IP Telephony Security

Eric Vyncke
Distinguished Consulting Engineer
Session Learning Objectives

- Explain some vulnerabilities in IP Telephony
- Explain how to rely on the network infrastructure to protect IPT
- Explain how IPT itself can be made secure by standard and proprietary protocols
Do You Know What a Phreaker (Voice) or a Hacker (Data) Looks Like?

- Attacks against IP Telephony endpoints
  - Reconnaissance
  - DHCP starvation
  - Eavesdropping/Man-in-the-middle
  - Directed TCP and ICMP attacks

- Attacks against IP Telephony servers
  - Worms, viruses and trojans
  - DoS and DDoS
  - Directed probes, floods

- Attacks against IP Telephony applications
  - Intercept administration and user traffic
  - Exploit programming weakness
  - Rogue servers
  - Toll fraud
Agenda

- IP Telephony in a Nutshell
- Risk Analysis
- Secure the Infrastructure
- Design a Secure IPT Network
- Secure the Voice
IP Telephony in a Nutshell

Configuration server
• Phone software
• Phone configuration

IP Telephony Server
• Phone registration
• Connecting phones
• Billing

1) Booting
2) Configuration
3) Registration
4) Call Signaling
5) Media Stream
Normal IP Telephony Traffic: Booting /1

802.1Q

DHCP Discover

DHCP Offer

DHCP Request

DHCP Confirm

L2 Switch

L3 Router

DHCP Server
Normal IP Telephony Traffic: Booting /2

ARP Request → L2 Switch → L3 Router → Server

ARP Reply

TFTP GET config file (multiple packets)

TFTP DATA (multiple)
Normal IP Telephony Traffic: Signalling/3

TCP/UDP Handshake for SCCP/SIP

SCCP/SIP registration

Key pressed …

Dial tone, ringing tones, …

Listen on UDP port x and send to IP address Y on port z
Normal IP Telephony Traffic: Media Stream /4

ARP Request

- ARP Reply

Dual ARP exchange

RTP Stream over dynamic UDP port
Agenda

- IP Telephony in a Nutshell
- Risk Analysis
- Secure the Infrastructure
- Design a Secure IPT Network
- Secure the Voice
Risk Analysis
Foreword

- The following slides are mainly applicable to Cisco IP phones running SCCP with a Cisco Call Manager
  But are also applicable to other IP Telephony protocols & products: SIP

- Threats
  Attacker has Ethernet or IP access to the network

- Other vulnerabilities are pure voice related
  Toll fraud
  Forwarding call to internal destination
  …
Vulnerabilities: Booting /1

- L2 Switch
- L3 Router

Switch allows only specific VLAN

- 802.1Q

- DHCP Discover
- DHCP Offer
- DHCP Request
- DHCP Confirm

Very little information leakage, mainly MAC address

Rogue DHCP server can reply w/ fake TFTP & router information

DHCP starvation/Pool depletion
Vulnerabilities: Booting /2

- ARP Request
- ARP Reply
- TFTP GET config file (multiple packets)
- TFTP DATA (multiple)

Fake ARP reply (can even be sent after original). Can pretend to be the router in order to get all traffic

Information leakage, can get configuration of any phones

Fake TFTP replies (difficult, must be synchronized w/ requests). Can pretend to be the IPT Server

Very little information leakage, mainly MAC address
Vulnerabilities : Signaling /3

TCP/UDP Handshake for SCCP/SIP

SCCP/SIP registration

Key pressed …

Dial tone, ringing tones, …

Listen on UDP port x and send to IP address Y on port z

Potential DoS against Call Manager (SYN flooding)

Relies on TCP 😊

Difficult to inject packets

Everything in the clear… can be sniffed and modified. Neither confidentiality nor integrity nor authentication
Vulnerabilities: Media Stream /4

L2 Switch

ARP Request

Fake ARP reply (can even be sent after original). Can pretend to be the other phone in order to get all traffic. **ARPSPOOF**

ARP Reply

Dual exchange

RTP Stream over dynamic UDP port

Assume good quality of transmission

Assume that the switch does not flood the frames on all ports. **CAM Flooding or MACOF**
Agenda

