VoIP Security

Hendrik Scholz
VoIP Entwickler
freenet Cityline GmbH
hendrik.scholz@freenet-ag.de

freenet?

- freenet = ISP, PSTN Carrier + Mehrwertdienste
- Produkt: freenet iPhone
  - Telefonie als IP Dienstleistung
  - PSTN Ersatz
- DSL Router mit VoIP Funktionalität
- Open Source Software
  - SIP Express Router ''SER''
  - Asterisk
  - Support der Open Source Community

Agenda

- Status Quo
- Angriffe
  - Mithören
  - Denial of Service
  - Identitätsmissbrauch
  - SPAM over IP Telephony
- Session Border Controller
- Ausblick

Status Quo

- VoIP als Call-by-Call Ersatz
- Beworben als PSTN-Ersatz
  - PSTN Funktionalität abgebildet
  - kein Presence, Instant Messaging
- VoIP als Re-Implementation der PSTN-Welt
  - vergleichbare Ansätze
  - ähnliche Probleme

Gefahren im VoIP Umfeld

Malformed Requests
Misrepresenting Authority
Conversation Alteration
Conversation Degrading
Request Looping
Call Teardown
Misrepresenting Identity
Unwanted Contact
Media Hijacking
User Call Flooding
Call Rerouting
False Caller Identification
Video Reconstruction
Eavesdropping
Fax Reconstruction
Spoofed Messages
Text Reconstruction
Misrepresenting Content
Theft of Services
Impersonation
Call Controller Flooding
Conversation Reconstruction
Call Pattern Tracking
Fax Alternation
Voicemail Reconstruction
Traffic Reconstruction
Number Harvesting
Call Hijacking
Misrepresenting Rights

