



## Mitigating Security Threats from a Practical Perspective



**Eric Vyncke**  
**evyncke@cisco.com**  
**Distinguished System Engineer**  
**Cisco Systems**

Evyncke IPT security © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

1

---

## Objectives

- Assuming knowledge of vulnerabilities in IP Telephony
- Explain how to rely on the network infrastructure to protect VoIP
- Explain how VoIP itself can be made secure by standard and proprietary protocols

Evyncke IPT security © 2008 Cisco Systems, Inc. All rights reserved. Cisco Public

2

---

## What Security Do You Have Now?

You Are Running Your Business Critical Applications on Your Network Today

- Is your current network security enough?
- Will VoIP make your network less secure?
- What are the risks of putting VoIP on your current network?
- Will everything you do for security now work with VoIP?

---

## Agenda

- **Secure the IP Telephony Endpoint**
- Secure the Infrastructure
- Design a Secure IPT Network
- Secure the IP Telephony

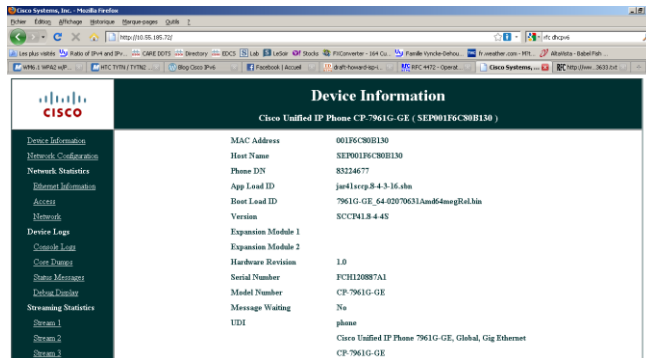
## Threats to IP Telephony Endpoints



- Reconnaissance
- DoS – DHCP starvation, flooding, fuzzing, etc.
- Eavesdropping / Man-in-the-middle
- Directed attacks – SPIT, spoofing, etc.

## Threat: Reconnaissance Browse into a IP Phone

- IP address/mask
- Default gateway
- DHCP server
- DNS server
- TFTP server
- Cisco CallManager(s)
- Directory server
- Logon server
- XML server
- If I'm reconning your network, I can learn an awful lot about your network by webbing into a single phone
- But, disabling web access also breaks XML pushing apps  
    **Instead, use ACLs to only allow port 80 between phones and servers**



## Mitigation: Hardening the Endpoints



- Signed firmware
- Signed config files
- Gratuitous ARP protection
- Hardened software against DoS
- Disable
  - PC port
  - Settings button
  - Speakerphone
  - Web access

Secure Shell Information	
Secure Shell User	<input type="text"/>
Secure Shell Password	<input type="text"/>
Product Specific Configuration	
<input type="checkbox"/> Disable Speakerphone	
<input type="checkbox"/> Disable Speakerphone and Headset	
PC Port *	Disabled
Settings Access *	Restricted
Gratuitous ARP *	Disabled
PC Voice VLAN Access *	Disabled
Web Access *	Disabled
Span to PC Port *	Disabled
Logging Display *	Disabled

## SPIT: SPAM over IP Telephony

- Still largely hypothetical
  - VoIP is mainly within an enterprise
  - Some VoIP in SP are in walled gardens (i.e. isolated from the Internet)
- Most current Firewalls or IDS/IPS won't catch these
- Advances being made
- Authenticated TLS will stop most SPIT attacks – the endpoints only accept packets from trusted devices

---

## Agenda

- Secure the IP Telephony Endpoint
- **Secure the Infrastructure**
- Design a Secure IPT Network
- Secure the IP Telephony

---

## Threats to the Infrastructure



- Denial of Service
  - CPU exhaustion
  - DHCP pool exhaustion
  - Sheer packet flooding
- Man-in-the-middle attack
  - Reroute traffic (ARP spoofing, rogue DHCP) to intercept voice
- Impersonation
  - Pretend to be a phone

---

## 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

- Network devices are used to enforce security policy
- 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 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 Prevent Layer 2 Tricks

- IPv4 layer-2 protection is pretty well understood  
Not everyone is aware of the IPv6 threats & mitigations
- 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.)