- IP Telephony in a Nutshell
- Risk Analysis
- **Secure the Infrastructure**
- Design a Secure IPT Network
- Secure the Voice
Securing the Infrastructure

- **Goal:** protect the voice through the infrastructure
  - Protecting the network element
  - Prevent layer 2 tricks
  - Don’t forget physical security
  - Protect the IPT servers!
Securing the Infrastructure
Protect the Network Elements

- Apply well-known and proven techniques to protect network elements
  - Secure login access
  - Follow sound password and authentication practices
  - Securely configure any network management functions
  - Use logging services to track access and configuration changes
  - NTP Authentication, Routing Authentication, Password encryption, SSH, AAA features, access control for SNMP, block telnet, turn off unused TCP/UDP service
  - Restrict Physical Access!
Securing the Infrastructure
Prevent Layer 2 Tricks

- CAM is the forwarding table for a switch
  Filled dynamically based on source MAC address
  If destination MAC address is unknown => flood frame within VLAN
  **CAM overflow**: sends zillions of fake source MAC to fill CAM
    => learning is disabled
    => all frames are flooded: no confidentiality
  **Prevention: port security** (small and finite number of MAC per port)

- DHCP
  **Rogue DHCP**: malicious (fake DNS, GW) allows for Man in the Middle Attacks
  **Prevention: DHCP snooping**, drop all replies coming from non trusted DHCP servers
Securing the Infrastructure
Prevent Layer 2 Tricks (cont.)

- ARP is the protocol to link MAC & IP addresses
  - **ARP spoofing**: attacked sends fake MAC/IP bindings
    - Redirect traffic to the attacker
    - Breach of confidentiality and integrity
  - **Prevention**: **DHCP snooping** to learn trusted bindings, drop all violation

- Virtual LAN used to logically segregate traffic on physical LAN
  - **VLAN Hopping**: sends/receives frames on another VLAN
  - **Prevention**: well known configuration techniques,
    - **dropping wrong VLAN** frames

- Spanning Tree Protocol, the ‘routing’ protocol, detects loops
  - **Fake BPDU** => re-routing, computation (DoS)
  - **Prevention**: **drop BPDU** on all access port, partially static topology
Securing the Infrastructure
A Word About Physical Security

- Be sure to remember the physical plant in your designs
- Access to network equipment must be controlled
- Keep network equipment well within recommended environmental limits
- Mission critical resources may require dispersion, to provide effective redundancy
- Killing power is an effective DoS attack
Securing the Infrastructure
IPT Servers

- They are essential to IPT
- Protected by
  - Strict security policy enforcement (firewall, …)
  - Host security: IPS, AV, …
  - Applying security fixes
  - RBAC management
Securing IPT Servers
Host-Based Intrusion Prevention

- Policy-Based, not signature based
- Zero Updates
- “Day Zero” support
- Effective against existing & previously unseen attacks
Agenda

- IP Telephony in a Nutshell
- Risk Analysis
- Secure the Infrastructure
- **Design a Secure IPT Network**
- Secure the Voice
Design a Secure IP Telephony Network

- Place all IP telephony servers, and IP phones on different security domains (logically separate networks)
- Enforce a security policy by limiting access from the data network to the IP telephony network
- Enforce security posture everywhere (to prevent worms degrading QoS)
- Place SCCP/SIP/MGCP aware firewalls in front of all IPT servers and gateways
- Design a voice network over a IPsec VPN when IPT is not protected
Firewall and NAT and IP Telephony

- Perform stateful inspection of voice signaling protocols exists for SIP, SCCP, H.323, and MGCP
- Issue if the signaling does not follow the media streams
Without Network Admission Control… Worms can Degrade QoS

1. Non-compliant endpoint attempts connection
2. Connection allowed
3. Infection spreads; endpoints exposed

Turbo worms: Severe impact on network quality
With Network Admission Control
Worms are Contained

1. Non-compliant endpoint attempts connection
2. Quarantine remediation
3. Infection containment; endpoints secured

BRANCH
Cisco Trust Agent

Corporate Net
Remediation
Quarantine VLAN

CAMPUS
Agenda

- IP Telephony in a Nutshell
- Risk Analysis
- Secure the Infrastructure
- Design a Secure IPT Network
- Secure the Voice
Hardening the Endpoints