http://voipsa.org/Activities/taxonomy.php

Angriffe

Mithören

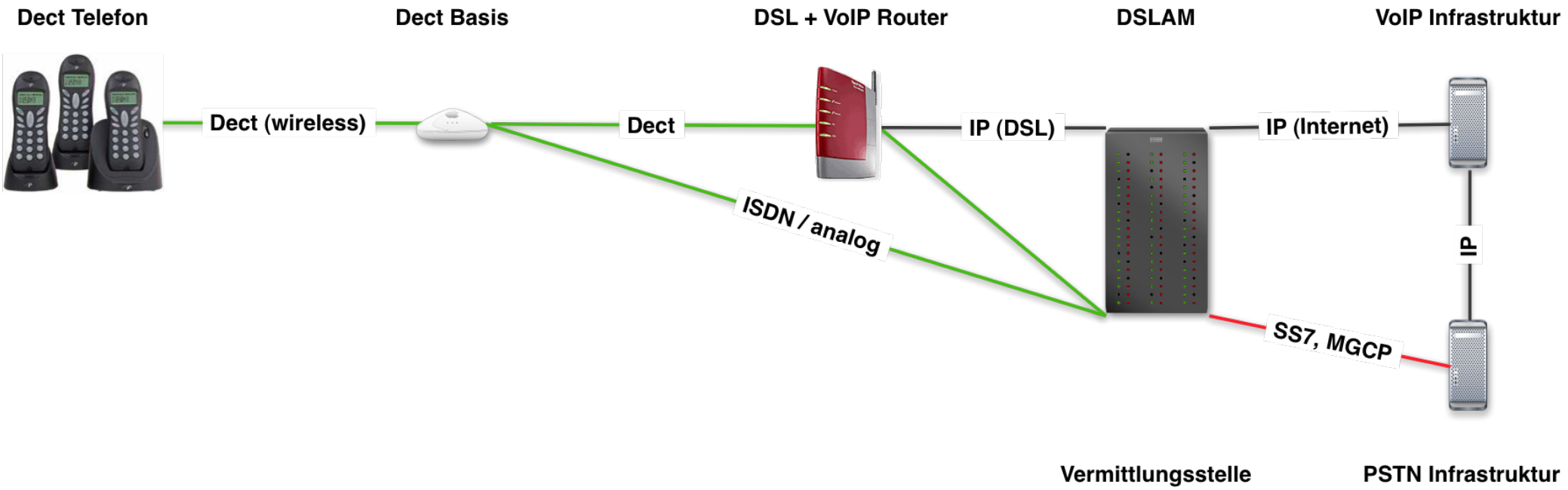
Denial of Service

Identitätsmissbrauch

SPAM over IP Telephony

