

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

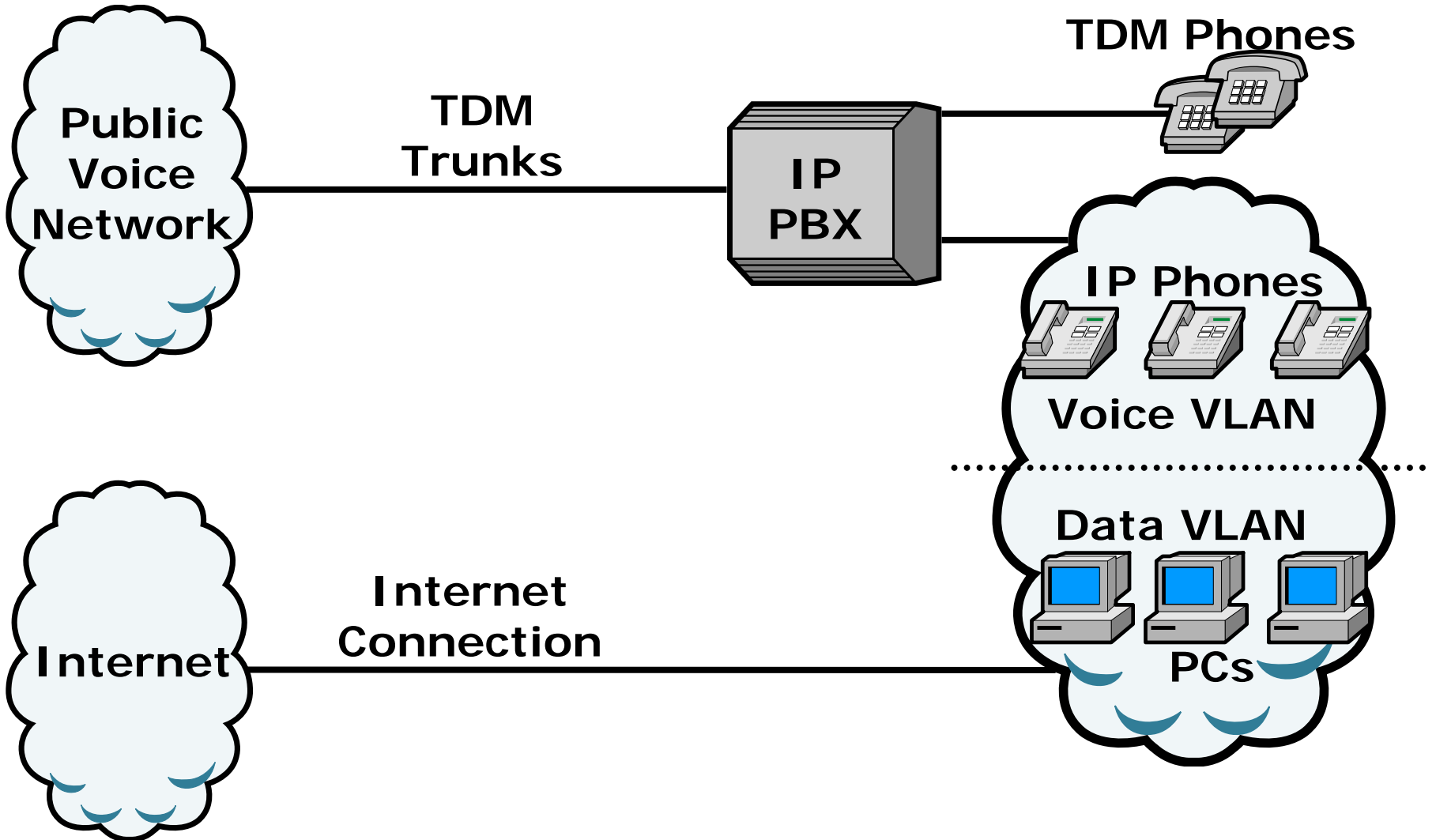
Ground rules:

- ◆ 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

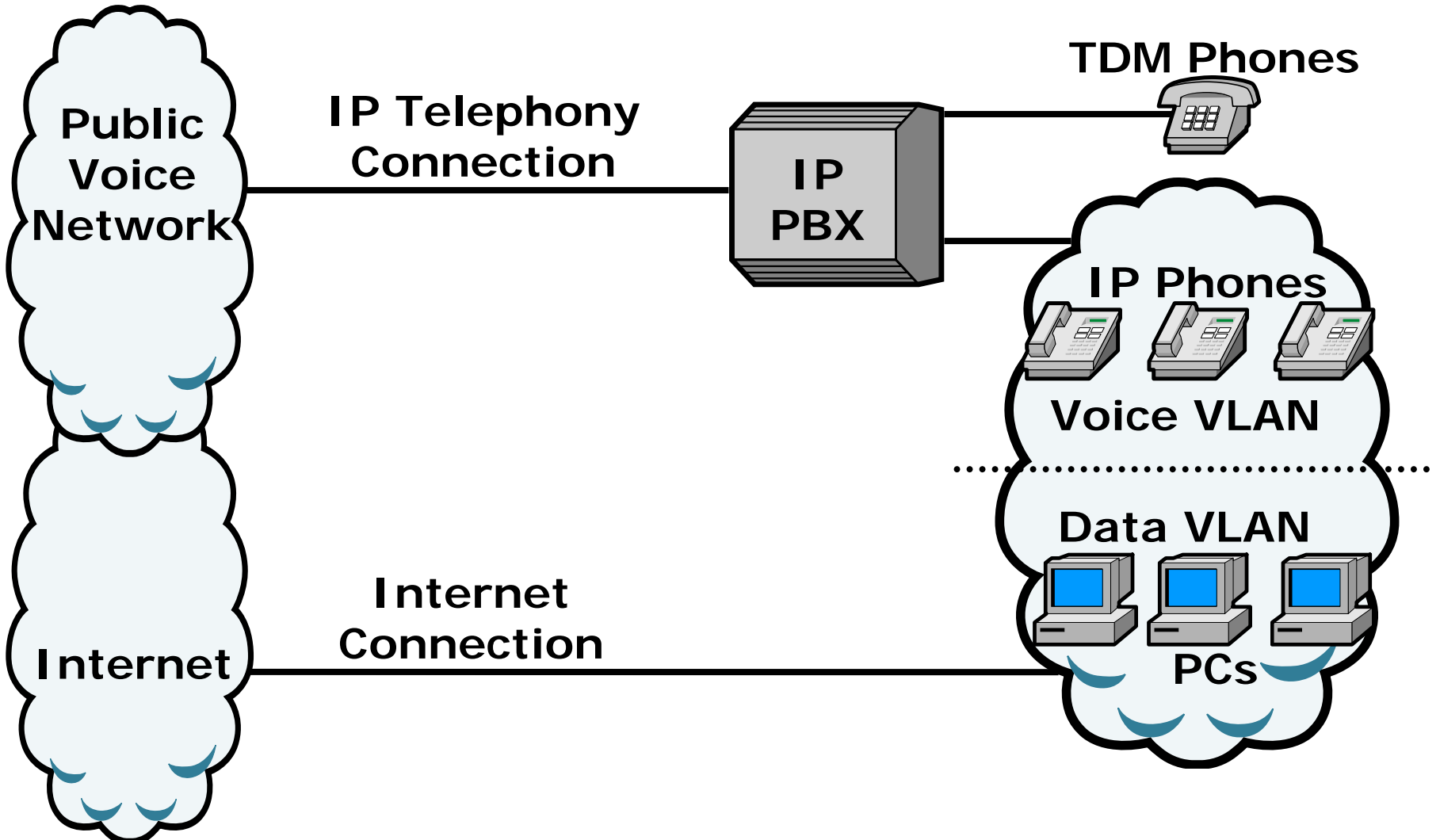
Scope:

- ◆ 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

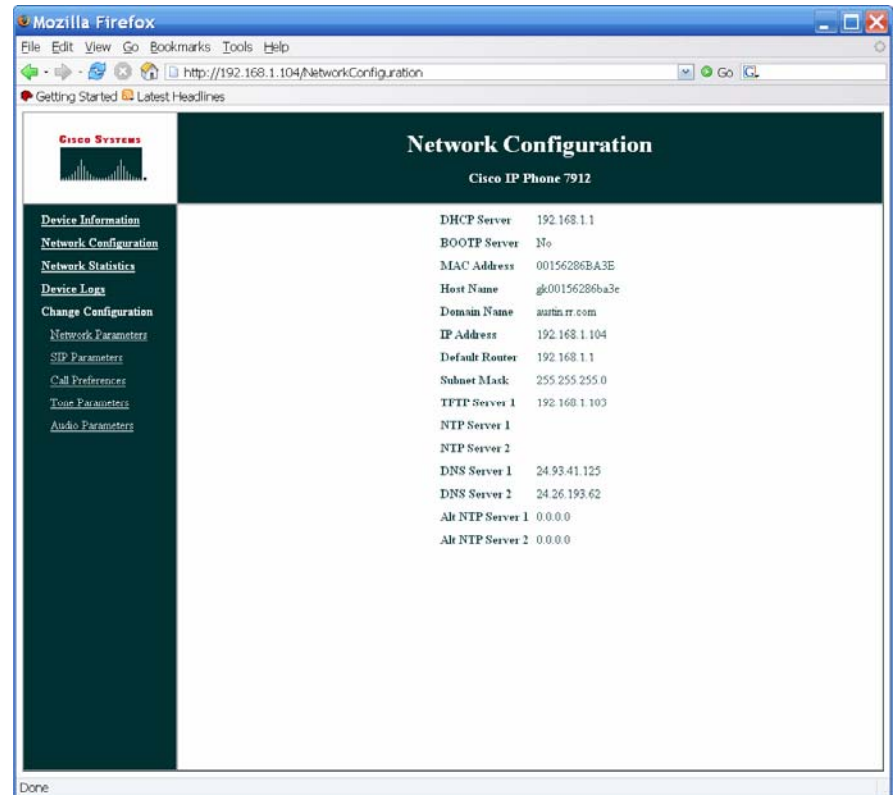
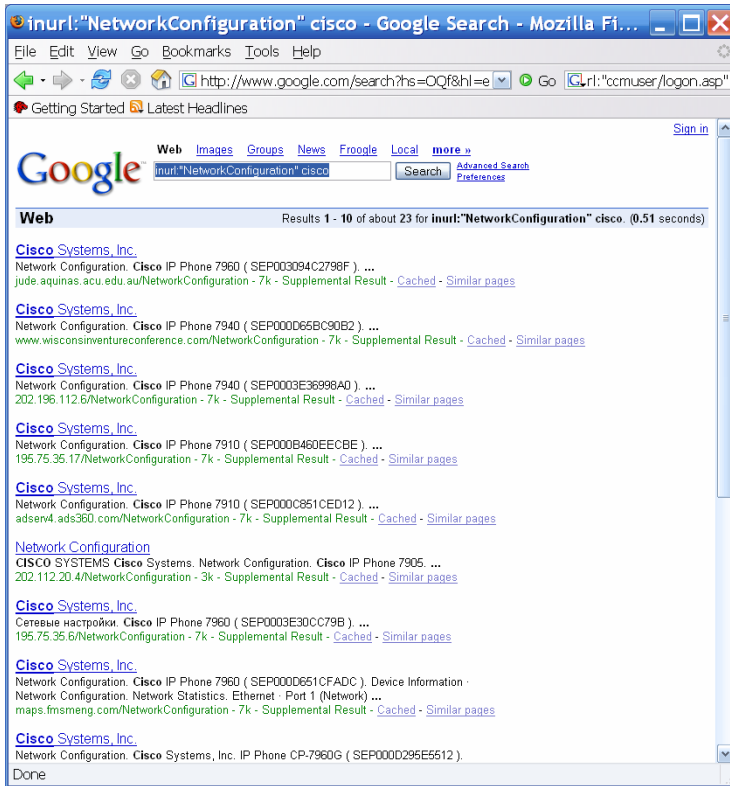
Search enterprise web site:

- ◆ 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



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

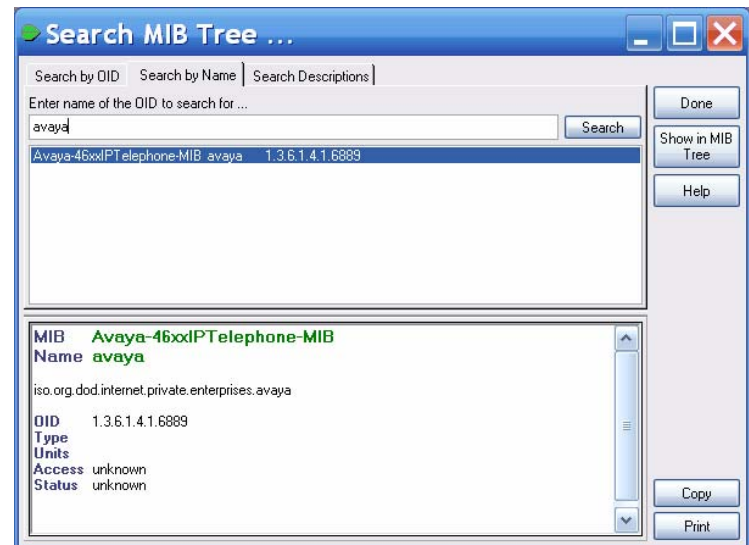
Test for default or weak passwords

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**



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

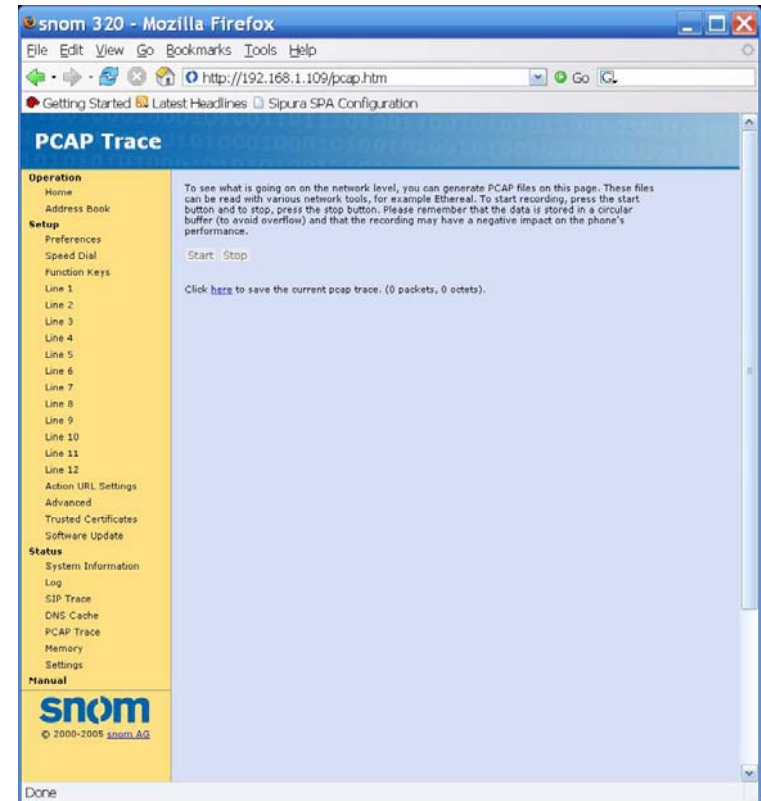
Test for default or weak passwords

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



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

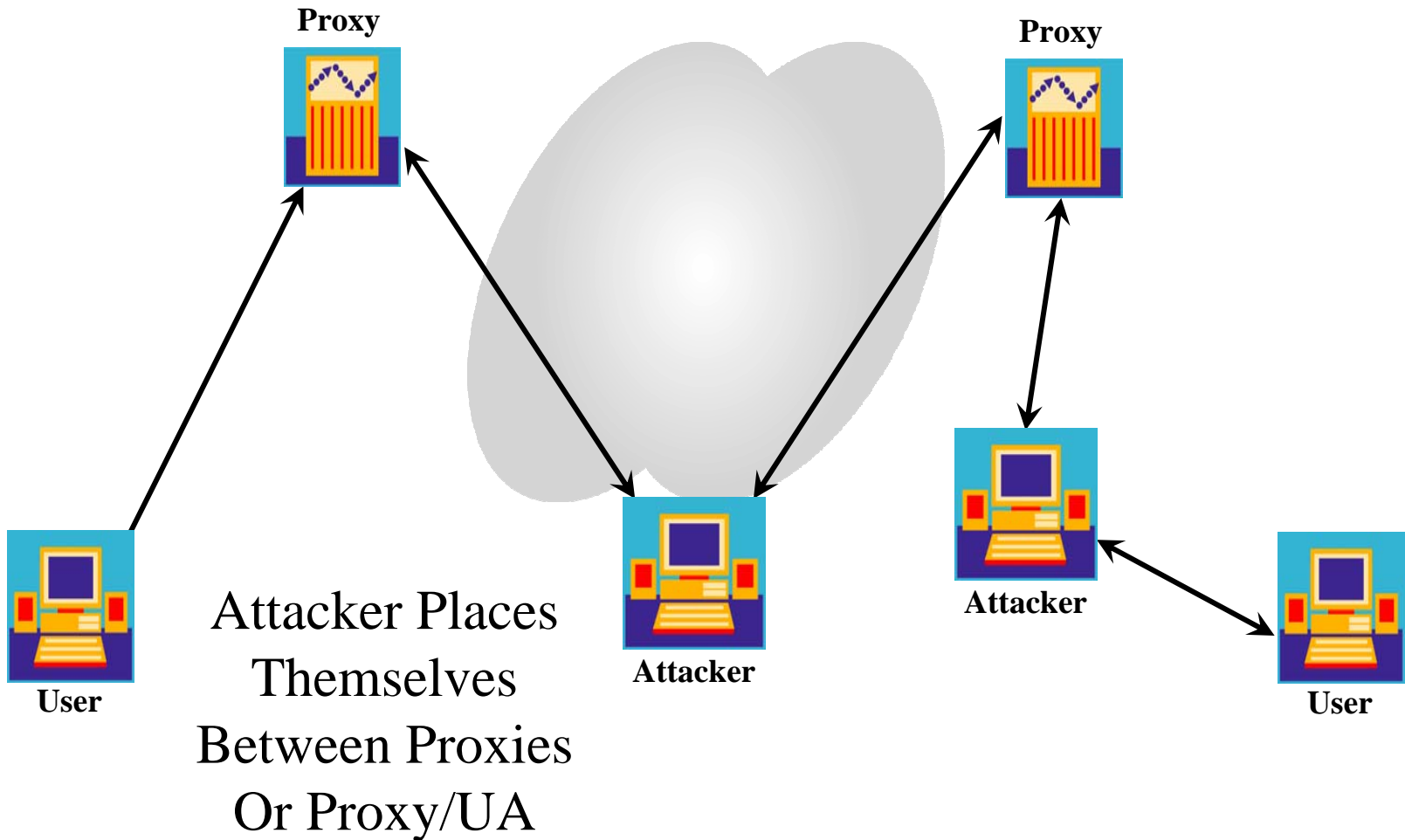
No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.1.101.65	10.1.101.1	SIP/SDP	Request: INVITE sip:7000@10.1.101.1;user=phone, with session description
2	0.001008	10.1.101.1	10.1.101.65	SIP	Status: 100 Trying
3	0.002304	10.1.101.1	10.1.101.65	SIP	Status: 180 Ringing
4	1.792547	10.1.101.1	10.1.101.65	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: B2B1B3B9C3DB55423A3737393E4D74D5C6BEBCC0CADBFC...

