[AG05] *Ralf Ackermann, Manuel Goertz:* **Voice over IP Security;** Die Zeitschrift fur Informations-Sicherheit, 05(05), Oktober 2005, S. 36-40.

Voice over IP Security

Sicherheitsrelevante Herausforderungen bei VoIP – eine kritische Bestandsaufnahme

Auch bei Voice over IP (VoIP) beginnt eine sinnvolle Vorgehensweise mit der Analyse und Klassifikation von Bedrohungen und Risiken. Zudem beleuchtet der vorliegende Beitrag den aktuellen Stand der Technik und nennt wichtige Fragen für ein „Best Practice"-Vorgehen in Sachen VoIP-Security.

Von Ralf Ackermann und Manuel Görtz, Darmstadt

Voice over IP (VoIP) hat sich vom eher experimentell und im begrenzten Umfang eingesetzten Telefonieverfahren heutzutage zu einer breit genutzten Technik mit einer weiterhin zu erwartenden großen Wachstumsdynamik entwickelt. Sowohl im privaten Umfeld als auch in Unternehmensnetzen kommt VoIP zunehmend zum Einsatz. Diese wichtige Rolle im Rückgrat teilweise sensitiver Kommunikationsprozesse führt zwangsläufig zu einer Reihe von Fragen sowohl hinsichtlich der Sicherheit der verfügbaren oder zukünftig einzusetzenden Systeme als auch zu deren sicherheitsrelevanten Implikationen und Wechselwirkungen mit anderen Teilen der Kommunikations- oder IT-Infrastruktur.

Generell bietet sich für VoIP-Systeme eine Klassifikation hinsichtlich dreier Kernaspekte an:

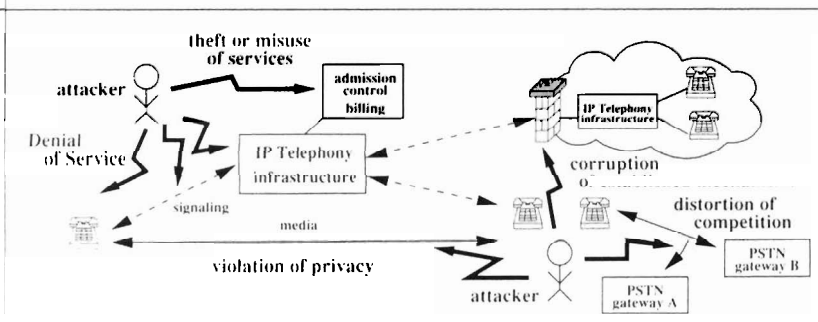
- *Protection Aspect:* Absicherung der Systemfunktion und der übertragenen Signalisierungs- und Mediendaten (vgl. Abb. 1)
- *Enabling Aspect:* fehlerfreier und hinsichtlich des Funktionsumfangs unbeschränkter Betrieb in Umgebungen mit bereits vorhandenen sicherheitsrelevanten Komponenten (z. B. Firewalls – vgl. Abb. 2) und
- *Management and Operation Aspect:* fortlaufender sicherer Betrieb (vgl. Abb. 3)

Eine derartige systematische Herangehensweise ermöglicht es Systeme, die unterschiedliche Signalisierungsverfahren (z. B. SIP oder H.323) benutzen, in vergleichbarer Art zu analysieren und generell vorhandene Angriffspunkte oder auch spezielle Notwendigkeiten zum Schutz zu erkennen. Für Mechanismen des Session Initiation Protocol (SIP) sei hier auf den <kes>-Beitrag „Protokollfragen – VoIP-Security bei SIP & Co." verwiesen [8].

Typische Angriffspunkte in einem VoIP-Telefonie-Szenario sind das Abhören von Signalisierungsdaten und Übertragungsinhalten, Attacken auf Call Routing und Abrechnung sowie das Ausnutzen von Verletzlichkeiten von Komponenten, die nicht unmittelbar für die VoIP-Funktion zuständig sind, aber entsprechende Rückwirkungen ermöglichen (vgl. Abb. 4–6).

