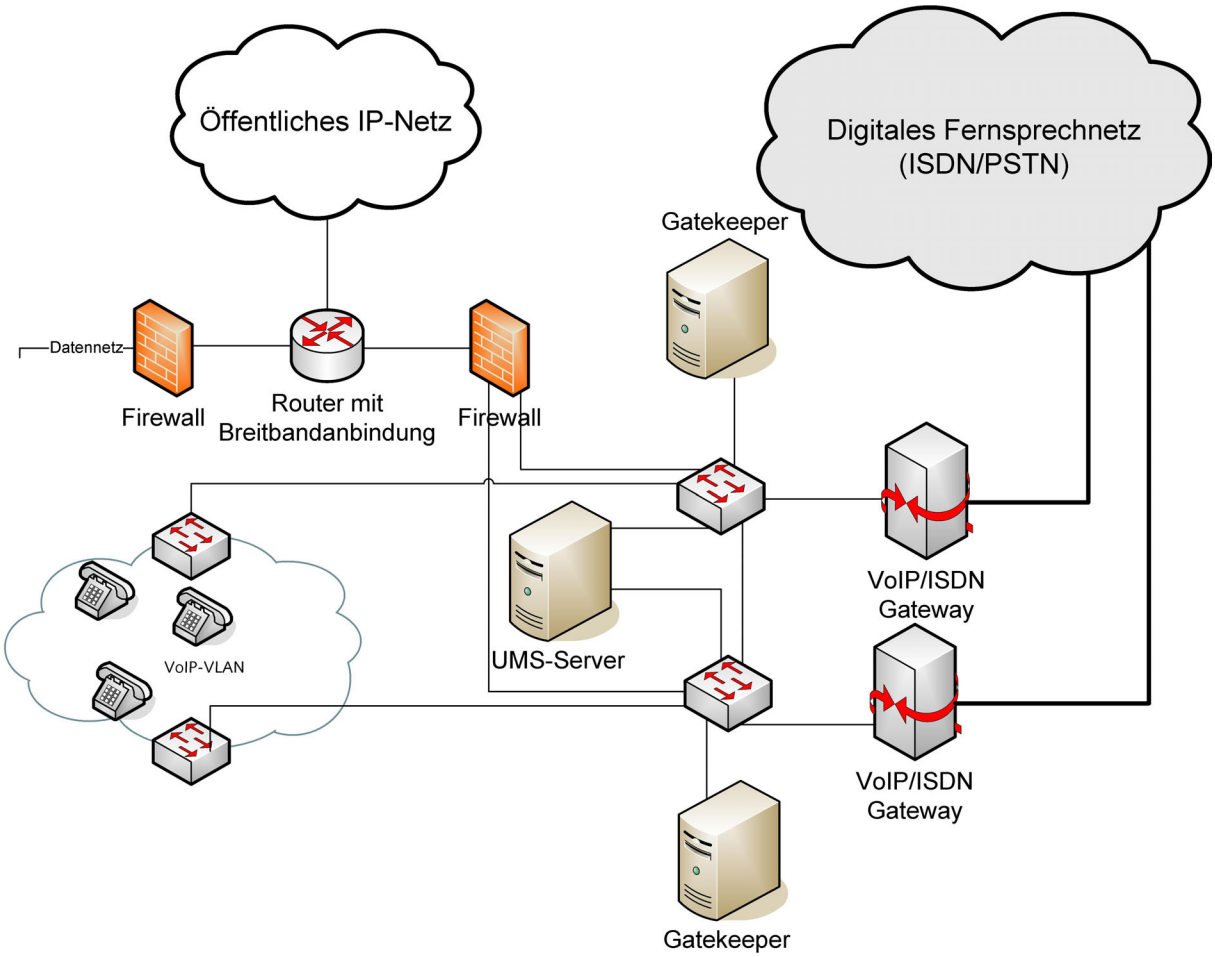

Abbildung 6.2 Einsatzbeispiel VoIP in Telefonieanwendungen mittlerer Göße

Maßnahmen

Komponente	Grundwert	Schutz-bedarf	Maßnahme
Switche/Verkabelung	Integrität	mittel	Physikalischer Schutz der Betriebsräume. Protokollierung des Zutritts.
Kabeltrassen, Räume mit VoIP-Komponenten	Verfügbarkeit	mittel	Sicherungsmaßnahmen gegen Feuer und Wasserschaden, die gewährleisten sollen, dass der Betrieb des zentralen Kommunikationssystems auch in Notfallsituationen zumindest temporär erhalten bleibt. Überspannungsschutz.
IP-Telefone/Switche	Verfügbarkeit	hoch	Versorgung der Endgeräte durch PoE.
Switche/Repeater	Verfügbarkeit	hoch	USV zur Aufrechterhaltung der Übertragungswege.
Zentrale VoIP-Middleware	Verfügbarkeit	hoch	USV zur Aufrechterhaltung der zentralen VoIP-Komponenten. Hierzu zählen der Gatekeeper (Aufrechterhaltung der internen Kommunikationsmöglichkeit) sowie des Gateways in das öffentliche Fernsprechnetz. Aufrechterhaltung der Serverfunktionen bei Totalausfall der Stromversorgung in der Größenordnung von 4h.
Switch/Router	Verfügbarkeit/ Integrität	mittel	Trennung von Sprach- und Datennetz: Aufteilung des Netzwerks in mehrere Broadcast-Domänen (VLANs). Die Verbindung der verschiedenen VLANs erfolgt über eine Firewall bzw. Router mit Layer3-Filter.
Switche/Router	Verfügbarkeit/	hoch	Maßnahmen gegen ARP-Spoofing (siehe Kapitel 4.2

Komponente	Grundwert	Schutz-bedarf	Maßnahme
	Integrität/ Vertraulichkeit		[5])
Switche/Router, VoIP-Middleware, IP-Telefone	Verfügbarkeit/ Integrität	Hoch	Maßnahmen gegen DHCP-Angriffe
Switche/Router	Verfügbarkeit/ Integrität/ Vertraulichkeit	hoch	Maßnahmen gegen VLAN-Angriffe, zusätzich Strukturierung der VLANs in „Producing VLAN“ (Server) und „Consuming VLAN“ (IP-Endgeräte).
Gateway in das öffentliche IP-Netz	Integrität/ Vertraulichkeit	hoch	Das VoIP-Gateway, das die interne VoIP-Infrastruktur mit dem öffentlichen IP-Netz verbindet ist durch eine Firewall zu sichern. Der externe Zugriff ist auf die benötigten VoIP-Ports des Gatekeepers zu beschränken.
Gatekeeper	Verfügbarkeit	hoch	Redundantes System mit automatischer oder halbautomatischer Funktionsübernahme nach Ausfall. Fortlaufende Spiegelung der Konfigurationsdatenbank.
Gateway in das öffentliche Netz	Verfügbarkeit	mittel	Redundantes System, mit automatischer oder halbautomatischer Funktionsübernahme nach Ausfall.
IP-Telefone	Vertraulichkeit	mittel	Verschlüsselung mittels SRTP
IP-Telefone	Vertraulichkeit	mittel	Verschlüsselung des Schlüsselaustausch mittels MIKEY oder durch Verschlüsselung der Signalisierung
VoIP-Middleware	Integrität	Hoch	Server-Systeme sollten nur als Minimalsystem installiert und konfiguriert sein. Einsatz eines gehärteten Betriebssystems.
VoIP-Middleware	Integrität	Hoch	Administrativer Zugang zu den Serversystemen ist zu beschränken. Administratoren sind bzgl. BDSG zu belehren und der Zugang ist auf eine Person + Vertreter zu beschränken. Nachweisbarkeit (Protokollierung) der Änderungen ist sicherzustellen. Protokolle und installierte Software ist regelmäßig zu kontrollieren.
VoIP-Middleware	Integrität	hoch	Fernwartungszugänge sind grundsätzlich nur über gesicherte Zugänge (Secure Shell oder VPN) zuzulassen.

Tabelle 6.2: Maßnahmenkatalog Mittlere Größe

Anmerkungen

Der Einsatz von Softphones bleibt ausgeschlossen. CTI-Funktionalitäten werden über einen eigenen Server abgehandelt.

6.3 Standortübergreifende Netze (VoIP im Primärbereich)

Einsatzszenario

Betrachtet wird folgendes Einsatzszenario: Ein Unternehmen plant die Telefonie-Anbindung eines neuen Standortes mittels VoIP. Dabei soll am neuen Standort eine abgesetzte TK-Anlage eingerichtet werden, die sich vollständig in das bisherige Telefonie-System integriert. Dabei ist es zunächst unerheblich, ob es sich bei der abgesetzten Anlage um eine herkömmliche TDM-basierte TK-Anlage oder eine VoIP-Anlage handelt.

Anforderungsprofil

Handelt es sich bei der abgesetzten Anlage, um eine VoIP-Anlage, sind die Anforderungen aus Kapitel 6.5 ebenfalls zu berücksichtigen.

Verfügbarkeit: Die telefonische Erreichbarkeit des Standortes muss unter den gleichen Verfügbarkeits-Anforderungen wie die Gesamt-Telefonie gewährleistet sein (siehe Kapitel 6.2). Externe Angriffe, die mit qualifizierten Mitteln durchgeführt werden, sollen ausgeschlossen werden.

Die Sprachqualität der Verbindung muss zu jedem Zeitpunkt eine problemlose, verständliche Sprachkommunikation ermöglichen. Die Sprachqualität sollte überwiegend nicht von der einer ISDN-Verbindung unterscheidbar sein und ist unabhängig von einem möglichen Aufkommen im Datennetz zu gewährleisten.

