

# Conducting an IP Telephony Security Assessment

Mark D. Collier  
Chief Technology Officer  
[mark.collier@securelogix.com](mailto:mark.collier@securelogix.com)



**SECURELOGIX**®  
C O R P O R A T I O N

[www.securelogix.com](http://www.securelogix.com)

# Presentation Outline

Ground rules and scope

Discovery

Security policy review and physical security checks

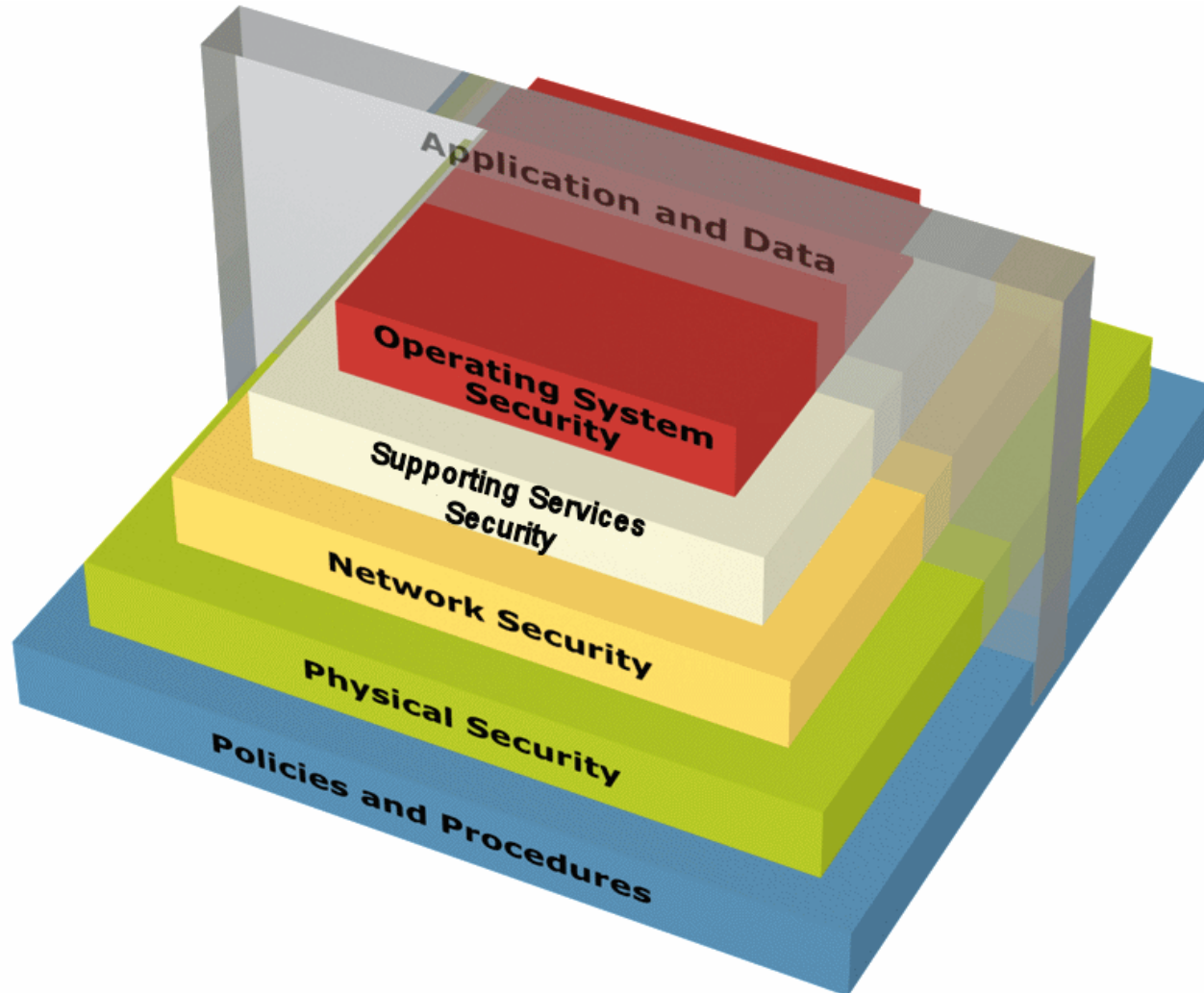
Platform tests

Network tests

Application tests

# Layers of Security

Essential to test at all layers



## Ground rules:

- ◆ Internal and/or external
- ◆ 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
- ◆ What tests should be avoided for which components

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

Search enterprise web site:

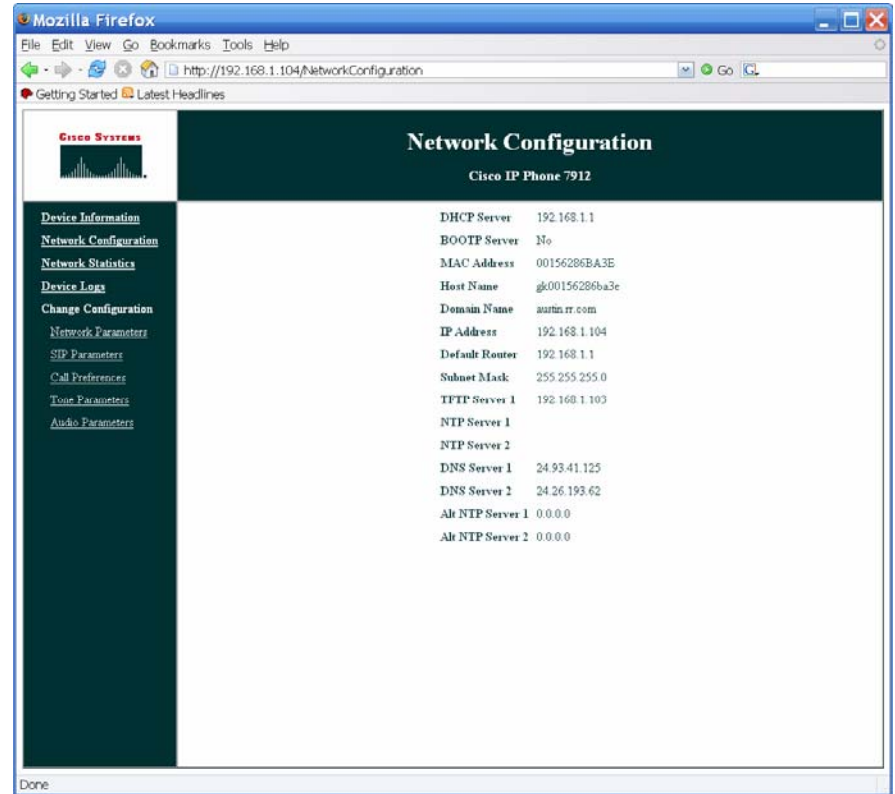
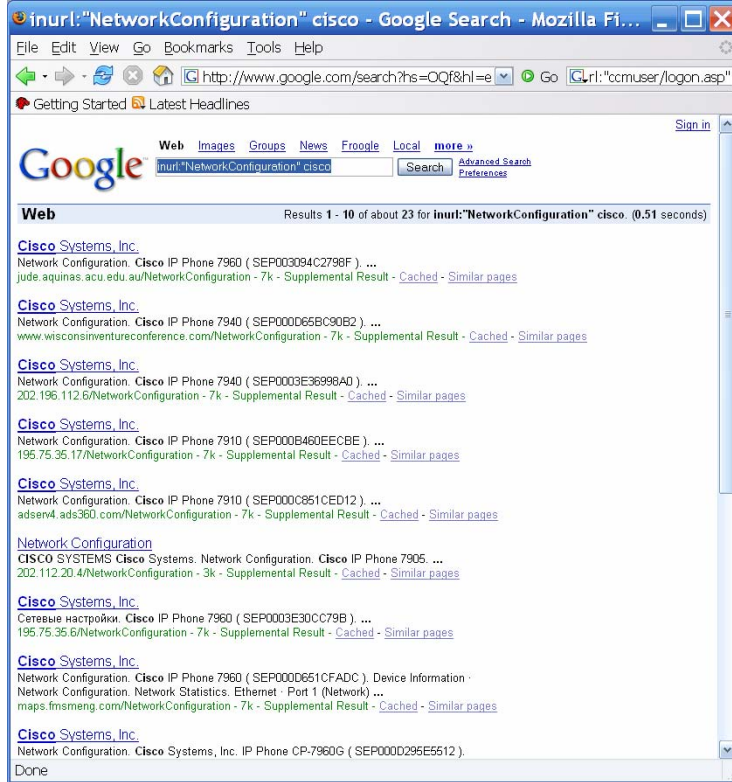
- ◆ Job listings
- ◆ Names, extensions, organization structure
- ◆ Voice mail greetings

Use Google to search for:

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

Use WHOIS and DNS to find IP addresses

# Discovery - Footprinting



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

Involves testing of IP-PBX and adjunct systems

Test for open or unnecessary network ports:

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

Test operating systems for known vulnerabilities:

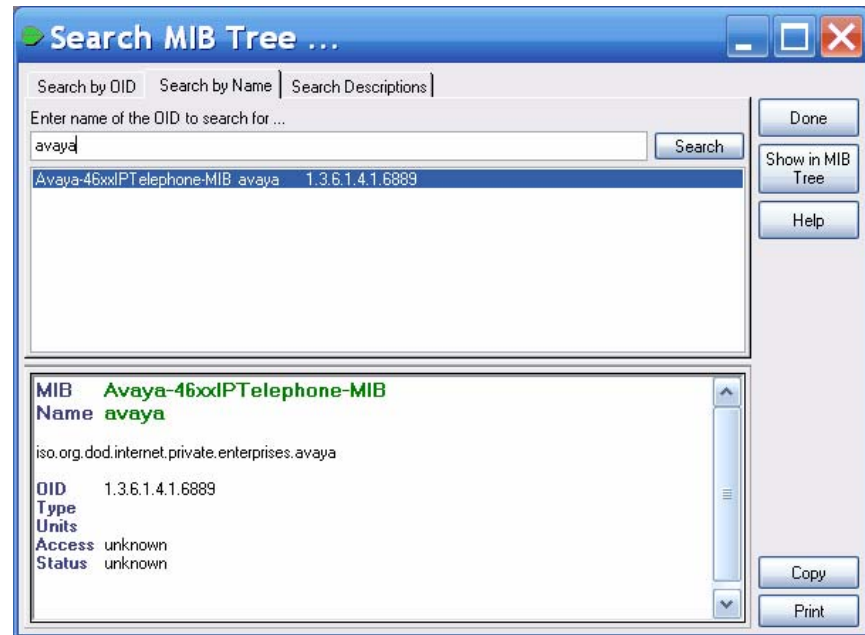
- ◆ Use general vulnerability scanners
- ◆ Use IP Telephony-specific scanners where possible

Test for default or weak passwords

Test for default configuration weaknesses

## 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**



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 name of the file and download it
- ◆ Configuration files have usernames, passwords, etc.
- ◆ It may also be possible to corrupt a software image

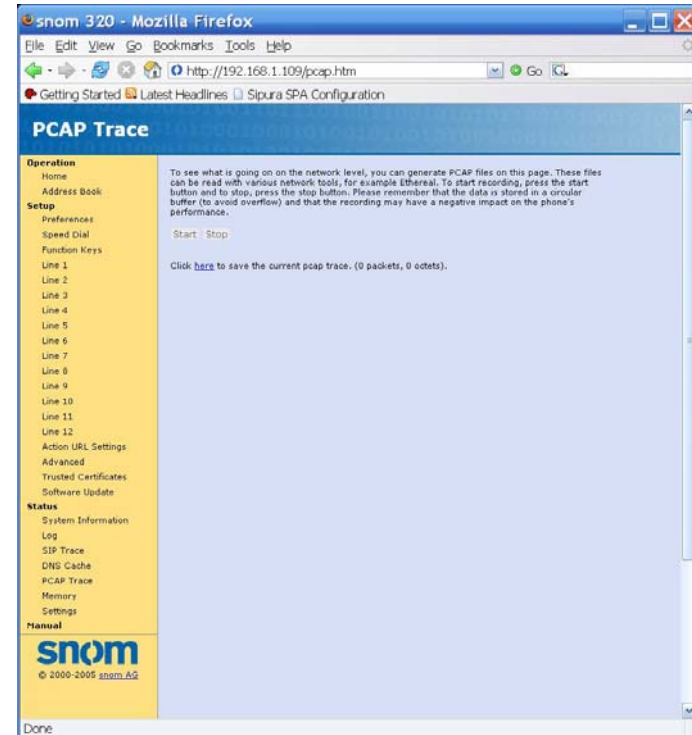
Test for open or unnecessary network ports:

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

Test for default or weak passwords

Test for weak local protections

- ◆ Check for admin access during boot
- ◆ Some IP phones have sniffers



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

## Test for network DoS vulnerabilities:

- ◆ UDP floods
- ◆ TCP SYN floods

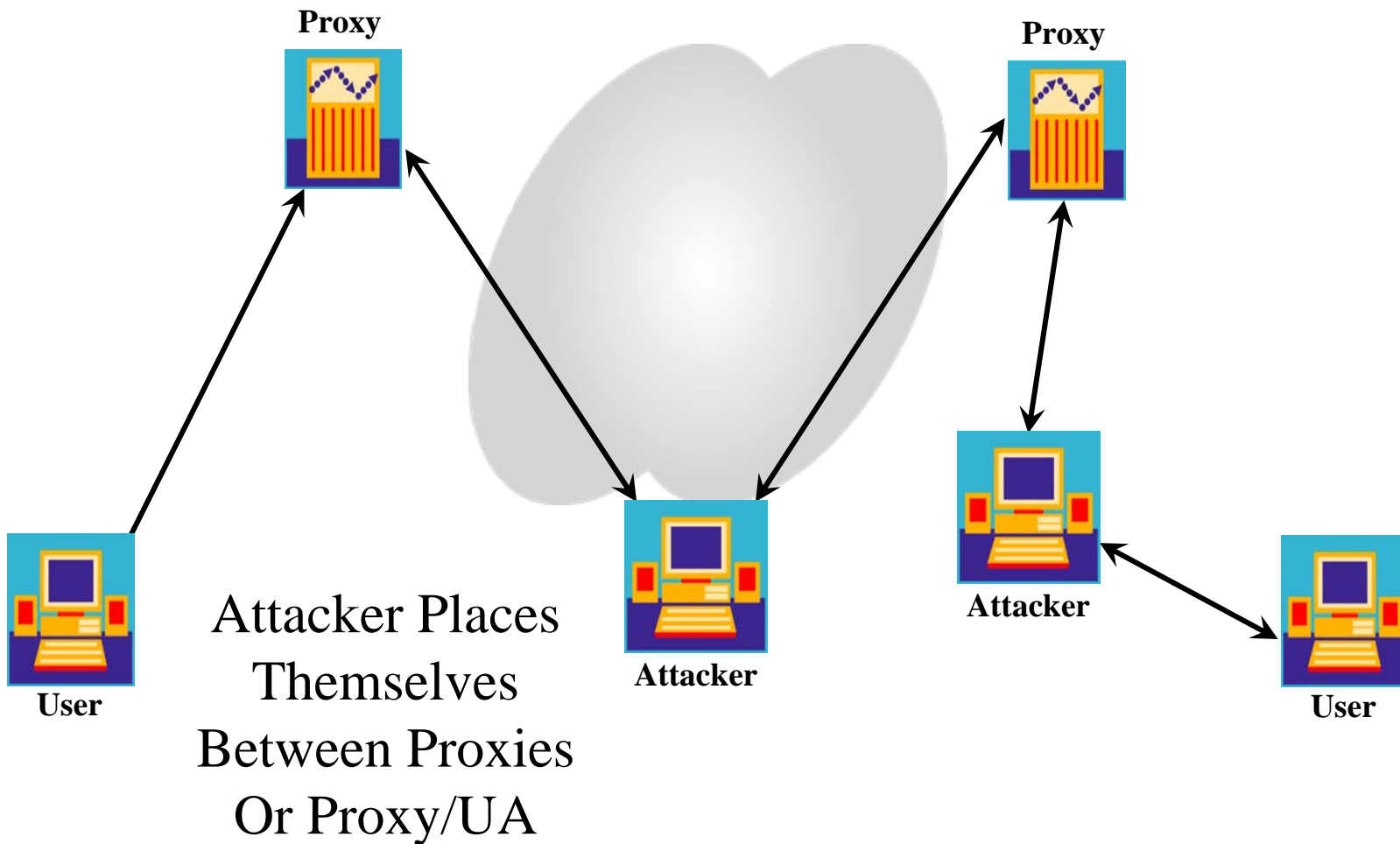
## Test for eavesdropping:

- ◆ Trivial to eavesdrop 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 – Man-in-the-Middle



