IP Telefonie: Protokolle, Herausforderungen, Lösungen und kritische Analyse der Sicherheit

Prof. Dr.-Ing. Ralf Steinmetz, Dipl.-Inf. Ralf Ackermann, Dipl.-Ing. Utz Rödig, Dipl.-Ing. Manuel Görtz, Dipl.-Ing. Markus Schumacher,
TU Darmstadt

1 Überblick

Paketvermittelte Netze wie das IP-basierte Internet werden immer häufiger nicht nur zur Datenkommunikation, sondern auch zur Übertragung von Sprache eingesetzt. In diesem Zusammenhang erscheinen neue Schlagworte wie „Voice over IP“, „Internet-Telefonie“ oder auch „IP-Telefonie“ und die Erwartung, durch eine Konvergenz der Netze Kosten einzusparen sowie neue Mehrwertdienste zu etablieren.
Um entsprechende Lösungen erfolgreich umsetzen zu können, ist ein grundlegendes Verständnis der Technologie, ihrer Besonderheiten und Chancen aber auch Risiken notwendig.
Innerhalb dieses Artikels stellen wir – nach einer Einführung der generellen Konzepte der IP-Telefonie – am Lehrstuhl KOM der TU Darmstadt entwickelte und eingesetzte Basiskomponenten für deren praktische Umsetzung vor. Abschließend zeigen wir unsere Erfahrungen bei der Evaluierung von Sicherheitsrisiken und Verletzlichkeiten der Systeme.

2 Historie und Grundlagen

Seit etwa 1990 gibt es Versuche zur Echtzeit-Sprachkommunikation über das Internet und seit 1995 existieren auch mehrere kommerzielle Produkte. Die erste (in der Regel noch proprietäre) Generation von entsprechenden Telefonie-Lösungen ermöglichte es, mit Hilfe von Mikrofon, Lautsprecher und Soundkarte Audioverbindungen zwischen mehreren Teilnehmern herzustellen.
Die zu übertragende Sprache wird dazu in den Endgeräten digitalisiert, geeignet komprimiert und in IP-Paketen unter Einsatz des Realtime Transport Protocols RTP

[7] zum korrespondierenden Gesprächspartner übertragen. Bei diesem erfolgt nach einem entsprechenden Ausgleich von Netzwerk-Laufzeitschwankungen (Jitter) die Decodierung und anschließende Wiedergabe. Verbindungen zum großen Nutzerkreis des etablierten konventionellen Telefonnetzes können über entsprechende IP-Telefonie-Gateways hergestellt werden.
Nach einer Phase eher experimentellen Betriebes bei dem von den Nutzern auch bestimmte Qualitäts- und Einschränkungen bezüglich des Umfanges der unterstützten Dienste toleriert wurden, befinden wir uns im Augenblick – getragen insbesondere von dem enormen Interesse der Anbieter etablierter Telefon-Anlagen und von Netzwerk-Equipment – im Abschnitt der Definition und Umsetzung von Diensten mit einem dem etablierten Telefonnetz vergleichbaren „Carrier Grade“ der Qualität und Stabilität. Dafür ist eine umfassende Standardisierung und die Realisierung stabiler und (betriebs-)sicherer Lösungen unbedingte Voraussetzung.

3 Grundlagen Signalisierung

Die IP-Telefonie nutzt eine Reihe von in **Bild 1** übersichtsmässig dargestellten unterschiedlichen Signalisierungs- und Übertragungs-Protokollen.
Während über die Art der Übertragung der Audiodaten mit RTP Übereinstimmung besteht, existieren im Augenblick für den gerade für den Dienst-Umfang besonders wichtigen Teil der Gesprächssignalisierung mit dem von der ITU definierten H.323 [21] und dem von der IETF getragenen Session Initiation Protocol SIP [19] zwei alternative Ansätze.

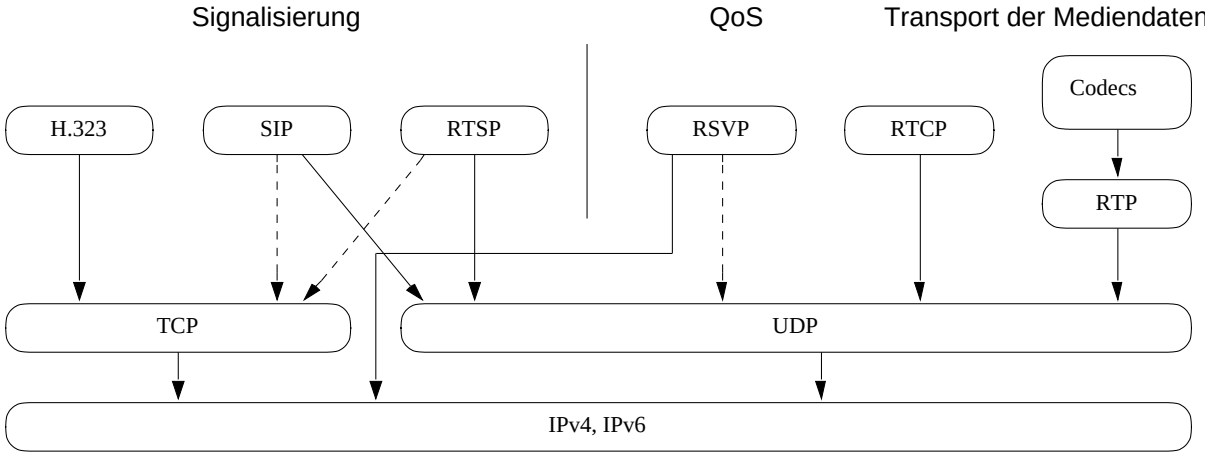

Bild 1 Zusammenwirkung der Protokolle

3.1 H.323

Die Protokollfamilie H.323 wurde von dem Standardisierungsgremium ITU-T mit dem Ziel verabschiedet, multimediale paketbasierte Kommunikation über – insbesondere IP-basierte – Netzwerke ohne spezielle QoS-Garantien zu ermöglichen. In der Protokoll-Definition ist ein umfassender Stack zusammengefasst worden, der unterschiedliche Schnittstellen für die Audio-, Video- und Datenübertragung bietet. Der Standard beschreibt weiterhin einzelne Komponenten, wie Terminals, Gatekeeper (GK), Gateways (GW) und Multicast Units (MCU), sowie die Mechanismen für deren Zusammenwirken (**Bild 2**).