Diese Szenarien zeigen, dass nicht nur das häufig diskutierte Risiko des Abhörens von Signalierungs- und Mediendaten eine sehr wichtige Rolle spielt. Vielmehr sind auch der generelle Schutz der Signalisierungsinformationen sowie eine wechselseitige Authentifizierung aller beteiligten Komponenten und die Robustheit von nicht primär für die Medienübertragung verantwortlichen, aber dennoch in VoIP-Infrastruktur- oder -End-Systemen eingesetzten Funktionen überaus wichtig. Zu jedem der genannten Angriffsmuster wurden 2001 in einer Untersuchung erfolgreiche Exploits für damals verfügbare (auch kommerzielle) Komponenten gefunden [1].

Abbildung 1
Angriffspunkte und Verletzbarkeiten von VoIP-Systemen



Angriffs-Tools

Potenziellen Angreifern stehen durch Open-Source-Code, der zunächst für den Aufbau und Betrieb von VoIP-Lösungen geschrieben wurde, leistungsfähige Bausteine auch für missbräuchliche Verwendung zur Verfügung. So können im Source-Code vorhandene und gut dokumentierte Implementierungen der Protokollstacks von VoIP-Systemen teilweise unmittelbar oder durch geringfügige Modifikation dazu genutzt werden, um mithilfe von Packet-Sniffer-Tools aufgezeichnete Signalisierungs- oder Mediendaten zu analysieren, auszugeben, gegebenenfalls modifiziert wieder einzuspielen oder sogar zum Zwecke von Angriffen komplett neu zu erzeugen (Näheres in [1,2]).

Nicht zuletzt wurde in entsprechenden Untersuchungen eine hohe Anfälligkeit der komplexen für die Signalisierung genutzten VoIP-Protokollimplementierungen gegen bewusst falsch formatierte oder in falscher Abfolge zugesandte Signalisierungsnachrichten festgestellt. Dies ist vor allem unter dem Aspekt möglicher Denial-of-Servive-Angriffe (DoS) kritisch, da hierbei mit relativ geringem versandten Datenumfang eine deutliche Schadwirkung erreicht werden kann. Gleiches gilt auch für die mit hoher Frequenz durchgeführte Abarbeitung von prinzipiell zulässigen Protokollsequenzen, etwa fortlaufende Registrierung und Deregistrierung von Teilnehmern oder einen wiederholten, jedoch vor seiner erfolgreichen Fertigstellung wieder abgebrochenen Sitzungsaufbau.

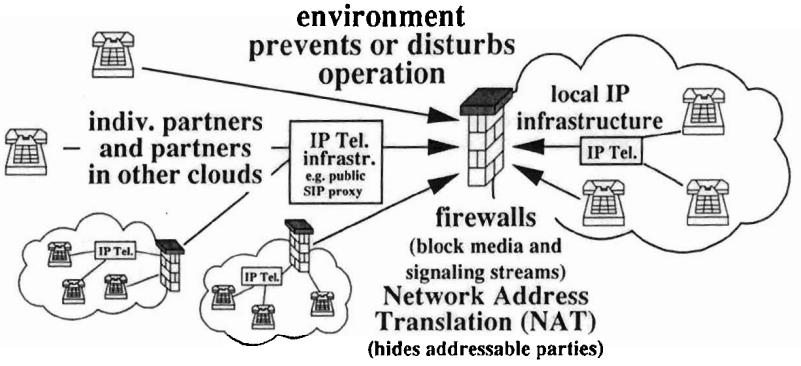


Abbildung 2: Aspekte der Einbindung von VoIP-Lösungen in Umgebungen mit bereits vorhandenen sicherheitsrelevanten Infrastrukturelementen

