INFONEWS

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

www.goSecurity.ch
Mit Sicherheit an der richtigen Adresse.

VoIP – Voice over IP

VoIP ist zu einem Dauerthema geworden. Grund genug, sich mit der Sicherheit auseinanderzusetzen. Auf den nachfolgenden Seiten erfahren Sie alles über die Technik von VoIP (H.323, SIP) und alles was bei einem Missbrauch geschehen kann. Dabei werden die unterschiedlichsten Risiken und Sicherheitsaspekte wie Soziale Angriffe, Lauschangriffe, Gesprächskontrolle und Störungen beleuchtet.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

1 Einleitung

Voice-over-IP ist in aller Munde. Praktisch in jedem Magazin oder Zeitschrift ist heute ein Artikel über die neue Art zu telefonieren enthalten.

Der Durchbruch von VoIP brachte Skype. Mehr als 100 Millionen Mal wurde diese Software bereits heruntergeladen. Britische Marktforscher gehen davon aus, dass ca. 5.3 Millionen Benutzer Skype auch regelmässig zum Telefonieren nutzen. Die Tendenz ist stark steigend. Dieser Erfolg ist auch der Grund dafür, dass Ebay erst kürzlich 2.6 Milliarden Dollar für Skype bezahlt hat und dies nun konsequent in Ihren Marktplatz integriert.

Doch Skype ist nicht die einzige Art, sich kostenlos mit anderen Menschen online zu verständigen. Diese Software-Alternativen wählen aber oft nicht ein proprietäres, das heisst ein selber entwickeltes Verfahren ein, sondern setzen auf anerkannte Standards.

In vielen Ländern gehört Voice-over-IP schon länger zum „Daily Business“. So finden in den USA 30 Prozent aller Telefonate über das Datenkabel statt, in Japan sind es 16 Millionen Meschen, die dieses Medium jeden Tag nutzen, was in etwa 50% der Breitbandnutzer entspricht.

In der Schweiz buhlen sich seit einigen Jahren zahlreiche Firmen um die Gunst der Kundschaft. Die grossen Telefongesellschaften sind dabei erst kürzlich auf diesen Zug aufgesprungen. Die Zahlen in der Schweiz sehen auch dementsprechend mager aus. Analysten gehen von einer Anwenderzahl im einstelligen Prozentbereich aus. Aber auch hier ist ein Wandel festzustellen.

Dieser Trend scheint momentan ungebrochen und so werden bis im Jahr 2010 weltweit 200 Millionen Nutzer von Voice-over-IP Techniken erwartet. 78% der Grossunternehmen werden bis dahin sogar komplett auf die neue Art zu telefonieren umgestellt haben.

Aus diesem Grund ist es wichtig, sich auch mit den Sicherheitsfunktionen auseinanderzusetzen. Bevor wir auf diese eingehen, einige Worte zur Technologie von VoIP.

Dieses Kapitel geht etwas vertiefter auf das Thema der Applikationen und Techniken ein. Bevor man Voice-over-IP einführt, sollte man sich auch über die verschiedenen Arten und technischen Möglichkeiten auseinander setzen. Ohne ein gewisses technisches Verständnis ist ein möglicher Schiffbruch nicht auszuschliessen.

Neben einigen proprietären Produkten (z.B. Skype) haben sich zwei Standards durchgesetzt: H.323 und SIP. Diese beiden Standards sind nicht kompatibel zueinander und stehen daher in direkter Konkurrenz. Ein guter Grund, sich diese einmal etwas detaillierter anzuschauen.

1.1 H.323

H.323 ist ein Dachstandard für ein ganzes Set von Einzelstandards für paketbasierte Multimedia-übermittlungen. Es wurde 1996 von der ITU-T definiert. Eine Stärke von H.323 ist die Verfügbarkeit, in der nicht nur das Rufmodell sondern auch zusätzliche

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Leistungsmerkmale im Bereich der Audio- und Videoübermittlung beinhaltet sind. Da der Standard auf ISDN aufbaut, ist es gut zwischen ISDN und IP Anlagen einzusetzen und kann somit einfach in bestehende ISDN Netze integriert werden. Jedoch muss dazu ein so genannter Gate-Keeper eingesetzt werden, da H.323 nicht mit IP zusammenarbeitet. Ein grosser Nachteil ist die damit verbundene Komplexität.

