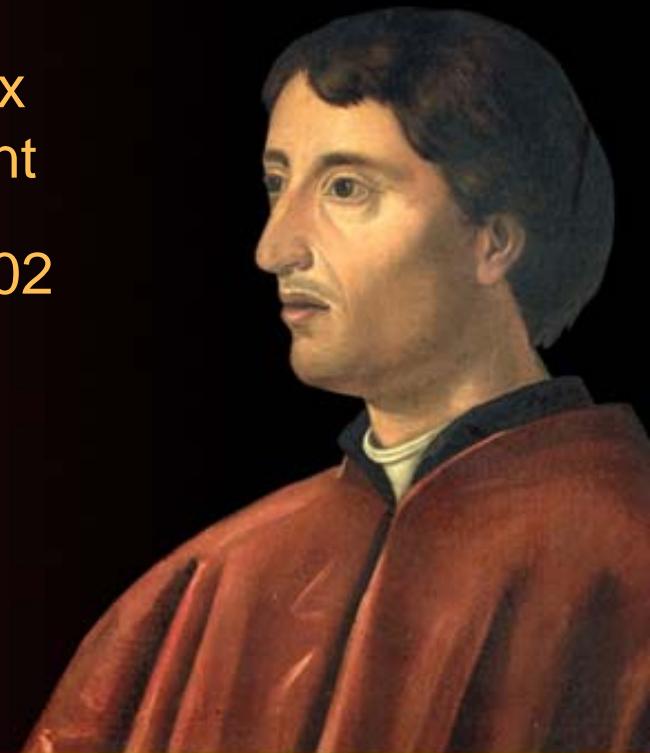


RSA[®]CONFERENCE2007

Exploiting Voice over IP Networks

Mark Collier, SecureLogix
David Endler, TippingPoint

February 7, 2007 - HT2-202



Who are we?



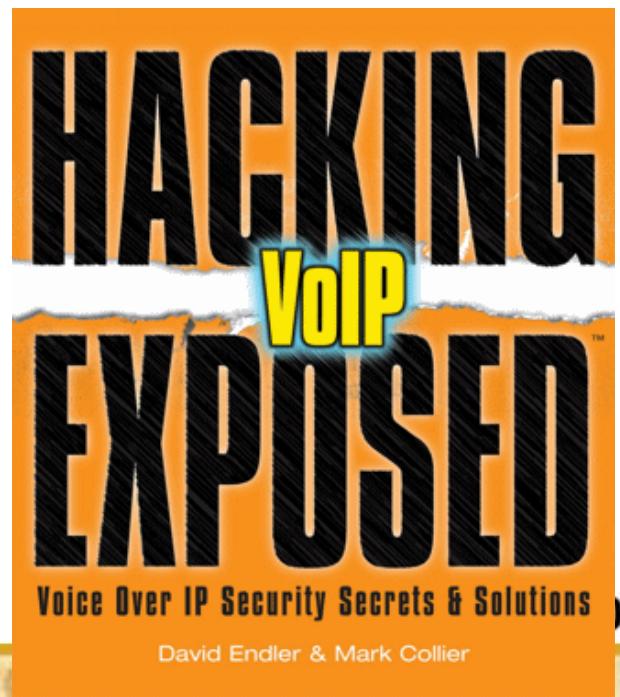
- **Mark Collier** is the chief technology officer at SecureLogix corporation, where he directs the company's VoIP security research and development. Mark also defines and conducts VoIP security assessments for SecureLogix's enterprise customers. Mark is actively performing research for the U.S. Department 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



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.

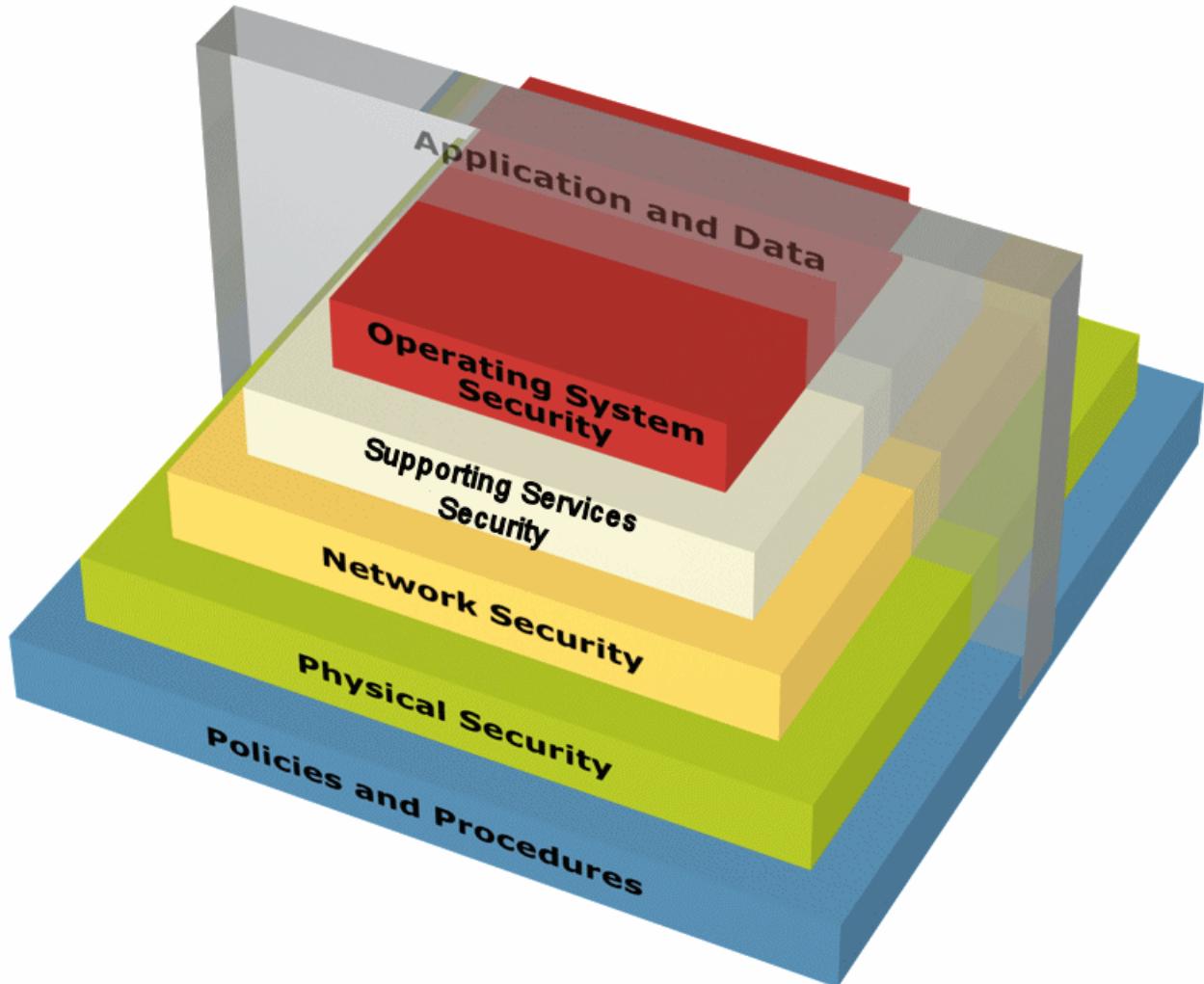
— “Voice Phishing”

- 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



VoIP Protocol and Application Security

OS Security

Supporting Service Security
(web server, database, DHCP)

Network Security (IP, UDP , TCP, etc)

