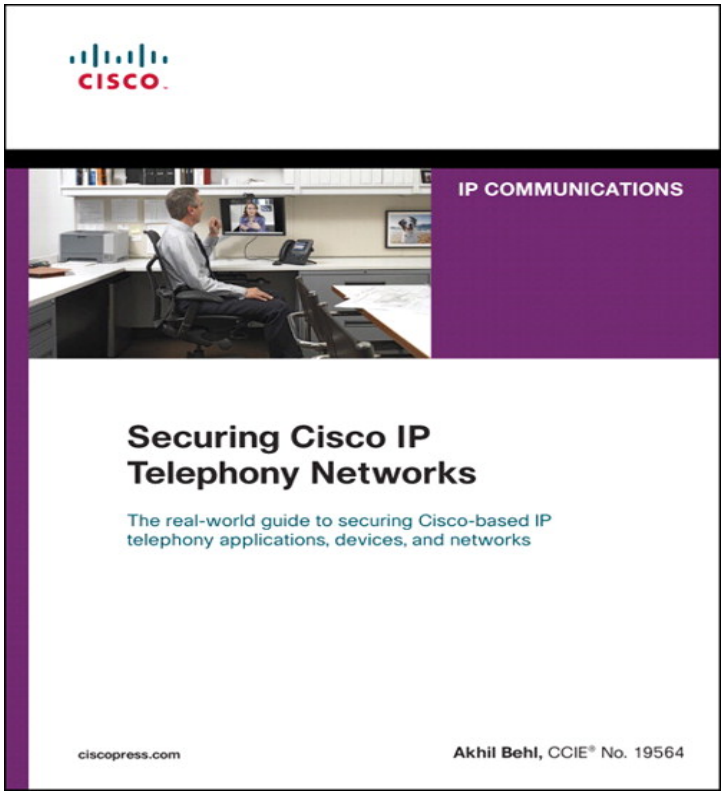
Cisco Support Community Presents
Tech-Talk Series

Understanding Cisco Unified Communications Security

Akhil Behl
Solutions Architect,
akbehl@cisco.com
Author of *Securing Cisco IP Telephony Networks*

Securing Cisco IP Telephony Networks

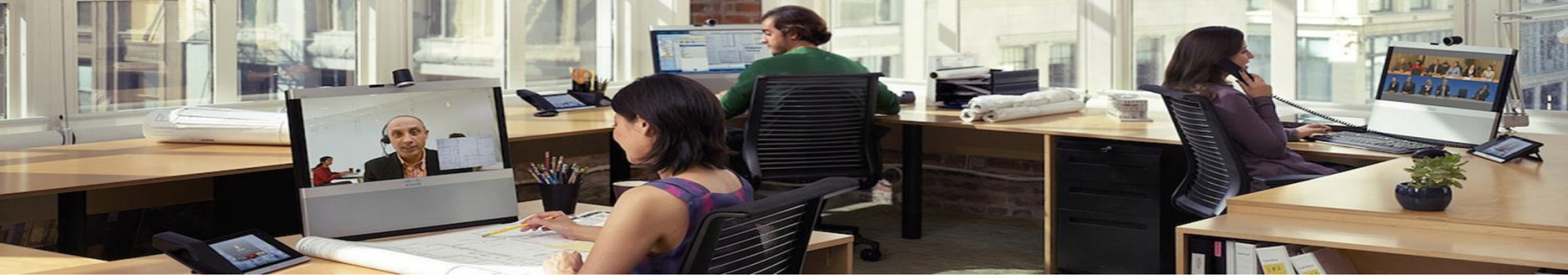


- Addresses the prominent void where UC and Security realms converge
- Security primer for new professional and refresher for experienced professionals
- Covers threats, risk assessment, security strategy development, security framework
- Covers network infrastructure security, UC application security, UC endpoint security, network management security, advance firewalling and Intrusion Prevention

- http://www.ciscopress.com/title/9781587142956
- http://www.amazon.com/dp/1587142953