1.2 SIP

Im Gegensatz zu H.323 wurde 1997 SIP mit Blick auf das Internet von der IETF entwickelt und orientiert sich an der Architektur von Internetanwendungen. Der Fokus wurde auf leichte Implementierung, Skalierbarkeit, Erweiterbarkeit und vor allem auf Flexibilität gesetzt. SIP vereinbart jedoch nur die Kommunikationsmodalitäten. Um über das Internet telefonieren zu können, benötigt es weitere geeignete Protokolle. Dazu werden unter anderem SDP (Session Description Protocol, RFC 2327) und RTP (Real Time Protocol, RFC 3550) eingesetzt. Der Aufbau von SIP-Nachrichten basiert auf dem http-Protokoll und verwendet einfache Textnachrichten. Als Nachteil von SIP ist die Übertragung der RTP Daten via UDP (verbindungslose Datenübermittlung). Die dafür verwendeten UDP-Ports werden dynamisch vergeben, was vor allem im Zusammenhang mit Firewalls oder NAT (Network Address Translation) ein grosses Problem darstellt. Die auftreffenden Daten können keiner Signalisierungsverbindung zugeordnet werden. IETF sieht aber mit einem neuen Protokoll ICE (Interactive Connectivity Establishment) eine Lösung vor.

1.3 H.323 und SIP im Vergleich

Eigenschaft	H.323	SIP
Standardisierungsgremium	ITU-T	IETF - RFC
Generelle Eigenschaften	Vollständiger Standard für Audio-, Video und Datenkonferenzen mit mehreren Unterstandards.	Protokoll für die Signalisierung von Multimedia-Sitzungen ohne Festlegung auf bestimmte Anwendungsbereiche
Komplexität	Hoch	Niedrig, da nur Signalisierung
Nachrichtencodierung	Binär	Textbasiert, HTML-ähnlich
Zusammenarbeit mit IP	Keine	Problemlos
Skalierbarkeit	Eingeschränkt	Ja
Anrufsteuerung	Gatekeeper	Endgerät
Authentifizierung, Verschlüsselung	Definiert in H.235	Keine Definition, verwendet wird oft IPSec, TLS, SRTP oder S/MIME
Mediatransportprotokoll	RTP/RTCP (UDP)	RTP/RTCP (UDP)
Signalisierungstransport	UDP oder TCP	UDP oder TCP

Danke der einfachen Anwendung von SIP scheint es so, als würde sich dieser Standard durchsetzen. Diverse Hersteller haben bereits auf SIP gesetzt und diesen in Ihre Geräte integriert.

1.4 SIP-Verbindungsaufbau

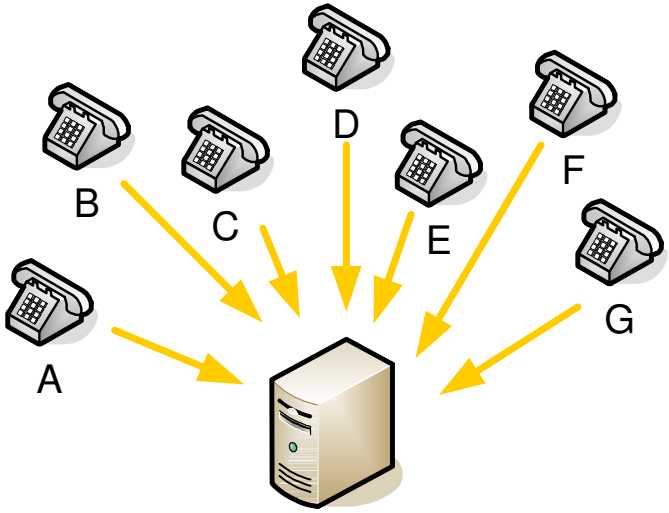
Ein SIP-basierter Telefonie-Server arbeitet vorwiegend im Proxy-Modus. Somit integriert er sowohl Client- wie auch Serverfunktionen und dient beiden Seiten als Stellvertreter für die Gegenstelle. Ein Verbindungsaufbau läuft folgendermassen ab:

goSecurity.ch/infonews

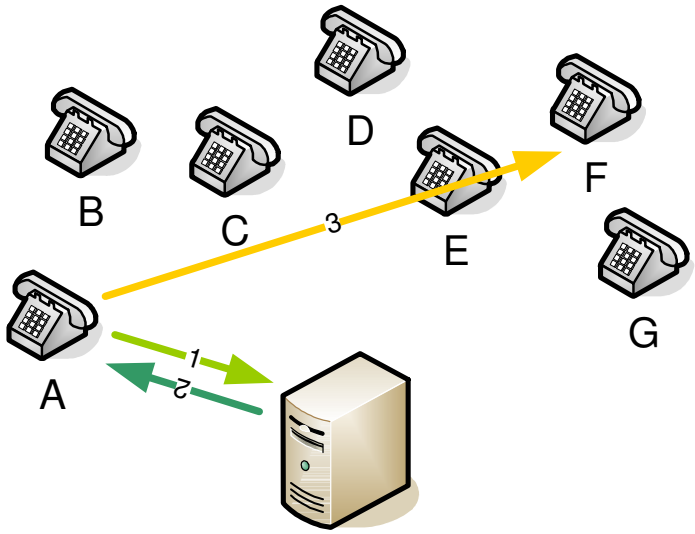
GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Bevor ein Verbindungsaufbau stattfinden kann, muss zuerst die Gegenstelle bekannt sein. Die meisten Internetnutzer haben dabei keine festzugeteilte IP-Adresse, sondern diese wird dynamisch vom Provider zugewiesen. Damit der Gesprächspartner trotzdem gefunden wird, melden sich alle Geräte an einem zentralen Server an. Will nun die Station A mit F telefonieren, wird zuerst der Server nach dessen Adresse gefragt:



Alle VoIP Telefone melden sich beim Server an.



1. *Server wird nach einer Adresse gefragt.*
2. *Server sendet Adresse zurück.*
3. *A stellt eine Verbindung zu F her.*

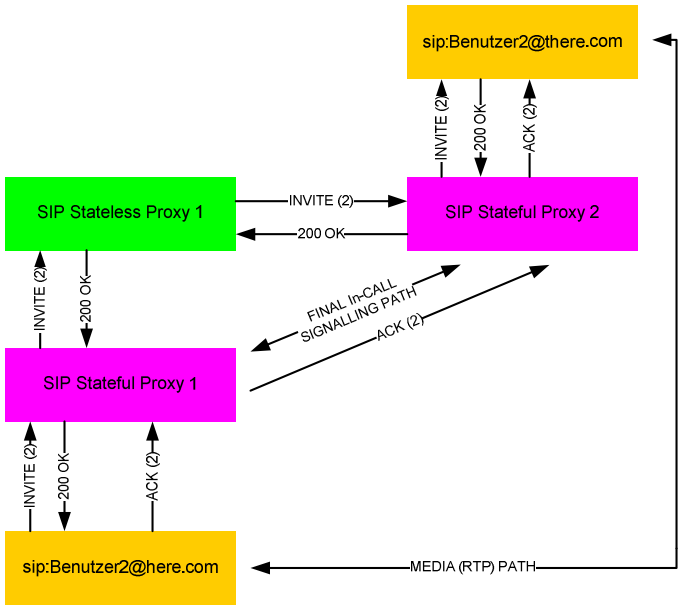
Sobald die Zieladresse bekannt ist, kann der Benutzer (benutzer1@here.com) mit dem Verbindungsaufbau starten. Er schickt dazu eine INVITE Anfrage via seinen Proxydienst an den Empfänger. Die dazwischenliegenden Netzwerkelemente nehmen dabei keine Veränderungen vor, sondern leiten das Paket bis zum Ziel weiter (INVITE (2)).

Nachdem die Anfrage beim Empfänger (benutzer2@here.com) ankommt, wird dies durch ein Signal, zum Beispiel ein Klingeln, signalisiert.

Wenn der Angerufene den Anruf entgegennimmt, wird via seinen Proxy die Bestätigung (200 OK) an den User1 zurückgeschickt.

Dieser muss die Annahme noch zusätzlich bestätigen (Acknowledge, ACK(2)). Diesmal jedoch auf direktem Weg.

Nachdem der Anruf auf beide Seiten bestätigt wurde, wird der Datenaustausch direkt via RTP aufgebaut (grosser Pfeil).



2 Security

Eine wichtige Organisation zur Identifikation von Gefahrenquellen ist die Voipsa (Voice-over-IP Security Alliance, http://www.voipsa.org/) zu welcher über 100 Provider, Hard- und Softwarehersteller angehören. In der aktuellen Studie „Threat Taxonomy“ wurden mehr als 60 Gefahrenpotentiale für VoIP-Netze, -Endgeräte und –Anwender umfassend beschrieben.

