Secure Unified Communications

Daniel Tirado  datirado@cisco.com
Ramón Romero  rromeror@cisco.com
True UC Security Requires a Secure Network AND Secure Telephony

Secure Unified Communications

“Organizations must focus on creating efficiencies across all aspects of UCC ownership. Including: Hygiene, Compliance, Integration, Security & Identity and Management.”
- Key Issues for Unified Communications & Collaboration; Gartner, 3/07
All Your Constituencies Have A Role In Building A Secure UC System

"Participation of a cross-section of relevant IT personnel in the planning process is crucial to a comprehensive and actionable UCC strategic plan." Gartner, March 2007
Secure UC: Today......
Security built as an integrated system

Security as an Option
- Very complex environment
- Higher integration cost
- Slower service / feature roll-out
- Larger management overhead
- Lowest common feature support
- Security risks not mitigated
- Lower reliability

Security as INTEGRAL to System
- Reduced complexity
- Tighter integration between network and applications
- Easier deployment and management
- Lower TCO
Secure UC Best Practices
Secure Unified Communications Risks
Best practice – Threats to Risk mapping

- There is no standard best practices for securing UC systems
- Provide a contextual framework to evaluate your security needs.
  - Identify what needs to be protected
  - How far you need to go to achieve your organizational goals
  - Maps risks to the right solutions
- Threats and Risks provide the context for what countermeasures to employ
- Security Policy embodies the goals of the organization and the guidelines for achieving a secure system
- Countermeasures should be based around a defense in depth architecture that leverages security functions in
  - Call Control
  - Endpoints
  - Applications
  - Network
Secure UC Threats and Risks Examples

- Eavesdropping – Greatest perceived risk
  Listening/Recording to audio or video conversations
  **Risk: Loss of Privacy (Regulatory Issues, Reputation)**

- Denial of Service (Internal)
  Loss of service
  **Risk: Loss of Productivity, Safety and Security impact (E911)**

- Compromised System Integrity
  Hacker control of applications or call control infrastructure
  **Risk: Financial (Toll Fraud), Data Theft, Regulatory Issues (Loss of Privacy)**

- Compromised UC Clients (e.g. Softphones)
  Hacker control of platforms that are UC Clients
  **Risk: Financial (Toll Fraud), Data Theft (Customer Information - IPCC Agent Desktop)**
Building A Secure UC System
Protecting all elements of the UC system

Infrastructure
Secure connectivity and transport

Endpoints
Authenticated IP phones, soft clients and other devices

Call Control
Secure Protocols for Call Management Features

Applications
Auto-attendant, Messaging, and Customer Care

Network as the Platform
## Balancing Risk

<table>
<thead>
<tr>
<th>Low \ Easy or Default</th>
<th>Medium \ Moderate and Reasonable</th>
<th>High \ Hard or Not Integrated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Separate Voice &amp; Data VLANs</td>
<td>UC-Aware Firewalls</td>
<td>UC Aware FW w/TLS Proxy</td>
</tr>
<tr>
<td>STP, BPDU Guard, SmartPorts</td>
<td>Encrypted Configuration Files</td>
<td>Rate Limiting</td>
</tr>
<tr>
<td>Basic Layer 3 ACL’s (Stateless)</td>
<td>Remote Access VPN</td>
<td>TLS &amp; SRTP for Phones</td>
</tr>
<tr>
<td>Standard OS Hardening</td>
<td>Security Event Management</td>
<td>802.1X &amp; NAC</td>
</tr>
<tr>
<td>Unmanaged CSA</td>
<td>Optional OS Hardening/Patching</td>
<td>Network Anomaly Detection</td>
</tr>
<tr>
<td>Anti-Virus (Windows Only)</td>
<td>Managed CSA (Windows only)</td>
<td>IPSec &amp; SRTP for Gateways</td>
</tr>
<tr>
<td>HTTPS</td>
<td>DHCP Snooping</td>
<td>Directory Integration (SLDAP)</td>
</tr>
<tr>
<td>Signed Firmware &amp; Configuration</td>
<td>Dynamic ARP Inspection</td>
<td>Scavenger Class QOS</td>
</tr>
<tr>
<td>Phone Security Settings</td>
<td>Dynamic Port Security/Source Guard</td>
<td>Intrusion Prevention Solution</td>
</tr>
</tbody>
</table>
Secure UC Campus
Network Infrastructure Security
Baseline – Intermediate - Advanced

**Basic**
- Spanning Tree Protection
  - BPDU Guard
  - Root Guard
- Basic Access Control Lists (ACLs)
- No static 802.1q trunks
- Separate Voice and Data VLANs
- Cisco Smart Ports (Auto QoS)

**Intermediate**
- User-Based Rate Limiting
- Dynamic Port Security
- DHCP Snooping
- Dynamic ARP Inspection
- IP Source Guard
- ASA/FWSM Firewalling & NAC

**Advanced**
- Advanced QoS (Scavenger Class, etc)
- 802.1x
Why do we need QoS for Security
Cisco Smart Ports

- Why do we need QoS for Security - Availability
  Guarantee service under emergency situation (E911)
  Prevent unauthorized applications gaining priority (P2P etc)

- What is Cisco Smart Ports
  A set of pre-configured macros based on Cisco recommended baselines (Desktop, Switch, Router, Wireless, Phone)
  Makes implementing basic QoS and security easier with Cisco infrastructure
  Available on all currently shipping access switches
  Default policy for voice vlan restricts bandwidth to 128k with rate limiting
  Default policy for voice ports includes Port Security