0000 00 0a 41 6b 83 eb 00 0b 82 00 be 00 08 00 45 c0 ...Ak....E.
 0010 00 e8 9f 36 00 00 fa 11 41 e5 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 0;.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... ..[O
 0060 4e 40 4c 4d 4d 4c 70 50 4e 4b 43 43 4e ff c6 AK... ..[O

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

Network – Man-in-the-middle



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

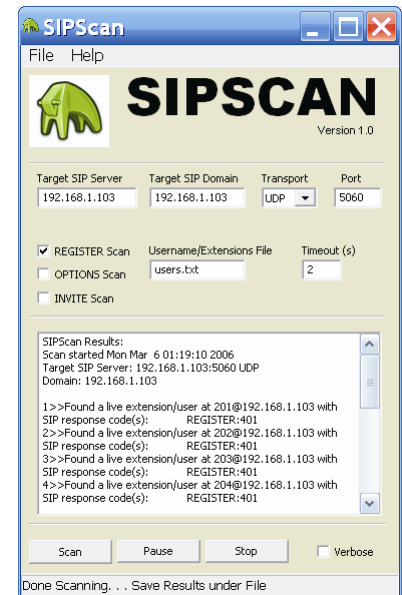
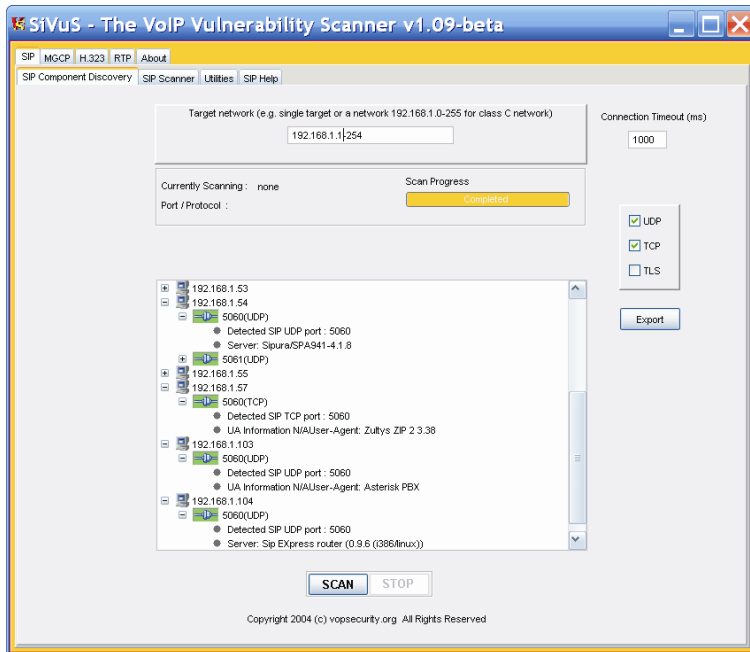
This will be especially true when IP Telephony is exchanged with a public network

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:



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: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
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