Vertraulichkeit: Die Vertraulichkeit von Gesprächs- und aller Verbindungsdaten ist gegenüber externen Angreifern, die über hohe qualifizierte Mittel verfügen, zu gewährleisten.

Integrität/Authentizität: Die Integrität der Kopplung ist zu gewährleisten sowie externe Manipulationsangriffe, die mit qualifizierten Mitteln durchgeführt werden, sind auszuschließen.

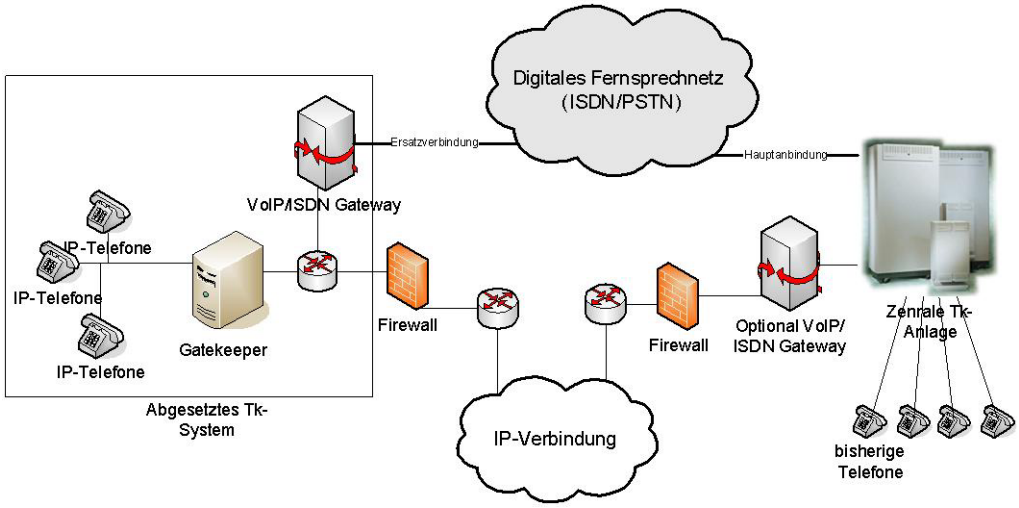

Abbildung 6.3 Einsatzbeispiel Kopplung von Standorten

Maßnahmen

Komponente	Grundwert	Schutz-bedarf	Maßnahme
Router / VoIP-ISDN Gateway	Vertraulichkeit	Hoch	Maßnahmen zur Sicherstellung der Vertraulichkeit von Gesprächsinhalten und Signalisierungsdaten. Aufbau eines VPN-Tunnels, der für VoIP ausgelegt ist.
Außenanbindung	Verfügbarkeit	Hoch	Maßnahmen zur Sicherstellung der Verbindungsqualität. Geeignete Maßnahmen sind: 1) bei geschalteten Festverbindungen, die zur gleichzeitigen Kopplung des Sprach- und Datennetzes genutzt werden, Class-of-Service-Maßnahmen wie Diffserv. 2) Bei Nutzung eines öffentlichen IP-Netzes, virtuelle Tunnel mit MPLS
Verbindung in das öffentliche Fernsprechnetz	Verfügbarkeit	Hoch	Es ist sicher zu stellen, dass der Standort auch bei Ausfall der Anlagen-Kopplung telefonisch erreichbar bleibt. Hierzu ist eine Anbindung der abgesetzten Anlage an das öffentliche Fernsprechnetz vorzusehen. Die Anzahl der verfügbaren Kanäle kann dabei eingeschränkt sein.
Firewall	Integrität/ Verfügbarkeit	Mittel	Zugriff über IP-Verbindung auf das VPN-Gateway begrenzen.

Tabelle 6.3: Maßnahmenkatalog Standortvernetzung

Anmerkungen

Prinzipiell lassen sich Anlagen derzeit nach drei Arten über eine IP-Verbindung koppeln:

1. Kopplung über eine dezidierte Standleitung. Eine dauerhaft dem Nutzer in voller Bandbreite zur Verfügung stehende Verbindung wird genutzt, um das Daten- und Sprachnetz zu koppeln. Gegenüber der Kopplung von Daten- und Sprachnetzen über jeweils separate Leitungen, ergeben sich Flexibilitätsvorteile (nicht verwendete Sprachkanäle können zur Datenübertragung genutzt werden) und ein Kosteneinsparpotenzial.

   In diesem Szenario ist darauf zu achten, dass eine Priorisierung der Sprachkommunikation beispielsweise mittels Diffserv erfolgt. In bestimmten Fällen kann Traffic-Shaping ebenfalls hilfreich sein.

2. Die Kopplung über ein öffentliches IP-Netz scheint aufgrund der geringen Kosten der Zugänge sehr attraktiv. Dies ist allerdings mit hohen Risiken für die Verfügbarkeit verbunden und sollte nur bei deutlichem Overprovisioning, d.h. bei sehr breiter Außenanbindung erfolgen, und durch ISDN-Wählverbindungen als Backup-Verbindungen gesichert werden.
3. Die Kopplung über eine virtuelle Verbindung Netzwerkverbindung, die eine bestimmte Dienstgüte garantiert, beispielsweise MPLS-Verbindungen. Werden Anlagen über öffentliche IP-Netze gekoppelt, sollte diese Art nach Möglichkeit gewählt werden.

Mittlere und große TK-Anlagen verfügen meist über Baugruppen zur Anlagen-Kopplung über IP. Alternativ lassen sich die Anlagen über eine normale ISDN-Baugruppe und einem nachgeschalteten ISDN-Gateway, ggf. unter Nutzung des standardisierten Q-SIG Protokolls, flexibel koppeln.

6.4 Campusnetze (VoIP in allen Bereichen)

Betrachtet wird in diesem Szenario der Einsatz eines umfassenden VoIP-Systems in einem Campusnetz. D.h. die Kommunikation zwischen einzelnen Standorten und Gebäuden erfolgt über ein im eigenen Verantwortungsbereich betriebenes Backbonenetz.

Wichtige funktionale Anforderung ist eine effiziente Nutzung der Übertragungskapazitäten, insbesondere des Backbones (kein doppeltes Backbone).

Anforderungen

Grundsätzlich sind die gleichen Anforderungen anzusetzen, die auch für VoIP-Systeme mittlerer Größe gefordert werden (siehe Kapitel 6.2). Zusätzliche Anforderungen sind vor allem:

Verfügb arkeit: Es gelten die gleichen Anforderungen wie sie auch für bisherige TDM-basierte Telefonie-Systeme gelten. Insbesondere sollen breitflächige Angriffe, beispielsweise durch Würmer keinerlei spürbare Auswirkungen auf die Telefonie haben. Angriffe, die mit qualifizierten Mitteln durchgeführt werden, sollen ausgeschlossen werden. Die Sprachqualität der Verbindung muss zu jedem Zeitpunkt eine problemlose, verständliche Sprachkommunikation ermöglichen. Die Sprachqualität sollte überwiegend nicht von der einer ISDN-Verbindung unterscheidbar sein und ist unabhängig von einem möglichen Aufkommen im Datennetz zu gewährleisten. Notrufmöglichkeiten sind einzurichten und deren Verfügbarkeit zu gewährleisten.

Vertraulichkeit: Die Vertraulichkeit der Gesprächsinhalte ist vor Angreifern, die über qualifizierte Mittel verfügen, zu gewährleisten. Die Vertraulichkeit der Verbindungsdaten ist gegenüber Angreifern, die über hohe qualifizierte Mittel verfügen, zu gewährleisten.

Integrität/Authentizität: Wie in Kapitel 6.2.

Damit kann in diesem Einsatzszenario von einem Sicherheitsbedarf der Schutzklasse 2 hoch ausgegangen werden.