Physical Security

Policies and Procedures

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

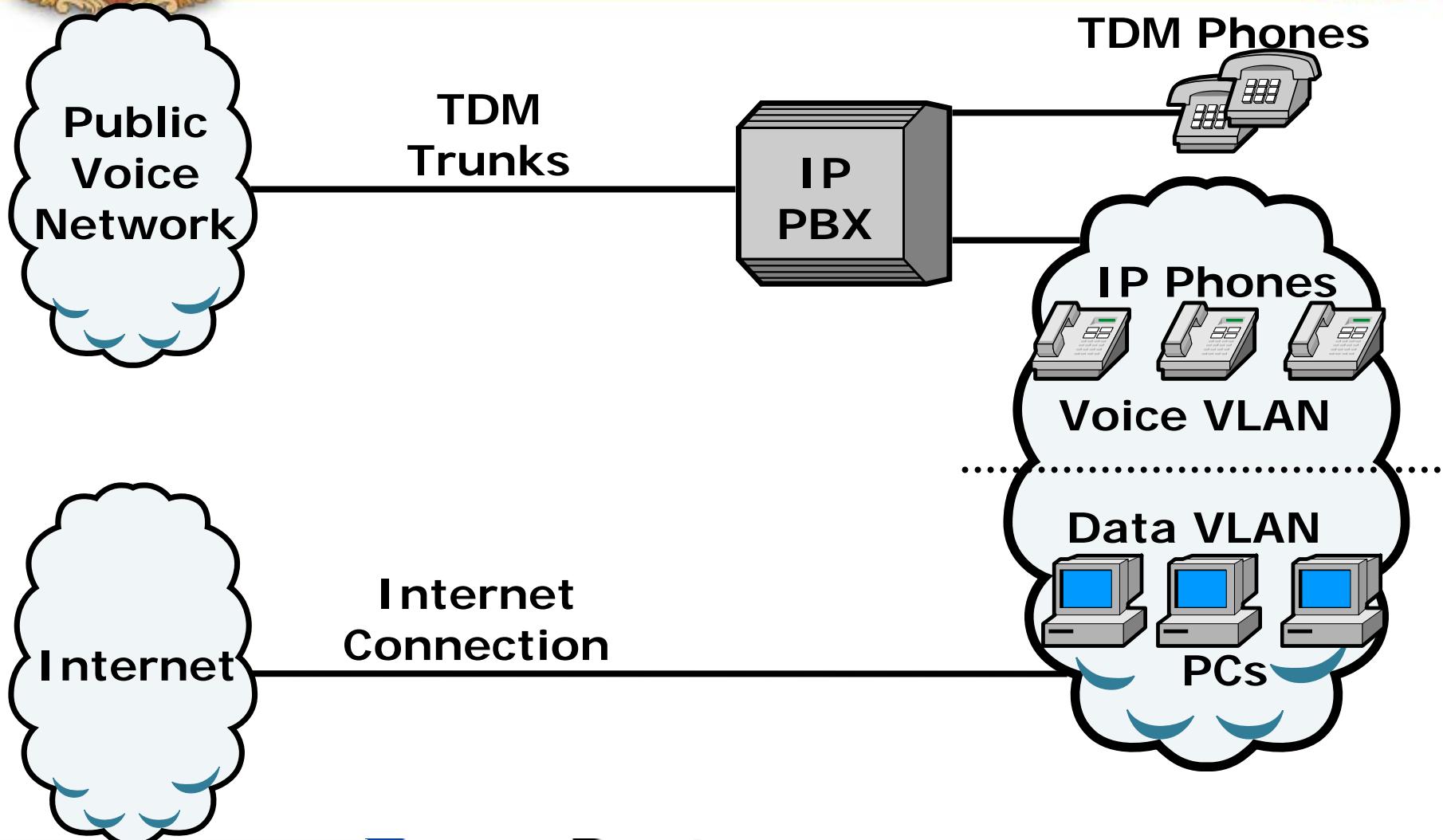
SQL Injection,
DHCP resource exhaustion

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

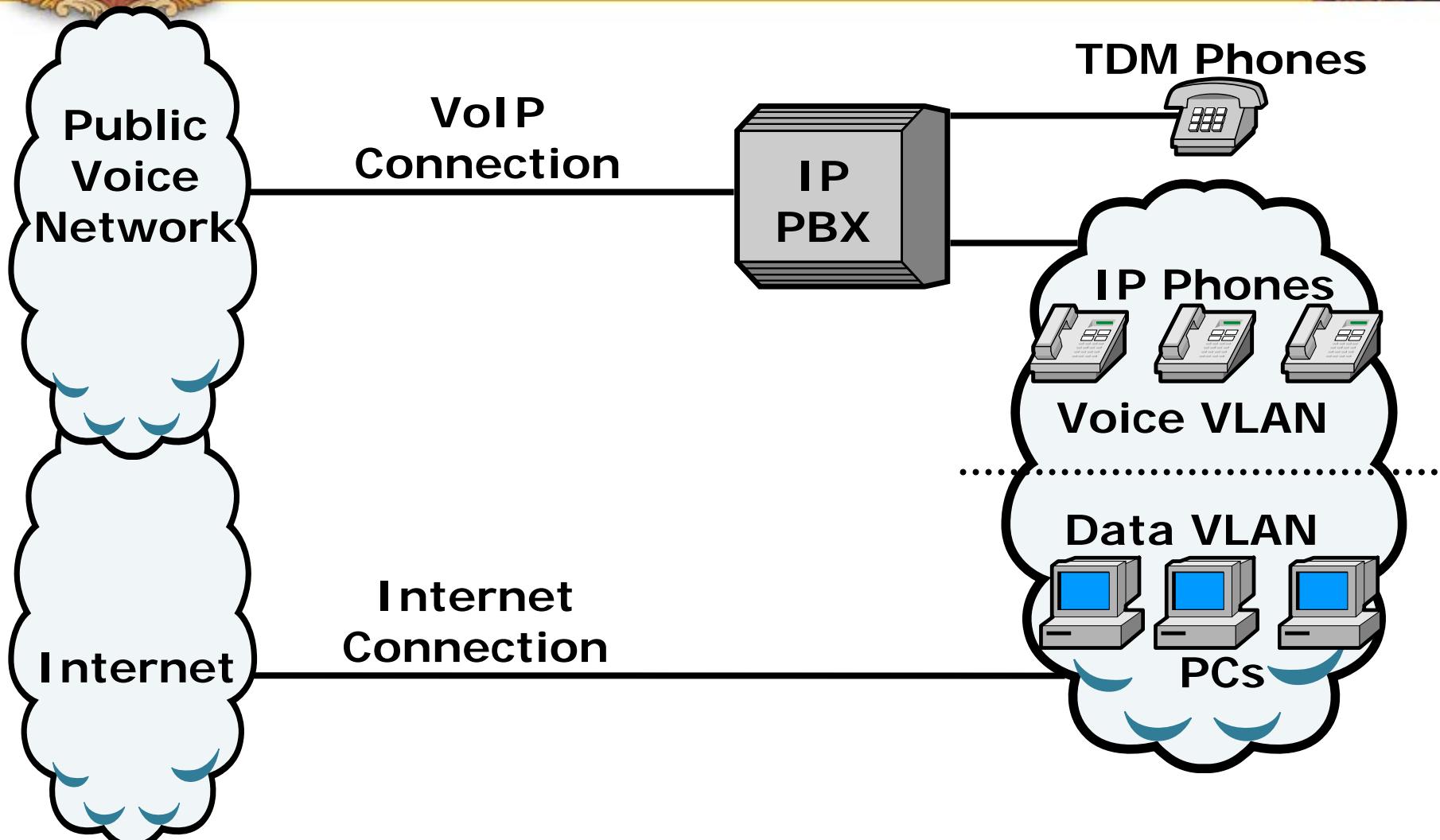
Total Call Server Compromise, Reboot, Denial of Service

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: inurl:"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



Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://192.168.1.104/NetworkConfiguration

Getting Started Latest Headlines

Cisco Systems

Network Configuration

Cisco IP Phone 7912

Device Information

Network Configuration **Selected**

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

Done

More Google Hacking



- inurl:"NetworkConfiguration" cisco

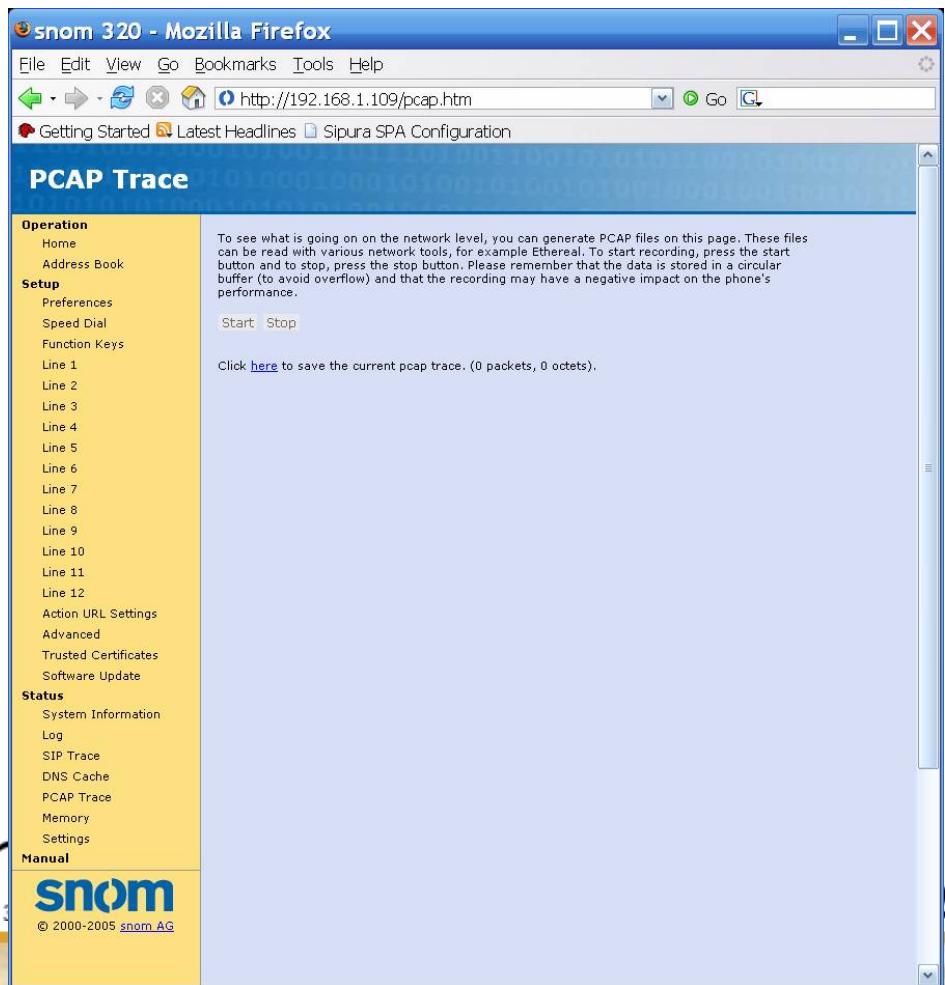
The screenshot shows a Mozilla Firefox browser window with the following details:

- Title Bar:** inurl:"NetworkConfiguration" cisco - Google Search - Mozilla Firefox
- Address Bar:** http://www.google.com/search?hs=OQ&hl=en
- Toolbar:** File, Edit, View, Go, Bookmarks, Tools, Help
- Navigation Buttons:** Back, Forward, Stop, Home, Refresh
- Search Bar:** inurl:"NetworkConfiguration" cisco
- Search Buttons:** Search, Advanced Search, Preferences
- Sign In:** Sign in
- Content Area:** Google search results for "inurl:"NetworkConfiguration" cisco".
 - Section:** Web
 - Results:** 1 - 10 of about 23 for inurl:"NetworkConfiguration" cisco. (0.51 seconds)
 - Links:**
 - [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 7980 (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) ...
imga.fnsmeng.com/NetworkConfiguration - 7k - Supplemental Result - Cached - Similar pages
 - [Cisco Systems, Inc.](#)
Network Configuration. Cisco Systems, Inc. IP Phone CP-7960G (SEP000D295E5512).
Done

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.cyveillance.com
- ◆ www.baytsp.com

Google Hacking Countermeasures

Cisco CallManager 4.1 Administration - Find and List Phones - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media

Address <https://ccm/CCMAdmin/phonelist.asp?findBy=name&match=begins&pattern=&submit1=Find&rows=20&wildcards=on&utilityList=> Go Links

System Route Plan Service Feature Device User Application Help

Cisco CallManager Administration
For Cisco IP Telephony Solutions

CISCO SYSTEMS

Find and List Phones [Add a New Phone](#)

5 matching record(s) for Device Name begins with ""

Find phones where Device Name begins with Find
and show 20 items per page. Allow wildcards. < Enter search text above >

To list all items, click Find without entering any search text, or use "Device Name is not empty" as the search.

Matching record(s) 1 to 5 of 5
Real-time Information Service returned information for 4 of 5 devices listed below.

