GO OUT IT-SECURITY HOSTING

klubschule MIGROS

instnova

interway net intelligence

SKYBOW

IT - Security Forum #4

# VoIP Security

Matthias Oswald

**Interway Communication GmbH**
matthias.oswald@interway.ch

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

instnova

interway net intelligence

SKYBOW

IT - Security Forum #4

## Agenda

- VoIP Technologie Primer
- Service Qualität
- Telefonie Szenario
- Identifikation der Sicherheitsprobleme
- Möglichkeiten der Absicherung
- Fazit

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

instnova

interway net intelligence

SKYBOW

IT - Security Forum #4

## Vorstellung des Referenten

- Matthias Oswald
  - Partner Interway Communication GmbH
  - Gegründet 1995
  - 11 Mitarbeiter(Innen)
  - davon 2 Lehrlinge Informatik Systemtechnik
  - Schwerpunkte: Internet Service Provider
    - Webhosting, ADSL
    - Server Housing / Colocation
    - Messaging Services & IT Security

3

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

instnova

interway net intelligence

SKYBOW

IT - Security Forum #4

## Agenda

- VoIP Technologie Primer
- Service Qualität
- Telefonie Szenario
- Identifikation der Sicherheitsprobleme
- Möglichkeiten der Absicherung
- Fazit

4

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

inetnova

interway net intelligence

SKYBOW

IT - Security Forum #4

# Ein VoIP Anruf


**1. Teilnehmer 1 wählt Identifikation (z.B. Nummer) von Teilnehmer 2**

Austausch von Signalisierungsinformationen

**2. Sprachübermittlung**

- Sprache wird im Codec digitalisiert und in RTP-UDP Paketen verschickt

**3. Ein Teilnehmer beendet das Gespräch**

Austausch von Signalisierungsinformationen

5

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

inetnova

interway net intelligence

SKYBOW

IT - Security Forum #4

# VoIP Protokolle

- Zwei konkurrierende Standards
  - H.323 von ITU (1996)
  - SIP (Session Initiation Protocol) vom IETF (1997)
- H.323 Dachstandard für ein ganzes Set von Einzelstandards für paketbasierte Multimediaübermittlung über Netze ohne QoS
- SIP spezifiziert lediglich ein Signalisierungsprotokoll auf Applikationsebene (RFC 3261)

6

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

instnova

interway net intelligence

SKYBOW

IT - Security Forum #4

# VoIP Protokolle – ein Vergleich

| Eigenschaft | H.323 | SIP |
|---|---|---|
| Standardisierungs-organisation | ITU-T | IETF - RFC |
| Generelle Eigenschaften | Vollständiger Standard für Audio- Video und Datenkonferenzen. Dachstandard mit mehreren Unterstandards. | Protokoll für die Signalisierung von Multimedia-Sitzungen ohne Festlegung auf bestimmte Anwendungsbereiche. |
| Komplexität | Hoch | Niedrig, nur Signalisierung |
| Nachrichtenkodierung | Binär | Textbasiert. -> HTML ähnlich |
| Authentifizierung Verschlüsselung | Definiert in H.235 | Nichts festgelegt. IPSec, TLS, SRTP, S/MIME |
| Mediatransportprotokoll | RTP/RTCP (UDP) | RTP/RTCP (UDP) |
| Signalisierungstransport | UDP oder TCP | UDP oder TCP |

7

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

instnova

interway net intelligence

SKYBOW

IT - Security Forum #4

# VoIP Protokolle – The Winner is:

# SIP!

- **Die Welt will's einfach**
- **Die Welt will SIP!**

8

# SIP Protokoll – SIP Nachrichten

SIP Systemkomponenten kommunizieren durch das versenden von Nachrichten und antworten.

| SIP Nachricht | Erklärungen |
|---|---|
| **REGISTER** | Mit dieser Nachricht registriert sich ein SIP User bei einem Registrar |
| **INVITE** | Einladung zu einer Sitzung, z.B. Anfrage für ein Telefongespräch |
| **ACK** | Bestätigung einer Nachricht |
| **CANCEL** | Aufhebung des vorher gesendeten Befehls. Wird z.B. an verschiedene Endsysteme ein INVITE geschickt und einer nimmt den Anruf entgegen schickt man den anderen ein CANCEL. |
| **BYE** | Eine bestehende Sitzung wird beendet |
| **OPTIONS** | Mit dieser Nachricht können die implementierten Methoden eines UAS abgefragt werden. |



