IPCOMM2006

September 25-27 • Gaylord Opryland • Nashville, TN

# Protect Yourself Against VoIP Hacking

**Mark D. Collier**
**Chief Technology Officer**
**SecureLogix Corporation**

# What Will Be Covered

How to assess the security of your IPT network:

- In house/external and ground rules/scope
- Discovery
- Security policy review and physical security checks
- Platform tests
- Network tests
- Application tests
- Links

# Ground Rules and Scope

Internal or with external consultants

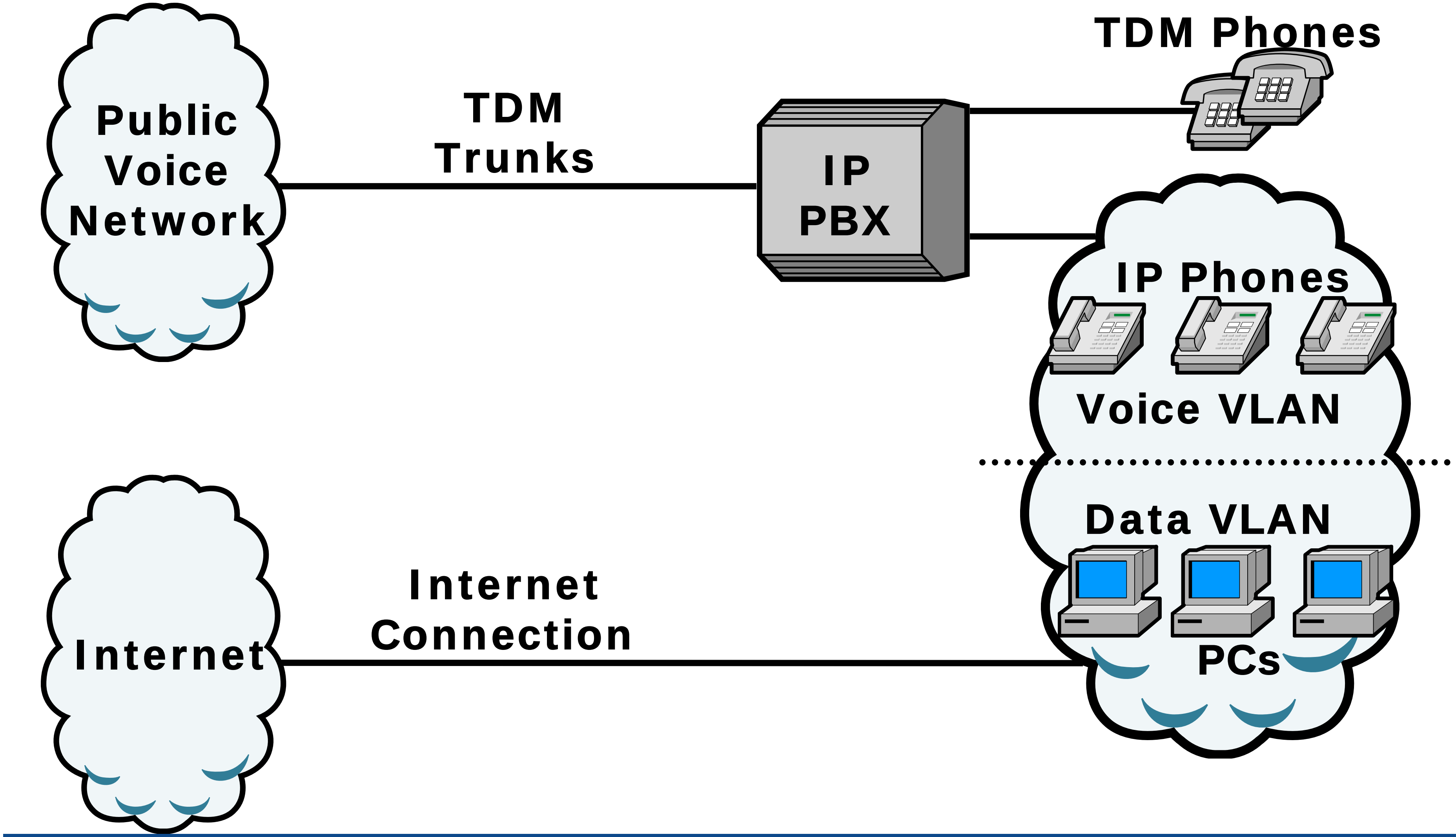
Ground rules:

- Internet and/or internal access
- How much information to start with
- Which group to work with, if any
- Agree how intrusive the test will be

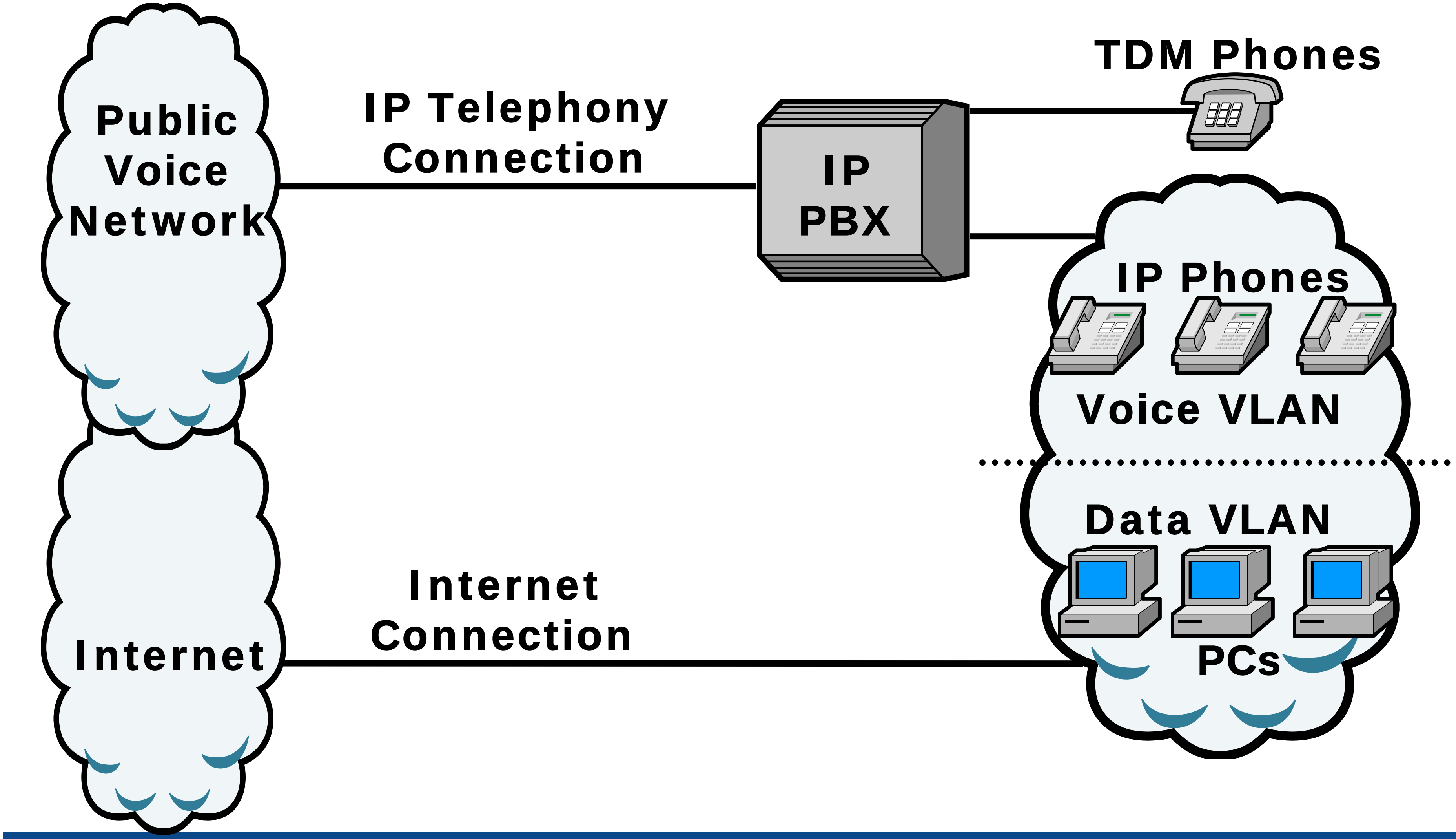
Scope:

- Number of sites
- Which systems/components to test

# Internal Access?



# External Access?



# Policy Review/Physical Security

Review IP Telephony security policy:

- Use as a guide to verify IP Telephony system configuration

Physical security:

- Essential for core components
- If the network is not physically secure, many attacks are trivial for insiders
- All other security is moot if physical security is lacking
- Don’t forget to protect the IP phones

# Security Policy/Physical Security Recommendations

Develop a written IP Telephony security policy.

Follow the security policy

Protect all core IP Telephony components

Enable protections for the IP phones

Control access to “public” IP phones

# Discovery - Footprinting

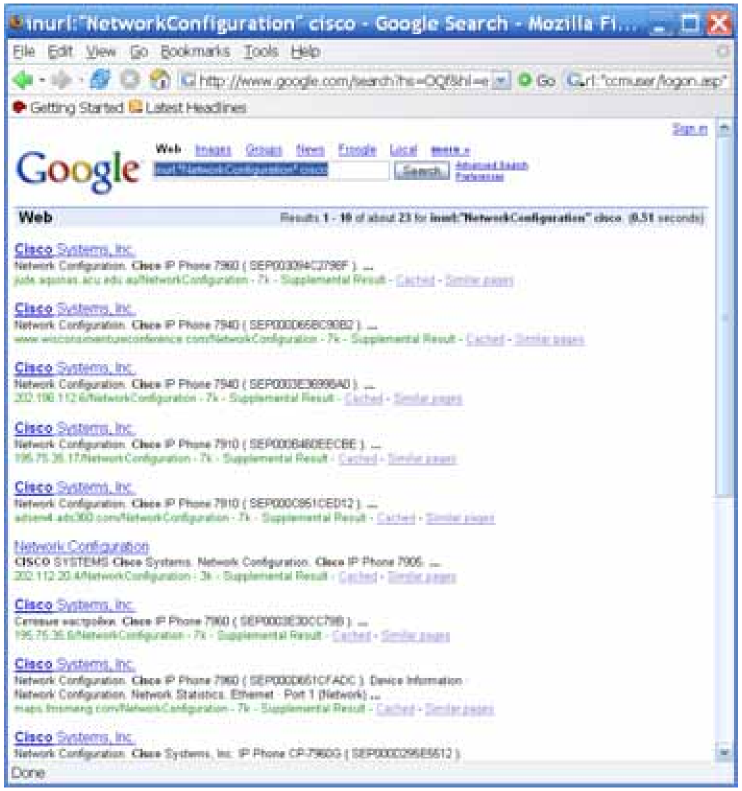
Search enterprise web site:

- Job listings
- Names, extensions, organization structure
- Voice mail greetings

Use Google to search for:

- Case studies/vendor Press Releases
- User resumes and postings
- Web based IP Telephony logins
- Vendor user forums

# Discovery - Footprinting


inurl:"NetworkConfiguration" cisco - Google Search - Mozilla Fi...
File Edit View Go Bookmarks Tools Help
http://www.google.com/search?hs=OQf&hl=e
Go
url:"ccmuser/logon.asp"
Getting Started Latest Headlines
Sign in
Google
Web Images Groups News Froogle Local more »
Search
Advanced Search
Preferences
Done

inurl:"NetworkConfiguration" cisco

Web — Results 1 - 10 of about 23 for inurl:"NetworkConfiguration" cisco. (0.51 seconds)

Cisco Systems, Inc.
Network Configuration. Cisco IP Phone 7960 ( SEP003094C2796F ) ...
jude.aquinas.acu.edu.au/NetworkConfiguration - 7k - Supplemental Result - Cached - Similar pages

Cisco Systems, Inc.
Network Configuration. Cisco IP Phone 7940 ( SEP000D65BC90B2 ) ...
www.wisconsinventureconference.com/NetworkConfiguration - 7k - Supplemental Result - Cached - Similar pages

Cisco Systems, Inc.
Network Configuration. Cisco IP Phone 7940 ( SEP0003E36998A0 ) ...
202.190.112.6/NetworkConfiguration - 7k - Supplemental Result - Cached - Similar pages

Cisco Systems, Inc.
Network Configuration. Cisco IP Phone 7910 ( SEP000B460EECBE ) ...
196.75.36.17/NetworkConfiguration - 7k - Supplemental Result - Cached - Similar pages

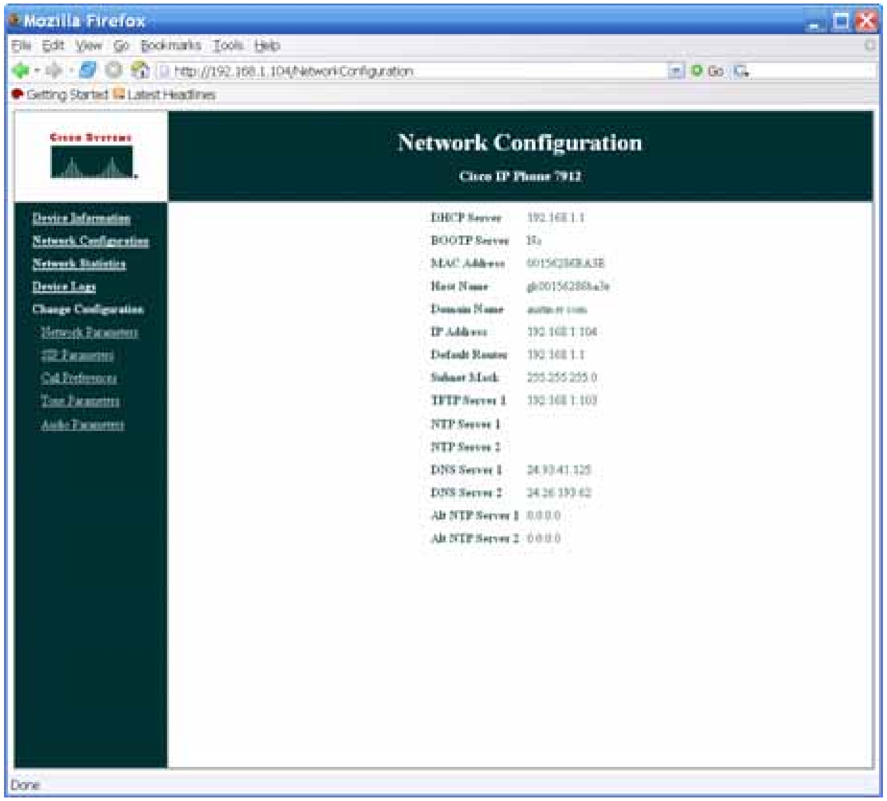
Cisco Systems, Inc.
Network Configuration. Cisco IP Phone 7910 ( SEP000C851CED12 ) ...
adsen4.ads360.com/NetworkConfiguration - 7k - Supplemental Result - Cached - Similar pages

Network Configuration
CISCO SYSTEMS Cisco Systems. Network Configuration. Cisco IP Phone 7905. ...
202.112.20.4/NetworkConfiguration - 3k - Supplemental Result - Cached - Similar pages

Cisco Systems, Inc.
Сетевые настройки. Cisco IP Phone 7960 ( SEP0003E30CC79B ) ...
195.75.36.6/NetworkConfiguration - 7k - Supplemental Result - Cached - Similar pages

Cisco Systems, Inc.
Network Configuration. Cisco IP Phone 7960 ( SEP000D651CFADC ). Device Information · Network Configuration. Network Statistics. Ethernet · Port 1 (Network) ...
maps.fmsmang.com/NetworkConfiguration - 7k - Supplemental Result - Cached - Similar pages

Cisco Systems, Inc.
Network Configuration. Cisco Systems, Inc. IP Phone CP-7960G ( SEP000D295E5612 )



## Network Configuration

Cisco IP Phone 7912

| | |
|---|---|
| DHCP Server | 192.168.1.1 |
| BOOTP Server | No |
| MAC Address | 00156288BA3E |
| Host Name | gb00156288ba3e |
| Domain Name | austin.rr.com |
| IP Address | 192.168.1.104 |
| Default Router | 192.168.1.1 |
| Subnet Mask | 255.255.255.0 |
| TFTP Server 1 | 192.168.1.103 |
| NTP Server 1 | |
| NTP Server 2 | |
| DNS Server 1 | 24.93.41.125 |
| DNS Server 2 | 24.28.193.62 |
| Alt NTP Server 1 | 0.0.0.0 |
| Alt NTP Server 2 | 0.0.0.0 |

## Discovery - Scanning

Use various available tools to find more IP addresses:

- **fping** and **nmap**

Identify IP Telephony systems:

- Identify the system
- Identify operating system and software versions
- **nmap** is probably the best tool for this
- **nmap** has a very good database for IP Telephony
- Some commercial scanners support this as well

# Discovery Recommendations

Remove what you can from corporate web site

Use google to determine your exposure

Make sure no systems are visible on the Internet

Make sure firewalls block scans

# Platform – IP PBX

Test for open or unnecessary network ports:

- **telnet** or other remote access
- Find application ports for later testing

Test operating systems for known vulnerabilities:

- Use general vulnerability scanners
- Use IP Telephony-specific scanners where possible

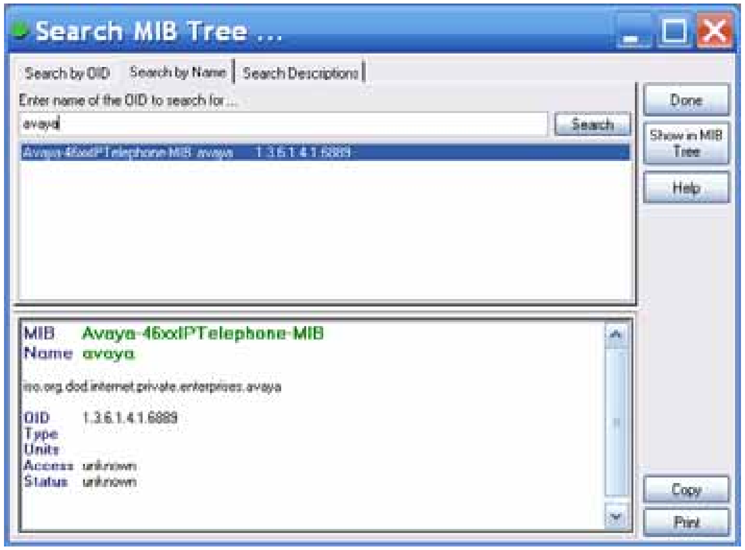
Test for default or weak passwords

Test for default configuration weaknesses

# Platform – IP PBX

Test for SNMP weaknesses:

- Simple SNMP sweeps can provide a lot of information
- If you know the device type, you can use **snmpwalk**
- You can find the OID using **Solarwinds** MIB database



Enter name of the OID to search for ...

avaya

```
Avaya-46xxIPTelephone-MIB  avaya     1.3.6.1.4.1.6889
```

```
MIB     Avaya-46xxIPTelephone-MIB
Name    avaya

iso.org.dod.internet.private.enterprises.avaya

OID     1.3.6.1.4.1.6889
Type
Units
Access  unknown
Status  unknown
```

# Platform – Support Services

Test DHCP and DNS

Test provisioning database

Test TFTP for open or unnecessary network ports:

- Many IP phones use TFTP for configuration/image files
- TFTP is rarely secured
- Use **tftpbrute** to guess the filename and download it
- Configuration files have usernames, passwords, etc.
- It may also be possible to corrupt a software image

# Platform – IP Phones

Test for open or unnecessary network ports:

- **telnet** or other remote access
- Find application ports for later testing

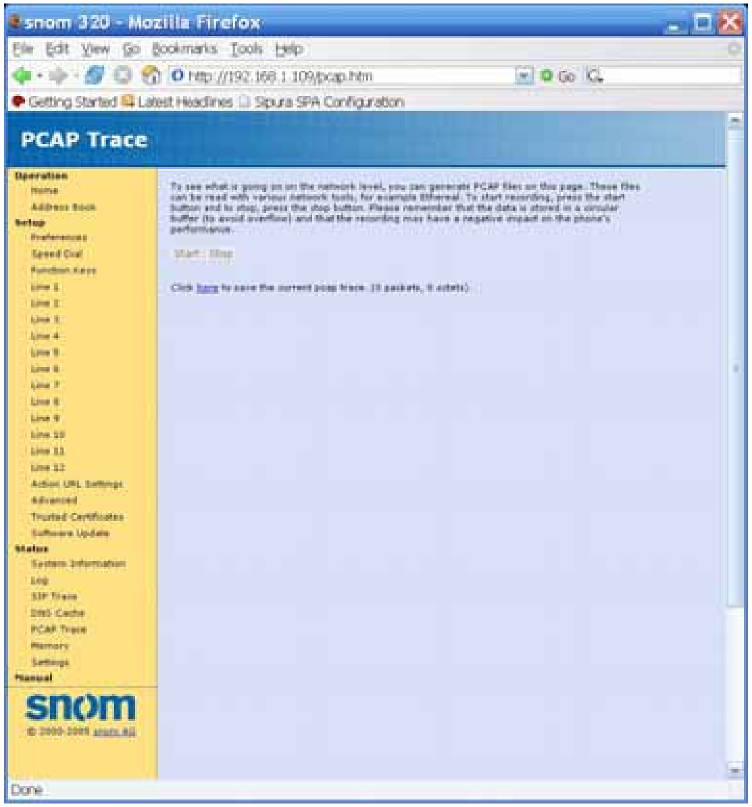
Test for default or weak passwords

Test for weak local physical protections

- Administrative access for some IP phones can be obtained when they are rebooted

# Platform – IP Phones

You can do some interesting things if you get access to certain IP phones



PCAP Trace

To see what is going on on the network level, you can generate PCAP files on this page. These files can be read with various network tools, for example Ethereal. To start recording, press the start button and to stop, press the stop button. Please remember that the data is stored in a circular buffer (to avoid overflow) and that the recording may have a negative impact on the phone's performance.

Click here to save the current pcap trace. (0 packets, 0 octets)

# Platform Recommendations

Remove unnecessary network services

Use secure network administration services

Use firewalls to block enumeration attempts

Use strong passwords – change them periodically

Use secure versions of SNMP

Secure DHCP, DNS, and database services

Avoid use of TFTP if possible

Prevent local manipulation of IP phones

# Network – General

The data network is used to transport IP Telephony signaling/media

Any component is a potential target

Test security on switches, routers, hubs, VPNs, etc.

The IP Telephony network enables attacks such as:

- Denial of Service (DoS)
- Eavesdropping
- Man-in-the-Middle (MITM) attacks

Test to determine if the network is vulnerable

# Network – DoS/Eavesdropping/MITM

Test for network DoS vulnerabilities:

- UDP floods
- TCP SYN floods

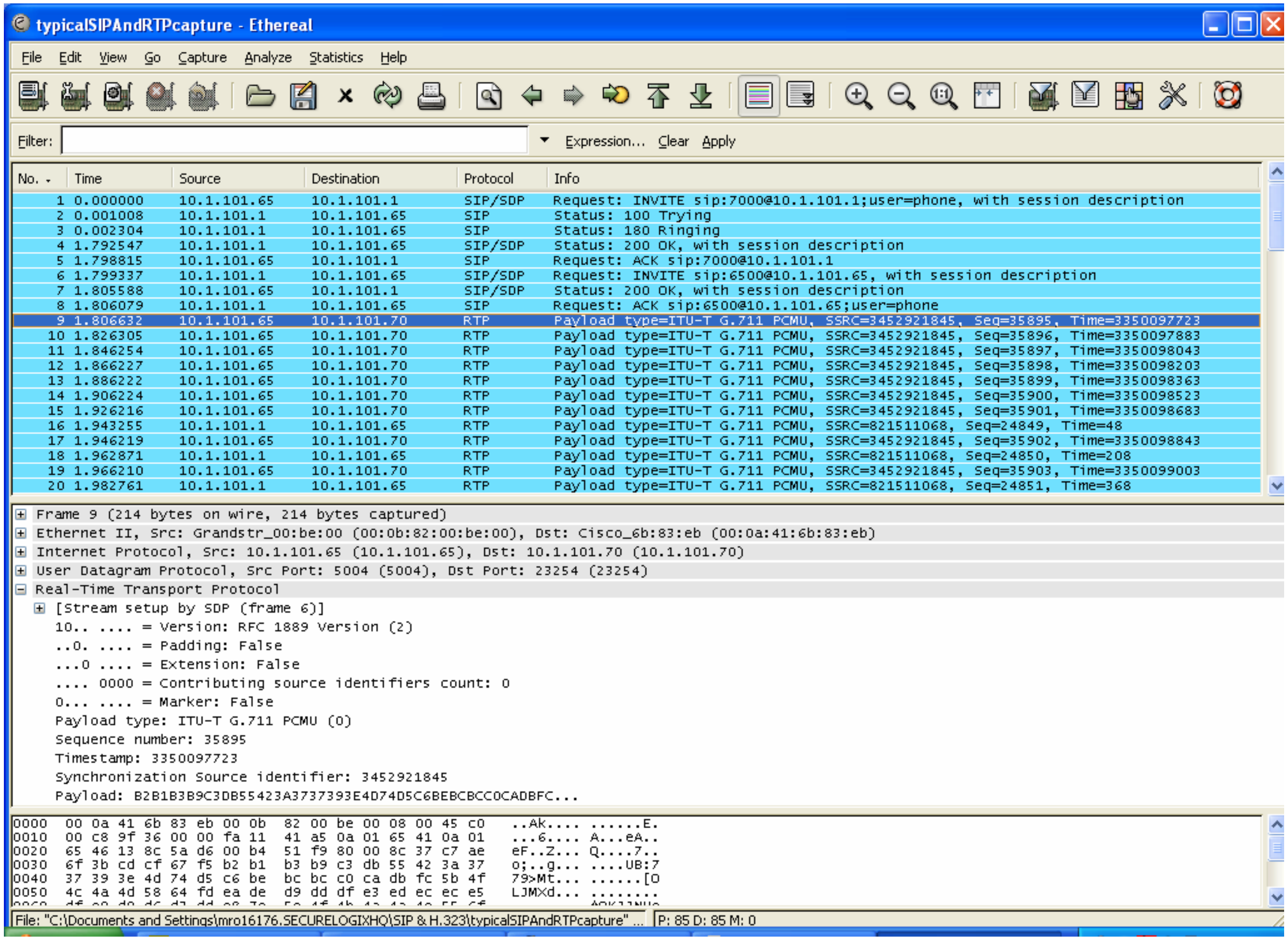
Test for eavesdropping:

- Easy to do if you have access to unencrypted data
- Test with **ethereal**, **CAIN**, **VOMIT**, **VoIPong**

Test for MITM vulnerabilities:

- Easy to attack depending on network
- Test with **ettercap**, **dsniff**

# Network – Eavesdropping


typicalSIPAndRTPcapture - Ethereal
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

