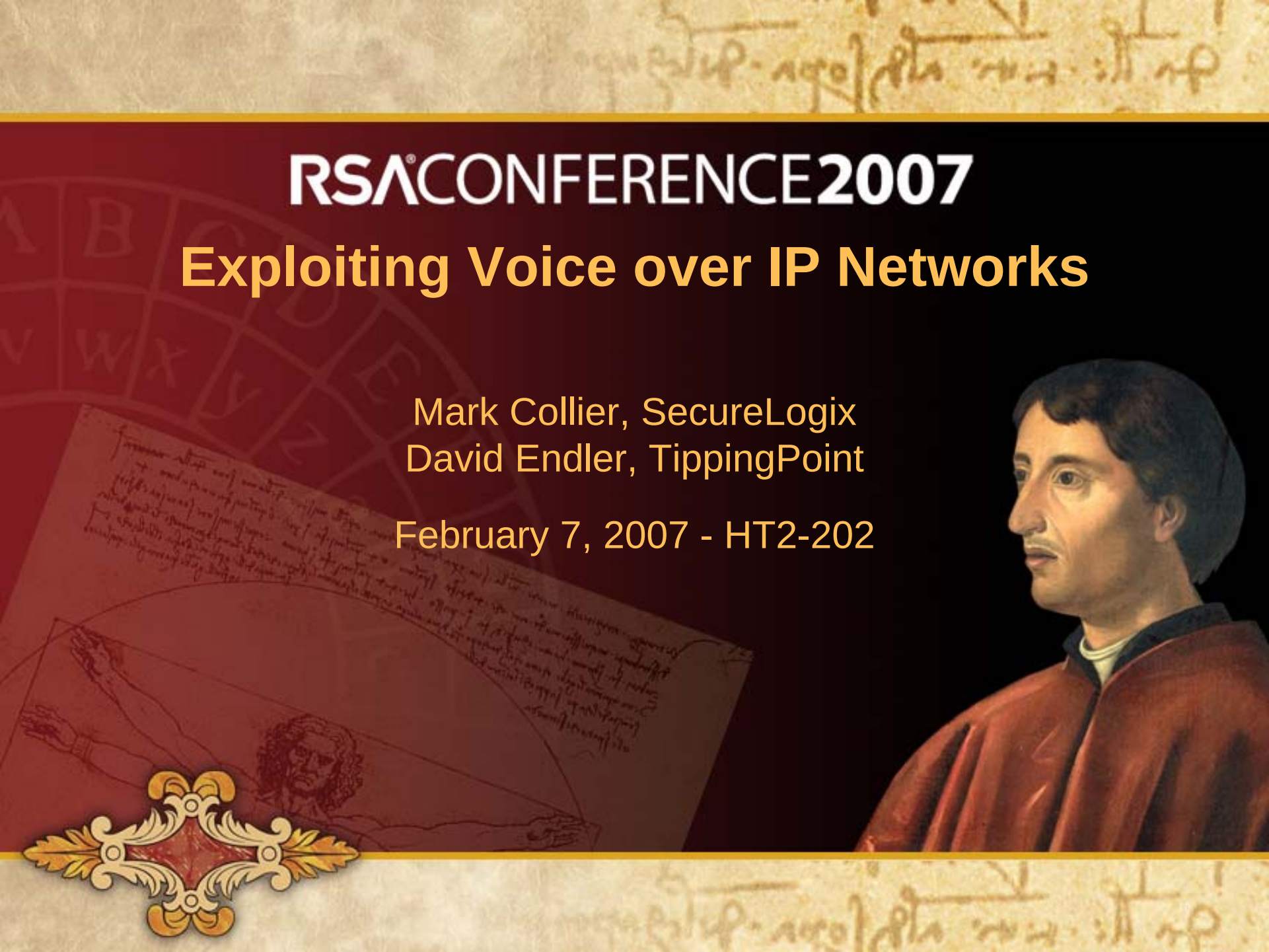
RSA CONFERENCE 2007

# Exploiting Voice over IP Networks

Mark Collier, SecureLogix
David Endler, TippingPoint

February 7, 2007 - HT2-202



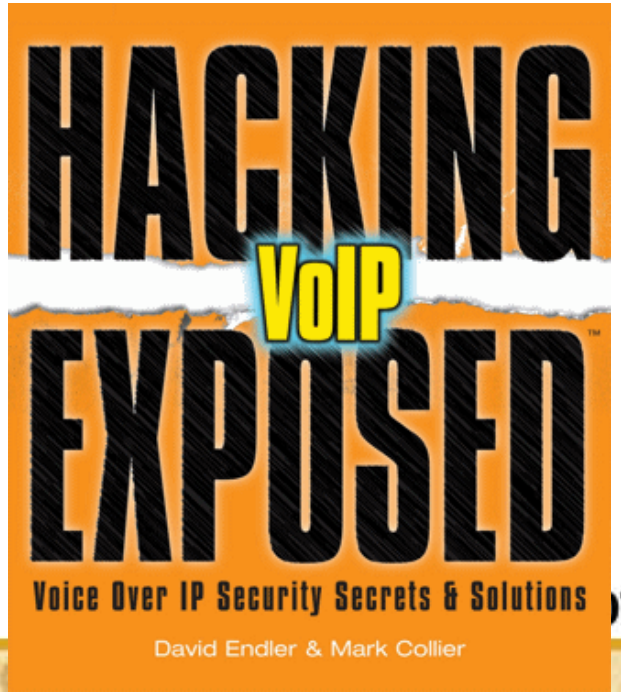
# Who are we?

- **Mark Collier** is the chief technology officer at SecureLogix corporation, where he directs the company's VoIP security research and development. Mark also defines and conducts VoIP security assessments for SecureLogix's enterprise customers. Mark is actively performing research for the U.S. Department of Defense, with a focus on developing SIP vulnerability assessment tools. Prior to SecureLogix, Mark was with Southwest Research Institute (SwRI), where he directed a group performing research and development in the areas of computer security and information warfare. Mark is a frequent speaker at major VoIP and security conferences, has authored numerous articles and papers on VoIP security and is also a founding member of the Voice over IP Security Alliance (VOIPSA). Mark graduated magna cum laude graduate from St. Mary's University, where he earned a bachelors' degree in computer science.

- **David Endler** is the director of security research for 3Com's security division, TippingPoint. In this role, he oversees 3Com's product security testing, VoIP security research center, and TippingPoint's vulnerability research teams. While at TippingPoint, David founded an industry-wide group called the *Voice over IP Security Alliance (VOIPSA)* in 2005 (http://www.voipsa.org). Previously, he has performed security research working for Xerox Corporation, the National Security Agency, and Massachusetts Institute of Technology. David has authored numerous articles and papers on computer security and was named one of the Top 100 Voices in IP Communications by *IP Telephony Magazine.* He graduated summa cum laude from Tulane University where he earned a bachelor's and master's degree in computer science.

# Shameless plug alert: We just wrote a book

- We took on this project in the realization that there were really no practical books on enterprise VoIP security that gave examples of how hackers attack VoIP deployments and correspondingly showed administrators how to defend against these attacks
- We spent more than a year of research writing new VoIP security tools, using them to test the latest VoIP products, and scouring the state of the art in the VoIP security field.
- Book was published December 1, 2006
  http://www.hackingvoip.com
  536 pages




SECURELOGIX CORPORATION TippingPoint a division of 3Com

# Agenda

**We take a phased approach in presenting the material:**

- PART I: Casing the Establishment
  - Chapter 1: Footprinting
  - Chapter 2: Scanning
  - Chapter 3: Enumeration
- PART II: Exploiting the VoIP Network
  - Chapter 4: VoIP Network Infrastructure Denial of Service
  - Chapter 5: Network Eavesdropping
  - Chapter 6: Network and Application Interception
- PART III: VoIP Session and Application Hacking
  - Chapter 11: Fuzzing VoIP
  - Chapter 12: Disruption of Service
  - Chapter 13: VoIP Signaling and Media Manipulation
- PART IV: Social Threats
  - Chapter 14: SPAMMING/SPIT
  - Chapter 15: VoIP Phishing

# PART I *Casing the Establishment*

- ***Part I. "Casing the Establishment" -*** The first part is introductory and describes how an attacker would first scan the whole network and then pick up specific targets and enumerate them with great precision in order to proceed with further advanced attacks through or from the hacked VoIP devices.
  - **"Footprinting"**
    - We begin the book by describing how a hacker first profiles the target organization by performing passive reconnaissance using tools such as Google, DNS, and WHOIS records, as well as the target's own website.
  - **"Scanning"**
    - A logical continuation of the previous chapter, this chapter provides a review of various remote scanning techniques in order to identify potentially active VoIP devices on the network. We cover the traditional UDP, TCP, SNMP, and ICMP scanning techniques as applied to VoIP devices.
  - **"Enumeration"**
    - Here, we show active methods of enumeration of various standalone VoIP devices, from softphones, hard phones, proxies, and other general SIP-enabled devices. Plenty of examples are provided, along with a demonstration of SIPScan, a SIP directory scanning tool we wrote.

# PART II *Exploiting the VoIP Network*

***Part II. "'Exploiting the VoIP Network" -*** This part is focused on exploiting the supporting network infrastructure on which your VoIP applications depend. We begin with typical network denial-of-service attacks and eventually lead up to VoIP conversation eavesdropping.

- **"VoIP Network Infrastructure Denial of Service"**
  - In this chapter, we introduce quality of service and how to objectively measure the quality of a VoIP conversation on the network using various free and commercial tools. Next, we discuss various flooding and denial of service attacks on VoIP devices and supporting services such as DNS and DHCP.
- **"Network Eavesdropping"**
  - This section is very much focused on the types of VoIP privacy attacks an attacker can perform with the appropriate access to sniff traffic. Techniques such as number harvesting, call pattern tracking, TFTP file snooping, and actual conversation eavesdropping are demonstrated.
- **"Network and Application Interception"**
  - The methods described in this chapter detail how to perform man-in-the-middle attacks in order to intercept and alter an active VoIP session and conversation. We demonstrate some man-in-the-middle methods of ARP poisoning.

# PART III *VoIP Session and Application Hacking*

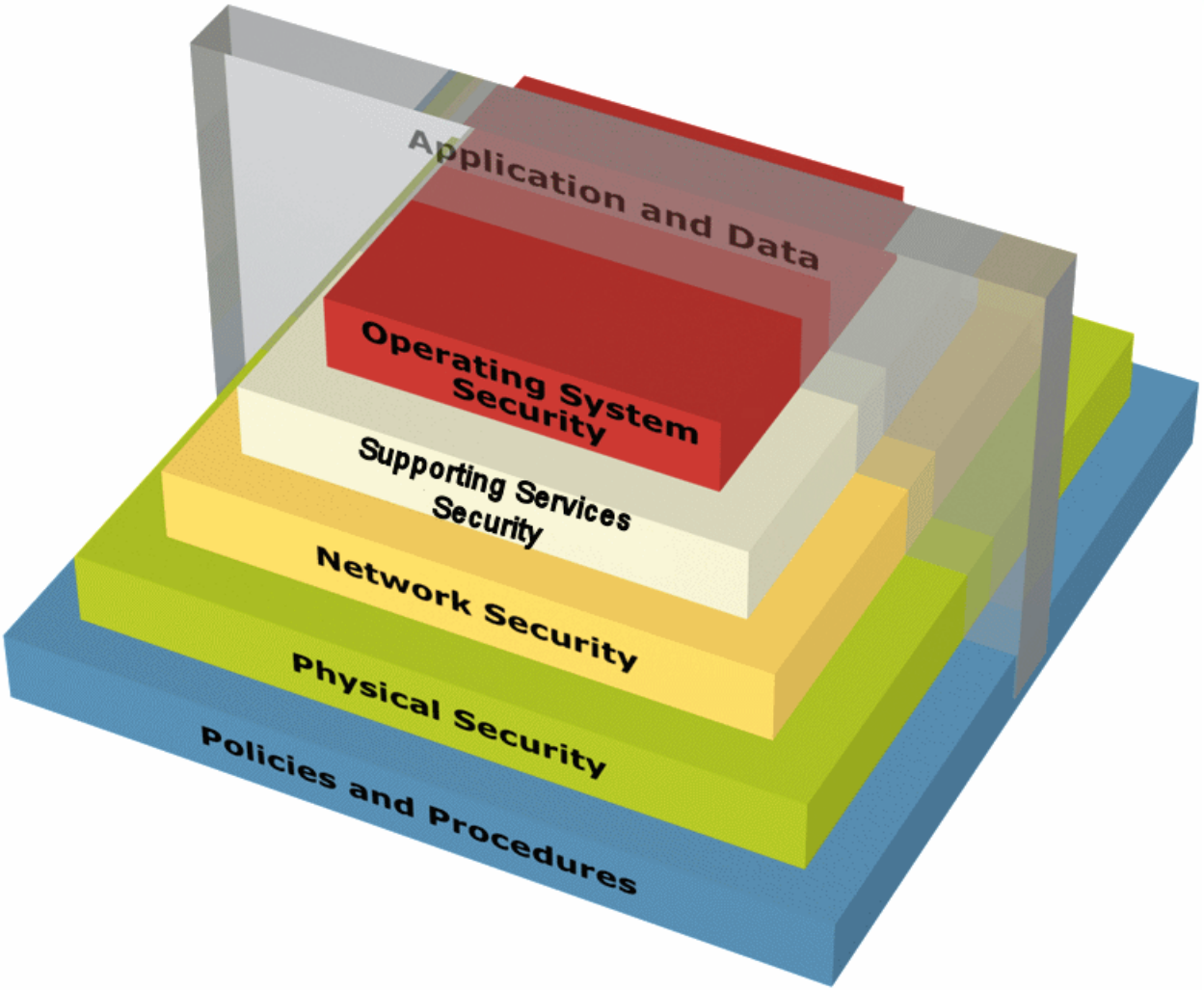
- ***Part III. "VoIP Session and Application Hacking" -*** We shift our attention from attacking the network and device to attacking the protocol. A fine art of protocol exploitation can hand intruders full control over the VoIP application traffic without any direct access and reconfiguration of the hosts or phones deployed.
  - **"Fuzzing VoIP"**
    - The practice of *fuzzing,* otherwise known as *robustness testing* or *functional protocol testing,* has been around for a while in the security community. The practice has proven itself to be pretty effective at automating vulnerability discovery in applications and devices that support a target protocol. In this chapter, we demonstrate some tools and techniques for fuzzing your VoIP applications.
  - **"Flood-Based Disruption of Service"**
    - In this chapter, we cover additional attacks that disrupt SIP proxies and phones by flooding them with various types of VoIP protocol and session-specific messages. These types of attacks partially or totally disrupt service for a SIP proxy or phone while the attack is under way. Some of the attacks actually cause the target to go out of service, requiring a restart.
  - **"VoIP Signaling and Media Manipulation"**
    - In this chapter, we cover other attacks in which an attacker manipulates SIP signaling or RTP media to hijack, terminate, or otherwise manipulate calls. We introduce no less than ten new tools to demonstrate these attacks. As with other attacks we have covered, these attacks are simple to execute and quite lethal.

# PART IV *Social Threats*

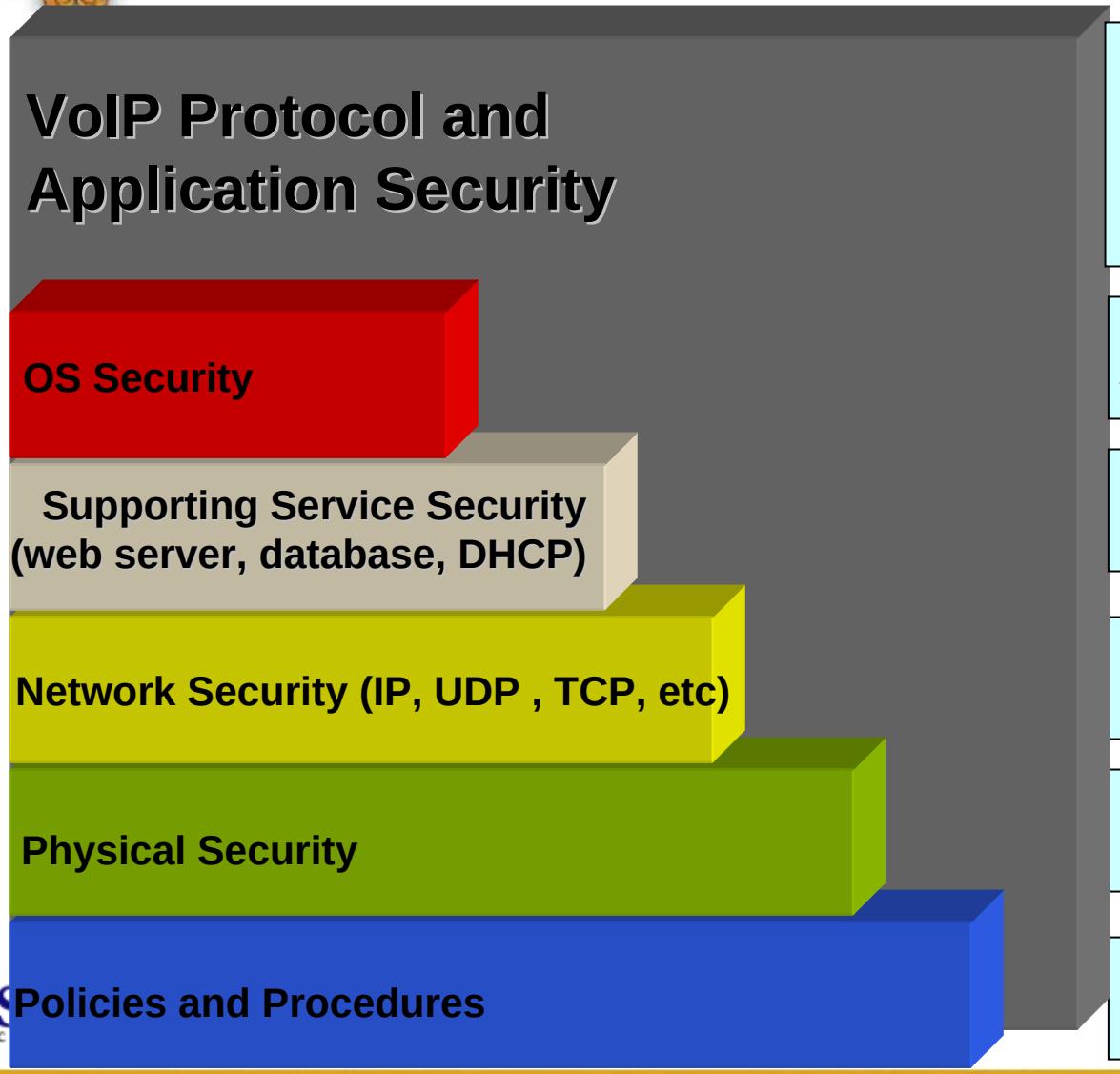
- ***Part IV. "Social Threats" -*** In the same way that the traditional email realm has been inundated with spam and phishing, so too are we starting to see the evolution of these social nuisances emerge into the VoIP world. This section focuses on how advertisers and scam artists will likely target VoIP users and how to help counter their advance.
  - **"SPAMMING/SPIT"**
    - *Voice SPAM* or *SPAM over Internet Telephony (SPIT)* is a similar problem that will affect VoIP. SPIT, in this context, refers to bulk, automatically generated, unsolicited calls. SPIT is like telemarketing on steroids. You can expect SPIT to occur with a frequency similar to email SPAM. This chapter describes how you can use the Asterisk IP PBX and a new tool called spitter to generate your own SPIT. This chapter also details how you can detect and mitigate SPIT.
  - **"Voice Phishing"**
    - Voice phishing relies on the effective gullibility of a victim trusting a phone number much more than an email link. Also, for a fraction of the cost, an attacker can set up an interactive voice response through a VoIP provider that is harder to trace than a compromised web server. Also, the nature of VoIP makes this type of attack even more feasible because most VoIP services grant their customers an unlimited number of calls for a monthly fee. This chapter details how these attacks are performed and how to detect them at their various stages.