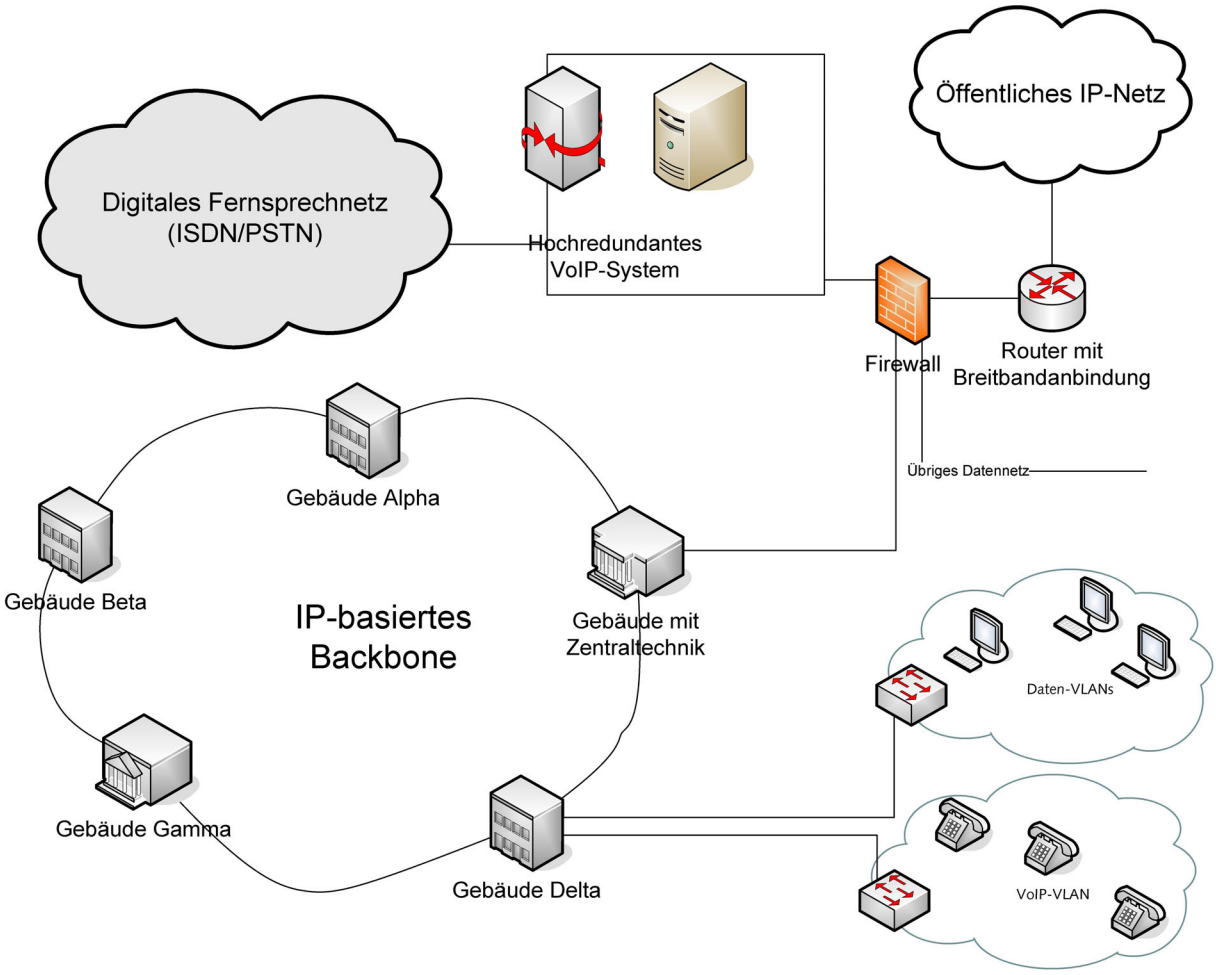

Abbildung 6. 4 Einsatzbeispiel Campusnetz

Maßnahmen

Komponente	Grundwert	Schutz-bedarf	Maßnahme
Backbone	Verfügbarkeit	hoch	Maßnahmen zur Sicherstellung der Dienstgüte. Maßnahmen sind beispielsweise die ganzheitliche Einführung von QoS wie MPLS (im Backbone) oder CoS-Maßnahmen wie beispielsweise Diffserv (bis zu den Endgeräten). Darüber hinaus zeigt sich, dass Overprovisioning eine geeignete und vielfach wirtschaftliche Maßnahme ist, eine entsprechende Dienstegüte im Netzwerk zu erreichen.
Backbone	Verfügbarkeit	hoch	USV zur Aufrechterhaltung der Übertragungswege. Ziel ist dabei die Sicherstellung der Kommunikationsmöglichkeit auch bei einem Totalausfall der Stromversorgung in einer Größenordnung von mindestens 4h.

Tabelle 6.4: Maßnahmenkatalog Campusnetz

6.5 Migration in bestehende TK-Systeme

Betrachtet wird folgendes Einsatzszenario: Ein Unternehmen/eine Behörde will ihr bestehendes, TDM-basiertes Telefonie-System erweitern und dabei VoIP-Technik einführen. Das bisherige Telefonsystem soll wie bisher weiterlaufen, das neue VoIP-System vollständig in das bisherige TK-

System integriert werden. Langfristig soll die VoIP-Technik das bisherige TK-System ersetzen. Die Verbindung zwischen VoIP- und bisherigem TK-System erfolgt über ISDN, ggf. unter Nutzung einer Q-SIG-Signalisierung.

Anforderungsprofil

Im Wesentlichen sind die gleichen Anforderungen wie bei einem mittleren VoIP-System gegeben (siehe Kapitel 6.2). Weitere Anforderungen sind:

Verfügbarkeit: Die VoIP-Erweiterung darf die Funktionalität des bisherigen Telefon-Systems nicht beeinträchtigen.

Vertraulichkeit.: Da die Verbindungsdaten des VoIP-Systems mit denen des zentralen TK-Systems abgeglichen werden, ist besondere Vorsicht im Umgang mit diesen Daten geboten.

Integrität/Authentizität: Es ist sicherzustellen, dass mit qualifizierten Mitteln kein Gebührenbetrug durchgeführt werden kann. Dies gilt insbesondere für die Schnittstelle zwischen VoIP-Anlage und bisherigem TK-System.

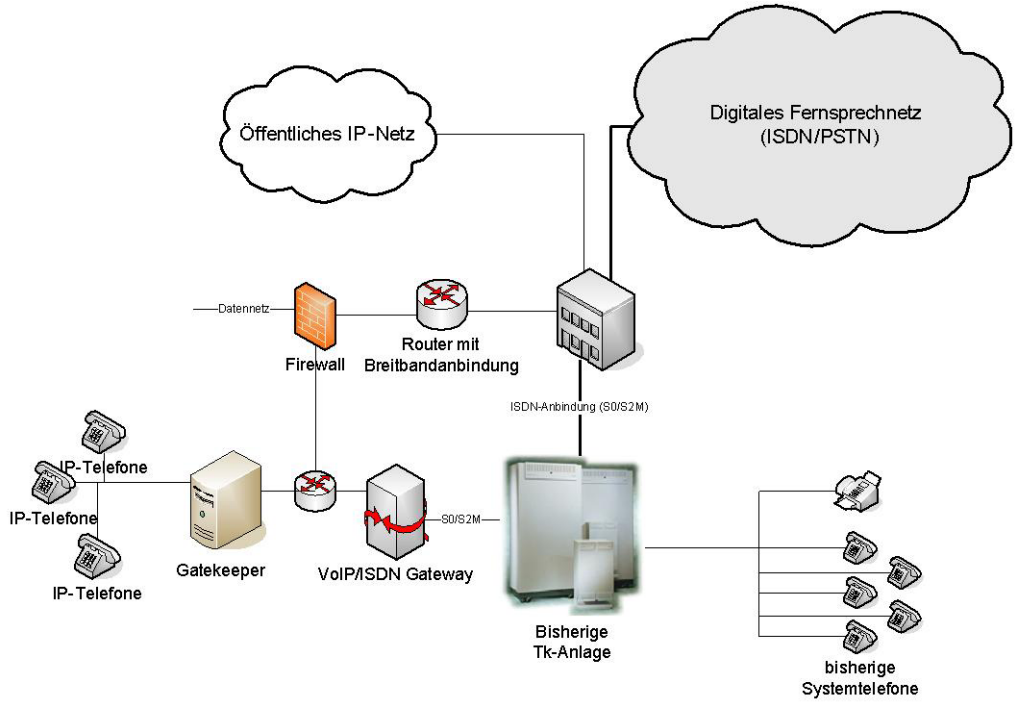

Abbildung 6. 5 Migration in bestehende TK-Systeme

Maßnahmen

Komponente	Grundwert	Schutz-bedarf	Maßnahme
Verbindung TK-System und VoIP-System	Integrität	hoch	Maßnahmen zur Sicherstellung der Integrität sind zu treffen. Die Übertragung (S0/S2M) ist üblicherweise ungesichert und sollte daher durch geeignete physikalische Maßnahmen gesichert werden (Aufstellung in unmittelbarer Nachbarschaft, geschützte Räume, bei örtlicher Entfernung Schutz der Kabeltrassen).

Tabelle 6.5: Maßnahmenkatalog Migration in bestehende TK-Systeme

Anmerkungen

Oftmals wird das bestehende Telekommunikationssystem bei der Migration zu VoIP nicht vollständig ersetzt, sondern zunächst durch ein zusätzliches VoIP-System ergänzt. Daher wird dieses

Einsatzszenario derzeit häufig in Betracht gezogen. Obwohl die Verfügbarkeitsanforderungen anfangs durch die weiterhin betriebene TK-Anlage geringer erscheint, sollten die für einen dauerhaften Betrieb notwendigen Anforderungen von Anfang gewährleistet werden.

6.6 Verschlusssachenkommunikation

Betrachtet wird folgendes Einsatzszenario: Die IP-Telefonie soll für die Kommunikation von Verschlusssachen eingerichtet werden. Dabei werden Informationen mit VS Vertraulich oder höher sowie der Kategorie Schutzklasse 2 und 3 ausgetauscht. Eine sehr hohe Verfügbarkeit ist erforderlich. Das TK-System wird ausschließlich zu dienstlichen Zwecken verwendet.

Anforderungen:

Verfügbarkeit: Für die Verfügbarkeit des Telefonie-Systems wird ein ununterbrochener Dauerbetrieb erwartet. Für die Endgeräte gilt eine maximale Ausfalldauer von <10 min. je Ausfall bei maximal 2 Ausfällen im Jahr.

Vertraulichkeit: Die Vertraulichkeit der Gesprächsinhalte ist vor Angreifern, die über hochqualifizierte Mittel verfügen, zu gewährleisten. Status-Informationen eines Teilnehmers sollen vertraulich gehalten werden.

Integrität/Authentizität: Manipulationsangriffe, die mit hochqualifizierten Mitteln durchgeführt werden, sind auszuschließen.

Damit kann in diesem Einsatzszenario von einem Sicherheitsbedarf der Schutzklasse 3 „sehr hoch“ ausgegangen werden.