Vor solchen Angriffen lassen sich Infrastruktursysteme nur schwer schützen, da sie letztlich exponiert aufgestellt sein müssen, um im regulären Betrieb verwendete Signalisierungsdaten korrekt erhalten und verarbeiten zu können. Hier wird die Wichtigkeit eines fortlaufenden Monitorings des Systemverhaltens sowie einer VoIP-spezifischen Intrusion Detection (IDS) mit der Möglichkeit zur zeitnahen Auslösung von Gegenmaßnahmen deutlich. Wird dadurch ein typisches Angriffsmuster identifiziert, so kann das angegriffene System beispielsweise durch entsprechend parametrisierte Filtermechanismen einer Firewall von der – falls möglich eindeutig bestimmten – Quelle des Angriffs abgeschirmt werden.

Eine Vielzahl der 2001 erkannten Probleme wurde von den VoIP-System-Anbietern mittlerweile behoben oder für neue Entwicklungen berücksichtigt. So kommt zum Beispiel für die nach wie vor via TFTP aktualisierbare Firmware von Cisco IP Phones heute ein kryptographischer Signaturmechanismus zum Einsatz, der verhindert, dass Originalsoftware unberechtigt durch modifizierte Versionen ersetzt werden kann.

Gute Besserung

Andere Verletzlichkeiten sind weiterhin anzutreffen. Hier ist beispielsweise die meist (bei physischem Zugriff auf Endgeräte) vorgesehene Möglichkeit des Rücksetzens auf Konfigurationen mit einem allgemein bekannten Passwort zu nennen, die möglicherweise aus einer Abwägung des zusätzlich erwarteten Wartungsaufwands heraus beibehalten wurde.

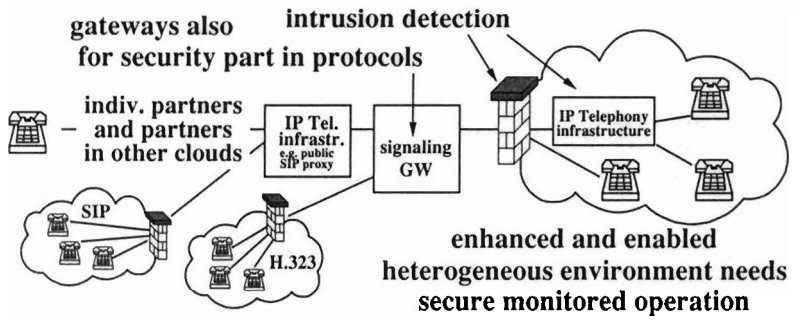


Abbildung 3: Aspekte des fortlaufenden sicheren Betriebs von VoIP-Installationen

Eine Reihe von Herstellern zeigt jedoch mittlerweile – wohl auch in der Folge etlicher publizierter Untersuchungen – ein gut ausgeprägtes Problembewusstsein und hält eigene Analysen und Einsatzempfehlungen bereit. Nicht zuletzt haben sich sicherheitsrelevante Fragen auch in der fortschreitenden Standardisierung der benutzten Signalisierungsprotokolle niedergeschlagen.

Entwicklungstrends

Generell kann man allgemeine Netzwerk-Schutzmechanismen auch für VoIP in Erwägung ziehen. Der häufig im Rahmen von Security-Konzepten oder White Papers (z. B. [3]) empfohlene Einsatz von VLAN- oder VPN-Mechanismen mit einer Trennung von Sprach- und allgemeinem Datenverkehr sowie dem Betrieb dedizierter und entsprechend sicher- und überwachbarer Interaktionspunkte (etwa zur Computer Telephony Integration, CTI) stellt besonders in Unternehmensnetzen eine leistungsfähige und gut praktikable Möglichkeit dar. Hinsichtlich ihres Einsatzes innerhalb eines weltweit nutzbaren VoIP-Systems sind ihnen jedoch gewisse Grenzen gesetzt, die auch den Einsatz alternativer Mechanismen wünschenswert und notwendig machen.