# SIP Protokoll – SIP Antworten

| Antwort Code | Bedeutung | Erklärungen / Beispiele |
|---|---|---|
| **1xx** | **Provisional** | Die Nachricht wurde Empfangen und wird verarbeitet:<br>Bsp: 180 – Ringing |
| **2xx** | **Success** | Die Nachricht wurde empfangen, verstanden und akzeptiert.<br>Bsp: 200 - OK |
| **3xx** | **Redirection** | Gibt Informationen über eine neuen Ort wo sich der gesuchte User befindet oder über neue Services die den gewünschten Anruf erfolgreich verarbeiten könnten.<br>Bsp: 301 – Moved Permanentely |
| **4xx** | **Client Error** | Der Server teilt dem Client mit dass er die Anfrage so nicht verarbeiten kann. Der Client sollte damit nicht noch einmal dieselbe Anfrage an denselben Server schicken.<br>Bsp: 401 – Unauthorized |
| **5xx** | **Server Error** | Diese Staus Codes werden zurückgeschickt wenn der Server interne Fehler feststellt.<br>Bsp: 500 – Server Internal Error |
| **6xx** | **Global Error** | Diese Antwort zeigt an dass der Server definitive Informationen über einen bestimmten User erhalten hat. Z.B. dass ein Befehl von keinem Server ausgeführt werden kann.<br>Bsp: 600 – Busy Everywhere |

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

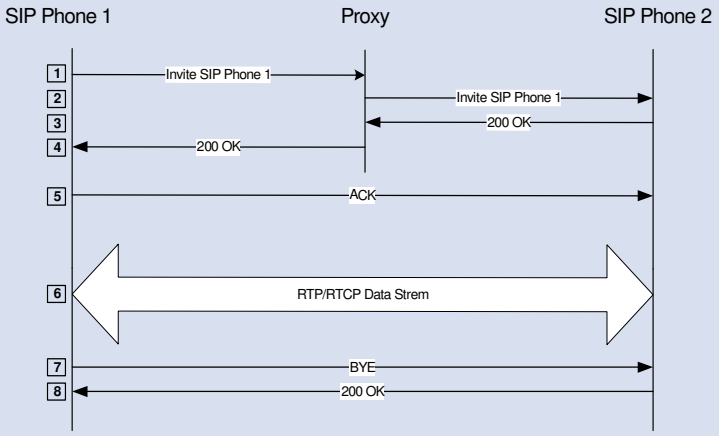
instnova

interway net intelligence

SKYBOW

IT - Security Forum #4

# SIP Protokoll – SIP Call mit Proxy




11

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

instnova

interway net intelligence

SKYBOW

IT - Security Forum #4

# Agenda

- VoIP Technologie Primer
- Service Qualität
- Telefonie Szenario
- Identifikation der Sicherheitsprobleme
- Möglichkeiten der Absicherung
- Fazit

12

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

instnova

interway net intelligence

SKYBOW

IT - Security Forum #4

## Service Qualität

- Hohe Verfügbarkeit
- Schneller Verbindungsaufbau
- Keine Verbindungsunterbrüche
- Gute Sprachqualität

13

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

instnova

interway net intelligence

SKYBOW

IT - Security Forum #4

## Sprachqualität – End to End Verzögerung

- End to End Verzögerungen setzen sich zusammen aus:
  - Kodierung und Kompression
  - Paketierung
  - Serialisierung
  - Netzwerkkomponenten
  - Signallaufzeiten
  - Pufferzeiten
- ITU Vorgabe: - 150ms gut, - 400ms zufriedenstellend