Anschlüsse zum Abhören

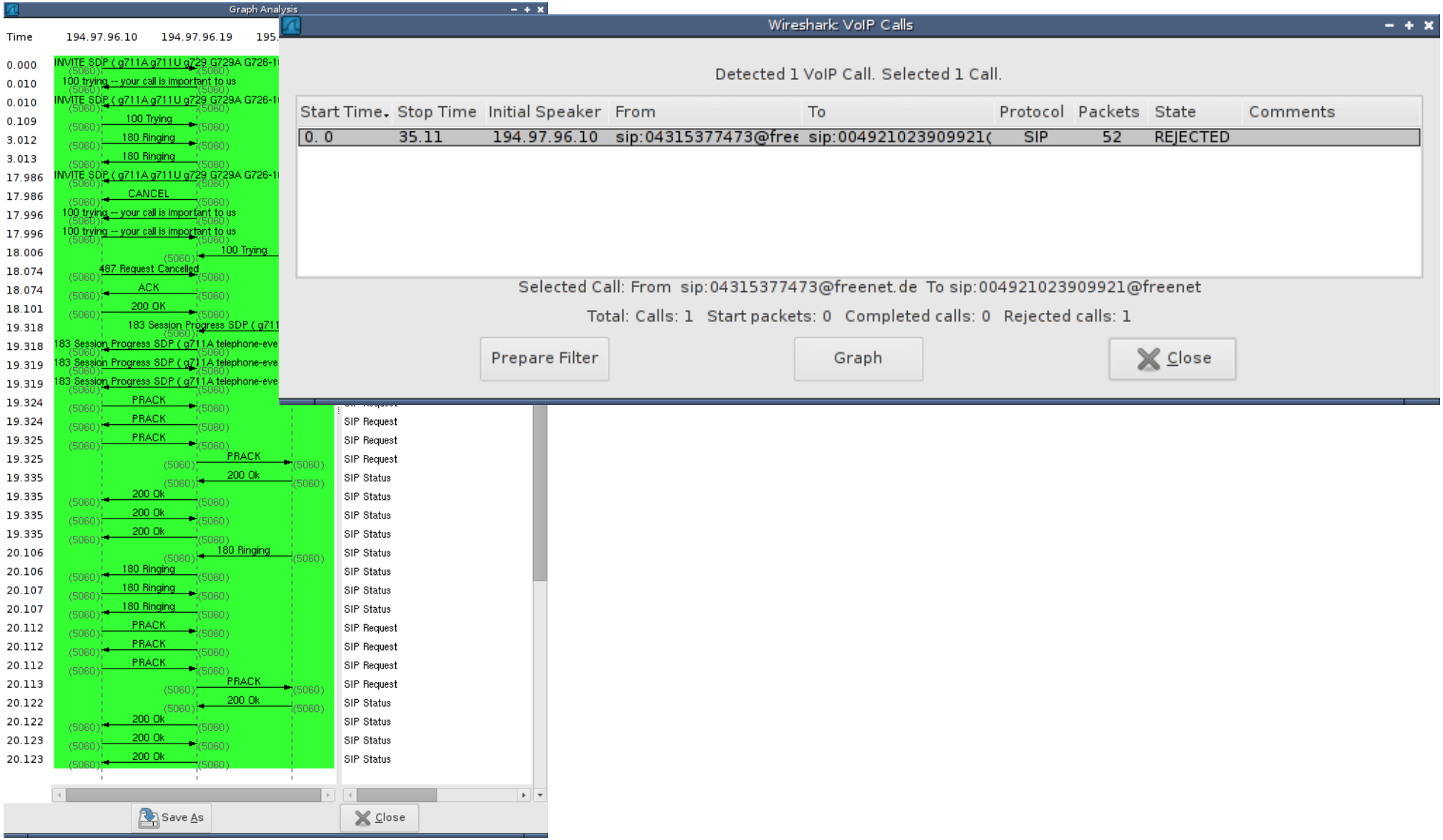
- zwischen Dect Handset und Dect Basis-Station
- IP-Ebene: zwischen VoIP Endgerät und ISP
- beim ISP / im freien Internet



