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

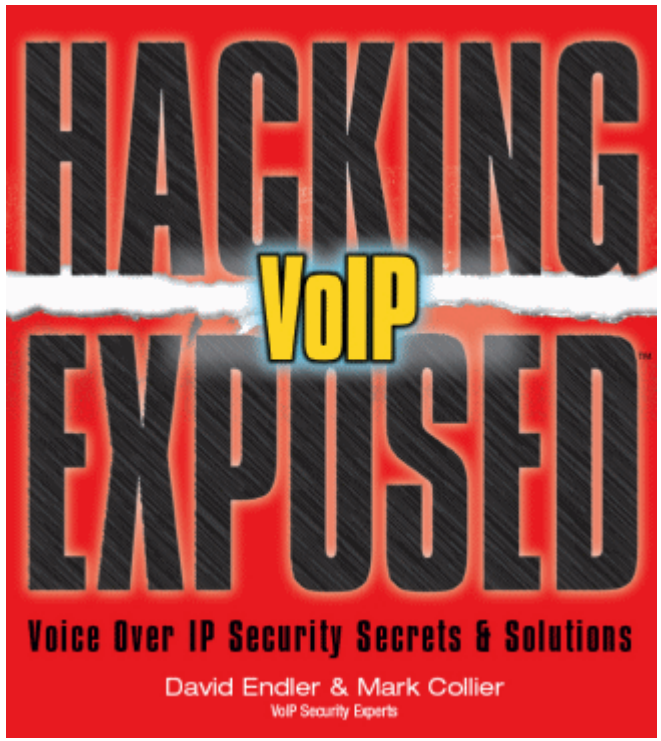
- David Endler, Director of Security Research for TippingPoint, a division of 3Com
- Mark Collier, CTO for SecureLogix Corporation

Shameless Plug

- This presentation includes research for our book coming

  out in December

  http://www.hackingvoip.com

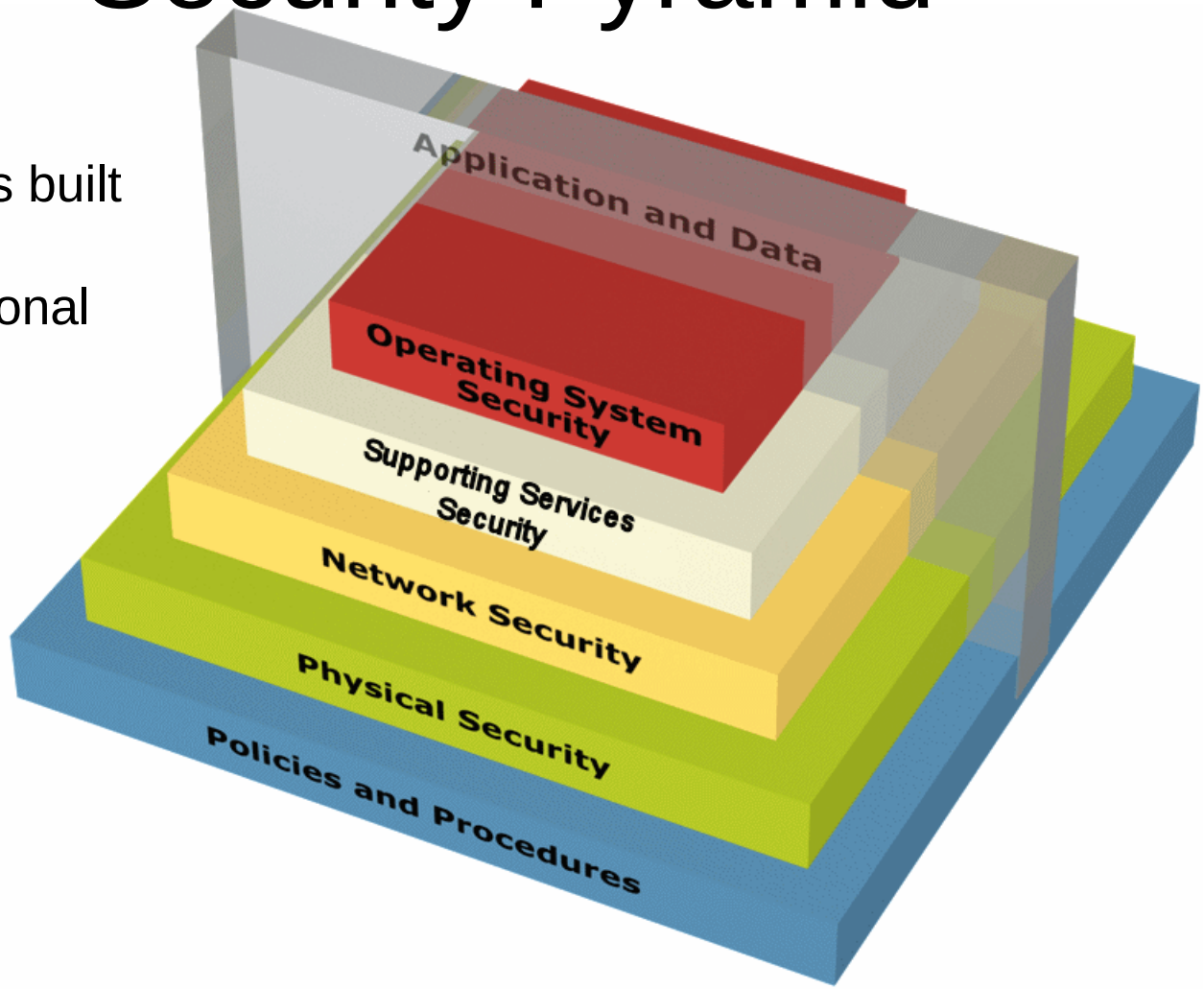


Introduction - VoIP Security

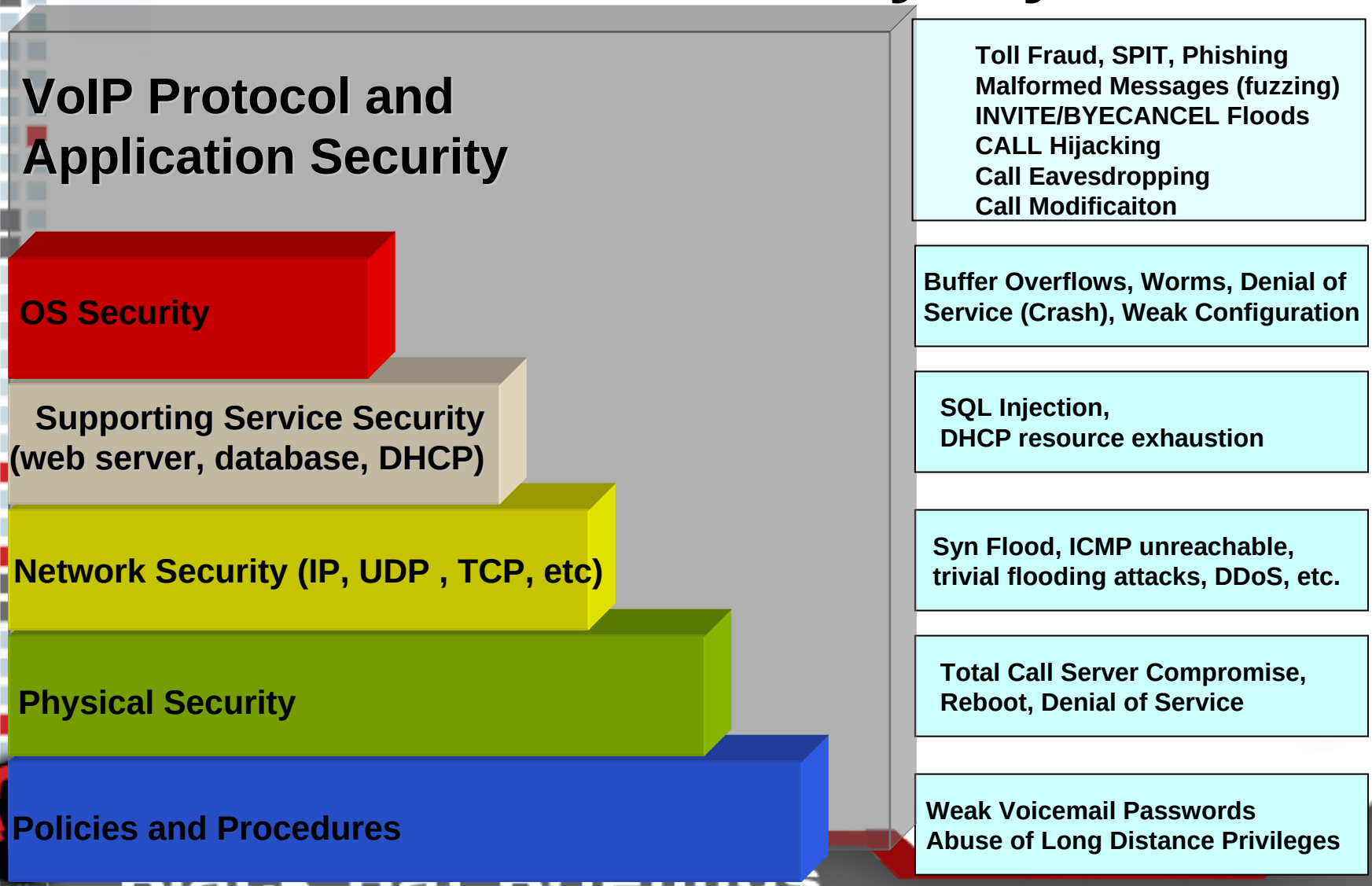
- History has shown that most advances and trends in information technology (e.g. TCP/IP, Wireless 802.11, Web Services, etc.) typically outpace the corresponding realistic security requirements. VoIP is no different.
- As VoIP infrastructure becomes more accessible to the common script kiddie, so will 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