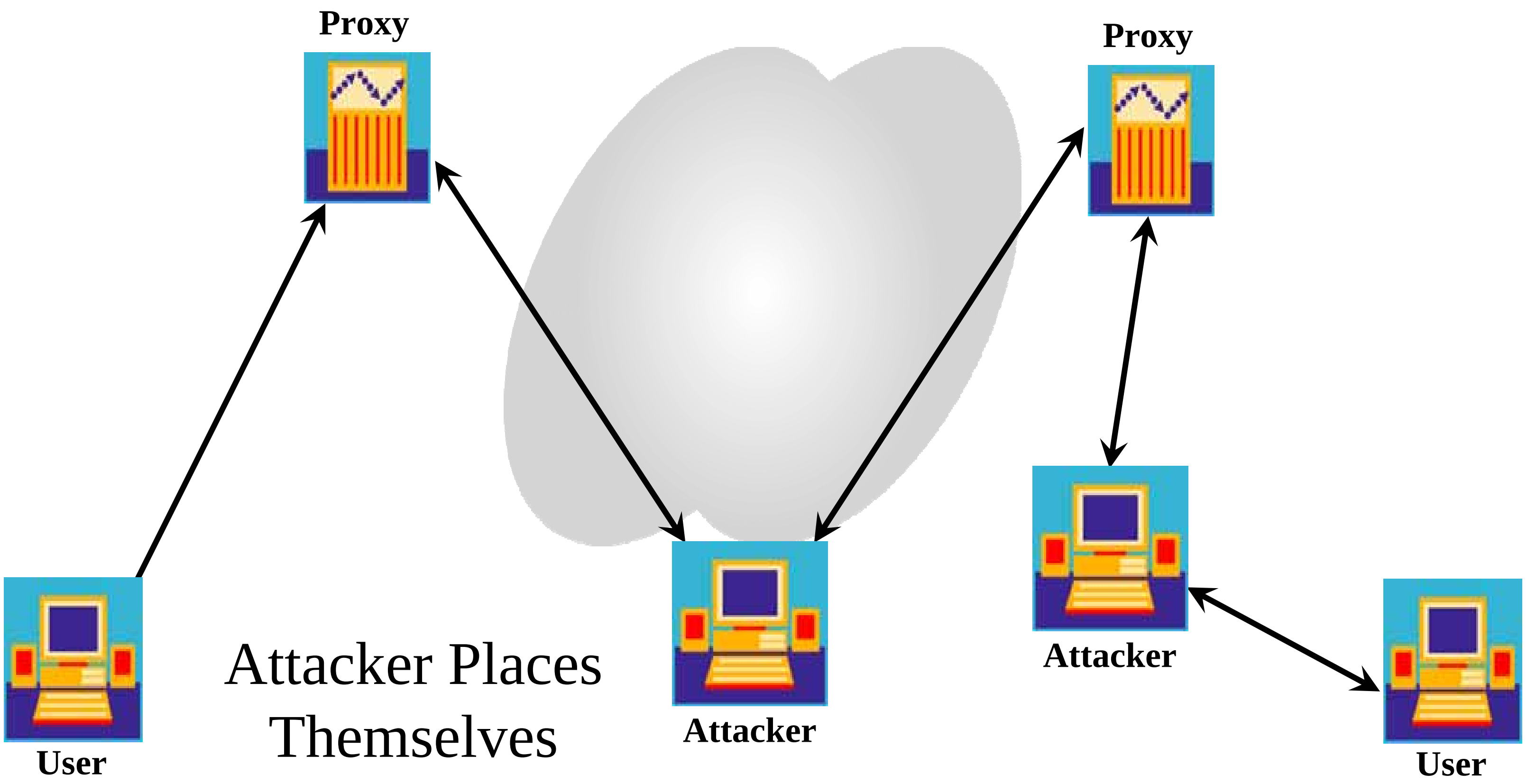
```
No. . Time     Source         Destination    Protocol  Info
  1 0.000000   10.1.101.65    10.1.101.1     SIP/SDP   Request: INVITE sip:7000@10.1.101.1;user=phone, with session description
  2 0.001008   10.1.101.1     10.1.101.65    SIP       Status: 100 Trying
  3 0.002304   10.1.101.1     10.1.101.65    SIP       Status: 180 Ringing
  4 1.792547   10.1.101.1     10.1.101.65    SIP/SDP   Status: 200 OK, with session description
  5 1.798815   10.1.101.65    10.1.101.1     SIP       Request: ACK sip:7000@10.1.101.1
  6 1.799337   10.1.101.1     10.1.101.65    SIP/SDP   Request: INVITE sip:6500@10.1.101.65, with session description
  7 1.805588   10.1.101.65    10.1.101.1     SIP/SDP   Status: 200 OK, with session description
  8 1.806079   10.1.101.1     10.1.101.65    SIP       Request: ACK sip:6500@10.1.101.65;user=phone
  9 1.806632   10.1.101.65    10.1.101.70    RTP       Payload type=ITU-T G.711 PCMU, SSRC=3452921845, Seq=35895, Time=3350097723
 10 1.826305   10.1.101.65    10.1.101.70    RTP       Payload type=ITU-T G.711 PCMU, SSRC=3452921845, Seq=35896, Time=3350097883
 11 1.846254   10.1.101.65    10.1.101.70    RTP       Payload type=ITU-T G.711 PCMU, SSRC=3452921845, Seq=35897, Time=3350098043
 12 1.866227   10.1.101.65    10.1.101.70    RTP       Payload type=ITU-T G.711 PCMU, SSRC=3452921845, Seq=35898, Time=3350098203
 13 1.886222   10.1.101.65    10.1.101.70    RTP       Payload type=ITU-T G.711 PCMU, SSRC=3452921845, Seq=35899, Time=3350098363
 14 1.906224   10.1.101.65    10.1.101.70    RTP       Payload type=ITU-T G.711 PCMU, SSRC=3452921845, Seq=35900, Time=3350098523
 15 1.926216   10.1.101.65    10.1.101.70    RTP       Payload type=ITU-T G.711 PCMU, SSRC=3452921845, Seq=35901, Time=3350098683
 16 1.943255   10.1.101.1     10.1.101.65    RTP       Payload type=ITU-T G.711 PCMU, SSRC=821511068, Seq=24849, Time=48
 17 1.946219   10.1.101.65    10.1.101.70    RTP       Payload type=ITU-T G.711 PCMU, SSRC=3452921845, Seq=35902, Time=3350098843
 18 1.962871   10.1.101.1     10.1.101.65    RTP       Payload type=ITU-T G.711 PCMU, SSRC=821511068, Seq=24850, Time=208
 19 1.966210   10.1.101.65    10.1.101.70    RTP       Payload type=ITU-T G.711 PCMU, SSRC=3452921845, Seq=35903, Time=3350099003
 20 1.982761   10.1.101.1     10.1.101.65    RTP       Payload type=ITU-T G.711 PCMU, SSRC=821511068, Seq=24851, Time=368
```

```
⊞ Frame 9 (214 bytes on wire, 214 bytes captured)
⊞ Ethernet II, Src: Grandstr_00:be:00 (00:0b:82:00:be:00), Dst: Cisco_6b:83:eb (00:0a:41:6b:83:eb)
⊞ Internet Protocol, Src: 10.1.101.65 (10.1.101.65), Dst: 10.1.101.70 (10.1.101.70)
⊞ User Datagram Protocol, Src Port: 5004 (5004), Dst Port: 23254 (23254)
⊟ Real-Time Transport Protocol
  ⊞ [Stream setup by SDP (frame 6)]
    10.. .... = Version: RFC 1889 Version (2)
    ..0. .... = Padding: False
    ...0 .... = Extension: False
    .... 0000 = Contributing source identifiers count: 0
    0... .... = Marker: False
    Payload type: ITU-T G.711 PCMU (0)
    Sequence number: 35895
    Timestamp: 3350097723
    Synchronization Source identifier: 3452921845
    Payload: B2B1B3B9C3DB55423A3737393E4D74D5C6BEBCBCC0CADBFC...
```

```
0000  00 0a 41 6b 83 eb 00 0b  82 00 be 00 08 00 45 c0   ..Ak.... ......E.
0010  00 c8 9f 36 00 00 fa 11  41 a5 0a 01 65 41 0a 01   ...6.... A...eA..
0020  65 46 13 8c 5a d6 00 b4  51 f9 80 00 8c 37 c7 ae   eF..Z... Q....7..
0030  6f 3b cd cf 67 f5 b2 b1  b3 b9 c3 db 55 42 3a 37   o;..g... ....UB:7
0040  37 39 3e 4d 74 d5 c6 be  bc bc c0 ca db fc 5b 4f   79>Mt... ......[O
0050  4c 4a 4d 58 64 fd ea de  d9 dd df e3 ed ec ec e5   LJMXd... ........
```

File: "C:\Documents and Settings\mro16176.SECURELOGIXHQ\SIP & H.323\typicalSIPAndRTPcapture" ... P: 85 D: 85 M: 0

# Network – Man-in-the-middle



Attacker Places Themselves Between Proxies Or Proxy/UA

# Network Recommendations

Use NAC or other means of controlling network access

Use rate limiting on switches to control DoS

Use signaling and media encryption to prevent eavesdropping

Configure switches to prevent MITM attacks

# Application - General

The “application” consists of the actual IP Telephony signaling and media exchanged over the network

The various components generating/consuming this information can be vulnerable to attack

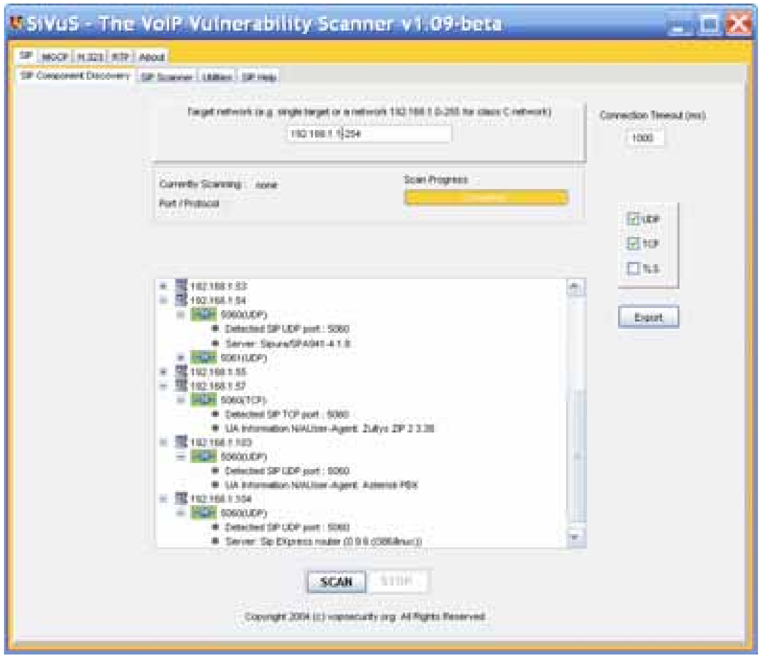
This will be especially true when IP Telephony is exchanged with a public network

The examples used are for SIP, but similar issues exist with other protocols

# Application – Scanning/Enumeration

Enumeration involves identification of valid users:

- Quite a few tools available
- SiVuS and SIPSCAN automate much of this for you:



SiVuS - The VoIP Vulnerability Scanner v1.09-beta

SIP | MGCP | H.323 | RTP | About
SIP Component Discovery | SIP Scanner | Utilities | SIP Help
Export
SCAN
STOP

Target network (e.g. single target or a network 192.168.1.0-255 for class C network): 192.168.1.1-254

Connection Timeout (ms): 1000

Currently Scanning : none

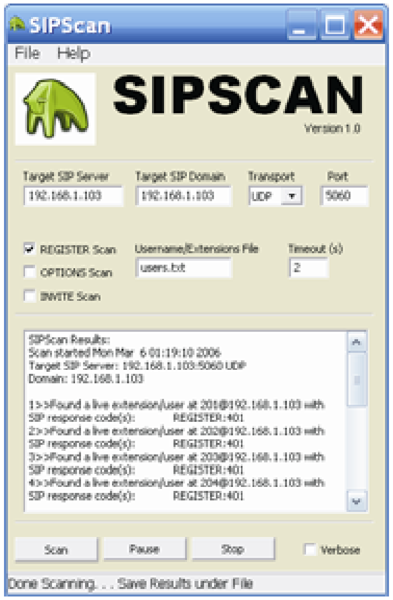
Port / Protocol

Scan Progress

☑ UDP
☑ TCP
□ TLS

```
192.168.1.53
192.168.1.54
  5060(UDP)
    Detected SIP UDP port : 5060
    Server: Sipura/SPA941-4.1.8
  5061(UDP)
192.168.1.55
192.168.1.57
  5060(TCP)
    Detected SIP TCP port : 5060
    UA Information NA/User-Agent: Zultys ZIP 2 3.38
192.168.1.103
  5060(UDP)
    Detected SIP UDP port : 5060
    UA Information NA/User-Agent: Asterisk PBX
192.168.1.104
  5060(UDP)
    Detected SIP UDP port : 5060
    Server: Sip EXpress router (0.9.6 (i386/linux))
```

Copyright 2004 (c) vopsecurity.org All Rights Reserved



SIPScan

Target SIP Server: 192.168.1.103

Target SIP Domain: 192.168.1.103

Transport: UDP

Port: 5060

☑ REGISTER Scan
□ OPTIONS Scan
□ INVITE Scan

Username/Extensions File: users.txt

Timeout (s): 2

```
SIPScan Results:
Scan started Mon Mar  6 01:19:10 2006
Target SIP Server: 192.168.1.103:5060 UDP
Domain: 192.168.1.103

1>>Found a live extension/user at 201@192.168.1.103 with
SIP response code(s):           REGISTER:401
2>>Found a live extension/user at 202@192.168.1.103 with
SIP response code(s):           REGISTER:401
3>>Found a live extension/user at 203@192.168.1.103 with
SIP response code(s):           REGISTER:401
4>>Found a live extension/user at 204@192.168.1.103 with
SIP response code(s):           REGISTER:401
```