Agenda

- ✓ Unified Communications Security
- ✓ How to secure Cisco UC products, CUCM/ Unity/CUPS & Cisco IP Telephony endpoints against internal & external threats?
- ✓ Types of certificates used for security of a UC endpoint
- ✓ Questions from the Cisco Support Community



- Data Networks have been under attack since the evolution of Internet. Now with VoIP becoming a part of Data network (utilizing its services) its under attack as well
- Securing Data Networks is the first and foremost step by any organization however, they completely tend to ignore UC Security aspect because of lack of confidence to secure a relatively new technology, cost and complexity involved, and various other factors
- UC Security is best defined as – *Securing what is an asset to an organization's daily life operations*

Threats that Pester the Sanctity of a UC Network

- Toll fraud
- Eavesdropping
- Phishing / Vhishing
- Packet Injection / Manipulation
- Identity Theft
- Denial of Service
- Hijacking calls
- Physical Assault

UC Security – What can be secured?

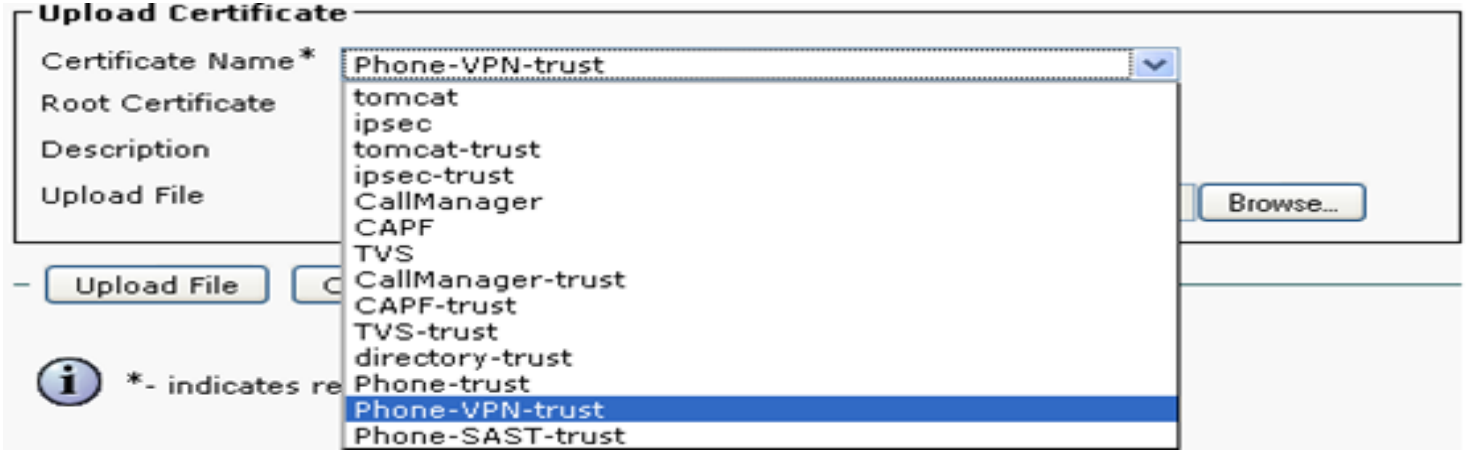
- Secure Network infrastructure (LAN, WAN, Wireless)
- Secure Unified Communications Equipment (Physical Security)
- Unified Communications Application Security (CUCM, CUC, CUPS,)
- Secure Voice, IM, Video, Conference Calls
- Remote Worker / Telecommuter Security
- Endpoint Security, Gateway Security
- Secure Network Management

Preventing Spoofing & Eavesdropping Attacks on UC Solution

- Spoofing attacks can be prevented by leveraging Layer 2 and Layer 3 security mechanisms
- DHCP Snooping, Port Security, Dynamic ARP inspection (DAI) and so on help thwart spoofing at Layer 2
- Eavesdropping can be restrained by using encryption for media and signaling
- Spoofing of Cisco IP Communicator, CUPC, and other soft clients can be prevented by via CAPF