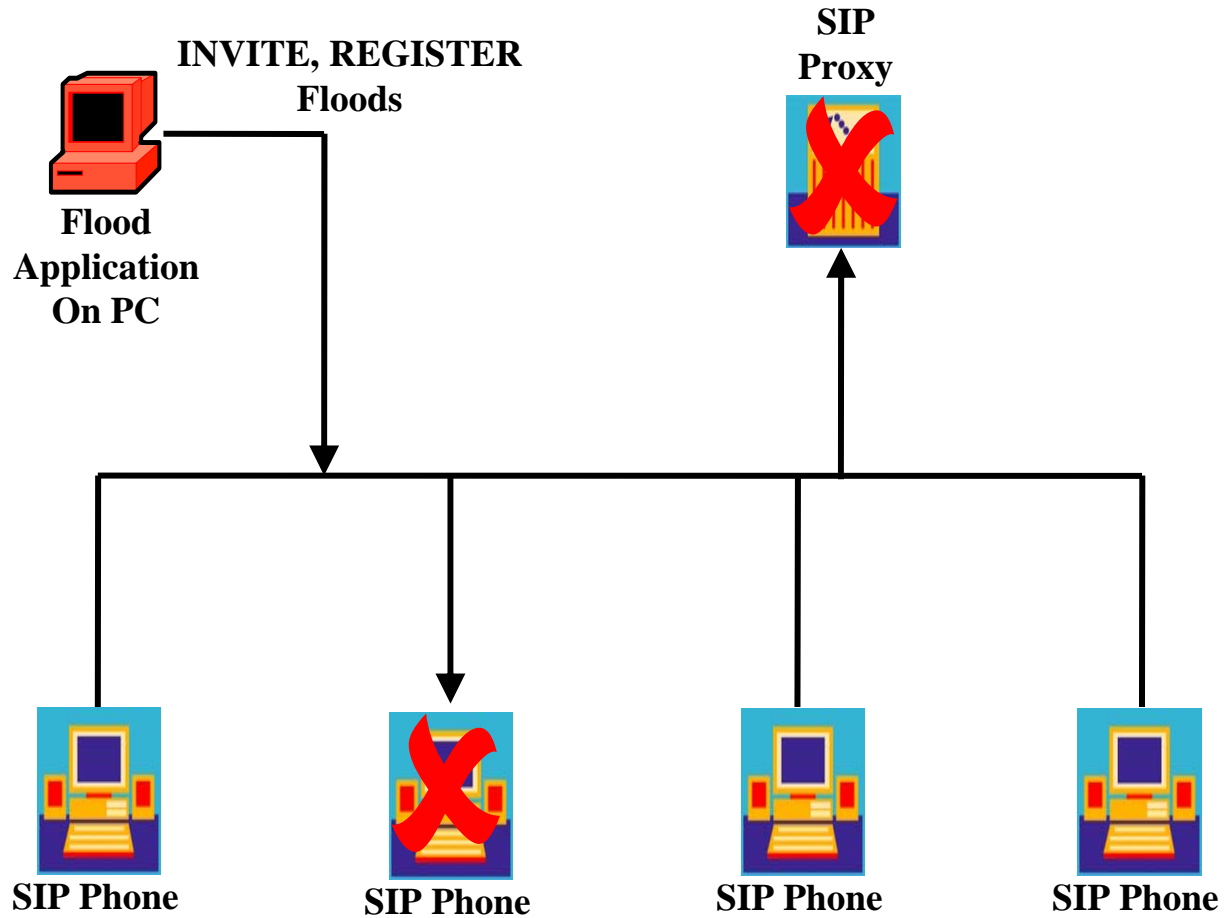
Application – Service Disruption

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

The screenshot displays the SiVuS - The VoIP Vulnerability Scanner v1.09-beta application window. The interface includes a menu bar with options like SIP, MGCP, H.323, RTP, and About. Below the menu is a toolbar with buttons for SIP Component Discovery, SIP Scanner, Utilities, and SIP Help. The main area is divided into several sections:

- SIP Message:** A form for configuring SIP message details. Fields include Method (INVITE), Transport (UDP), Called User (boqus), Domain/Host (10.1.101.2), Port (5060), Via (SIP/2.0/TCP 10.1.101.3), To (<sip:boqus@10.1.101.2>), From (root <sip:root@10.1.101.3>), Call-ID (yoQ51x1PJaR@10.1.101.3), Cseq (123456 INVITE), Contact (<sip:root@10.1.101.3>), Subject (SIVuS Test), Content-type (application/sdp), User Agent (SIVuS Scanner), Expires (7200), and Max-Forwards (70). A checkbox for "Use SDP?" is checked.
- SDP message:** A text area containing SDP content: v=0, o=user 29739 7272939 IN IP4 192.168.1.2, s=.
- Conversation Log:** A text area showing a log of the SIP message: 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=TiplajEKMa, To: <sip:bogus@10.1.101.2>, Call-ID: yoQ51x1PJaR@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.

At the bottom of the window, there are controls for starting and stopping the scan, along with a progress bar. The "Source Port" is set to 5060, "Packets to Send" is 1000000, and the "Message Generation Progress" is at 43%. A checkbox for "Randomize Source Port" is present and unchecked.