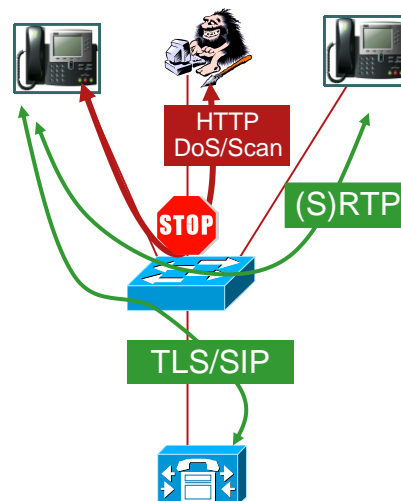
- ARP is the protocol to link MAC & IP addresses
  - ARP spoofing:** attacked sends fake MAC/IP bindings
    - Redirect traffic to the attacker
    - Breach of confidentiality and integrity
  - Prevention: DHCP snooping** to learn trusted bindings, drop all violation
- Virtual LAN used to logically segregate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

Use VLAN ACL (a cheap transparent firewall) to enforce a strict policy to the phones:

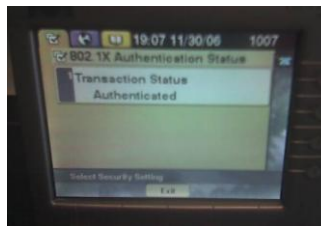
(S)RTP among phones  
HTTP/TLS/SIP with servers  
DHCP/TFTP  
Ping from NOC/servers

- That's all: DENY the rest
  - Phones have no reason to send TCP or ICMP to each other
- Stops all TCP and ICMP attacks against the phones!

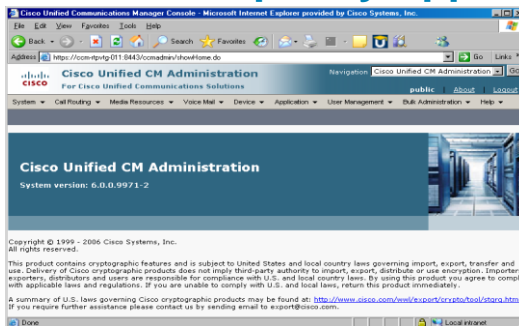


## Securing the Infrastructure Use of IEEE 802.1x to Limit VLAN Access

- Strong authentication of phones
- EAP-MD5  
    With pre-shared key in flash
- EAP-TLS  
    With X.509 cert (see later)



## Threats to IP Telephony Applications



- Intercept (or guess) credentials
- Trick users – Phishing / Pharming
- Exploit programming weakness – Fuzzing
- Toll fraud
- Forward sensitive messages

---

## 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

---

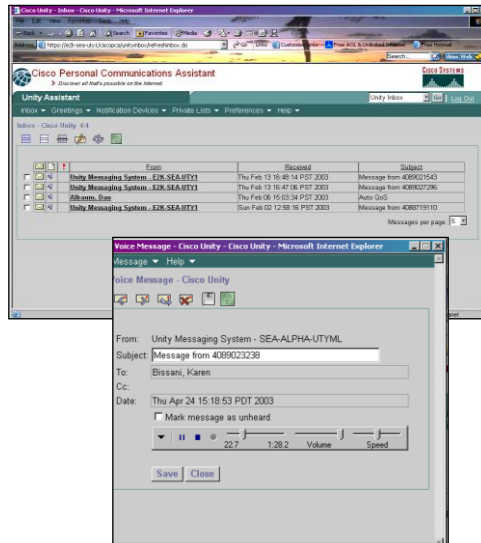
## Prevent User Toll Fraud



- Call forwarding, remote call forwarding, and trunk-to-trunk transfers
- Partitions and Calling Search Spaces limit what parts of the dial plan certain phones have access to
- Dial plan filters control access to exploitive phone numbers
- Ad hoc conference calls can optionally be dropped when the originator hangs up
- Forced Authentication Codes or Client Matter Codes prevent unauthorized calls and provide a mechanism for billing and tracking

## Private Secure Messaging

- Encrypts voicemail messages
- Only intended recipients have the keys to decrypt
- Can't be forwarded



## Agenda

- Secure the IP Telephony Endpoint
- Secure the Infrastructure
- **Design a Secure IPT Network**
- Secure the IP Telephony

---

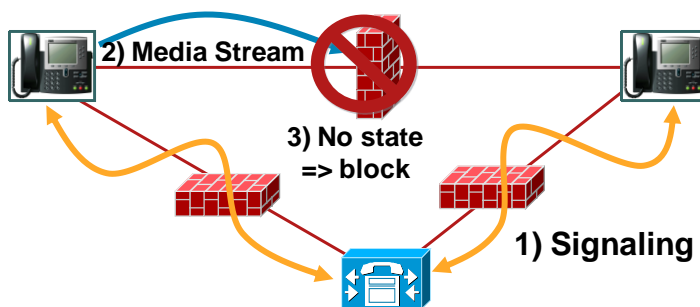
## Design a Secure IP Telephony Network

- Place all IP telephony servers, and IP phones on different security domains (logically separate networks)  
Interesting fact: people starts deploying IPv6 IPT
- Enforce a security policy by limiting access from the data network to the IP telephony network
- 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 (or 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