CUCM Certificates

- Security By Default (ITL, TVS)
- CAPF (Secure Conferencing, Voice Calls)
- MIC, LSC
- IPSec
- Secure LDAP / Secure Web Pages (Tomcat)
- VPN Phone



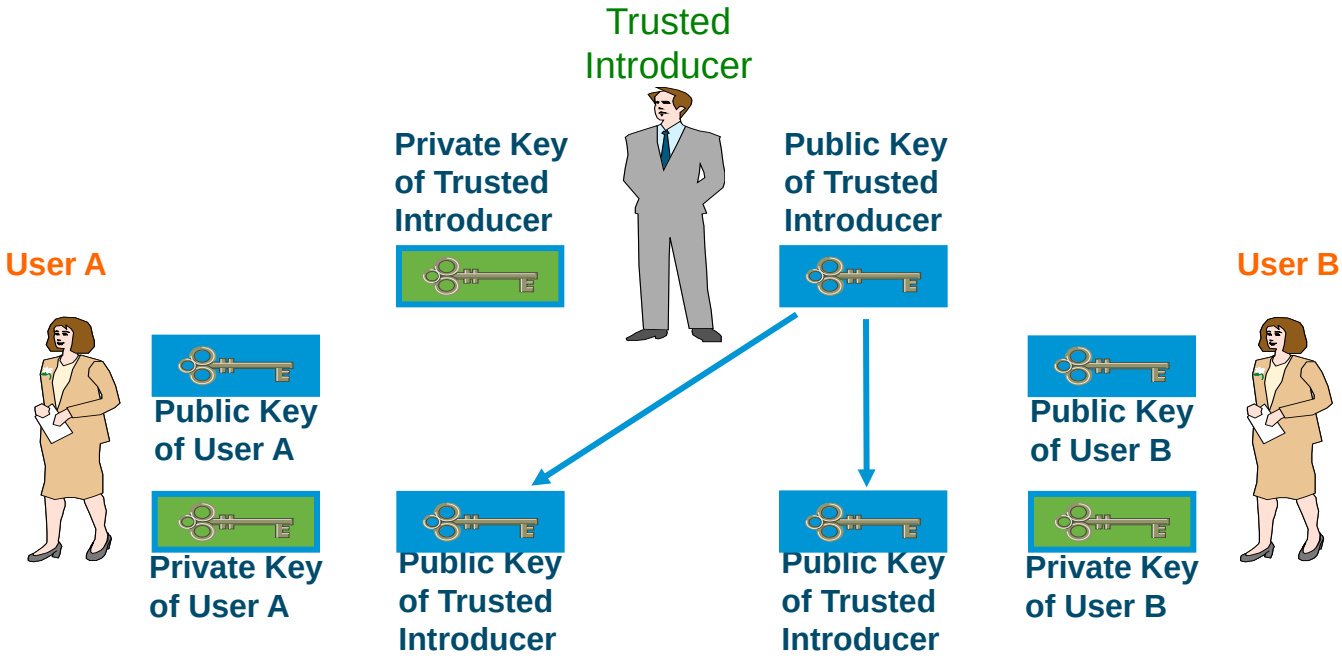
Security By Default (SBD)

- Automatic phone security features
  - Signing of phone configuration files
  - Phone configuration file encryption
  - HTTPS with Tomcat and other Web services
- SBD generates Initial Trust List (ITL) automatically without user intervention upon installation of cluster
- Secure signaling and media still require running the CTL Client and the use of the hardware eTokens

Cisco UC PKI System

- Public Key Infrastructure (PKI) maps certificates to entities to securely validate and verify their identity
- Uses a hierarchical model by adding a **Common Trust Introducer**
- Trust introducer guarantees authenticity and integrity of public keys of other entities by use of certificates, signed by the introducer