# VoIP Security Pyramid

- VoIP security is built upon the many layers of traditional data security:



# Slice of VoIP Security Pyramid




Toll Fraud, SPIT, Phishing
Malformed Messages (fuzzing)
INVITE/BYECANCEL Floods
CALL Hijacking
Call Eavesdropping
Call Modificaiton

Buffer Overflows, Worms, Denial of Service (Crash), Weak Configuration

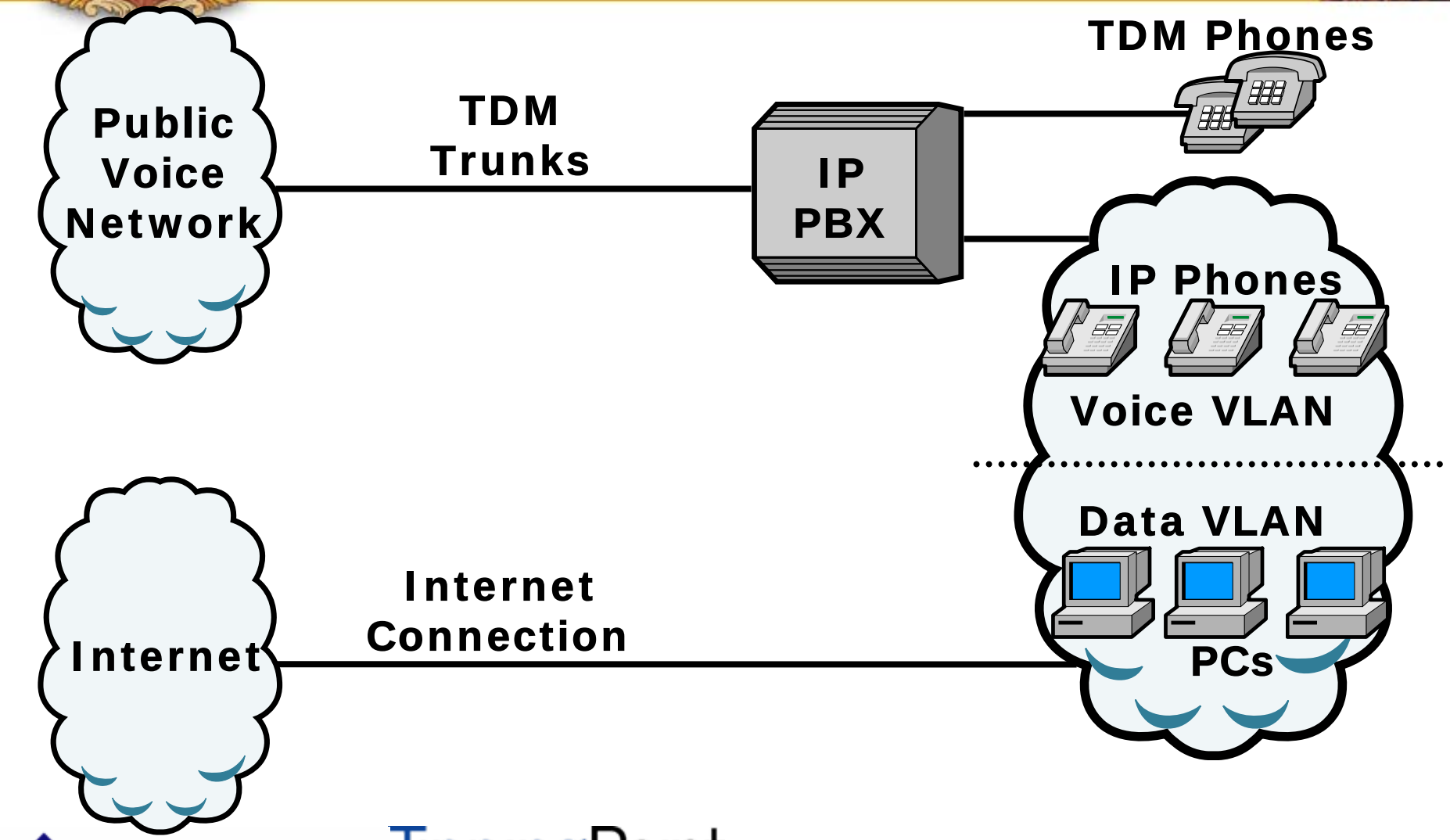
SQL Injection,
DHCP resource exhaustion

Syn Flood, ICMP unreachable, trivial flooding attacks, DDoS, etc.

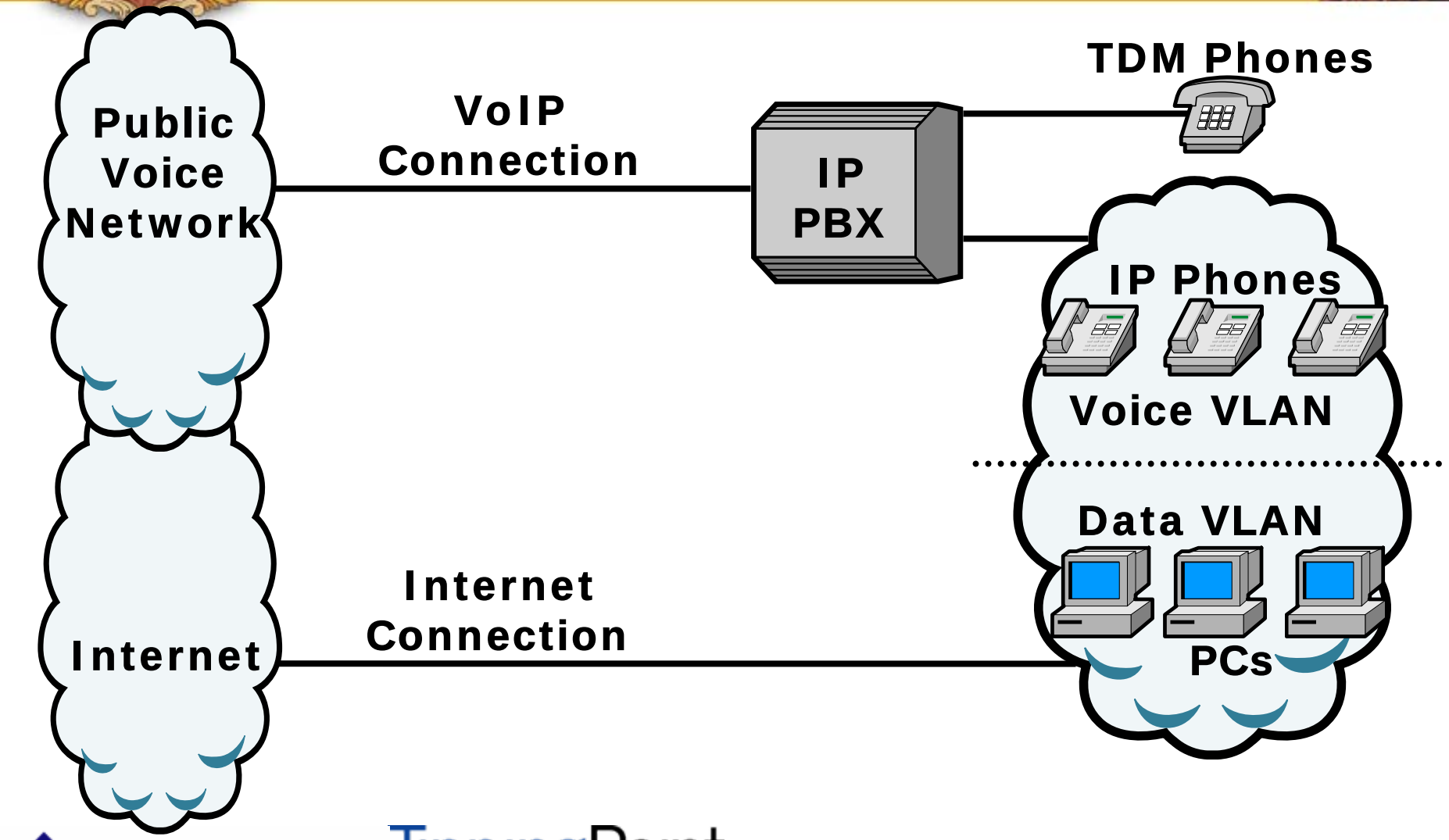
Total Call Server Compromise, Reboot, Denial of Service

Weak Voicemail Passwords
Abuse of Long Distance Privileges

# Introduction
# Campus VoIP



# Introduction
# Public VoIP



# Agenda

- PART I: Casing the Establishment
- PART II: Exploiting the VoIP Network
- PART III: VoIP Session and Application Hacking
- PART IV: Social Threats
- PART V: VoIP Security Trends

# Casing the Establishment

This is the process a hacker goes through to gather information about your organization and prepare their attack

Consists of:

- Footprinting
- Scanning
- Enumeration

# Footprinting

- Involves basic remote reconnaissance using well known online tools like SamSpade and Google
- Use Google to sift through:
  - Job listings
  - Tech Support
  - PBX main numbers

# Footprinting

- Google Job postings (or directly go to the target web site):

**“Required Technical Skills:**

**Minimum 3-5 years experience in the management and implementation of Avaya telephone systems/voice mails:**

*** Advanced programming knowledge of the Avaya Communication Servers and voice mails.”**

# Footprinting

- Google the target's Tech Support:
  - "XXXX Department has begun a new test phase for Cisco Conference Connection (CCC). This is a self-serve telephone conferencing system that is administered on-campus and is **available at no charge for a 90 day test period** to faculty and staff. The system has been subject to live testing by a small group and has proven itself ready for release to a larger group. In exchange for the free use of the conferencing system, we will request your feedback on its quality and functionality. "

# Footprinting

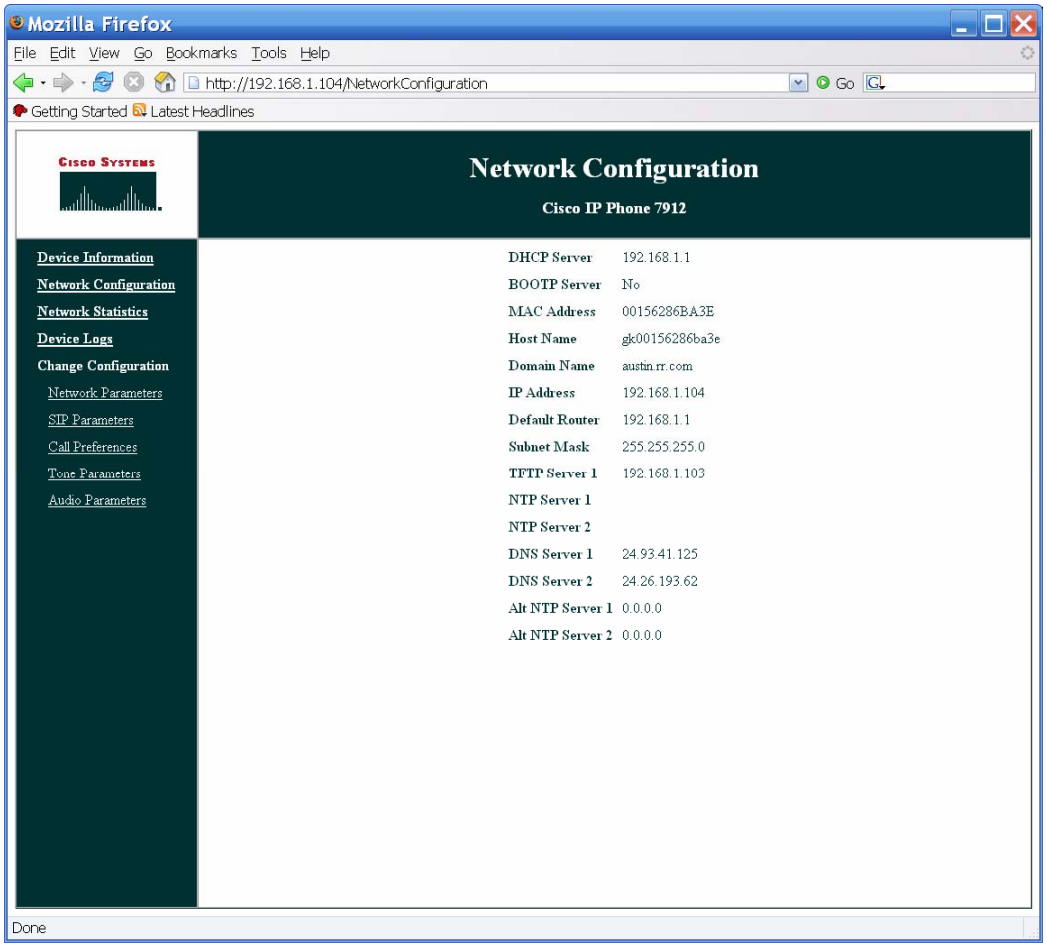
- Use Google to find main switchboard and extensions.
  - “877 111..999-1000..9999 site:www.mcgraw-hill.com”

- Call the main switchboard and listen to the recording.
- Check out our VoIP Voicemail Database for help in identifying the vendor at http://www.hackingvoip.com

# Google Hacking

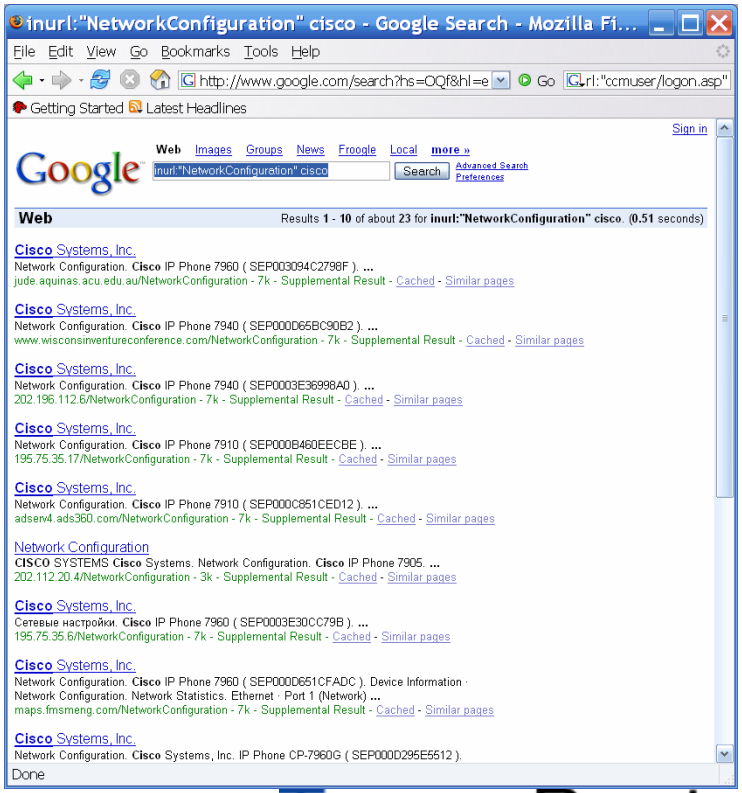
- Most VoIP devices (phones, servers, etc.) also run Web servers for remote management
- Find them with Google
  - Type: inrul:”ccmuser/logon.asp”
  - Type: inurl:”ccmuser/logon.asp” site:example.com
  - Type: inurl:”NetworkConfiguration” cisco
- VoIP Google Hacking Database at http://www.hackingvoip.com