14

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

inetnova

interway net intelligence

SKYBOW

IT - Security Forum #4

## Sprachqualität – weitere Einflussfaktoren

- **Jitter** – Varianz der Verzögerung
  - Bekämpfung durch Prio. des Sprachverkehrs
- **Echo** – störendes „Sich-selbst-hören“
  - entstehen bei D/A Wandlung
  - Fehlanpassungen in analogen Komponenten
  - Bekämpfung mit Echokompensationsverfahren
- **Verzerrungen**
  - durch Paketverlust oder Komprimierung
  - Bekämpfung durch Prio. des Sprachverkehrs

15

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

inetnova

interway net intelligence

SKYBOW

IT - Security Forum #4

## Service Qualitäte – Netzwerk QoS

- VoIP Vorteil: Datennetz kann für Daten und Voice genutzt werden.
- VoIP Nachteil: Datennetz wird für Daten und Voice genutzt
- Computerdaten sind nicht anfällig auf Verzögerungen und Varianz in der Verzögerung
- Sprachdaten schon!
- Sprachkanal braucht 16 – 80 kbps. In Konkurrenz zu Daten
- Europa: gute Resultate mit QoS auf Kundenrouter
- Weltweit: QoS auf ganzem Netz nötig

16

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

inetnova

interway net intelligence

SKYBOW

IT - Security Forum #4

# Agenda

- VoIP Technologie Primer
- Service Qualität
- Telefonie Szenario
- Identifikation der Sicherheitsprobleme
- Möglichkeiten der Absicherung
- Fazit

17

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

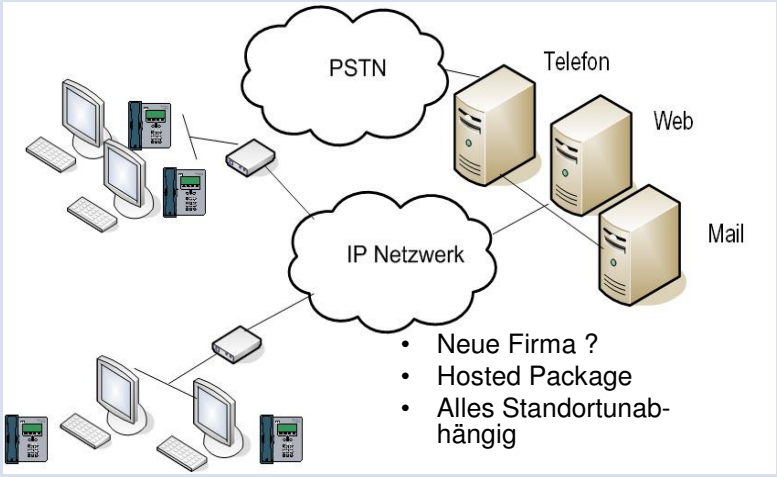
inetnova

interway net intelligence

SKYBOW

IT - Security Forum #4

# Telefonie Szenario




18

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

inetnova

interway net intelligence

SKYBOW

IT - Security Forum #4

## Agenda

- VoIP Technologie Primer
- Service Qualität
- Telefonie Szenario
- Identifikation der Sicherheitsprobleme
- Möglichkeiten der Absicherung
- Fazit

19

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

inetnova

interway net intelligence

SKYBOW

IT - Security Forum #4

## VoIP - Sicherheitsprobleme

- Sicherheit heisst auch bei VoIP

- Verfügbarkeit
- Integrität
- Vertraulichkeit

20

# VoIP - Sicherheitsprobleme

Gruppierung der möglichen Angriffe anhand folgender Fragestellungen:

1.Welcher Grundpfeiler der Sicherheit wird angegriffen
- Verfügbarkeit
- Integrität
- Vertraulichkeit