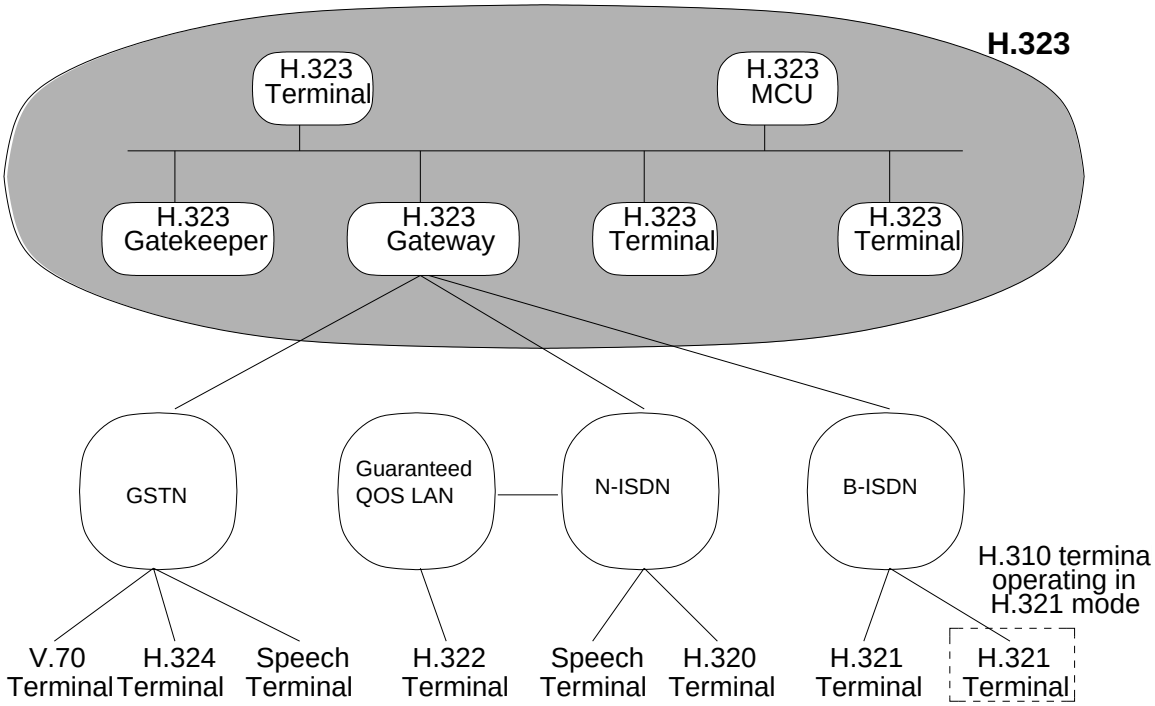

Bild 2 H.323 Komponenten

Eine zentrale H.323 Komponente bildet dabei der sogenannte Gatekeeper, der als zentrale Instanz für alle Telefonate innerhalb einer H.323-Zone fungiert. Er übernimmt u.a. die Zuordnung von Telefonnummer und symbolischen Namen, unter denen Teilnehmer bei ihm registriert sind, zu IP-Adressen sowie das Bandbreitenmanagement. Damit ist er einer klassischen Vermittlungsanlage (PBX) vergleichbar.

3.2 Session Initiation Protocol SIP

Das Session Initiation Protocol (SIP) dient zum Aufbau, Modifizieren und Terminieren von Sitzungen (Multimedia-Konferenzen, Internet-Telefonie-

Gesprächen). Die Teilnehmer können dabei mit Hilfe von SIP Invitations eine Benachrichtigung des angerufenen Gesprächspartners auslösen sowie Parameter (wie z.B. zu nutzende Codecs, Ports) mitteilen und aushandeln.
Das Protokoll unterstützt Mobilität durch Mechanismen zur Weiter- bzw. Umleitung von Requests an den aktuellen Aufenthaltsort eines Teilnehmers. Dazu können Benutzer ihren aktuellen Standort im System registrieren. (**Bild 3**) zeigt den Gesprächsaufbau mit seinen Signalisierungs-Primitiven in einem einfachen Szenario.

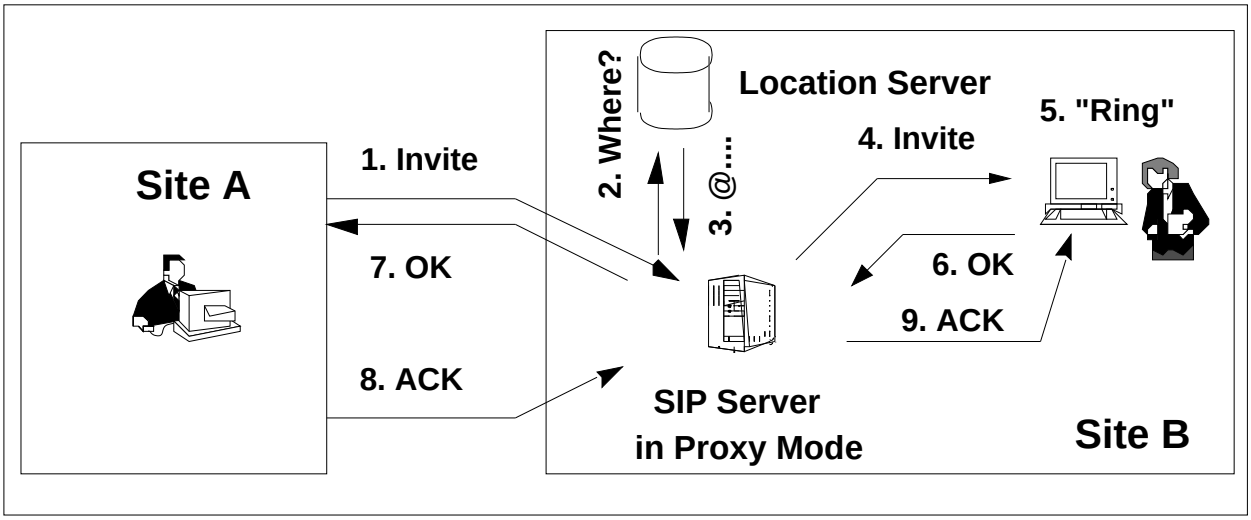

Bild 3 SIP Gesprächsaufbau

SIP ist völlig unabhängig von anderen Konferenz-Steuerungsprotokollen sowie von den Transport-Protokollen der unteren Schichten. Damit ist es äußerst flexibel und kann leicht mit zusätzlichen Eigenschaften ausgestattet werden. Eine Reihe von Herstellern entwickeln z. Z. eigene SIP-fähige Endgeräte, bzw. passen vorhandene H.323 Clients und Systeme für die Interaktion mit diesem Protokoll an.

3.3 Erweiterungen und Integration der Ansätze

Der komplexe, nicht leicht umzusetzende und mit einer Reihe von Nachteilen behaftete H.323 Ansatz hat eine sehr starke Verbreitung gefunden und nimmt zunächst noch eine vorherrschende Rolle ein, die nicht zuletzt aus seiner bisherigen Favorisierung durch die Industrie resultiert. Es zeigt sich jedoch, dass sich das eher „leichtgewichtige“ und offene SIP zunehmend zu einer wichtigen Alternative entwickelt. In der Art eines „Umbrella-Standard“ überdecken die dahingehenden Bemühungen der äußerst aktiven IETF Working Groups mittlerweile neben der eigentlichen Gesprächs-Signalisierung auch weitergehende Aspekte wie den der Präsenz-Dienste und des Instant-Messaging, aber auch des Zusammenwirkens mit dem Call Routing, Firewalls, QoS Mechanismen und dem Billing. Mit der

Verfügbarkeit entsprechender leistungsfähiger Gateways [15][17] werden beide Protokoll-Familien zukünftig auch gemeinsam einsatzfähig sein.

