

VoIP Security: How Secure is Your IP Phone?

Dan York, CISSP

Director of IP Technology, Office of the CTO

Chair, Mitel Product Security Team

Member, Board of Directors, VoIP Security Alliance (VOIPSA)

IP Telephony Solutions for Government Conference


April 18, 2006

Security concerns in telephony are not new...



Image courtesy of the Computer History Museum

Nor are our attempts to protect against threats...



Models for Hand-set Phone


A Telephone Silencer – the HUSH-A-PHONE

A solution of three phone problems of subscribers

Safeguarding Privacy: So others cannot hear confidential matters
Eliminating Phone Talk Annoyance: Quieting the office for personnel efficiency
Improving Hearing in Noisy Places: By keeping surrounding noises out of the transmitter

Write for Booklet T-E.

Hush-A-Phone Corporation, 43 W. 16th St., N. Y. City



Models for Pedestal Phone

Image courtesy of Mike Sandman – <http://www.sandman.com/>

First objective is to employ best practices and plug the obvious holes...



A Few Security Terms

→ Denial of Service (DoS)

- Repetitive attacks that limit normal access to services

→ Virus

- Attached to a program and propagates when that program is executed

→ Worm

- Move through a network quickly from device to device, both intranet and Internet

→ Trojan horse

- Viruses and worms hide in other programs – hence the name

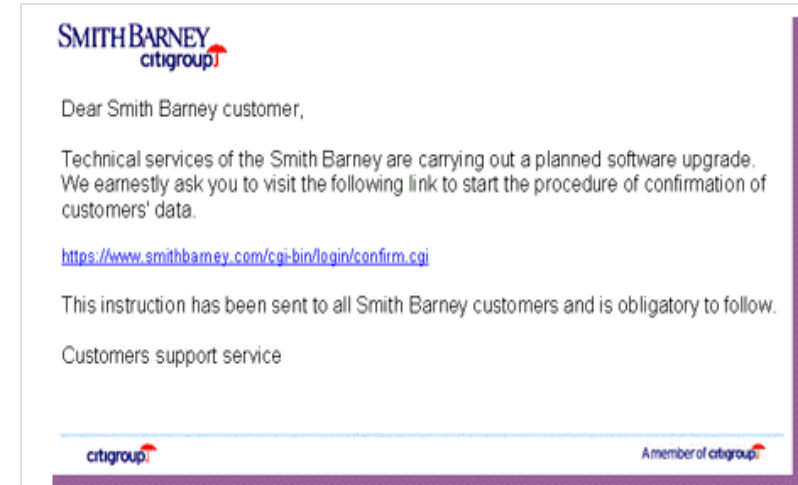
→ Spoofing

- Changing your MAC or IP address to impersonate another device

→ Spam for Internet Telephony (SPIT)

- Telemarketing in the age of VoIP

→ Phishing

A screenshot of a phishing website titled 'Details Confirmation'. The page has a header with the Smith Barney logo and 'crtigroup'. Below the header, there is a section titled 'Please Confirm Your User Information'. This section contains several input fields: 'ATM/Debit Card:', 'PIN-code:', 'Expiration Date:', 'User Name:', 'Password:', and 'E-mail Address:'. Each field has a corresponding input box. Below these fields is a 'Confirm' button. To the right of the input fields, there is a sidebar with four links: 'Forgot your User Name or Password?', 'Enroll Now to take full advantage of Smith Barney Access.', 'Guests please Register.', and 'Privacy and Security Your personal information is secure and confidential.'