# Google Hacking



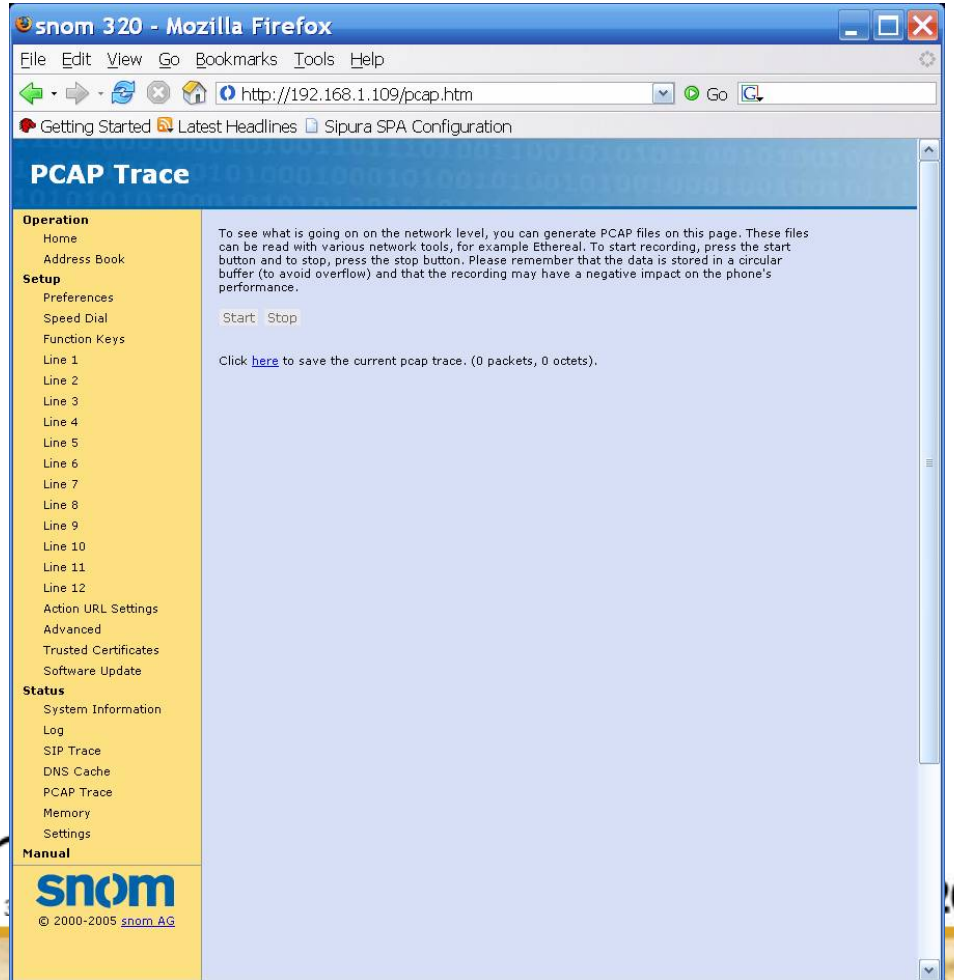
# More Google Hacking

- inurl:"NetworkConfiguration" cisco



# Google Hacking with a Twist

- **Snom phones have a packet capture feature.**
- **Yikes!**



# Google Hacking Countermeasures

Determine what your exposure is

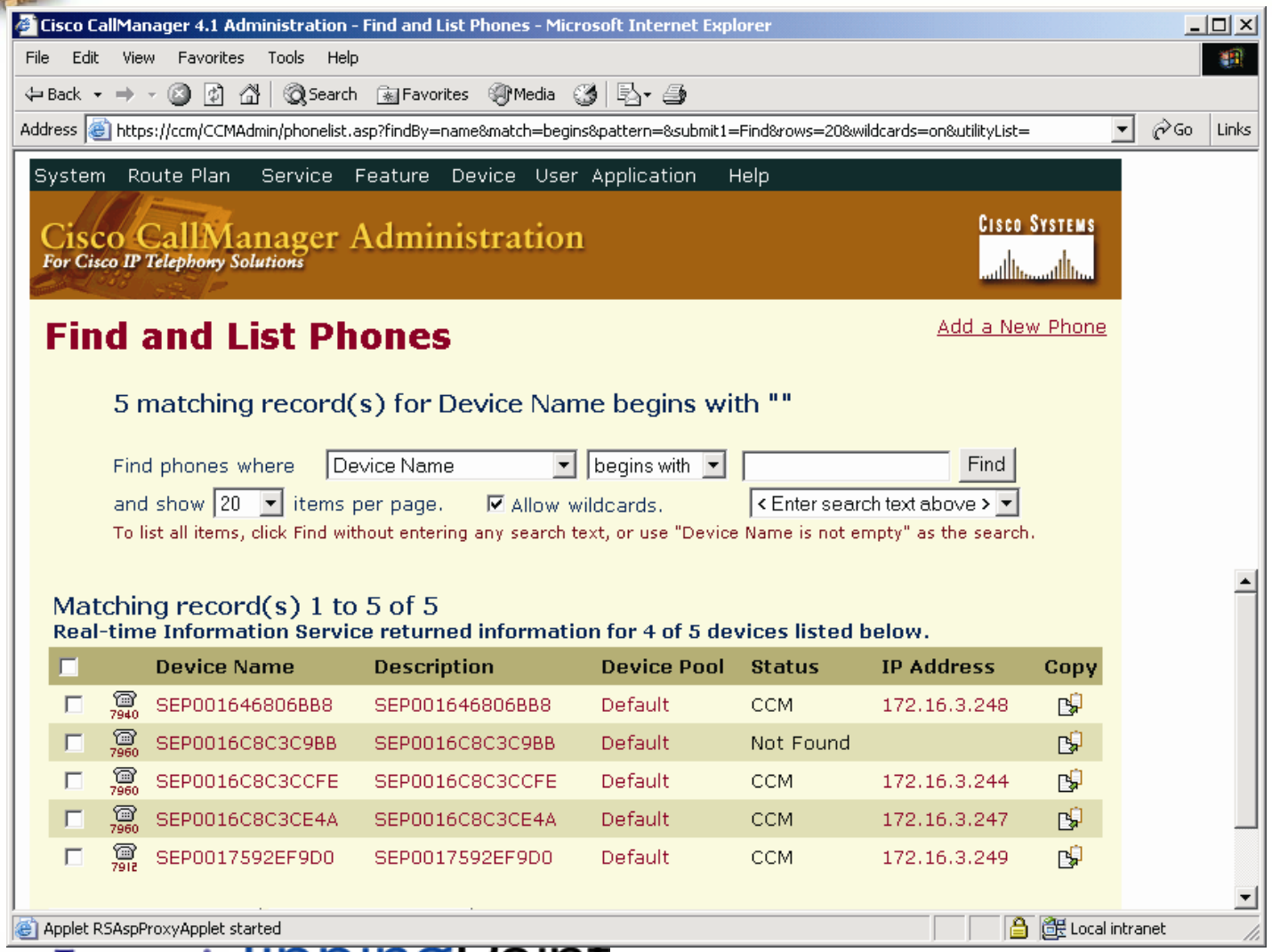
Be sure to remove any VoIP phones which are visible to the Internet

Disable the web servers on your IP phones

There are services that can help you monitor your exposure:

- www.cyveilance.com
- ww.baytsp.com

# Google Hacking Countermeasures



# Scanning Introduction

Steps taken by a hacker to identify IP addresses and hosts running VoIP

Consists:

- Host/device discovery
- Port scanning and service discovery
- Host/device identification

# Host/Device Discovery

Consists of various techniques used to find hosts:

- Ping sweeps
- ARP pings
- TCP ping scans
- SNMP sweeps

# Host/Device Discovery Using nmap

```
nmap -O -P0 192.168.1.1-254
Interesting ports on 192.168.1.21:
(The 1671 ports scanned but not shown below are in state: filtered)
PORT   STATE SERVICE
23/tcp open  telnet
MAC Address: 00:0F:34:11:80:45 (Cisco Systems)
Device type: VoIP phone
Running: Cisco embedded
OS details: Cisco IP phone (POS3-04-3-00, PC030301)
Interesting ports on 192.168.1.23:
(The 1671 ports scanned but not shown below are in state: closed)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:15:62:86:BA:3E (Cisco Systems)
Device type: VoIP phone|VoIP adapter
Running: Cisco embedded
OS details: Cisco VoIP Phone 7905/7912 or ATA 186 Analog Telephone Adapter
Interesting ports on 192.168.1.24:
(The 1671 ports scanned but not shown below are in state: closed)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0E:08:DA:DA:17 (Sipura Technology)
Device type: VoIP adapter
Running: Sipura embedded
OS details: Sipura SPA-841/1000/2000/3000 POTS<->VoIP gateway
```

# Scanning

- SIP enabled devices will usually respond on UDP/TCP ports 5060 and 5061
- SCCP enabled phones (Cisco) responds on UDP/TCP 2000-2001
- Sometimes you might see UDP or TCP port 17185 (VXWORKS remote debugging!)

# Port Scanning/Service Discovery Countermeasures

- Using non-Internet routable IP addresses will prevent external scans
- Firewalls and IPSs can detect and possibly block scans
- VLANs can be used to partition the network to prevent scans from being effective

# Enumeration Introduction

- Involves testing open ports and services on hosts/devices to gather more information
- Includes running tools to determine if open services have known vulnerabilities
- Also involves scanning for VoIP-unique information such as phone numbers
- Includes gathering information from TFTP servers and SNMP

# Enumeration

- Will focus on four main types of VoIP enumeration here
  - SIP “user agent” and “server“ scraping
  - SIP phone extensions (usernames)
  - TFTP configuration files
  - SNMP config information

# Enumeration

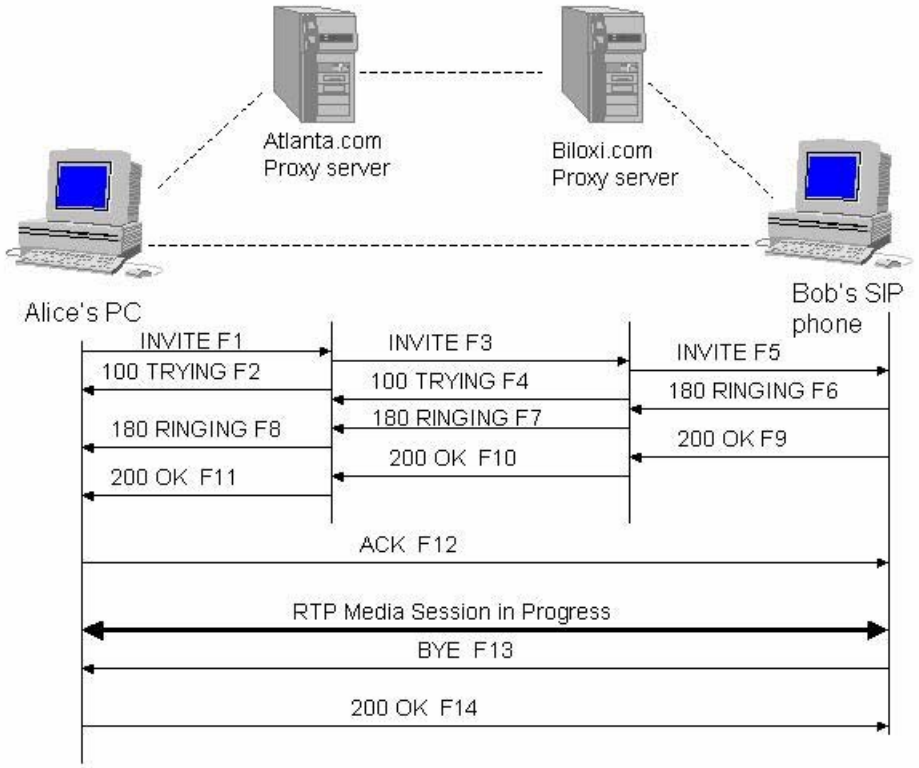
- SIP Messages

| SIP Request | Purpose | RFC Reference |
|---|---|---|
| INVITE | to initiate a conversation | RFC 3261 |
| BYE | to terminate an existing connection between two users in a session | RFC 3261 |
| OPTIONS | to determine the SIP messages and codecs that the UA or Server understands | RFC 3261 |
| REGISTER | to register a location from a SIP user | RFC 3261 |
| ACK | To acknowledge a response from an INVITE request | RFC 3261 |
| CANCEL | to cancel a pending INVITE request, but does not affect a completed request (for instance, to stop the call setup if the phone is still ringing) | RFC 3261 |

# Enumeration

- SIP responses (RFC 3261) are 3-digit codes much like HTTP (e.g. 200 ok, 404 not found, etc.). The first digit indicates the category of the response:
- · 1xx Responses - Information Responses
- · 2xx Responses - Successful Responses
- · 3xx Responses - Redirection Responses
- · 4xx Responses - Request Failures Responses
- · 5xx Responses - Server Failure Responses
- · 6xx Responses - Global Failure Responses

# The SIP Trapezoid



# Enumeration

- Use the tool netcat to send a simple OPTIONS message

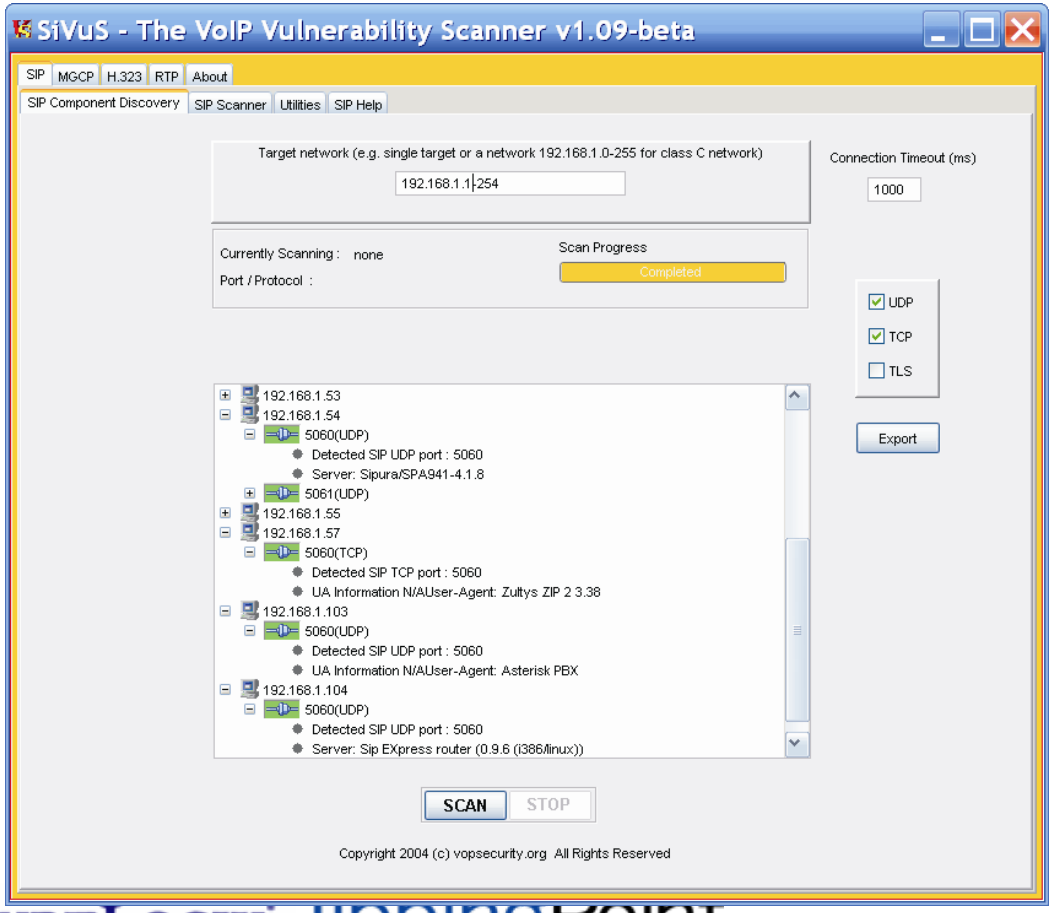
- [root@attacker]# nc 192.168.1.104 5060

```
OPTIONS sip:test@192.168.1.104 SIP/2.0
Via: SIP/2.0/TCP 192.168.1.120;branch=4ivBcVj5ZnPYgb
To: alice <sip:test@192.168.1.104>
Content-Length: 0


SIP/2.0 404 Not Found
Via: SIP/2.0/TCP 192.168.1.120;branch=4ivBcVj5ZnPYgb;received=192.168.1.103
To: alice <sip:test@192.168.1.104>;tag=b27e1a1d33761e85846fc98f5f3a7e58.0503
Server: Sip EXpress router (0.9.6 (i386/linux))
Content-Length: 0
Warning: 392 192.168.1.104:5060 "Noisy feedback tells:  pid=29801 req_src_ip=192.168.1.120 req_src_port=32773
      in_uri=sip:test@192.168.1.104 out_uri=sip:test@192.168.1.104 via_cnt==1"
```

# Enumeration

- Automate this using SiVuS http://www.vopsecurity.org



# Enumeration

- SIP extensions are useful to an attacker to know for performing Application specific attacks (Registration hijacking, voicemail brute forcing, caller id spoofing, etc.)
- Let’s go back to our netcat example

# Enumeration

- Use the tool netcat to send a simple OPTIONS message for a username “test”. If the username exists, we would expect a 200 response (OK) instead of 404 (Not found).

- [root@attacker]# nc 192.168.1.104 5060

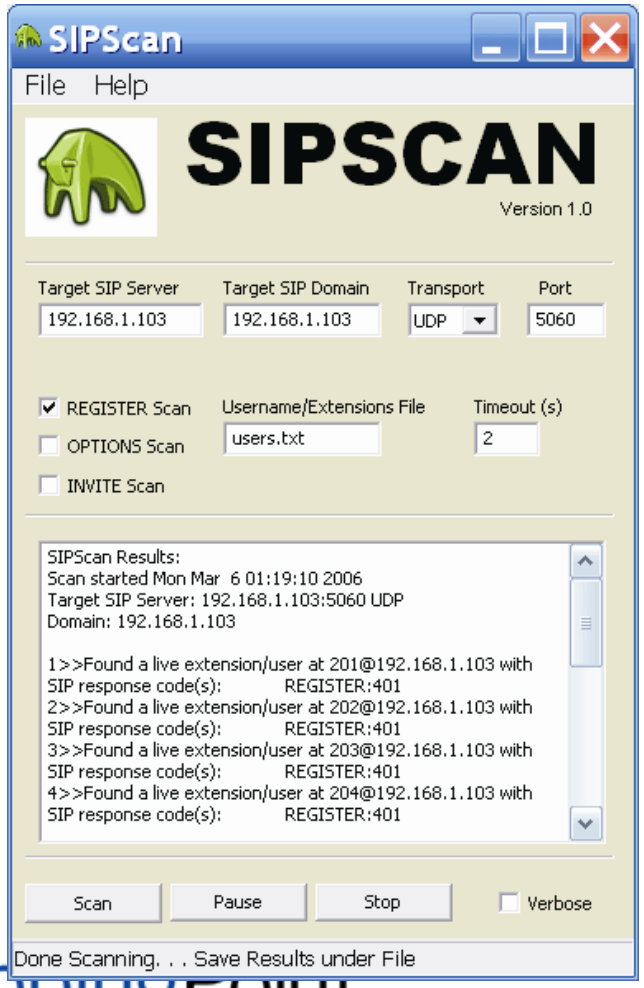
```
OPTIONS sip:test@192.168.1.104 SIP/2.0
Via: SIP/2.0/TCP 192.168.1.120;branch=4ivBcVj5ZnPYgb
To: alice <sip:test@192.168.1.104>
Content-Length: 0


SIP/2.0 404 Not Found
Via: SIP/2.0/TCP 192.168.1.120;branch=4ivBcVj5ZnPYgb;received=192.168.1.103
To: alice <sip:test@192.168.1.104>;tag=b27e1a1d33761e85846fc98f5f3a7e58.0503
Server: Sip EXpress router (0.9.6 (i386/linux))
Content-Length: 0
```

# Directory Scanning

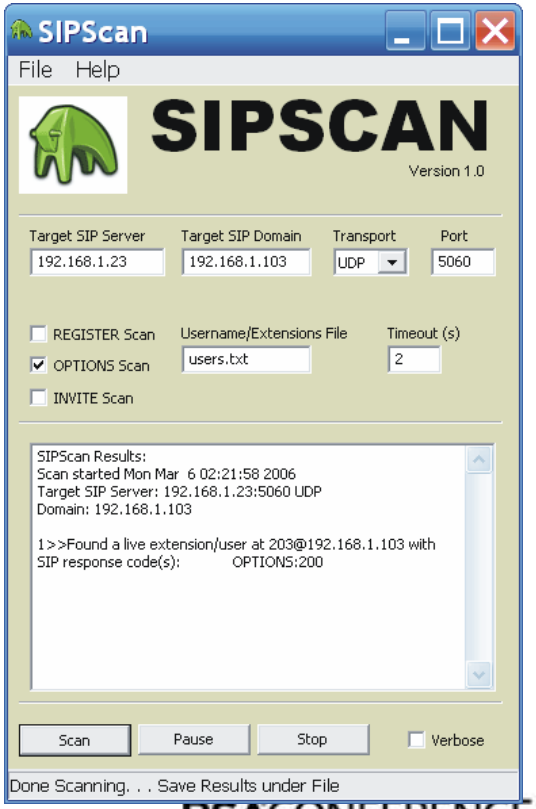
- Let's automate this.  We wrote a tool called SIPSCAN to help. Available at http://www.hackingvoip.com
- Not only can you use OPTIONS, but INVITE and REGISTER as well.