Für den Schutz von Signalisierungsinformationen können neben einer anwendungsspezifischen Verschlüsselung auch Hop-by-Hop-basierte Sicherheitsmechanismen genutzt werden. Entsprechende Verfahren wie der Einsatz von HTTP Digest Authentication, die Verwendung von S/MIME zur Verschlüsselung von Nachrichtenkörpern oder auch der Einsatz von Transport Layer Security (TLS) sind insbesondere im Rahmen der SIP-Standardisierung Teil der Basisstandards geworden und in der Regel in Infrastruktur- und Endsystemen auch implementiert.

Die SIP-Mechanismen zum Schutz von Registrierungsinformationen sind praktisch durchgängig in professionell genutzten Systemen im Einsatz und werden sowohl von kommerziellen als auch Open-Source-Infrastrukturkomponenten unterstützt. Hier sind beispielsweise der SIP Express Router SER (www.iptel.org) oder die IP PBX asterisk (www.asterisk.org) zu nennen. Eine kryptographisch geschützte Authentifizierung sowie bei allen nachfolgenden Signalisierungsschritten genutzte Authentifizierungsinformationen (Nonce und Authentication Response) stellen sicher, dass nur der berechtigte Nutzer sein meist per Prepaid angelegtes Gesprächsguthaben nutzen kann.

Allerdings führt der Einsatz von Verschlüsselungsmechanismen auf Netzwerkebene (etwa IPSec) für Mediendaten zu einer Reihe von Problemen, die vor allem aus dem entstehenden Header-Overhead, der zusätzlichen Verzögerung durch Ver- und Entschlüsselung sowie der Erschwernis oder völligen Unmöglichkeit von Quality-of-Service-Mechanismen (QoS) zur dedizierten und bevorzugten Weiterleitung der verzögerungssensitiven Sprachdaten resultieren (vgl. [4]).

Mechanismen zur direkten Verschlüsselung von Mediendaten sind jedoch mittlerweile mit dem Secure Real-Time Transport Protokoll (SRTP, RFC 3711) in standardisierter Form vorhanden und können sowohl mit unterschiedlichen Verschlüsselungsalgorithmen (bevorzugt dem AES) als auch zum Schlüsselaustausch entweder im Rahmen der Session-Sig-

nalisierung oder dem davon unabhängigen MIKEY-Protokoll (Multimedia Internet Keying, RFC 3830), eingesetzt werden. Allerdings sind diese Mechanismen, möglicherweise auch unter dem Aspekt der hierdurch erschwerten bis beinahe unmöglichen „Legal Interception" sowie des erhöhten Hardware-Aufwands derzeit kaum im Einsatz.

Bei H.323-basierten Produkten, die H.235 umsetzen, kann hier ein höherer Umsetzungsgrad der dort vorgesehenen Sicherheitsmechanismen konstatiert werden. Diese ermöglichen sowohl einen Schutz der Signalisierungs- als auch der Mediendaten und können daher einer Reihe der bereits beschriebenen Angriffe wirkungsvoll standhalten.

Protokollvielfalt

Neben dem von der Internet Engineering Task Force (IETF) entwickelten SIP gewinnt im Rahmen des gestiegenen Einsatzes der IP-basierten Open-Source-„Telefonanlage" asterisk zunehmend auch das Inter Asterisk Exchange Protokoll IAX an Bedeutung. IAX wurde ursprünglich proprietär entwickelt, jedoch später offen gelegt und in der Version V2 auch als Internet-Draft entworfen (www.cornfed.com/iax.pdf). Anders als bei der in H.323 und SIP genutzten unabhängigen Übertragung von Signalisierungs- und Mediendaten werden beim IAX beide Datenströme in *einer* Art von Protokollpaketen verpackt. Dies ermöglicht einerseits eine Aggregation von Daten, die zu unterschiedlichen Gesprächen gehören (Trunking), und vereinfacht zudem durch die Verwendung eines einzigen Ports, der zusätzlich sowohl für den Versand als auch den Empfang genutzt wird (Symmetric Signaling and Media Streaming), eine bessere Übertragung durch Firewalls oder NAT-Systeme (Network Address Translation).