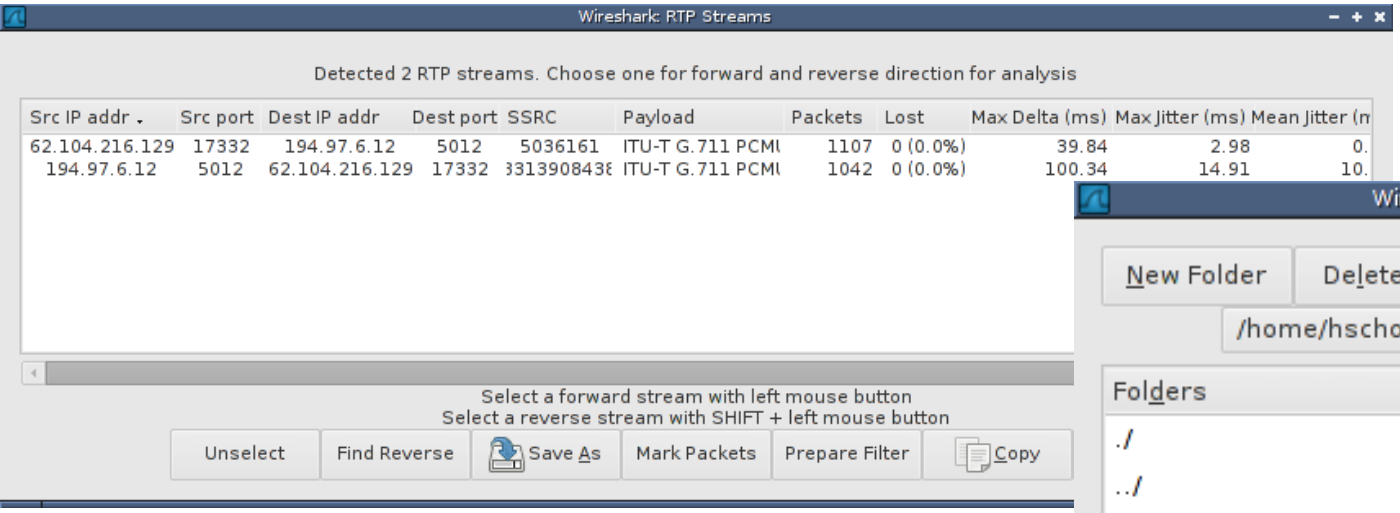
VoIP Mithoeren im LAN

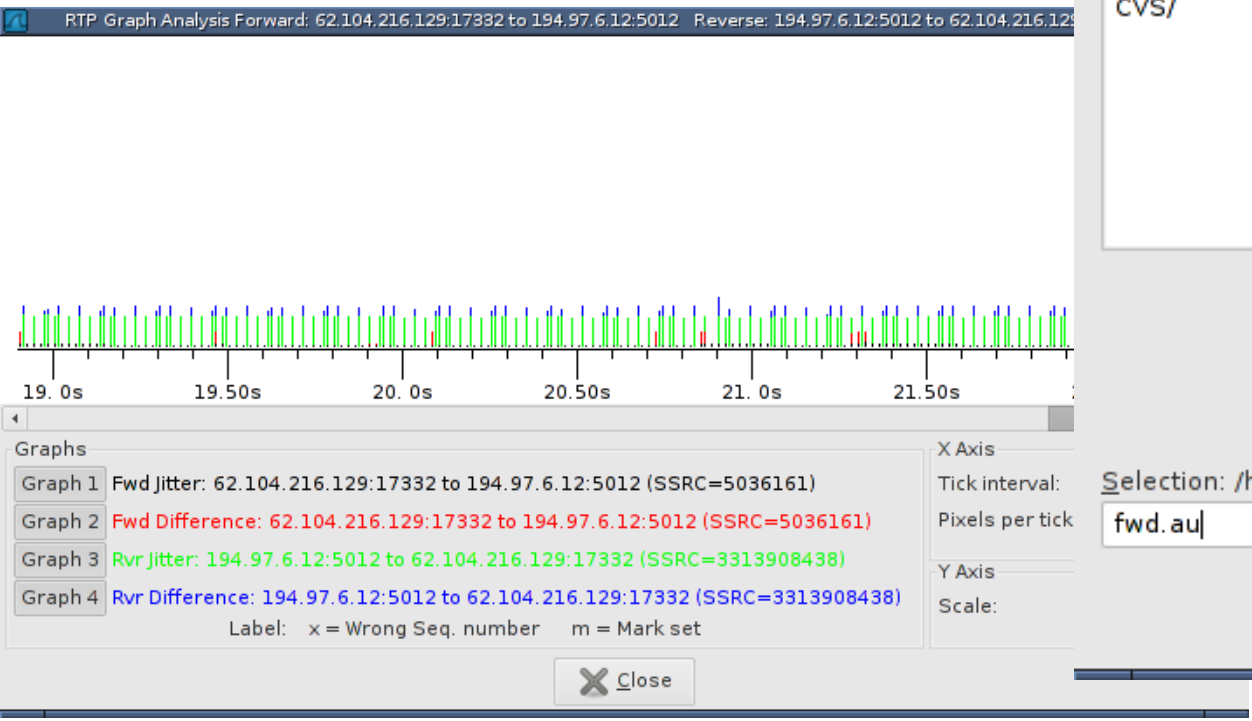
- Voraussetzungen
  - Zugang zu Datenstrom (SIP + RTP)
  - Zugriff in Echtzeit oder aus Mitschnitt
    - ggf. grosse Datenmengen
  - Wireshark von http://wireshark.org/
- Absicherung
  - getrennte Vlans fuer Voice und Daten
  - SIP + RTP Verschlüsselung