# Directory Scanning Demo



# Directory Scanning on Cisco SIP

- Use SIPSCAN to query the phone's extension



# TFTP Enumeration

- Almost all phones we tested use TFTP to download their configuration files upon bootup
- Rarely is the TFTP server well protected
- If you can guess the name of the configuration file, you can download it.
- Some config files have passwords, services, and usernames in them!

# TFTP Enumeration

- **Go to http://www.hackingvoip.com to see a list of commonly named VoIP config files**
- **Use a tool called TFTPBRUTE**

**[root@attacker]# perl tftpbrute.pl 192.168.1.103 brutefile.txt 100**

```
tftpbrute.pl, , V 0.1
TFTP file word database: brutefile.txt
TFTP server 192.168.1.103
Max processes 100
<snip>
 Processes are: 11
 Processes are: 12
*** Found  TFTP server remote filename : sip.cfg
*** Found  TFTP server remote filename : 46xxsettings.txt
 Processes are: 13
 Processes are: 14
*** Found  TFTP server remote filename : sip_4602D02A.txt
*** Found  TFTP server remote filename : XMLDefault.cnf.xml
*** Found  TFTP server remote filename : SipDefault.cnf
```

# TFTP Enumeration Countermeasures

It is difficult not to use TFTP, since it is so commonly used by VoIP vendors

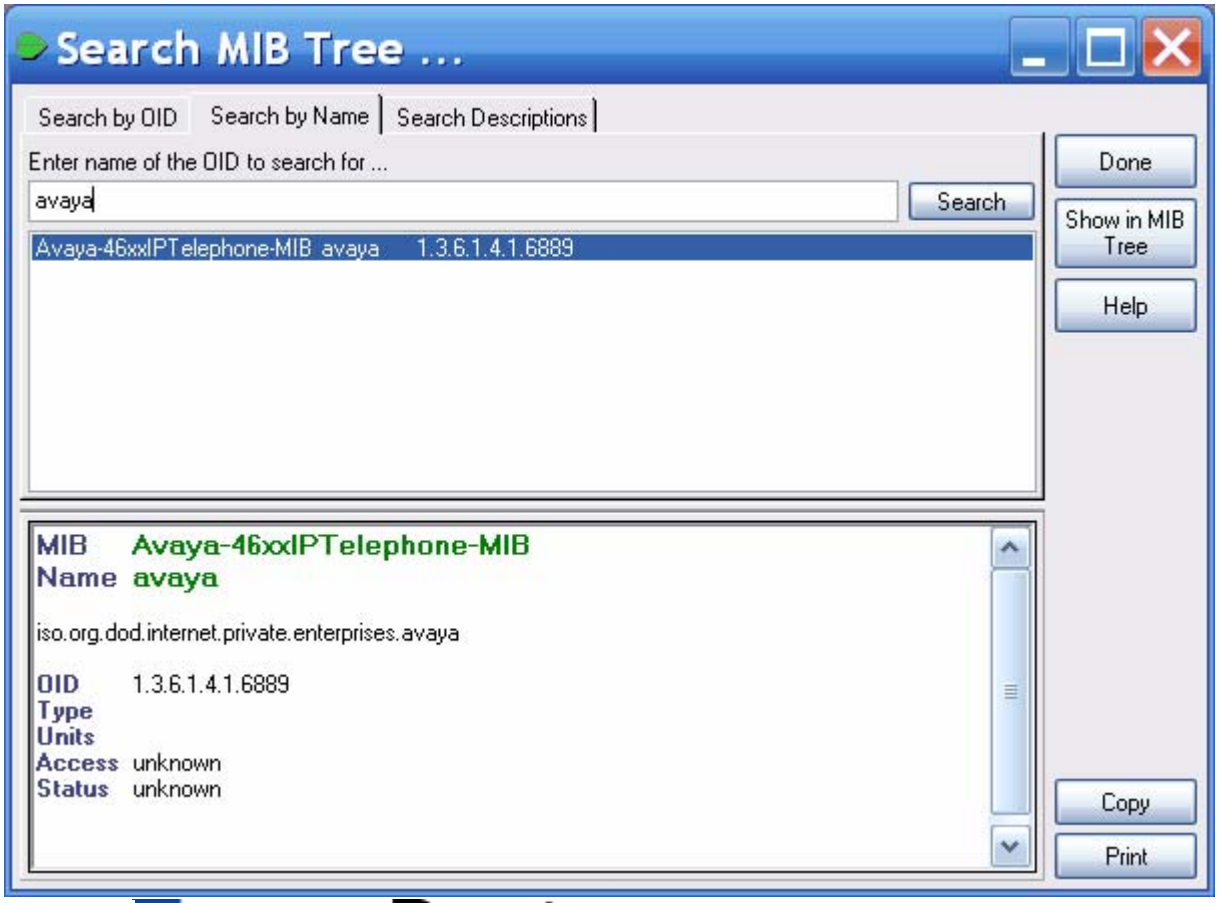
Some vendors offer more secure alternatives

Firewalls can be used to restrict access to TFTP servers to valid devices

# SNMP Enumeration

- SNMP is enabled on some VoIP phones
- Simple SNMP sweeps will garner lots of juicy information
- If you know the device type, you can use the tool snmpwalk with the specific OID
- Find the OID using Solarwinds MIB database

# SNMP Enumeration



# SNMP Enumeration

```
[root@domain2 ~]# snmpwalk -c public -v 1 192.168.1.53 1.3.6.1.4.1.6889
SNMPv2-SMI::enterprises.6889.2.69.1.1.1.0 = STRING: "Obsolete"
SNMPv2-SMI::enterprises.6889.2.69.1.1.2.0 = STRING: "4620D01B"
SNMPv2-SMI::enterprises.6889.2.69.1.1.3.0 = STRING: "AvayaCallserver"
SNMPv2-SMI::enterprises.6889.2.69.1.1.4.0 = IpAddress: 192.168.1.103
SNMPv2-SMI::enterprises.6889.2.69.1.1.5.0 = INTEGER: 1719
SNMPv2-SMI::enterprises.6889.2.69.1.1.6.0 = STRING: "051612501065"
SNMPv2-SMI::enterprises.6889.2.69.1.1.7.0 = STRING: "700316698"
SNMPv2-SMI::enterprises.6889.2.69.1.1.8.0 = STRING: "051611403489"
SNMPv2-SMI::enterprises.6889.2.69.1.1.9.0 = STRING: "00:04:0D:50:40:B0"
SNMPv2-SMI::enterprises.6889.2.69.1.1.10.0 = STRING: "100"
SNMPv2-SMI::enterprises.6889.2.69.1.1.11.0 = IpAddress: 192.168.1.53
SNMPv2-SMI::enterprises.6889.2.69.1.1.12.0 = INTEGER: 0
SNMPv2-SMI::enterprises.6889.2.69.1.1.13.0 = INTEGER: 0
SNMPv2-SMI::enterprises.6889.2.69.1.1.14.0 = INTEGER: 0
SNMPv2-SMI::enterprises.6889.2.69.1.1.15.0 = STRING: "192.168.1.1"
SNMPv2-SMI::enterprises.6889.2.69.1.1.16.0 = IpAddress: 192.168.1.1
SNMPv2-SMI::enterprises.6889.2.69.1.1.17.0 = IpAddress: 255.255.255.0
...
SNMPv2-SMI::enterprises.6889.2.69.1.4.8.0 = INTEGER: 20
SNMPv2-SMI::enterprises.6889.2.69.1.4.9.0 = STRING: "503"
```

# SNMP Enumeration Countermeasures

Disable SNMP on any devices where it is not needed

Change default public and private community strings

Try to use SNMPv3, which supports authentication

# Agenda

- PART I: Casing the Establishment
- PART II: Exploiting the VoIP Network
- PART III: VoIP Session and Application Hacking
- PART IV: Social Threats
- PART V: VoIP Security Trends

# Attacking The Network

The VoIP network and supporting infrastructure are vulnerable to attacks

Most attacks will originate inside the network, once access is gained

Attacks include:

- Network infrastructure DoS
- Network eavesdropping
- Network and application interception

# Attacking The Network
# Gaining Access

Several attack vectors include:

- Installing a simple wired hub
- Wi-Fi sniffing
- Compromising a network node
- Compromising a VoIP phone
- Compromising a switch
- Compromising a proxy, gateway, or PC/softphone
- ARP poisoning
- Circumventing VLANs

# Attacking The Network Gaining Access

Some techniques for circumventing VLANs:

- If MAC filtering is not used, you can disconnect a VoIP phone and connect a PC
- Even if MAC filtering is used, you can easily spoof the MAC
- Be especially cautious of VoIP phones in public areas (such as lobby phones)

# Attacking The Network
# Gaining Access

Some other VLAN attacks:

- MAC flooding attack
- 802.1q and ISL tagging attack
- Double-encapsulated 802.1q/Nested VLAN attack
- Private VLAN attack
- Spanning-tree protocol attack
- VLAN trunking protocol attack

# Network Infrastructure DoS

The VoIP network and supporting infrastructure are vulnerable to attacks

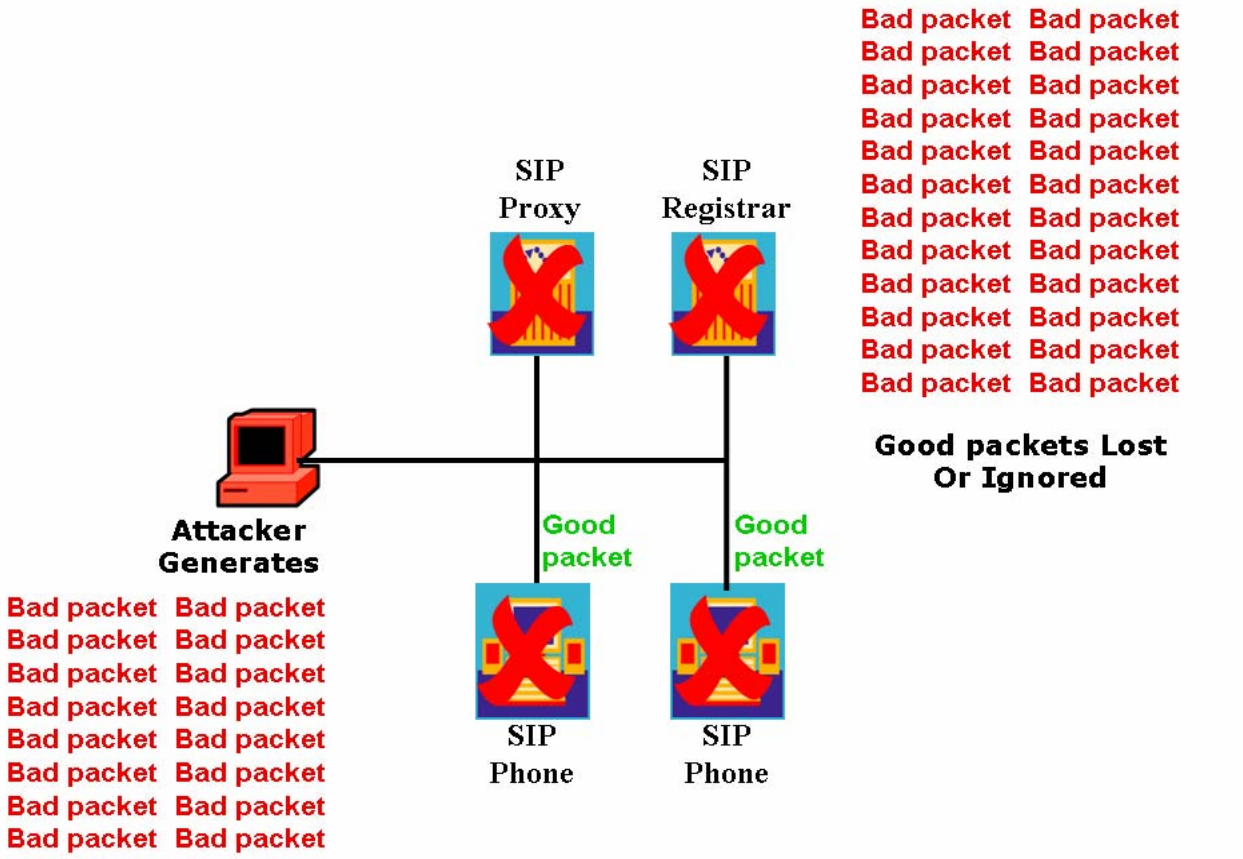
VoIP media/audio is particularly susceptible to any DoS attack which introduces latency and jitter

Attacks include:

- Flooding attacks
- Network availability attacks
- Supporting infrastructure attacks

# Flooding Attacks Introduction

Flooding attacks generate so many packets at a target, that it is overwhelmed and can't process legitimate requests



# Flooding Attacks
# Call Quality

VoIP is much more sensitive to network issues than traditional data applications like web and email:

- Network Latency – amount of time it takes for a packet to travel from the speaker to the listener
- Jitter – occurs when the speaker sends packets at constant rates but they arrive at the listener at variable rates
- Packet Loss – occurs under heavy load and oversubscription

Mean Opinion Score – subjective quality of a conversation measured from 1 (unintelligible) to 5 (very clear)

R-value – mathematical measurement from 1 (unintelligible) to 100 (very clear)

# Flooding Attacks
# Call Quality

Software applications (wireshark, adventnet, Wildpackets, etc.)

Hardware Appliances (Aglient, Empirix, Qovia,, etc.)

Integrated router and switches (e.g. Cisco QoS Policy Manager)

# Flooding Attacks
# Types of Floods

Some types of floods are:

- UDP floods
- TCP SYN floods
- ICMP and Smurf floods
- Worm and virus oversubscription side effect
- QoS manipulation
- Application flooding

# Flooding Attacks Countermeasures

Layer 2 and 3 QoS mechanisms are commonly used to give priority to VoIP media (and signaling)

Use rate limiting in network switches

Use anti-DoS/DDoS products

Some vendors have DoS support in their products (in newer versions of software)

# Network Availability Attacks

This type of attack involves an attacker trying to crash the underlying operating system:

- Fuzzing involves sending malformed packets, which exploit a weakness in software
- Packet fragmentation
- Buffer overflows

# Network Availability Attacks Countermeasures

A network IPS is an inline device that detects and blocks attacks

Some firewalls also offer this capability

Host based IPS software also provides this capability

# Supporting Infrastructure Attacks

VoIP systems rely heavily on supporting services such as DHCP, DNS, TFTP, etc.

DHCP exhaustion is an example, where a hacker uses up all the IP addresses, denying service to VoIP phones

DNS cache poisoning involves tricking a DNS server into using a fake DNS response

# Supporting Infrastructure Attacks Countermeasures

Configure DHCP servers not to lease addresses to unknown MAC addresses

DNS servers should be configured to analyze info from non-authoritative servers and dropping any response not related to queries

# Network Interception Introduction

The VoIP network is vulnerable to Man-In-The-Middle (MITM) attacks, allowing:

- Eavesdropping on the conversation
- Causing a DoS condition
- Altering the conversation by omitting, replaying, or inserting media
- Redirecting calls

Attacks include:

- Network-level interception
- Application-level interception

# Network Interception
# ARP Poisoning

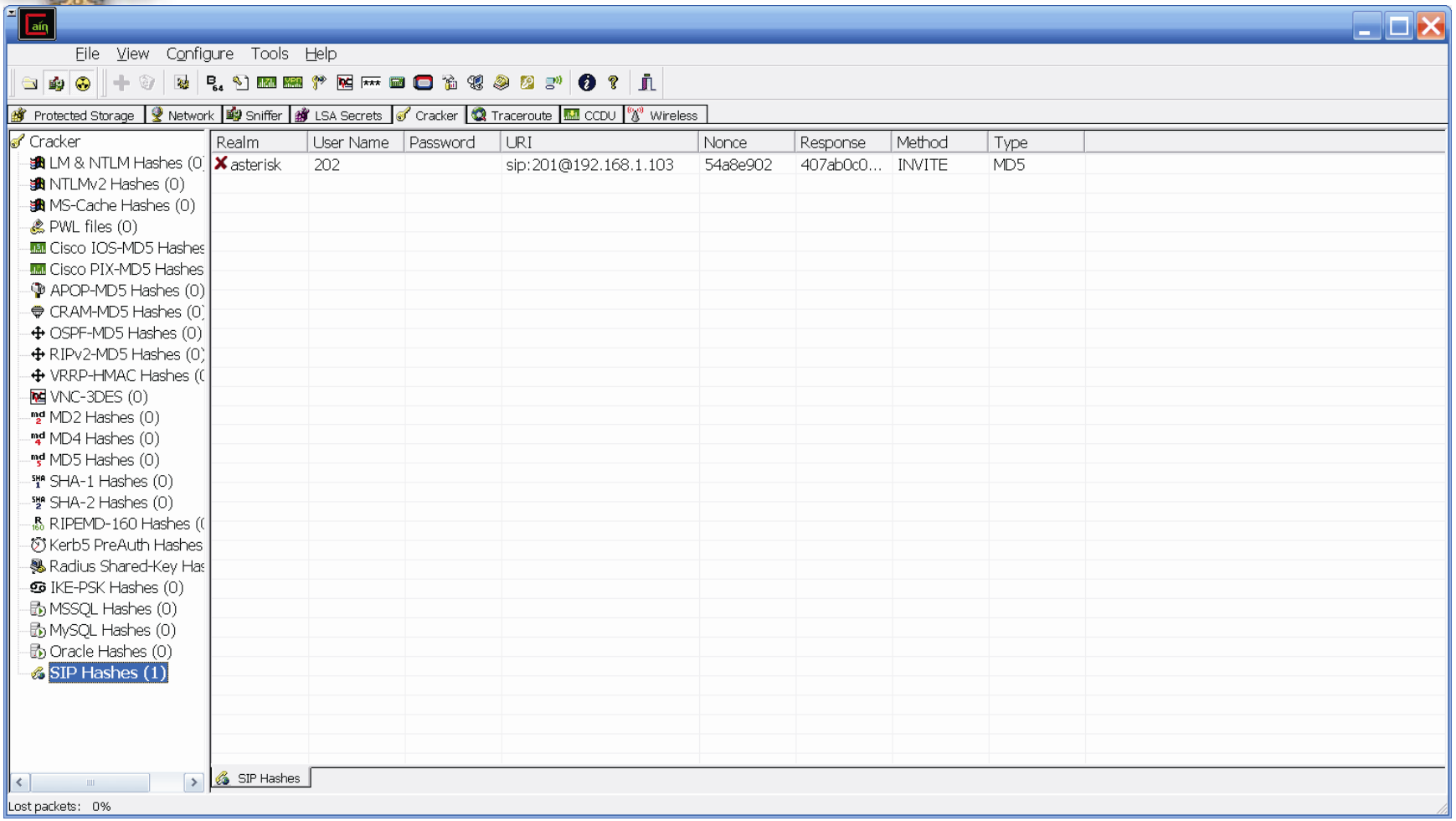
The most common network-level MITM attack is ARP poisoning