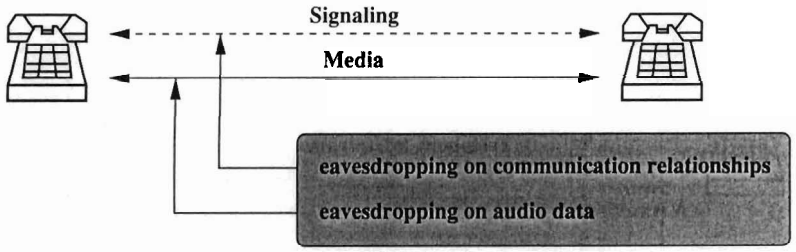


Abbildung 4: Abhören ungeschützter Signalisierungs- oder Mediendaten

Auch die zur reinen Sprachübertragung nur noch in begrenztem Umfang genutzte H.323-Protokoll-Suite erlebt derzeit im Bereich der Video-Telefonie- und -Konferenz-Systeme eine nennenswerte Nutzung, obwohl auch dort – wie übrigens in den aktuellen und zukünftigen Mobilfunknetzen der dritten (3GPP) und nachfolgenden Generationen – bevorzugt SIP zum Einsatz kommt.

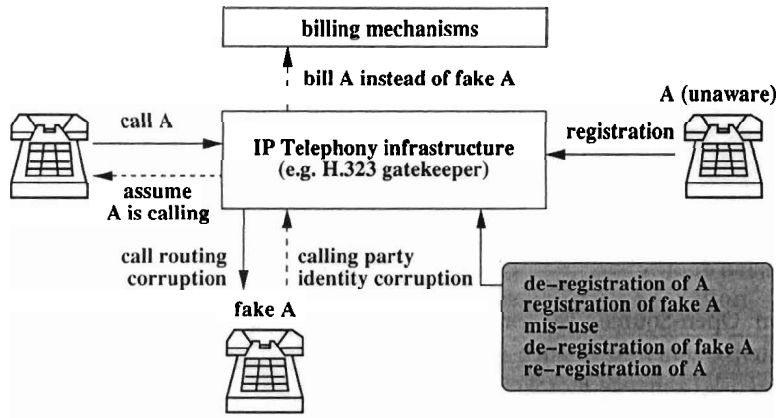


Abbildung 5: Angriffe auf das Call-Routing aufgrund fehlenden kryptographischen Schutzes der Signalisierung oder unzureichender Authentifizierung

Vor allem im Individualbereich, dort allerdings mit einer signifikanten und stetig steigenden Nutzerzahl, kommt häufig Skype zum Einsatz. Dessen Protokoll kombiniert aus dem Peer-2-Peer-Bereich bekannte Mechanismen zur Nutzerlokalisierung mit einer Kombination unterschiedlicher Verfahren zur Traversierung von NAT-Systemen. Einerseits sind die übertragenen Daten effizient kodiert und offenbar – zumindest teilweise – verschlüsselt. Aufgrund der proprietären und bisher nicht offen gelegten Art des Protokolls existieren bisher jedoch nur wenige, durch eine Protokollanalyse gewonnene Erkenntnisse über die genaue Art der verwendeten Verfahren [5].

Einsatzempfehlungen

_____ Wählen Sie eine systematische und ganzheitliche Herangehensweise, die neben einer Analyse der verfügbaren sicherheitsrelevanten Basismechanismen und des möglichen Einsatzes von Voice over IP in Ihrer speziellen Umgebung die Aspekte des fortlaufenden Monitorings und der Reaktion im Problemfall berücksichtigt.