□ Verbose

Done Scanning. . . Save Results under File

# Application – Fuzzing

“Fuzzing” is a term used to describe functional protocol testing

Involves sending various forms of malformed protocol requests, to test protocol processing software

Fuzzing has resulted in identification of many vulnerabilities in protocol processing software

# Application – Fuzzing

```
INVITE sip:6713@192.168.26.180:6060;user=phone SIP/2.0
Via: SIP/2.0/UDP 192.168.22.36:6060
From: UserAgent<sip:6710@192.168.22.36:6060;user=phone>
To: 6713<sip:6713@192.168.26.180:6060;user=phone>
Call-ID: 96561418925909@192.168.22.36
Cseq: 1 INVITE
Subject: VovidaINVITE
Contact: <sip:6710@192.168.22.36:6060;user=phone>
Content-Type: application/sdp
Content-Length:0
```

# Application – Fuzzing

```
INVITE sip:6713@192.168.26.180:6060;user=phone SIP/2.0
Via: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
From: UserAgent<sip:6710@192.168.22.36:6060;user=phone>
To: 6713<sip:6713@192.168.26.180:6060;user=phone>
Call-ID: 96561418925909@192.168.22.36
Cseq: 1 INVITE
Subject: VovidaINVITE
Contact: <sip:6710@192.168.22.36:6060;user=phone>
Content-Type: application/sdp
Content-Length:0
```

# Application – Fuzzing

Most vendors test their protocol implementations

Still a good idea though to test deployed system

There are freeware and commercial fuzzers available:

- www.ee.oulu.fi/research/ouspg/protos/index.html
- www.codenomicon.com

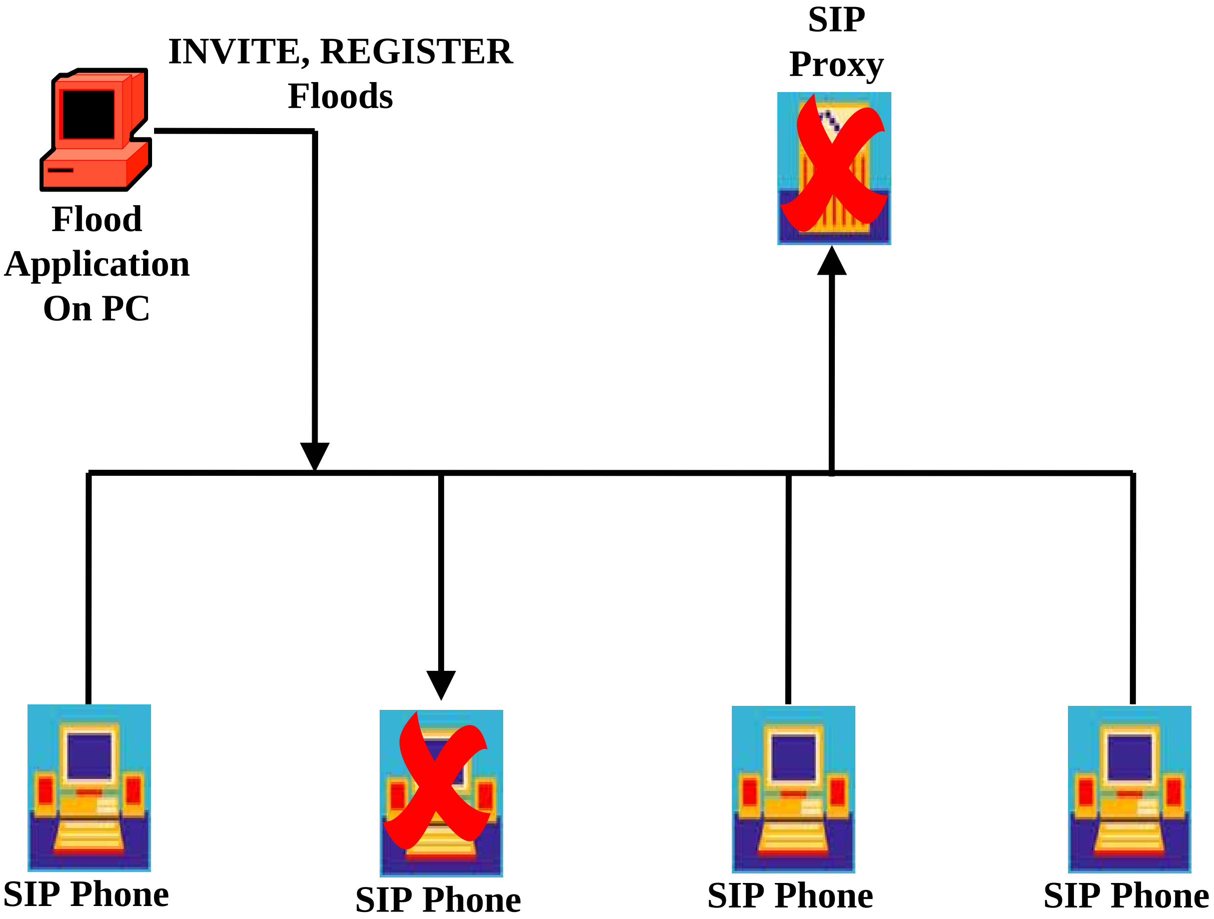
# Application – Service Disruption

There are many types of service disruptions possible

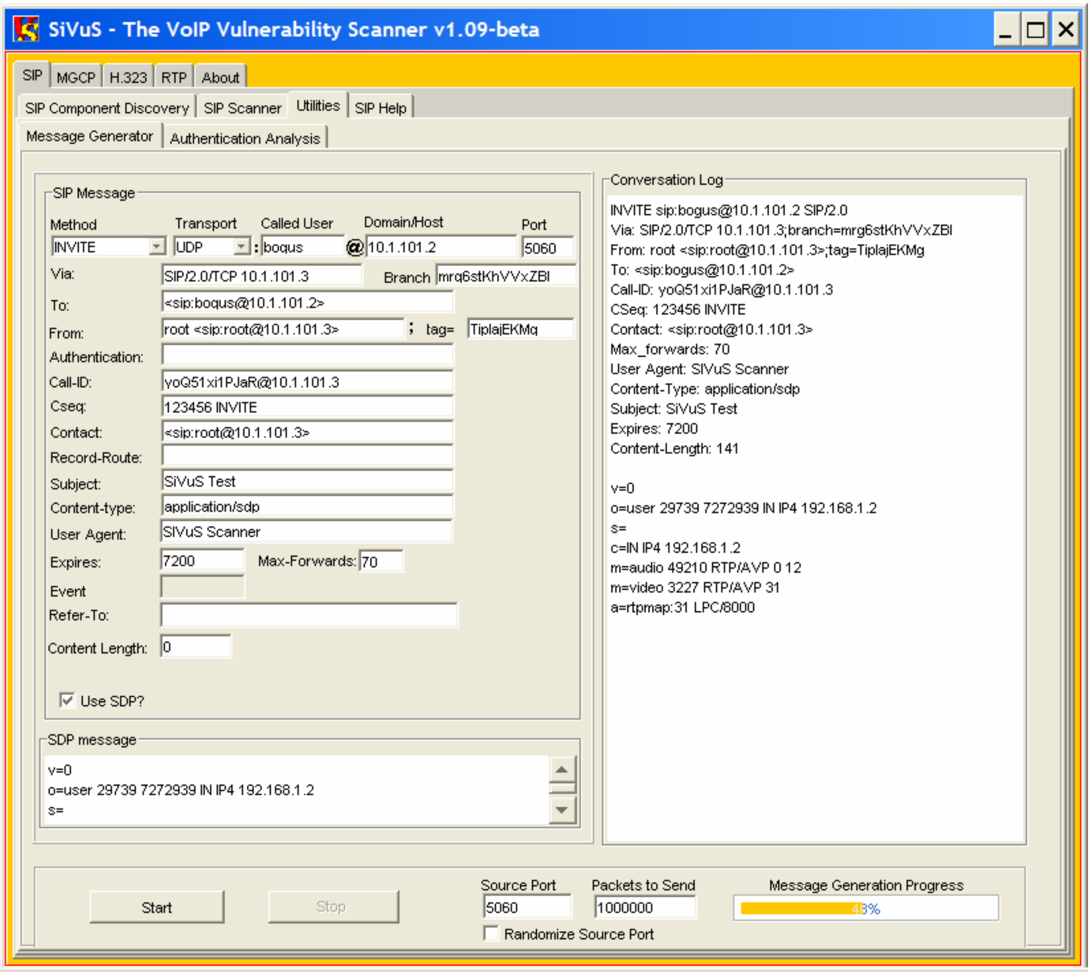
Testing for them is necessary, to determine if your system is vulnerable

The following several slides describe several types of possible attacks

# Application – Denial of Service



# Application – Denial of Service



SIP Message

| Method | Transport | Called User | Domain/Host | Port |
|---|---|---|---|---|
| INVITE | UDP | bogus | @ 10.1.101.2 | 5060 |

Via: SIP/2.0/TCP 10.1.101.3 Branch mrg6stKhVVxZBI

To: <sip:bogus@10.1.101.2>

From: root <sip:root@10.1.101.3> ; tag= TiplajEKMg

Authentication:

Call-ID: yoQ51xi1PJaR@10.1.101.3

Cseq: 123456 INVITE

Contact: <sip:root@10.1.101.3>

Record-Route:

Subject: SiVuS Test

Content-type: application/sdp

User Agent: SIVuS Scanner

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

```
INVITE sip:bogus@10.1.101.2 SIP/2.0
Via: SIP/2.0/TCP 10.1.101.3;branch=mrg6stKhVVxZBI
From: root <sip:root@10.1.101.3>;tag=TiplajEKMg
To: <sip:bogus@10.1.101.2>
Call-ID: yoQ51xi1PJaR@10.1.101.3
CSeq: 123456 INVITE
Contact: <sip:root@10.1.101.3>
Max_forwards: 70
User Agent: SIVuS Scanner
Content-Type: application/sdp
Subject: SiVuS Test
Expires: 7200
Content-Length: 141

v=0
o=user 29739 7272939 IN IP4 192.168.1.2
s=
c=IN IP4 192.168.1.2
m=audio 49210 RTP/AVP 0 12
m=video 3227 RTP/AVP 31
a=rtpmap:31 LPC/8000
```