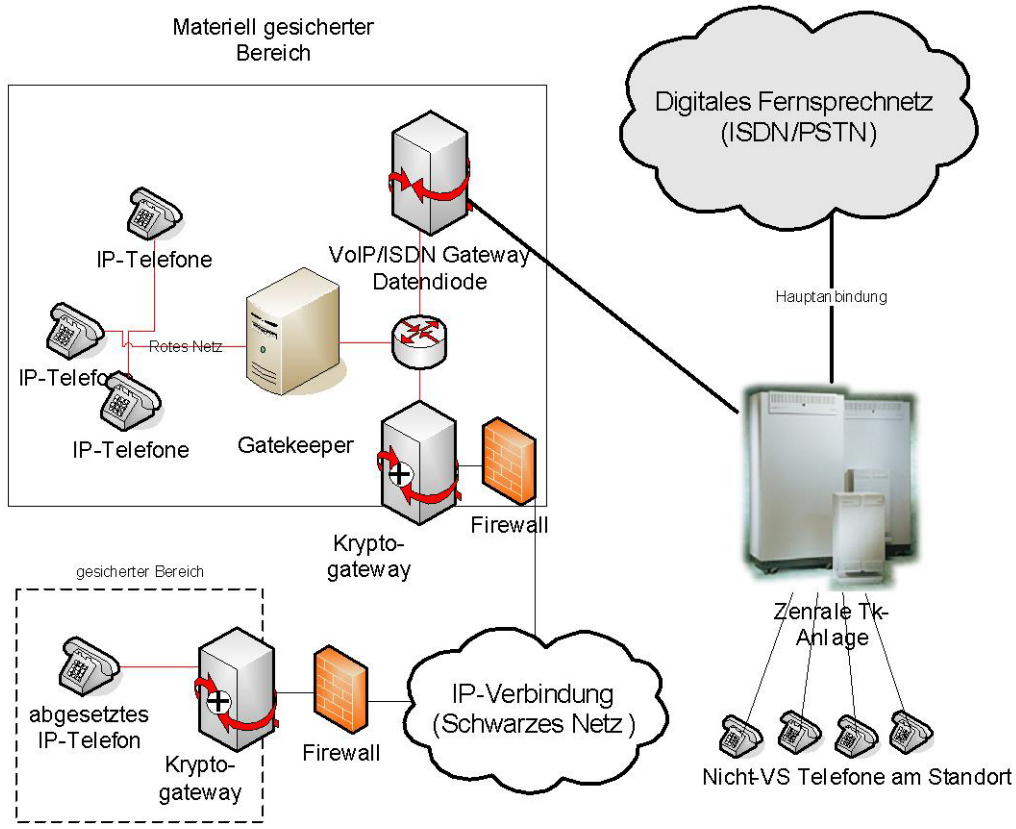

Abbildung 6.6 Einsatzbeispiel bei hoher Vertraulichkeit

Maßnahmen

Komponente	Grundwert	Schutz-bedarf	Maßnahme

Komponente	Grundwert	Schutz-bedarf	Maßnahme
Kabeltrassen, Räume mit VoIP-Komponenten	Integrität	hoch	Sicherungsmaßnahmen zum physikalischen Schutz/materielle Sicherheit sind zu ergreifen. Der Zutritt zu den Räumen ist auf ein Minimum zu beschränken und zu dokumentieren. Separate Schließzylinder (kein Schließsystem), Ersatzschlüssel kann bei Sicherheitsbeauftragten hinterlegt werden.
Räume, IP-Telefone, VoIP-Middleware	Vertraulichkeit	hoch	Es sind Maßnahmen zur Abstrahlsicherheit zu treffen. Reichen Räume- und Gebäudedämpfung nicht aus, sind technische Maßnahmen (Zonengerät oder zugelassenes Gerät) einzusetzen.
Kabeltrassen, Räume mit VoIP-Komponenten	Verfügbarkeit	mittel	Sicherungsmaßnahmen gegen Feuer und Wasserschaden, die gewährleisten sollen, dass der Betrieb des zentralen Kommunikationssystems auch in Notfallsituationen zumindest temporär erhalten bleibt. Überspannungsschutz.
IP-Telefone/Switche	Verfügbarkeit	hoch	Versorgung der Endgeräte durch PoE.
Switche/Repeater	Verfügbarkeit	hoch	USV zur Aufrechterhaltung der Übertragungswege.
Zentrale VoIP-Middleware	Verfügbarkeit	hoch	USV zur Aufrechterhaltung der zentralen VoIP-Komponenten. Hierzu zählen der Gatekeeper (Aufrechterhaltung der internen Kommunikationsmöglichkeit) sowie des Gateways in das öffentliche Fernsprechnetz. Aufrechterhaltung der Serverfunktionen bei Totalausfall der Stromversorgung in der Größenordnung von 4h.
Switch/Router	Verfügbarkeit/ Integrität/ Vertraulichkeit	hoch	Trennung von Sprach- und Datennetz: Aufteilung des Netzwerks in mehrere Broadcast-Domänen (VLANs). Die Verbindung der verschiedenen VLANs erfolgt über eine Firewall bzw. Router mit Layer3-Filter.
Switch/Router IP-Telefone	Vertraulichkeit	hoch	Separates Netz für den „Rot“-Bereich (physikalisches Rot-Netz) oder Verschlüsselung unmittelbar am Endgerät (logisches Rot-Netz).
Switche/Router	Authentikation	hoch	Zugang des IP-Endgerätes zum Netz nur nach erfolgter Authentifizierung. Authentifizierung mittels IEEE 802.1x
Switche/Router	Verfügbarkeit/ Integrität/ Vertraulichkeit	hoch	Maßnahmen gegen ARP-Spoofing
Switche/Router, VoIP-Middleware, IP-Telefone	Verfügbarkeit/Integrität	hoch	Maßnahmen gegen DHCP-Angriffe
Switche/Router	Verfügbarkeit/ Integrität/ Vertraulichkeit	hoch	Maßnahmen gegen VLAN-Angriffe, zusätzich Strukturierung der VLANs in „Producing VLAN“ mit Servern und „Consuming VLAN“ mit den IP-Endgeräte.
Verbindung in das öffentliche IP-Netz	Integrität/ Vertraulichkeit	hoch	Das Netz sollte sowohl vom internen Datennetz als auch vom öffentlichen IP-Netz vollständig getrennt sein oder durch eine zertifizierte Datendiode gekoppelt werden.
Gateway in das öffentliche Fernsprechnetz	Integrität/ Vertraulichkeit	hoch	Das PSTN-Gateway sollte zertifiziert und für die Nutzung als Datendiode freigegeben sein, da es sich dabei prinzipiell um einen Übergang zwischen einem Roten und einem Schwarzen Bereich handelt.

Komponente	Grundwert	Schutz-bedarf	Maßnahme
Gatekeeper	Verfügbarkeit	hoch	Redundantes System mit automatischer oder halbautomatischer Funktionsübernahme nach Ausfall. Fortlaufende Spiegelung der Konfigurationsdatenbank.
Gateway in das öffentliche Fernsprechnetz	Verfügbarkeit	mittel	Redundantes System, mit automatischer oder halbautomatischer Funktionsübernahme nach Ausfall.
Netzkomponenten	Verfügbarkeit	mittel	Sicherstellung einer ausreichenden Bandbreite durch Overprovisioning.
IP-Telefone	Integrität/ Verfügbarkeit	mittel	Sicherstellung der Funktionalität der IP-Telefone, beispielsweise durch Einsatz formal evaluierter Endgeräte.
IP-Telefone	Vertraulichkeit	hoch	Verschlüsselung mittels SRTP
IP-Telefone	Vertraulichkeit	hoch	Schlüsselaustausch mittels MIKEY oder durch Verschlüsselung der Signalisierung.
IP-Telefone	Interität/ Vertraulichkeit	hoch	Passwortschutz der TK-Endgeräte
Verschlüsselungs-gateways	Vertraulichkeit	hoch	Bei verlassen eines gesicherten Hoheits-Bereichs, Einsatz eines für die entsprechende VS-Stufe freigegebenen kryptographischen Verschlüsselungssystems und Verwendung von entsprechendem Schlüsselmaterial.
VoIP-Middleware	Integrität	hoch	Server-Systeme sollten nur als Minimalsystem installiert und konfiguriert sein. Einsatz eines gehärteten Betriebssystems.
VoIP-Middleware	Integrität	hoch	Server-Systeme sollten nur als Minimalsystem installiert und konfiguriert sein. Einsatz eines gehärteten Betriebssystems.
VoIP-Middleware	Integrität	hoch	Administrativer Zugang zu den Serversystemen ist möglichst auf eine Person + Vertreter zu beschränken. Administratoren sind bzgl. BDSG zu belehren und verfügen über die notwendigen Ermächtigungen. Nachweisbarkeit (Protokollierung) der Änderungen ist sicherzustellen. Protokolle und installierte Software sind regelmäßig zu kontrollieren.
VoIP-Middleware	Integrität	hoch	Fernwartungszugänge sind grundsätzlich nur über gesicherte Zugänge (Secure Shell oder VPN) zuzulassen. Werden Informationen der Stufen VS-Geheim und höher verarbeitet, ist eine Fernwartung auszuschließen.

Tabelle .6: Maßnahmenkatalog für hohe Vertraulichkeit

Anmerkungen:

Derzeit existieren keine IP-Telefone, die explizit für Verschlusssachen freigegeben bzw. die über eine entsprechende Kryptierungsmöglichkeit verfügen. Der Einsatz von VoIP-Verbindungen zur Kommunikation von VS-eingestuften Informationen hat daher über entsprechend freigegebene IP-Verschlüsselungsgateways zu erfolgen.