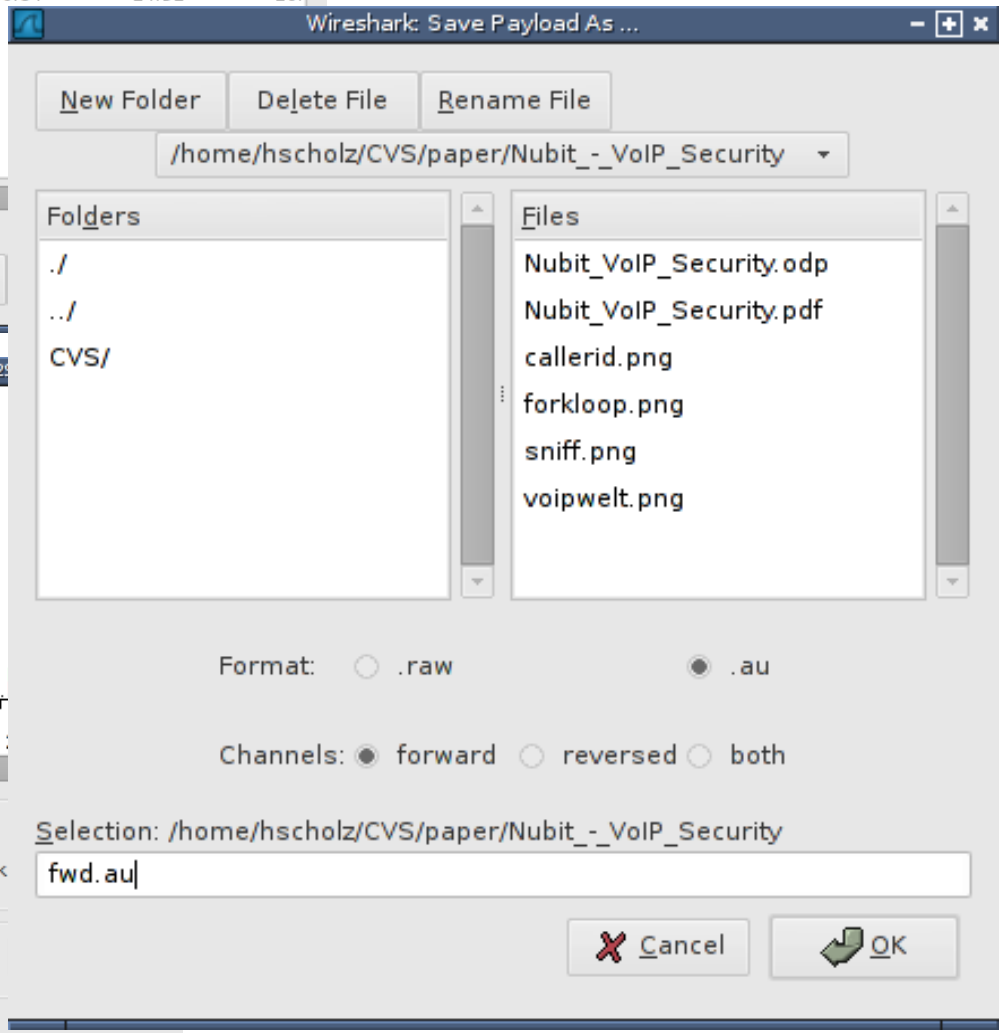
Wireshark


Graph Analysis
Time
194.97.96.10
194.97.96.19
0.000 INVITE SDP (g711A g711U g729 G729A G726-1
0.010 100 trying -- your call is important to us
0.010 INVITE SDP (g711A g711U g729 G729A G726-1
0.109 100 Trying
3.012 180 Ringing
3.013 180 Ringing
17.986 INVITE SDP (g711A g711U g729 G729A G726-1
17.986 CANCEL
17.996 100 trying -- your call is important to us
17.996 100 trying -- your call is important to us
18.006 100 Trying
18.074 487 Request Cancelled
18.074 ACK
18.101 200 OK
19.318 183 Session Progress SDP (g711
19.318 183 Session Progress SDP (g711A telephone-eve
19.319 183 Session Progress SDP (g711A telephone-eve
19.319 183 Session Progress SDP (g711A telephone-eve
19.324 PRACK
19.324 PRACK
19.325 PRACK
19.325 PRACK
19.335 200 Ok
19.335 200 Ok
19.335 200 Ok
19.335 200 Ok
20.106 180 Ringing
20.106 180 Ringing
20.107 180 Ringing
20.107 180 Ringing
20.112 PRACK
20.112 PRACK
20.112 PRACK
20.113 PRACK
20.122 200 Ok
20.122 200 Ok
20.123 200 Ok
20.123 200 Ok
(5060)
SIP Request
SIP Status
Save As
Close
Wireshark: VoIP Calls
Detected 1 VoIP Call. Selected 1 Call.
Start Time
Stop Time
Initial Speaker
From
To
Protocol
Packets
State
Comments
0. 0
35.11
194.97.96.10
sip:04315377473@free
sip:004921023909921(
SIP
52
REJECTED
Selected Call: From sip:04315377473@freenet.de To sip:004921023909921@freenet
Total: Calls: 1 Start packets: 0 Completed calls: 0 Rejected calls: 1
Prepare Filter
Graph
Close

Wireshark


Wireshark: RTP Streams
Detected 2 RTP streams. Choose one for forward and reverse direction for analysis
Src IP addr | Src port | Dest IP addr | Dest port | SSRC | Payload | Packets | Lost | Max Delta (ms) | Max Jitter (ms) | Mean Jitter (m
62.104.216.129 | 17332 | 194.97.6.12 | 5012 | 5036161 | ITU-T G.711 PCMU | 1107 | 0 (0.0%) | 39.84 | 2.98 | 0.
194.97.6.12 | 5012 | 62.104.216.129 | 17332 | 3313908438 | ITU-T G.711 PCMU | 1042 | 0 (0.0%) | 100.34 | 14.91 | 10.
Select a forward stream with left mouse button
Select a reverse stream with SHIFT + left mouse button
Unselect
Find Reverse
Save As
Mark Packets
Prepare Filter
Copy