The Challenge of Security

The Implications are Clear

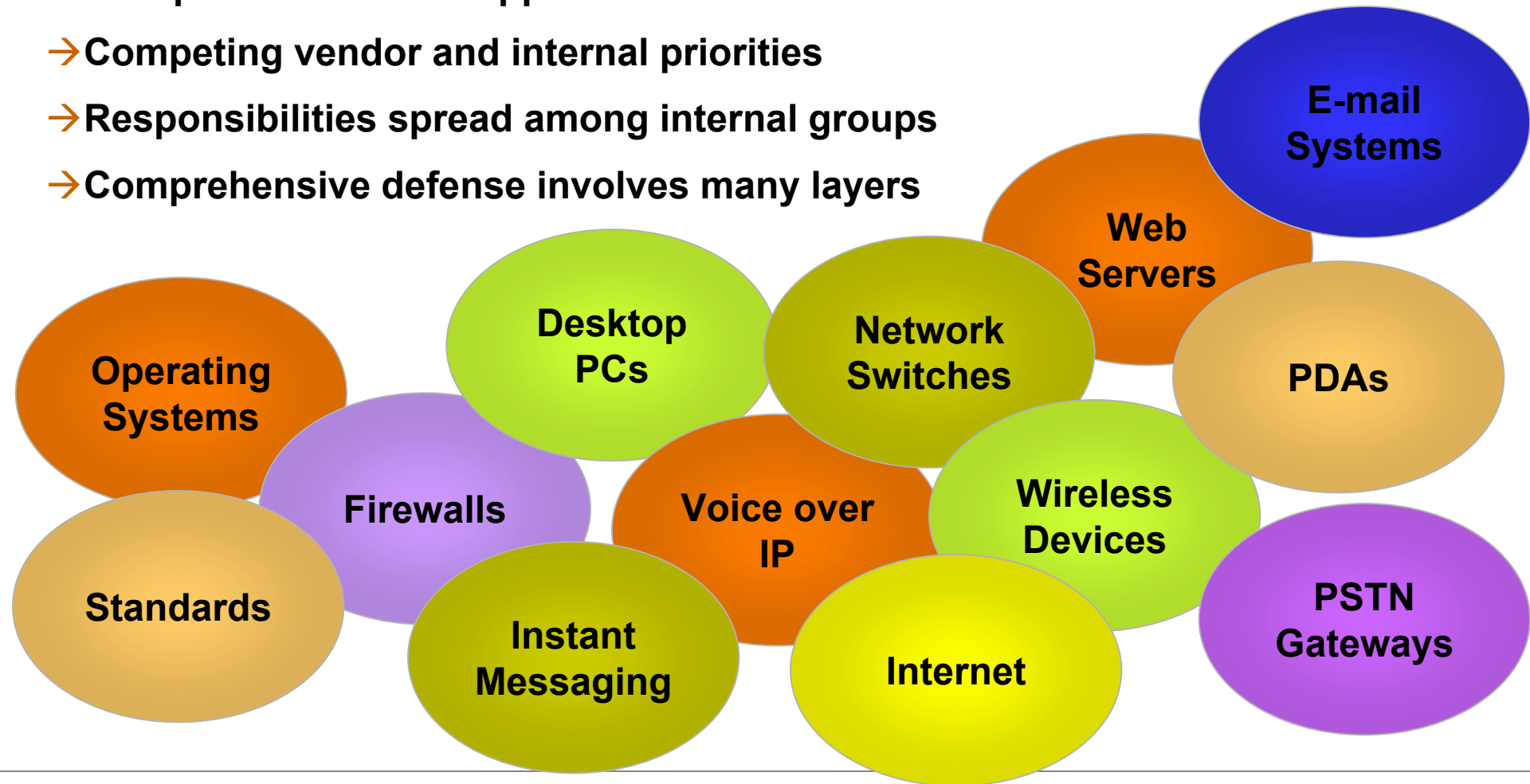
- **Ensure privacy and appropriate access to information**
- **Maximize service availability**
- **Cost avoidance**
- **Confidence to extend services to broadest group of users:**
 - Local, remote, mobile
- **Legal ramifications in some regions**
- **Security is strategic**

The Noise is Deafening

- **“VoIP Security” makes the headlines in countless articles**
- **Everyone is issuing security advisories**
 - **Manufacturers of software and hardware**
 - **Security research firms**
 - **Vendors of security products / training / services**
 - **Government (or quasi-government) entities**
 - **Computer Emergency Response Team (CERT)**
 - CERT Coordination Center – <http://www.cert.org/>
 - **U.S. Computer Emergency Readiness Team – <http://www.us-cert.gov/>**
 - **U.K.’s National Infrastructure Security Coordination Center (NISCC)**
<http://www.niscc.gov.uk>
 - **AUS-CERT – <http://www.auscert.org.au/>**
- **Each day brings more to your inbox and news**

The Problem is Complex

- Multiple vendors and applications
- Competing vendor and internal priorities
- Responsibilities spread among internal groups
- Comprehensive defense involves many layers



What is the Industry Doing to Help?