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

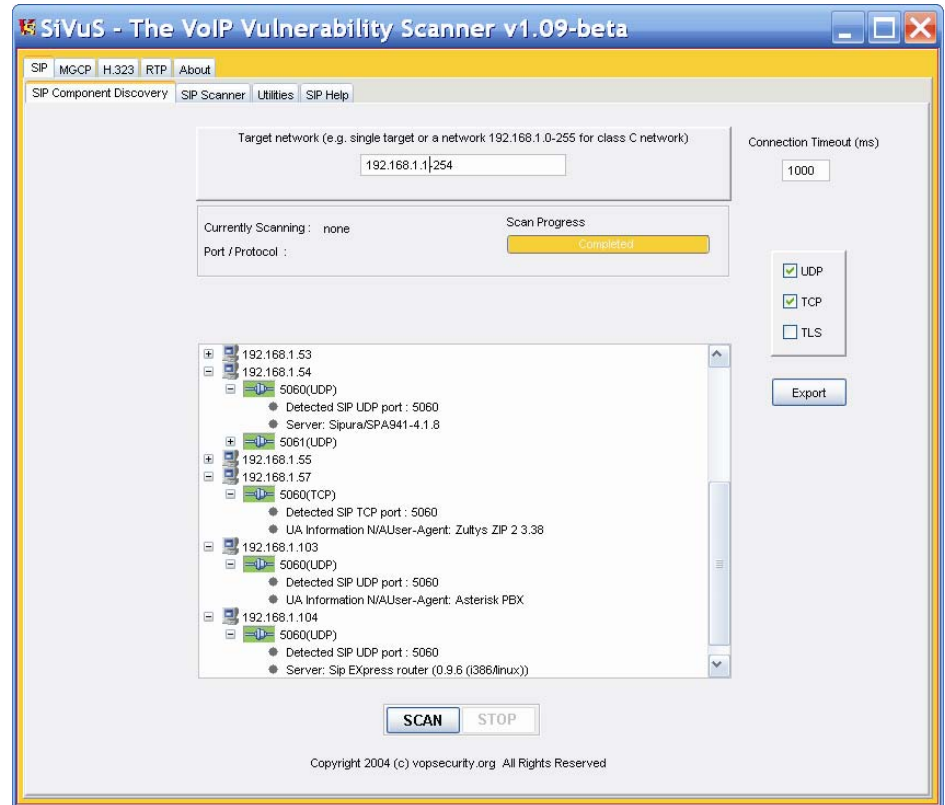
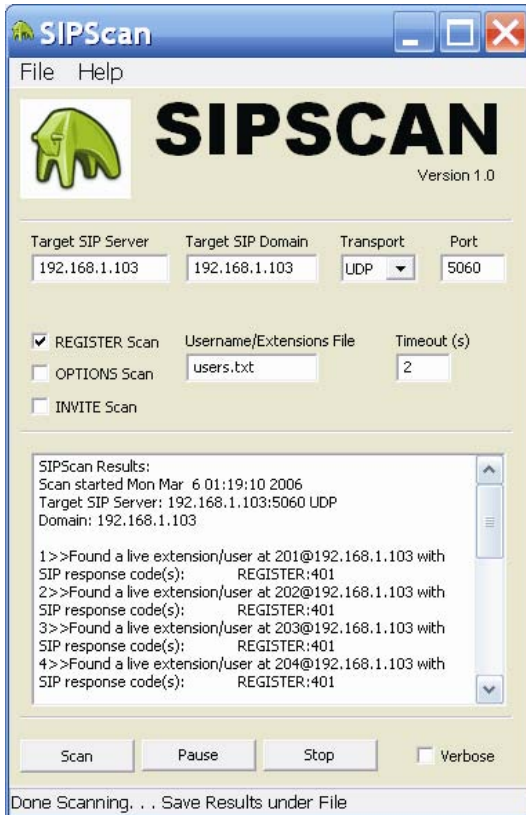
This will be especially true when IP Telephony is exchanged with a public network

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

# Application - Enumeration

Enumeration involves identification of valid users:

- ◆ Quite a few tools available
- ◆ SIPSCAN and SiVuS automates 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

```
INVITE sip:6713@192.168.26.180:6060;user=phone SIP/2.0
Via: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaa...
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
```

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](http://www.ee.oulu.fi/research/ouspg/protos/index.html)
- ◆ [www.codenomicon.com](http://www.codenomicon.com)

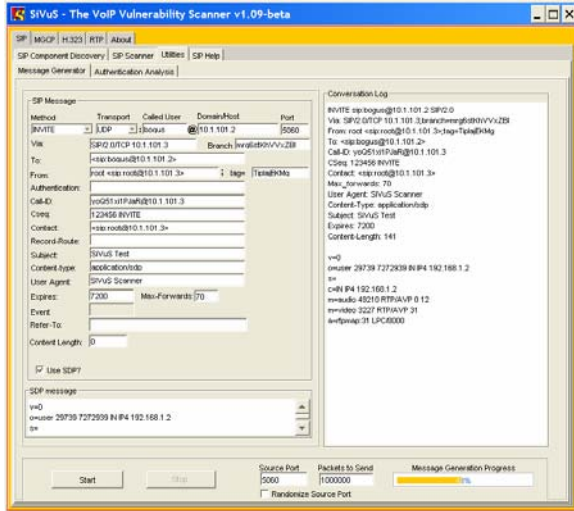
There are many types of service disruptions possible