2.Welche VoIP Komponente wird angegriffen
- Client
- Netzwerk
- Telefonieserver





# VoIP - Angriffsübersicht

| Nr. | Beschreibung | Verletzung der | | | Angriff auf | | |
|---|---|---|---|---|---|---|---|
| | | Vertr. | Verf. | Int. | Clt. | Net. | Pxy. |
| 1 | SIP Call Setup Forking | x | | | x | x | x |
| 2 | SIP Flooding (DoS) | | x | | x | | x |
| 3 | SIP Call Hijacking / Impersonating | x | | | x | | x |
| **4** | **SIP Call termination** | | **x** | | **x** | | **x** |
| 5 | SIP Identity Spoofing – Telefonieren auf fremde Rechnung | | | x | x | | x |
| 6 | RTP Paket Injection – Datastream verändern | | x | x | x | x | x |
| 7 | RTP Stream aufzeichnen/mithören | x | | | x | x | x |
| 8 | RTCP Paket Injection – Codec wechsel | | x | | x | | x |
| 9 | Multicast Forking | x | | | | x | |
| 10 | Verfälschte IP/TCP/SIP/SDP Pakete. Instabilität der Systeme | | x | | x | | x |
| **11** | **Voice Spam – autom.Telefonanrufe** | | | | **x** | | |
| 12 | Asterisk OS Angriff | x [1)] | x [1)] | x [1)] | | | x |
| 13 | Asterisk SW schwäche | x [1)] | x [1)] | x [1)] | | | x |
| 14 | Asterisk Angriff auf Konfigurationsinterface WebGUI / Telnet / SSH | x [1)] | x [1)] | x [1)] | | | x |
| 15 | CDR verändern | | | x | | | x |

1) Verletzung ist abhängig von der ausgenützten Schwachstelle und kann daher u.U. In allen Bereichen eine Verletzung bedeuten.

# VoIP Angriff – SIP Call Termination

- **Technischer Hintergrund:**
  SIP spezifiziert zwei Nachrichten um einen Call zu beenden
  1. BYE ( reguläre Beendigung eines Calls)
  2. CANCEL (Beendigung Signalisierung)
- **Angriff:**
  Kennt man die Call-ID kann jedermann eine BYE Nachricht schicken.Der Angreifer könnte zudem sofort nach der Signalisierung eine CANCEL Nachricht an den eigentlichen Empfänger schicken und den Call selber entgegennehmen.
- **Verletzung:**
  Verfügbarkeit und Vertraulichkeit

IT - Security Forum #4

23

# VoIP Angriff – SIP Call Termination

- **Voraussetzung**
  - Angreifer benötigt Zugang zum Signalisierungspfad
  - Wird Call-ID genügend zufällig gewählt hat der Angreifer ohne abhören kaum eine Chance ein Gespräch zu beenden.
- **Angegriffene Komponenten**
  - Angriff erfolgt auf Endgeräte oder auf VoIP PBX
- **Massnahmen zur Verhinderung**
  Der Zugang zum Signalisierungspfad muss verhindert werden!
  - Chiffrierung des Nachrichtenaustausches
  - Richtige Konfiguration der Netzwerkgeräte
  - Richtige Konfiguration der SIP-Server

IT - Security Forum #4

24

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

instnova

interway net intelligence

SKYBOW

IT - Security Forum #4

# VoIP Angriff – Voice Spam

- **Technischer Hintergrund**
  Spam ist sattsam aus dem Mailumfeld bekannt. Es ist denkbar, dass in einem VoIP Netzwerk unerwünschte Sprachnachrichten an eine grosse Anzahl von Benutzer geschickt wird.
- **Angriff**
  Der Angreifer sammelt SIP Account Infos und sendet Nachricht. Gegenüber heutiger Telefonie tendiert VoIP-VoIP zu gratis was Spam erst attraktiv macht.
- **Verletzung**
  Missbrauch der Ressourcen.

25

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

instnova

interway net intelligence

SKYBOW

IT - Security Forum #4

# VoIP Angriff – Voice Spam

- **Voraussetzung**
  Angreifer kennt UserID des Empfängers
- **Angegriffene Komponente**
  Endgeräte und VoiceMailboxen
- **Massnahmen zur Verhinderung**
  Schwierig zu verhindern.
  - Anrufe nicht kostenlos machen
  Ansonsten Methoden analog Spam Bekämpfung
  - Nur Anrufe von verifizierten Anrufern entgegennehmen
  - Blacklists von VoiceSpam Servern
  - Sprachanalyse des Inhalts

26

IT - Security Forum #4

# Agenda

- VoIP Technologie Primer
- Service Qualität
- Telefonie Szenario
- Identifikation der Sicherheitsprobleme
- Möglichkeiten der Absicherung
- Fazit