- VoIP Security Alliance - <http://www.voipsa.org/>
- “VOIPSA’s mission is to promote the current state of VoIP security research, VoIP security education and awareness, and free VoIP testing methodologies and tools.”
- Membership includes:
 - Mitel, Avaya, Nortel, Siemens, Alcatel, Extreme Networks, etc.
 - Now over 100 members on the Technical Board of Advisors
- Projects: Threat Taxonomy, Security Requirements, Security Research, Best Practices, Testing
- Public “VOIPSEC” mailing list for discussion of VoIP security issues
 - <http://www.voipsa.org/VOIPSEC/> (and yes, it’s all CAPS)
- “VoIP Security Threat Taxonomy” released in late 2005
- Next project - industry-wide “Best Practices”

- So what are the actual threats to IP Telephony?



Understanding IP Telephony Security Threats

Confidentiality
Integrity
Availability

Security Threats ... Confidentiality

Confidentiality
Integrity
Availability

→ Voice

- Threat – Eavesdropping, man-in-the-middle attacks
- Consequences – confidentiality breach between called and calling parties which can be used for personal or company gain

→ Call Control

- Threat – exposure of information about users, systems, patterns
- Consequences – privacy breach and / or malicious usage

→ Defense Strategies

- Physical protection (wiring closets, equipment rooms)
- Use of Ethernet switching instead of shared media
- Use VLANs, VPNs where applicable (just like your data network!)
- Encrypt conversations and call control, secure the media stream – SRTP
- Ensure routing tables, instructions, account codes are well maintained and password protected

Security Threats ... Integrity

Confidentiality
Integrity
Availability

→ Ensure that packets get from one point to another without modification

→ Voice

- Threat – impersonation of user, injection of other audio
- Consequences – ranging from unlimited to annoyance

→ Call Control

- Threat – fraudulent use of telephony resources – toll fraud, impersonation
- Consequences – increased costs and / or malicious usage

→ Passwords

- Threat – discovery of a user, system or application password
- Consequences – unlimited, depending on the role and function of the discovered password

→ Defense Strategies:

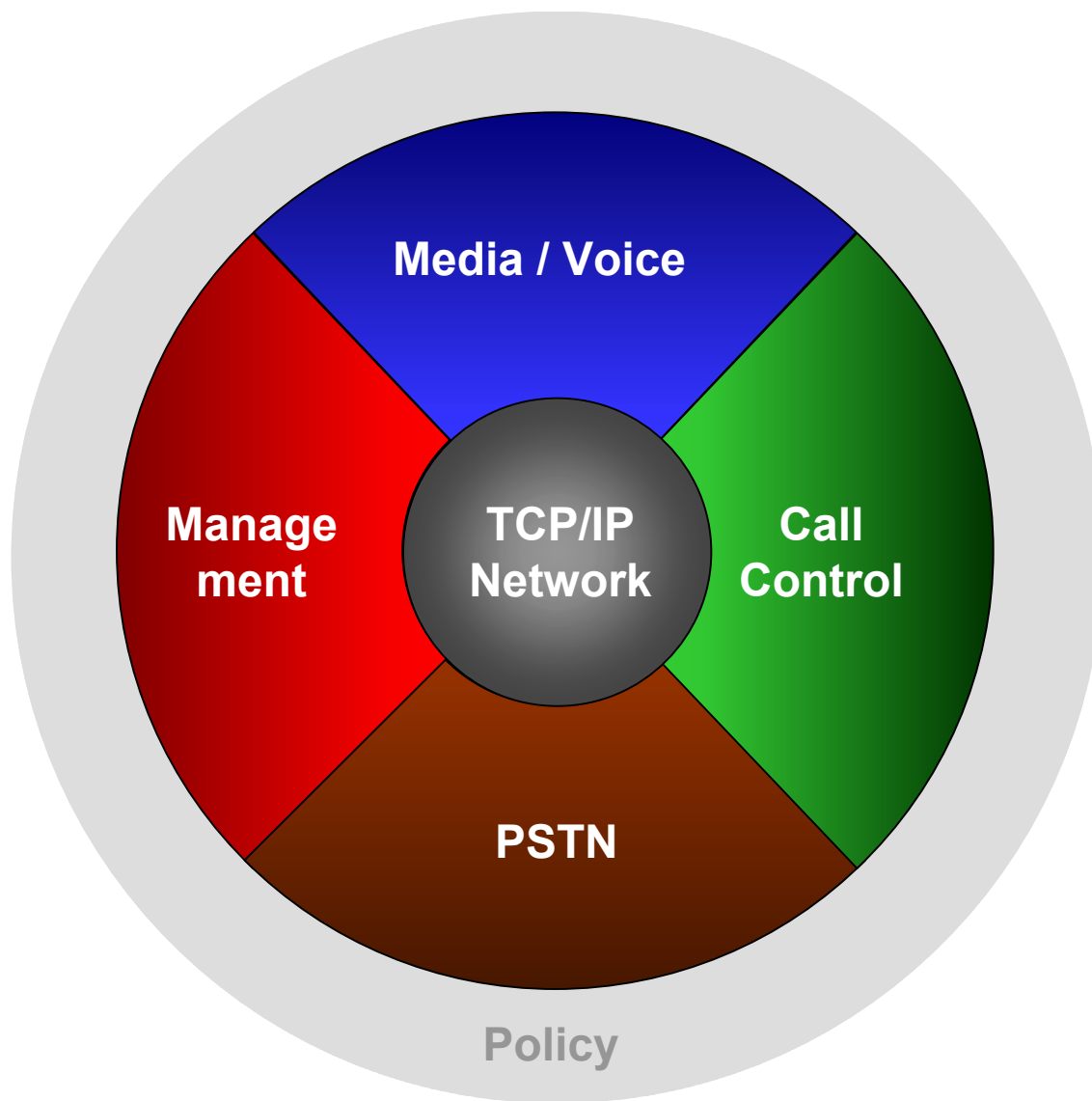
- Use encryption for secure communications
- Change default password, minimum length, enforce periodic change
- Never exchange passwords in clear text
- Password maintenance, delete ex-employees, security codes

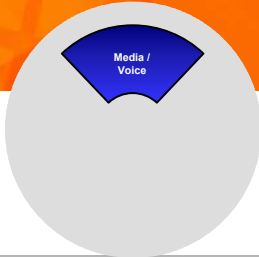
Security Threats ... Availability

Confidentiality
Integrity
Availability

- Ensure that communication services are available to users
- Avoid any adverse effects resulting from a denial of service (DoS) attack or computer worm
- Denial of Service:
 - Threat – Teardrop, SMURF or Ping of Death
 - Consequences – partial or total loss of telephony or related services
- Defense Strategies:
 - Rigorous virus updates and OS patches
 - Intrusion detection systems
 - Protect access from external sources (firewall)
 - Limit access from internal sources (firewall)
 - Use of 802.1 p/q (VLAN) to isolate and protect voice domain bandwidth from data domain Denial of Service (DoS) floods