RTP Graph Analysis Forward: 62.104.216.129:17332 to 194.97.6.12:5012 Reverse: 194.97.6.12:5012 to 62.104.216.12
19. 0s
19.50s
20. 0s
20.50s
21. 0s
21.50s
Graphs
Graph 1 Fwd Jitter: 62.104.216.129:17332 to 194.97.6.12:5012 (SSRC=5036161)
Graph 2 Fwd Difference: 62.104.216.129:17332 to 194.97.6.12:5012 (SSRC=5036161)
Graph 3 Rvr Jitter: 194.97.6.12:5012 to 62.104.216.129:17332 (SSRC=3313908438)
Graph 4 Rvr Difference: 194.97.6.12:5012 to 62.104.216.129:17332 (SSRC=3313908438)
Label: x = Wrong Seq. number m = Mark set
X Axis
Tick interval:
Pixels per tick
Y Axis
Scale:
Close


Wireshark: Save Payload As ...
New Folder
Delete File
Rename File
/home/hscholz/CVS/paper/Nubit_-_VoIP_Security
Folders
./
../
CVS/
Files
Nubit_VoIP_Security.odp
Nubit_VoIP_Security.pdf
callerid.png
forkloop.png
sniff.png
voipwelt.png
Format: .raw .au
Channels: forward reversed both
Selection: /home/hscholz/CVS/paper/Nubit_-_VoIP_Security
fwd.au
Cancel
OK

Angriffe

Mithören

Denial of Service

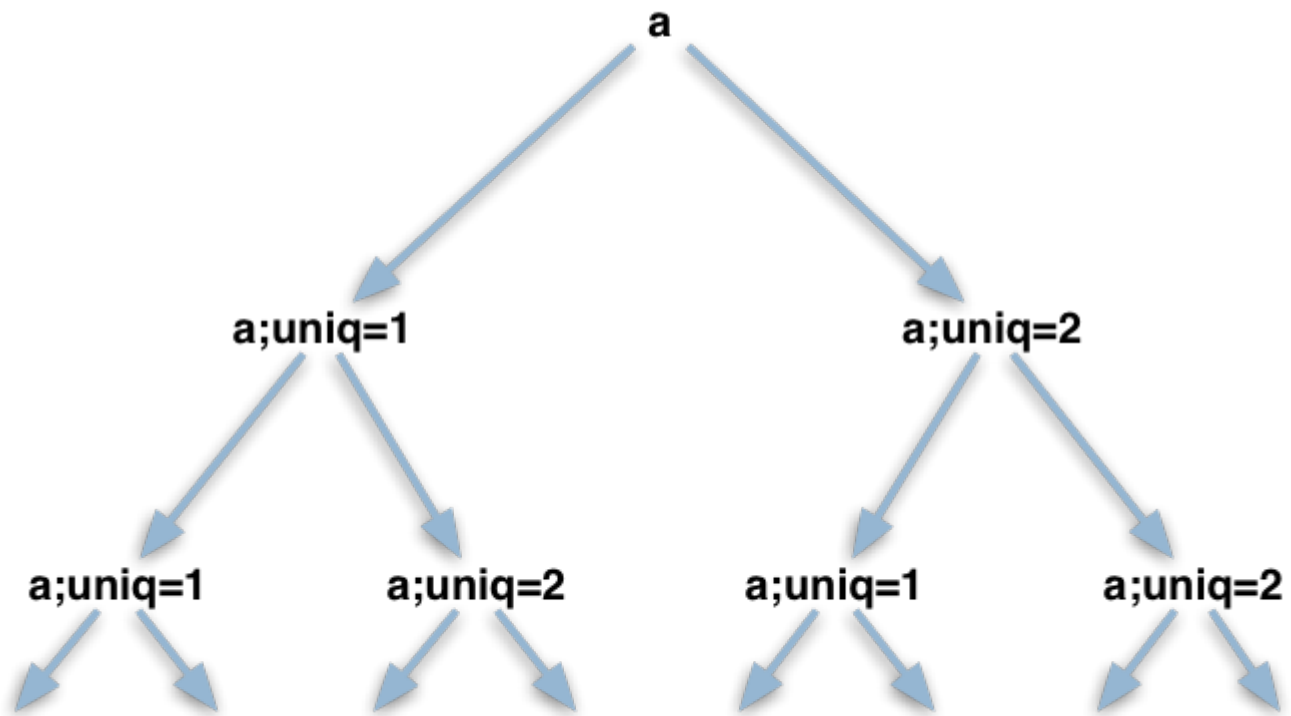
Identitätsmissbrauch

SPAM over IP Telephony

Denial Of Service

- Denial of Service gegen Infrastruktur
- Traffic Amplification
  - SIPit 19, draft-ietf-sip-fork-loop-fix-04
  - doppelte Registrierung eines Users
  - Multiplikation der INVITES durch paralleles Klingeln
  - rekursives Auflösen des Ziel-Contacts
  - 70 Schritte: 1.180.591.620.717.411.303.424 INVITEs