IT - Security Forum #4

# VoIP – Absicherungsmassnahmen

Eine VoIP Absicherungsstrategie muss mehrschichtig angelegt werden:

- Absicherung des Netzwerkes
- Absicherung des Systems (VoIP PBX)
- Absicherung der Applikation (VoIP PBX)
- Absicherung durch organisatorische Massnahmen
- Absicherung durch rechtliche Massnahmen

# Gefahreneinschätzung

| Nr. | Beschreibung | Verletzung der | | | Angriff auf | | |
|---|---|---|---|---|---|---|---|
| | | Vertr. | Verf. | Int. | Clt. | Net. | Pxy. |
| 1 | SIP Call Setup Forking | x | | | x | x | x |
| 2 | SIP Flooding (DoS) | | x | | x | | x |
| 3 | SIP Call Hijacking / Impersonating | x | | | x | | x |
| **4** | **SIP Call termination** | | **x** | | **x** | | **x** |
| 5 | SIP Identity Spoofing – Telefonieren auf fremde Rechnung | | | x | x | | x |
| 6 | RTP Paket Injection – Datastream verändern | | x | x | x | x | x |
| 7 | RTP Stream aufzeichnen/mithören | x | | | x | x | x |
| 8 | RTCP Paket Injection – Codec wechsel | | x | | x | | x |
| 9 | Multicast Forking | x | | | | x | |
| 10 | Verfälschte IP/TCP/SIP/SDP Pakete. Instabilität der Systeme | | x | | x | | x |
| **11** | **Voice Spam – autom.Telefonanrufe** | | | | **x** | | |
| 12 | Asterisk OS Angriff | x [1)] | x [1)] | x [1)] | | | x |
| 13 | Asterisk SW schwäche | x [1)] | x [1)] | x [1)] | | | x |
| 14 | Asterisk Angriff auf Konfigurationsinterface WebGUI / Telnet / SSH | x [1)] | x [1)] | x [1)] | | | x |
| 15 | CDR verändern | | | x | | | x |

Rot: Gefahr konnte nicht verringert werden. Gelb: Gefahr konnte gemindert werden Grün: Gefahr konnte auf Minimum red. werden

29

# Agenda

- VoIP Technologie Primer
- Service Qualität
- Telefonie Szenario
- Identifikation der Sicherheitsprobleme
- Möglichkeiten der Absicherung
- Fazit

30

GO OUT IT-SECURITY HOSTING
klubschule MIGROS
inetnova
interway net intelligence
SKYBOW
IT - Security Forum #4

# Fazit

- Auswertung zeigt ein deutliches Bild
  - Die meisten Sicherheitsmassnahmen zielen auf die PBX-Infrastruktur
  - Dort können auch gute Resultate erzielt werden
- Clientseitig kann nur mit Empfehlungen gedient werden.
- Der aktuelle Sicherheitsstandard beim Kunden bleibt unklar.
- Die Sicherheitsschlacht wird beim Kunden geschlagen.

31

GO OUT IT-SECURITY HOSTING
klubschule MIGROS
inetnova
interway net intelligence
SKYBOW
IT - Security Forum #4

# Fazit allgemein

- Integration von Multimediaanwendungen in unsere Datennetze ist viel mehr als nur ein Hype.
- SIP Protokoll ist klarer Favorit durch seine Einfachheit.
- In der Einfachheit liegt aber auch die Gefahr. Es wäre wünschenswert gewesen, dass wir unsere Lektion aus den Sicherheitsproblemen im Internet gelernt haben.

32

GO OUT IT-SECURITY HOSTING

klubschule MIGROS

inside nova

interway net intelligence

SKYBOW

IT - Security Forum #4

# Fazit allgemein

- Erkenntnis:
  Gestartet mit dem Anspruch Voice sicher auszugestalten sind wir beim Absichern einer normalen IT Infrastruktur gelandet.
- Wie prophezeit, wird Telefonie in Zukunft nur wie eine weitere IT Applikation behandelt werden müssen.
- Die Verschmelzung von Sprache und Daten hat definitiv und unwiderruflich begonnen.

33