Problematisch sind weiterhin die Übergänge zwischen IP-basiertem Telefonienetz und dem ISDN-Netz. Wegen der fehlenden Interoperabilität ist derzeit keine verschlüsselte Ende-zu-Ende Kommunikation zwischen Endgeräten in unterschiedlichen Netzen möglich. Allerdings sind einige Entwicklungen hin zu einer interoperablen Sicherheitsarchitektur beispielsweise mit SCIP [SCIP05] und [AlkStu2002] in der Entwicklung.

Zum Aufbau verlässlicher Gateways mit einem Rot/Schwarz-Übergang (z. B. um IP-Telefonen im Rot-Bereich unverschlüsselte Kommunikation in das Fernsprechnetz zu ermöglichen) sind Systeme mit gehärteter (z. B. SINA-Linux, bzw. SE-Linux) oder mehrseitig sicherer (Perseus) Betriebssystemarchitektur erforderlich. Die Evaluierung nach formalen Kriterien kann dabei helfen die Sicherheit des Systems nachvollziehbar zu dokumentieren.

7. Abschließende Sicherheitsbetrachtung

7.1 Fördernde und hemmende Faktoren von VoIP

Die zukünftige Entwicklung von VoIP wird essentiell davon abhängen, ob es gelingt die VoIP-Systeme mit der gleichen Verlässlichkeit zu betreiben, die Anwender von ihrem bisherigen Telefoniesystem gewohnt sind. Hierzu gehört neben einer hohen Verfügbarkeit, einer verlässlichen Funktionalität vor allem eine einwandfreie Sprach- und Verbindungsqualität.

Während es bei IT-Systemen vielfach hingenommen wird, dass beispielsweise die Netzanbindung temporär ausfällt oder gestört ist, wird ein Ausfall der Telekommunikation deutlich kritischer gesehen. Dies gilt auch für Bereiche, die nicht notwendigerweise eine erhöhte Verfügbarkeitsanforderung haben, wie beispielsweise klassische Backoffice-Bereiche. Auch die verlässliche Funktionalität der Systeme gilt im Telefonie-Bereich als Standard. Telefone, die regelmäßig „abstürzen“ oder rebooten beeinträchtigen die Akzeptanz des Gesamtsystems genauso wie komplizierte Menüführungen oder fehlerhafte Software.

Ein wichtiges Kriterium, das vor allem zu Anfang die Verbreitung von VoIP verhinderte, ist die Sprach- und Verbindungsqualität von VoIP-basierten Systemen. Die Sprachqualität wurde inzwischen deutlich erhöht, vor allem durch rasant gestiegene Bandbreiten und verbesserte Codecs. Die Gewährleistung einer dauerhaft verlässlichen Verbindungsqualität ist jedoch nach wie vor mit einem hohen technischen Aufwand verbunden, der vielfach noch gescheut wird. Dies gilt insbesondere bei der Einführung von VoIP in bestehende IP-Netze.

Die Sicherheit spielt derzeit eine verhältnismäßig untergeordnete Rolle in der Wahrnehmung von VoIP-Systemen. Dies ist vor allem im Zusammenhang der (noch) vergleichsweise geringen Anzahl von veröffentlichten Angriffen auf VoIP-basierte Telefoniesysteme zurückzuführen. Es dürfte eine Frage der Zeit sein, bis erste „spektakuläre“ Angriffe bekannt werden. Spätestens dann dürfte die Sicherheit von VoIP-Systemen zu einem zentralen Kriterium bei der weiteren Bewertung dieser Technologie werden.

Wichtigster Entwicklungsfaktor für VoIP bleibt jedoch das vermeintliche oder tatsächliche Einsparpotenzial beim Einsatz von VoIP-Systemen und bleibt damit auch im Spannungsfeld zum Aufwand, der für die Sicherheit aufzubringen ist.

7.2 Entwicklungsperspektiven VoIP-Sicherheit

Mit der weiteren Verbreitung von VoIP-Systemen im produktiven und im kommerziellen Einsatz, ist mit einem kontinuierlichen Ansteigen der Angriffe zu rechnen. Mittelfristig dürften damit auch die Erfahrungswerte bzgl. der praktischen Sicherheit von VoIP-Systemen steigen. Dies ist für die weitere Entwicklung sicherer VoIP-Systeme und für deren verlässlichen Einsatz von großer Bedeutung.

Im Bereich kryptographischer Protokolle zeigt sich seit wenigen Jahre ebenfalls eine intensive Forschungstätigkeit hin zur Optimierung vorhandener und Entwicklung neuer Verfahren, die die Anforderungen paketorientierter Sprachverbindungen erfüllen.

Weiterhin Handlungsbedarf besteht im Angebot von VoIP-Komponenten, die entsprechende Sicherheitsmaßnahmen unterstützen. Insbesondere im Endgerätebereich ist die Auswahl geeigneter und zufriedenstellender Geräte derzeit äußerst gering.

7.3 Fazit

VoIP ist eine Technologie, die beim Einsatz entsprechender Sicherheitsmaßnahmen nicht nur eine ernsthafte Alternative zur klassischen Telefonie darstellt, sondern aufgrund der Synergiepotenziale die bisherigen Technologien in vielen Bereichen langfristig sukzessive ablösen wird.

Gleichzeitig wird klar, dass die unbedarfte Einführung von VoIP erhebliche Bedrohungspotenziale mit sich bringen kann. Im Vergleich von Standard-Installationen zu TDM-basierten Telefonie-Lösungen, ist der ungesicherte Einsatz von VoIP-Technologie mit deutlich größeren Risiken verbunden. Denn die VoIP-Systeme erben die Sicherheitsrisiken der IP-Welt und darüber hinaus behalten sie die meisten aus der TK-Welt.

Geeignete Sicherheitsmaßnahmen sind heute technisch und organisatorisch realisierbar. Allerdings unterstützt nur ein Bruchteil der aktuell auf dem Markt befindlichen Systeme die erforderlichen Sicherheitsmaßnahmen im erforderlichen Umfang. Bei der Auswahl eines Systems sollten daher die realisierten Sicherheitsmaßnahmen im Fokus stehen und nicht nur reine Funktionalitätsgesichtspunkte in die Entscheidung einbezogen werden.

Die für einen verlässlichen Betrieb von VoIP-Systemen notwendigen Sicherheitsmaßnahmen sind jedoch mit einem substanziellen technischen und finanziellen Aufwand verbunden, der die angestrebten Kosteneinsparungen möglicherweise vermindert. Die Kosten für die erforderlichen Sicherheitsmaßnahmen müssen daher bereits frühzeitig in die Planungen mit einbezogen werden.

Am Ende sollte die Entscheidung für oder gegen den Einsatz von VoIP-Systemen immer zugunsten der IT-Sicherheit ausfallen

8. Abkürzungsverzeichnis/Glossar

ABFN (Augmented Backus Naur Form der Nachrichten)
ACF (Admission Confirmation)
ACK (Acknowledgement)
ACL (Access Control List)
AES (Advanced Encryption Standard)
AH (Authentication Header)
ALG (Application Level Gateway)
ARP (address resolution protocol)
ARQ (Admission Request)
ATM (Asynchronous Transfer Protocol)
BPDU (Bridge Protocol Data Unit)
CA (Control Agent)
CoS (Class of Service)
CRCX (CreateConnection)
CSRC (Contributing Source Identifiers)
ENUM (tElephone NUmber Mapping)
HRSP (Hot Standby Router Protocol)
IAX (Inter-Asterisk EXchange (IAX) Protocol)
IAX2 (InterAsterisk eXchange Protocol Version 2)
ICE (Interactive Connectivity Establishment)
IETF (Internet Engineering Task Force)
IETF (Internet Engineering Task Force)
IKE (Internet Key Exchange)
IPTSP (IP Telephony Service Providing)
IRDP (ICMP Router Discovery Protocol)
ITAD (IP Telephony Administrative Domain)
ITU-T (International Telecommunication Union, Telecommunication Standardization Sector)
MCU (Multipoint Control Unit)
MDCX (Modify-Connection)
Megaco (Media Gateway Protocol)
MG (Media Gateway)
MGCP (Media Gateway Control Protocol)
MIDCOM (Middlebox Communications)
MIKEY (Multimedia Internet Keying)
MPLS (Multi-Protocol Label Switching)
NAPTR (Naming Authority Pointer)
NAT (Network Address Translation)
NIDS (Network Intrusion Detection System)
PAT (Port Address Translation)
PCM (Pulse Code Modulation)
PDH (Plesiochronous Digital Hierarchy)
PGP (Pretty Good Privacy)

PSTN (Public Switched Telephone Network)
PSTN (Public Switched Telephone Network)
PT (Payload Type)
QoS (Quality of Service)
RCF (Register Confirmation)
RFC (Request for Comments)
RQNT (NotificationRequest)
RRJ (Refgistration Reject)
RRQ (Register Request)
RTP (Real Time Protocol)
RTTP (Real Time Transport Protocol)
SA (Security Association)
SAD (Security Association Database)
SCCP (Skinny Client Control Protocol)
SCIP (Secure Communication Interoperability Protocol)
SCN (Switched Circuit Network)
SDH (Synchronous Digital Hierarchy)
SDP (Session Description Protocol)
SIP (Session Initiation Protocol)
SIP (Session Initiation Protocol)
SPD (Security Policy Database)
SRTP (Secure Real Time Protocol
SRTP (Secure Real-Time-Transport Protocol)
SSRC (Synchronisation Source Identifier)
STP (Spanning Tree Protocol)
STUN (Simple Traversal of User Datagram Protocol (UDP) Through NATs)
TDM (Time Division Multiplex)
TDM (Time Division Multiplex)
TFTP (Trivial File Transfer Protocol)
TKIP (Temporal Key Integrity Protocol)
TLS (Transport Layer Security)
TRIB (Telephony Routing Information Base (TRIB)
TRIP (Telephony Routing over IP)
TURN (Traversal Using Relay NAT)
UA (User Agent)
UDP (User Datagram Protocol)
UpnP (Universal Plug and Play)
VRRP (Virtual Router Redundancy Protocol)
WDM (Wavelength Division Multplex)
WEP (Wired Equivalent Privacy)