Agenda

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

Demo SIP Test Bed

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. "

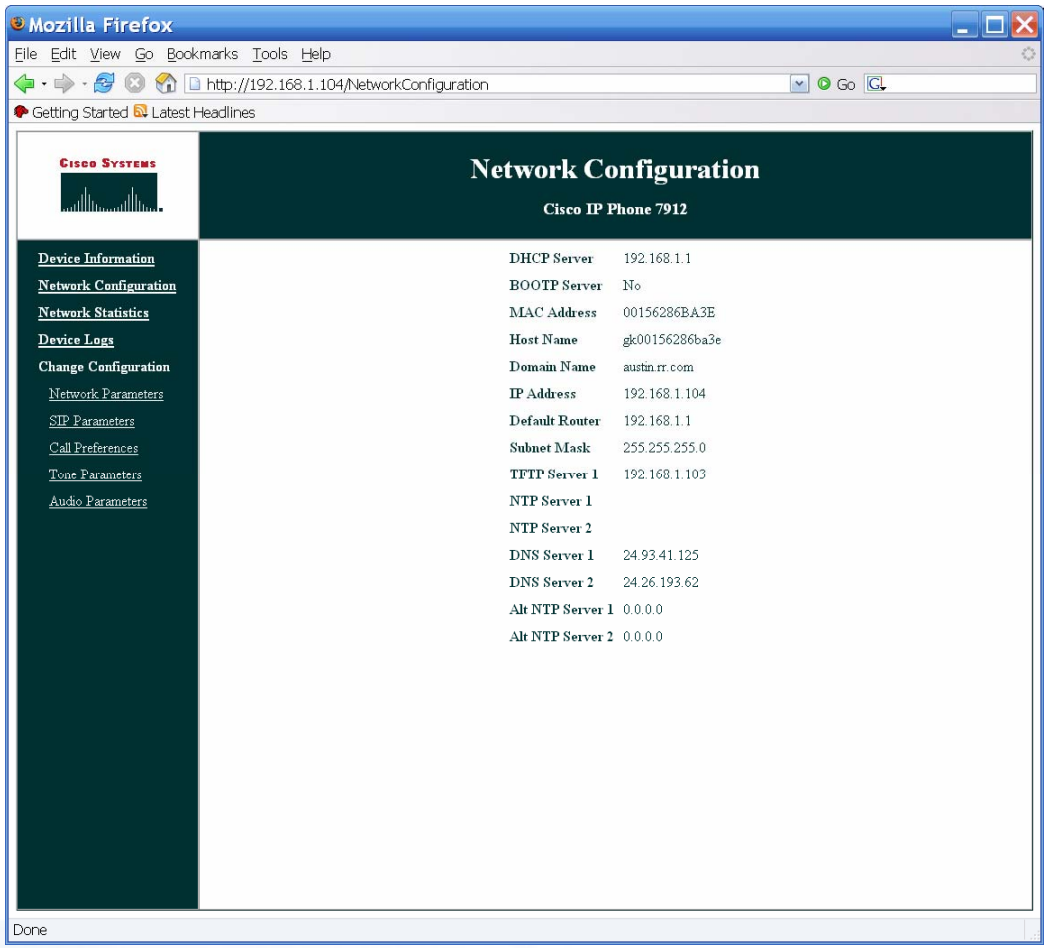
Footprinting

- 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

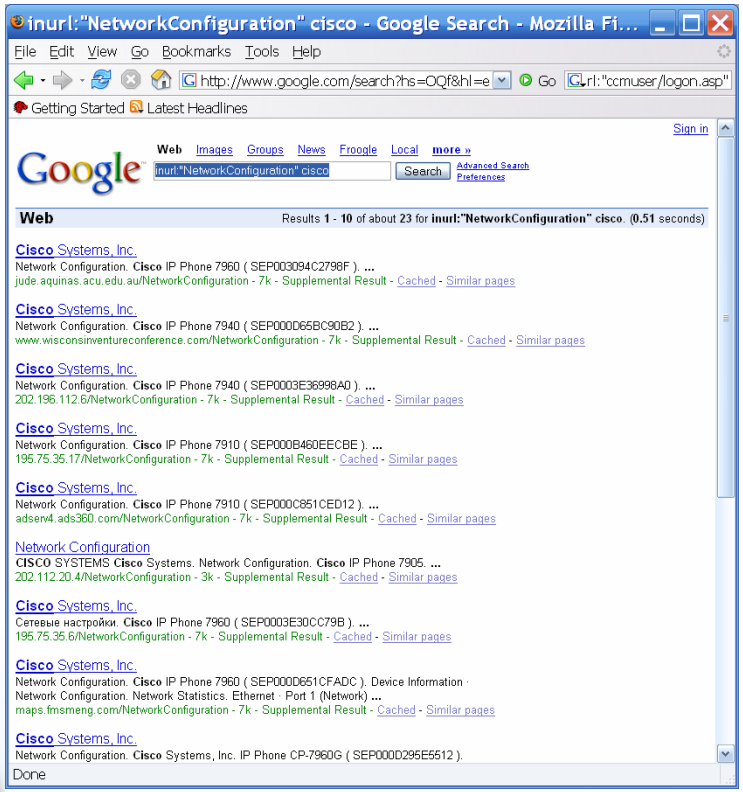
- Most VoIP devices (phones, servers, etc.) also run Web servers for remote management
- Find them with Google
- VoIP Google Hacking Database at http://www.hackingvoip.com