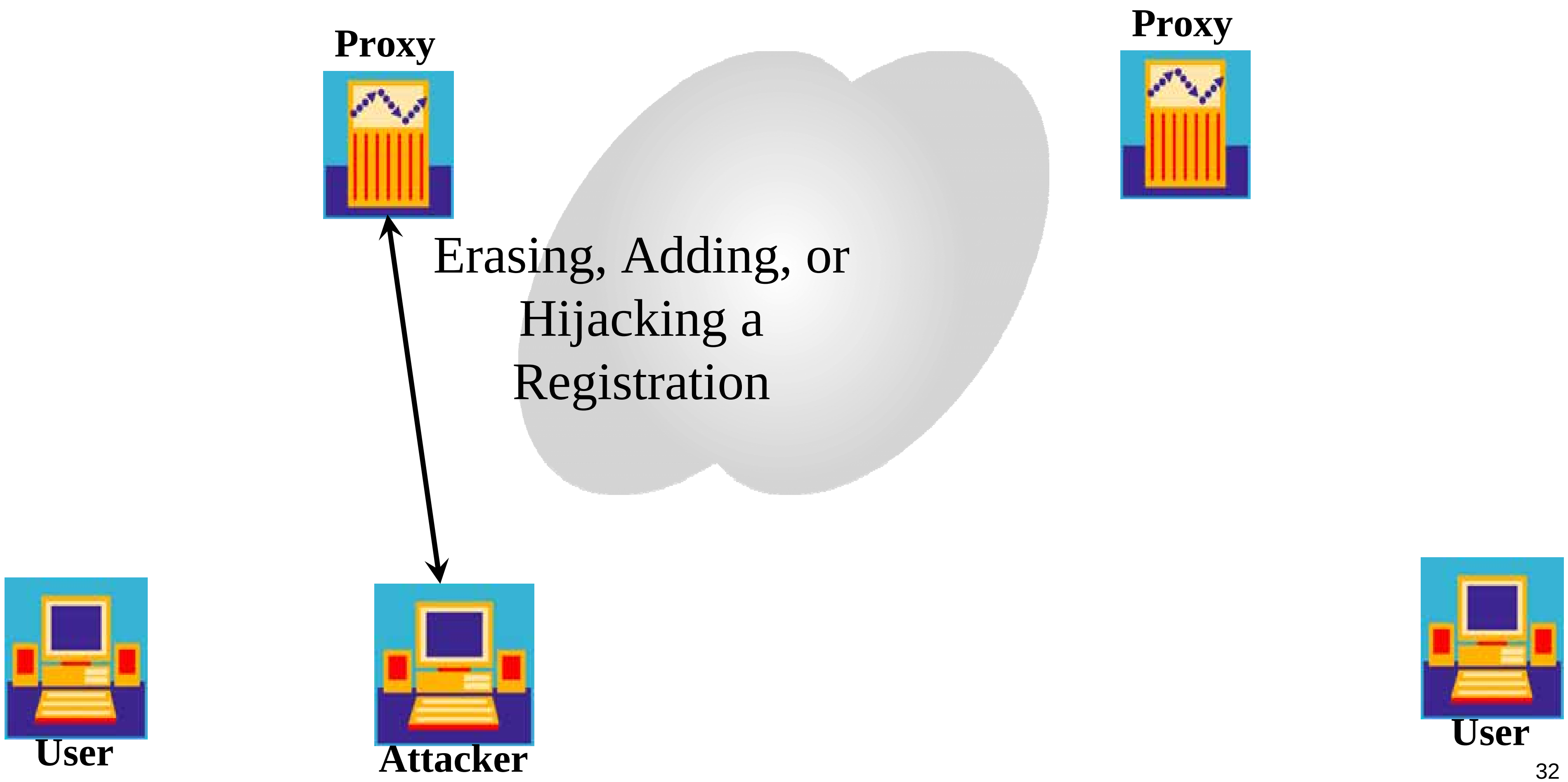
Source Port: 5060

Packets to Send: 1000000

□ Randomize Source Port

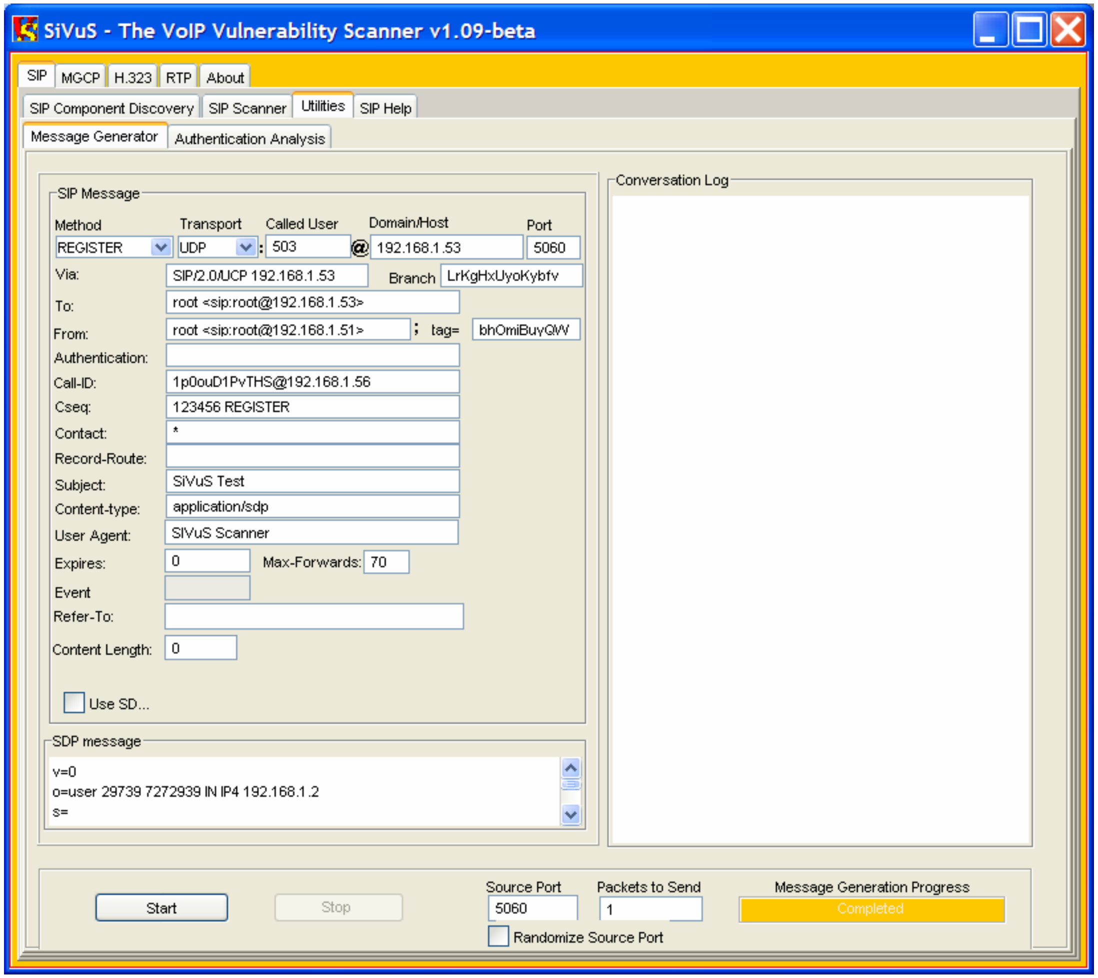
Message Generation Progress: 48%

# Application – Registration Manipulation



Erasing, Adding, or Hijacking a Registration

# Application – Registration Manipulation



SIP Message

| Method | Transport | Called User | Domain/Host | Port |
|---|---|---|---|---|
| REGISTER | UDP | : 503 | @ 192.168.1.53 | 5060 |

Via: SIP/2.0/UCP 192.168.1.53 Branch LrKgHxUyoKybfv

To: root <sip:root@192.168.1.53>

From: root <sip:root@192.168.1.51> ; tag= bhOmiBuyQW

Authentication:

Call-ID: 1p0ouD1PvTHS@192.168.1.56

Cseq: 123456 REGISTER

Contact: *

Record-Route:

Subject: SiVuS Test

Content-type: application/sdp

User Agent: SIVuS Scanner

Expires: 0 Max-Forwards: 70

Event

Refer-To:

Content Length: 0

□ Use SD...