Denial of Service



Unintentional DDOS

- ungewollte Denial of Service Angriffe
- ausgelöst durch
  - Konfigurationsfehler
  - Fehlimplementation
  - Retransmissons durch timer/Firewall-Probleme
- Quelle: legitime Endgeräte/Kunden
  - schwer zu blocken

Unintentional DDOS Beispiel

- T-DSL 24h Zwangstrennung
- Router-Feature: Zwangstrennung nachts
- Default-Einstellung: 3 Uhr morgens
  - NTP synchronisiert

- Last-Problem: Alle Kunden registrieren sich um 3 Uhr neu
  - 3-6x Authentisierung gegen Datenbank
  - 20-30 Pakete pro Account

Angriffe

Mithören

Denial of Service

Identitätsmissbrauch

SPAM over IP Telephony

Identitätsmissbrauch

- Anwendung der Identität
  - Rufnummernanzeige
  - Authentisierung
- Betrugsfall Mobil-Mailbox Authentisierung
  - Kunde ruft eigene Mailbox an
  - eigene Rufnummer als Authentisierung statt PIN
  - Problem: Rufnummer fälschbar

Rufnummernanzeige in VoIP

- Implementation
  - Remote-Party-ID Header
  - RFC 3323, 3325 'Privacy Extensions'
  - propritäre Implementationen 'Set-Caller-ID'
- Problem
  - kein eindeutiger vorgeschriebener Standard

Caller-ID Angriff

- alle Header werden gesetzt
- ISP ignoriert 'unbekannten' Header
- PSTN Gateway nutzt falschen Header

INVITE sip:0049311@123.org
From: "foo" <0049199123@123.org>
Remote-Party-ID: <sip:**001800999**@123.org>
P-Asserted-Identity: <sip:**001800999**@123.org>
Authorization: ... username="0049199123" ...

INVITE sip:0049311@123.org
From: "foo" <0049199123@123.org>
Remote-Party-ID: <sip:**0049199123**@123.org>
P-Asserted-Identity: <sip:**001800999**@123.org>