9. Literaturverzeichnis

[AGS05] André Adelsbach, Sebastian Gajek und Jörg Schwenk: *Phishing - Die Täuschung des Benutzers zur Preisgabe geheimer Benutzerdaten;* in Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Tagungsband zum 9. Deutscher IT-Sicherheitskongress des BSI, Secumedia-Verlag Ingelheim, 2005

[AlkStu03] Ammar Alkassar und Christian Stüble: *A Security Framework for Integrated Networks;* MILCOM 2003, IEEE Military Communications Conference, Boston, 2003

[ALRL04] Algirdas Aviziensis, Jean-Claude Laprie, Brian Randell und Carl Landwehr: *Basic Concepts and Taxonomy of Dependable and Secure Computing*; IEEE Interactions on Dependable and Secure Computing, Vol. 1, No. 1, Januar-März, 2004

[Arnold04] Alfred Arnold: *Jenseits von WEP;* CT, Heft 21/04, Heise Verlag, 2004

[ASSS05] Ammar Alkassar, Ahmad-Reza Sadeghi, Marcel Selhorst und Christian Stüble: *Towards Secure Computing Platforms with Open-Source and Trusted Computing*; in Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Tagungsband zum 9. Deutscher IT-Sicherheitskongress des BSI, Secumedia-Verlag Ingelheim 2005

[AuAn01] Andreas Aurand: *LAN-Sicherheit und Network Security Assessment*; dpunkt.Verlag, 2004

[Ba2005] Daniel Bachfeld: Forscher erzeugen unterschiedliche X.509-Zertifikate mit gleichem MD5-Hash; Heise Newsticker, http://www.heise.de/newsticker/meldung/print/57038, Heise Verlag, 2005

[BaAn01] Anatol Badach*: Voice over IP: Grundlagen und Protokolle für Multimedia-Kommunikation*; Carl Hanser Verlag, 2004

[BBR02] R. Barbieri, D. Bruschi und E. Rosti: *Voice over IPSec: Analysis and Solutions,* http://www.acsac.org/2002/papers/92.pdf, 2002

[BDSG90] *Bundesdatenschutzgesetz vom 20. Dezember 1990, BGBl. I, 2954*, zuletzt geändert durch Art.2, Abs.5 des Begleitgesetzes zum Telekommunikationsgesetz (BegleitG) vom 17.Dezember 1997 (BGBl. I 3108)

[BGW01] Nikita Borisov, Ian Goldberg und David Wagner*: Intercepting Mobile Communications: The Insecurity of 802.11;* ACM SIGMOBILE 2001Annual International Conference on Mobile Computing and Networking, 2001

[BS03] J. Bellardo und S. Savage*: 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions;* Proceedings of USENIX Security Symposium, 2003

[CA-2003-06] CERT: *Multiple vulnerabilities in implementations of the Session Instantiation Protocol (SIP)*; CERT Advisory CA-2003-06, http://www.cert.org/advisories/CA-2003-06.html, 2003

[CA-2004-01] CERT*: Multiple H.323 Message Vulnerabilities* ; CERT Advisory CA-2004-01, http://www.cert.org/advisories/CA-2004-01.html, 2004

[CC2000] Common Criteria (CC) 2.1*: Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria for Information Technology Security Evaluation),* Version 2.1; bekannt gemacht im Bundesanzeiger vom 20.09.2000, abrufbar unter http://www.bsi.de/cc/

[Cisco03] Cisco Systems: *Security Notice: Cisco Security Notice: W32.BLASTER Worm Mitigation Recommendations, Revision 1.8*; http://www.cisco.com/warp/public/707/cisco-sn-20030814-blaster.pdf, August 2003

[DaPe00] Jonathan Davidson und James Peters: *Voice over IP – Fundamentals*, Cisco-Press, 2000

[DISA04] Defense Information Systems Agency: *Voice over Internet Protocol (VoIP) Security Checklist*; Developed for the Department of Defense (FOUO), July 2004

[FMS01] S. Fluhrer, I. Mantin und A. Shamir: *Weaknesses in the Key Scheduling Algorithm of RC4*; SAC '01: Revised Papers from the 8th Annual International Workshop on Selected Areas in Cryptography, LNCS 2259, Springer Verlag, 2001

[G04] Miek Gieben: *DNSSEC: The Protocol, Deployment, and a Bit of Development;* Internet Protocol Journal, Vol. 7, No. 2, S. 17-28, Juni 2004

[GN04] S. Grech und J. Nikkanen*: A Security Analysis of Wi-Fi Protected Access*; Nordsec Workshop, 2004

[Goe01] Dennis Göhr: *Bewertung der Dienstgüte von Audio- und Videodiensten;* Diplomarbeit, Technische Universität Braunschweig, 2001

[GSHB04] Bundesamt für Sicherheit in der Informationstechnik – BSI: *IT-Grundschutzhandbuch;*. BSI, http://www.bsi.de/gshb/, November 2004

[H03] John Holmblad: *The Evolving Threats to the Availability and Security of the Domain Name Service;* SANS Institute, 2003

[HWS03] Christian Helmuth, Andreas Westfeld und Michael Sobirey: *µSINA - Eine mikrokernbasierte Systemarchitektur für sichere Systemkomponenten*. in Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): IT-Sicherheit im verteilten Chaos, Tagungsband 8. Deutscher IT-Sicherheitskongress des BSI, Secumedia-Verlag Ingelheim 2003.

[IAX2] M. Spencer und F. Miller: *Inter-Asterisk EXchange (IAX) Version 2*, Internet-Draft, www.cornfed.com/iax.pdf, Januar 2005

[IEEE01] IEEE Standard 802.1x-2001: *Port Based Network Access Control*; IEEE, Juni 2001

[IEEE03] IEEE Standard 802.3af-2003: *Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements. Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications. Amendment: Data Terminal Equipment (DTE). Power via Media Dependent Interface (MDI)*, IEEE, Juni 2003

[IKEv2] Internet Engineering Task Force (IETF): *Internet Key Exchange Protocol v2*; IETF Draft, approved as a proposed standard, http://www.ietf.org/internet-drafts/draft-ietf-ipsec-ikev2-17.txt

[ITSEC91] Department of Trade and Industry: *Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik*; London, UK, Juni 1991, abrufbar unter http://www.bsi.bund.de/zertifiz/itkrit/itsec.htm

[ITUT02] ITU-T : *Recommendation H.248.1 : Gateway control protocol: Version 2 ;* Mai 2002

[ITUT03a] ITU-T*: Recommendation H.225.0, Version 5: Call signalling protocols and media stream packetization for packet-based multimedia communication systems;* Juli 2003

[ITUT03b] ITU-T: *Recommendation H.323, Version 5: Packet-based multimedia communications systems*; Juli 2003

[ITUT05] ITU-T: *Recommendation H.245, Version 9: Control protocol for multimedia communication;* Januar 2005

[ITUT96a] ITU-T*: Recommendation G.113: Transmission Systems and Media. General Characteristics of International Telephone Connections and International Telephone Circuits. Transmission Impairments*; Februar 1996

[ITUT96b] ITU-T*: Recommendation G.114 : Transmission Systems and Media. General Characteristics of International Telephone Connections and International Telephone Circuits. One-way Transmission Time*; Februar 1996

[ITUT98] ITU-T: *Recommendation H.450.1: Generic functional protocol for the support of supplementary services in H.323*; Februar 1998

[Klein01] Tobias Klein*: Linux-Sicherheit: Security mit Open-Source-Software – Grundlagen und Praxis*; dpunkt-Verlag, 2001

[Klein03] Alan Klein: *Security Analysis: Traditional Telephony and IP Telephony;* SANS Institute, 2003

[Klima05] Vlastimil Klima: Fi*nding MD5 Collisions on a Notebook PC Using Multi-message Modifications*; 2005/102, eprint Archiv, IACR, http://eprint.iacr.org/2005/102, 2005

[KS04] P. Kroma und S. Schreiber: *Störfunk;* Heise Security, http://www.heise.de/security/artikel/print/45490, Heise Verlag, März 2004

[KWF05] Richard D. Kuhn, Thomas J. Walsh und Steffen Fries: *Security Considerations for Voice Over IP Systems*; Recommendations of the National Institute of Standards and Technology, 2005

[Lix98] Bruno Lix: *Interpretation von Daten über aktuell genutzte Bandbreiten und Prognose des künftigen Bedarfs;* In: DFN-Mitteilungen, Heft 48, Seiten 18-20,.Verein zur Förderung eines Deutschen Forschungsnetzes e.V., Berlin, Deutschland, 1998

[ÖIT] Stabsstelle IKT-Strategie des Bundes: *Österreichisches IT-Sicherheitshandbuch, Teil 1: IT-Sicherheitsmanagement, Version 2.2, November 2004*

[Pohl04] Hartmut Pohl: *Taxonomie und Modellbildung in der Informationssicherheit*; Datenschutz und Datensicherheit (DuD), Band 28, Seiten 678-685, 2004

[PROTOS] Secure Programming Group: *PROTOS – Security Testing of Protocol Implementations;* Oulu University, http://www.ee.oulu.fi/research/ouspg/protos, 2005