---

## Agenda

- Secure the IP Telephony Endpoint
- Secure the Infrastructure
- Design a Secure IPT Network
- **Secure the IP Telephony**

---

## 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

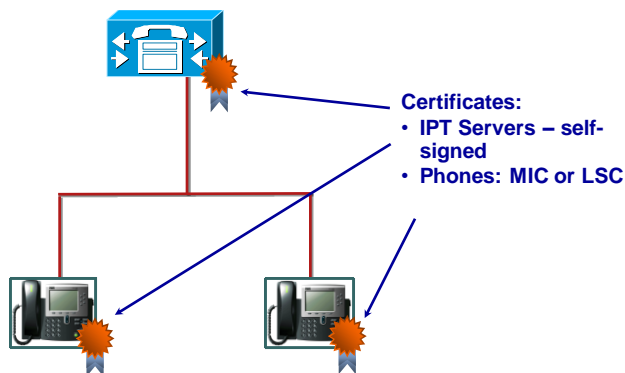
---

## 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
  - Supersedes MIC
  - Can be erased via factory reset

---

## Every Device has a RSA Key Pair & Certificate



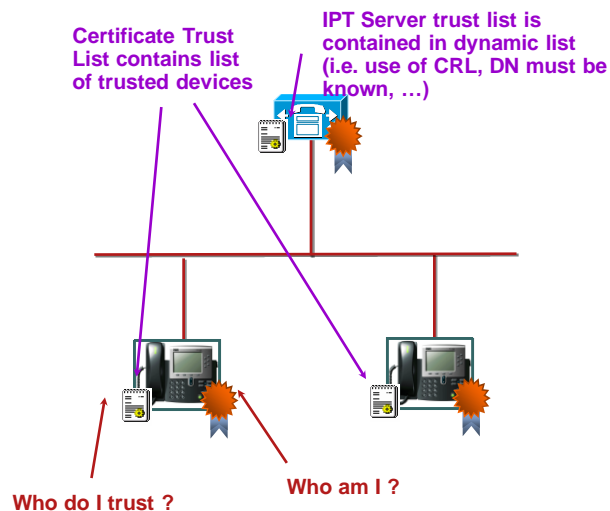
---

## 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.
  - Loaded to phone during first boot and trusted
  - Reload on each subsequent boot and checked against the previous CTL

---

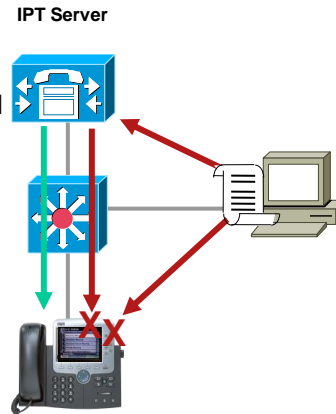
## Trusted Certificates



## 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  
Signed config files  
Encrypted config Files



## Protecting Signaling TLS: Transport Layer Security

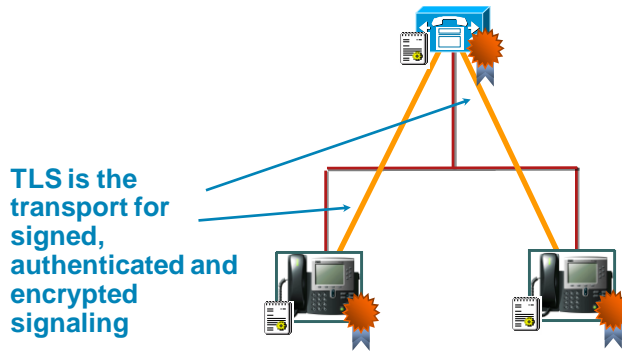
Supports any application protocol

HTTP	SCCP	SIP	LDAP
TLS			
TCP			
IP			

- Bi-directional PKI establishes **Authentication**
- HMAC provides **Integrity**
- Encryption offers **Confidentiality**