4 Einige ausgewählte Entwicklungen an der TU Darmstadt

4.1 Ein erweiterter SIP User Agent

Ein SIP User Agent erlaubt es dem Nutzer, sich bei einem SIP-Location-Server, einem sogenannten Registrar anzumelden und damit seinen aktuellen Standort bekannt zu geben.
Der in **Bild 4** gezeigte User Agent i2tel (Intelligent Internet Telephony) entstand auf Basis des zum Vovida SIP Stacks vorhandenen Programms sua. Aufgrund der Wahl von Unix als Software-Plattform ist die Anbindung einer (hier mit Tcl/Tk realisierten) Nutzeroberfläche unter Nutzung von Interprocess Communications Mechanismen vergleichsweise einfach möglich. Tcl/Tk wird auch für die (auch dem Anwender mögliche) Konfiguration und Erweiterung des Funktionsumfanges durch Scripting benutzt.
Alternativ und interoperabel zu dem von den Autoren verwendeten und erweiterten Client sind mittlerweile mit kphone [12] (als Teil des KDE2-Projektes) und dem von der Columbia University New York entwickelten und an Forschungseinrichtungen unter gewissen Restriktionen kostenlos lizenzierten Programm sipc [10] weitere SIP-Applikationen verfügbar. Das große Interesse der Industrie zeigt sich in der zunehmenden Anzahl auch kommerzieller User Agents [16].

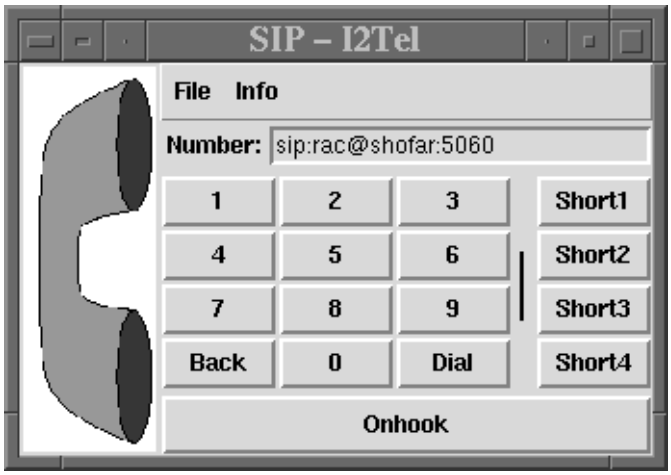

Bild 4 SIP User Agent i2tel

4.2 Ein SIP/H.323 Gateway

Im Augenblick findet die Schaffung von Übergängen zwischen den Signalisierungsprotokollen H.323 und SIP eine große internationale Beachtung.
Auf der Basis der entsprechenden IETF Standardisierungsvorschläge [20] wurden dafür erste Implementierungen realisiert [15][17].
Detaillierte Informationen zu einem von den Autoren unter Linux und mit Nutzung der (eingeschränkt) frei verfügbaren Komponenten OpenH323 und Vovida-SIP-Stack realisierten Lösungen können [17] entnommen werden.

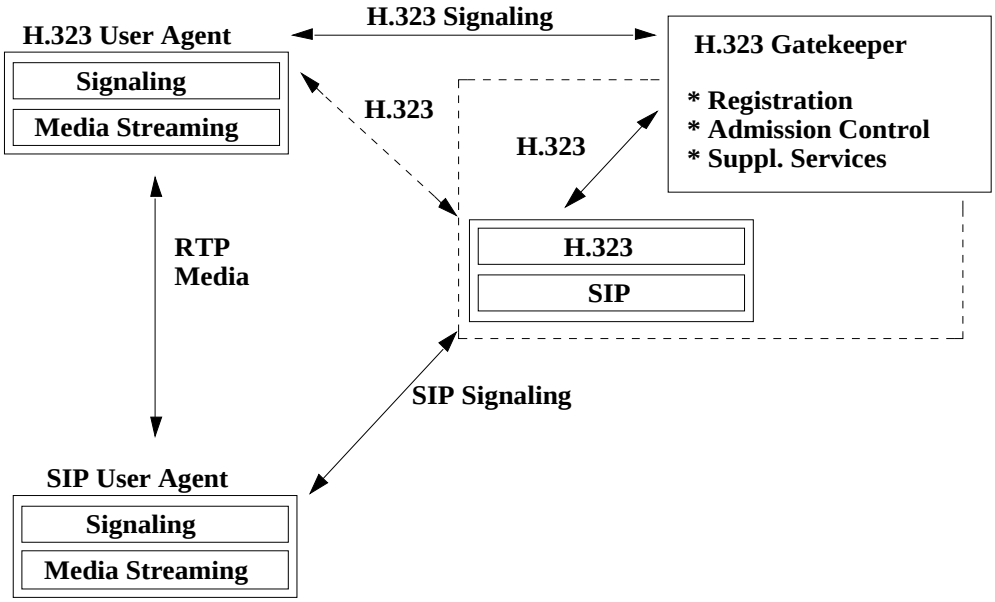

Bild 5 SIP H.323 Gateway

Wie in **Bild 5** gezeigt, wird dabei durch die Gateway-Komponente die Abbildung, Umsetzung und Weiterleitung der entsprechenden Signalisierungs-Nachrichten vorgenommen. Durch das Gateway erfolgt der Gesprächsaufbau mit seinen einzelnen Phasen (Auslösung des Rufes, „Klingeln“ beim Angerufenen, Gesprächsannahme und Aushandlung der Verbindungsparameter wie zu verwendende Ports und Codecs) in für die Teilnehmer transparenter Art. Die per RTP übertragenen Medienströme werden dann anschließend zwischen den Teilnehmern direkt versandt.

5 4 Eine Sicherheitsbetrachtung

Für die Nutzung der IP-Telefonie in einem über einen Experimentalbetrieb herausgehenden Grad ist die Sicherheit entsprechender Lösungen eine wichtige und zu hinterfragende Anforderung. Da mittlerweile von einer Reihe von Herstellern entsprechende Lösungen verfügbar werden, wurden entsprechende Überlegungen zur formalen Klassifizierung von Angriffspunkten und Verletzlichkeiten sowie praktische Experimente zu deren Ausnutzung ausgeführt und nachfolgend beschrieben.
Eine Systemkomponente zeigt dann ein (Sicherheits-) Risiko, wenn sie in ungenügender Weise gegen Missbrauch geschützt ist. Sobald diese Verletzlichkeit einmal ausgenutzt wurde, ist die für das jeweilige System vorgesehene Sicherheit gefährdet [5]. Um die möglichen Gründe und die Beschaffenheit der noch aufzuzeigenden Verletzlichkeiten zu verstehen, werden wir zuerst die Eigenschaften des ausgewerteten IP-Telefonie-Szenarios beschreiben.

5.1 Generisches IP Telefonie Szenario

Bild 6 zeigt Teile, die typischerweise verwendet werden, um ein IP-Telefonie-Szenario aufzubauen. Normalerweise umfasst dies – unabhängig vom verwendeten Protokoll (H.323, SIP oder sonstige) – eine Signalisierungs- und eine Medientransport-Ebene sowie verschiedene Telefonie-Komponenten.