Involves tricking a host into thinking the MAC address of the attacker is the intended address

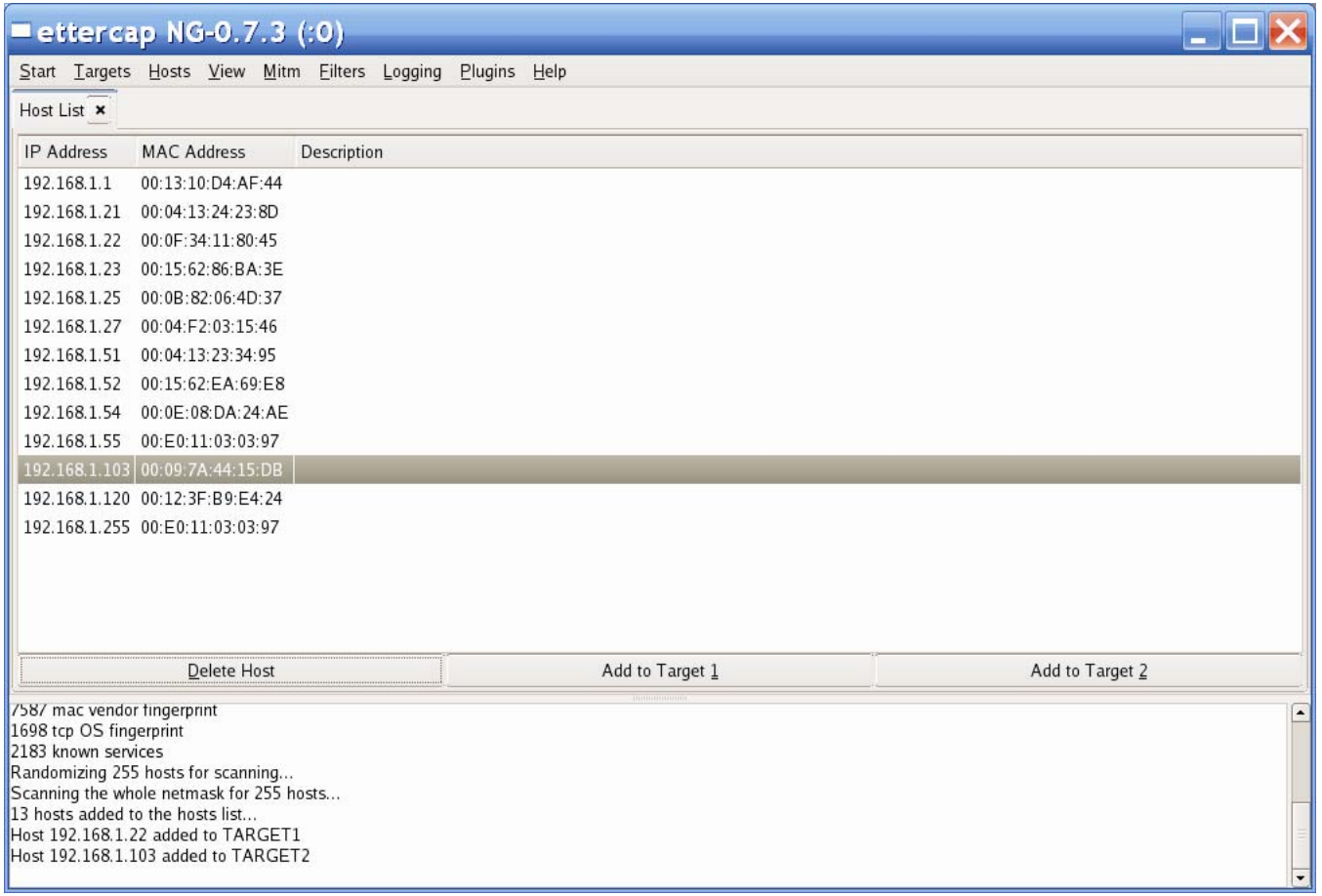
There are a number of tools available to support ARP poisoning:

- Cain and Abel
- ettercap
- Dsniff
- hunt

# Network Interception
# ARP Poisoning



# Network Interception
# ARP Poisoning



# Network Interception Countermeasures

Some countermeasures for ARP poisoning are:

- Static OS mappings
- Switch port security
- Proper use of VLANs
- Signaling encryption/authentication
- ARP poisoning detection tools, such as arpwatch

# Network Eavesdropping Introduction

VoIP signaling, media, and configuration files are vulnerable to eavesdropping

Attacks include:

- TFTP configuration file sniffing
- Number harvesting and call pattern tracking
- Conversation eavesdropping

# TFTP/Numbers/Call Patterns

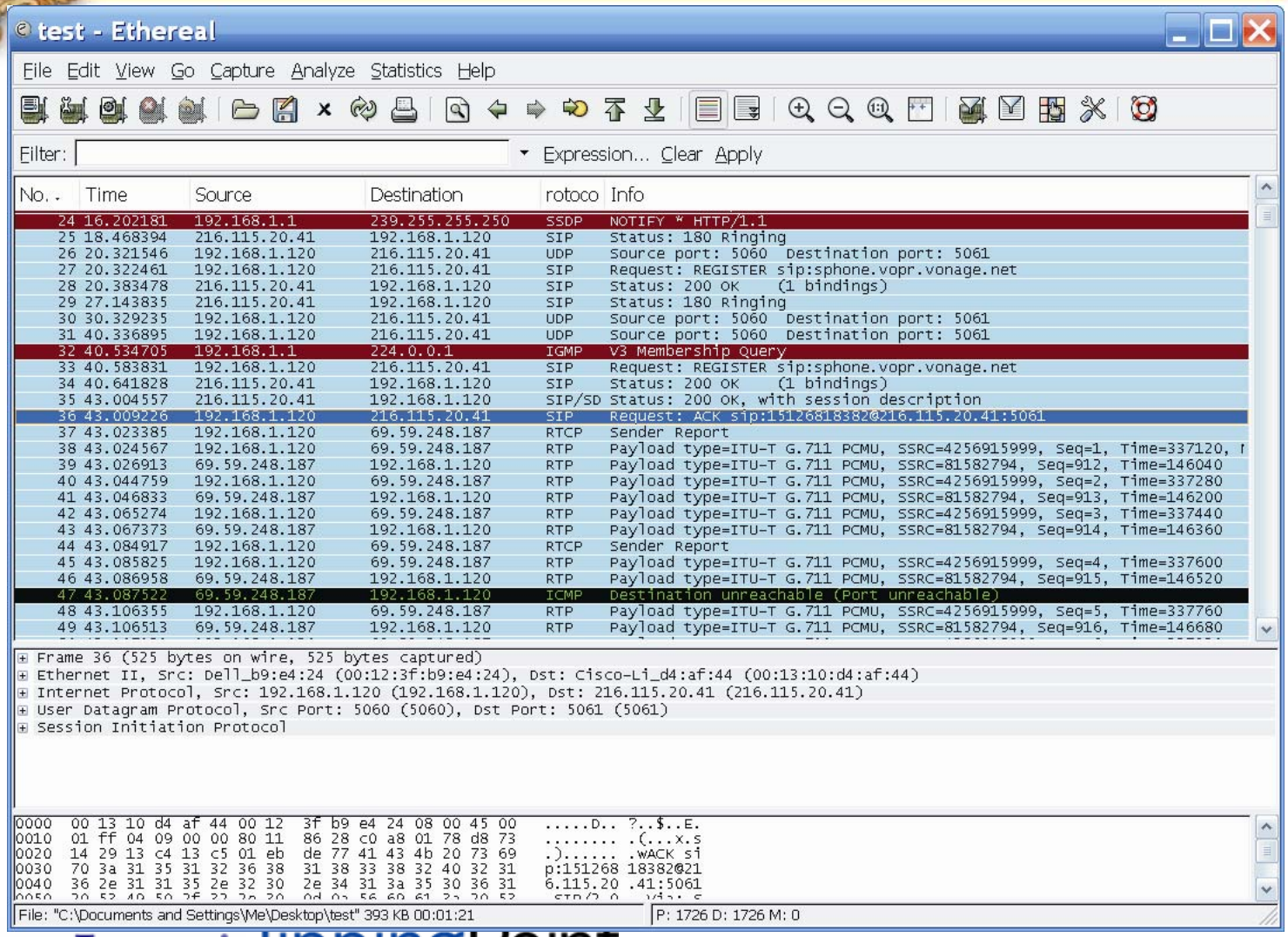
TFTP files are transmitted in the clear and can be sniffed

One easy way is to connect a hub to a VoIP phone, reboot it, and capture the file

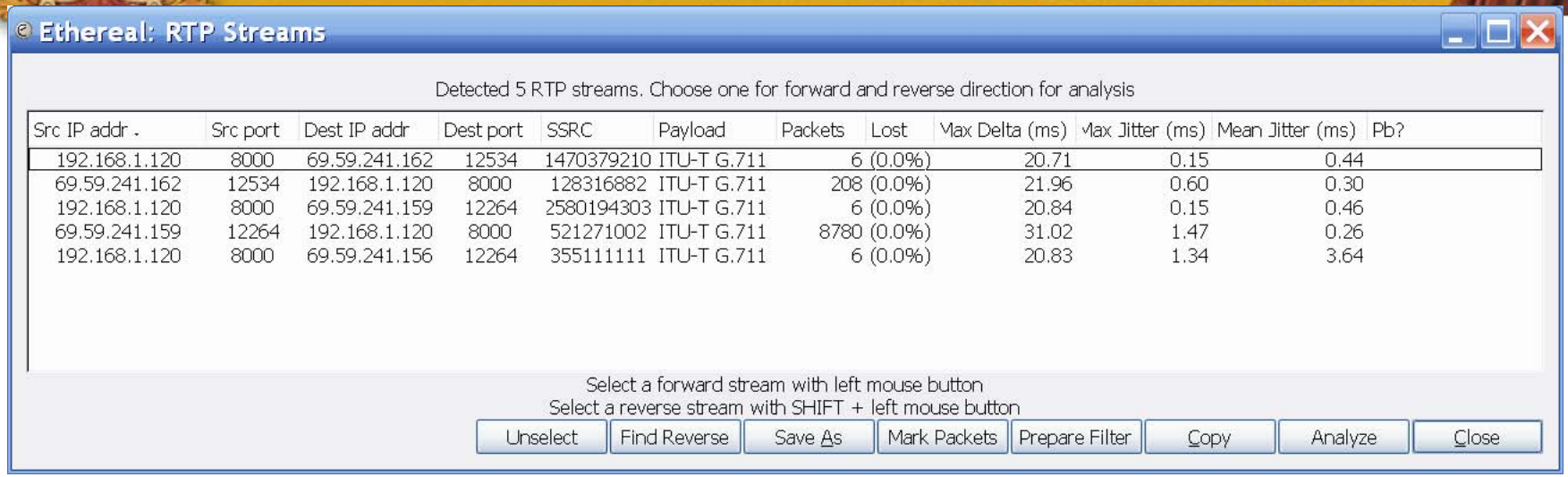
By sniffing signaling, it is possible to build a directory of numbers and track calling patterns

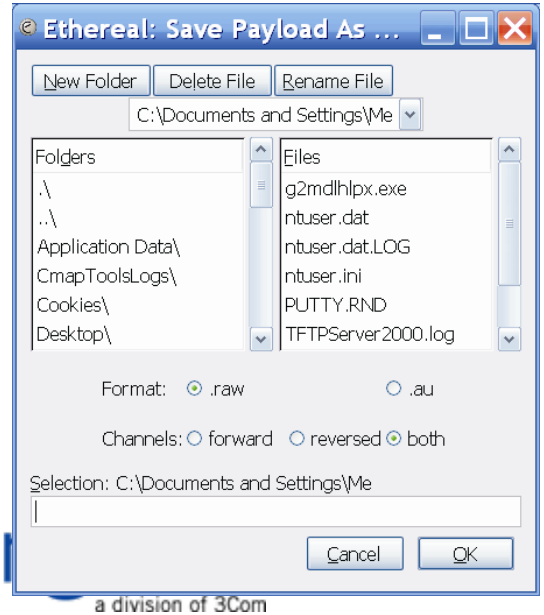
voipong automates the process of logging all calls

# Conversation Recording Wireshark

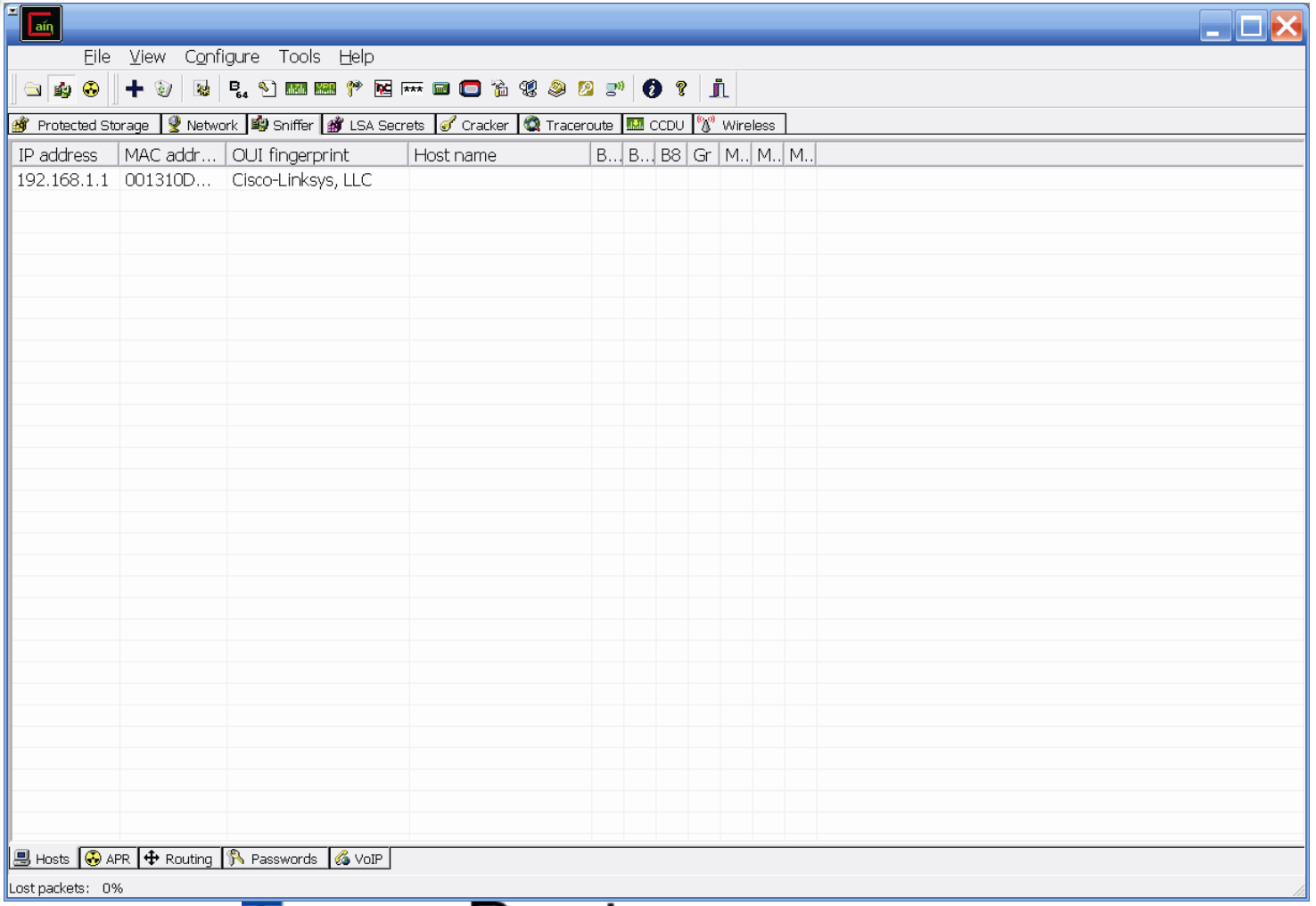


# Conversation Recording Wireshark



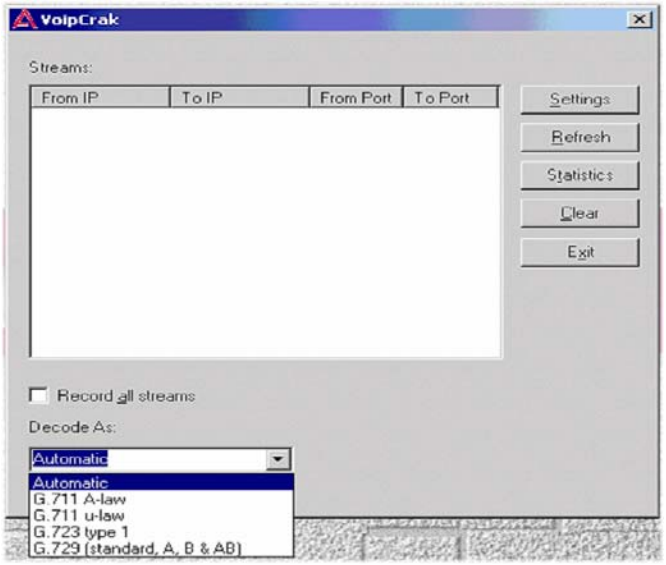
# Conversation Recording
# Cain And Abel