_____ Überprüfen Sie, ob Sie Mechanismen wie den Einsatz von VLANs oder VPNs in Ihren Einsatzumgebungen nutzen können, ohne dabei bestimmte potenzielle Teilnehmer auszuschließen oder den verfügbaren Dienstumfang einzuschränken. Beachten Sie beim Einsatz von Tunnelmechanismen, dass Sie im Falle von Audio- oder Videodaten verzögerungssensitive Echtzeitinformationen übertragen und daher beispielsweise der Einsatz TCP-basierter Tunnel ungeeignet ist.

_____ Aktivieren Sie verfügbare Mechanismen zur Authentifizierung in den von Ihnen betriebenen Endsystemen und Infrastrukturkomponenten. Setzen Sie in der Regel eine restriktive Policy für die Anmeldung von Teilnehmern um.

_____ Setzen Sie entweder Komponenten ein, die offen gelegte, standardisierte Protokolle verwenden, oder informieren Sie sich beim Einsatz herstellerspezifischer Lösungen über dafür entworfene und umgesetzte Sicherheitskonzepte.

_____ Setzen Sie Mechanismen ein, die Auffälligkeiten in der von Ihnen betriebenen VoIP-Infrastruktur erkennen und Ihnen ermöglichen, auf diese zu reagieren. Ziehen Sie dazu insbesondere eine Interaktion mit Firewalls und Intrusion-Detection-Systemen in Betracht.

_____ Informieren Sie sich fortlaufend über aktuelle Weiterentwicklungen im Bereich der VoIP Sicherheit, aber auch neue denkbare Angriffsmuster.

Firewalls und NAT

Die Übertragung von Signalisierungs- und Mediendaten über voneinander unabhängige Verbindungen, deren Parameter zudem teilweise mehrstufig und dynamisch ausgehandelt werden, hat den Einsatz von VoIP-Lösungen in Umgebungen mit Firewalls und Network Address Translation (NAT) in der Vergangenheit durchaus erschwert. Dies führte bis hin zu Empfehlungskatalogen für bestimmte zu verwendende Router oder aufwändige – und teilweise dennoch nur mit Funktionseinschränkungen verwendbaren – Erweiterungen von Firewalls. Diesen Problembereich inklusive praktikabler Lösungen diskutiert umfassend die Doktorarbeit „Firewall-Architekturen für Multimedia-Applikationen" von Utz Roedig [6].

Neben der Standardisierung und einer mittlerweile breiten Verwendung von Protokollmechanismen wie Simple Traversal of UDP over NAT (STUN), Traversal Using Relay NAT (TURN) oder Interactive Connectivity Establishment (ICE) wurden auch bei der Realisierung von VoIP-Anwendungen Fortschritte durch eine firewall-freundliche Implementierung sowie den Einsatz von Symmetric Signaling und Symmetric Media Streaming erreicht. Beide Verfahren versenden ausgehende Daten von demselben Port, über den auch empfangen wird, sodass in durchlaufenen NAT-Elementen oder Firewalls jeweils ein abgehender Datenstrom ein geöffnetes Mapping für einen eingehenden Datenstrom ermöglicht.

Dies ist allerdings von einer entsprechenden Implementierung bei beiden Kommunikationspartnern abhängig und erklärt den Umstand der oft beobachteten korrekten Funktion proprietärer oder homogener Installationen bei gleichzeitigen (teilweisen) Nutzungsbeeinträchtigungen in heterogenen Szenarien. Beispielsweise können nach erfolg-

reichem Sitzungsaufbau dann einer oder beide Sprachkanäle „fehlen".