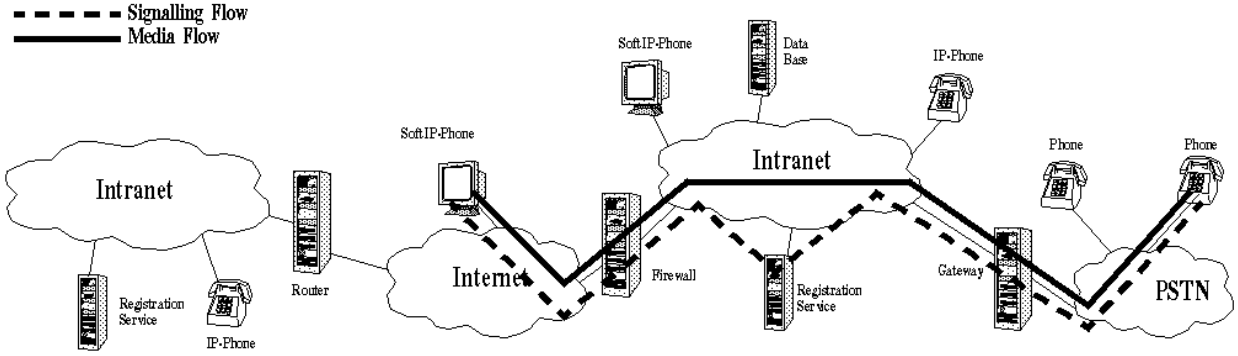

Bild 6 Generisches IP Telefonie Szenario

Die Signalisierungsebene wird verwendet, um die notwendigen Signalisierungs-Informationen zwischen den Komponenten zu transportieren. Nachdem ein Anruf aufgebaut wurde, wird die Medientransportebene dazu benutzt, um die Sprachdaten zwischen den Komponenten, z.B. Terminals oder Gateways, zu befördern. Oft erfolgt die Konfiguration der Komponenten über Fernzugriff, so dass auch Verwaltungsdaten transportiert werden müssen. Dies könnte als zusätzliche dritte

Ebene betrachtet werden, oft wird aber diese Funktion als Ergänzung zur Signalebene angesehen.
Für eine Sicherheitsbewertung muss eine Reihe von (teilweise korrespondierenden) Fakten berücksichtigt werden. Zunächst sind beide verwendeten Ebenen abhängig von derselben Infrastruktur – dem IP-Netzwerk. Verglichen mit der konventionellen Telefonie im öffentlichen Telefonnetz (mit SS#7), wo ein gewisser Grad an Isolation existiert, erhöht sich dadurch das Risiko des Systemmissbrauchs.
Zweitens wird die Netzwerk-Infrastruktur nicht von einer einzelnen administrativen Instanz oder auch nur einem kleinen (vertrauenswürdigen) Kreis von Anbietern gepflegt und verwaltet. Gefährdungen auf Signalisierungs- und Medienebene können daher auf unzuverlässigen Netzwerkteilen, -komponenten oder Betreibern beruhen.
Letztlich wird das IP-Netzwerk, das für die Signalisierungs- und Medienebenen verwendet wird, auch von anderen Diensten genutzt, und sowohl Endsystem wie auch Infrastruktur-Komponenten sind oft komplex ausgerüstete Computersysteme, die auch viele anderweitige Aufgaben ausführen können.
Anhand dieser Tatsachen kann darauf geschlossen werden, dass nicht nur Telefonie-bezogene Sicherheitsprobleme (z.B. möglicherweise fehlender Datenschutz bei den übertragenen Audio-Daten) auftreten können. Der sich ergebende Umfang an Sicherheitsproblemen ist beträchtlich größer als bei einem standardmäßigen, auf dem öffentlichen Telefonnetz basierenden Telefonie-System. Wir werden uns im Weiteren auf IP-Telefonie-spezifische Probleme konzentrieren, und nicht näher darauf eingehen, dass Router oder andere allgemeine Infrastruktur-Komponenten ebenfalls verwundbar sind.

5.2 Verletzliche Ziele in H.323

Bild 7 beschreibt ein Szenario, in dem H.323-basierte Komponenten verwendet werden. Es gilt als repräsentativ für die üblichen Betriebsbereiche und kann durch geringfügige Modifikationen auf andere, individuelle Konfigurationen angepasst werden.

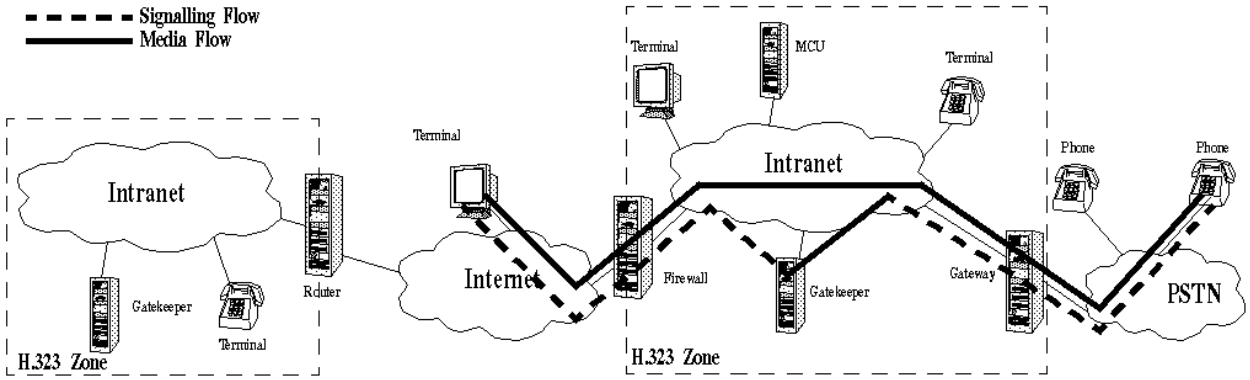

Bild 7 H.323 IP Telefonie Szenario

Mögliche Risiken und davon abgeleitete Angriffspunkte:

- Sowohl Signalisierungs- als auch Medientransportebene können Ziel eines Angriffs sein. Dies gilt für die Integrität und Vertraulichkeit der transportierten Daten, die Authentifizierung sowie die (für die Abrechnung kostenpflichtiger Dienste wichtige) nachfolgende Unleugbarkeit der Kommunikationsbeziehungen.
- Sowohl die Audio-Daten insbesondere aber auch die Signalisierungs-Information, die zwischen den Komponenten ausgetauscht werden, sind anfällig für Abhörversuche, Störungen und sogar aktive Manipulationen. Die Herausforderungen treten noch klarer hervor, wenn wir eine offene Umgebung betrachten, in der Auffinden, Auswahl und die Verwendung von Diensten und Übertragungspunkten von und zur Vermittlungsstelle (vergleichbar mit dem konventionellen „Call Routing“) dem Wettbewerb mehrerer Dienstanbieter unterliegen.
- Wenn die Identität eines Endsystems oder einer Infrastruktur-Komponente korrumpiert werden kann, dann führt dies sogar dann zu zusätzlichen Risiken, wenn Standard- und nichtgefährdete Signalisierungsmechanismen verwendet werden. Wenn ein böswilliger Benutzer sich (unter Vortäuschung einer falschen Identität) an einem H.323 Gatekeeper (oder SIP Server/Registrar) anmelden kann, kann er die Berechtigungen des von ihm angegriffenen Benutzers nutzen. Dies beinhaltet einen möglichen Eingriff in den Datenschutz (da zumindest eingehende Anrufe zum Angreifer weitergeleitet werden und er dadurch Kenntnis erhält, wer anruft). Weiterhin können hierdurch auch Dienste, die kostenpflichtig sind werden, missbraucht werden.
- Die (Anwendungs-)Umgebung, die für eine spezifische IP-Telefonie-Funktion zum Einsatz kommt, kann Ziel eines Angriffs sein. Dazu gehören z.B. auch die administrativen Schnittstellen, über die die IP-Telefonie-Funktionen konfiguriert

werden, die wiederum im (ebenfalls potentiell angreifbaren) Betriebssystem eingebettet sind.