<input type="checkbox"/>	Device Name	Description	Device Pool	Status	IP Address	Copy
<input type="checkbox"/>	7940 SEP001646806BB8	SEP001646806BB8	Default	CCM	172.16.3.248	<input type="button"/>
<input type="checkbox"/>	7960 SEP0016C8C3C9BB	SEP0016C8C3C9BB	Default	Not Found		<input type="button"/>
<input type="checkbox"/>	7960 SEP0016C8C3CCFE	SEP0016C8C3CCFE	Default	CCM	172.16.3.244	<input type="button"/>
<input type="checkbox"/>	7960 SEP0016C8C3CE4A	SEP0016C8C3CE4A	Default	CCM	172.16.3.247	<input type="button"/>
<input type="checkbox"/>	7912 SEP0017592EF9D0	SEP0017592EF9D0	Default	CCM	172.16.3.249	<input type="button"/>

Applet RSAProxyApplet started

Local intranet

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

Gathering Information
Scanning



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

Gathering Information
Scanning

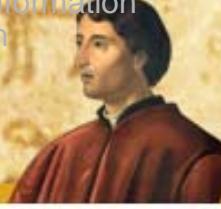


Using non-Internet routable IP addresses will prevent external scans

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

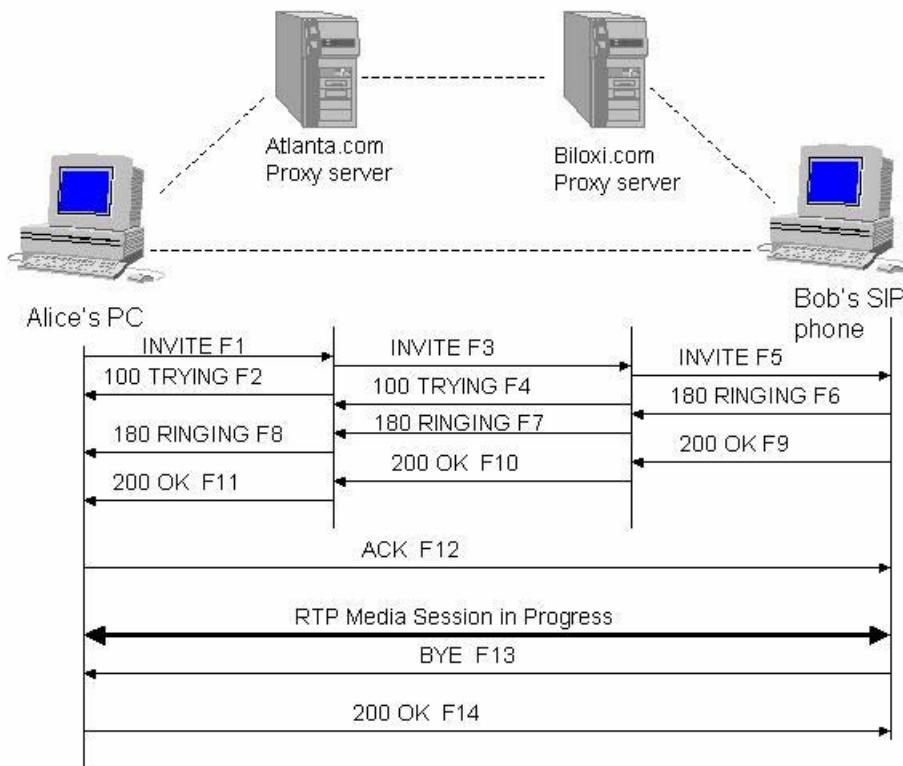
SIP Request	Purpose	RFC Reference
INVITE	to initiate a conversation	RFC 3261
BYE	to terminate an existing connection between two users in a session	RFC 3261
OPTIONS	to determine the SIP messages and codecs that the UA or Server understands	RFC 3261
REGISTER	to register a location from a SIP user	RFC 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

