

Voice Over IP Security

Mark D. Collier
Chief Technology Officer
SecureLogix Corporation

mark.collier@securelogix.com
www.securelogix.com
www.voipsecurityblog.com



Outline

Outline

- Introduction
- Gathering Information
- Attacking the Network
- Attacking the Application
- Attacking Vendor Platforms
- Social Attacks
- Traditional System Attacks
- Conclusions and Resources



Introduction

Introduction

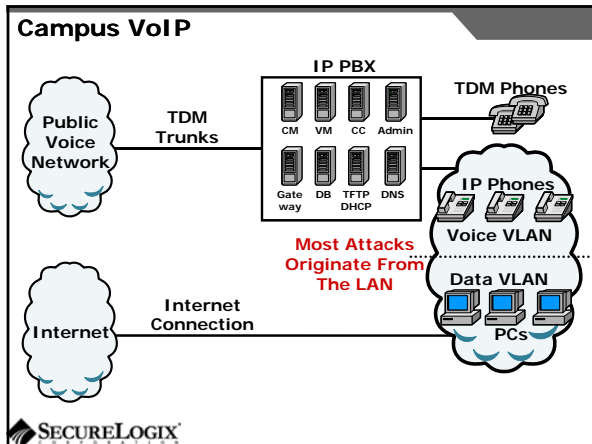
VoIP systems are vulnerable:

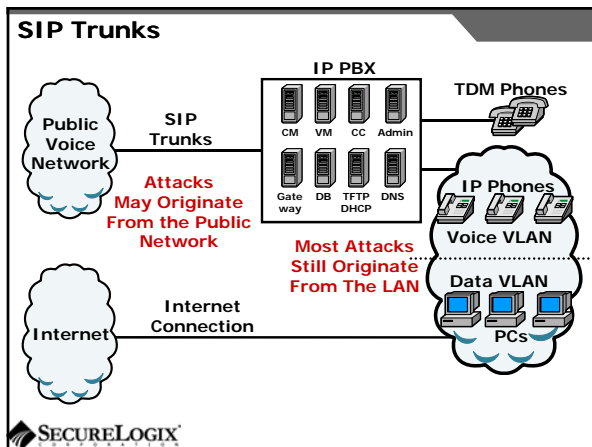
- ◆ Platforms, networks, and applications are vulnerable
- ◆ VoIP-specific attacks are becoming more common
- ◆ Security isn't always a consideration during deployment
- ◆ Application/traditional security is still a big issue

The threat is increasing:

- ◆ VoIP deployment is growing
- ◆ Deployments are critical to business operations
- ◆ Greater integration with the data network
- ◆ More attack tools being published







Footprinting

Gathering Information
Footprinting

First step in gathering information prior to an attack

Footprinting does not require network access

An enterprise website often contains useful information

Google is very good at finding details on the web:

- ◆ Vendor press releases and case studies
- ◆ Resumes of VoIP personnel
- ◆ Mailing lists and user group postings
- ◆ Web-based VoIP logins

SECURELOGIX

Footprinting Countermeasures

- It is difficult to control what is on your enterprise website, but it is a good idea to be aware of what is on it
- Try to limit amount of detail in job postings
- Remove technical detail from help desk web pages
- Be sure to remove any VoIP phones which are visible to the Internet
- Disable the web servers on your IP phones



Scanning

- Process of finding VoIP hosts and running services
- The first step is gaining access to the network:
 - ◆ Insider access
 - ◆ Malware delivered via email, trojan, etc.
 - ◆ Non-secure wireless, modems, etc.
 - ◆ Poorly secured “public” device like a lobby phone
 - ◆ Compromised network device

VLANs are pretty easy to overcome

- ◆ Its possible to hook up a lap top and spoof IP and MAC addresses



Scanning

- Once network access is obtained, next step is to scan for VoIP hosts
- nmap is commonly used for this purpose
- After hosts are found, scans are used to find running services
- After hosts are found and ports identified, the type of device can be determined
- Network stack fingerprinting is a common technique for identifying hosts/devices



Gathering Information
Scanning

Scanning Tools

The image shows three screenshots of network scanning tools. On the left is SuperScan 4.0, a comprehensive scanning tool with various options. In the middle is Nmap, showing its command-line interface and scan results. On the right is MAC Address Discovery, which displays a list of discovered MAC addresses and their corresponding manufacturers.