- Sogar Systeme und Funktionen, die nicht unmittelbar involviert sind, können angegriffen werden. So könnte z.B. eine von einem IP-Telefonie-Gespräch durchlaufene Firewall geschwächt werden, weil sie IP-Telefonie-Kommunikation unterstützt (und zeitweise gewisse Kommunikationswege öffnet, die dann nicht für die normale erwünschte Konversationen, sondern für Angriffe verwendet werden können).

Der nächste Abschnitt gibt eine Auswahl aus den untersuchten Verletzlichkeits-beispielen wieder, die entsprechend der Klassifizierung eingeordnet werden können.

6 Fallstudie

Wir stellen ausgewählte Verletzlichkeiten eines auf H.323-basierenden IP-Telefonie-Szenarios (**Bild 8**) vor, das Gatekeeper und Gateways beinhaltet, die den Übergangspunkt für den (in der Regel Kosten erzeugenden und damit für Angriffe sensitiven) Übergang zur klassischen Telefonnetzwelt darstellen.

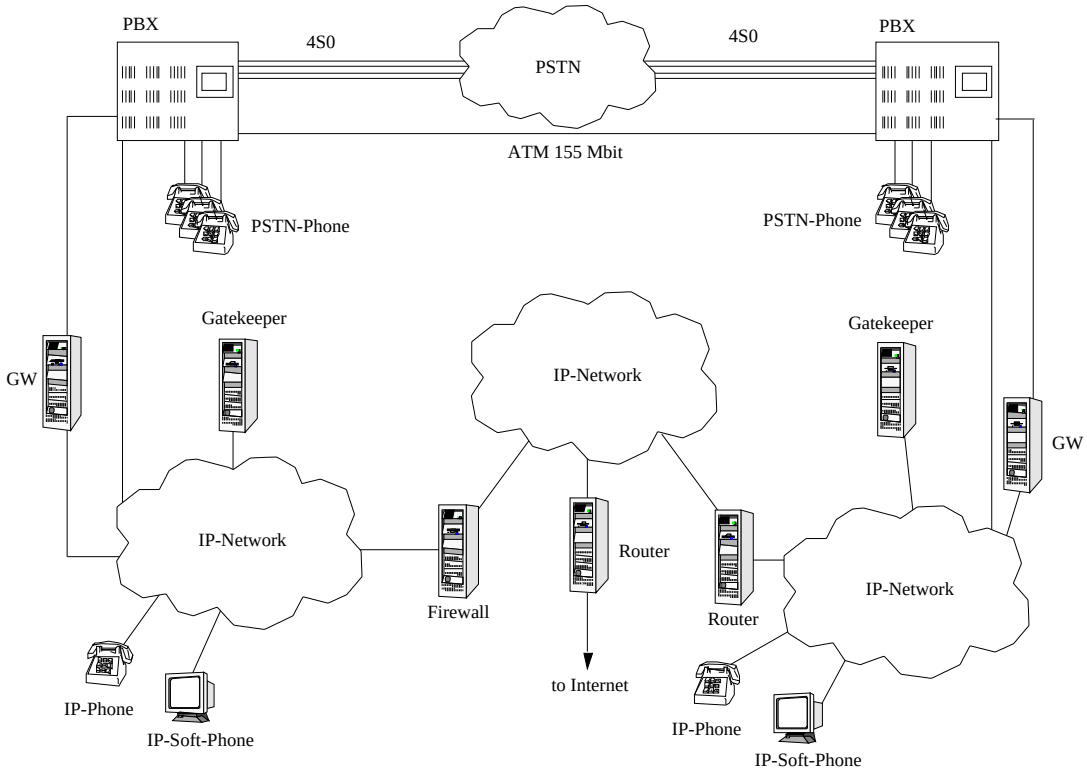

Bild 8 Untersuchtes Test Szenario

Die konventionellen Komponenten der privaten Vermittlungsstellen und ihre administrativen IP-Zugriffsstellen (die weitere mögliche Angriffspunkte bilden) werden im Bild nur aus Gründen der Vollständigkeit aufgezeigt.

6.1 Angriffe auf Endsysteme

6.1.1 Übernahme der Kontrolle eines Endgerätes

IP-Telefonie-Endsysteme befinden sich oft an öffentlich zugänglichen Orten (z.B. in Büroräumen oder auf frei betretbaren Gebäude-Fluren). Sobald ein Angreifer physischen Zugriff auf das in unserem Szenario untersuchte IP-Telefon hat, kann er es auf die werksseitige Ursprungskonfiguration zurücksetzen. Damit erhält er vollen Zugriff auf alle Konfigurationsmöglichkeiten des Geräts. (Im weiteren Text werden jeweils kursiv und in einem Rahmen einige Beispiele zu den typischen Eigenschaften der Verletzlichkeiten oder spezielle dazu benutzte Source Code-Fragmente aufgezeigt).

Dem Handbuch des untersuchten Systems entnehmbare Anweisungen:

Wiederherstellen der werksseitigen Ursprungseinstellungen
Eingabe des 6-stelligen Passworts: 124816
Zugriff auf das Verwaltungsmenü
Im Auslieferungs-Zustand lautet das Administrator Passwort 123456

Erlangen des administrativen Zugriffs auf die Telefon-Endgerät

Beispiele wie das Offenhalten von „Hintertüren“ oder schwache Ausgangs-Passwörter sind keine Mängel, die spezifisch für IP-Telefonie-Szenarien sind, sie wurden in vielen anderen Anwendungen bereits hinreichend beschrieben und untersucht, dennoch treten sie hier erneut auf. Die Schnittstelle für die Fernverwaltung (über HTTP), die das IP-Telefon verwendet, ist ebenso für Angriffe anfällig. Das Administrator-Passwort wird im Klartext versandt, wodurch die Kommunikation z.B. für Ausspionieren, angreifbar wird. Darüber hinaus kann das Administrator-Passwort auch anhand einer Reihe von automatisierten Brute-Force Versuchen angegriffen werden (wegen seiner begrenzten Länge und eingeschränktem Alphabet, da das Passwort normalerweise über die Telefontastatur eingegeben werden muss).
Sobald ein erster unerlaubter Zugriff auf das System erfolgreich war, kann das administrative Passwort sowohl für den lokalen (manuellen) wie auch für den