- Signed firmware
- Signed config files
- Disable
  - PC port
  - Settings button
  - Speakerphone
  - Web access

These Features Were All Introduced in CCM 3.3(3), Except Disable Web Access and Config Signing Which Were Introduced in CCM 4.0
Securing the IP Telephony Itself

- Plain SIP/SCCP protocols:
  - No authentication
  - No integrity
  - No confidentiality

- Secure SIP/SCCP protocols
  - With authentication: using X.509 certificates
  - With integrity and confidentiality
    - Rely on cryptographically secure protocols

- Secure firmware and configuration with RSA signatures
Authentication of IP Phones
Types of Certificates in Phones

- Manufacturing Installed Certificate (MIC)
  - Installed in non-erasable, non-volatile memory
  - Rooted in Manufacturer Certificate Authority

- Locally Significant Certificate (LSC)
  - Installed by local authority
  - Supercedes MIC
  - Can be erased via factory reset
Every Device has a RSA Key Pair & Certificate

Certificates:
• IPT Servers – self-signed
• Phones: MIC or LSC
Certificate Trust List: CTL

- List of devices (certificates) that a device should trust on the network.
- Actually replaces the Certificate Revocation List
  - White list instead of a black list
  - Goal is scalability and performance
- Phones need to trust IPT Servers, TFTP, Gateways, …
  - Created by CTL Client on admin workstation.
  - Signed by USB crypto Token.
  - Loaded to phone during first boot and trusted
  - Reload on each subsequent boot and checked against the previous CTL
Trusted Certificates

Certificate Trust List contains list of trusted devices

IPT Server trust list is contained in dynamic list (i.e. use of CRL, DN must be known, …)

Who am I?

Who do I trust?
Securing TFTP

- TFTP is used to download firmware and configurations into phones
- Many companies disallow TFTP as an insecure protocol
- Cisco solves that by securing the payload that TFTP carries
  - Signed firmware images
    - Introduced in CCM 3.3(3)
  - Signed config files
    - Introduced in CCM 4.0
  - Encrypted config Files
    - Introduced in CCM 5.0

1 On 7905/11/12/40/41/60/61/70/71
2 Not on 05/12/40/60 SCCP Loads
Protecting Signaling
TLS: Transport Layer Security

Supports any application protocol

<table>
<thead>
<tr>
<th>HTTP</th>
<th>SCCP</th>
<th>SIP</th>
<th>LDAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS</td>
<td>TCP</td>
<td>IP</td>
<td></td>
</tr>
</tbody>
</table>

- Needs secure method to exchange shared secret
  - Bi-directional PKI pairs for mutual authentication
  - Shared secret exchanged using RSA
- Computes Hashed Message Authentication Code (HMAC)
  - Allows MD5 or SHA1
- Conventional cryptography using shared secret
  - DES, 3DES, AES
  - RC2, RC4
  - IDEA

- Bi-directional PKI establishes Authentication
- HMAC provides Integrity
- Encryption offers Confidentiality
Protecting the Signaling

TLS is the transport for signed, authenticated and encrypted signaling
SRTP: Secure RTP

- RFC 3711 for transport of secure media
- Uses AES-128 for both authentication and encryption
- High throughput, low packet expansion

<table>
<thead>
<tr>
<th>V</th>
<th>P</th>
<th>X</th>
<th>CC</th>
<th>M</th>
<th>PT</th>
<th>sequence number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>timestamp</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>synchronization source (SSRC) identifier</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>contributing sources (CCRC) identifiers</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>...</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RTP extension (optional)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RTP payload</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SRTP MKI -- 0 bytes for voice</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Authentication tag -- 4 bytes for voice</td>
</tr>
</tbody>
</table>

Encrypted portion

Authenticated portion
Protecting the Media Streams

SRTP is the transport for authenticated and encrypted media
The Complete Picture

IPSec and SRTP to MGCP and H.323 *
Gateways

TLS to SIP Trunks
Including
• In SRST mode
• Over H.323 ICT

SCCP TLS and SRTP Support in 7911/7940/7960/7941/7961/7970/7971

SIP TLS and SRTP Support in 7911/7941/7961/7970/7971

Full Interoperability Between Secure SCCP and Secure SIP

TLS and SRTP for Apps
• Cisco Unity® 4.0(5)
• IPCC 7.0
• CTI
Some Caveats with Firewalls

- If signaling is encrypted, how can firewall inspect the traffic?
- IETF is investigating multiple solutions: MIDCOM, NSIS, …
  Stay tuned

1) Signaling

2) What is this?