Cisco UC PKI Model



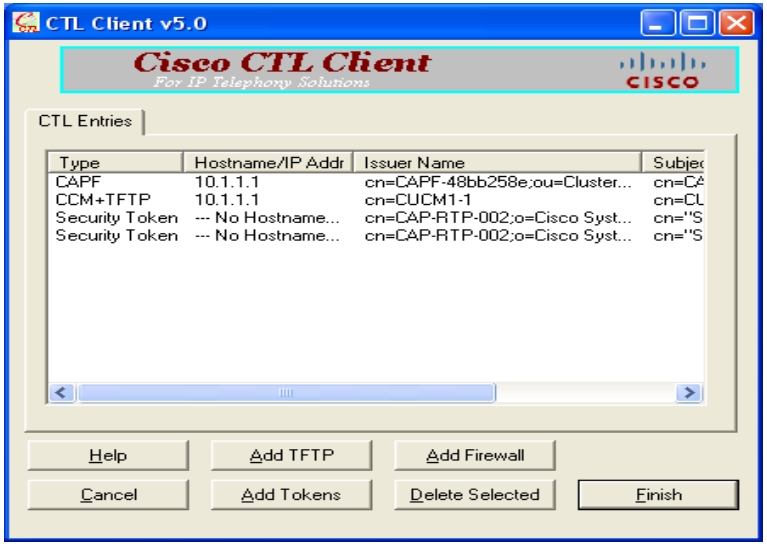
- Every entity, including the trusted introducer, needs to generate its own public & private key pair
- Each entity obtains the public key of the trust introducer and verifies its authenticity & integrity

Q & A

eToken and CTL Client Application

- USB eTokens can be ordered with part number KEY-CCM-ADMIN-K9= or KEYUCM-ADMIN2-K9=
- Cisco CTL client is Windows based software client used to create or update the CTL
- The CTL is signed by Cisco CTL client using the private key from one of the administrator security tokens, which are all signed by the Cisco CA