Angriffe

Mithören

Denial of Service

Identitätsmissbrauch

SPAM over IP Telephony

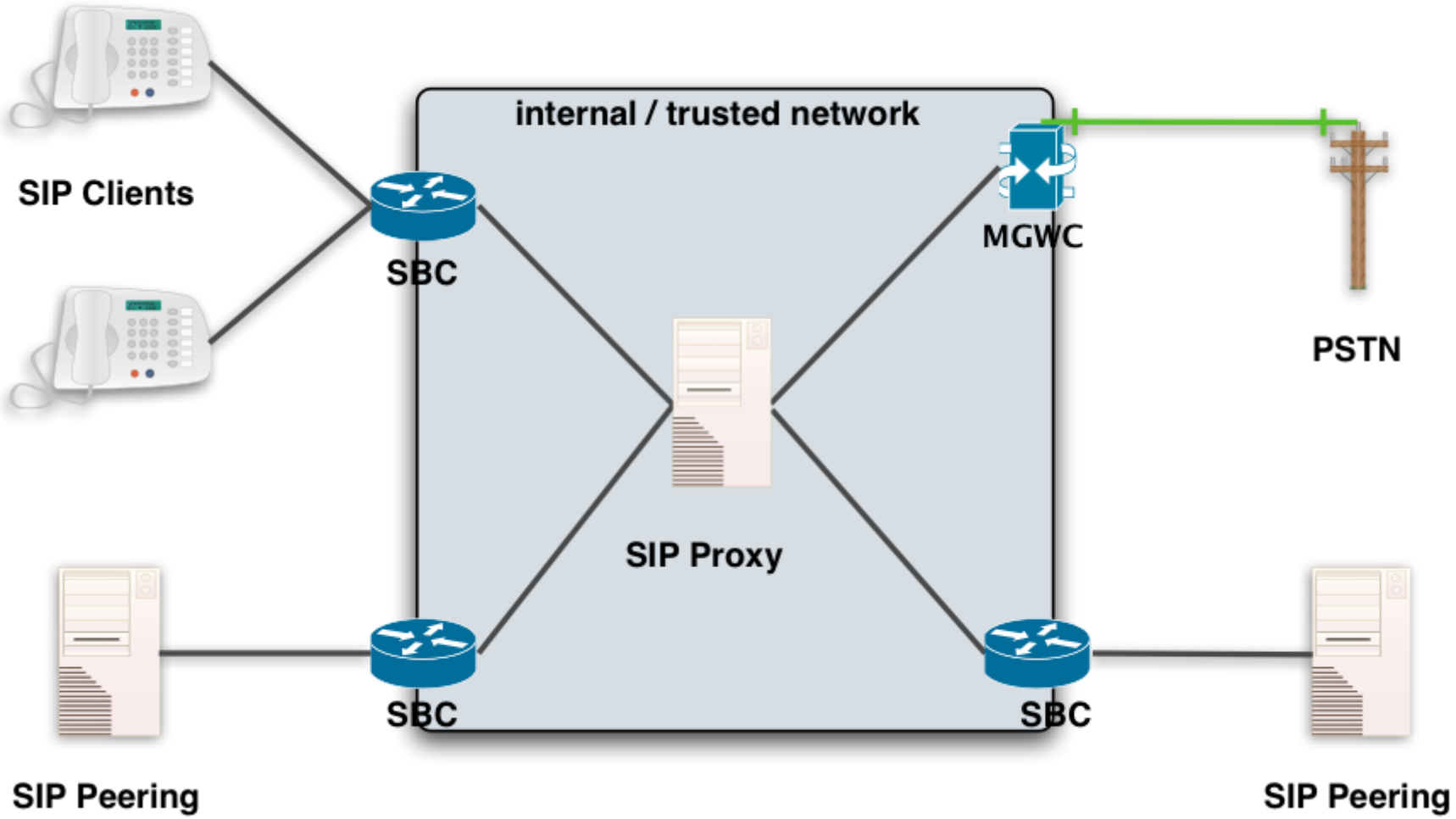
SPIT - Spam over IP Telephony

- Spam over IP Telephony
  - Werbeanrufe
  - noch kein akutes Problem
- Projekte
  - http://spit-abwehr.de/ vom ULD
  - NEC: draft-niccolini-sipping-feedback-spit-02
- Vorbereitung
  - Datensammlung: Number Harvesting
  - gefälschte Accounts

Session Border Controller

- angebliche Lösung für
  - Billing
  - Infrastructure Hiding
  - Schutz der Privatsphäre, anonyme Calls
  - Security Probleme
  - Hochverfügbarkeit
  - Lawful Interception

Session Border Controller



SBC - Probleme

- SBC mitten im Call-Flow
  - Features abhängig vom SBC
- Verfügbarkeit
  - Redundanzkonzept schwer erreichbar
  - Retransmissions treffen Standby-Maschinen
- Kosten
  - teuer, insbesondere durch Sprach-Daten
  - Support-Verträge

Ausblick

- SPIT
  - Peer-2-Peer SIP als Problem
    - SPIT am Schutz des ISP vorbei
  - SMS Spam
  - “Spam goes VoIP – Number Harvesting for Fun and Profit”
- VoIP botnets
  - Soft-/Hardware-Monokultur
  - Ausnutzen der VoIP-API, Bandbreite
  - Resale von Resourcen

VoIP als PSTN Ersatz

- Anforderungen an VoIP
  - Erreichbarkeit, Verfügbarkeit
  - Notruf Lokalisierung
  - Gesetze
    - Lawful Interception
    - TKV – Abrechnungsgenauigkeit
- Features
  - Applikation jenseits vom Festnetz

Fragen
&
Antworten

<hendrik.scholz@freenet-ag.de>
http://www.wormulon.net/