Fernzugriff (WWW) auf einen Wert, der dem Angreifer bekannt ist, umgesetzt und für zukünftige, böswillige Transaktionen verwendet werden. Die Gerätekonfiguration ist nun für den Angreifer sichtbar und kann benutzt werden, um zusätzliche Information über das betroffene Netzwerk, über die Benutzerkennungen und E.164 Nummern sowie für die Wiederherstellung von Werten nach einem Angriff zu erhalten. In unserem Beispiel können Details wie z.B. die IP-Adressen der IP-Telefone, ihre E.164 Nummer und die IP-Adresse der H.323. Gatekeeper, an denen die Anmeldung stattfindet, beschafft und geändert werden. Damit kann ein Angreifer die Merkmale eines Telefons so verändern, dass es sich bei einem anderen Gatekeeper (z.B. unter Kontrolle des Angreifers) anmeldet. Der Angreifer hat somit Lese- und sogar modifizierenden Zugriff auf die IP-Telefonie-Signalisierung, was wiederum für die Informationsbeschaffung über die Kommunikationskontakte (wer ruft wen an) verwendet werden kann. Weiterhin wird hierdurch der kalkulierte Abbau oder sogar die Verweigerung von Kommunikationsdiensten ermöglicht (der Benutzer kann keine Anrufe von bestimmten anderen Telefonen entgegen nehmen oder dorthin tätigen); oder es wird der Zugriff auf zu Telefonnetz-Teilnehmern ausgehende Gesprächsinhalte ermöglicht, wenn diese Gespräche über ein vom Angreifer ausgewähltes und für diesen zugreifbares Gateway geleitet werden.
Das Erschleichen von Zugriffen auf die Geräteverwaltung ist letztlich sogar dazu nutzbar, die Firmware des Endgerätes zu verändern (die das Gerät in unserem Falle für Updates aus dem Netzwerk laden kann). Obwohl dies (noch – d.h. solange noch keine Entwicklungs-APIs für Telefon-Firmware verfügbar sind – was sich mit den zukünftigen konfigurierbaren „Java-Telefonen“ verändern kann) einen hohen Aufwand für den Angreifer bedeutet, sind die Konsequenzen massiv, da eine in das Gerät neu eingespielte Firmware genau die gleichen Funktionalitäten wie das Originalgerät bieten würde, aber ständig eine Hintertür für weitere Angriffe eröffnen kann.

6.1.2 DoS Angriff über IP Telefonie Signalisierung

Die von uns ausgewerteten Endsysteme (sowohl ein kommerzielles Hardware-Telefon als auch das Open Source Programm ohphone [14]) waren nicht in der Lage, einem Angriff, bei dem unerwartete oder inkorrekte H.323 Signalisierungs-PDUs versandt wurden, zu widerstehen. Dies hatte zur Folge, dass ein System entweder zeitweise nicht verfügbar war, oder dass das System sogar ganz ausfiel, weil das Gerät blockierte, abstürzte oder neu startete.
Im Fall eines Angriffes mit Anmeldung unter einer gefälschten Identität – den wir nachfolgend noch detailliert beschreiben werden – kann ein böswilliger Angreifer zuerst eine DoS-Attacke anwenden, um (eventuell auch nur zeitweise) die Pakete

aus dem Ursprungssystem zu unterdrücken, während er die Anmeldung/Abmeldung eines anderen, böswilligen Endsystems startet.

6.1.3 Vorgehen und Implikationen bei DoS Angriffen

Das untersuchte IP-Telefon benutzt einen integrierten WWW Server, mit dem das Gerät verwaltet und einige seiner Einstellungen abgefragt werden können. Dieser WWW Server und seine Implementierungsmängel (obwohl nicht grundlegend verantwortlich für die IP-Telefonie-Funktionen des Gerätes) machen es für böswillige Angriffe anfällig. Wenn an den integrierten WWW-Server eine ausreichend lange URL versandt wird, kann das Gerät (abhängig von der Länge des URL Strings) entweder ausser Betrieb gesetzt werden oder es wird neu gestartet.

```
/* verwendet Standard TCP-Socket Kommunikation an Port 80 (HTTP) */
...
memset(query_string, 0x1, 256);
query string [256] = 0x0;
write(sock, query string, sizeof(query string));
...
```

Denial of Service Angriff auf den HTTP Server des Telefons

Für den Angriff sind seitens des Angreifers nur geringfügige Fertigkeiten, einfache Methoden und wenig Aufwand notwendig (wir haben den Angriff unter Nutzung eines Standard-Browsers, mit einem Telnet Tool oder einem minimalen Test-Programm durchgeführt), dennoch können gleichzeitig alle Endsysteme einer Installation attackiert werden.

6.1.4 Angriff auf die Privatsphäre des Anwenders

IP-Telefonie-Anwendungen benutzen mit dem UDP-Protokoll versandte RTP-Pakete [7], um Audio-Datenströme zu befördern. Obwohl Grundmechanismen für die Benutzung symmetrisch verschlüsselter [1] Audio-Payloads in RTP-Paketen in einem entsprechenden RTP-Profil [6] beschrieben werden, ist deren Anwendung bisher nicht weit verbreitet. Ein potentieller Abhörer muss die Datenströme, die die Audioverbindung(en) repräsentieren, zunächst identifizieren. Da die Ports, die hierfür verwendet werden, typischerweise dynamisch ausgehandelt werden, ist dies nicht unmittelbar trivial. Mit den öffentlich verfügbaren IP-Telefonie Protokoll-Stacks und mit einer sehr detaillierten Beschreibung des Protokollmechanismus wird ein Angriff jedoch sogar für einen Laien immer einfacher. Für die Untersuchung haben wir eine Methode entwickelt und getestet, die es uns erlaubt, Anrufe unbemerkt zu überwachen und/oder aufzuzeichnen. Dabei kann über spezielle Kriterien aus der Menge des innerhalb eines Netzes geführten IP-Telefonie-

Gespräche selektiert werden (so kann man z.B. eine E.164 Nummer, deren Gespäche abgehört werden sollen, spezifizieren).

```
/* uses libpcap for packet capturing */
...
#define RTP.PAYLOAD.OFFSET 0 + 14 +20 + 8 + 12
...
while (!finished)
(packet (u char ) pcap next(pcap, &pkthdr);
...
write(audio fd, (unsigned char )packet RTP.PAYLOAD.OFFSET,
rtp.payload.size);
...
```

Abhören von Audiodaten durch Zugriff auf die (ungeschützte) RTP-Payload

Anstatt eines Shared Ethernets wird in der Regel eine strukturierte Verkabelung mit dedizierten Leitungen zu jedem Teilnehmer als grundlegende Voraussetzung für einen ausreichenden Datendurchsatz und geringe Audio-Paketverzögerung angesehen. Daher wird oft damit argumentiert, dass der Einsatz von Switches anstatt von Hubs die Problematik des unberechtigten Zugriffs auf Datenverbindungen eingrenzt. Neuere Veröffentlichungen zeigen jedoch, wie anfällig auch solche Konfigurationen für Angriffe sind. Nachdem gefälschte ARP-Antworten an einen Switch gesandt werden, beginnt dieser, Daten nicht nur zum dedizierten Port eines Benutzers zu senden, sondern diese auf alle Switch-Interfaces (und damit auch zum Angreifer) zu übertragen.

6.2 Angriffe auf Infrastruktur Komponenten

6.2.1 Angriff auf die Gatekeeper Anmeldung

Während der Anmeldung an einem Gatekeeper registriert ein H.323 Gerät seine IP-Adresse, seine E.164 Nummer und eine beliebige Anzahl zusätzlicher symbolischer Namen (sogenannte Aliase). Dieser Mechanismus ist Teil der H.225 RAS-Signalisierung (RAS = Registration, Admission, Status) und erlaubt eine vergleichsweise leichte Selbstkonfiguration und Mobilität der Geräte innerhalb einer vorgegebenen lokalen Umgebung.