Security Aspects of IP Telephony





The Media Path

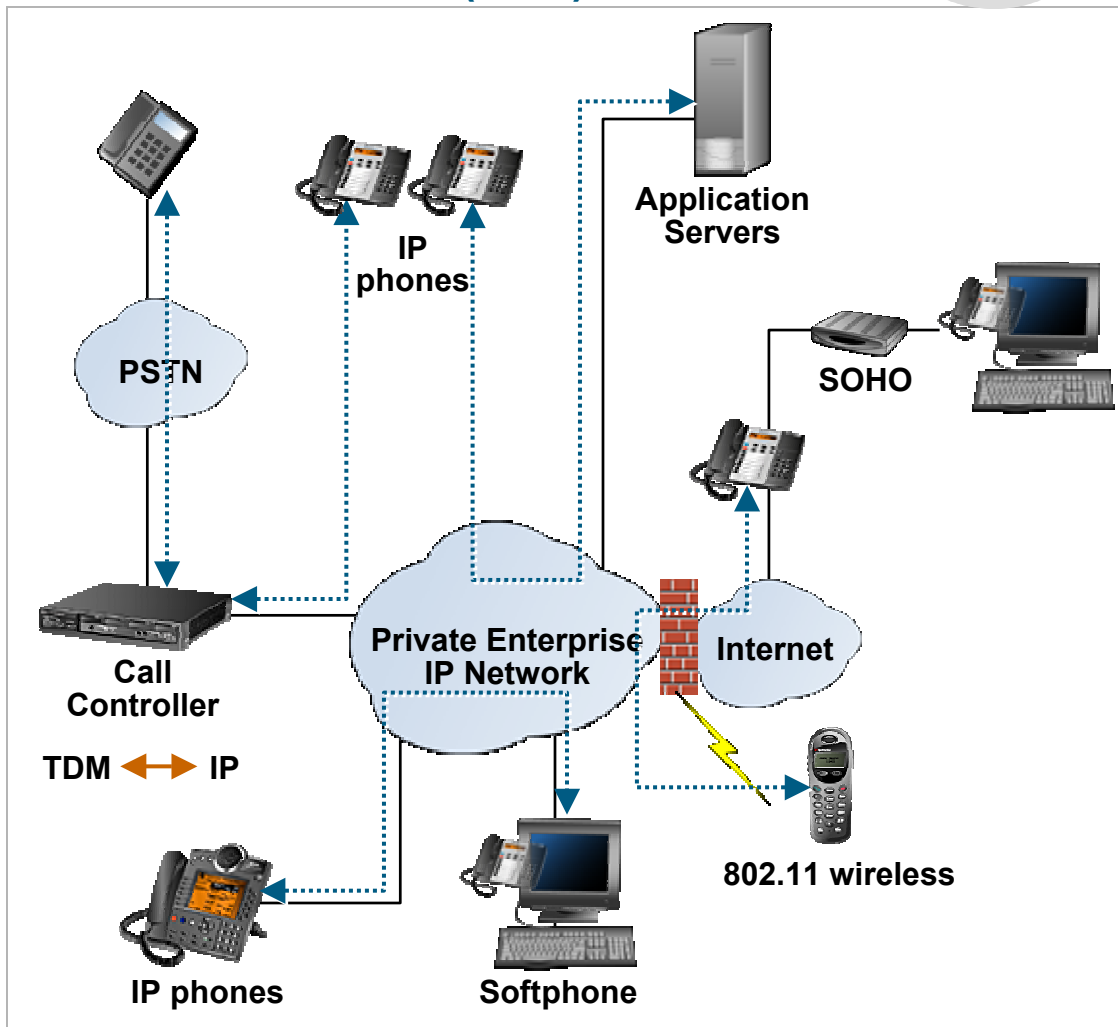
→ Threats:

- Eavesdropping – particularly if over wireless or open Internet (sniffing)
- Degraded voice quality through Denial of Service (DoS) attack

→ Defense Strategies:

- Encryption of voice path
- WPA, WPA2 for wireless
- VLANs
- Packet filtering

Real-Time Protocol (RTP) Packets



The Signalling Path

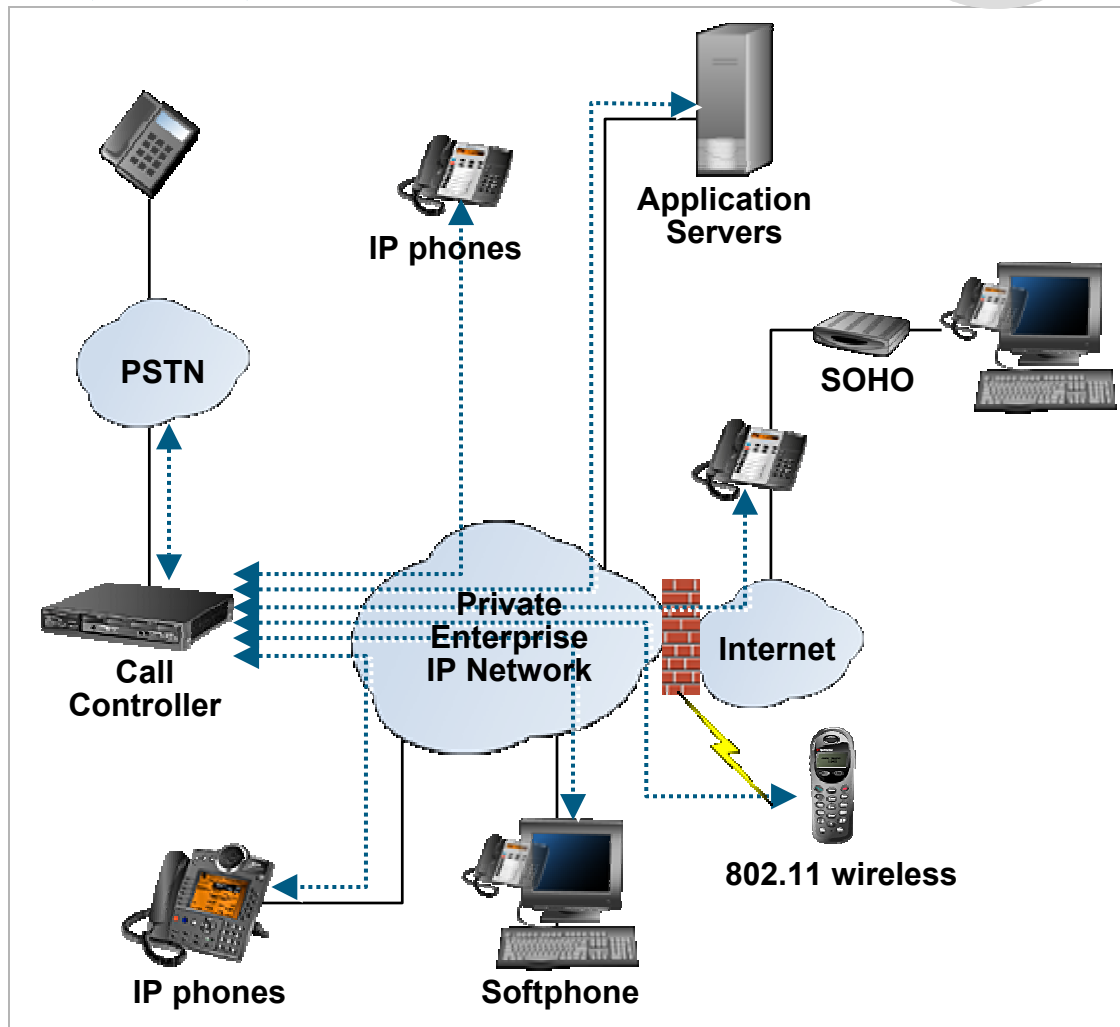
→ Threats:

- Denial of Service
- Impersonation
- Snooping account codes
- Toll fraud

→ Defense Strategies:

- Signalling path encryption
- Encrypted set firmware loads
- Proper system programming