SDP message

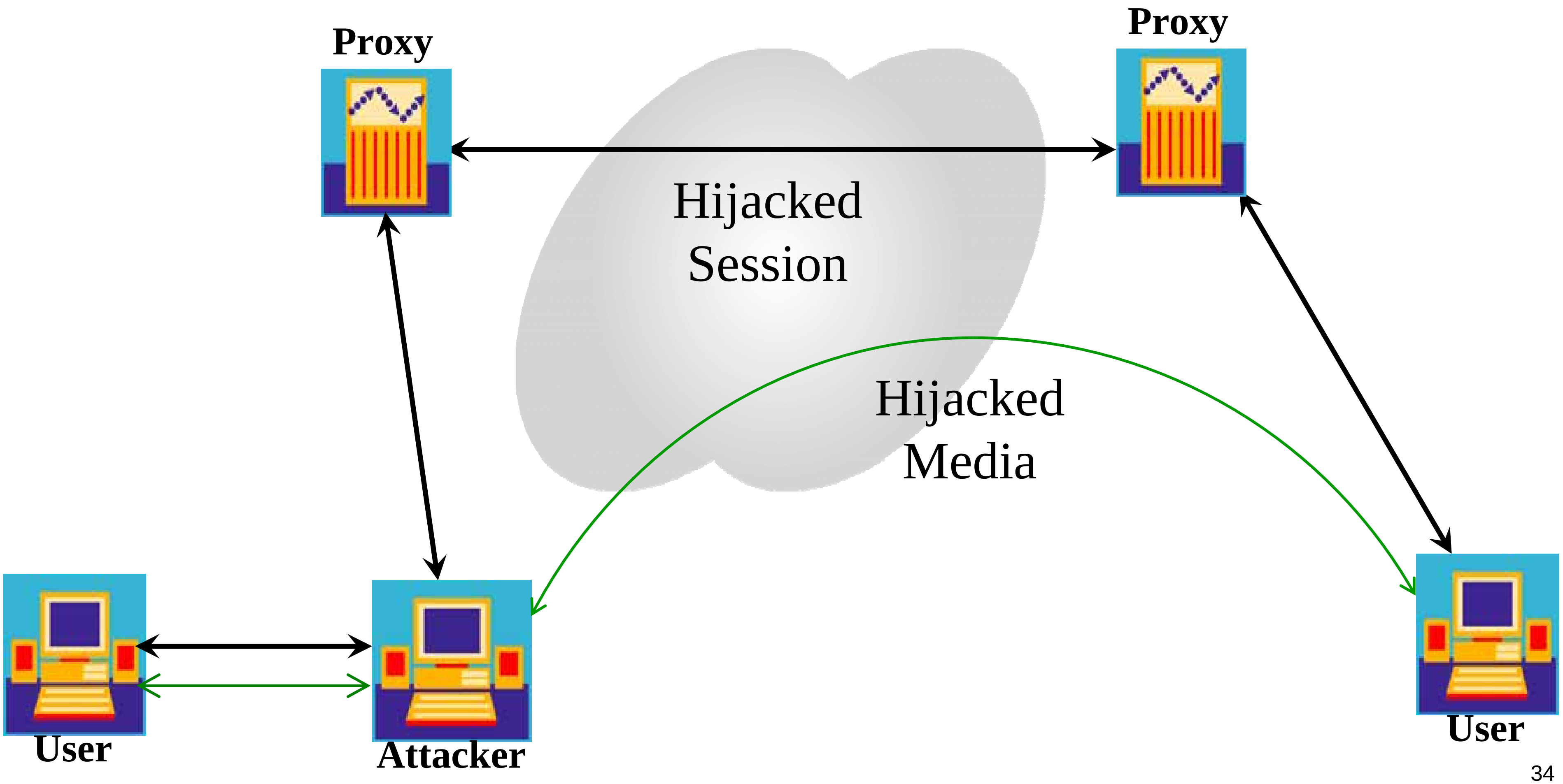
```
v=0
o=user 29739 7272939 IN IP4 192.168.1.2
s=
```