Typischerweise verfolgt der Gatekeeper eine bestimmte Policy, die angibt, ob nur eine bereits vorkonfigurierte Menge an E.164 Nummern / symbolischer Namen und IP-Adressen zur Anmeldung zugelassen wird, oder ob sich jedes potentielle Endsystem anmelden kann. Dies ist eine rein administrative Entscheidung, die nicht im Umfang der eigentlichen H.323-Standardspezifikation enthalten ist. Im besten Falle stellen Gatekeeper (fein granular) konfigurierbar frei welche Verfahrensweise,

eingesetzt werden soll, und verwenden eine restriktive Standard-Verfahrensweise. Diese ist vorkonfiguriert und läßt willkürliche Zugriffe nicht zu. Auf die Systeme, die wir untersucht haben, trifft dies jedoch nicht zu.
Bei traditionellen Nebenstellensystemen sind Rechte (wie z.B. ob eine bestimmte Person Ferngespräche oder internationale Gespräche führen darf) normalerweise an die Benutzerkennung gebunden. Dieser Mechanismus kann ohne zusätzliche (z.B. kryptographische) Schutzvorkehrungen durch „Diebstahl“ oder durch Nachahmung von Benutzerkennungen ausgenutzt werden. Wenn die Anmeldung nicht eingegrenzt wird, kann der Anmeldemechanismus zum Missbrauch von Kommunikationsdiensten ausgenutzt werden, wobei dies oft beinhaltet, dass Aussenstellen mittels IP Telefonie über Gateways im regulären Telefonnetz anrufen, ohne für diesen Dienst zu zahlen. Auch können so Kosten mit Anrufen bei Servicenummern verursacht werden, wobei ein Angreifer aus den Verbindungen zu diesen möglicherweise finanzielle Vorteile zieht.

```
/* uses OpenH323 for PDU generation */
/* we show the unregistration part */
/* an attacker can register then */
...
UnRegReq.m callSignalAddress.SetSize(1);
(UnRegReq.m callSignalAddress[0]).SetTag(
H225 TransportAddress::e ipAddress);
H225 TransportAddress ipAddress                    &
h225 transportaddress ipaddress =
(UnRegReq.m callSignalAddress[0]);
h225 transportaddress ipaddress.m ip[0] = ip[0];
h225 transportaddress ipaddress.m ip[1] = ip[1];
h225 transportaddress ipaddress.m ip[2] = ip[2];
h225 transportaddress ipaddress.m ip[3] = ip[3];
h225 transportaddress ipaddress.m port.SetValue(port);
...
sendto(sock, data d, data s, 0, (struct sockaddr )&name, size-
of(name));
...
```

Angriff durch gefälschte Gatekeeper An- bzw. Abmeldungen

Als Mindestschutz könnten z.B. nur Abmeldeaufforderungen, die die IP-Adresse des zuvor angemeldeten Teilnehmers enthalten, befolgt werden, während andere nicht berücksichtigt werden oder sogar Warnungen oder Alarm beim System-

administrator auslösen. Da die (Ab-) Anmelde-IP-Adresse in der (normalerweise ungeschützten) H.323 PDU-Last enthalten ist, kann sie leicht gefälscht werden. Zusätzliche Überprüfungen (z.B. der Test, ob die IP Quellenadresse des PDU mit der korrekten Stelle übereinstimmt) müssen entweder hinsichtlich ihrer allgemeinen Anwendbarkeit bewertet werden (z.B. im Falle von Bevollmächtigungsvorgängen oder zusätzlicher, aus dem Gateway stammenden Mitteilungen), oder sie können mittels Manipulation an der IP Schicht durchbrochen werden. (Dies stellt zwar eine Zusatzbelastung für den Angreifer dar, kann aber auch überlistet werden, was ebenfalls gezeigt werden kann.)
Rein kryptographische Methoden wie die in H.235 [2] beschriebenen H.323 Protokollerweiterungen bilden eine bessere Basis für Schutzmechanismen. Sie sind jedoch in den von uns ausgewerteten Geräten nicht implementiert.

6.2.2 DoS Angriffe auf Gatekeeper

Wir konnten alle betrachteten Gatekeeper (sowohl kommerzielle wie auch Open Source [4,13]) daran hindern, ihre normalen Aufgaben auszuführen, indem wir ihnen eine große Anzahl von entweder regulären (zyklischen Endgeräteanmeldungen bzw. -abmeldungen) oder irregulären H.323 PDUs zusandten. Dadurch steht der IP-Telefonie-Dienst entweder nur für eine gewisse Zeit oder überhaupt nicht mehr zur Verfügung (falls der Gatekeeper zum Absturz gezwungen wurde).
Hier ist zu erwähnen, dass für diese DoS-Angriffe nur eine verhältnismäßig geringe Bandbreite benötigt wird, da sie die Signalisierung betreffen. Es ist generell schwierig, einen Gatekeeper zu schützen (z.B. anhand einer Firewall), wenn er regelmäßige Kommunikationsbeziehung mit “Draussen” für seine normalen Aufgaben aufrechterhalten muss (z.B. wenn Clients regelmäßig anrufen dürfen).

6.3 Zusammenfassende Aussagen zur Sicherheit

6.3.1 Ergebnisse der Bewertung

Die von uns beschriebenen Szenarien wurden innerhalb unserer universitären Umgebung ausgewertet, und – sobald einmal IP-Telefone (auf der gegenwärtigen Sicherheitsebene) regulär in den öffentlich zugänglichen Netzwerksegmenten unseres Universitätsbereiches installiert werden – halten wir diese auch für ziemlich realistisch. Die Installation in nur einem einzigen Netzwerk (damals für Daten und Sprachverkehr verwendet) war einer der vielen Gründe, mit dem Einsatz von IP-Telefonie zu beginnen – so dass Szenarien, die auf den Einsatz zweier separater (d.h. in diesem Fall beide IP-) Netzwerke abzielen, als nicht realistisch angesehen werden.

Sogar wenn potentiell ein gewisses Niveau an „Abgrenzung“ durch die Verwendung von VLAN Techniken erzielt werden könnte, würde dies jedoch auch die erfolgsversprechenden Möglichkeiten für die enge Interaktion bzgl. System und Telefonie eingrenzen, was ja eigentlich die Basis für neue und innovative Dienste bildet.
Es sollte auch erwähnt werden, dass es bei beim konventionellen Telefonnetz nur wenige Einstiegspunkte auf zentrale Komponenten gibt, die allerdings ein sehr hochspezialisiertes Wissen über die Geräte erfordern. Dies ist abweichend von der Situation, die im IP-Umfeld vorherrschen. Hier reicht für die Angriffe ein Zugriff auf IP-Netzwerk, in dem auch die IP-Telefonie-Infrastrukturkomponenten zu erreichen sind. Das Wissen über diese Komponenten, wie z.B. die H.323-Gatekeeper oder H.323-zu -Telefonnetz-Gateways, sind in Form von Open Source Projekten [3] [13] offen. Die Implementierungen sind frei verfügbar und können leicht beschafft, angepasst und eingesetzt werden.

6.3.2 Mögliche Gegenmaßnahmen

Dieser Artikel konzentriert sich absichtlich auf die Suche (basierend auf der theoretischen Analyse der Protokolle und Szenarien), Beschreibung und praktische Ausnutzung von Verletzlichkeiten. Wir verweisen nur kurz auf mögliche Gegenmaßnahmen, die in zwei Klassifizierungen unterteilt werden können:

- kurzfristig und mehr oder weniger reine “Fehlerbehebung” (was definitiv notwendig ist, aber nicht die Problemsituation im allgemeinen ändert),
- längerfristig und umfassend (was wir als ein generelles Muss für die praktische Durchführbarkeit und den Erfolg von IP-Telefonie-Lösungen sehen).