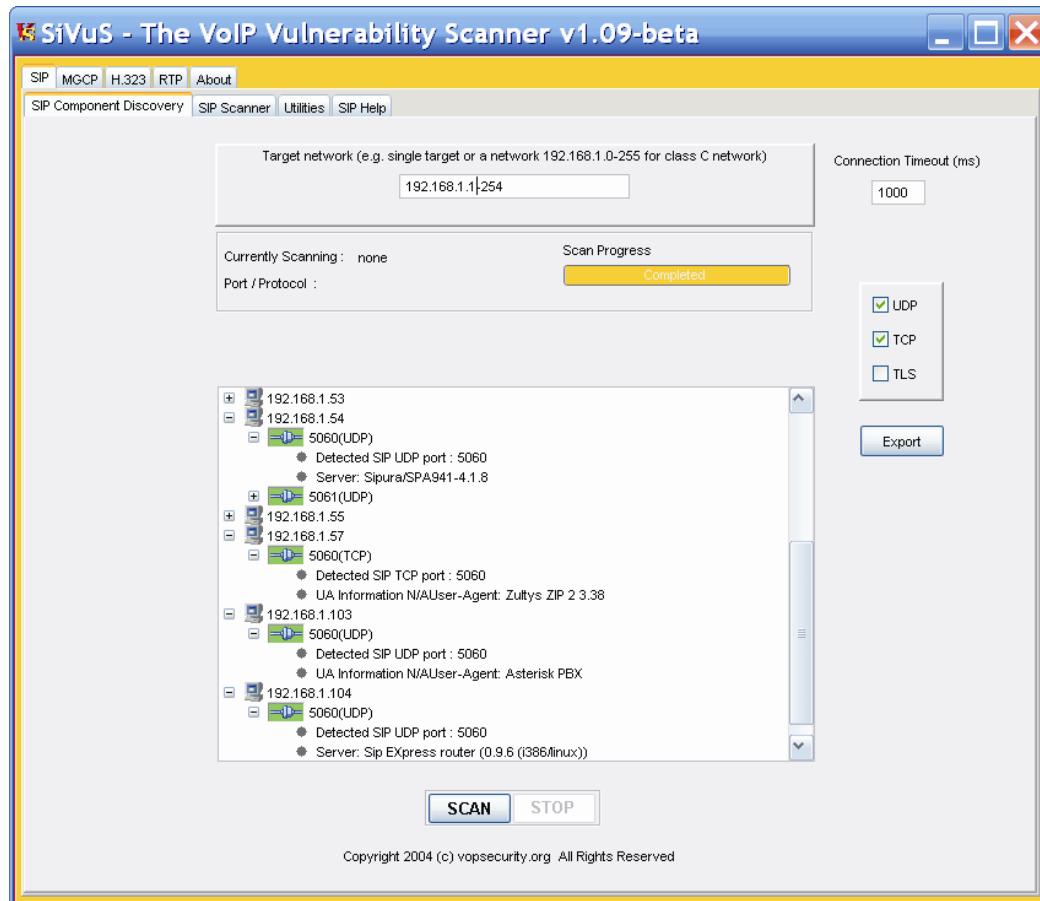
```
[root@attacker]# nc 192.168.1.104 5060
OPTIONS sip:test@192.168.1.104 SIP/2.0
Via: SIP/2.0/TCP 192.168.1.120;branch=4ivBcVj5ZnPYgb
To: alice <sip:test@192.168.1.104>
Content-Length: 0
```

```
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

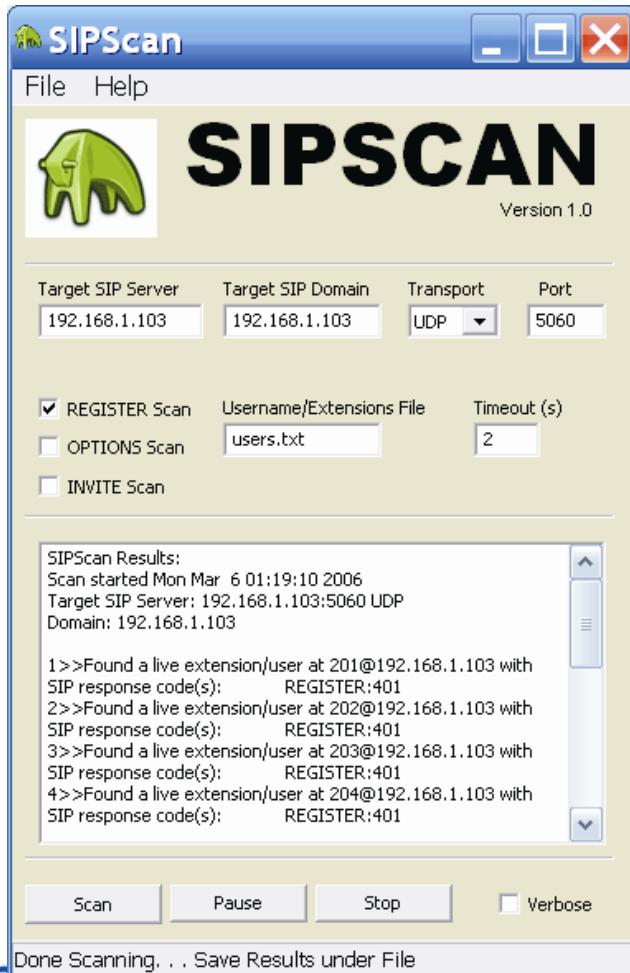
```
Via: SIP/2.0/TCP 192.168.1.120;branch=4ivBcVj5ZnPYgb;received=192.168.1.103
To: alice <sip:test@192.168.1.104>;tag=b27e1a1d33761e85846fc98f5f3a7e58.0503
Server: Sip EXPress router (0.9.6 (i386/linux))
Content-Length: 0
```

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.

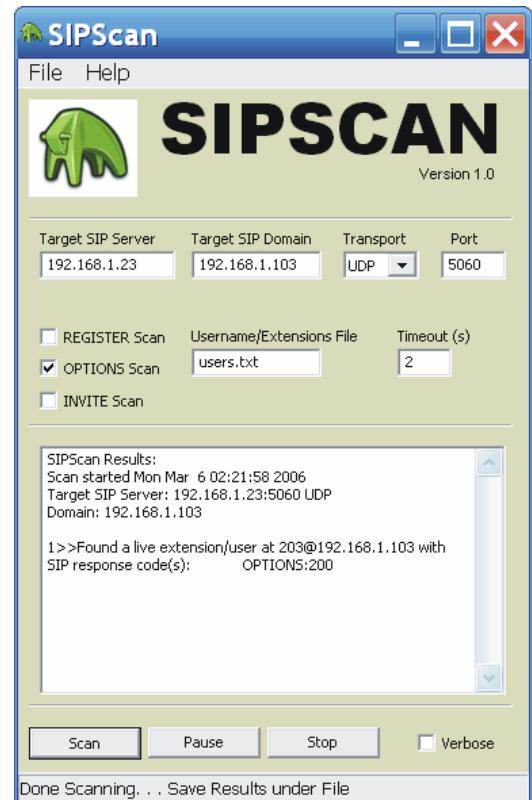
Directory Scanning Demo



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



Search MIB Tree ...

Search by OID | Search by Name | Search Descriptions

Enter name of the OID to search for ...

avaya

Search

Done

Show in MIB Tree

Help

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

Copy

Print

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

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

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

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:

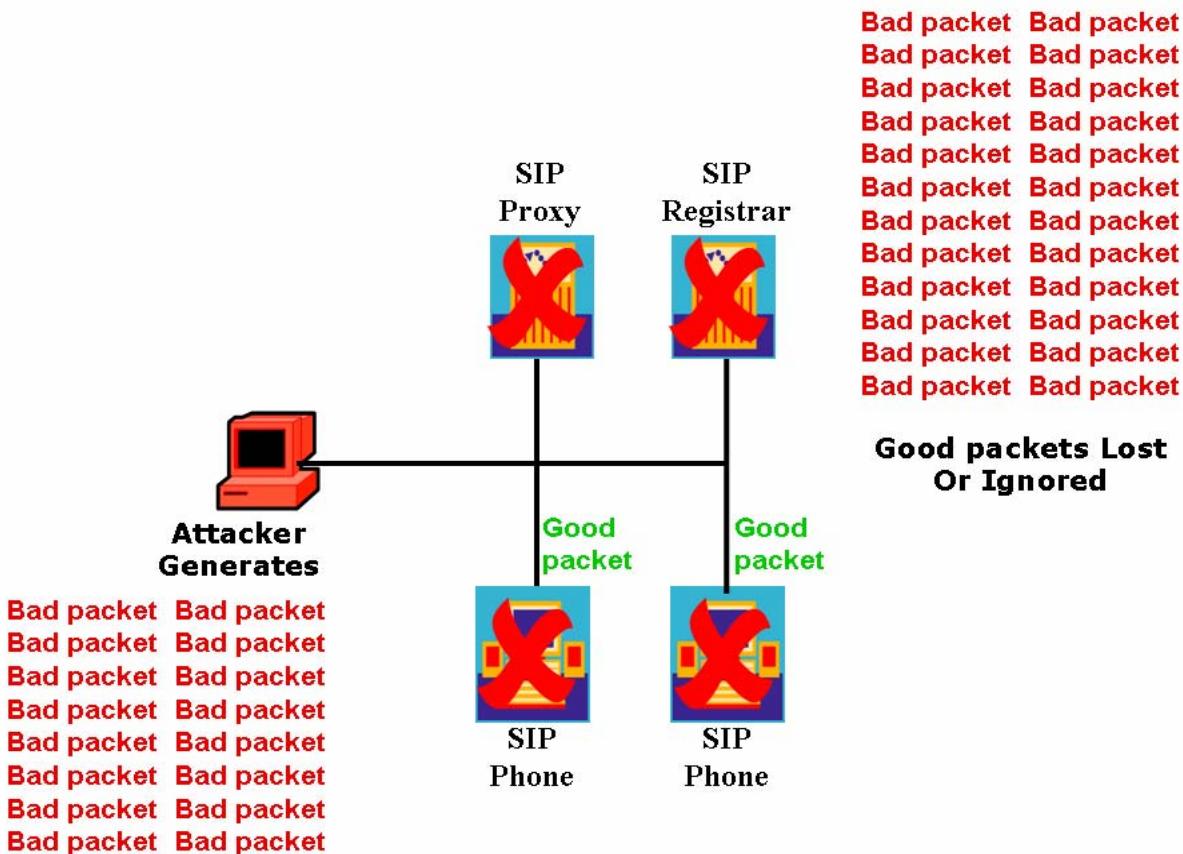
- ◆ Flooding attacks
- ◆ Network availability attacks
- ◆ Supporting infrastructure attacks

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



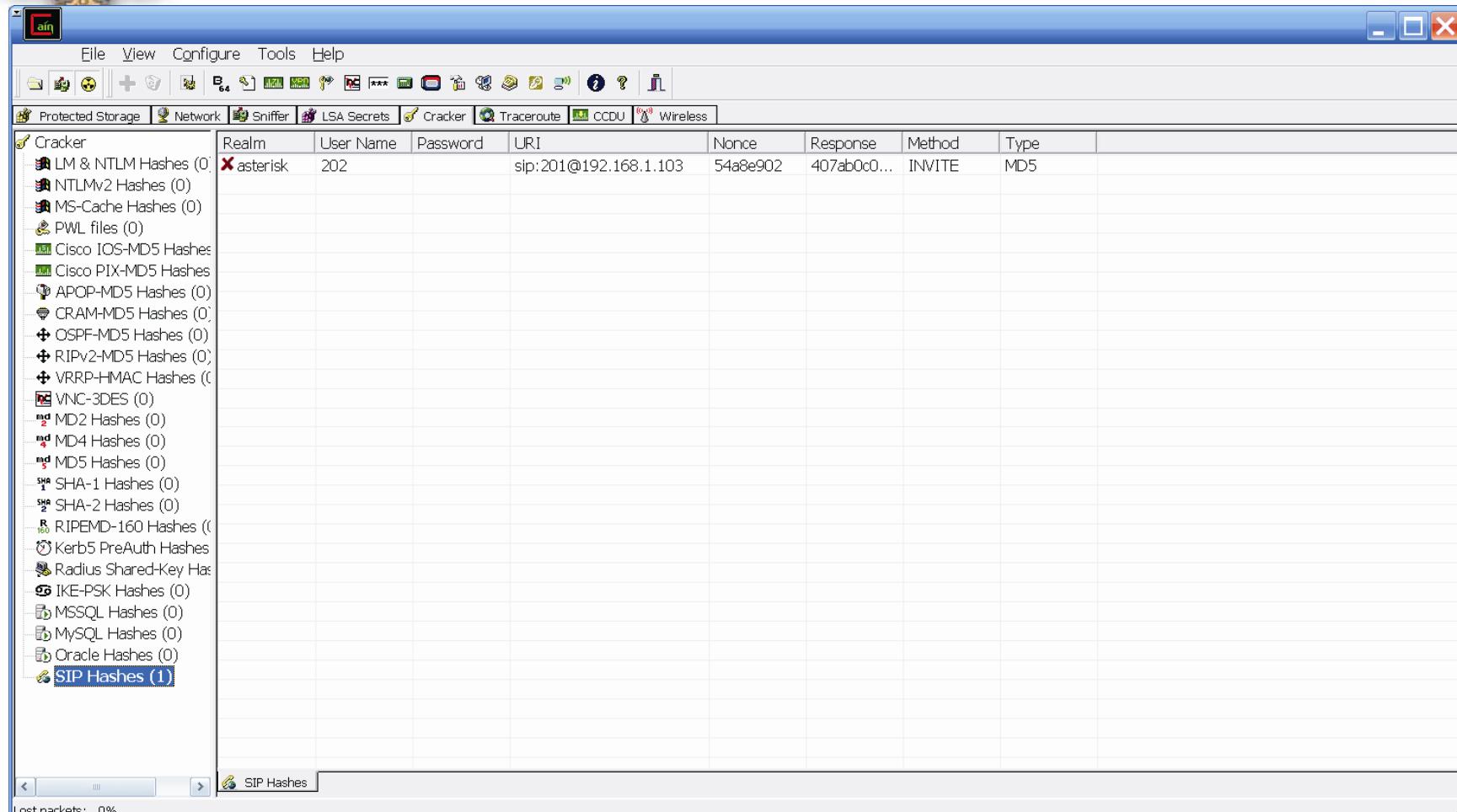
The most common network-level MITM attack is ARP poisoning

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



The screenshot shows the Cain & Abel tool interface. The main window title is 'Cain'. The menu bar includes 'File', 'View', 'Configure', 'Tools', and 'Help'. The toolbar contains various icons for file operations, network sniffing, and cracking. The main menu bar has tabs: 'Protected Storage', 'Network', 'Sniffer', 'LSA Secrets', 'Cracker', 'Traceroute', 'CCDU', and 'Wireless'. The 'Cracker' tab is selected. The main pane displays a table with the following data:

Realm	User Name	Password	URI	Nonce	Response	Method	Type
asterisk	202		sip:201@192.168.1.103	54a8e902	407ab0c0...	INVITE	MD5

The left sidebar, under the 'Cracker' tab, shows a tree view of hash types. The 'SIP Hashes' node is expanded, showing one item: 'SIP Hashes (1)'. The status bar at the bottom left shows 'Lost packets: 0%'. The status bar at the bottom right shows 'SIP Hashes'.

Network Interception ARP Poisoning



ettercap NG-0.7.3 (:0)

Start Targets Hosts View Mitm Filters Logging Plugins Help

Host List x

IP Address	MAC Address	Description
192.168.1.1	00:13:10:D4:AF:44	
192.168.1.21	00:04:13:24:23:8D	
192.168.1.22	00:0F:34:11:80:45	
192.168.1.23	00:15:62:86:BA:3E	
192.168.1.25	00:0B:82:06:4D:37	
192.168.1.27	00:04:F2:03:15:46	
192.168.1.51	00:04:13:23:34:95	
192.168.1.52	00:15:62:EA:69:E8	
192.168.1.54	00:0E:08:DA:24:AE	
192.168.1.55	00:E0:11:03:03:97	
192.168.1.103	00:09:7A:44:15:DB	
192.168.1.120	00:12:3F:B9:E4:24	
192.168.1.255	00:E0:11:03:03:97	

Delete Host Add to Target 1 Add to Target 2