3) Media Stream

4) Unknown traffic => Drop!
Simple but Efficient Solution

- Works even if signaling is not see or is encrypted
- Relies on a trusted zone and accept return traffic

2) What is this? I don't care

3) Media Stream

4) From trusted zone
   => Allow and install state

5) Return traffic matches state
   => allow

Trusted device: PSTN gateways, Unity servers
Some Caveats with Multiple Domains…

- Multiple domains => how do build trust end to end?
- Work in progress in SIP environments
- Concept of Session Border Controller

Application gateways for SIP & RTP
Conclusion
## Security Is a Balance Between Risk and Cost

### Cost—Complexity—Manpower—Overhead

<table>
<thead>
<tr>
<th>Bronze</th>
<th>Silver</th>
<th>Gold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default, Easy, No-Brainer</td>
<td>Moderate, Reasonable</td>
<td>New, Hard, Not Integrated</td>
</tr>
<tr>
<td>Basic Layer 3 ACLs</td>
<td>Simple Firewalls</td>
<td>Complex Firewalls</td>
</tr>
<tr>
<td>Standard OS Hardening</td>
<td>Rate Limiting</td>
<td>NAC / 802.1X</td>
</tr>
<tr>
<td>Unmanaged CSA</td>
<td>Catalyst® Integrated Security</td>
<td>Network Anomaly Detection</td>
</tr>
<tr>
<td>Antivirus</td>
<td>VPN—SOHO/Mobile</td>
<td>Security Info Management</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Optional OS Hardening</td>
<td></td>
</tr>
<tr>
<td>SLDAP</td>
<td>Managed CSA/VMS</td>
<td></td>
</tr>
<tr>
<td>Signed Firmware and Configs</td>
<td>Directory Integration</td>
<td></td>
</tr>
<tr>
<td>Phone Security Settings</td>
<td>TLS / SRTP to Phones</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IPSec / SRTP to Gateways</td>
<td></td>
</tr>
</tbody>
</table>
Conclusion

- Security for IPT is usually desirable
- Security for IPT can be delivered
  - Within the network infrastructure
  - By the IPT protocols
- Security is not a barrier for deployment
- BTW: apply the same paranoia to data as well
Further Reading

Outside Publications

- NetworkWorldFusion: Breaking Through IP Telephony  

- US DoD PBX1 and PBX2 Accreditation  

- NIST: ‘Security Considerations for VoIP Systems’  

- eWeek: ‘VoIP Is As Secure As You Make It’  
  http://www.eweek.com/article2/0,1759,1592801,00.asp

- Ziff Davis: ‘Securing Your Network for VoIP’  

- Converge!: ‘Enterprise Security – An Enabler of VoIP’  
  http://www.convergedigest.com/blueprint/ttp04/z4cisco1.asp?ID=141&ctgy=4
Further Reading

Cisco Whitepapers and App Notes

- VTG VP Discusses Cisco's Leadership in Protecting IPT

- CallManager and IP Telephony Design Guides
  www.cisco.com/go/srnd

- SAFE Security Blueprints
  www.cisco.com/go/security

- Cisco IP Telephony Security Collateral
  www.cisco.com/go/ipcsecurity

- 802.1X and IPT Positioning Paper
  Cisco Internal – Contact Your Local Account Team
Further Reading

Cisco Documentation

- Cisco CallManager Security, Virus Protection Guides, and TCP / UDP Port Lists

- Configuring IPSec Between a Microsoft Windows 2000

- Proxy EAPOL-Logoff Release Note

- Signed Firmware Release Note
Q & A