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

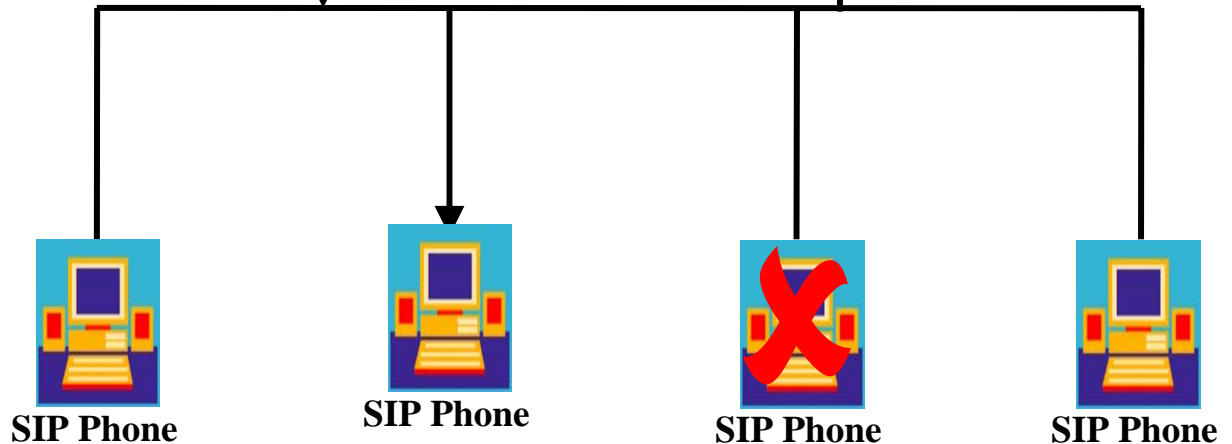
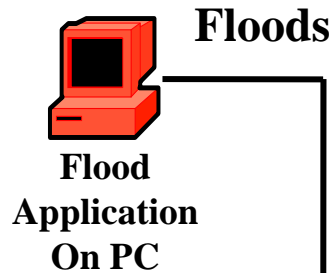
The following several slides describe several types of possible attacks