```
7587 mac vendor fingerprint
1698 tcp OS fingerprint
2183 known services
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
13 hosts added to the hosts list...
Host 192.168.1.22 added to TARGET1
Host 192.168.1.103 added to TARGET2
```

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 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



test - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Clear Apply

No. .	Time	Source	Destination	rotoco	Info
24	16.202181	192.168.1.1	239.255.255.250	SSDP	NOTIFY * HTTP/1.1
25	18.468394	216.115.20.41	192.168.1.120	SIP	Status: 180 Ringing
26	20.321546	192.168.1.120	216.115.20.41	UDP	Source port: 5060 Destination port: 5061
27	20.322461	192.168.1.120	216.115.20.41	SIP	Request: REGISTER sip:ophone.vopr.vonage.net
28	20.383478	216.115.20.41	192.168.1.120	SIP	Status: 200 OK (1 bindings)
29	27.143835	216.115.20.41	192.168.1.120	SIP	Status: 180 Ringing
30	30.329235	192.168.1.120	216.115.20.41	UDP	Source port: 5060 Destination port: 5061
31	40.4336895	192.168.1.120	216.115.20.41	UDP	Source port: 5060 Destination port: 5061
32	40.534705	192.168.1.1	224.0.0.1	IGMP	V3 Membership Query
33	40.583831	192.168.1.120	216.115.20.41	SIP	Request: REGISTER sip:ophone.vopr.vonage.net
34	40.641828	216.115.20.41	192.168.1.120	SIP	Status: 200 OK (1 bindings)
35	43.004557	216.115.20.41	192.168.1.120	SIP/SD	Status: 200 OK, with session description
36	43.009226	192.168.1.120	216.115.20.41	SIP	Request: ACK sip:15126818382@216.115.20.41:5061
37	43.023385	192.168.1.120	69.59.248.187	RTCP	Sender Report
38	43.024567	192.168.1.120	69.59.248.187	RTP	Payload type=ITU-T G.711 PCMU, SSRC=4256915999, Seq=1, Time=337120, t
39	43.026913	69.59.248.187	192.168.1.120	RTP	Payload type=ITU-T G.711 PCMU, SSRC=81582794, Seq=912, Time=146040
40	43.044759	192.168.1.120	69.59.248.187	RTP	Payload type=ITU-T G.711 PCMU, SSRC=4256915999, Seq=2, Time=337280
41	43.046833	69.59.248.187	192.168.1.120	RTP	Payload type=ITU-T G.711 PCMU, SSRC=81582794, Seq=913, Time=146200
42	43.065274	192.168.1.120	69.59.248.187	RTP	Payload type=ITU-T G.711 PCMU, SSRC=4256915999, Seq=3, Time=337440
43	43.067373	69.59.248.187	192.168.1.120	RTP	Payload type=ITU-T G.711 PCMU, SSRC=81582794, Seq=914, Time=146360
44	43.084917	192.168.1.120	69.59.248.187	RTCP	Sender Report
45	43.085825	192.168.1.120	69.59.248.187	RTP	Payload type=ITU-T G.711 PCMU, SSRC=4256915999, Seq=4, Time=337600
46	43.086958	69.59.248.187	192.168.1.120	RTP	Payload type=ITU-T G.711 PCMU, SSRC=81582794, Seq=915, Time=146520
47	43.087522	69.59.248.187	192.168.1.120	ICMP	Destination unreachable (Port unreachable)
48	43.106355	192.168.1.120	69.59.248.187	RTP	Payload type=ITU-T G.711 PCMU, SSRC=4256915999, Seq=5, Time=337760
49	43.106513	69.59.248.187	192.168.1.120	RTP	Payload type=ITU-T G.711 PCMU, SSRC=81582794, Seq=916, Time=146680

+ Frame 36 (525 bytes on wire, 525 bytes captured)
+ Ethernet II, Src: Dell_b9:e4:24 (00:12:3f:b9:e4:24), Dst: Cisco-Li_d4:af:44 (00:13:10:d4:af:44)
+ Internet Protocol, src: 192.168.1.120 (192.168.1.120), Dst: 216.115.20.41 (216.115.20.41)
+ User Datagram Protocol, Src Port: 5060 (5060), Dst Port: 5061 (5061)
+ Session Initiation Protocol

0000 00 13 10 d4 af 44 00 12 3f b9 e4 24 08 00 45 00D. ?..\$..E.
0010 01 ff 04 09 00 00 80 11 86 28 c0 a8 01 78 d8 73(....x.5
0020 14 29 13 c4 13 c5 01 eb de 77 41 43 4b 20 73 69).WACK si
0030 70 3a 31 35 31 32 36 38 31 38 33 38 32 40 32 31 p:151268 18382@21
0040 36 2e 31 31 35 2e 32 30 34 31 3a 35 30 36 31 6.115.20 .41:5061
0050 20 65 40 50 3f 52 20 0d 02 56 60 61 20 20 63 ctn?n vA...c