SIP, H.323, others



The Management Path

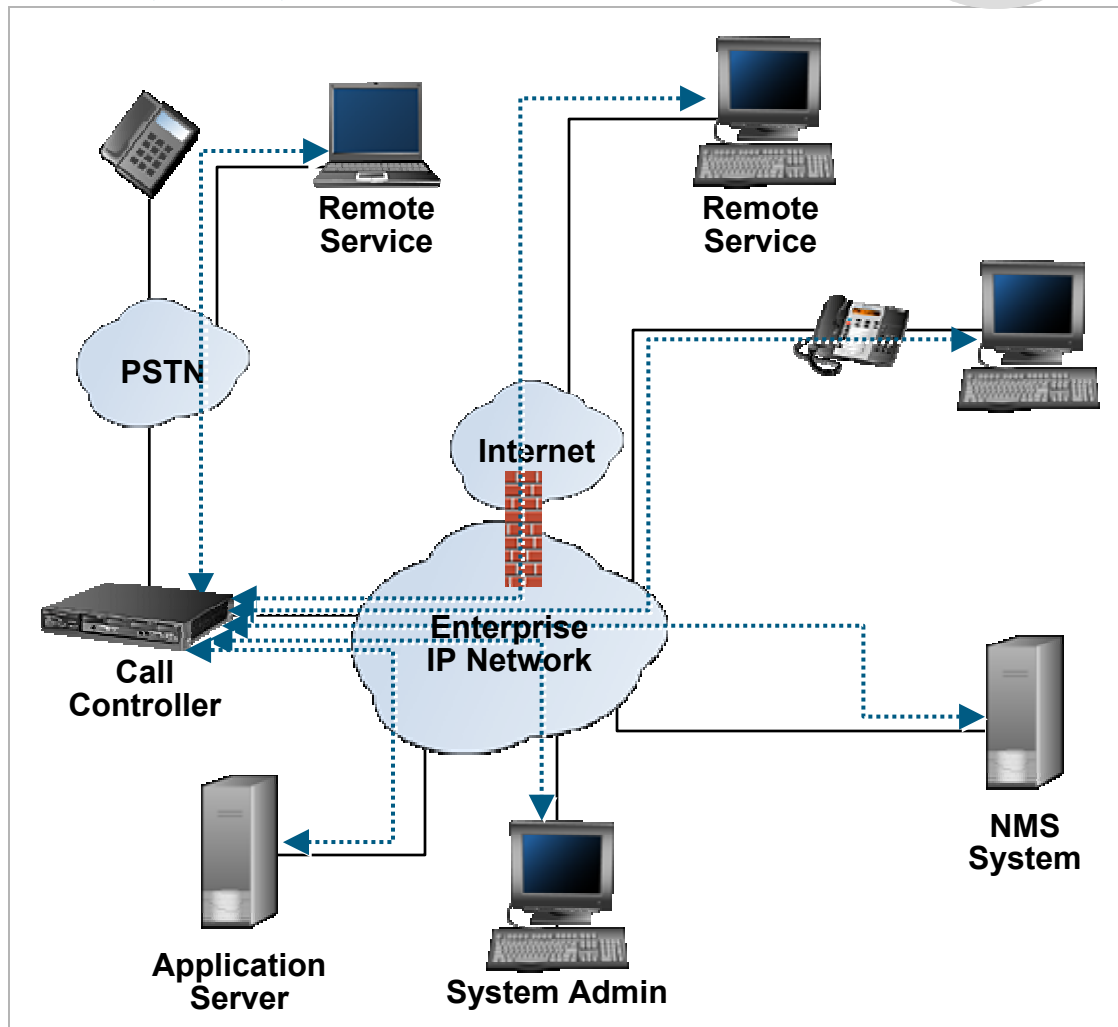
→ Threats:

- Snooping passwords
- Denial of service
- Application Impersonation
- Monitoring call patterns
- Malicious system modifications

→ Defense Strategies:

- DoS defenses in network infrastructure
- Changing default passwords
- Ensure physical security
- Authentication – secure port access
- Secure Socket Layer (SSL)

