Protect Yourself Against VoIP Hacking

Mark D. Collier
Chief Technology Officer
SecureLogix Corporation
What Will Be Covered

How to assess the security of your IPT network:

- In house/external and ground rules/scope
- Discovery
- Security policy review and physical security checks
- Platform tests
- Network tests
- Application tests
- Links
Ground Rules and Scope

Internal or with external consultants

Ground rules:
- Internet and/or internal access
- How much information to start with
- Which group to work with, if any
- Agree how intrusive the test will be

Scope:
- Number of sites
- Which systems/components to test
Internal Access?

- Public Voice Network
- TDM Trunks
- IP PBX
- TDM Phones
- Voice VLAN
- Data VLAN
- IP Phones
- PCs
- Internet Connection
- Internet
External Access?

Public Voice Network

Internet

IP Telephony Connection

IP PBX

TDM Phones

IP Phones

Voice VLAN

Data VLAN

Pcs

Internet Connection
Policy Review/Physical Security

Review IP Telephony security policy:

- Use as a guide to verify IP Telephony system configuration

Physical security:

- Essential for core components
- If the network is not physically secure, many attacks are trivial for insiders
- All other security is moot if physical security is lacking
- Don’t forget to protect the IP phones
Security Policy/Physical Security Recommendations

Develop a written IP Telephony security policy.

Follow the security policy

Protect all core IP Telephony components

Enable protections for the IP phones

Control access to “public” IP phones
Discovery - Footprinting

Search enterprise web site:

- Job listings
- Names, extensions, organization structure
- Voice mail greetings

Use Google to search for:

- Case studies/vendor Press Releases
- User resumes and postings
- Web based IP Telephony logins
- Vendor user forums
Discovery - Footprinting

Google search results for "Network Configuration cisco" showing Cisco Systems, Inc. network configuration results.

Mozilla Firefox window showing a network configuration interface with details such as IP address, MAC address, hostname, and other network configuration parameters.
Discovery - Scanning

Use various available tools to find more IP addresses:

- **fping** and **nmap**

Identify IP Telephony systems:

- Identify the system
- Identify operating system and software versions
- **nmap** is probably the best tool for this
- **nmap** has a very good database for IP Telephony
- Some commercial scanners support this as well
Discovery Recommendations

Remove what you can from corporate web site
Use google to determine your exposure
Make sure no systems are visible on the Internet
Make sure firewalls block scans
Platform – IP PBX

Test for open or unnecessary network ports:

- `telnet` or other remote access
- Find application ports for later testing

Test operating systems for known vulnerabilities:

- Use general vulnerability scanners
- Use IP Telephony-specific scanners where possible

Test for default or weak passwords

Test for default configuration weaknesses
Test for SNMP weaknesses:

- Simple SNMP sweeps can provide a lot of information
- If you know the device type, you can use `snmpwalk`
- You can find the OID using **Solarwinds** MIB database
Platform – Support Services

Test DHCP and DNS

Test provisioning database

Test TFTP for open or unnecessary network ports:

- Many IP phones use TFTP for configuration/image files
- TFTP is rarely secured
- Use `tftpbrute` to guess the filename and download it
- Configuration files have usernames, passwords, etc.
- It may also be possible to corrupt a software image
Platform – IP Phones

Test for open or unnecessary network ports:
- `telnet` or other remote access
- Find application ports for later testing

Test for default or weak passwords

Test for weak local physical protections
- Administrative access for some IP phones can be obtained when they are rebooted
Platform – IP Phones

You can do some interesting things if you get access to certain IP phones
Platform Recommendations

Remove unnecessary network services
Use secure network administration services
Use firewalls to block enumeration attempts
Use strong passwords – change them periodically
Use secure versions of SNMP
Secure DHCP, DNS, and database services
Avoid use of TFTP if possible
Prevent local manipulation of IP phones
Network – General

The data network is used to transport IP Telephony signaling/media

Any component is a potential target

Test security on switches, routers, hubs, VPNs, etc.