Application – Registration Manipulation



Erasing, Adding, or
Hijacking a
Registration

Proxy

Proxy



Attacker

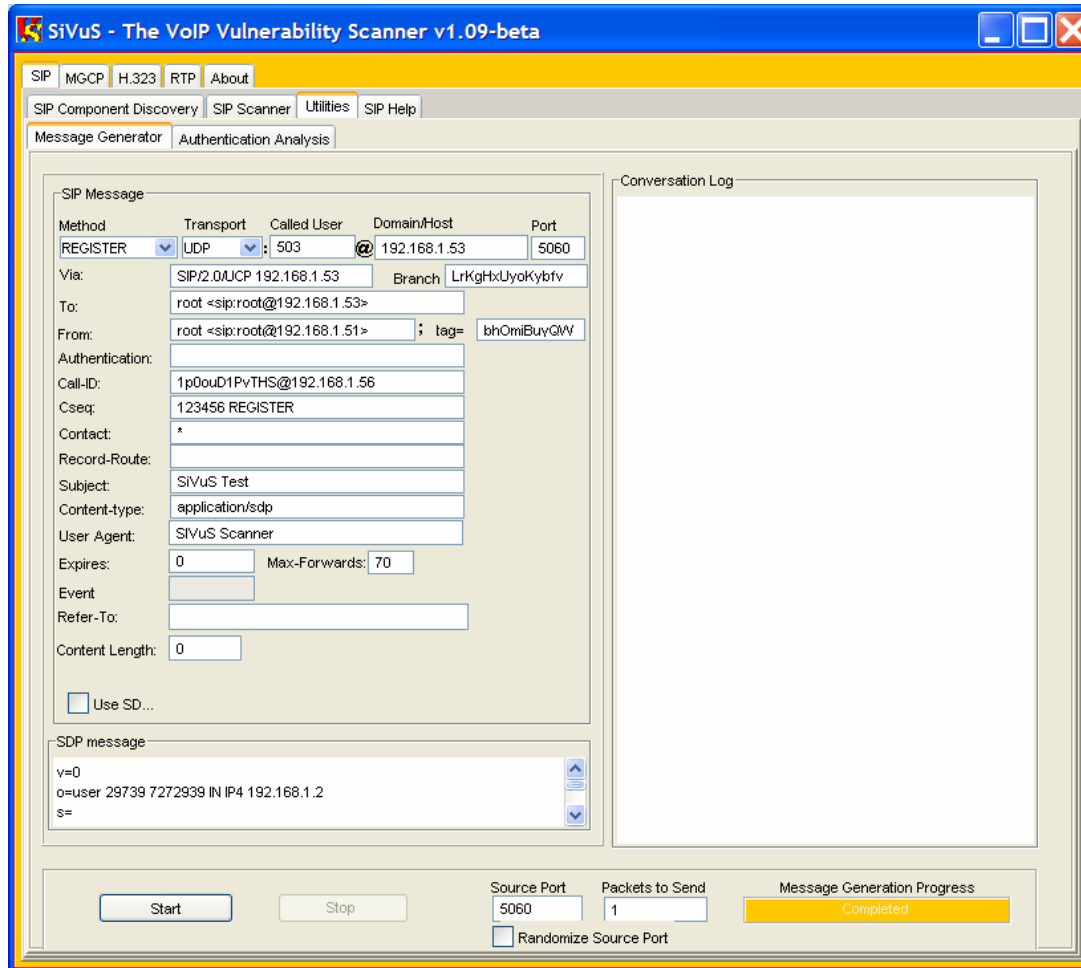


User

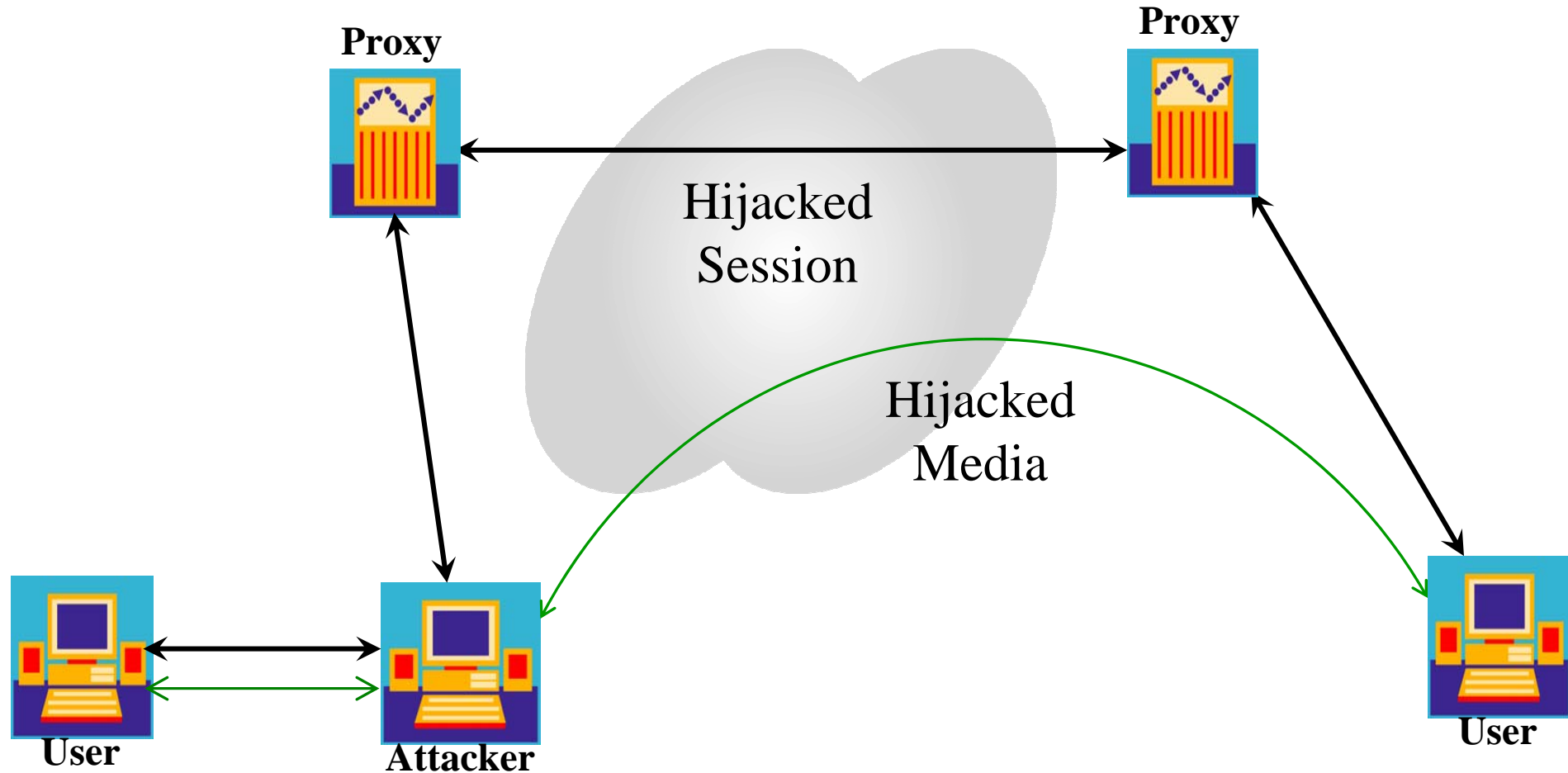


User

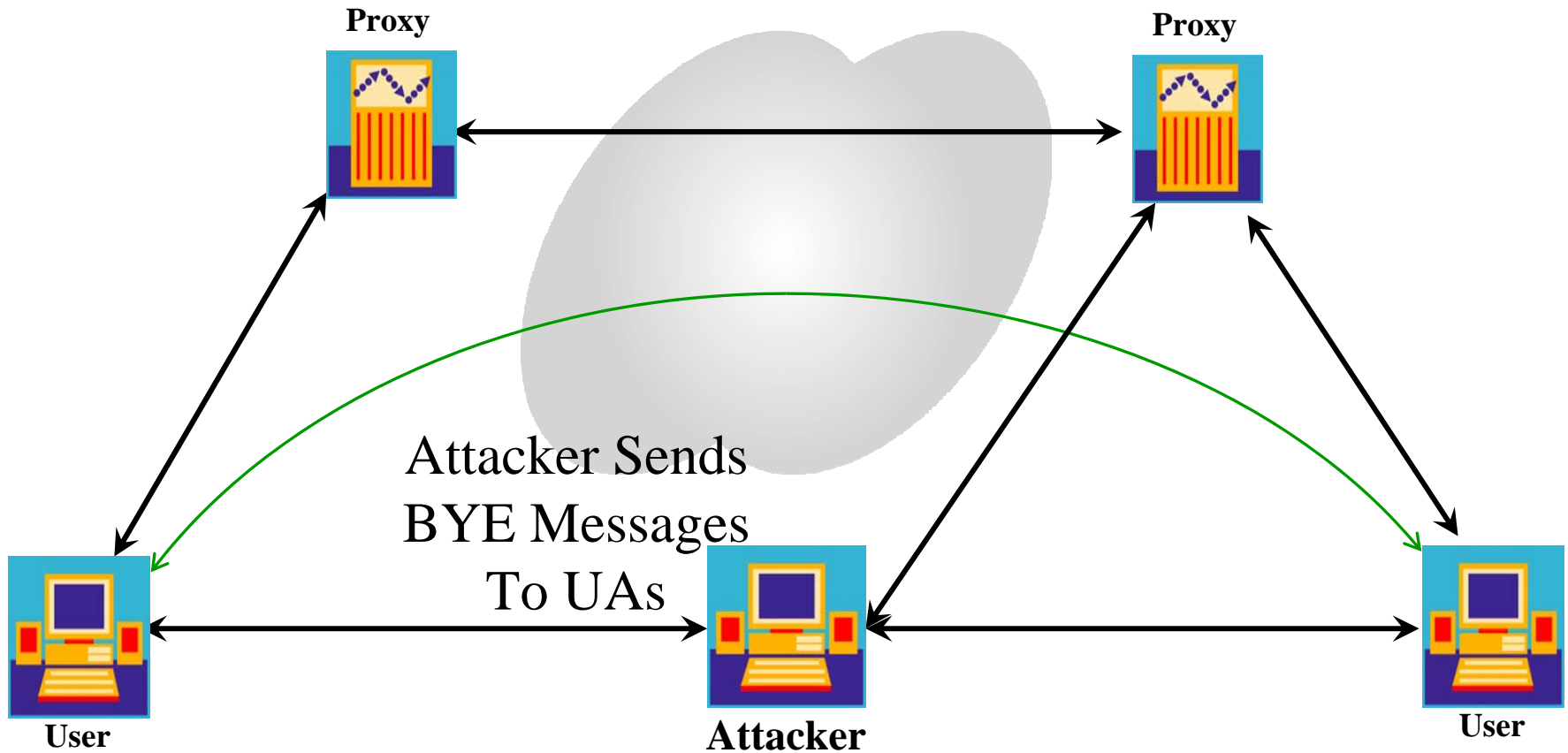