MAC Address Discovery

IP Address	MAC Address	Vendor
192.168.1.100	00:0C:29:00:00:00	VMware, Inc.
192.168.1.1	08:00:2B:01:00:00	Intel Corporation
192.168.1.20	08:00:2B:01:00:00	Intel Corporation
192.168.1.200	08:00:2B:01:00:00	Intel Corporation
192.168.1.201	08:00:2B:01:00:00	Intel Corporation
192.168.1.202	08:00:2B:01:00:00	Intel Corporation
192.168.1.203	08:00:2B:01:00:00	Intel Corporation
192.168.1.204	08:00:2B:01:00:00	Intel Corporation
192.168.1.205	08:00:2B:01:00:00	Intel Corporation
192.168.1.206	08:00:2B:01:00:00	Intel Corporation
192.168.1.207	08:00:2B:01:00:00	Intel Corporation
192.168.1.208	08:00:2B:01:00:00	Intel Corporation
192.168.1.209	08:00:2B:01:00:00	Intel Corporation
192.168.1.210	08:00:2B:01:00:00	Intel Corporation
192.168.1.211	08:00:2B:01:00:00	Intel Corporation
192.168.1.212	08:00:2B:01:00:00	Intel Corporation
192.168.1.213	08:00:2B:01:00:00	Intel Corporation
192.168.1.214	08:00:2B:01:00:00	Intel Corporation
192.168.1.215	08:00:2B:01:00:00	Intel Corporation
192.168.1.216	08:00:2B:01:00:00	Intel Corporation
192.168.1.217	08:00:2B:01:00:00	Intel Corporation

SECURELOGIX

Gathering Information
Scanning

Scanning Some Well Known Ports

SIP enabled devices will usually respond on UDP/TCP ports 5060 and 5061

H.323 devices use multiple ports, including TCP 1720, UDP 1719

SCCP phones (Cisco) use UDP/TCP 2000-2001

Unistim (nortel) uses UDP/TCP 5000

MGCP devices use UDP 2427

Sometimes you might see UDP or TCP port 17185 (VXWORKS remote debugging!)

SECURELOGIX

Gathering Information
Scanning

Scanning Countermeasures

Use firewalls and Intrusion Prevention Systems (IPSs) to detect and block scans

Using non-Internet routable IP addresses will prevent external scans

VLANs can be used to partition the network

Disable unnecessary ports and services on hosts

Enable logging if possible

Use secure (SNMPv3) version of SNMP

Change SNMP public strings

SECURELOGIX

Enumeration

Gathering Information
Enumeration

Involves testing open ports and services on hosts to gather more information

Includes running tools to determine if open services have known vulnerabilities

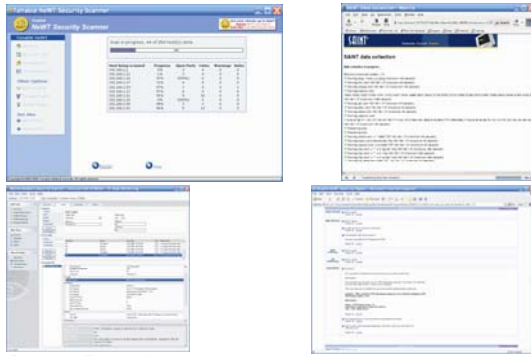
Also involves scanning for VoIP-unique information such as phone numbers

Includes gathering information from TFTP servers and SNMP



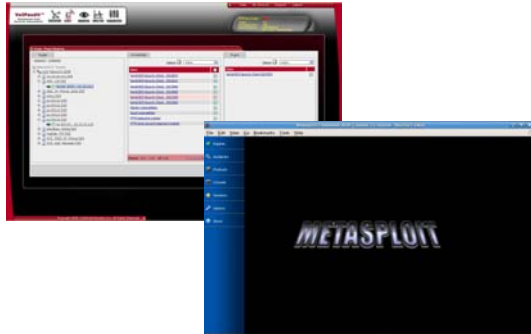
Enumeration Vulnerability Scanning Tools