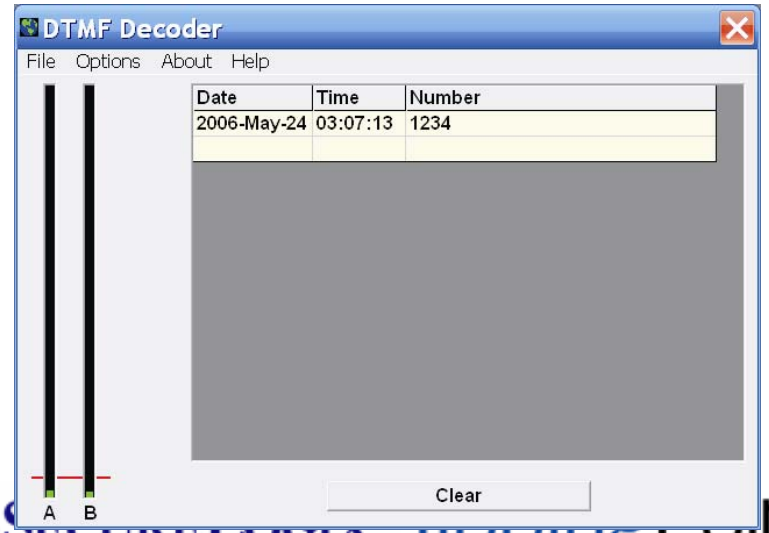


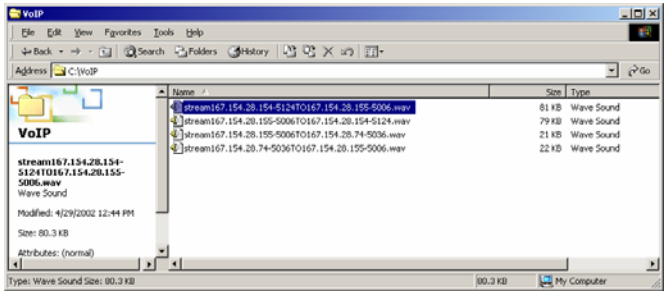
# Conversation Recording Other Tools

Other tools include:

- vomit
- Voipong
- voipcrack (not public)
- DTMF decoder



# Network Eavesdropping Countermeasures

Place the TFTP server on the same VLAN as the VoIP phones and use a firewall to ensure that only VoIP phones communicate with it

Use encryption:

- Many vendors offer encryption for signaling
  - Use the Transport Layer Security (TLS) for signaling
- Many vendors offer encryption for media
  - Use Secure Real-time Transport Protocol (SRTP)
- Use ZRTP
- Use proprietary encryption if you have to

# Agenda

- PART I: Casing the Establishment
- PART II: Exploiting the VoIP Network
- PART III: VoIP Session and Application Hacking
- PART V: Social Threats
- PART V: VoIP Security Trends

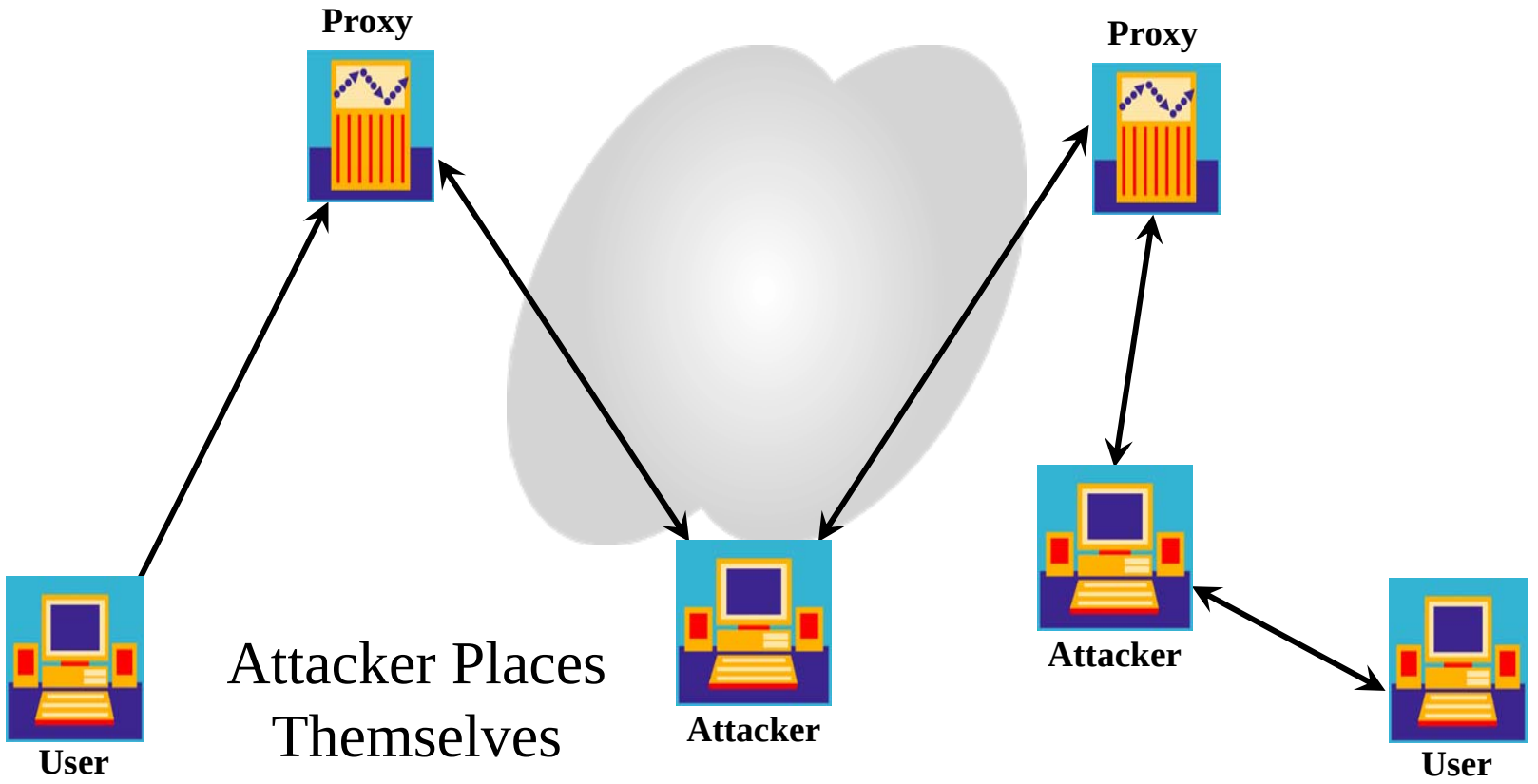
# Application Interception Introduction

It is also possible to perform a MITM attack at the application layer

Some possible ways to perform this attack include:

- Registration hijacking
- Redirection attacks
- VoIP phone reconfiguration
- Inserting a bridge via physical network access

# Application Interception




Attacker Places Themselves Between Proxies Or Proxy/UA

# Application Interception Countermeasures

Some countermeasures to application-level interception are:

- Use VLANs for separation
- Use TCP/IP
- Use signaling encryption/authentication (such as TLS)
- Enable authentication for requests
- Deploy SIP firewalls to protect SIP proxies from attacks

# Fuzzing

- Functional protocol testing (also called “fuzzing”) is a popular way of finding bugs and vulnerabilities.
- Fuzzing involves creating different types of packets for a protocol which contain data that pushes the protocol's specifications to the point of breaking them.
- These packets are sent to an application, operating system, or hardware device capable of processing that protocol, and the results are then monitored for any abnormal behavior (crash, resource consumption, etc.).

# Fuzzing

- Fuzzing has already led to a wide variety of Denial of Service and Buffer Overflow vulnerability discoveries in vendor implementations of VoIP products that use H.323 and SIP.
- PROTOS group from the University of Oulu in Finland responsible for high exposure vulnerability disclosures in HTTP, LDAP, SNMP, WAP, and VoIP.
- http://www.ee.oulu.fi/research/ouspg/protos/index.html

# 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: 9656141892590 9@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: 168

v=0
o=- 238540244 238540244 IN IP4 192.168.22.36
s=VOVIDA Session
c=IN IP4 192.168.22.36
t=3174844751 0
m=audio 23456 RTP/AVP 0
a=rtpmap:0 PCMU/8000
a=ptime:20
```

SDP Payload

SECURELOGIX CORPORATION TippingPoint a division of 3Com

RSACONFERENCE2007

# Fuzzing

```
INVITE sip:6713@192.168.26.180:6060;user=phone SIP/2.0
Via: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
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: 9656141892590 9@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: 168