6.3.3 IP Telefonie spezifischer Ansatz

Sowohl IETF als auch ITU zeigen neuerdings weitere Bemühungen, Standardisierungen anzubieten, die auch den Sicherheitsaspekt abdecken. Die ITU z.B. bietet einige Erweiterungen zum H.323 Rahmenwerk, die spezifizieren, wie Sicherheit hinzu gefügt werden kann [2]. Bei SIP sind kryptographische Authentifizierung und Datenschutzeinrichtungen innerhalb der Basis-RFC bereits definiert. Eine Übersicht über diese sicherheitsbezogenen Erweiterungen für den IP-Telefonie-Standard befindet sich in [5]. Wie in diesem Beitrag aufgezeigt, sind diese Protokollerweiterungen notwendig, um einige der Sicherheitsproblematiken lösen zu können, sie stellen aber keine allgemeine und automatische Sicherheitslösung für bereits durchbrochene Systemkonzeptionen dar.

6.3.4 Herstellen eines Security Improvement Feedback Loops

In [8] haben wir das Konzept eines Security Improvement Feedback-Loop (SIF) (Rückkopplung zur Verbesserung der Sicherheit) vorgestellt. Darunter verstehen wir die systematische Art und Weise, Sicherheitsschwächen zu verstehen und effiziente Lösungen auszuarbeiten. Das SIF-Konzept besteht aus vier Schritten:

- **Observation:** Sicherheitsschwächen bestehender Systeme werden beobachtet und in verschiedenen Formen wie z.B. Mailing Listen, Newsgroups und Artikeln reflektiert.
- **Informationsabfrage:** aus unterschiedlichen Quellen werden Informationen zusammengetragen. Im Fall von elektronischen Dokumenten kann dies automatisch erfolgen. Bei der Eingabe von Informationen aus nicht-digitalen Quellen können Anwender durch formularähnliche Schnittstellen unterstützt werden.
- **Sortieren:** die Daten werden anhand eines einheitlichen, hoch strukturierten Datenschemas umgewandelt, da dies für die weitere maschinenbasierte Verarbeitung vorteilhafter ist. Sortierfilter können eingesetzt werden, um die Bedeutung der Informationen, die in Datenbanken bzgl. Verletzlichkeit gespeichert werden, zu gewichten.
- **Analyse und Verwertung:** wie in [9] beschrieben, helfen entsprechende Datensuchprozeduren Muster zu identifizieren und zu verbessern, die selbst wiederum angewandt werden können, um neue Systeme zu konstruieren oder bestehende zu verbessern. Dieses Wissen kann z.B. zur Ausarbeitung von Sicherheitskonzeptprofilen und Sicherheitsrichtlinien genutzt werden, und direkt in Sicherheits-Tools eingehen. Somit wird die Sicherheit neuer und bestehender System verbessert, da bekannte Fehler nicht wieder auftreten sollten. Die Rückkopplung ist damit vollständig.

Der Ansatz über die Datensuche liefert wertvolle Einsichten für die Verbesserung der Sicherheit. Unser langfristiges Ziel ist es, eine Reihe umfassender Sicherheitsprofile für sichere verteilte Anwendungsdomänen zu identifizieren, unter denen die IP Telefonie nur eine ist.

7 Ausblick

Allgemein wird erwartet, dass sich bei der IP-Telefonie ein enormes Potential aus dem Zusammenwirken der unterschiedlichen Dienste ergibt. Aber die aufgezeigten Probleme können und müssen von den Geräteherstellern korrigiert werden und

sollten bei zukünftigen Entwicklungen auf jeden Fall vermieden werden. Wir sind davon überzeugt, dass ein kritischer Blick auf die gegenwärtige Situation hilfreich ist, um mögliche Gefahren für den Anwender, den Operator und die Herstellerinteressen zu vermeiden, sobald die Geräte einmal in größeren Mengen installiert werden.

Anmerkung: Beiträge zu dieser Publikation stammen aus **Entwicklung und Nutzung von IP-Telefonie Anwendungen auf UNIX Systemen und Verletzlichkeiten und Sicherheitslimitationen gegenwärtiger IP-Telefoniesysteme**

8 Literatur:

[1] D. Balenson: Privacy enhancement for Internet electronic mail: Part III: Algorithms, modes and identifiers, RFC 1423, January 1993.

[2] ITU-T. Security and Encryption for H Series (H.323 and other H.245 based) Multimedia Terminals. ITU-T Recommendation H.235, February 1998.

[3] OpenH323 Project. OpenH323. http://www.openh323.org/.

[4] OpenH323 Project. OpenH323 Gatekeeper; http://www.opengatekeeper.org.

[5] Christoph Rensing, Utz Roedig, Ralf Ackermann, and Ralf Steinmetz: A Survey of Requirements and Standardization Efforts for IP-Telephony-Security. In M. Schumacher and R. Steinmetz, Editors, Sicherheit in Netzen und Medienströmen, Informatik aktuell, pages 50-60. Springer Verlag, September 2000.

[6] H. Schulzrinne: RTP profile for audio and video conferences with minimal control. RFC 1890, January 1996.

[7] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson: RTP: A Transport Protocol for Real-Time Applications. RFC 1889, January 1996.

[8] Markus Schumacher, Ralf Ackermann, and Ralf Steinmetz: Towards Security at all Stages of a System's Life Cycle. In 2000 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), 2000.

[9] Markus Schumacher, Christian Haul, Michael Hurler, and Alejandro Buchmann: Data-Mining in Vulnerability Databases. (90), 2000.

[10] Columbia University SIP UA sipc; http://www.cs.columbia.edu/hgs/sipc/.

[11] Java Telephony API (JTAPI); http://java.sun.com/products/jtapi/.

[12] kphone and libdissipate; http://www.div8.net/dissipate/.
[13] Openh323 Gatekeeper; http://www.willamowius.de/ openh323gk.html.
[14] OpenH323, Part of the Linux VOXILLA Telecom Project; http://www.openh323.org/.
[15] SIP-H.323 Signaling Gateway; http://www.cs.columbia.edu/kns10/ research/gw/.
[16] The Softswitch Consortium; http://www.softswitch.org/.
[17] R. Ackermann, V. Darlagiannis, and R. Steinmetz: Implementation of a H.323/SIP Gateway; Technical Report TR-2000-02, Darmstadt University of Technology, Industrial Process and System Communications (KOM), July 2000.
[18] Siemens SIP software for LP5100; http://www.mediatrix.com/corpo/ pressrelease/SiemensSIPPhone.html.
[19] M. Handley, H. Schulzrinne, E. Schooler, and J. Rosenberg: SIP: Session Initiation Protocol, RFC 2543, March 1999.
[20] K. Singh and H. Schulzrinne: Interworking between SIP/SDP and H.323, Internet Draft draft-singh-sip-h323-01.txt.
[21] International Telecommunication Union: Packet based Multimedia Communication Systems, Recommendation H.323, Telecommunication Standardization Sector of ITU, Geneva, Switzerland, February 1998.