File: "C:\Documents and Settings\Me\Desktop\test" 393 KB 00:01:21 | P: 1726 D: 1726 M: 0

Conversation Recording Wireshark

Ethereal: RTP Streams

Detected 5 RTP streams. Choose one for forward and reverse direction for analysis

Src IP addr.	Src port	Dest IP addr	Dest port	SSRC	Payload	Packets	Lost	Max Delta (ms)	Max Jitter (ms)	Mean Jitter (ms)	Pb?
192.168.1.120	8000	69.59.241.162	12534	1470379210	ITU-T G.711	6	(0.0%)	20.71	0.15	0.44	
69.59.241.162	12534	192.168.1.120	8000	128316882	ITU-T G.711	208	(0.0%)	21.96	0.60	0.30	
192.168.1.120	8000	69.59.241.159	12264	2580194303	ITU-T G.711	6	(0.0%)	20.84	0.15	0.46	
69.59.241.159	12264	192.168.1.120	8000	521271002	ITU-T G.711	8780	(0.0%)	31.02	1.47	0.26	
192.168.1.120	8000	69.59.241.156	12264	355111111	ITU-T G.711	6	(0.0%)	20.83	1.34	3.64	

Select a forward stream with left mouse button
Select a reverse stream with SHIFT + left mouse button

Unselect Find Reverse Save As Mark Packets Prepare Filter Copy Analyze Close

Ethereal: Save Payload As ...

New Folder Delete File Rename File
C:\Documents and Settings\Me

Folders	Files
..\	g2mdllhpx.exe
..\Application Data\	ntuser.dat
..\CmapToolsLogs\	ntuser.dat.LOG
..\Cookies\	ntuser.ini
..\Desktop\	PUTTY.RND
	TFTPServer2000.log

Format: .raw .au

Channels: forward reversed both

Selection: C:\Documents and Settings\Me

Cancel OK

Conversation Recording

Cain And Abel



The screenshot shows the Cain and Abel software interface. The title bar reads "Cain". The menu bar includes "File", "View", "Configure", "Tools", and "Help". The toolbar contains icons for various functions like Protected Storage, Network, Sniffer, LSA Secrets, Cracker, Traceroute, CCDU, and Wireless. The main window has tabs for "Protected Storage", "Network", "Sniffer", "LSA Secrets", "Cracker", "Traceroute", "CCDU", and "Wireless". The "Network" tab is selected, showing a table with columns: IP address, MAC addr..., OUI fingerprint, Host name, and several MAC address fields. One row is populated with "192.168.1.1", "001310D...", "Cisco-Linksys, LLC", and "B... B... B8 Gr M.. M.. M..". At the bottom, there are more tabs for "Hosts", "APR", "Routing", "Passwords", and "VoIP". A status bar at the bottom shows "Lost packets: 0%".

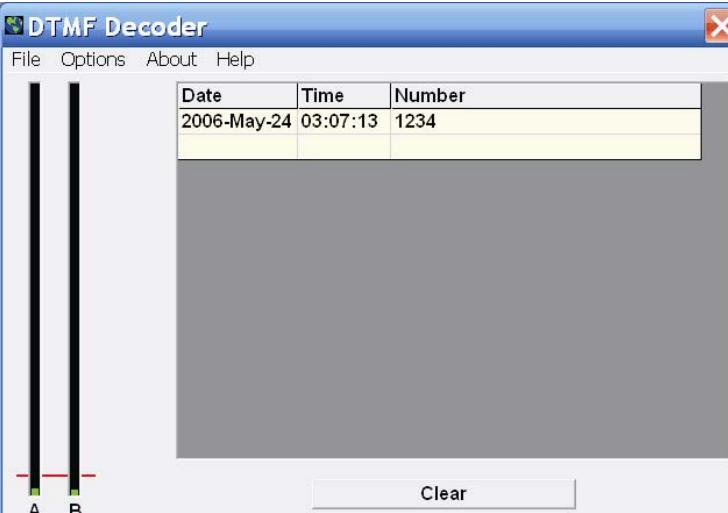
Conversation Recording

Other Tools

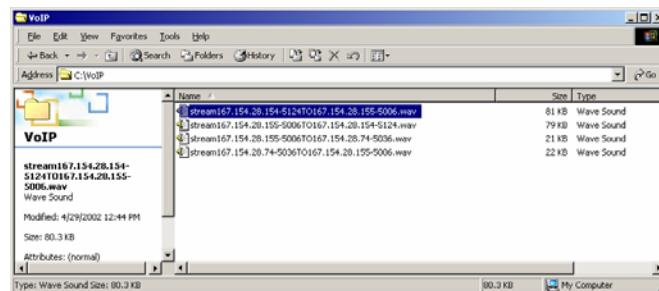
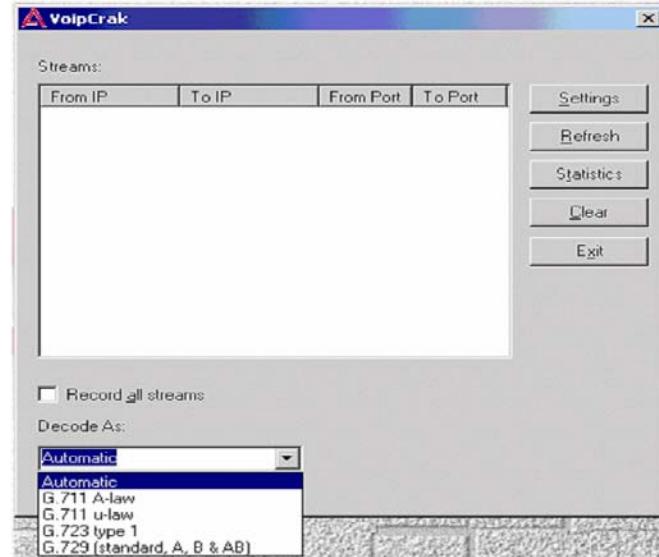


Other tools include:

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



voipcrack.com
a division of 3Com



rsaconference2007

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

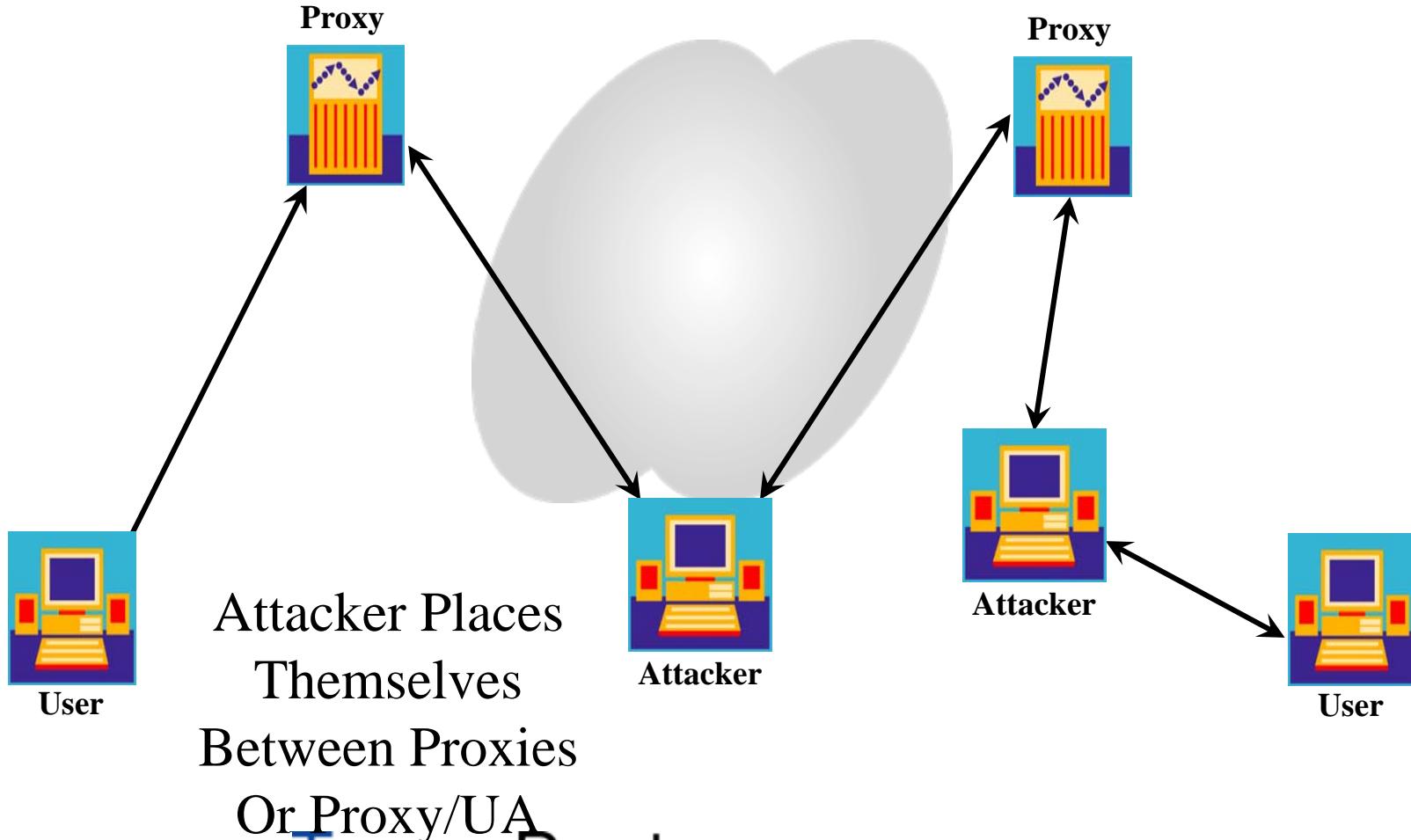


It is also possible to perform a MITM attack at the application layer

Some possible ways to perform this attack include:

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

Application Interception



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: 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: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa...
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa...
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

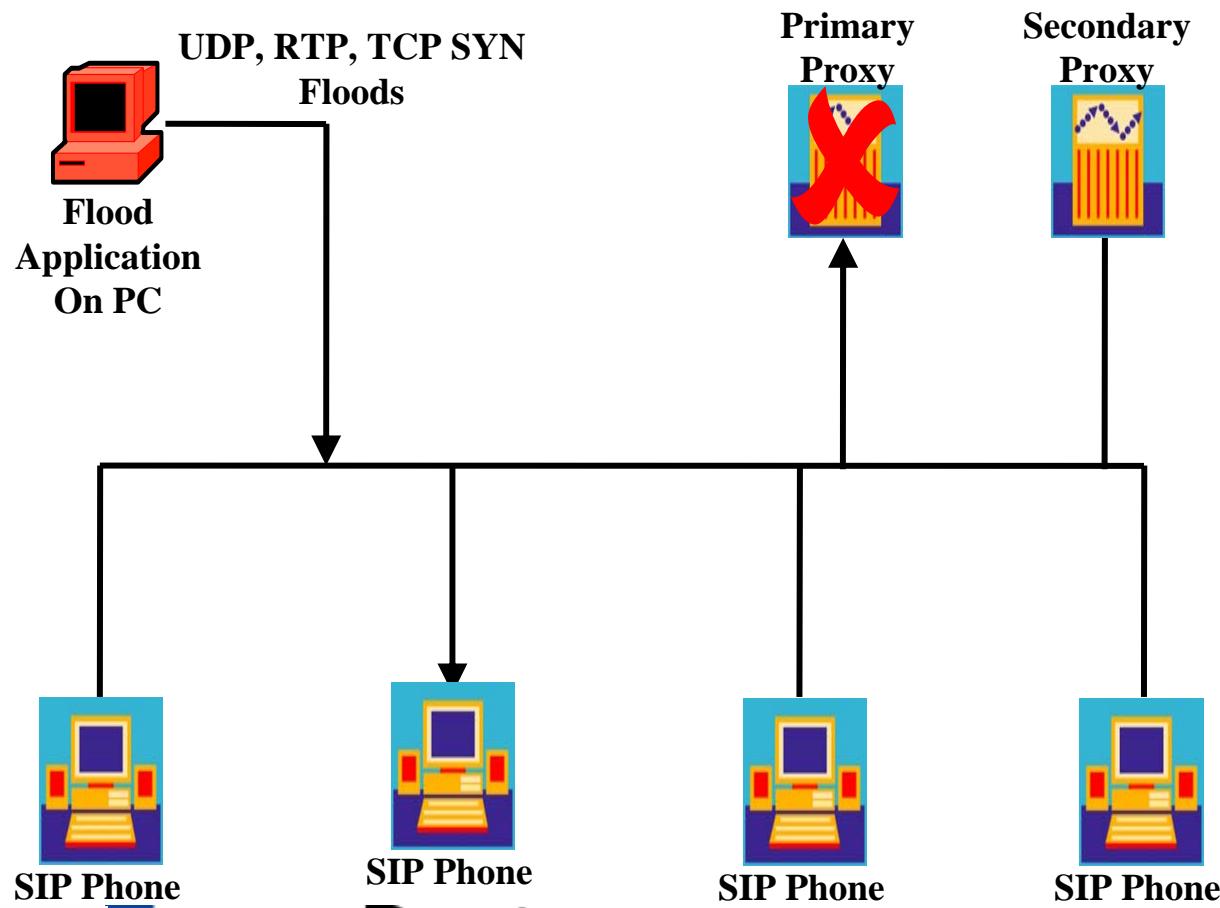
Fuzzing



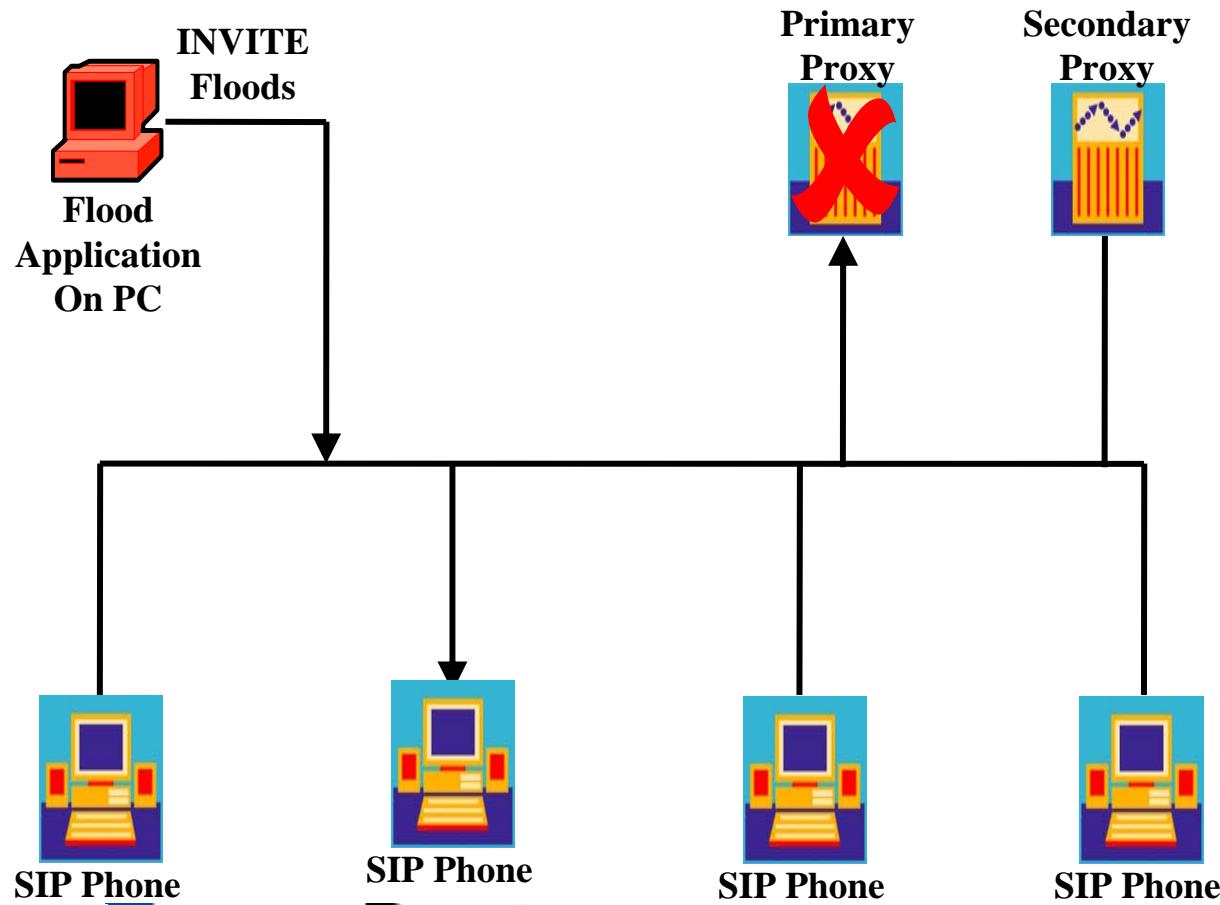
Fuzzing VoIP protocol implementations is only at the tip of the iceberg:

- 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**

Disruption of Service



Disruption of Service



INVITE Flood



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
INVITE	UDP	:bogus	@10.1.101.2	5060
Via:	SIP/2.0/TCP 10.1.101.3		Branch	mro6stKhVvxBzI
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=
```