Google Hacking



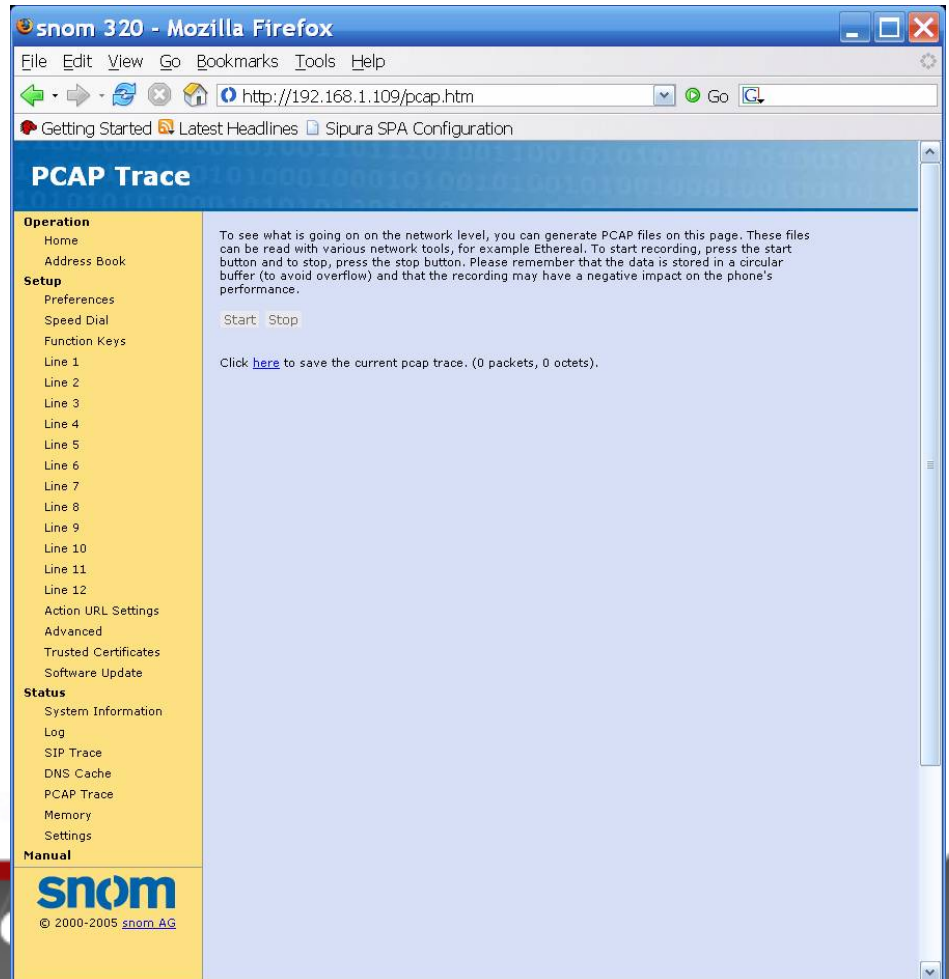
Footprinting

- inurl:"NetworkConfiguration" cisco



Footprinting

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



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

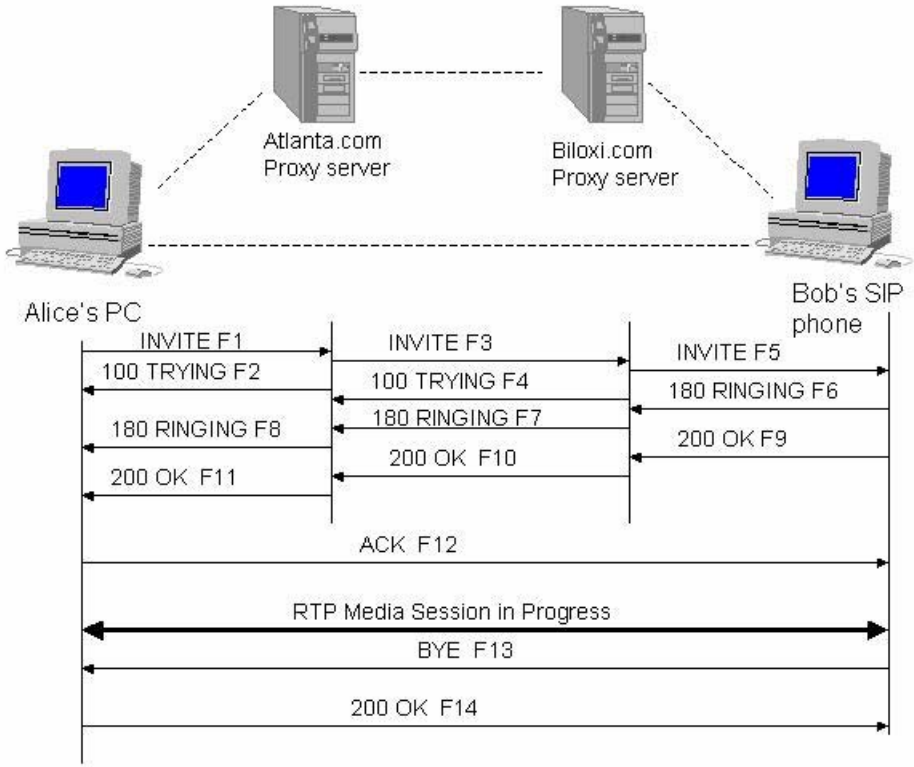
- SIP Messages

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

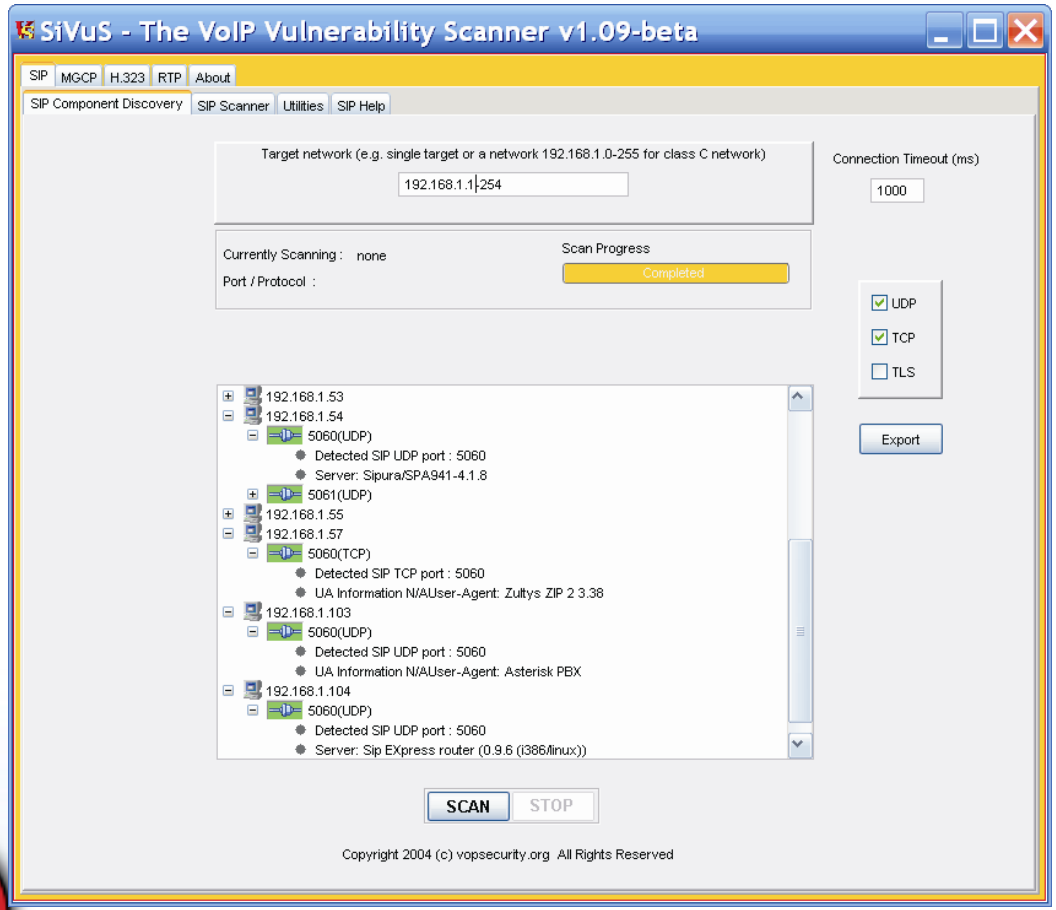
- [root@attacker]# nc 192.168.1.104 5060

```
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

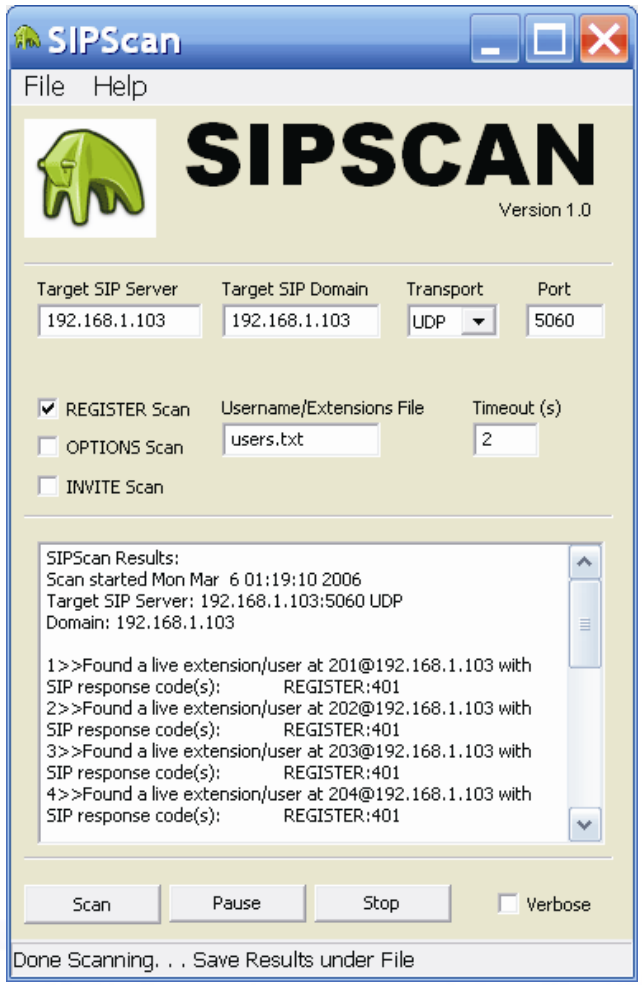
```
OPTIONS sip:test@192.168.1.104 SIP/2.0
Via: SIP/2.0/TCP 192.168.1.120;branch=4ivBcVj5ZnPYgb
To: alice <sip:test@192.168.1.104>
Content-Length: 0


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

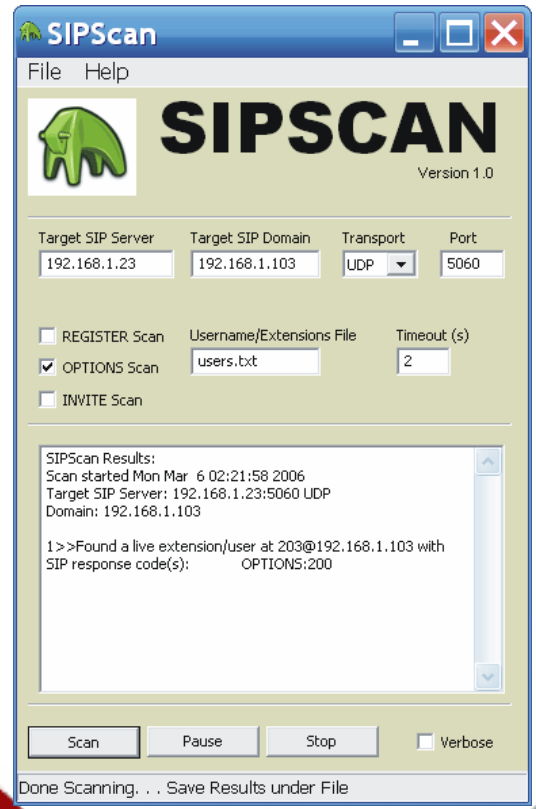
- Let's automate this. We wrote a tool called SIPSCAN to help. Available at http://www.hackingvoip.com
- Not only can you use OPTIONS, but INVITE and REGISTER as well.
- DEMO of SIPSCAN