2.1 Soziale Angriffe

Diese Art von Angriffen zielt auf die Persönlichkeit einer Person. Es wird versucht, möglichst viele Informationen über die Person zu erfahren um anschliessend diese Identität zu übernehmen. Viele Provider von Voice-over-IP-Diensten erleichtern dies, indem die eigene Rufnummer, die so genannte Caller ID, relativ einfach gefälscht werden kann. Damit ist es möglich, eine x-beliebige Nummer zu übernehmen, die beim Angerufenen auf dem Display erscheint und so Vertrauen erweckt. Erschwerend kommt hinzu, dass viele Anbieter eine unterdrückte Rufnummer trotzdem mitschicken. Angezeigt wird diese im Display zwar nicht, aber mittels einer Protokollanalyse sind alle Angaben sichtbar. Bei Anrufen auf Notfallnummern macht dies zwar Sinn, jedoch sollte die unterdrückte Nummer nicht bei allen Anrufen mitgeschickt werden.

Diese Technik hat auch einen eigenen Namen erhalten Vishing (analog dem Phising per Email) Mit den gestohlenen Identitäten wird bereits heute im Internet gehandelt.

Ein weiterer Faktor sind Spam-Meldungen. Wie bei Email bereits unrühmlich bekannt, nimmt auch Spam über

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

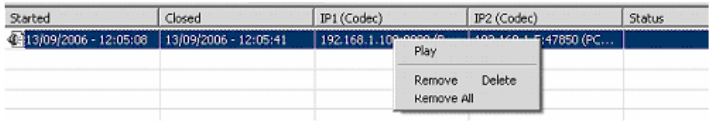
Voice-over-IP Medien schnell zu (SPIT). Für den Versender solcher Werbemitteilungen sind keine oder nur marginale Kosten verbunden, der Empfänger hingegen muss sich eine gesprochene Mitteilung anhören. Daher gilt, wie bei Emailadressen, nur vertrauenswürdigen Personen und Institutionen die eigene Rufnummer bekannt geben.

Viele Hersteller sind daran, Lösungen gegen SPIT zu erarbeiten. In den kommenden Monaten ist hier sicherlich mehr zu erfahren.

2.2 Lauschangriffe

Lauschangriffe sind eine klassische Methode, die aus vielen Filmen bekannt ist. Auch bei digitalen Nachrichten wird versucht, den gesprochenen Text mitzuhören. Dazu müssen jedoch die Datenpakete abgefangen und zusammengesetzt werden. Im Internet sind bereits zahlreiche Tools verfügbar, die diese Arbeit automatisch übernehmen. Jedoch kann nicht einfach ein Kabel „angezapft" werden, sondern die Pakete müssen über den eigenen Rechner umgeleitet werden. «Man in the middle Attacken» nennt man diese Möglichkeit. Damit dies erst möglich wird, muss der Benutzer dazu gebracht werden, eine Software einzuspielen. Hier kommt wieder der soziale Faktor als wichtigstes Argument. Gelingt es dem Benutzer eine Software unterzujubeln (dies können zum Beispiel Viren, Trojanische Pferde oder eine Email mit „Beilage" sein), werden alle Pakete zuerst an den Angreifer geschickt und erst dann weiter an den eigentlichen Empfänger.

Der folgende Screenshot zeigt eine mit Cain&Abel aufgezeichnete VoIP Verbindung. Ein Klick auf Play genügt und das aufgezeichnete Gespräch wird abgespielt.



Hier hilft nur eine rigorose Verschlüsselung des Datenstromes. VPN oder SRTP verschlüsseln den Datenstrom so, dass er nicht mehr abgehört werden kann.

2.3 Gesprächskontrolle

Gelingt es, eine Verbindung so zu übernehmen, sind nebst dem Abhören auch Manipulationen am Gespräch möglich, so zum Beispiel das Verändern von Inhalten, Rufumleitungen oder dem Beenden des Gespräches.

2.4 Störungen

Anders als bei der bekannten Telefonie, können Voice-over-IP Geräte mit relativ kleinem Aufwand gestört werden. Zu den bekanntesten Angriffen zählt DoS (Denial of Service). Ziel ist es, die Infrastruktur so zu „beschäftigen", dass ein normaler Betrieb nicht mehr möglich ist. Wahlwiese werden so viele Datenpakete an den Empfänger geschickt, dass die Leitung überlastet, oder es wird eine Schwachstelle im Endgerät ausgenutzt, welche das Gerät zum Absturz bringt. In der Folge können weder Telefonate empfangen noch gemacht werden. Wie bei DoS-Angriffen auf eine Webseite, ist ein Schutz der Voice-over-IP-Infrastruktur nur sehr schwer möglich.