Start Stop

Source Port: 5060 Packets to Send: 1000000

Message Generation Progress: 48% Randomize Source Port

Conversation Log

```
INVITE sip:bogus@10.1.101.2 SIP/2.0
Via: SIP/2.0/TCP 10.1.101.3;branch=mro6stKhVvxBzI
From: root <sip:root@10.1.101.3>;tag=TiplajEKMq
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
```

Check Sync Reboot



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
NOTIFY	UDP	: 501	@ 192.168.1.51	2051
Via:	SIP/2.0/UCP 192.168.1.103;branch=LrKgHxUyoKybfv			
To:	root <sip:root@192.168.1.51>			
From:	root <sip:root@192.168.1.103> ; tag= bhOmiBuyQW			
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			
<input type="checkbox"/> Use SD...				

SDP message

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

Source Port: 5060
Packets to Send: 1
Randomize Source Port:

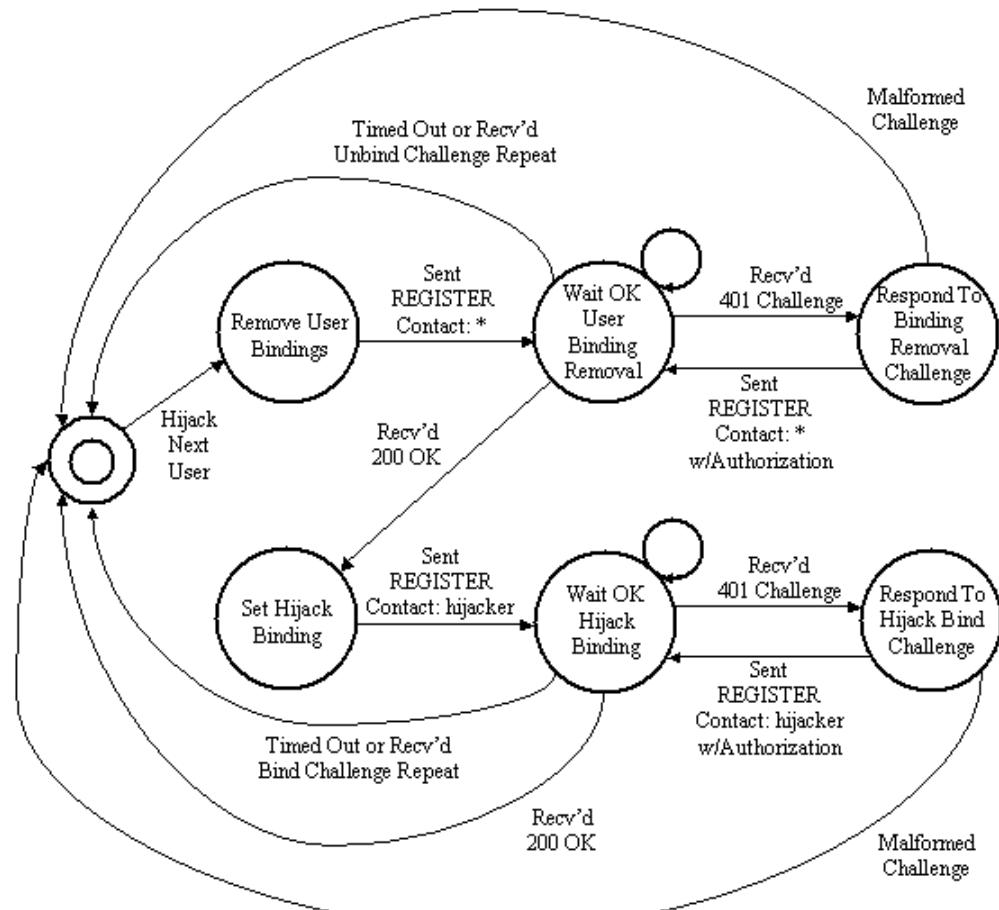
Message Generation Progress: Completed

Conversation Log

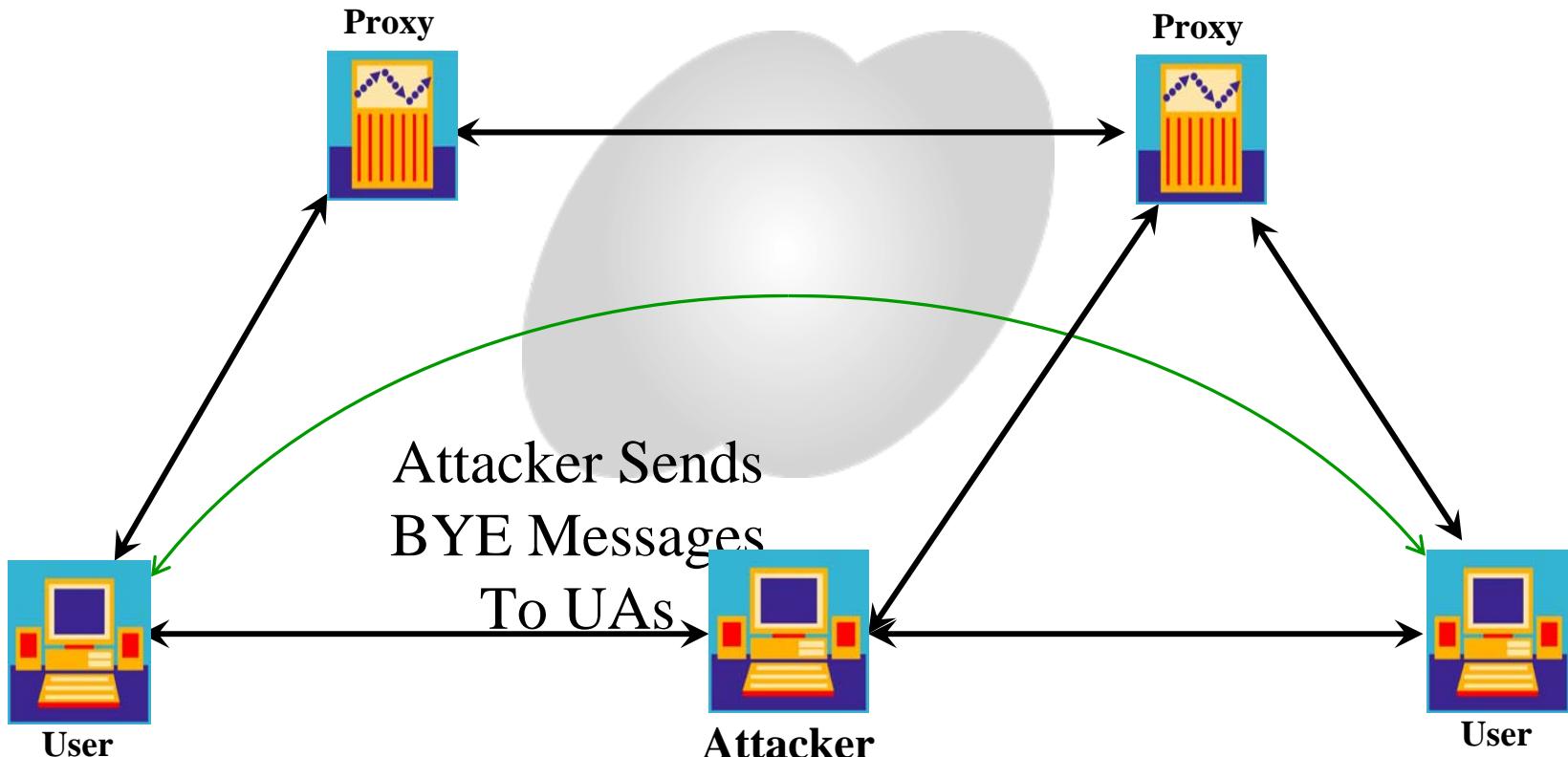
```
NOTIFY sip:501@192.168.1.51 SIP/2.0
Via: SIP/2.0/UCP 192.168.1.103;branch=LrKgHxUyoKybfv
From: root <sip:root@192.168.1.103>;tag=bhOmiBuyQW
To: root <sip:root@192.168.1.51>
Call-ID: 1p0ouD1PvTHS@192.168.1.56
CSeq: 123456 NOTIFY
Max_forwards: 70
User Agent: SiVuS Scanner
Event: check-sync
Content-Type: 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=LrKgHxUyoKybfv
From: root <sip:root@192.168.1.103>;tag=bhOmiBuyQW
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
```

Signaling Manipulation



Signaling Manipulation



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/UCP 192.168.1.53 Branch LrKgHxUyoKybfv			
To:	root <sip:root@192.168.1.53>			
From:	root <sip:root@192.168.1.51> ; tag= bhOrniBuyQW			
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 SD...