Application – Registration Manipulation



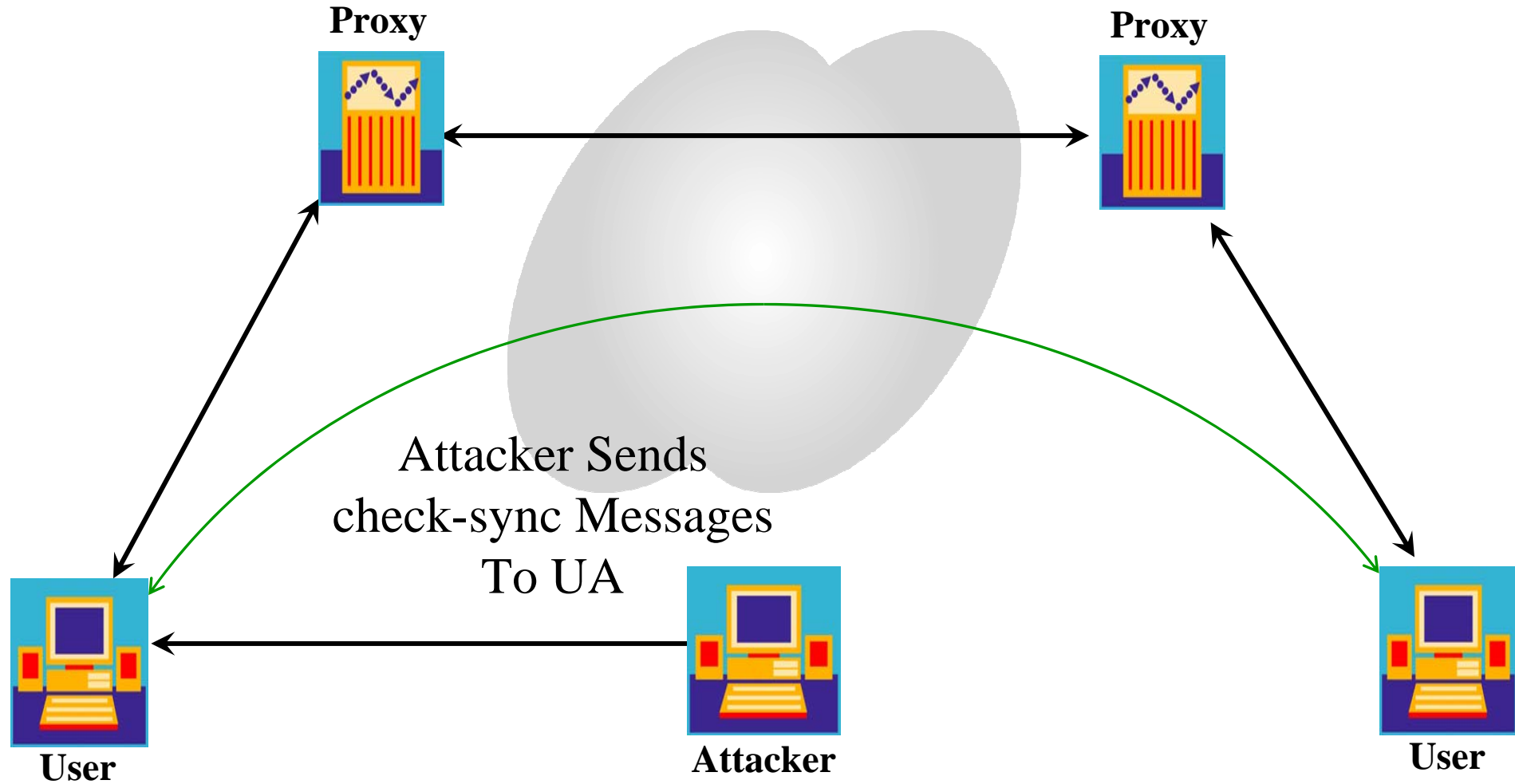
Application – Registration Hijacking



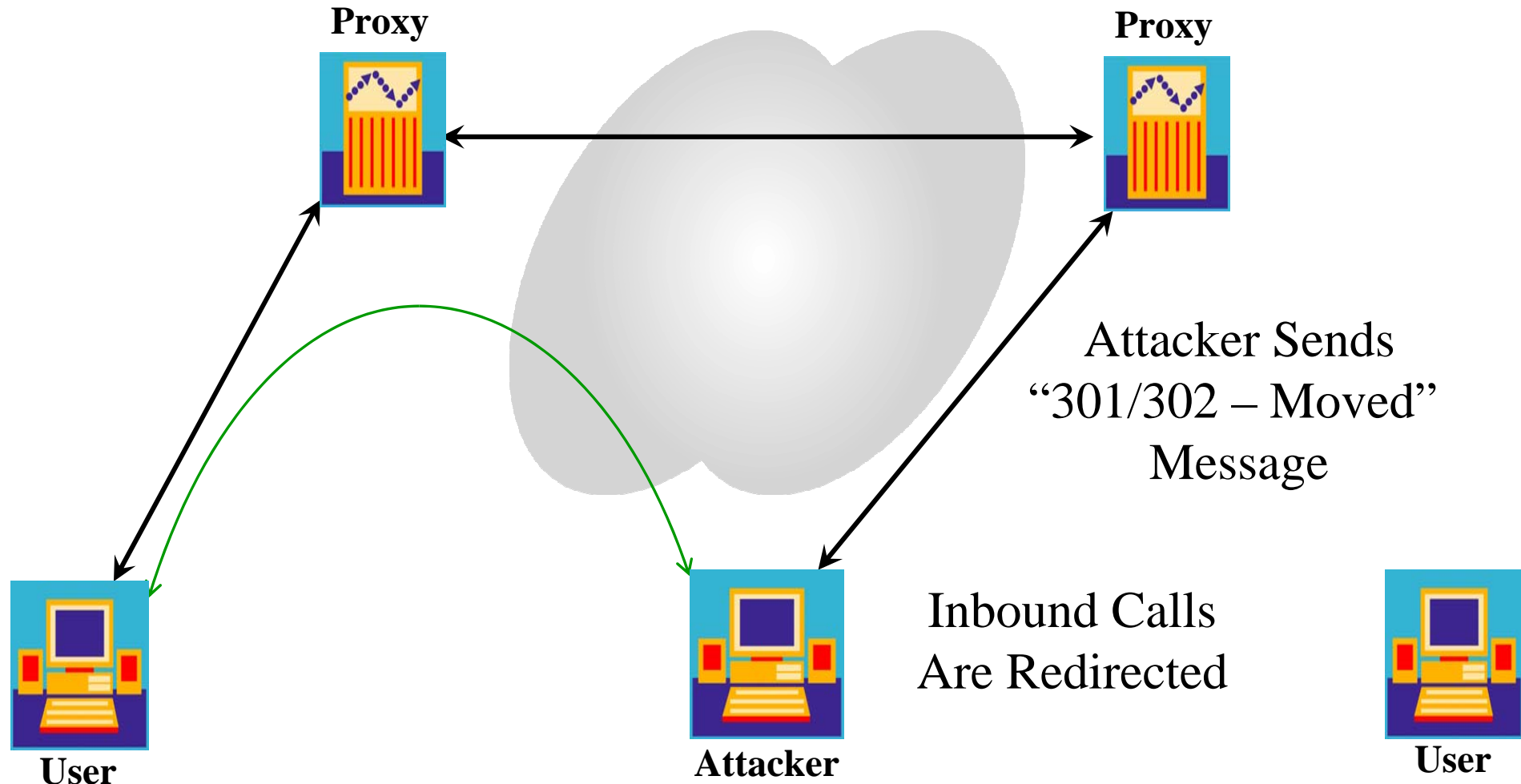
Application – Session Teardown



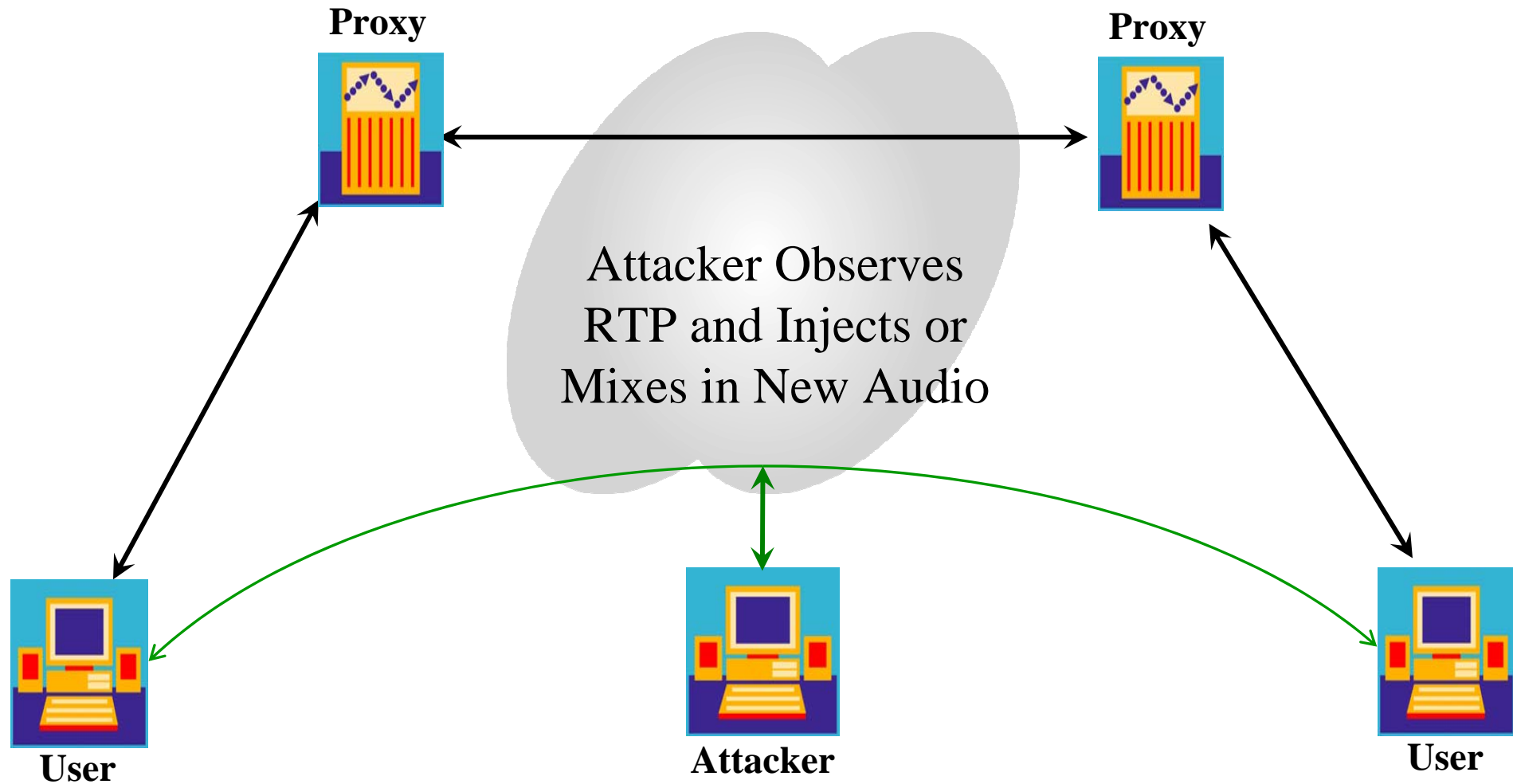
Application – Check Sync Reboot



Application – Redirection



Application – RTP Injection/Mixing



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

IPCOMM2006

September 25-27 • Gaylord Opryland • Nashville, TN

QUESTIONS?

Contact:

Mark D. Collier

mark.collier@securelogix.com

www.securelogix.com

(210) 863-9001