Directory Scanning Demo



Directory Scanning on Cisco SIP

- Use SIPSCAN to query the phone's extension



Demo SIP Test Bed

TFTP Enumeration

- Almost all phones we tested use TFTP to drawn 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

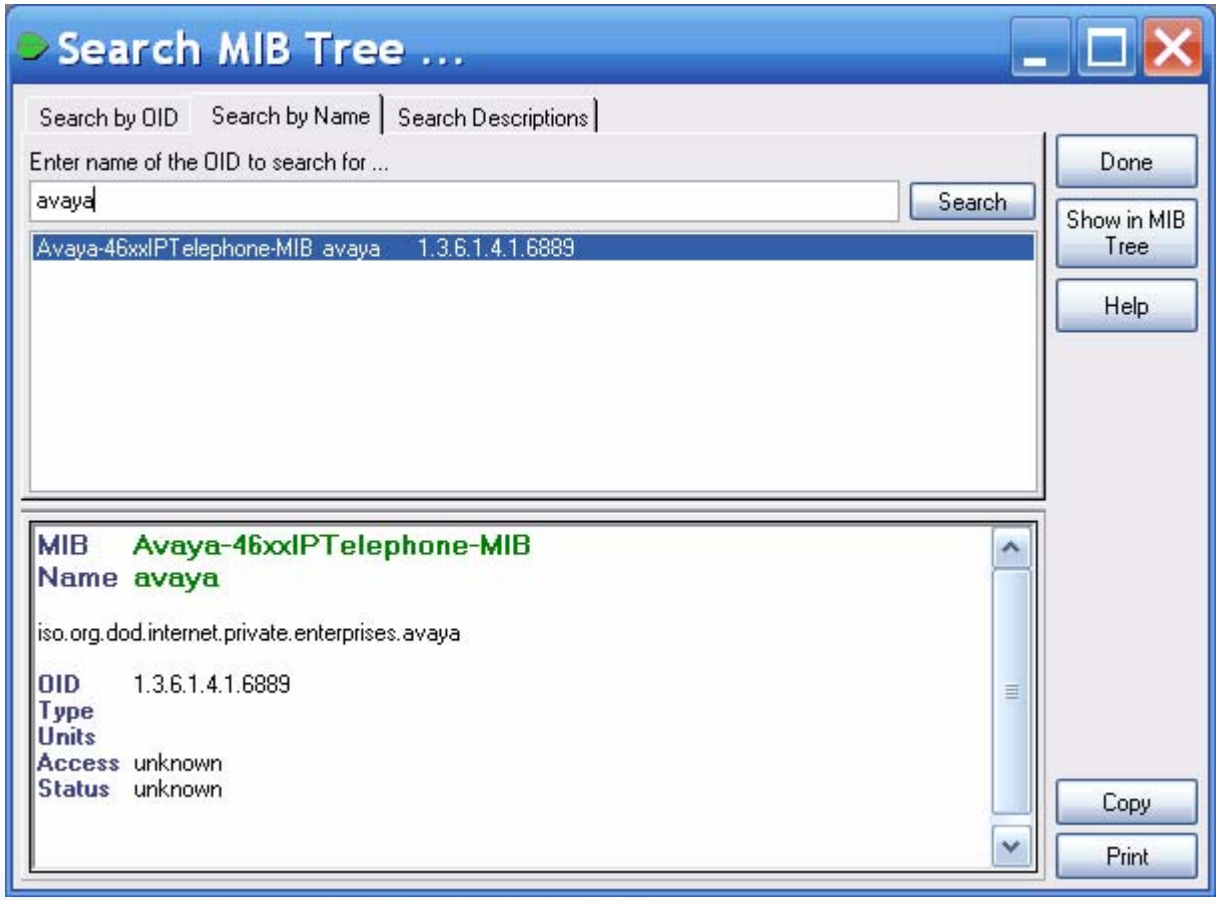
- Go to http://www.hackingvoip.com to see a list of commonly named VoIP config files
- Use a tool called TFTPBRUTE

```
[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



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.)

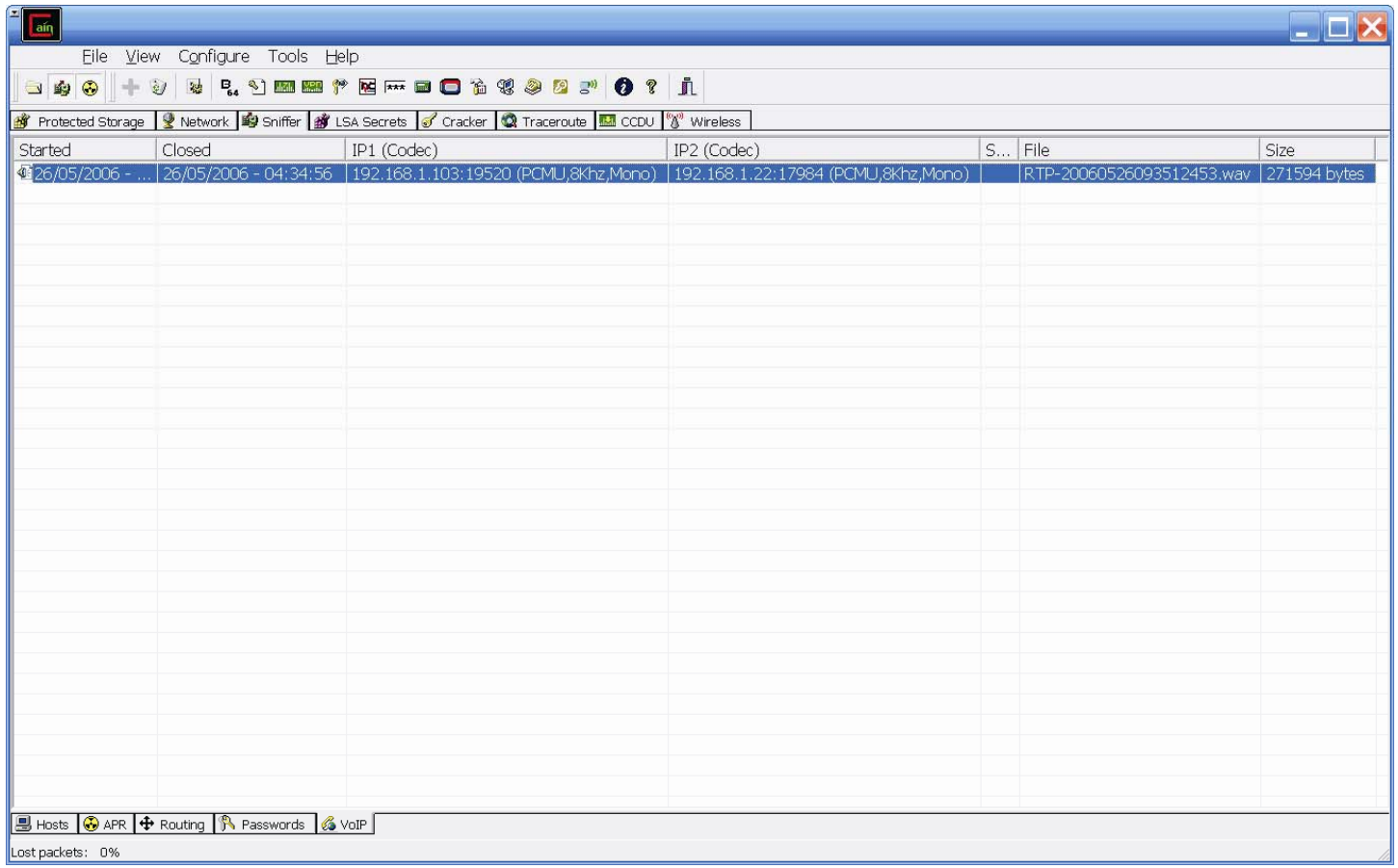
Sniffing in the Network

- 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



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

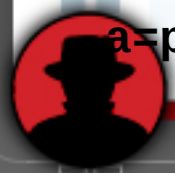
- Fuzzing has already led to a wide variety of Denial of Service and Buffer Overflow vulnerability discoveries in vendor implementations of VoIP products that use H.323 and SIP.
- PROTOS group from the University of Oulu in Finland responsible for high exposure vulnerability disclosures in HTTP, LDAP, 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: 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

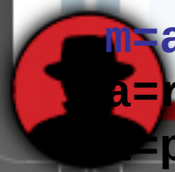


Fuzzing

```
INVITE sip:6713@192.168.26.180:6060;user=phone SIP/2.0
Via: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
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