Einige Provider im VoIP Bereich bieten eine Dienstleistung an, welche DoS Attacken erkennen und verhindern können. So wird die eigene Infrastruktur geschützt und Gespräche können weiterhin geführt werden. Klären Sie daher ab, ob Ihr jetziger oder zukünftiger Partner dies anbietet.

2.5 Weitere Schutzmöglichkeiten

Dass die oben beschriebenen Gefahren real sind, zeigen die verschiedenen Tools und Anleitungen, die im Internet abrufbar sind. Schutzmöglichkeiten umzusetzen ist jedoch nicht einfach. Nicht alle Hersteller implementieren die Standard-Voice-over-IP-Protokolle in der gleichen Art und Weise.

Folgende Varianten können eine Lösung für die bereits erwähnten Gefahren sein:

- SIP Implementierung des Herstellers
- das Secure Real-Time Transport Protocol SRTP
- VPN-Verschlüsselung
- Zfone von Phil Zimmermann

2.5.1 SIP-Implementierung des Herstellers

Es gibt die Möglichkeit Anwender und Proxies per Digest Authentication zu autorisieren. Auch Signatur- und Verschlüsselungsmöglichkeiten für die Nachrichten sowie ein Tunneling-Modus für die SIP-Header sind im Standard vorgesehen. Hierfür wir jedoch eine Public Key Infrastructure (PKI) oder eine ähnliche Verschlüsselungstechnik vorausgesetzt. (siehe auch INFONEWS 3/04, elektronische Signatur)

2.5.2 SRTP

Bei dem Secure Real-Time Transport Protocol (SRTP) handelt es sich um die verschlüsselte Variante des Real-Time Transport Protocol (RTP). Es ist im RFC 3711 festgehalten. SRTP verschlüsselt nur den Nutzinhalt eines Datenpakets mit AES (Advanced-Encryption-Standard, Nachfolger von DES). Die Header-Informationen des Pakets, die Absender und Adressat enthält, bleiben von der Verschlüsselung unberührt.

2.5.3 VPN

Mit einem Virtual Private Network werden die Verbindungspartner durch einen sicheren Tunnel miteinander verbunden. Jeglicher Inhalt wird dabei verschlüsselt, im Gegensatz zu SRTP auch die Header-Informationen. Die Ver- und Entschlüsselung kann jedoch nicht im Endgerät bewerkstelligt werden, sondern es müssen zusätzliche Geräte angeschafft werden. Oft kann dies aber durch eine vorhandene Firewall gelöst werden.

2.5.4 Zfone

Um nicht auf Resultate der Hersteller zu warten, hat Phil Zimmermann, der Entwickler von PGP, eine Lösung zur Verschlüsselung von Voice-over-IP Datenpakete entwickelt: Zfone. Diese Software funktioniert mit den meisten auf dem Markt verfügbaren Geräten und ist sehr einfach in der Anwendung. Somit kann der eigene Telefonverkehr nicht mehr abgehört werden. Das Tool kann kostenlos unter http://zfoneproject.com/ heruntergeladen werden.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Zfone ist unabhängig von Zertifizierungsstellen. Die Verschlüsselung wird von den Clients im Peer-to-Peer-Verfahren durchgeführt. Zfone ist jedoch keine eigenständige Telefonie-Software, sondern lediglich ein Zusatz. Es fängt die VoIP-Pakete ab, verschlüsselt bzw. entschlüsselt diese und leitet sie weiter. Das Programm soll neue Anrufe selbstständig erkennen und zeigt dem Nutzer in einem kleinen Fenster an, ob das aktive Telefonat gesichert abläuft.

3 Zusammenfassung

Wie jedes Netzwerkprotokoll hat auch VoIP seine Schwachstellen. Mit geeigneten Massnahmen kann jedoch die Verbindung vor Manipulation und Abhören sicher geschützt werden. Für die Planung und Umsetzung muss genügend Zeit eingeplant werden. Es lohnt sich, die zur Verfügung stehenden Funktionen ausgiebig zu testen. Sollten diese für die eigenen Ansprüche nicht genügen, müssen Alternativen wie SRTP, VPN oder Zfone zum Zug kommen.

Hinweis:

Weitere Informationen zu VoIP, deren Umsetzung und Einführung im Unternehmen sowie Vor- und Nachteilen können im BPX Booklet „VoIP; Praxisleitfaden für Unternehmen – Erfolg durch vernetzte Kommunikation“ von unserem Andreas Wisler sowie Gerd Frera, nachgelesen werden. Es ist für 30 Franken bestellbar unter http://www.bpx.ch/booklet/voice_over_ip_voip.htm.