Fragen zum VoIP-Einsatz

Eine Sicherheitsbewertung im Vorfeld der Beschaffung oder beim Einsatz einer VoIP-Lösung sollte die drei eingangs angesprochenen Schwerpunkte berücksichtigen. Naturgemäß bilden hierfür Security Whitepapers von Herstellern und Lösungsanbietern eine gute Grundlage. Offen gelegte Abläufe ermöglichen zudem einen kritischen Vergleich mit dem Stand der Technik für die eingesetzten Basismechanismen.

Während, wie bereits angesprochen, einige der Kritikpunkte aus der bereits angesprochenen Untersuchung von 2001 [1] mittlerweile behoben wurden, zeigen sich im breiten Einsatz teilweise auch nichtstandardisierter, proprietärer Mechanismen eine Reihe von neuen Angriffspunkten. Nicht zuletzt spielen

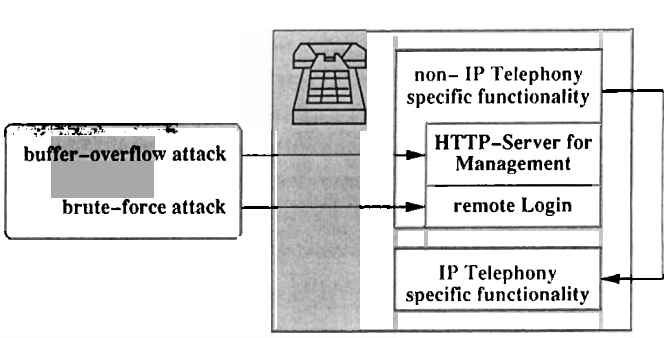


Abbildung 6. Angriffe unter Ausnutzung von Verletzlichkeiten nicht unmittelbar für die VoIP-Funktionen verantwortlicher Komponenten

im Rahmen von „Managed VoIP"-Installationen die Bereitstellung und Absicherung entsprechender Schnittstellen zur Fernkonfiguration und Wartung eine sehr wichtige Rolle: Gerade dort kann und sollte man auf die bisher vor allem für Firewall- und VPN-Systeme etablierten Mechanismen zurückgreifen.

Im Übrigen empfiehlt sich eine genauere Betrachtung der folgenden Fragen:

_____ Wurden wesentliche Informationen über den vorgesehenen Einsatzrahmen und seine Besonderheiten erfasst (z. B. die Existenz von Firewalls oder die beabsichtigte Anbindung von Teilnehmern über NAT) und können sie bei der Auswahl und Bewertung der Lösung berücksichtigt werden?

_____ Existieren von dem vorgesehenen Anbieter oder (ggf. auch Open Source) Produkt Unterlagen, die sicherheitsrelevante Eigenschaften und Implikationen entsprechend der einführend genannten Klassifizierung diskutieren und belastbare Aussagen hierzu machen?

_____ In welchem Umfang sind von speziellen Protokollen (z. B. SRTP) bereitgestellte Funktionen erwünscht oder sogar unverzichtbar und in welchem Rahmen werden sie von der einzusetzenden Lösung zur Verfügung gestellt?

_____ Existieren Erfahrungen oder sogar eine Zertifizierung hinsichtlich der Härtung gegen Angriffe mit typischen Angriffs-Tools?

_____ Können durch Einsatz von nicht VoIP-spezifischen Sicherheitsmechanismen die angestrebten sicherheitsrelevanten Eigenschaften erzielt werden? Gibt es Randbedingungen oder spezielle Nutzungsanforderungen, die dies erschweren oder verhindern? Sind verwendete Mechanismen standardisiert oder zumindest offen gelegt oder können über Systemfunktionen und beteiligte Komponenten nur unzureichende Aussagen getroffen werden?

Für die Zukunft scheint absehbar, dass nicht zuletzt wegen der gegebenen Komplexität der zu bewertenden Faktoren auch passende Zertifizierungen und Bewertungen durch herstellerübergreifende und unabhängige Institutionen eine zunehmend wichtige Rolle spielen werden.