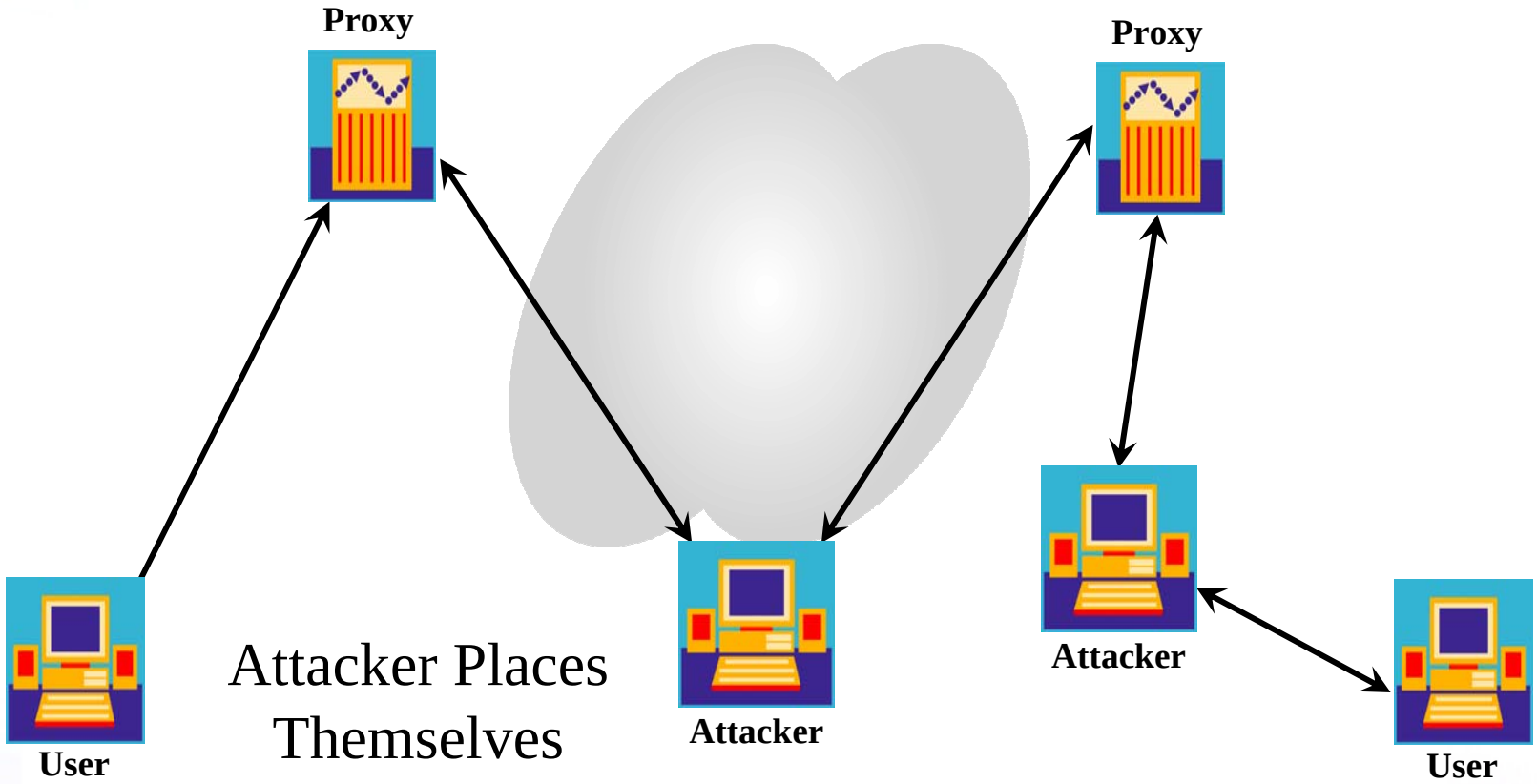
Fuzzing VoIP protocol implementations is only at the tip of the iceberg:

- 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**

Agenda

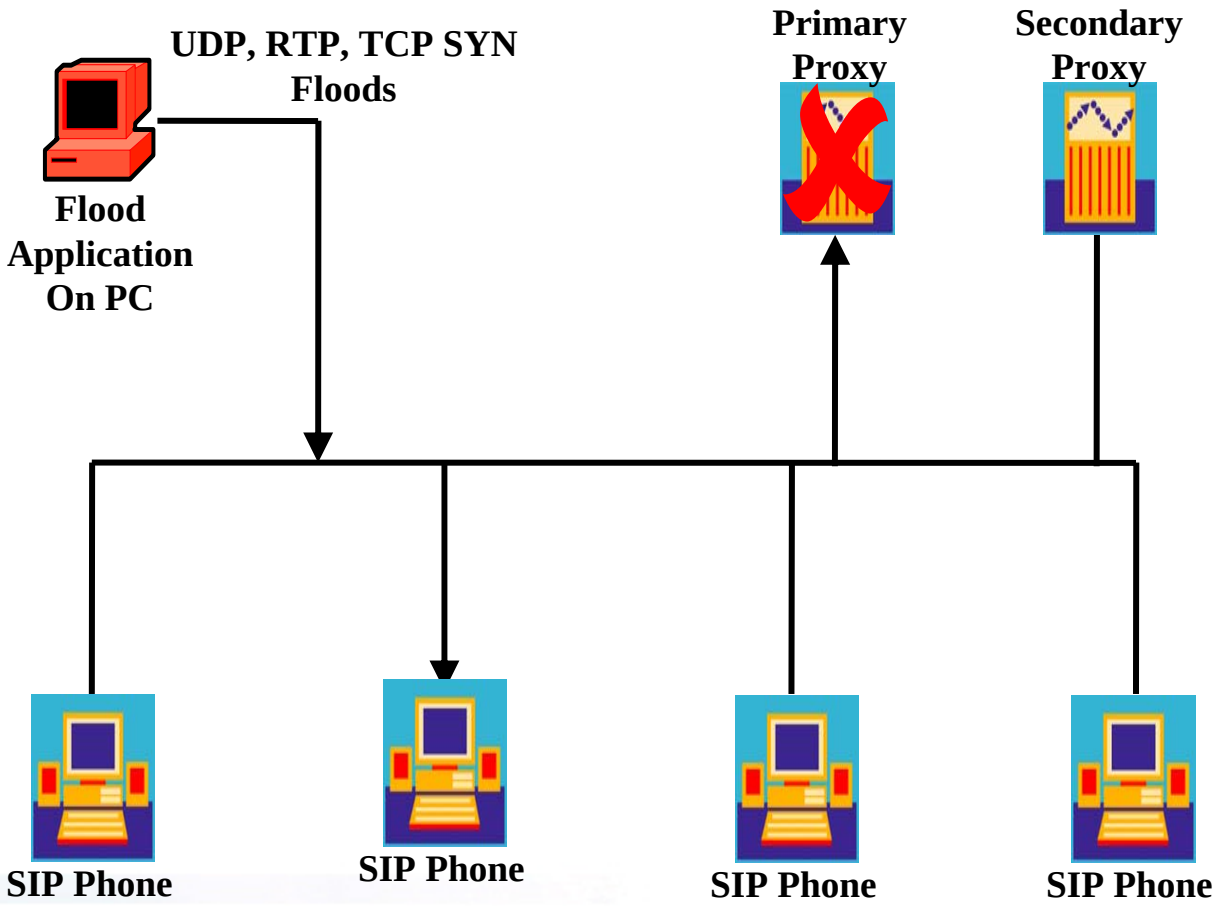
- Introductions
- Casing the Establishment
- Exploiting the Underlying Network
- Exploiting VoIP Applications
- Social Threats (SPIT, PHISHING, etc.)