The IP Telephony network enables attacks such as:

- Denial of Service (DoS)
- Eavesdropping
- Man-in-the-Middle (MITM) attacks

Test to determine if the network is vulnerable
Network – DoS/Eavesdropping/MITM

Test for network DoS vulnerabilities:

- UDP floods
- TCP SYN floods

Test for eavesdropping:

- Easy to do if you have access to unencrypted data
- Test with `ethereal`, `CAIN`, `VOMIT`, `VoIPong`

Test for MITM vulnerabilities:

- Easy to attack depending on network
- Test with `ettercap`, `dsniff`
Network – Man-in-the-middle

Attacker Places Themselves Between Proxies Or Proxy/UA
Network Recommendations

Use NAC or other means of controlling network access

Use rate limiting on switches to control DoS

Use signaling and media encryption to prevent eavesdropping

Configure switches to prevent MITM attacks
Application - General

The “application” consists of the actual IP Telephony signaling and media exchanged over the network.

The various components generating/consuming this information can be vulnerable to attack.

This will be especially true when IP Telephony is exchanged with a public network.

The examples used are for SIP, but similar issues exist with other protocols.
Enumeration involves identification of valid users:

- Quite a few tools available
- SiVuS and SIPSCAN automate much of this for you:

![SiVuS](image1)

![SIPSCAN](image2)
“Fuzzing” is a term used to describe functional protocol testing.

Involves sending various forms of malformed protocol requests, to test protocol processing software.

Fuzzing has resulted in identification of many vulnerabilities in protocol processing software.
Application – 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: 0
**Application – Fuzzing**

```
INVITE sip:6713@192.168.26.180:6060;user=phone SIP/2.0
Via:aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
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: 0
```
Application – Fuzzing

Most vendors test their protocol implementations

Still a good idea though to test deployed system

There are freeware and commercial fuzzers available:

- www.ee.oulu.fi/research/ouspg/protos/index.html
- www.codenomicon.com
Application – Service Disruption

There are many types of service disruptions possible.

Testing for them is necessary, to determine if your system is vulnerable.

The following several slides describe several types of possible attacks.
Application – Denial of Service
Application – Denial of Service
Application – Registration Manipulation

Erasing, Adding, or Hijacking a Registration
Application – Registration Manipulation
Application – Registration Hijacking
Application – Session Teardown

Attacker Sends BYE Messages To UAs
Application – Check Sync Reboot

Attacker Sends check-sync Messages To UA
Application – Redirection

Inbound Calls Are Redirected

Attacker Sends “301/302 – Moved” Message

Inbound Calls Are Redirected
Application – RTP Injection/Mixing

Attacker Observes RTP and Injects or Mixes in New Audio
Other Attack Tools

dirscan – active directory scanning
authtool – cracks digest authentication passwords
invite_flood – generates a flood of INVITE requests
register_flood – generates a flood of REGISTER requests
udpflood/rtpflood – generates a flood of UDP or RTP packets
eraseRegistrations – removes a registration
addRegistrations – adds one or more bogus registrations
reghijacker – hijacks a registration (with authentication)
tear down – tears down a call
checkSyncReboot – reboots a phone
rtpinjector – injects/mixes audio
sip_rogue – application level MITM tool

more on the way…
Application – Recommendations

Use application firewalls to monitor signaling and media for attacks

Use authentication to prevent rogue devices from injecting packets

Use encryption prevent signaling and media eavesdropping
Links

SIP attack tools – www.hackingvoip.com
ethereal – www.ethereal.com
wireshark – www.wireshark.com
SiVuS – www.vopsecurity.org
Cain and Abel - http://www.oxid.it/cain.html
Codenomicon – www.codenomic.com
Asterisk – www.asterisk.org
Trixbox – www.trixbox.org
Key Points to Take Home

In order to secure your VoIP network, you must understand the issues.

You need to actively test your network, to find out if vulnerabilities exist.

There are many tools available to enable this.

It is a good idea to enlist the help of a trusted third party to perform or assist with the testing.
QUESTIONS?

Contact:
Mark D. Collier
mark.collier@securelogix.com
www.securelogix.com
(210) 863-9001