[PRS+01] B. Pfitzmann, J. Riordan, C. Stüble, M. Waidner und A. Weber: *The PERSEUS System Architecture*; IBM Technical Report RZ 3335 (#93381), IBM Research Division, Zurich Laboratory, 2001

[PS05] Joachim Posegga und Jan Seedorf: *Voice Over IP: Unsafe at any Bandwidth?,* EURESCOM Summit 2005, Heidelberg, Deutschland, 2005

[ReJö04] Jörg Rech: *Wireless LANs, 802.11-WLAN-Technologie und praktische Umsetzung im Detail. 2004;* Heise Verlag, 2004

[RFC1027] Internet Engineering Task Force (IETF): *Using ARP to Implement Transparent Subnet Gateways;* RFC 1027, http://www.rfc.net/rfc1027.html, Oktober 1987

[RFC1256] Internet Engineering Task Force (IETF): *ICMP Router Discovery Messages;* RFC 1256, http://www.rfc.net/rfc1631.html, September 1991

[RFC1631] Internet Engineering Task Force (IETF): *The IP Network Address Translator (NAT);* RFC 1631, http://www.rfc.net/rfc1631.html, Mai 1994

[RFC1633] Internet Engineering Task Force (IETF): *Integrated Services in the Internet Architecture: an Overview;* RFC 1633, http://www.rfc.net/rfc1633.html, Juni 1994

[RFC1889] Internet Engineering Task Force (IETF): *RTP: A Transport Protocol for Real-Time Applications;* RFC 1889, http://www.rfc.net/ rfc1889.html, Januar 1996

[RFC2205] Internet Engineering Task Force (IETF): *Resource Reservation Protocol (RSVP) -- Version 1 Functional Specification;* RFC 2205, http://www.rfc.net/rfc2205.html, September 1997

[RFC2210] Internet Engineering Task Force (IETF): *Use of RSVP with IETF Integrated Serviceses*; RFC 2210, http://www.rfc.net/rfc2210.html, September 1997

[RFC2246] Internet Engineering Task Force (IETF): *The TLS Protocol Version 1.0;* RFC 2246, http://www.rfc.net/rfc2246.html, Januar 1999

[RFC2327] Internet Engineering Task Force (IETF): *SDP: Session Description Protocol*; RFC2327, http://www.rfc.net/rfc2327.html, April 1998

[RFC2474] Internet Engineering Task Force (IETF): *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*; RFC 2474, http://www.rfc.net/rfc2474.html, Dezember 1998

[RFC2475] Internet Engineering Task Force (IETF): *An Architecture for Differentiated Services*; RFC 2475, http://www.rfc.net/rfc2475.html, Dezember 1998

[RFC3015] Internet Engineering Task Force (IETF): *Megaco Protocol Version 1.0;* RFC 3015, http://www.rfc.net/rfc3015.html, November 2000

[RFC3118] Internet Engineering Task Force (IETF): *Authentication for DHCP Messages*; RFC 3118, http://www.rfc.net/rfc2205.html, Juni 2001

[RFC3209] Internet Engineering Task Force (IETF): *RSVP-TE: Extensions to RSVP for LSP Tunnels;* RFC3209, http://www.rfc.net/rfc3209.html, Dezember 2001

[RFC3219] Internet Engineering Task Force (IETF): *Telephony Routing over IP (TRIP);* RFC 3219, http://www.rfc.net/rfc3219.html, Januar 2002

[RFC3220] Internet Engineering Task Force (IETF): *IP Mobility Support for IPv4;* RFC 3220, http://www.rfc.net/rfc3220.html, Januar 2002

[RFC3260] Internet Engineering Task Force (IETF): *New Terminology and Clarifications for Diffserv;* RFC3260, http://www.rfc.net/rfc3260.html, April 2002

[RFC3261] Internet Engineering Task Force (IETF): *SIP: Session Initiation Protocol;* RFC 3261, http://www.rfc.net/rfc3261.html, Juni 2002

[RFC3261] Internet Engineering Task Force (IETF): *SIP: Session Initiation Protocol;* RFC3261, Internet Engineering Task Force (IETF), http://www.rfc.net/rfc3261.html, Juni 2002

[RFC3453] Internet Engineering Task Force (IETF): *Media Gateway Control Protocol (MGCP) Version 1.0;* RFC 3453, http://www.rfc.net/rfc3453.html, April 2002

[RFC3489] Internet Engineering Task Force (IETF): *STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs);* RFC 3489, http://www.rfc.net/rfc3489.html, März 2003

[RFC3525] Internet Engineering Task Force (IETF): *Gateway Protocol Version 1;* RFC 3525, http://www.rfc.net/rfc3525.html, Juni 2003

[RFC3711] Internet Engineering Task Force (IETF): *The Secure Real-time Transport Protocol (SRTP);* RFC 3711, http://www.rfc.net/rfc3711.html, März 2004

[RFC3761] Internet Engineering Task Force (IETF): *The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM);* RFC 3761, http://www.rfc.net/rfc3761.html, April 2004

[RFC3851] Internet Engineering Task Force (IETF): *S/MIME Version 3.1 Message Specification*; RFC 3851*,* RFC 3851, Internet Engineering Task Force (IETF), http://www.rfc.net/rfc3851.html, Juli 2004

[RFC3853] Internet Engineering Task Force (IETF)*: S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP)*; RFC 3853, http://www.rfc.net/rfc3853.html, Juli 2004

[RFC791] Internet Engineering Task Force (IETF): *Internet Protocol;* RFC 791, http://www.rfc.net/rfc791.html, September 1981

[RHA04] M. Raya, J.-P. Hubaux und I. Aad: *DOMINO: A System to Detect Greedy Behavior in IEEE 802.11 Hotspots;* Proceedings of ACM MobiSys, 2004

[RiOs05] Vincent Rijmen und Elisabeth Oswald: *Update on SHA-1*; 2005/010, eprint Archiv, IACR, http://eprint.iacr.org/2005/010, 2005

[Sch05] Jörg Schwenk: *Sicherheit und Kryptographie im Internet.* 2. Auflage, Vieweg Verlag Wiesbaden, 2005

[Schmidt05] Michael Schmidt: *Der WEP-Wall bricht;* Heise Security, http://www.heise.de/security/artikel/print/59098, Heise Verlag, Mai 2005

[SCIP05] Secure Communications Interoperability Protocol–SCIP; früher Future Narrowband Digital Terminal FNBDT; Zusammenfassung in: Ronald Krebs; *Providing Global Secure Communications Interoperability Using SCIP/FNBDT*; in Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Tagungsband zum 9. Deutscher IT-Sicherheitskongress des BSI, Secumedia-Verlag Ingelheim, 2005

[SiGe02] Gerd Siegmund: *Technik der Netze*; 5. Auflage, Hüthig Verlag, Heidelberg, 2002

[SIR02] A. Stubblefield, J. Ioannidis und A. Rubin*: Using the Fluhrer, Mantin, and Shamir Attack to Break WEP;* Proceedings of the 2002 Network and Distributed Systems Symposium, Februar 2002

[TDDSG97] Gesetz über den Datenschutz bei Telediensten vom 22. Juli 1997, BGBl I 1997, 1870, 1871; zuletzt geändert durch Art. 3 und 4 Abs. 2 G v. 14.12.2001 I 3721

[TKG96] Telekommunikationsgesetz vom 25. Juli 1996, BGBl I 1996, 1120; zuletzt geändert am 5. 5.2004

[TKÜV02] *Telekommunikationsüberwachungsverordnung–TKÜV*; Kurzform zu Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation vom 22. Januar 2002.

[Tuck04] Greg S. Tucker: *Voice over Internet Protocol (VoIP) and Security;* SANS Institute, Oktober, 2004

[Vomit] Niels Provos: VOMIT: *A Voice Over Missconfigured Internet Telephones;* http://vomit.xtdnet.nl

[WaKu05] Thomas J. Walsh und Richard D. Kuhn: *Challenges in Securing Voice over IP;* IEEE Security&Privacy Magazine, Mai/Juni 2005

[Wong05] Luis C. Wong: *An Overview of 802.11 Wireless Network Security Standards & Mechanisms*, SANS Institute, 2005