Source Port: 5060

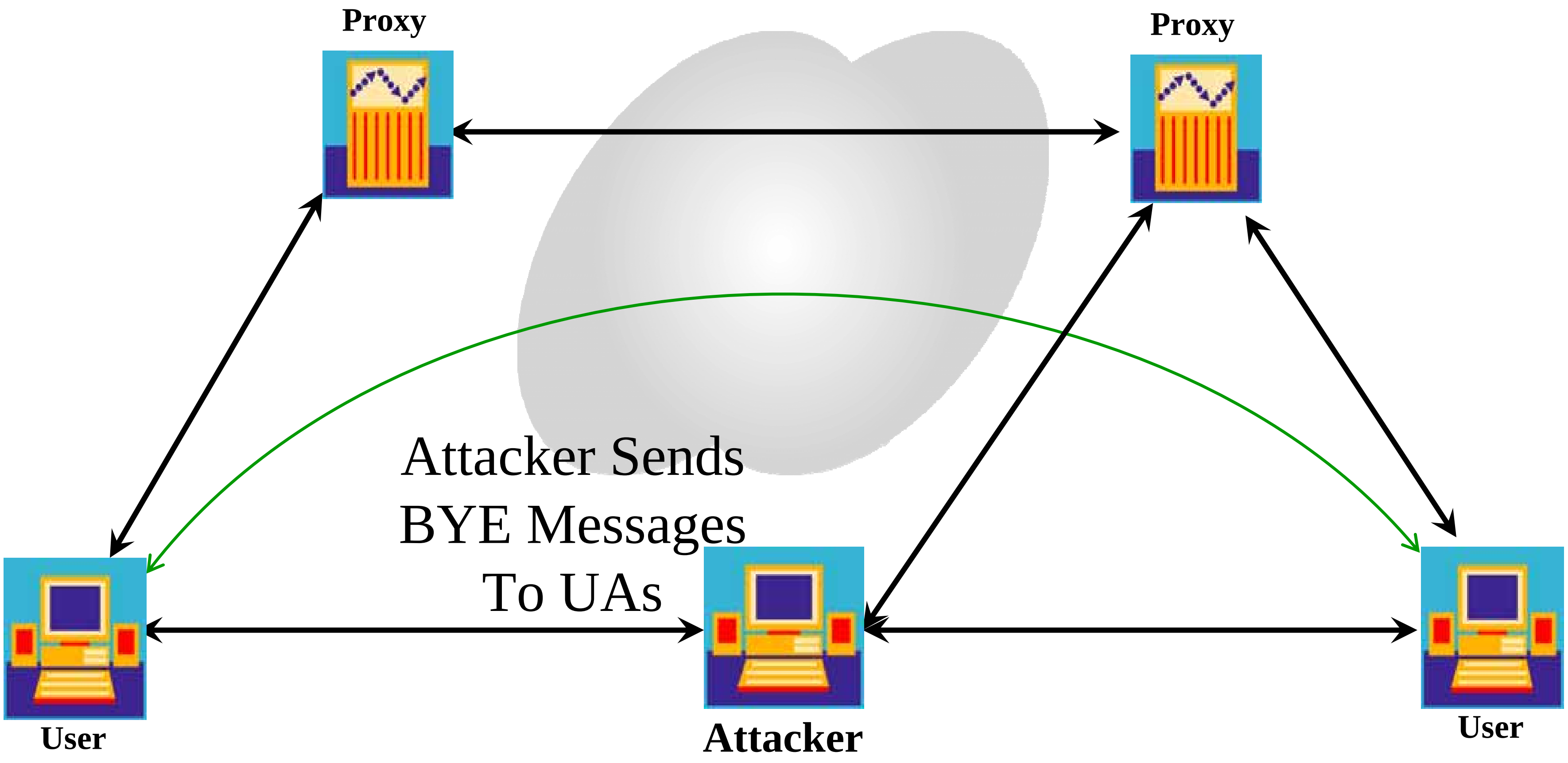
Packets to Send: 1

□ Randomize Source Port

# Application – Registration Hijacking

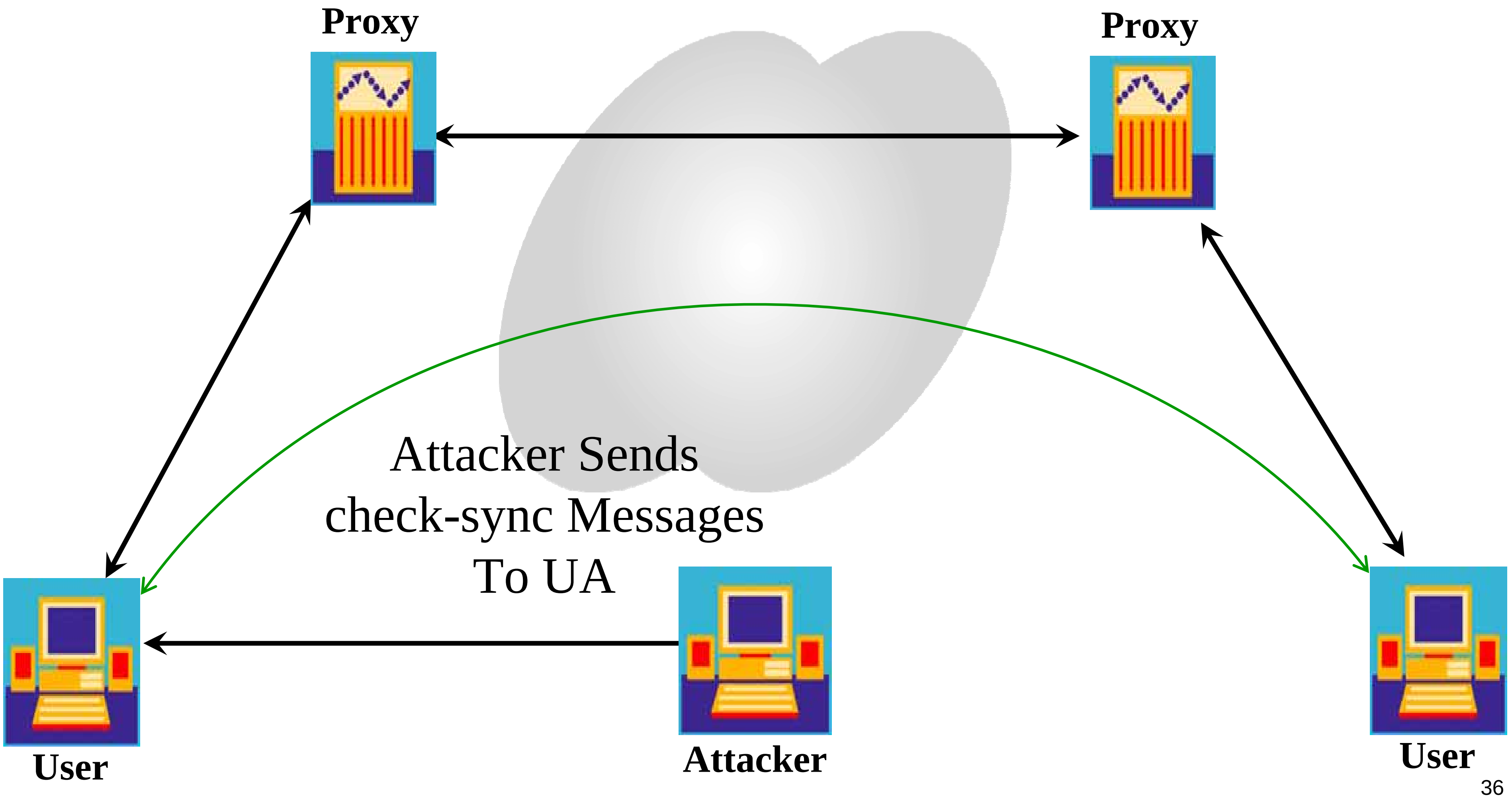


# Application – Session Teardown



Attacker Sends
BYE Messages
To UAs

# Application – Check Sync Reboot



Proxy

Proxy

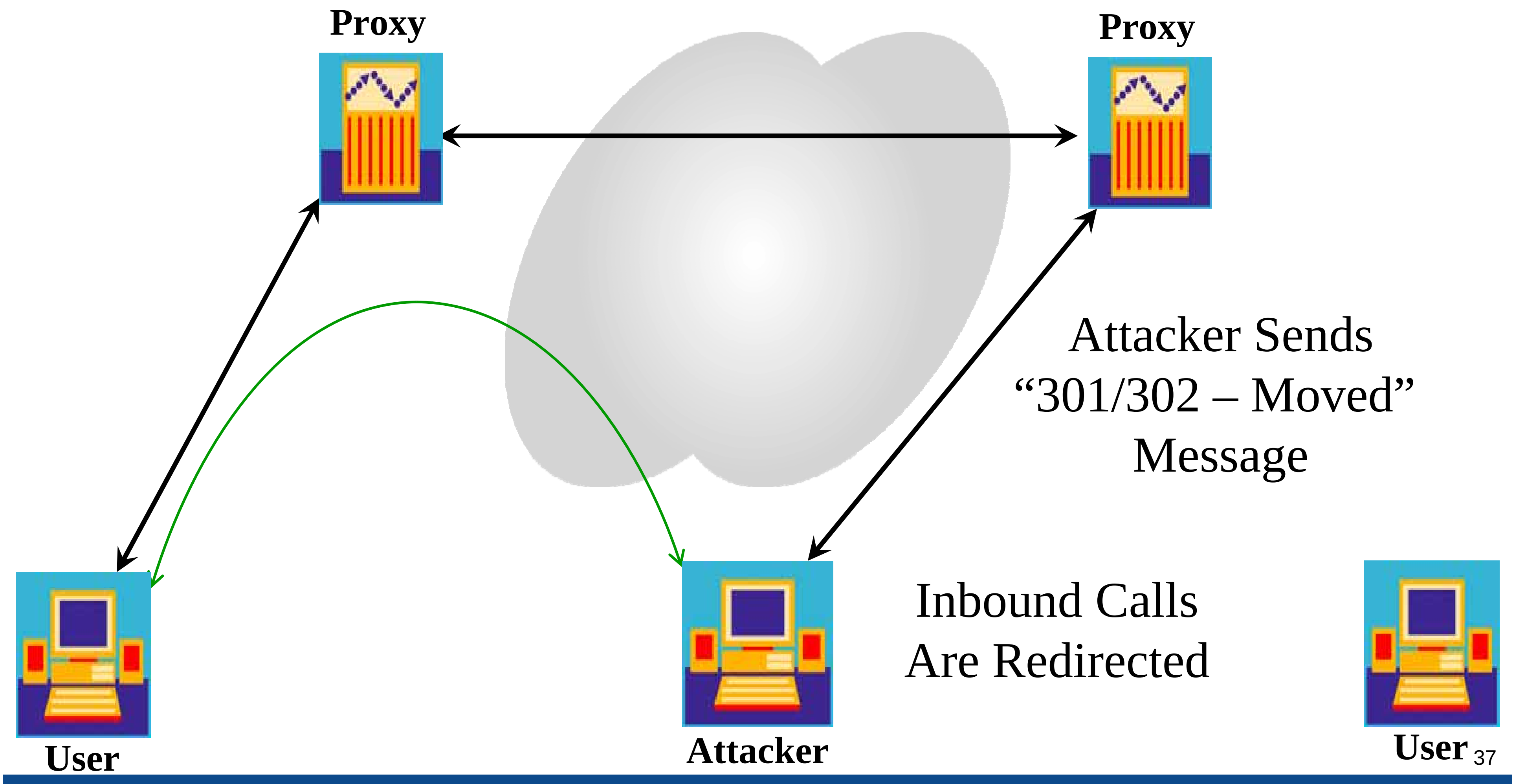
Attacker Sends
check-sync Messages
To UA

User

Attacker

User

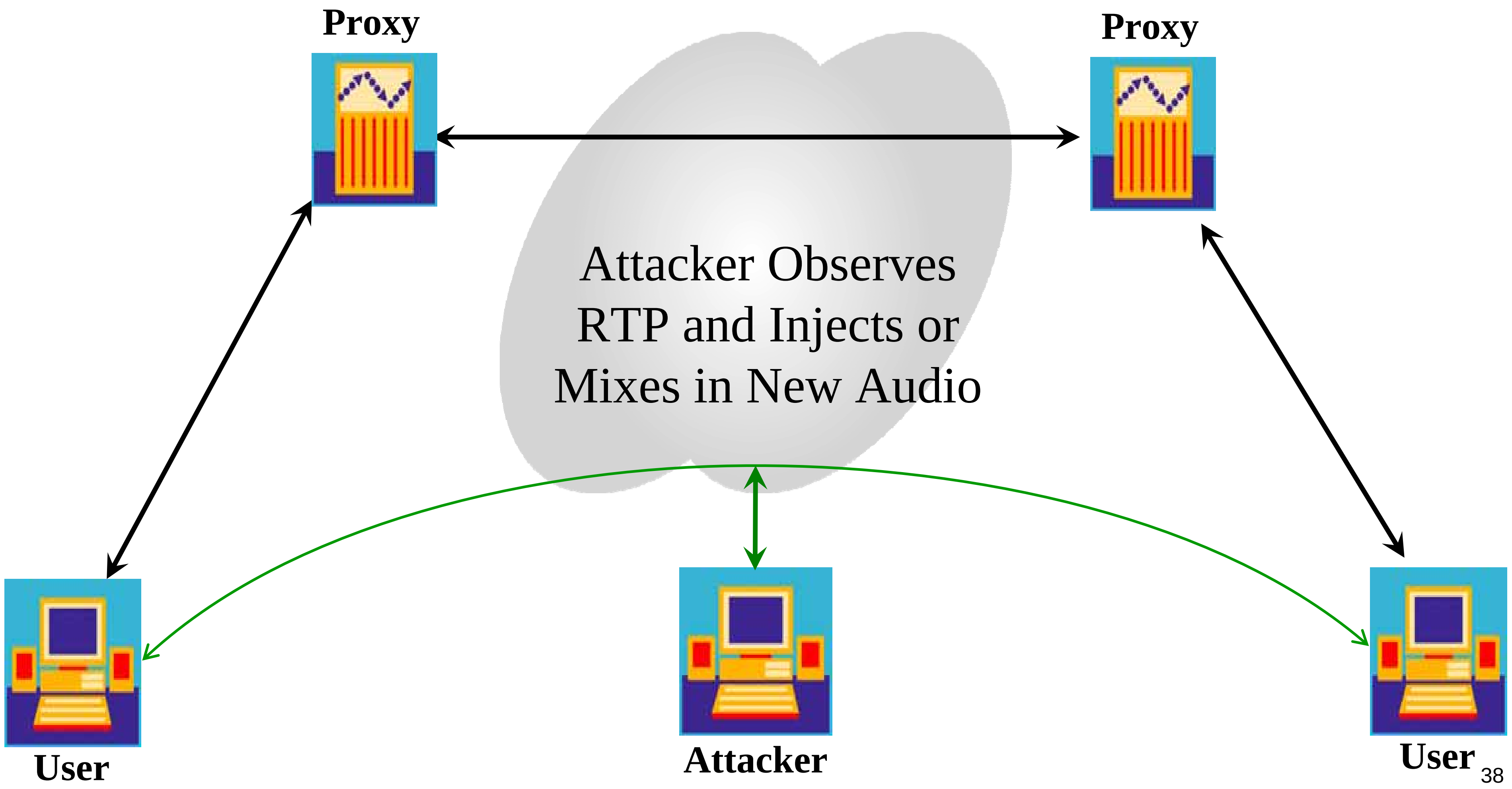
# Application – Redirection



Attacker Sends "301/302 – Moved" Message

Inbound Calls Are Redirected

# Application – RTP Injection/Mixing



Proxy

Proxy

Attacker Observes RTP and Injects or Mixes in New Audio

User

Attacker

User

# Other Attack Tools

dirscan – active directory scanning

authtool – cracks digest authentication passwords

invite_flood – generates a flood of INVITE requests

register_flood – generates a flood of REGISTER requests

udpflood/rtpflood – generates a flood of UDP or RTP packets

erase_registrations – removes a registration

add_registrations – adds one or more bogus registrations

reghijacker – hijacks a registration (with authentication)

teardown – tears down a call

check_sync_reboot – reboots a phone

rtpinjector – injects/mixes audio

sip_rogue – application level MITM tool

more on the way...

# Application – Recommendations

Use application firewalls to monitor signaling and media for attacks

Use authentication to prevent rogue devices from injecting packets

Use encryption prevent signaling and media eavesdropping

# Links

SIP attack tools – www.hackingvoip.com

ethereal – www.ethereal.com

wireshark – www.wireshark.com

SiVuS – www.vopsecurity.org

Cain and Abel - http://www.oxid.it/cain.html

Fuzzing - http://www.ee.oulu.fi/research/ouspg/protos/index.html

Codenomicon – www.codenomicon.com

Asterisk – www.asterisk.org

Trixbox – www.trixbox.org

## Key Points to Take Home

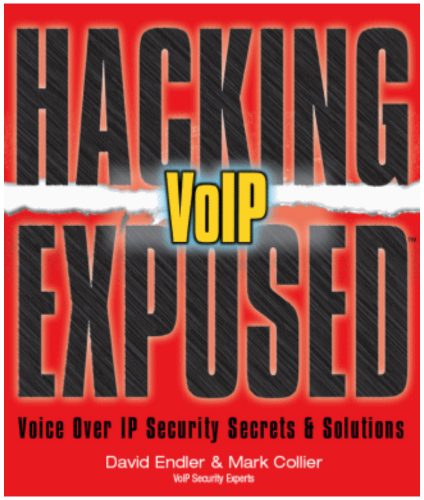
In order to secure your VoIP network, you must understand the issues

You need to actively test your network, to find out if vulnerabilities exist

There are many tools available to enable this

It is a good idea to enlist the help of a trusted third party to perform or assist with the testing

# QUESTIONS?


HACKING
VoIP
EXPOSED
Voice Over IP Security Secrets & Solutions
David Endler & Mark Collier
VoIP Security Experts

**Contact:**
Mark D. Collier
mark.collier@securelogix.com
www.securelogix.com
(210) 863-9001

SecureLogix® Corporation