v=0
o=- 238540244 238540244 IN IP4 192.168.22.36
s=VOVIDA Session
c=IN IP4 192.168.22.36
t=3174844751 0
m=audio 23456 RTP/AVP 0
a=rtpmap:0 PCMU/8000
a=ptime:20
```

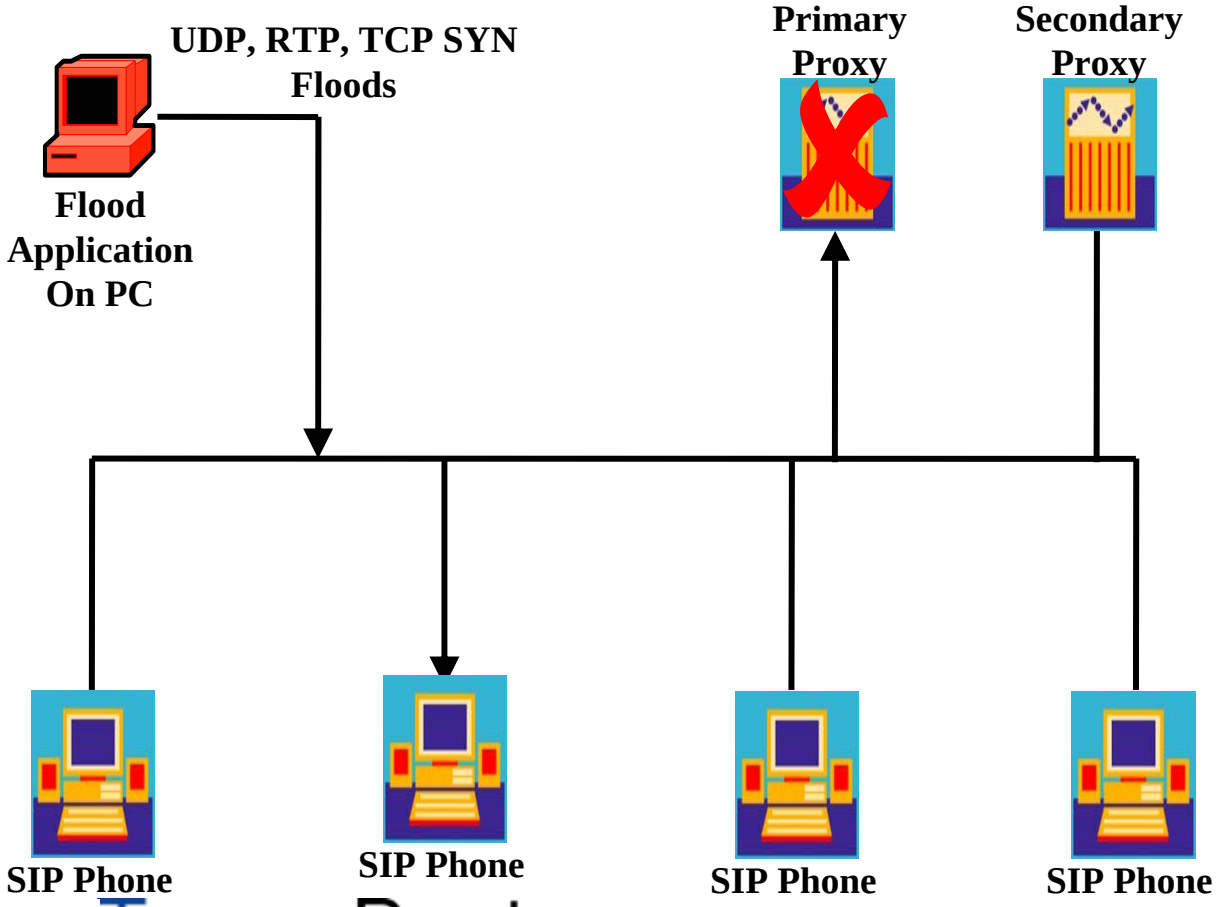
SDP Payload

# Fuzzing

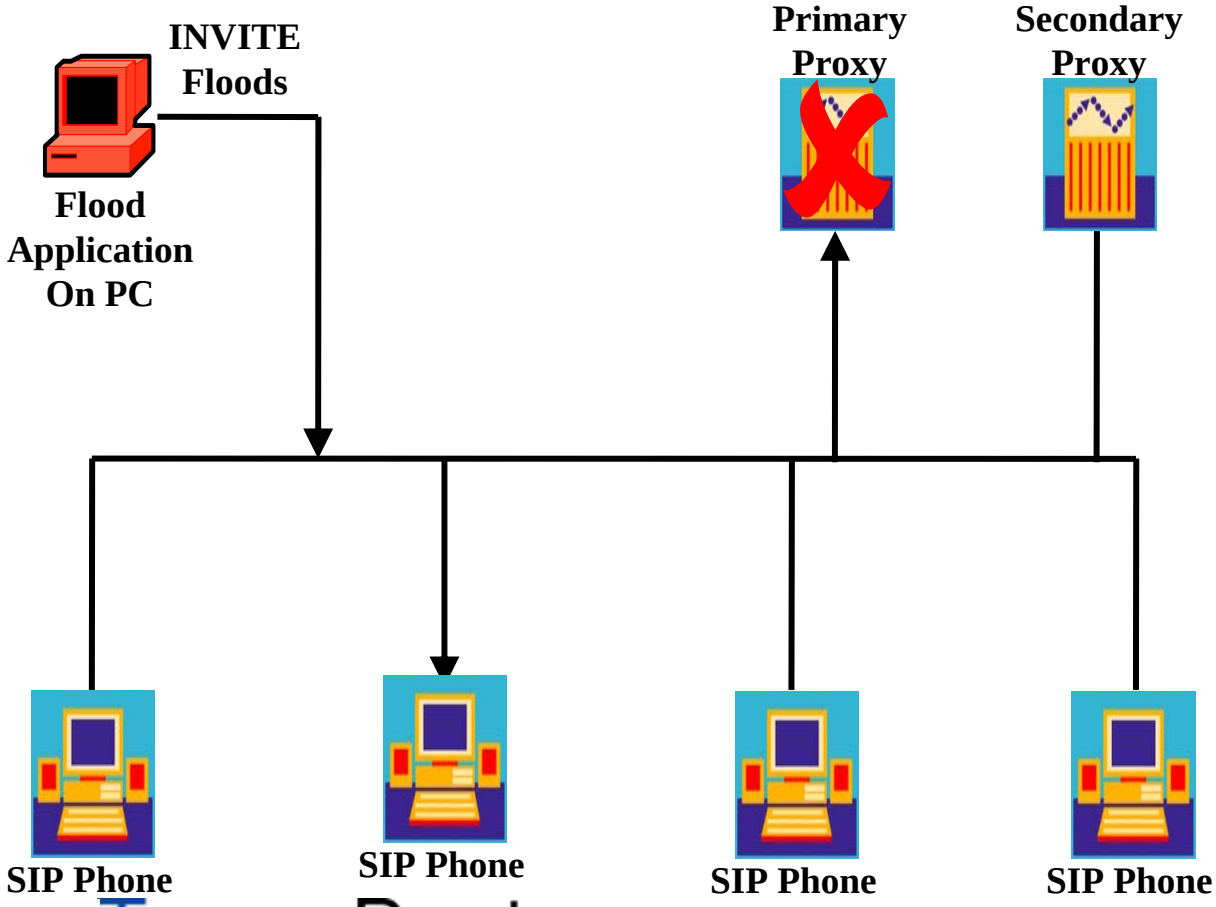
Fuzzing VoIP protocol implementations is only at the tip of the iceberg:

- Intelligent Endpoint Signaling
  - **SIP/CMSS**
  - **H.225/H.245/RAS**
- Master-Slave Endpoint Signaling
  - **MGCP/TGCP/NCS**
  - **Megaco/H.248**
  - **SKINNY/SCCP**
  - **Q.931+**
- SS7 Signaling Backhaul
  - **SIGTRAN**
  - **ISTP**
  - **SS7/RUDP**
- Accounting/Billing
  - **RADIUS**
  - **COPS**
- Media Transfer
  - **RTP**
  - **RTCP**

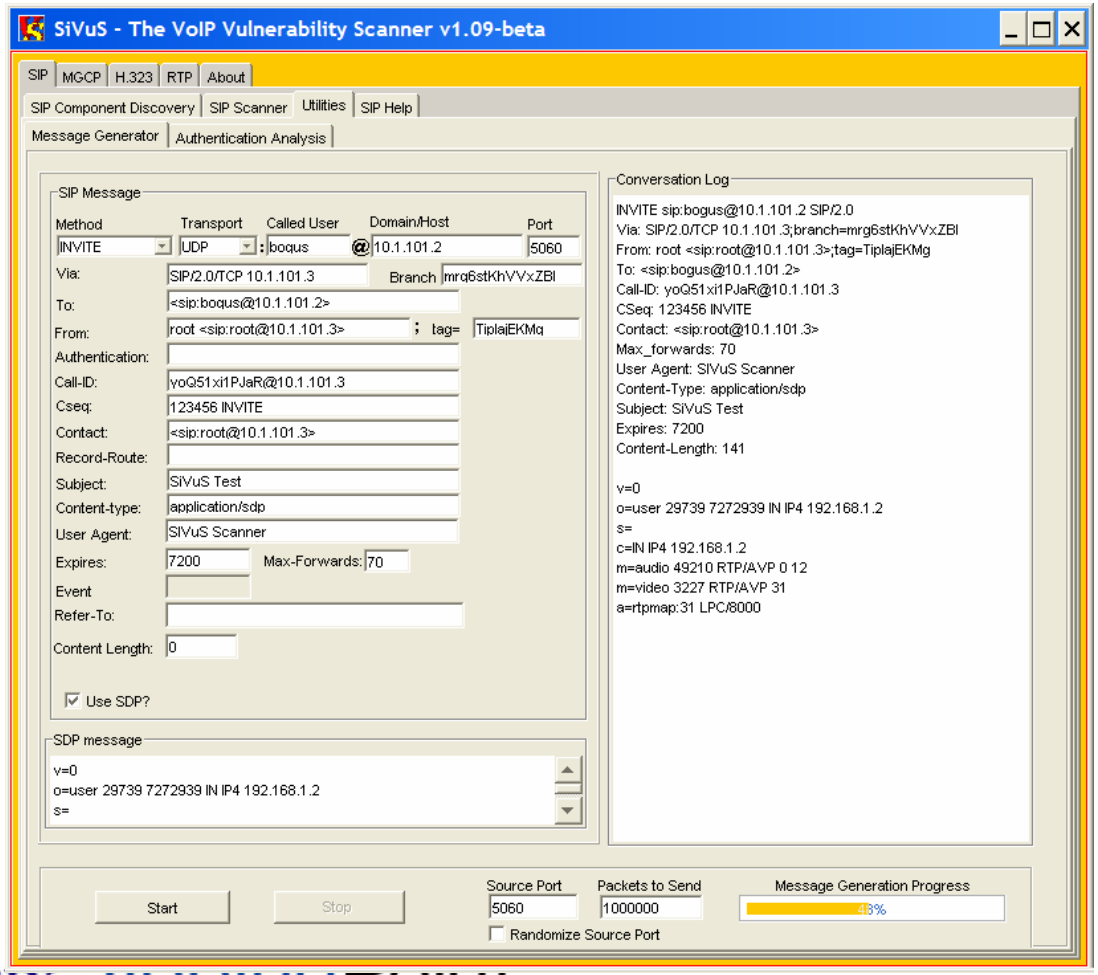
# Disruption of Service



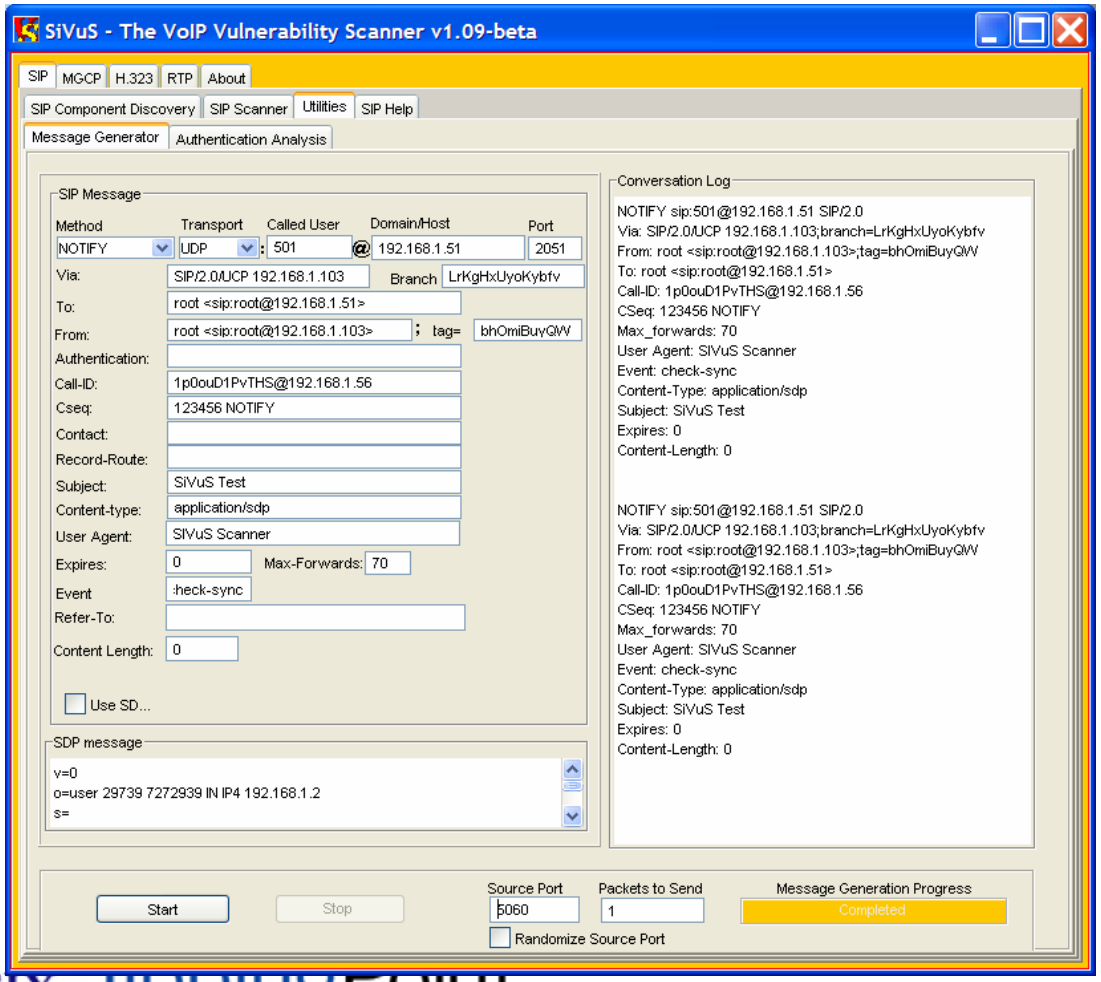
# Disruption of Service



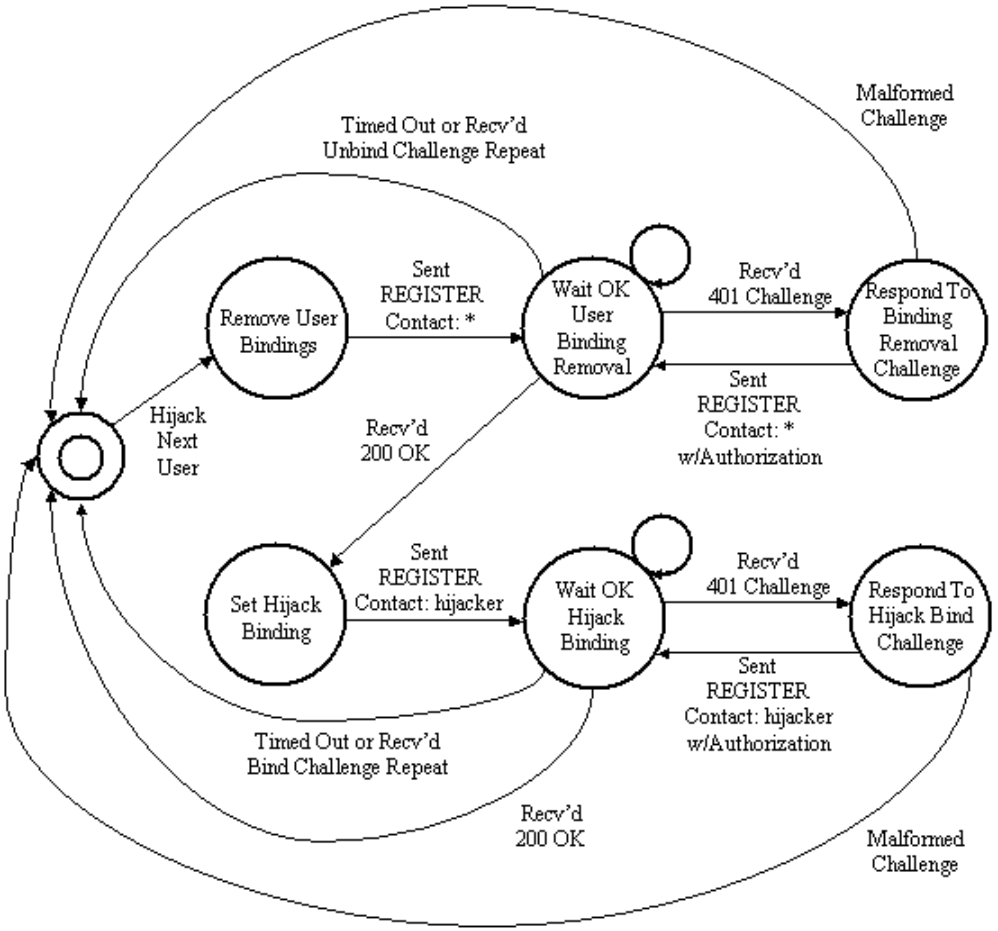
# INVITE Flood



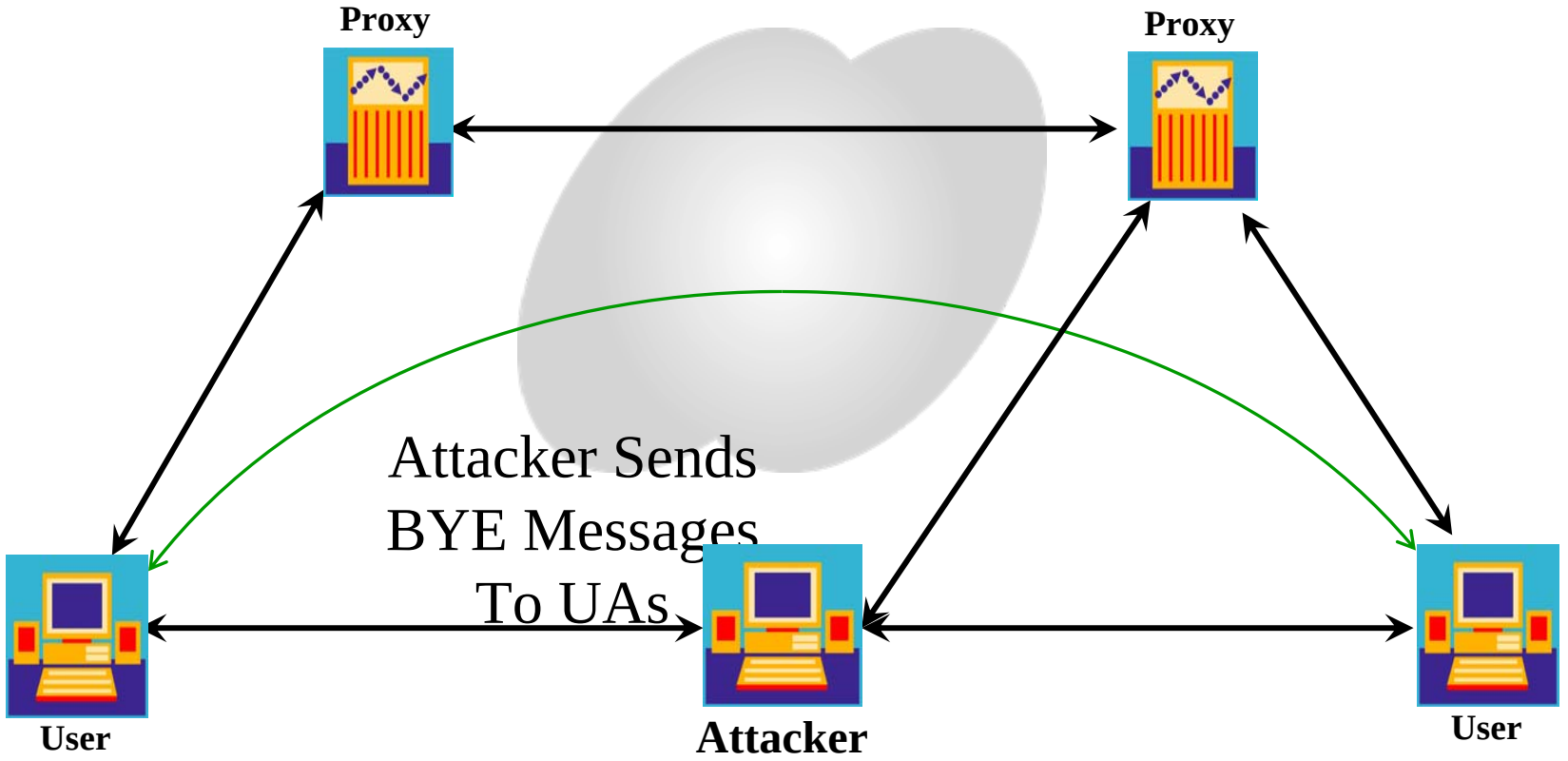
# Check Sync Reboot



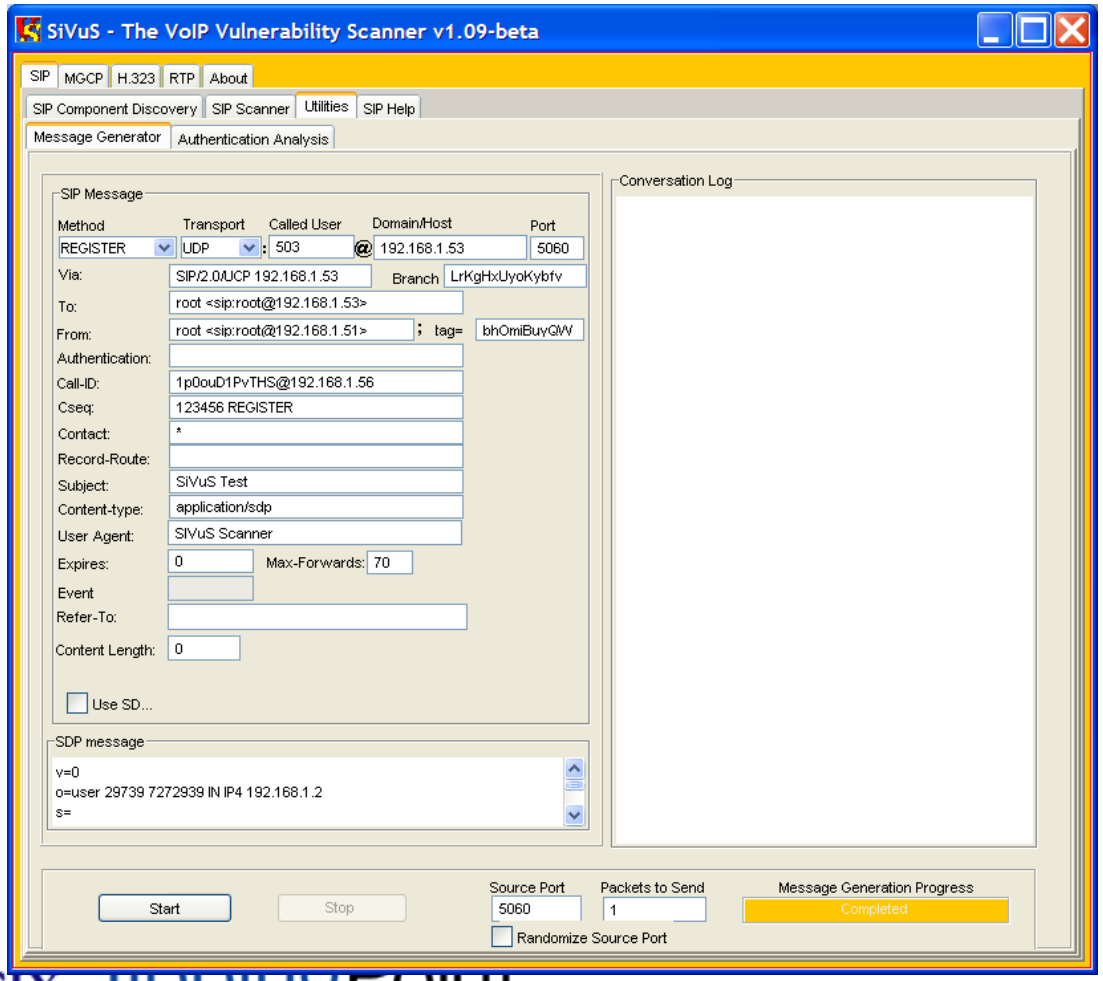
# Signaling Manipulation



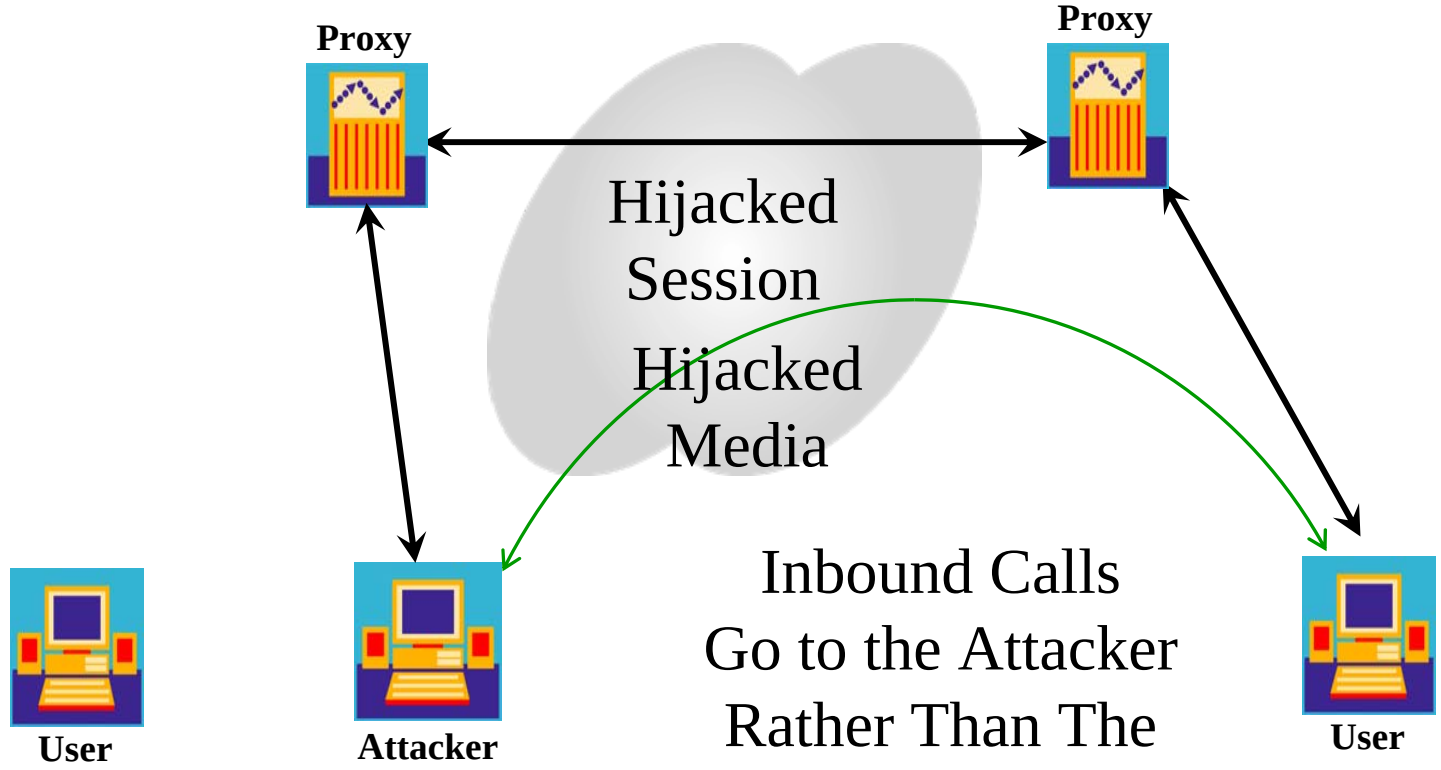
# Signaling Manipulation



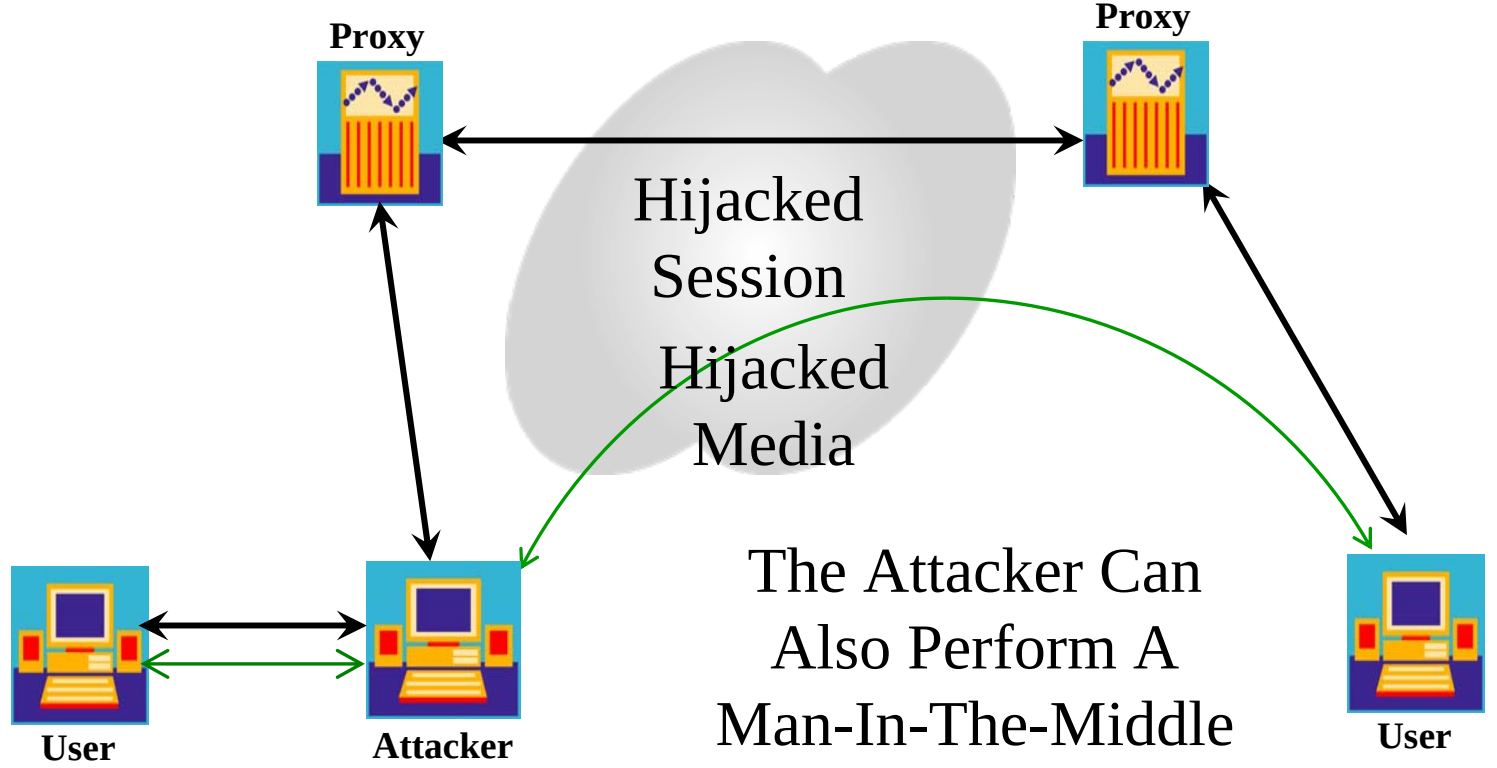
# Erase Registrations



# Signaling Manipulation



# Signaling Manipulation




The Attacker Can Also Perform A Man-In-The-Middle Attack

# Agenda

- PART I: Casing the Establishment
- PART II: Exploiting the VoIP Network
- PART III: VoIP Session and Application Hacking
- **PART V: Social Threats**
- PART V: VoIP Security Trends

# SPIT






SECURELOGIX CORPORATION TippingPoint a division of 3Com

RSA CONFERENCE 2007

# SPIT

- Asterisk (http://www.asterisk.org) turns out to be a fairly useful tool for performing SPIT.
- Trixbox (http://www.trixbox.org) is the single CD ISO with Asterisk and lots of management tools.
- Spitter is a tool we released at http://www.hackingvoip.com

# SPIT

- Popularity Dialer (http://www.popularitydialer.com) is an example of what Asterisk can be modified to do
- Used to send phone calls with prerecorded conversation in the future

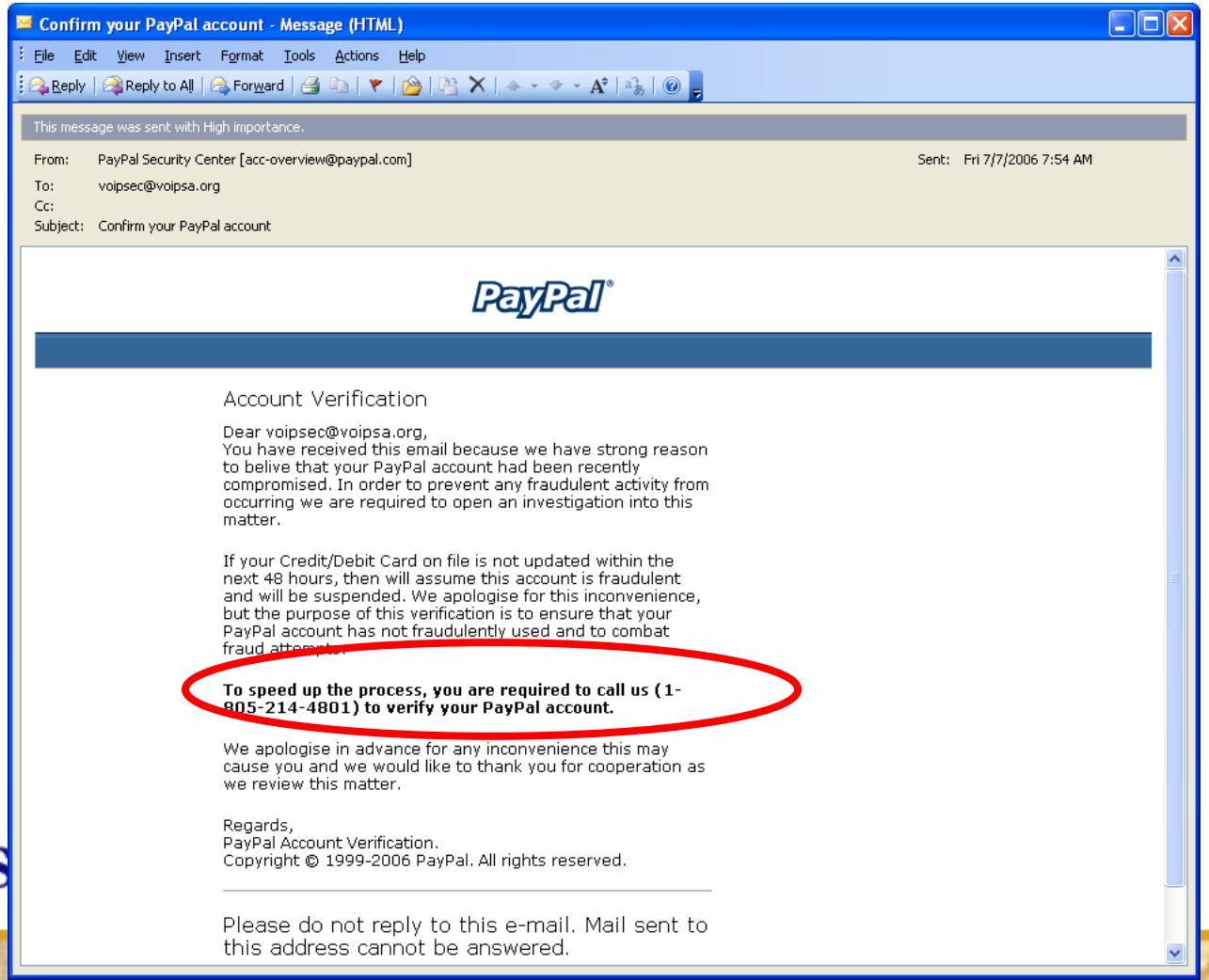
# VoIP Phishing

- “Hi, this is Bob from Bank of America calling.  Sorry I missed you.  If you could give us a call back at 1-866-555-1324 we have an urgent issue to discuss with you about your bank account.”

- Hello.  This is Bank of America.  So we may best serve you, please enter your account number followed by your PIN.

# VoIP Security Trends

- This year also saw the emergence of *Voice Phishing:*



# VoIP Security Trends

- When victims dial the phone number, the recording requests that they enter their account number.
- Hacker comes back later and reconstructs the touch tones that were recorded by the backend VoIP system