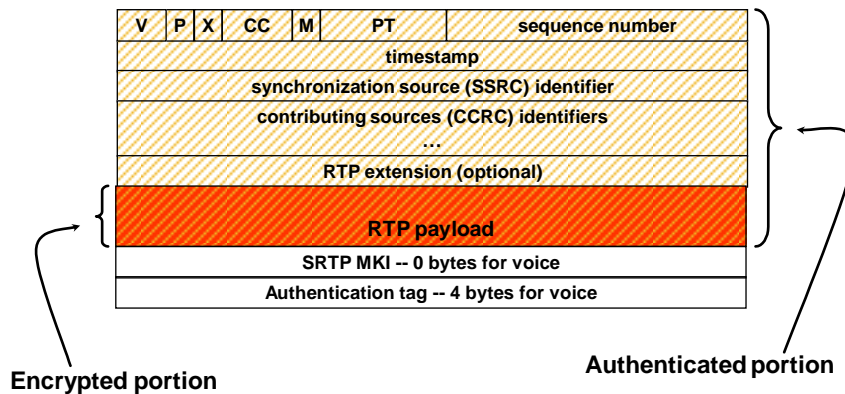
- Needs secure method to exchange shared secret
  - Bi-directional PKI pairs for mutual authentication
  - Shared secret exchanged using RSA
- Computes Hashed Message Authentication Code (HMAC)
  - Allows MD5 or SHA1
- Conventional cryptography using shared secret
  - DES, 3DES, AES
  - RC2, RC4
  -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

## Protecting the Signaling

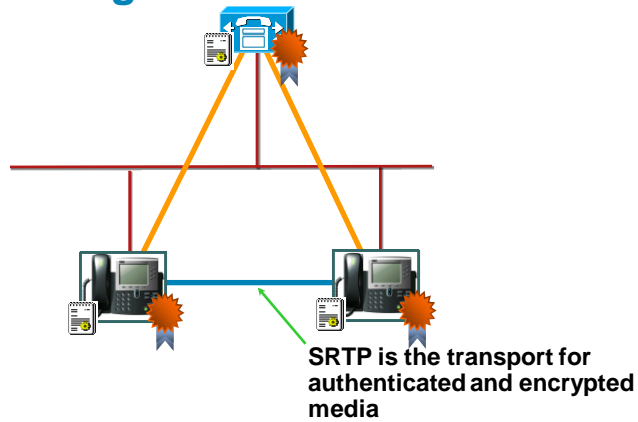


## SRTP: Secure RTP

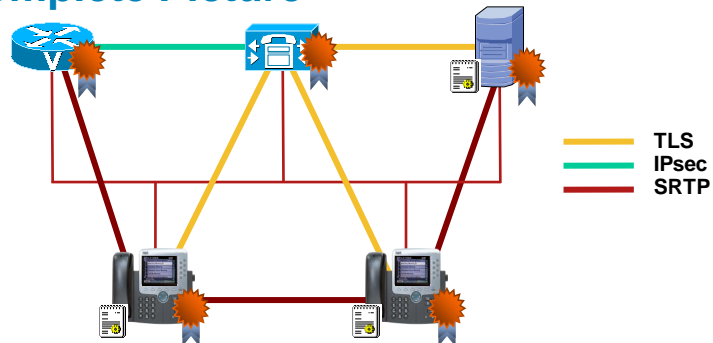
- RFC 3711 for transport of secure media
- Uses AES-128 Counter Mode for both authentication and encryption



## Protecting the Media Streams



## The Complete Picture



- IPsec secures MGCP and H.323  
Up to the admin
- SRTP secures media  
HMAC-SHA1 and AES-128 CM

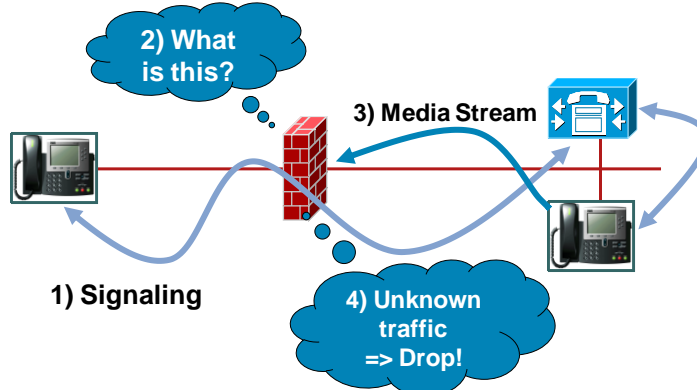
---

## Encryption Performance Considerations

- SRTP adds 4 bytes and 15 microseconds
- SRTP works with cRTP or IPsec
- IPsec
  - Adds 60+ bytes (and more serialization latency)
  - Incompatible with cRTP
- TLS less than 10% performance impact