Gathering Information
Enumeration



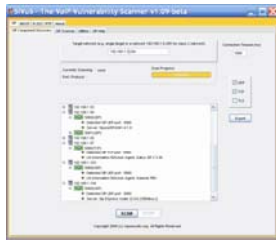
Enumeration Vulnerability Scanning Tools

Gathering Information
Enumeration



Enumeration Directory Scanning

Gathering Information
Enumeration



Enumeration SNMP

Gathering Information
Enumeration

SNMP is enabled by default on most IP PBXs and IP phones

If you know the device type, you can use snmpwalk with the appropriate OID

You can find the OID using Solarwinds MIB

Default “passwords”, called community strings, are common



Enumeration TFTP

Gathering Information
Enumeration

Almost all phones use TFTP to download their configuration files

The TFTP server is rarely well protected

If you know or can guess the name of a configuration or firmware file, you can download it without even specifying a password

The files are downloaded in the clear and can be easily sniffed

Configuration files have usernames, passwords, IP addresses, etc. in them



Enumeration Countermeasures

- Disable unnecessary services
- Enable logging
- Upgrade your applications and make sure you continually apply patches
- Some firewalls and IPSs can detect and mitigate vulnerability scans
- Use authentication or TLS when using SIP
- Consider more secure alternatives to TFTP
- Disable SNMP if not needed. Change community strings.



Network 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 against supporting infrastructure services, such as DHCP, TFTP, DNS, are also possible
- Any direct attack against a network element (IP PBX, switch, router, gateway, etc.) can affect VoIP service



Network DoS Flooding Attacks

- Some types of floods are:
- ◆ UDP floods
 - ◆ TCP SYN floods
 - ◆ ICMP and Smurf floods
 - ◆ Worm and virus oversubscription side effect
 - ◆ QoS manipulation
 - ◆ Application flooding (INVITE floods, REGISTER floods)
- Shared links with large amounts of traffic are especially vulnerable



Network DoS 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



Network DoS Countermeasures

Use QoS to give priority to media and signaling

Use rate limiting in network switches

A firewall or IPS can be used to detects and blocks attacks

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

Host based IPS software also provides this capability

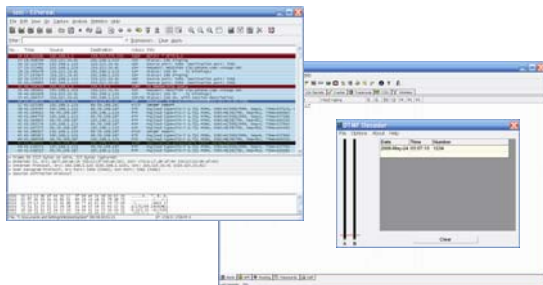
Maintain patches

Configure DHCP servers only lease addresses to known MAC addresses



Network Eavesdropping

VoIP signaling, media, are vulnerable to eavesdropping



Network Eavesdropping Countermeasures

Attacking The Network
Eavesdropping

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



Network Interception

Attacking The Network
Network Interception

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 (registration hijacking)



Network Interception ARP Poisoning

Attacking The Network
Network Interception

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




Attacking The Network
Network Interception

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




Attacking The Application
Fuzzing

Fuzzing

Fuzzing describes attacks where malformed packets are sent to a VoIP system in an attempt to crash it

Research has shown that VoIP systems, especially those employing SIP, are vulnerable to fuzzing attacks



Attacking The Application
Fuzzing


Fuzzing Public Domain Tools

There are many public domain tools available for fuzzing:

- ◆ Protos suite ◆ Scapy ◆ SIP Proxy
- ◆ Asteroid ◆ SipBomber ◆ SIPp
- ◆ Fuzzy Packet ◆ SFTF ◆ SIPsak
- ◆ NastySIP

There are some commercial tools available:

- ◆ Beyond Security BeStorm
- ◆ Codenomicon
- ◆ MuSecurity Mu-4000 Security Analyzer
- ◆ Security Innovation Hydra




Attacking The Application
Fuzzing

Fuzzing Countermeasures

Make sure your vendor has tested their systems for fuzzing attacks

An VoIP-aware firewall or IPS can monitor for and block fuzzing attacks

Consider running your own tests




Attacking The Application
Application Floods

Flood-Based DoS

Several tools are available to generate floods at the application layer:

- ◆ rtpflood – generates a flood of RTP packets
- ◆ inviteflood – generates a flood of SIP INVITE requests
- ◆ regflood – generates a flood of SIP REGISTER requests
- ◆ CRCXflood – generates a flood of MGCP connection requests
- ◆ SiVuS – a tool which a GUI that enables a variety of flood-based attacks

Virtually every device we tested was susceptible to these attacks




Attacking The Application
Application Floods

Flood-Based DoS Countermeasures

There are several countermeasures you can use for flood-based DoS:

- ◆ Use VLANs to separate networks
- ◆ Use TCP and TLS for SIP connections
- ◆ Use rate limiting in switches
- ◆ Enable authentication for requests
- ◆ Use SIP firewalls/IPSs to monitor and block attacks



Signaling/Media Manipulation

Attacking The Application
Sig/Media Manipulation

In SIP and RTP, there are a number of attacks possible, which exploit the protocols:

- ◆ Registration removal/addition
- ◆ Registration hijacking
- ◆ Redirection attacks
- ◆ Session teardown
- ◆ SIP phone reboot
- ◆ RTP insertion/mixing



Signaling/Media Manipulation Countermeasures

Attacking The Application
Sig/Media Manipulation

Some countermeasures for signaling and media manipulation include:

- ◆ Use digest authentication where possible
- ◆ Use TCP and TLS where possible
- ◆ Use SIP-aware firewalls/IPSs to monitor for and block attacks
- ◆ Use audio encryption to prevent RTP injection/mixing



Attacking The Platforms

Attacking The Platform

The major vendors, including Nortel, Cisco, and Avaya all offer strong security

Some default configurations are not as secure as they should be

The major vendor systems are vulnerable to the types of attacks described so far

The major vendors offer additional security measures – but it is up to the customer to use them



Nortel CS1000

Attacking The Platform
Nortel

The CS1000 is Nortel's enterprise class PBX
Uses VxWorks or RHEL 4 as the operating system
Uses Nortel's proprietary UNISlim protocol for signaling.
Can use H.323 and SIP
Nortel has the expected set of ports open on their systems
Nortel uses TFTP and SNMP
Nortel IP Line Fundamentals and Nortel IP Phone
Fundamentals are great resources



Nortel Advisories/Exploits

Attacking The Platform
Nortel

Advisories:

- ◆ CS1000 ELAN Remote Denial of Service Vulnerability
- ◆ Nortel UNISlim IP Softphone Buffer-Overflow
- ◆ Nortel IP Phone forced re-authentication
- ◆ Nortel IP Phone Surveillance Mode

Exploit tools:

- ◆ dial
- ◆ terminateConnection
- ◆ pickupPickup
- ◆ changeDisplay



Avaya Communication Manager

Attacking The Platform
Avaya

The Avaya Communication Manager is Avaya's enterprise-class offering
Avaya uses Linux and VxWorks as the underlying operating system on many components
Uses H.323 with proprietary extensions for signaling. Can use SIP
Avaya has the expected set of ports open on their systems
Avaya uses TFTP and SNMP
Some great information on their website
support.avaya.com/security/



Attacking The Platform
Avaya


Avaya Advisories/Exploits

Advisories:

- ◆ Apache HTTP Server 2.2.6, 2.0.61 and 1.3.39 'mod_status' Cross-Site Scripting Vulnerability
- ◆ PHP Chunk_Split() Function Integer Overflow Vulnerability
- ◆ Apache Mod_AutoIndex.C Undefined Charset Cross-Site Scripting Vulnerability

Exploits:

- ◆ Vnak
- ◆ H22regreject



Attacking The Platform
Avaya

Cisco Unified Call Manager

The Cisco Unified Call Manager is Cisco's enterprise class offering


Version 4.1 is based on Windows. Versions 5.x and 6.x are based on Linux

Uses SCCP (skinny) for signaling. Also uses H.323 and MGCP and can use SIP

Cisco has the expected set of ports open on their systems

Cisco TFTP and SNMP

A Must Read Document is the Solution Reference Network Design (SRND) for Voice communications



Attacking The Platform
Cisco

Cisco Media Gateways


Cisco integrates media gateway functionality into routers

Cisco media gateways use MGCP or H.323

MGCP uses UDP port 2427 and is susceptible to a range of attacks including DoS

H.323 is susceptible to a range of attacks including toll fraud, which is not visible to the Call Manager

Attacks against media gateways can affect all external traffic and/or generate large amounts of toll fraud




Attacking The Platform
Cisco

Cisco Advisories/Exploits

Advisories:

- ◆ CUCM SQL Injection and Cross-Site Scripting Vulnerabilities
- ◆ CUCM and Openser SIP Remote Unauthorized Access Vulnerability
- ◆ CUCM Remote Denial of Service and Buffer Overflow Vulnerabilities
- ◆ CUCM CTL Provider Heap Buffer Overflow Vulnerability



Social Attacks
Voice SPAM

Voice SPAM


Voice SPAM refers to bulk, automatically generated, unsolicited phone calls

Similar to telemarketing, but occurring at the frequency of email SPAM

Not an issue yet, but will become prevalent when:

- ◆ The network makes it very inexpensive or free to generate calls
- ◆ Attackers have access to VoIP networks that allow generation of a large number of calls

It is easy to set up a voice SPAM operation, using Asterisk, tools like “spitter”, and free VoIP access



Social Attacks
Voice SPAM


Voice SPAM Countermeasures

Some potential countermeasures for voice SPAM are:

- ◆ Authenticated identity movements, which may help to identify callers
- ◆ Legal measures

Enterprise voice SPAM filters:

- ◆ Black lists/white lists
- ◆ Approval systems
- ◆ Audio content filtering
- ◆ Turing tests



VoIP Phishing

Social Attacks
Phishing

Similar to email phishing, but with a phone number delivered through email or voice

When the victim dials the number, the recording requests entry of personal information



VoIP Phishing Countermeasures

Social Attacks
Phishing

Traditional email spam/phishing countermeasures come in to play here.
Educating users is a key



Traditional System Attacks

Traditional System
Attacks

Legacy systems still account for approximately 90% of enterprise handsets

Legacy public trunks still account for approximately 99% of public access

Legacy issues are still common and many do not “go away” with VoIP

Common issues include:

- ◆ Unauthorized and poorly secured modems
- ◆ Toll fraud



Traditional System Attacks


Traditional System Attacks Modem Issues

Unauthorized modems are very common

Users connect analog lines to PCs with modems and have unmonitored access to the Internet

Poorly secured, authorized modems are also common

Many critical PBXs are managed via modems




Traditional System Attacks

Traditional System Attacks Toll Fraud

Despite lower rates, toll fraud remains a major issue, especially for international calls

Toll fraud does not go away with VoIP

As covered earlier, toll fraud can actually be easier to enact with VoIP systems




Traditional System Attacks

Traditional System Attacks Countermeasures

Class restrictions in PBXs can help, but are unique to each system

Firewalls such as those provided by the SecureLogix ETM System can detect and mitigate these attacks



Conclusions

Conclusions

The most prevalent threats to VoIP deployments today are denial of service, and hacking of the underlying and supporting infrastructure

The major IP PBX vendors can be secured, but security has to be considered during deployments

It's important to consider your existing network security posture first before adding VoIP components

A VoIP security assessment and penetration test will help identify vulnerabilities

Don't ignore legacy threats – they are much more common than VoIP threats right now



Some Resources

Conclusions

www.voipsa.com

www.blueboxpodcast.com

www.voipsecurityblog.com

www.nortel.com

www.cisco.com

www.avaya.com

www.securelogix.com