Nicht diskutiert wurden im Rahmen dieses Beitrages die regulatorischen und rechtlichen Aspekte des VoIP-Einsatzes, zu denen bereits unter anderem die Bundesnetzagentur (vormals Regulierungsbehörde für Post und Telekommunikation, RegTP) umfangreiche Anhörungen und Klärungen vorgenommen hat [7]. Für den sich abzeichnenden Bereich der absehbaren Belästigung beispielsweise durch automatisiert ausgeführte Anrufe (Schlagwort: Voice Spam oder Spit) sei auf den bereits angesprochenen <kes>-Beitrag [8] verwiesen. Denkbare Abwehrmechanismen sind hier beispielsweise Black und White Lists oder die Implementierung eines Challenge-Response-Schrittes („Bitte drücken Sie zunächst die DTMF Taste x!"), bevor ein Gespräch zum Angerufenen signalisiert wird. Auch durch die Übertragung von Kontextinformationen in der Phase des Gesprächsaufbaus ergeben sich eine Reihe von Möglichkeiten, aber auch Herausforderungen im Hinblick auf die Sicherung der Privatsphäre von VoIP-Nutzern [9].

Ausblick

Als hoffnungsvoller Schritt ist zudem die Bildung anbieterübergreifender Organisationen wie der VoIP Security Alliance (VOIPSA, www.voipsa.org) zu nennen, die verschiedene Projekte, unter anderem zur Analyse von „Security Requirements", der Bildung eines Bedrohungsschemas (Threat Taxonomy) und später der Festschreibung von Best Practices, angekündigt hat. ■

Literatur

[1] Ralf Ackermann, Markus Schumacher, Utz Roedig und Ralf Steinmetz, Vulnerabilities and Security Limitations of current IP Telephony Systems, in: Proceedings of the Conference on Communications and Multimedia Security (CMS 2001), S. 53, Darmstadt, Mai 2001, www.kom.e-technik.tu-darmstadt.de/publications/abstracts/ASRS01-1.html

[2] Ralf Ackermann, Gateways and Components for Supplementary IP Telephony Services in Heterogeneous Environments, Doktorarbeit, Juli 2003, http://elib.tu-darmstadt.de/diss/000359/

[3] Cisco, Security in SIP-Based Networks, White Paper, Januar 2003, www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper09186a00800ae41c.shtml

[4] D. Richard Kuhn, Thomas J. Walsh, Steffen Fries, Security Considerations for Voice Over IP Systems, in: Recommendations of the National Institute of Standards and Technology, Januar 2005, http://csrc.nist.gov/publications/nistpubs/#sp800-58

[5] Salman A. Baset, Henning Schulzrinne, An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol, TR cucs-039-04, IRT, Columbia University, New York, September 2004, www.cs.columbia.edu/~library/2004.html

[6] Utz Roedig, Firewall-Architekturen für Multimedia-Applikationen, Doktorarbeit, TU Darmstadt KOM, 2002, http://elib.tu-darmstadt.de/diss/000276/

[7] Bundesnetzagentur, Anhörung zu VoIP, Stellungnahmen, Auswertung und Eckpunkte, www.bundesnetzagentur.de/enid/am.html

[8] Andrew Graydon, Protokollfragen, VoIP-Security bei SIP & Co., <kes> 2005#2, S. 55

[9] Manuel Görtz, Effiziente Echtzeitkommunikationsdienste durch Einbeziehung von Kontexten, Doktorarbeit, TU Darmstadt, Fachbereich Elektrotechnik und Informationstechnik, 2005, http://elib.tu-darmstadt.de/diss/000592/

Dr. Ralf Ackermann ist Leiter der Forschungsgruppe Ubiquitous Communication Services am Lehrstuhl Multimedia Kommunikation (KOM) der TU Darmstadt sowie im Bereich der Open-Source-Entwicklung und -Beratung tätig. Dr. Manuel Görtz ist aktives Mitglied dieser Forschungsgruppe.