Application-Level Interception

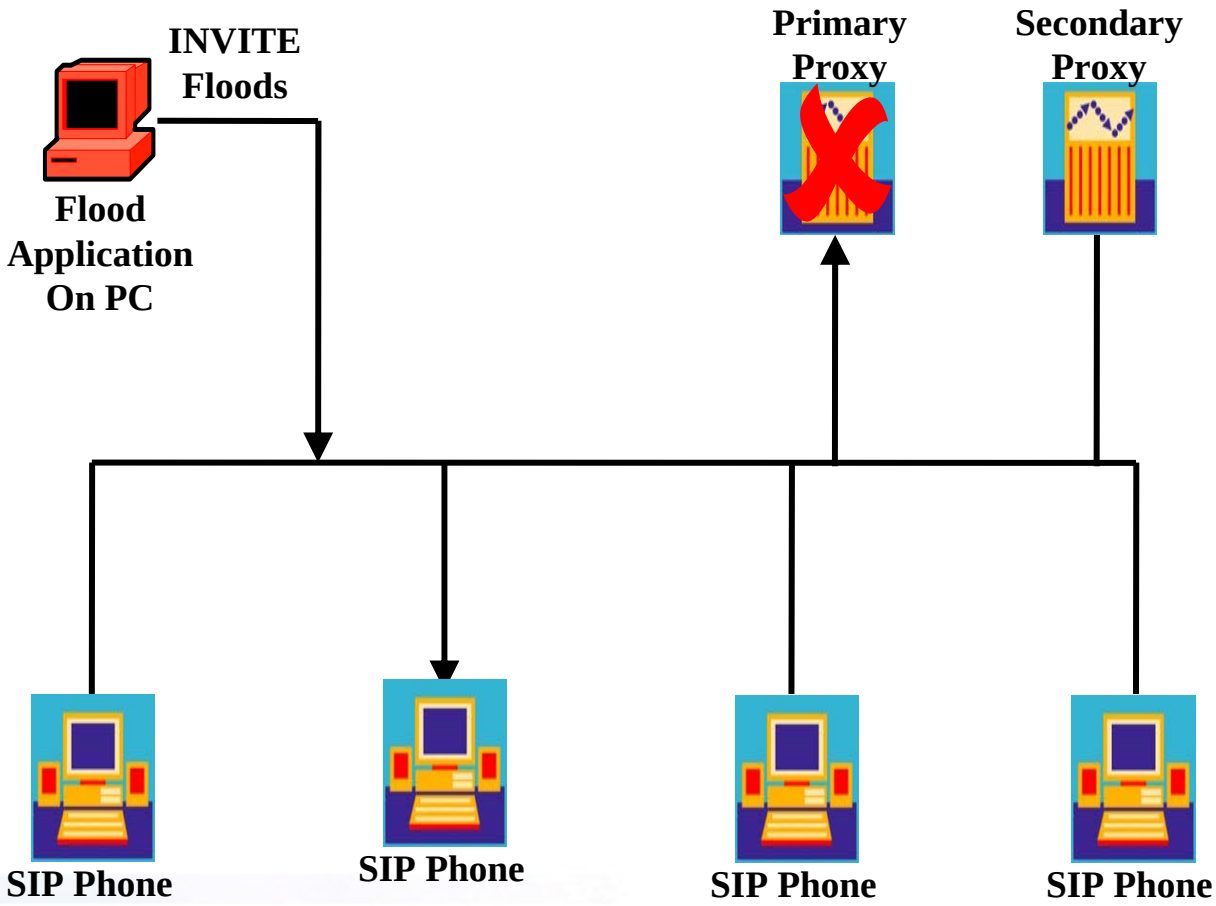


Attacker Places Themselves Between Proxies Or Proxy/UA

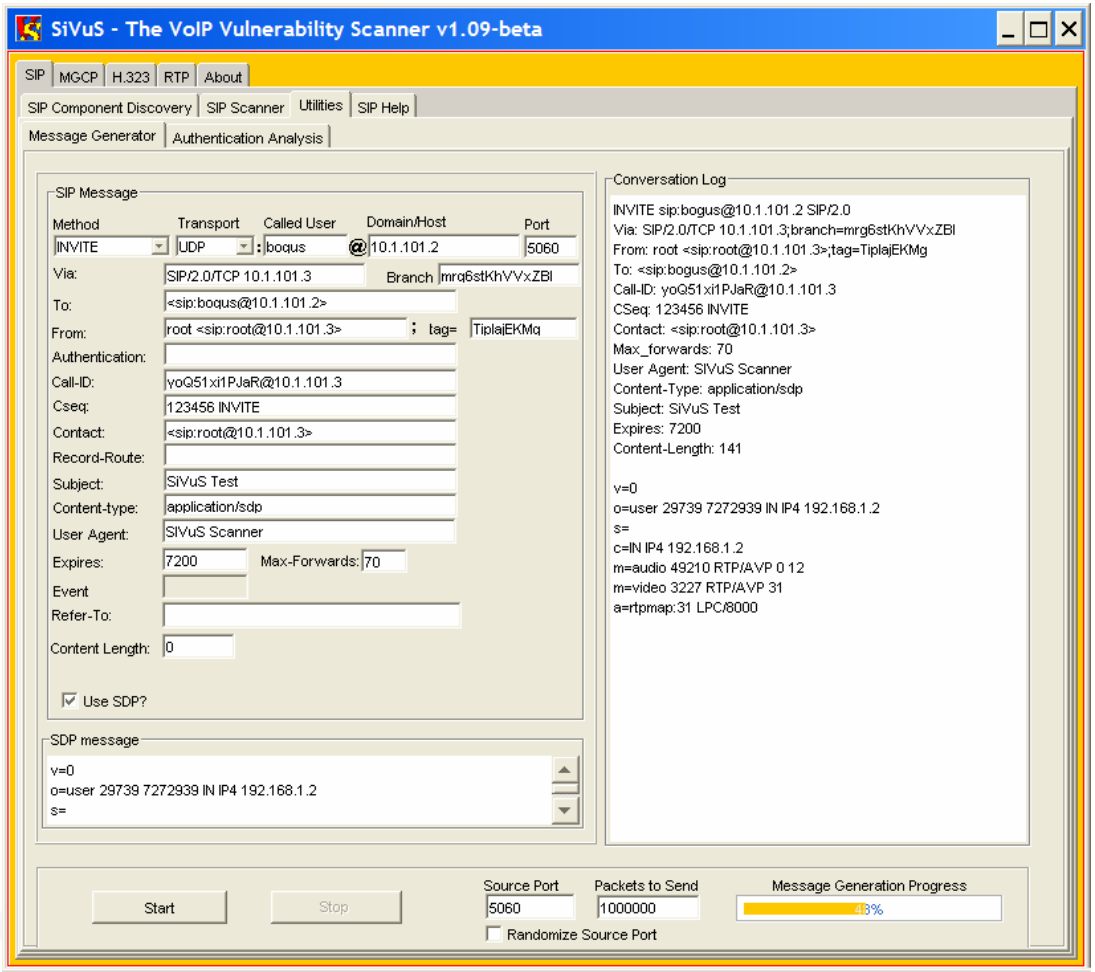
Disruption of Service



Disruption of Service

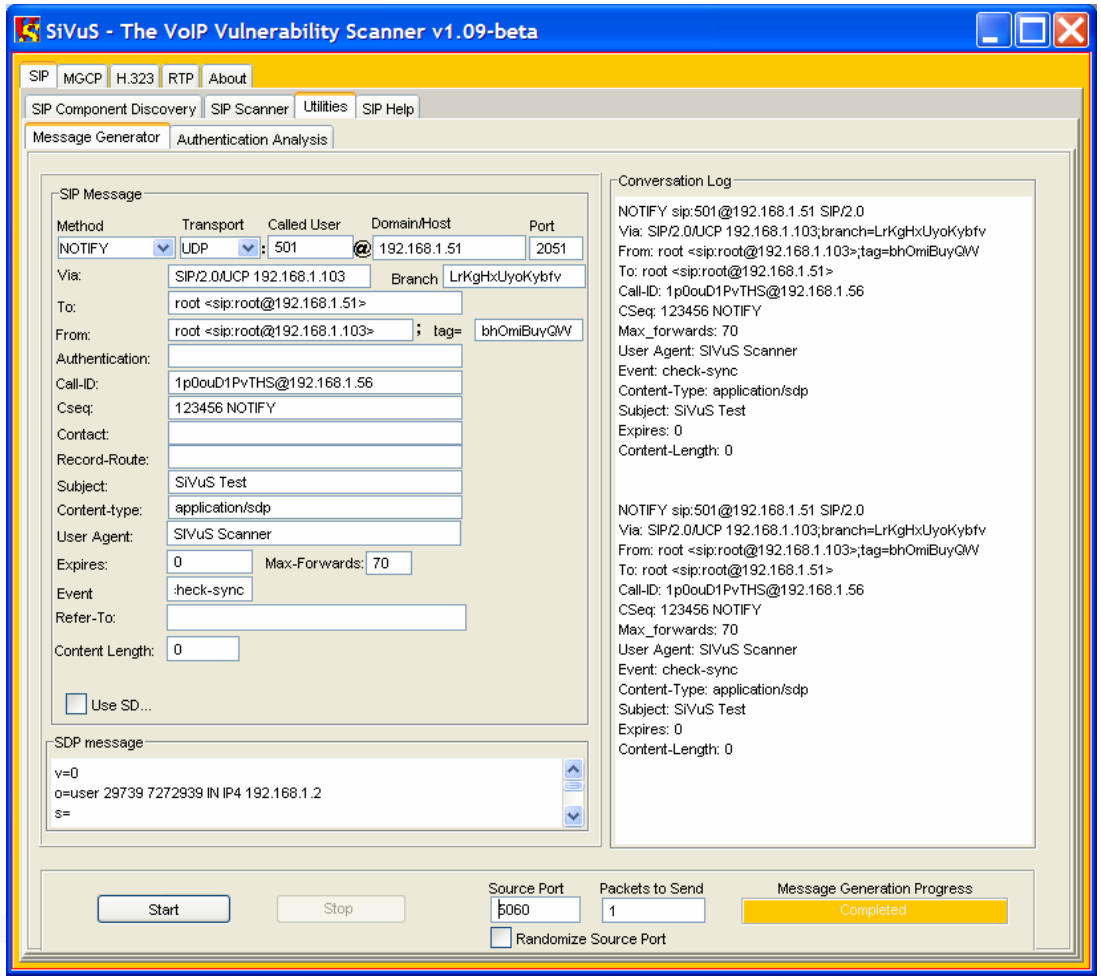


INVITE Flood



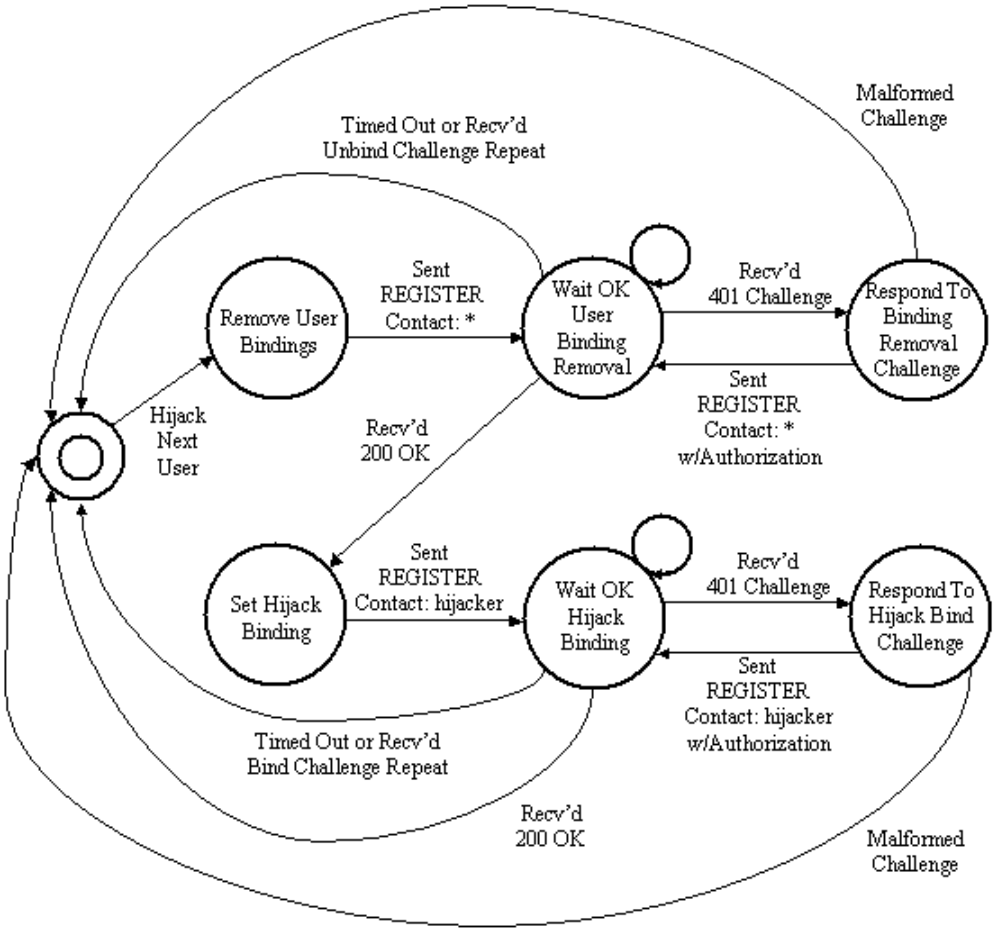
Demo SIP Test Bed

Check Sync Reboot

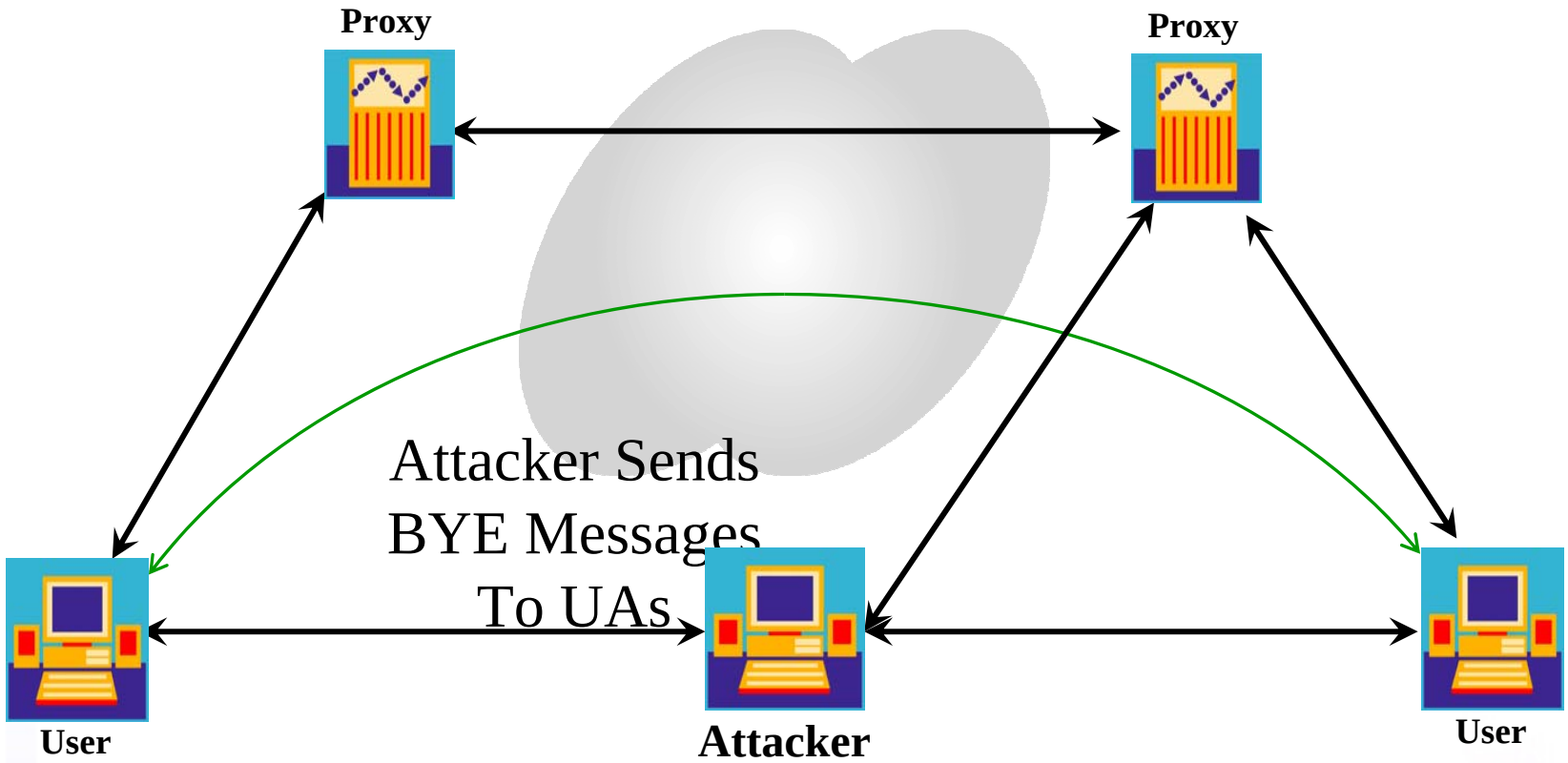