Security Token



CTL Client

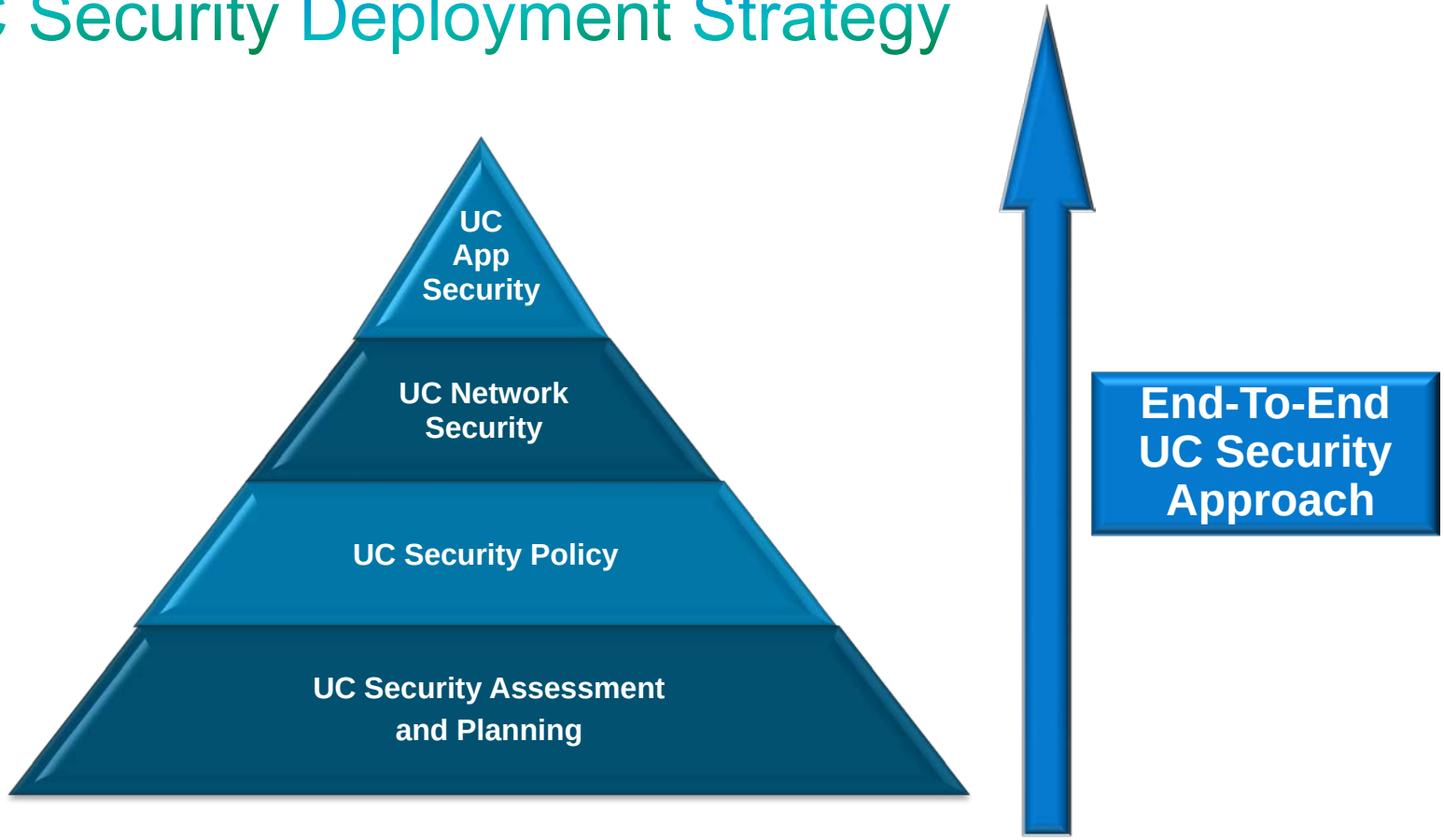
Ports used by UC Applications

- All UC applications have certain common ports for communication with other applications, endpoints & soft clients however, each application has a set of its specific ports. For a list of ports as per the version of application in your network, refer to that product's security guide

- CUCM 9.x Security Guide: http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/security/9_0_1/secugd/CUCM_BK_CCB00C40_00_cucm-security-guide-90.pdf

- Cisco Unity Connection 9.x Security Guide: http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/security/guide/9xcucsecx.html

Cisco UC Security Deployment Strategy

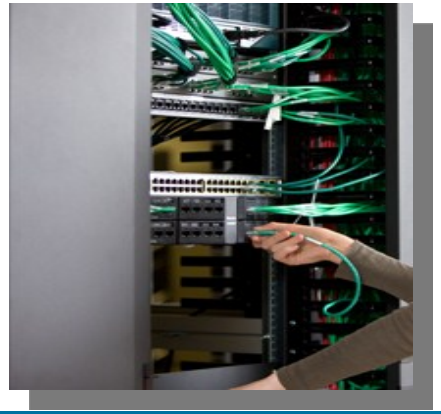


End to End UC Security – Demystified

Physical

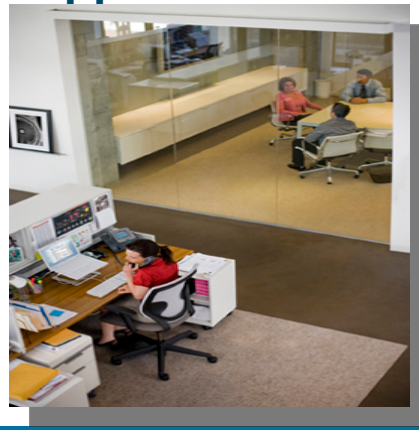
- Building Security
- Data Center Access Security
- Wiring Closet Security
- CCTV Security

Network Security



- Access Layer Security
- Core and Distribution Layer Security
- Wireless Network Security
- Remote Site Security
- Firewalls and Intrusion Prevention

UC Application Security



- UC Platform Security
- Gateway Security, UC Endpoint Security
- UC Application Security
- Ecosystem (3rd Party) Application Security

Thank you.