Anhang A: Tabelle Übersicht Sicherheitsmaßnahmen

Sicherheitsmaßnahme	Grundwert			Schutzklassen			Maßnahmengruppe
	Verfügbarkeit	Vertraulichkeit	Integrität	1	2	3	
Sicherungsmaßnahmen für einen physikalischen Schutz	X	X	X		X	X	
Sicherungsmaßnahmen für unterbrechungsfreie Stromversorgung der Netzkomponenten	X				X	X	
Sicherungsmaßnahmen für unterbrechungsfreie Stromversorgung der VoIP-Middleware	X				X	X	
Sicherungsmaßnahmen für unterbrechungsfreie Stromversorgung der Endgeräte	X				X	X	
Trennung von Sprach- und Datennetz		X	X		X	X	
Statischer MAC-Eintrrag	X			X			Maßnahmen zur Geräteauthentikation
Authentifizierung nach IEEE 801.x	X				X	X	Maßnahmen zur Geräteauthentikation
Sicherungsmaßnahmen gegen ARP-Spoofing	X	X	X		X	X	Maßnahmen gegen Störungen der Anwendung (DoS) und Basisdienste
Maßnahmen gegen DHCP-Attacken	X	X	X		X	X	Maßnahmen gegen Störungen der Anwendung (DoS) und Basisdienste
Maßnahmen gegen STP-Attacken	X	X	X		X	X	Maßnahmen gegen Störungen der Anwendung (DoS) und Basisdienste
Anti-Spoofing Filter	X				X	X	
Maßnahmen gegen VLAN-Angriffe	X	X	X		X	X	
Struktur von LANs und Zugang der VLANs	X	X	X		X	X	
Sicherheitsmaßnahmen zum Schutz des Netzzugang aus dem öffentlichen Netz ins LAN	X	X	X	X	X	X	
Maßnahmen gegen IP-Spoofing	X	X	X		X	X	
Maßnahmen gegen ICMP-Redirect	X	X	X		X	X	
Maßnahmen gegen IRDP-Spoofing	X	X	X		X	X	
Maßnahmen gegen Route Injection	X	X	X		X	X	
Maßnahmen gegen HSRP- und VRRP-Angriffe	X	X	X		X	X	
Maßnahmen gegen Ping Flood, SYN Flood und LAND Flood	X					X	Maßnahmen gegen Störungen der Anwendung (DoS) und Basisdienste
Redundante Netzkomponenten und Server	X				X	X	
Diffserv sowie Class-of-Service nach IEEE 802.1p	X				X	X	Dienstegüte und Monitoring der Netzwerk-Performance
Overprovisioning der Bandbreite	X				X	X	Dienstegüte und Monitoring der Netzwerk-Performance
Multi-Protocol-Label Switching (MPLS)	X				X	X	Dienstegüte und Monitoring der Netzwerk-Performance
Traffic Shaping	X			X	X	X	Dienstegüte und Monitoring der Netzwerk-Performance
Störungsmanagement und Eskalationsprozesse	X				X	X	
Security Management	X	X	X		X	X	
H.235v3 Annex I / H.235v3 Annex G		X	X	X	X	X	Maßnahmen gegen das Abhören und die Manipulation von Medienströmen
SRTP		X	X	X	X	X	Maßnahmen gegen das Abhören und die Manipulation von Medienströmen
IPSEC		X	X	X	X	X	Maßnahmen gegen das Abhören und die Manipulation von Medienströmen
H.235 / H.235v3 Annex D / H.235v3 Annex E / H.235v3 Annex F		X	X	X	X	X	Maßnahmen gegen Manipulation der Signalisierung und Gebührenbetrug
S/MIME		X	X	X	X	X	Maßnahmen gegen Manipulation der Signalisierung und Gebührenbetrug
SIP über TLS		X	X	X	X	X	Maßnahmen gegen Manipulation der Signalisierung und Gebührenbetrug

Sicherheitsmaßnahme	Grundwert			Schutzklassen			Maßnahmengruppe
	Verfügbarkeit	Vertraulichkeit	Integrität	1	2	3	
Paketfilter auf Layer 3 und Layer 4 (Stateless Packet Filter)			X	X	X	X	Firewalls und NIDS
Zustandsbasierter Portfilter auf Layer 3 und Layer 4 (stateful packet inspection)			X			X	Firewalls und NIDS
Application Level Gateway	X					X	Firewalls und NIDS
NIDS	X					X	Firewalls und NIDS
Administration und Zugänge nur über gesicherte Verbindungen (SSH/VPN)		X	X	X	X		Administrationszugänge
Administration nur an Konsole		X	X			X	Administrationszugänge
Datenbackup	X			X	X	X	
Softwaresicherheit, Integrität der installierten Software			X		X	X	
Betriebssystemsicherheit, gehärtetes System			X			X	
Evaluierte Endgeräte			X			X	
Vertrauenswürdige Firmwareupdates bei den Endgeräten			X	X	X	X	
Vertrauenswürdiges Konfigurieren und Digitale Zertifikate bei den Endgeräten			X		X	X	

Erläuterung: Die erste Spalte gibt die Sicherheitsmaßnahme wieder; in den Spalten „Grundwert“ sind jeweils die zugehörigen Schutzziele angegeben und in den Spalten „Schutzklassen“ die Schutzklassen in der eine Sicherheitsmaßnahme erforderlich ist. In der letzten Spalte ist jeweils aufgeführt zu welcher Maßnahmenkategorie eine Sicherheitsmaßnahme gehört.

Anhang B: Begriffserläuterungen Angriffe

Angriff mit einfachen Mitteln: Unter einem Angriff mit einfachen Mitteln wird hier der Angriff auf das IT-System durch Personen mit geringem Fachwissen oder beschränkten finanziellen und technischen Mitteln sowie durch zufällig handelnde Personen verstanden. Typische Beispiele für solche Angriffe sind der „Spieltrieb" des Mitarbeiters oder die Angriffe von „Hobby-Hackern" sowie Vandalismus und grober Unfug.

Angriff mit qualifizierten Mitteln: Unter einem Angriff mit qualifizierten Mitteln wird hier der Angriff auf das IT-System durch Personen mit krimineller Energie sowie Expertenwissen und umfangreichen finanziellen und technischen Mitteln verstanden. Typische Beispiele für solche Angriffe sind die Leistungserschleichung aufgrund von Konfigurationsänderungen durch den Administrator (bei TK-Anlagen: Gebührenbetrug) oder die Aktivitäten der organisierten Kriminalität sowie der physikalische Zugriff auf Leitungen außerhalb des eigenen Verantwortungsbereichs.

Angriffe mit hochqualifizierten Mitteln: Unter einem Angriff mit hochqualifizierten Mitteln wird hier der Angriff auf das IT-System durch Personen mit Wissen auf Entwicklerniveau sowie nahezu beliebig umfangreichen finanziellen und technischen Mitteln verstanden. Typische Beispiele für solche Angriffe sind das Abhören von Gesprächen oder Räumen durch gezielte Änderung der Betriebssoftware des Telekommunikationssystemes oder der Zugriff auf Leitungen, Hard- und Software innerhalb des eigenen Verantwortungsbereichs.

Anhang C: Informationsstruktur

Kategorie	Verschlusssachen (VS)	Personenbezogene Daten (PersDat)	Sonstige schutzbedürftige Informationen (SchutzInfo)
	Verschlusssachen (VS) sind im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse, unabhängig von ihrer Darstellungsform. Sie werden entsprechend ihrer Schutzbedürftigkeit von einer amtlichen Stelle oder auf deren Veranlassung eingestuft.	Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (§ 3 Abs. 1 Bundesdatenschutzgesetz (BDSG). Sicherheitsmaßnahmen müssen in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen	Sonstige schutzbedürftige Informationen dienen, ohne Verschlusssache oder personenbezogene Daten zu sein, der Erfüllung von Aufgaben der Behörde und/oder zur Wahrung ihrer Interessen und ihres Ansehens und sind deswegen zu schützen. Solche Informationen sind z. B. logistische Daten, Haushaltsdaten, Planungsdaten, Betriebsdaten, Einsatzdaten. Die Informationen werden entsprechend ihrer Schutzbedürftigkeit in drei Schutzbereiche unterteilt.
Schutzklasse 1	**VS- NUR FÜR DEN DIENSTGEBRAUCH** Wenn die Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein kann.	**PersDat 1** Kriterium: Betroffener kann in seinem Ansehen geschädigt werden. Daten, die der Identifikation dienen (z. B. Name, Adresse, Rufnummer, Akad. Titel) oder vergleichbare Daten (z. B. Berufs- oder Dienstbezeichnung) aber auch Organigramme und Einkommensverhältnisse.	**SchutzInfo 1** Informationen, deren Verlust der Vertraulichkeit, Verbindlichkeit, Integrität oder Verfügbarkeit die Erfüllung von Aufgaben der Behörde erschweren kann oder für ihre Interessen oder ihr Ansehen nachteilig sein kann. Informationen, die keinem Dienstgeheimnis unterliegen (z. B. Gesetzestexte, Texte aus öffentlich zugänglichen Quellen), brauchen nicht gegen den Verlust der Vertraulichkeit geschützt zu werden.
Schutzklasse 2	**VS- VERTRAULICH** Wenn die Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder schädlich sein kann.	**PersDat 2** Kriterium: Betroffener wird in seiner sozialen Existenz bedroht. Daten, die dem allgemeinen oder einem besonderen Amtsgeheimnis unterliegen. Einem besonderen Amtsgeheimnis unterliegen z. B. Personalaktendaten, Daten in Sicherheitsakten, Daten über religiöse und politische Anschauungen, medizinische Daten, psychologische Gutachten.	**SchutzInfo 2** Informationen, deren Verlust der Vertraulichkeit, Verbindlichkeit, Integrität oder Verfügbarkeit die Erfüllung von Aufgaben der Behörde gefährden kann oder für ihre Interessen oder ihr Ansehen schädlich sein kann.

Schutzklasse 3	**GEHEIM** Wenn die Kenntnisnahme durch Unbefugte die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder gefährden oder ihren Interessen schweren Schaden zufügen kann. **STRENG GEHEIM** Wenn die Kenntnisnahme durch den Bestand oder lebenswichtige Interessen der Bundesrepublik Deutschland oder eines ihrer Länder gefährden kann.	**PersDat 3** Kriterium: Betroffener wird in seiner physischen Existenz bedroht. Daten, die einem Berufsgeheimnis unterliegen oder deren Sensitivität gleichwertig ist. Beispielsweise Daten von Personen, die dem Zeugenschutzprogramm unterliegen, Adressen von polizeilichen V-Leuten.	**SchutzInfo 3** Informationen, deren Verlust der Vertraulichkeit, Verbindlichkeit, Integrität oder Verfügbarkeit die Erfüllung der Aufgaben der Behörde ausschließen kann oder ihrem Interesse oder ihrem Ansehen schweren Schaden zufügen kann.