Demo SIP Test Bed

Signaling Manipulation

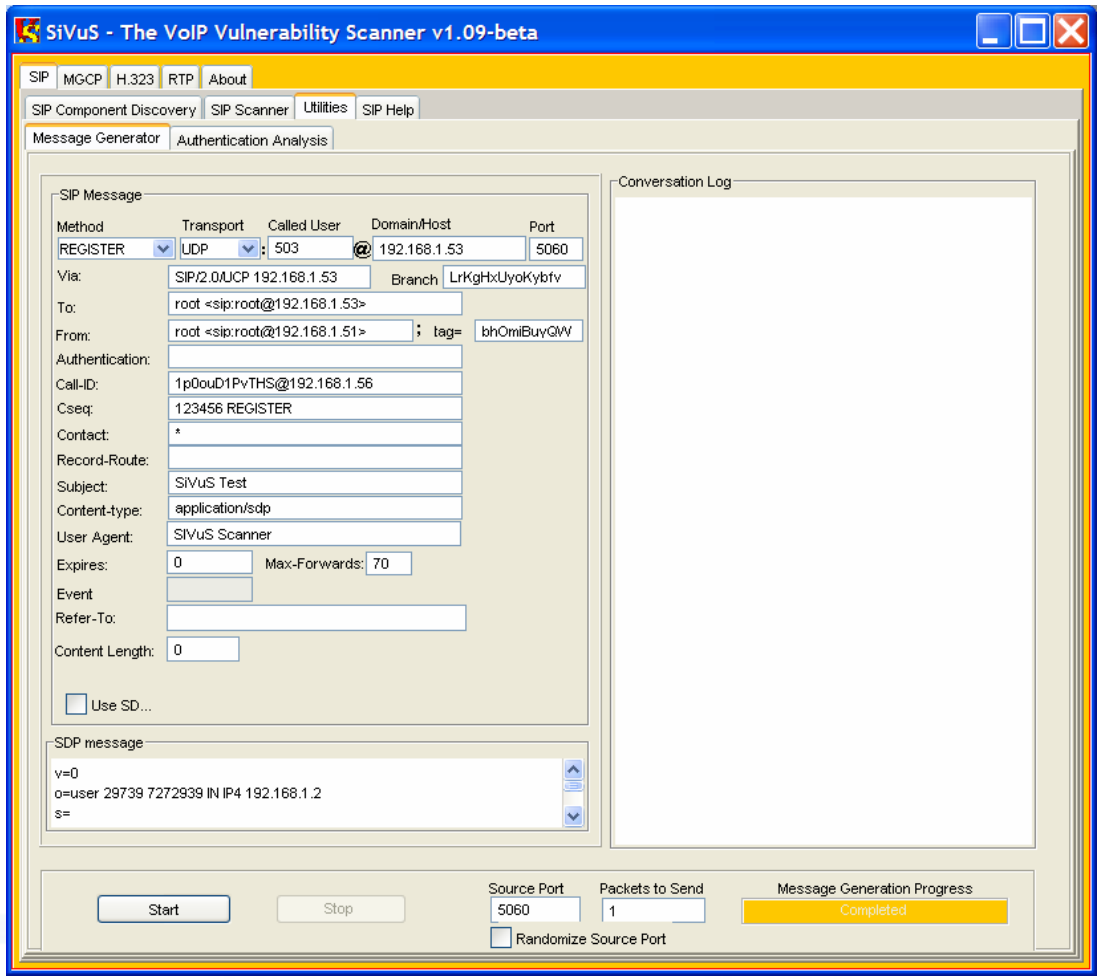


Signaling Manipulation



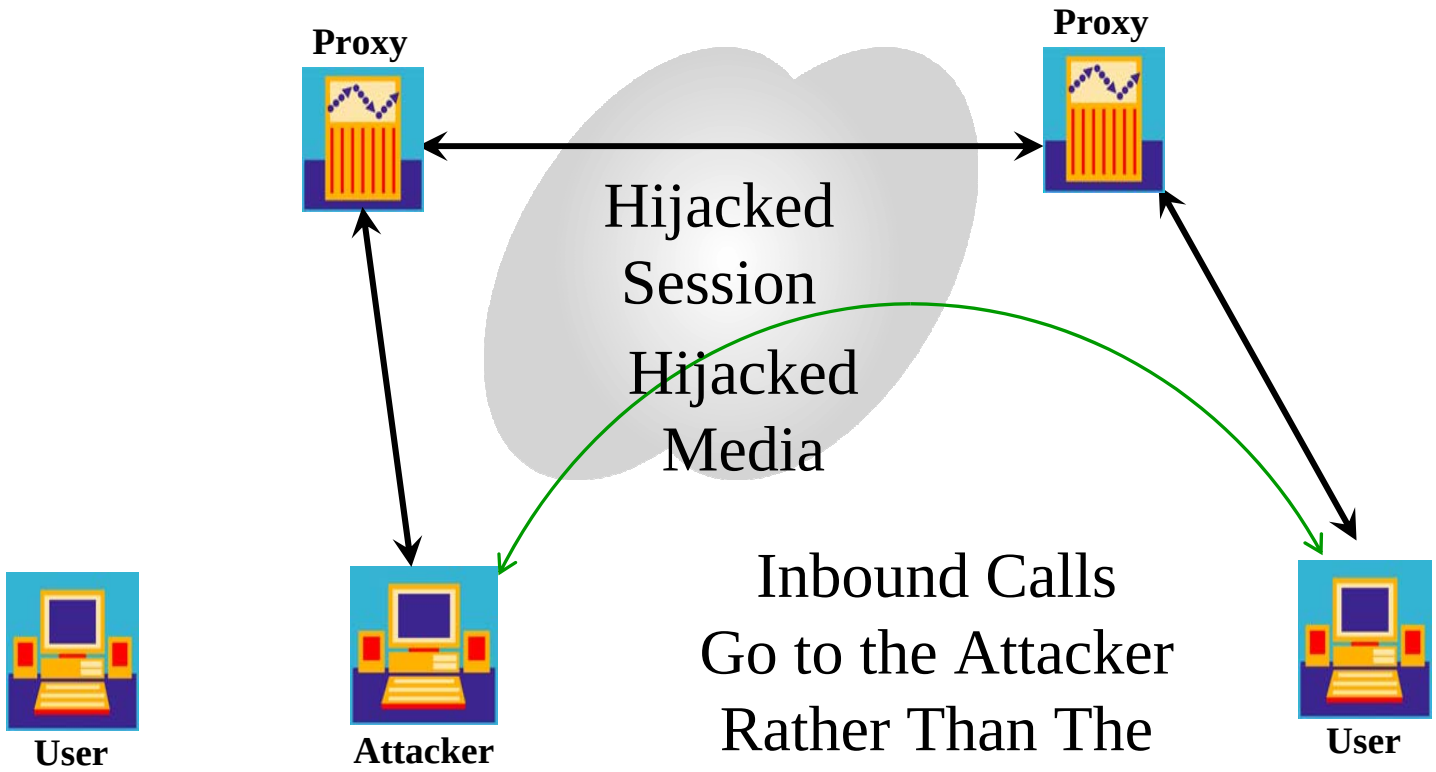
Demo SIP Test Bed

Erase Registrations

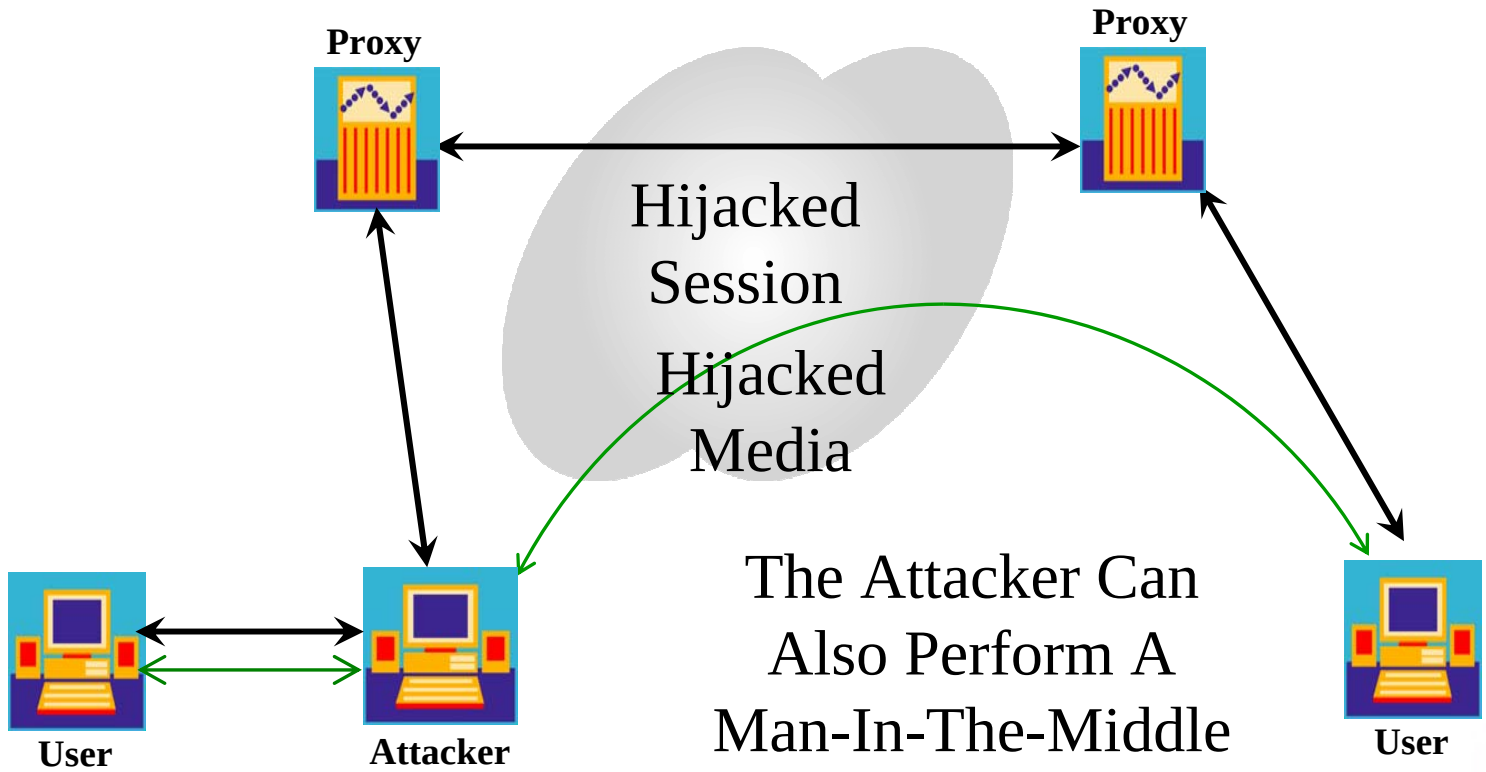


Demo SIP Test Bed

Signaling Manipulation



Signaling Manipulation



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

Demo SIP Test Bed

Agenda

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

SPIT


VIAGRA
Pfizer
3 pills - 100mg
$85
ORDER


4 film-coated tablets
Cialis 20 mg
film-coated tablets
tadalafil


GARANTIE
SPANISH FLY
Voedingssupplement
Dietary supplement
15 ml


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!

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 modifed 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