- What the Benefit?
  Smart Ports simplify secure deployment of access ports
Secure UC - Cisco Security Appliances

Solving UC Security Challenges
Cisco ASA and Secure UC Deployment Topologies

SP SIP Network

Worm/Virus Spyware Exploit

Unwanted Application

Illegal Access

Trusted Network

Untrusted Network
Cisco ASA Features To Protect Cisco Unified Communications Manager

- **Dynamic port opening** for voice and applications
- Ensure SIP, SCCP, H.323, MGCP requests conform to standards
- Prevent inappropriate SIP Methods from being sent to Communication Manager
- Network **Rate Limit SIP Requests**
- Policy enforcement of calls (whitelist, blacklist, caller/called party, SIP URI)
- Enable only “registered phones” to make calls
- Enable inspection of encrypted phone calls
- Use IPS functionality with voice/video signatures to target latest UC vulnerabilities
Large Enterprise Customer Challenge
Solving the Firewall & Encryption Integration Problem

Customer Security policy mandates
- All Servers, including CUCM, must be firewalled for their protection
- Key end users must have all phone calls encrypted

Firewalls need to inspect the signaling traffic to
- Open Media pinholes
- Apply Protocol Conformance
- Apply Application Inspection and Control (AIC)

Encrypted calls must encrypt the signaling (TLS) because phones have the media encryption keys sent to them by CUCM via the signaling

Problem
Two key security functions cannot co-exist or integrate

Customer Options
Choose Encryption or Firewalling, but not Both

Cisco Solution
The ASA TLS Proxy (ASA 8.0)
Encrypted Voice Security Solution
Security – UC – Network Integration

CUCM encrypted calls with SRTP/TLS can now be inspected by Cisco ASA 5500 Adaptive Security Appliances:

- Maintains integrity and confidentiality of call while enforcing security policy through advanced SIP/SCCP firewall services
- TLS signaling is terminated and inspected, then re-encrypted for connection to destination (HW Based encryption)
- Dynamic port is opened for SRTP encrypted media stream, and automatically closed when call ends
Secure UC Remote Access/Mobility

Cisco ASA 8.0.4 Release
Secure Remote Access
Technical Challenges – Data to UC enabled remote access

Demands on Secure Connectivity Today
- Seamless user experience
- Access to a variety of applications including UC and collaboration tools
- Consistent access from a number of diverse clients (IP Phones, Mobile, Laptop)

User Expectations

Device Proliferation
- iPhone, Windows Mobile, Android
- Thin Client/ Embedded

Increased Mobility
- Digital nomads, full-time remote employees, teleworkers

Platform Diversification
- Windows, MacOS, Linux
Cisco ASA 5500 Series UC Proxy Features
Unification of Data and UC Remote Access Services

Simplified and Secure Deployment of Remote phones, Mobile clients, and Presence architectures

Cisco ASA – strategic remote access platform

IPSec VPN  Clientless SSL VPN  SSL VPN  Phone Proxy  Mobility Proxy  Presence Federation Proxy
Cisco ASA Phone Proxy
Remote Access and Voice/Data Segmentation

Secure Remote Access:
- Leverage native Cisco IP Phone encryption (TLS/SRTP) to enable secure calls from IP Phones on untrusted, remote networks
- Seamless deployment and operation with minimal impact on existing UC infrastructure
- Simplified user experience – Plug and play
- A Remote Access UC Solution for UC devices
Cisco ASA Mobility Proxy
Integration with Cisco Unified Mobility Solutions

Secure Mobility: ASA protection for Cisco Mobility Solution

- Core component of mobility architecture
- Converges Mobility onto a common remote access platform
- Protection for Cisco Mobility Protocol (MMP)
- Protection for the CUMA Enterprise Server (TLS Proxy)
Cisco ASA and Presence
Integration with Cisco and 3rd party Presence Solutions

Secure Presence
- Enterprises with Cisco Presence Servers can now collaborate securely with enterprises with Microsoft Presence Servers
- Presence information can be shared between two organizations
- All Cisco ASA UC security capabilities apply to Presence traffic
- Cisco ASA: Strategic Platform for converged remote access and mobility for UC Applications and Services
NAC & IPS
Cisco NAC Profiler

1. NAC Profiler Collector (a software agent running on Cisco NAC Server) discovers and profiles devices and consolidates the information to send to the NAC Profiler Server.
2. NAC Profiler Server aggregates all of the information from the Collectors and maintains a database of all network-attached endpoints (e.g. phones, printers, badge readers, modalities, etc.).
3. NAC Profiler Server continuously maintains the Filters List via the NAC API and provisions the appropriate access decisions (allow, deny, check, “role”, or ignore).
4. NAC Profiler Collector continuously monitors behavior of profiled devices (to prevent spoofing) and updates Profiler Server.
Cisco IPS Business-Protection Solutions

Cisco Unified Communications Protection Solution
Includes Call Devices, Call Manager Applications, Operating Systems, IP Networks, and Voice Protocols

Cisco IPS Unified Call Manager Protection Package
Local Event Correlation
- Call-Anomaly Detection
- Voice and IP Traffic-Aware Detection
- Vulnerability Protection for SIP/SCCP/H.323, etc.
- SIP/SCCP/H.323 Protocol-Anomaly Detection

Traffic Normalization

Intrusion Prevention Solution Platform

Comprehensive, Collaborative Network Intrusion Protection for Business Solutions