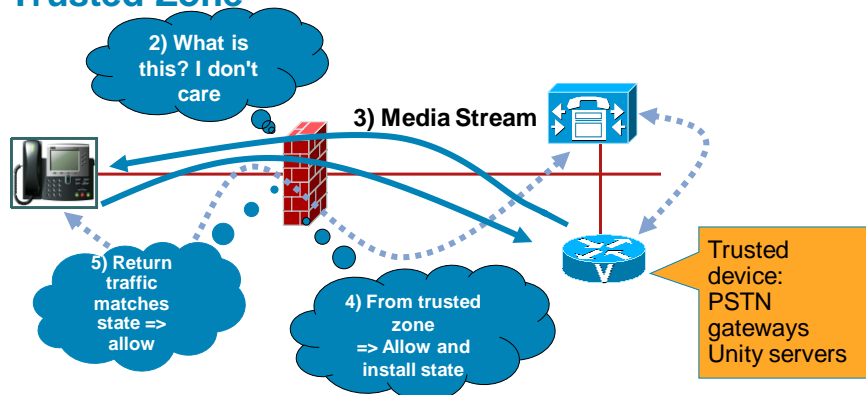
---

## Some Caveats with Firewalls



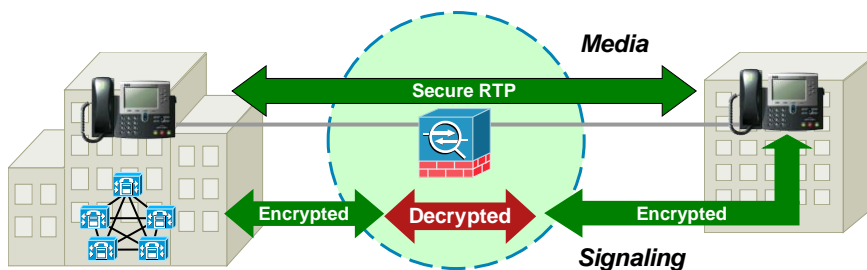
- If signaling is encrypted, how can firewall inspect the traffic?

## Simple but Efficient Solution: Trusted Zone



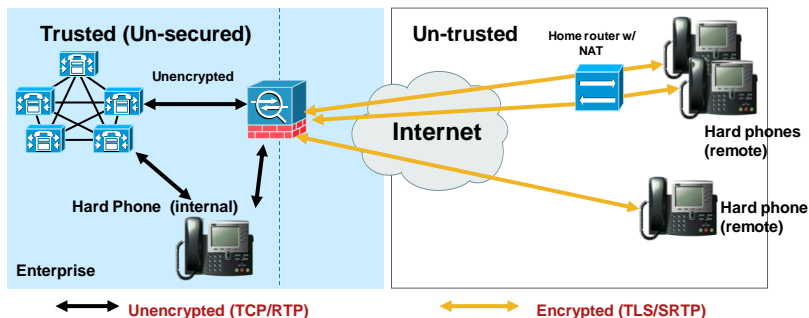
- Works even if signaling is not seen or is encrypted
- Relies on a trusted zone and accept return traffic

## More Elegant Solution: TLS Proxy (circuit level gateway)



- The TLS-proxy has a X.509 Certificate, is listed in the CTL, and has a copy of the CTL.
- The signaling connection is made over two separate TLS sessions from the Proxy to the CM and the Proxy to the phone.
- The firewall is now able to look into the signaling and perform inspection of the packets.

## Phone Proxy (Application proxy) —Remote Access



What Does the Phone Proxy Achieve?

- Secures remote phones by forcing the phones to do encrypted signaling and media
- Terminates TLS signaling from Phone and initiate TCP to CUCM
- Terminates SRTP and initiate RTP/SRTP to the called party
- More efficient than IPsec VPN (esp. for smart phones)

Evyncke IPT security © 2008 Cisco Systems, Inc. All rights reserved.

Cisco Public

41

Conclusion



Evyncke IPT security © 2008 Cisco Systems, Inc. All rights reserved.

Cisco Public

42

## Conclusion

- Security for IPT is usually desirable
  - Don't forget old voice was vulnerable (voice recorder, taps, ...)
- Security for IPT can be delivered
  - Within the network infrastructure
  - By the IPT protocols (but not always implemented even if free!)
- Security is not a barrier for deployment
- *BTW: apply the same paranoia to data as well*

## Q & A