SDP message

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

Start Stop

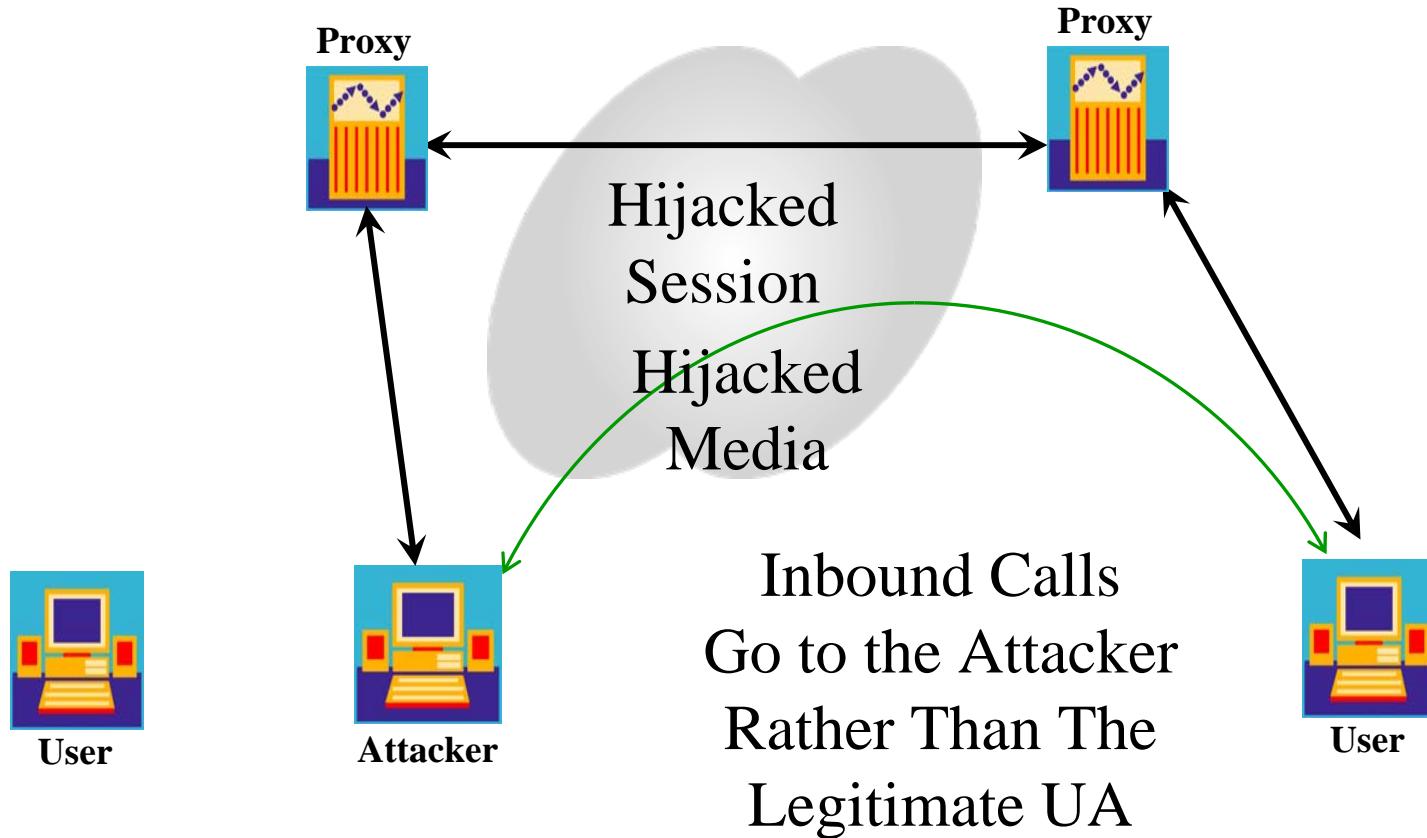
Source Port 5060 Packets to Send 1

Randomize Source Port

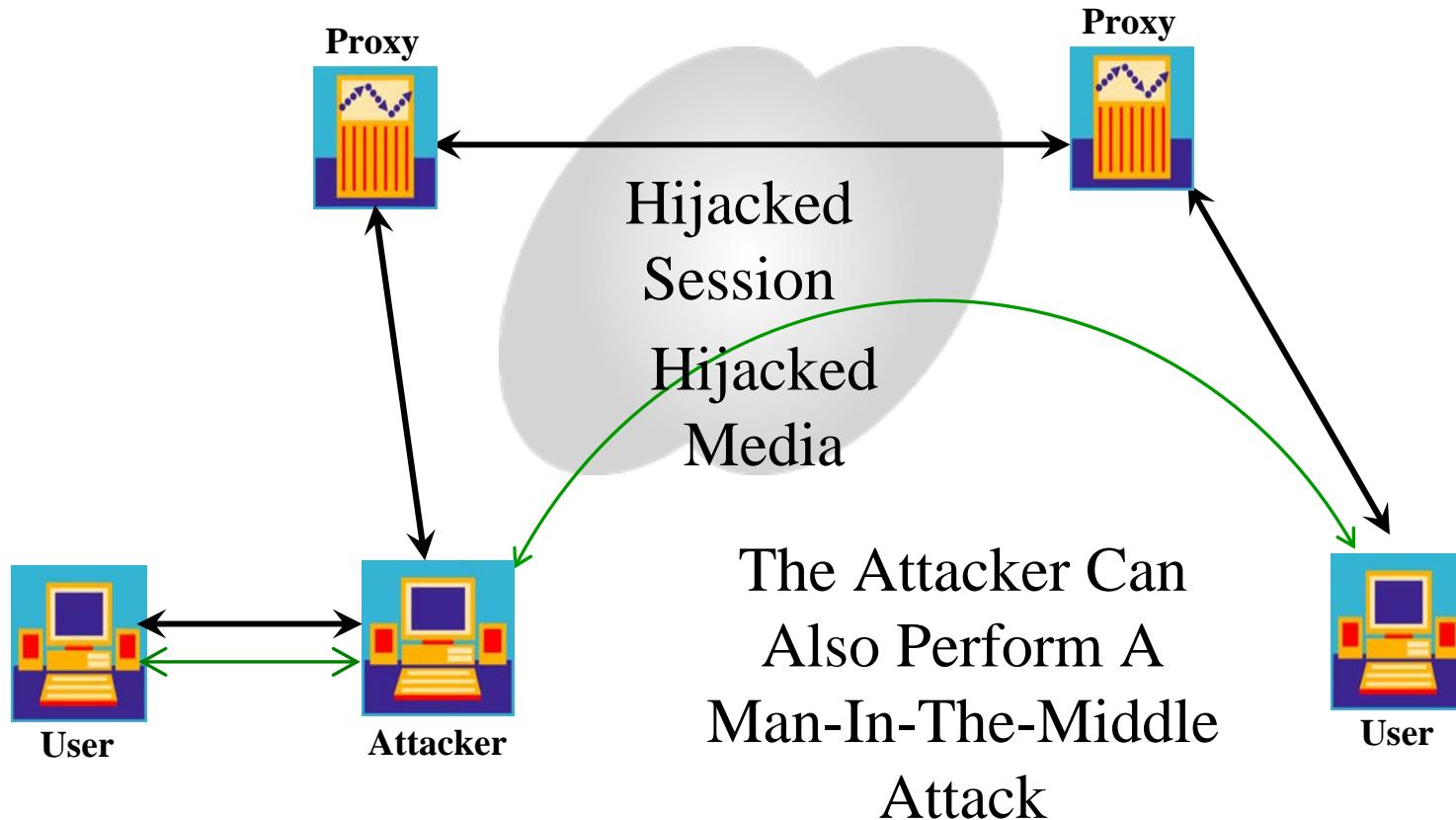
Message Generation Progress Completed

The screenshot shows the SiVuS VoIP Vulnerability Scanner interface. The main window title is "SiVuS - The VoIP Vulnerability Scanner v1.09-beta". The menu bar includes SIP, MGCP, H.323, RTP, and About. Below the menu is a toolbar with SIP Component Discovery, SIP Scanner, Utilities, and SIP Help. The main content area has two tabs: "Message Generator" (selected) and "Authentication Analysis". The "Message Generator" tab displays a SIP message configuration window. The SIP message fields include Method (REGISTER), Transport (UDP), Called User (: 503), Domain/Host (@ 192.168.1.53), and Port (5060). Other fields like Via, To, From, Authentication, Call-ID, Cseq, Contact, Record-Route, Subject, Content-type, User Agent, Expires, Event, Refer-To, and Content Length are also present. Below the SIP message is an SDP message window showing a single line: "v=0 o=user 29739 7272939 IN IP4 192.168.1.2 s=". At the bottom of the message generator window are "Start" and "Stop" buttons, and settings for "Source Port" (5060), "Packets to Send" (1), and a checkbox for "Randomize Source Port". The "Message Generation Progress" bar is shown as "Completed".

Signaling Manipulation



Signaling Manipulation

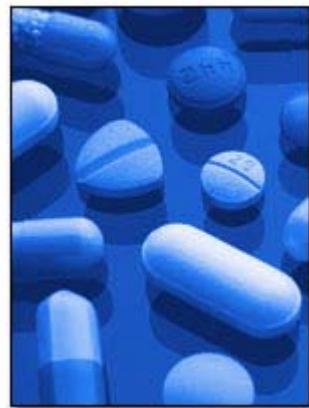


Agenda



- 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



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>



- 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*:

This message was sent with High importance.

From: PayPal Security Center [acc-overview@paypal.com]
To: voipsec@voipsa.org
Cc:
Subject: Confirm your PayPal account

Sent: Fri 7/7/2006 7:54 AM

PayPal®

Account Verification

Dear voipsec@voipsa.org,
You have received this email because we have strong reason to believe that your PayPal account had been recently compromised. In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter.

If your Credit/Debit Card on file is not updated within the next 48 hours, then will assume this account is fraudulent and will be suspended. We apologise for this inconvenience, but the purpose of this verification is to ensure that your PayPal account has not fraudulently used and to combat fraud attempts.

To speed up the process, you are required to call us (1-805-214-4801) to verify your PayPal account.

We apologise in advance for any inconvenience this may cause you and we would like to thank you for cooperation as we review this matter.

Regards,
PayPal Account Verification.
Copyright © 1999-2006 PayPal. All rights reserved.

Please do not reply to this e-mail. Mail sent to this address cannot be answered.

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

Cleaning Nimda Virus from Cisco CallManager 3.x and CallManager Applications Servers [Cisco CallManager] - Cisco Systems - ...

MS Windows W32.Blast.Worm Affects Cisco CallManager and IP Telephony Applications [Cisco Unified CallManager] - Cisco Systems - Mozilla Firefox

MS Windows W32.Blast.Worm Affects Cisco CallManager and IP Telephony Applications [Cisco Unified CallManager] - Cisco Systems - Mozilla Firefox

Cisco Security Advisory: "Code Red" Worm - Customer Impact - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

File Edit View Go Bookmarks Tools Help

Matasano Chargen Metasploit Arbor Networks Secu... Voice of VOIPSA Slashdot SANS - Internet Stor...

http://www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml

Matasano Chargen Metasploit Arbor Networks Secu... Voice of VOIPSA Slashdot SANS - Internet Stor...

Solutions Products Ordering Support Partners Training Corporate

Security Advisories

Cisco Security Advisory: "Code Red" Worm - Customer Impact

Document ID: 46345

Revision 2.3

Last Update 2001 November 01 12:00 UTC

For Public Release 2001 July 20 12:00 UTC

Please provide your [feedback](#) on this document.

Contents

[Summary](#)
[Affected Products](#)
[Details](#)
[Impact](#)
[Software Versions and Fixes](#)
[Obtaining Fixed Software](#)
[Workarounds](#)

Feedback you

Please rate this document

Excellent Good Average Fair Poor

Done Done

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



Voice over IP Security Alliance (VOIPSA) - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

Getting Started Latest Headlines

http://www.voipsa.org/ Go

VOIPSA ACTIVITIES VOIPSEC RESOURCES MEMBERSHIP ABOUT

VOIP 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.

GET INVOLVED NOW!

VOIP SECURITY ARTICLES

Dial VoIP for Vulnerability
Voice over IP offers great savings in long-distance calls. But without extensive safeguards, VoIP can expose your phone system to the havoc affecting the rest of the Web.

Cambridge prof warns of Skype botnet threat
Voice-over-IP apps could be used to cloak networks of zombies, used to launch denial of service attacks, a Cambridge professor has warned.

What will generate the real heat in '06?
It will be the year of voice spam and of the first Trojans, viruses and scams targeted at VoIP rather than

VOIPSA NEWS

October 24 VoIP Security Alliance Delivers VoIP Security Framework

March 28 VoIP Security Alliance Elects Board of Directors, Announces Projects and Issues Call for Participation for everyone

February 07 VoIP Leaders Form Alliance for VoIP Security Research and Testing

VOIPSEC

VoIP traffic model
- Prof. Dr. Christoph Ruland

A different view on the nature of P...
- Paine, Richard H

Voipsec Digest, Vol 14, Issue 5
- Browne, Derek

VoIP, Firewalls and NATs
- Christopher A. Martin

VoIP, Firewalls and NATs
- Mikael Johansson

[JOIN THE VOIPSEC FORUM]

Transferring data from www.voipsa.org...

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