- A presentation at Black Hat Las Vegas this past August demonstrated how easy it was to set up a malicious spoofed VoIP answering system.

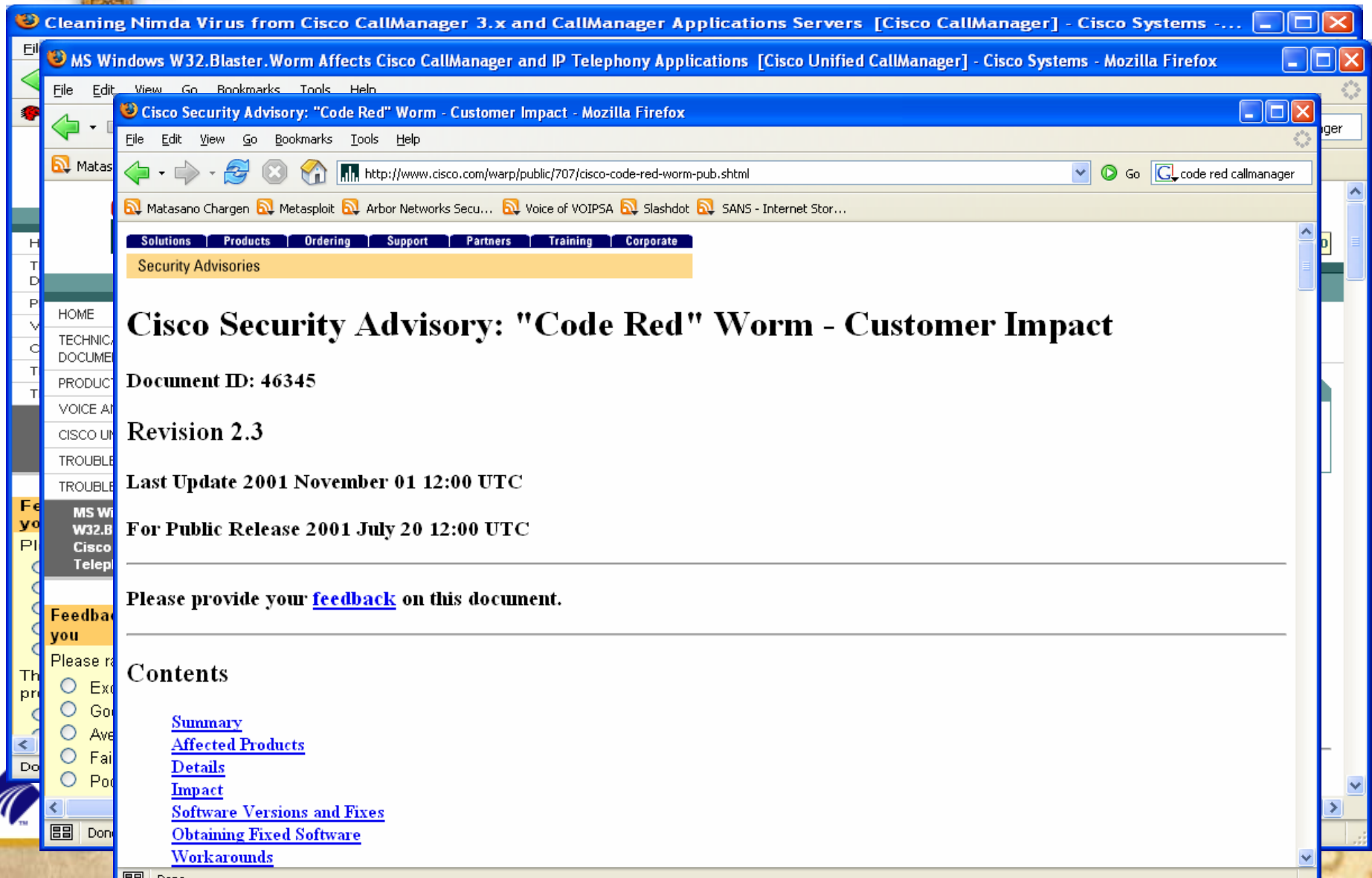
# Agenda

- PART I: Casing the Establishment
- PART II: Exploiting the VoIP Network
- PART III: VoIP Session and Application Hacking
- PART V: Social Threats
- PART V: VoIP Security Trends

# VoIP Security Trends

- Traditionally, the most prevalent threats to VoIP have been the same that have plagued data networks for years: worms, denial of service, and exploitation of the supporting infrastructure (routers, Windows servers, etc.) – see next slide.
- The hacking community however has started to show greater interest in VoIP – one measure is that there was an entire track on VoIP security at the Blackhat conference in Las Vegas
- More and more VoIP specific attack tools are being developed and released. The tools are becoming more sophisticated and easy to use.

# Example of Data Threats affecting VoIP



# VoIP Security Trends

- VoIP technology has seen rapid adoption during the past year. At the same time, there has been an increase in security scrutiny of typical components of a VoIP network such as the call proxy and media servers and the VoIP phones themselves.
- Various products such as Cisco Unified Call Manager, Asterisk and a number of VoIP phones from various vendors have been found to contain vulnerabilities that can either lead to a crash or a complete control over the vulnerable server/device.
- SANS Top 20 Internet Security Attack Targets (2006 annual update) - VoIP section: http://www.sans.org/top20/#n1

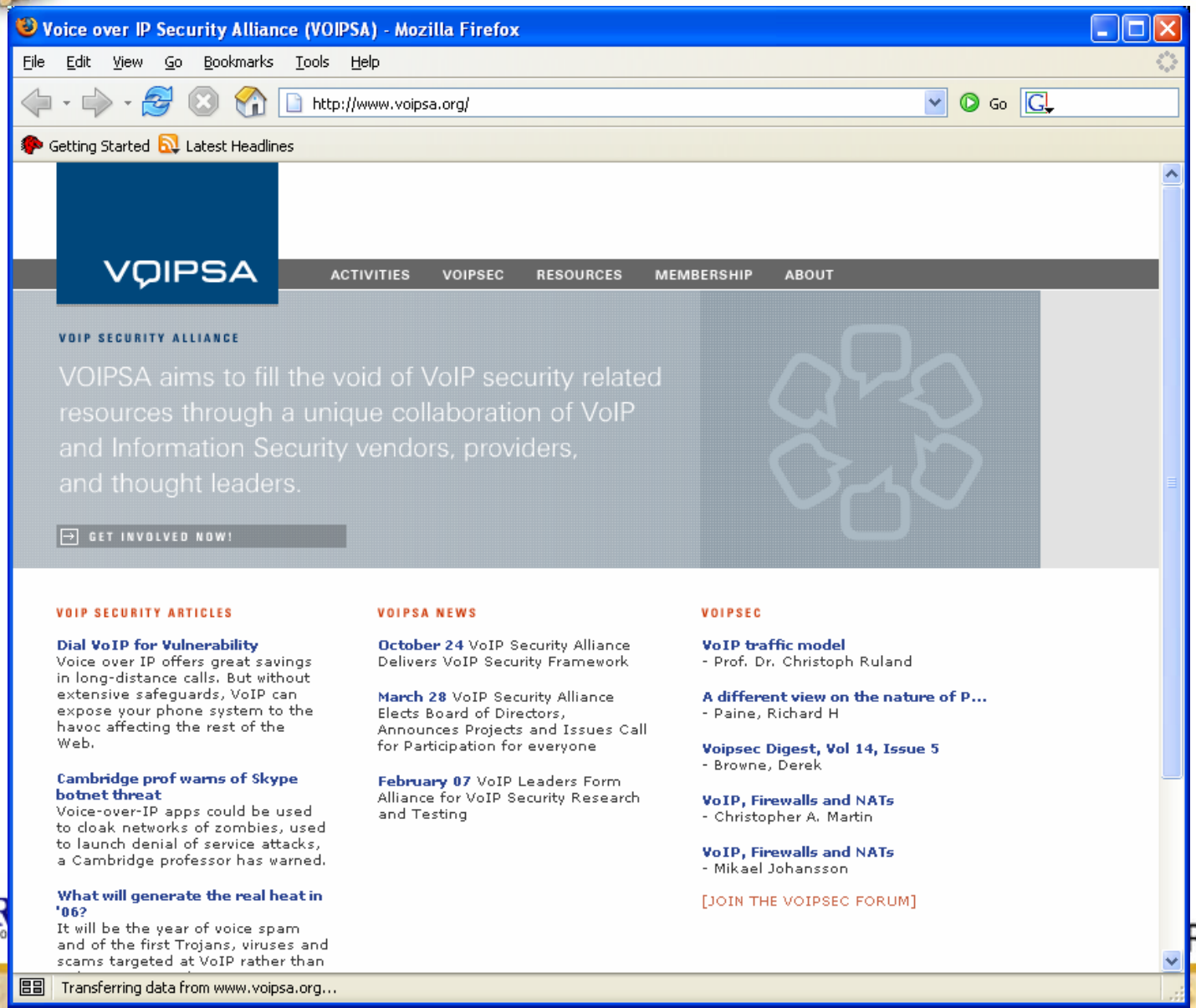
# VoIP Security Trends

- This year also saw the emergence of *Voice Phishing* as a real threat. This has the potential to skyrocket in much the same way spyware and email phishing attacks have.

# VOIPSA Update

- The Voice over IP Security Alliance (VOIPSA) aims to fill the void of VoIP security related resources through a unique collaboration of VoIP and Information Security vendors, providers, and thought leaders. http://www.voipsa.org
- The first industry group focused on VOIP Security (http://www.voipsa.org) on Feb 7th, 2005

# VOIPSA Update



# VOIPSA Update

VOIPSA projects:

- Threat Taxonomy - completed
  Definition of a glossary of terms and a taxonomy to organize and describe types of security threats for use by projects within VOIPSA and communications with the press, industry and public.

Best Practices – About to start formally

# Thank you!

**Dendler@tippingpoint.com**

**Mark.Collier@securelogix.com**

SECURELOGIX CORPORATION TippingPoint a division of 3Com

RSA CONFERENCE 2007