# Application – Service Disruption

## DoS Attacks

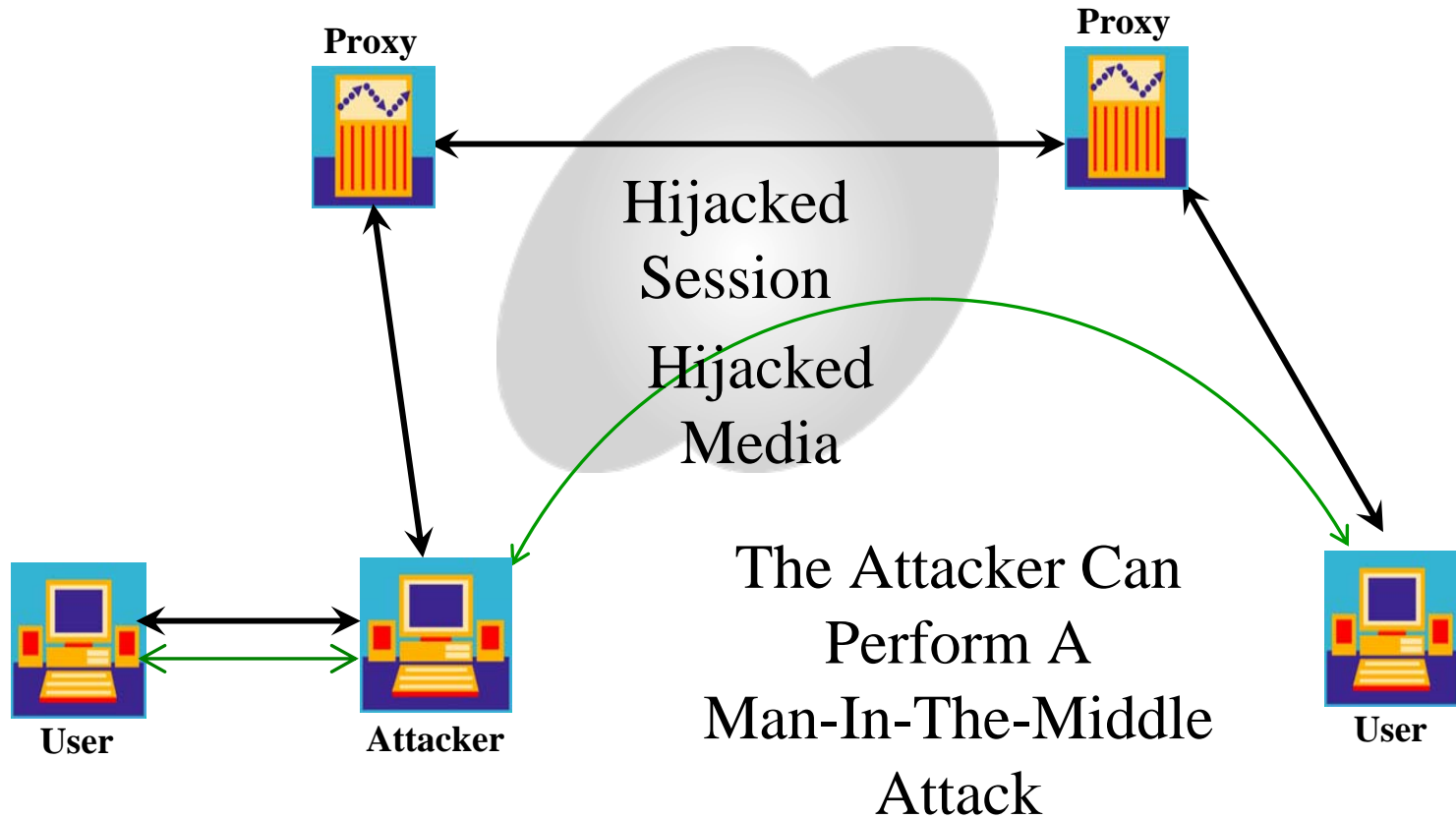


**UDP, RTP, TCP SYN  
INVITE, REGISTER**



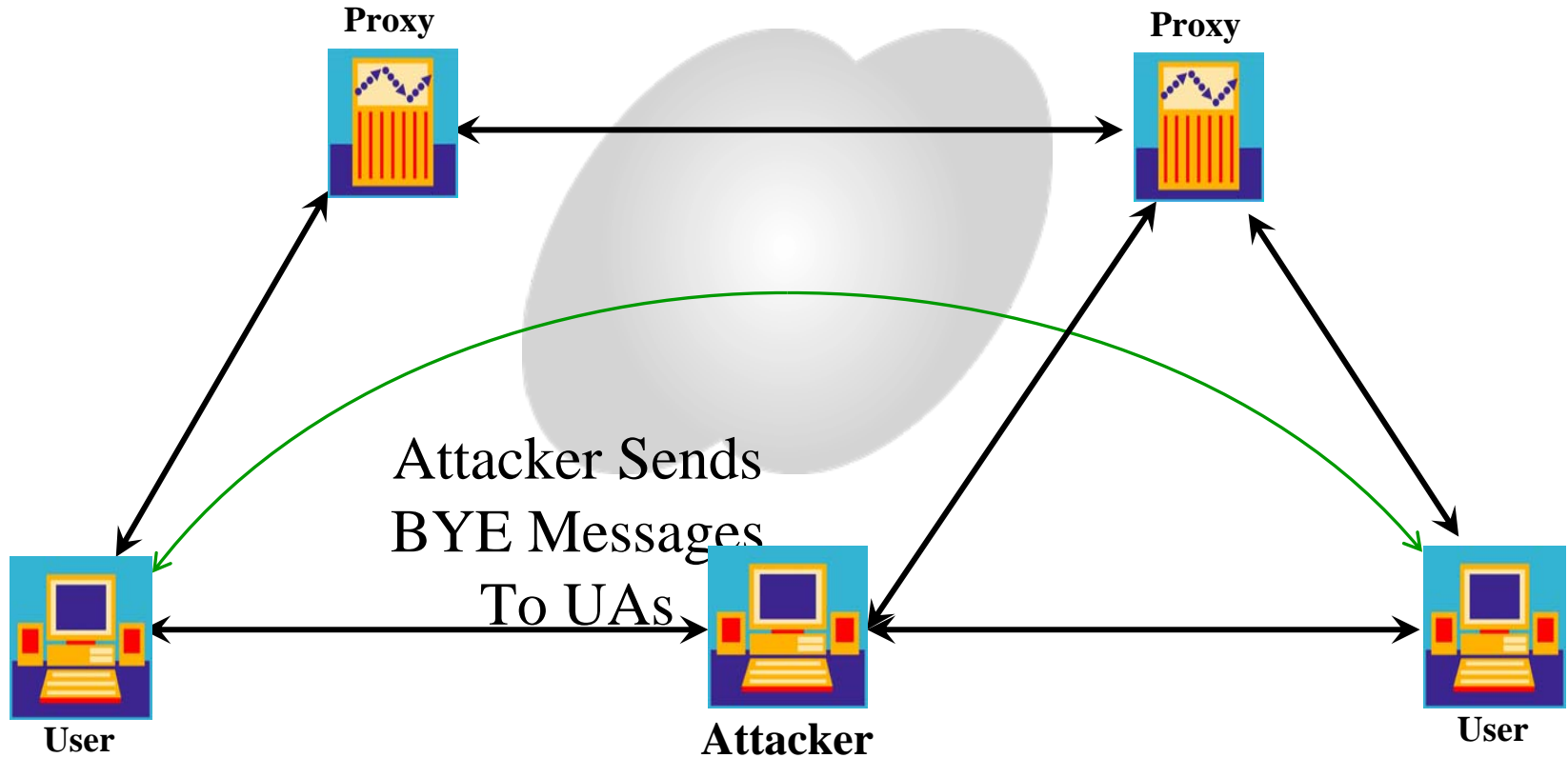
# Application – Service Disruption

## Registration Hijacking and Manipulation



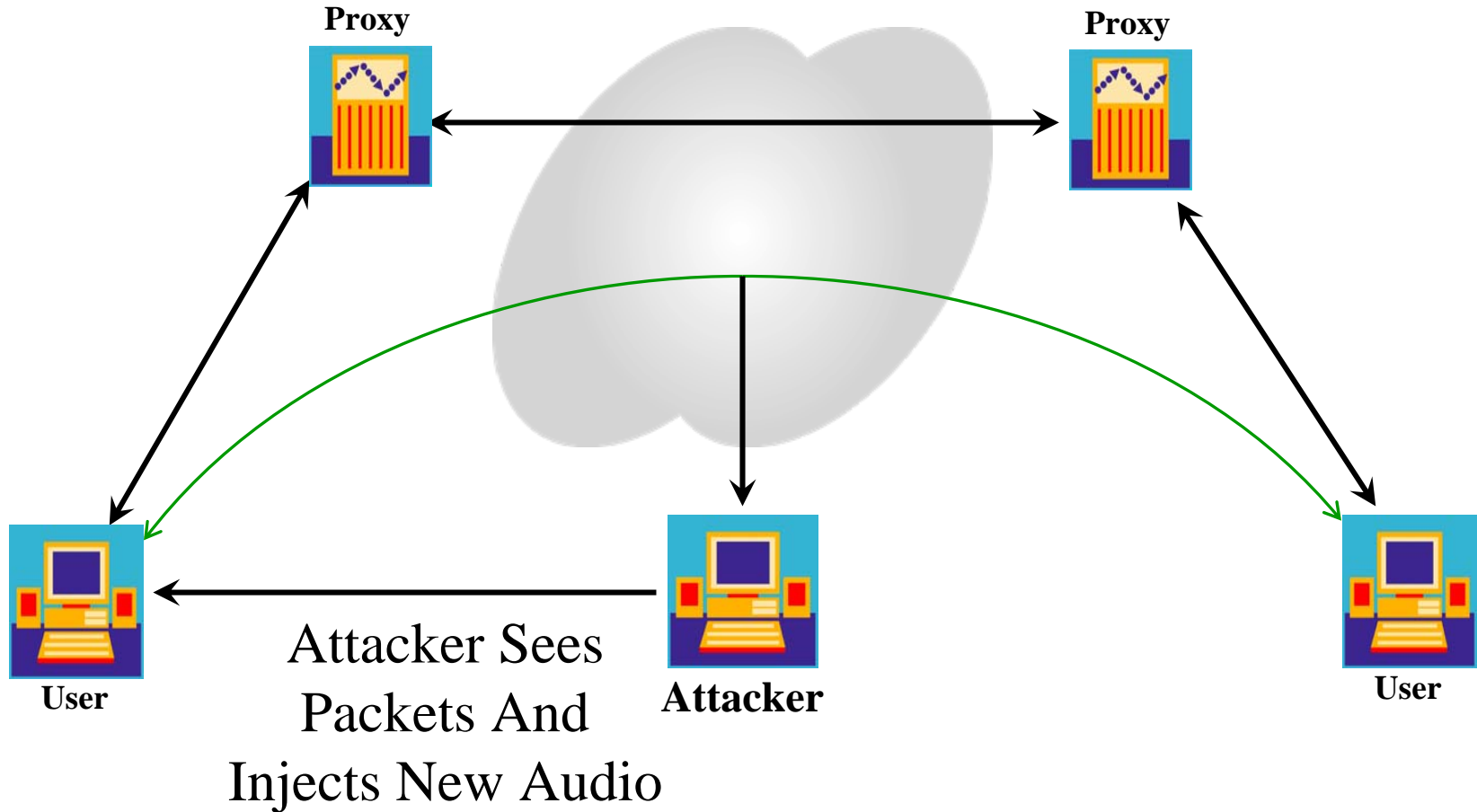
# Application – Service Disruption

## Session Teardown



# Application – Service Disruption

## RTP Injection



# Summary

A comprehensive IP Telephony security assessment addresses the entire IP Telephony system

An IP Telephony security assessment is recommended when you deploy your system and as you expand

SecureLogix, [www.securelogix.com](http://www.securelogix.com), along with other vendors, offers IP Telephony security assessments

See [www.hackingexposedvoip.com](http://www.hackingexposedvoip.com) for more information