Examples – Telnet, HTTP, FTP, SNMP, XML, TAPI



PSTN and Legacy Devices

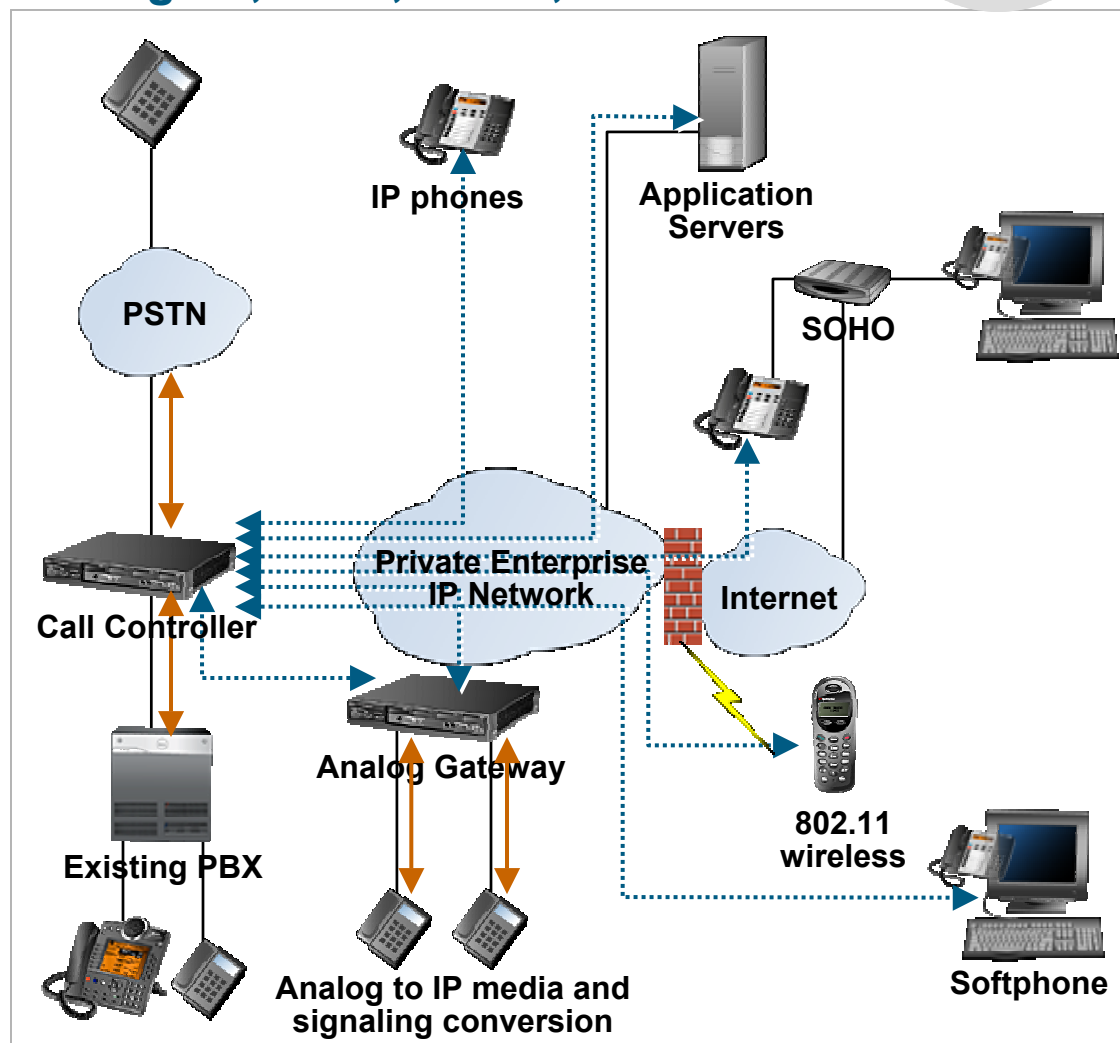
Analog LS, ISDN, Q.SIG, DPNSS

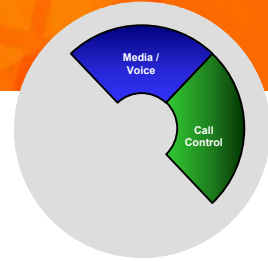
→ Threats:

- Toll fraud via public network attack
- Impersonation
- Feature access

→ Defense Strategies:

- Class of Restriction (COR)
- Class of Service (COS)
- Account Codes
- Trunk Restrictions
- Interconnect Restrictions





What about SPIT? (“SPam over Internet Telephony”)

- Makes for great headlines, but not a real threat today
- Fear is script/tool that:
 1. Iterates through calling SIP addresses:
111@sip.company.com, 112@sip.company.com, 113@sip.company.com , etc.
 2. Opens an audio stream if call is answered (by person or voicemail)
- Reality is that today such direct connections are generally not allowed
- This will change as companies make greater use of SIP trunking and/or directly connect IP-PBX systems to the Internet (and allow incoming calls from any other IP endpoint)
- Until that time, PSTN provides a de facto firewall
 - Telemarketers have to initiate unsolicited calls through the PSTN
- Note that VoIP just might give you *more* control...



IEEE 802.1X

- How do you know who is plugging into your network jacks?
- Network device must be authenticated before switch port is opened
- IEEE 802.1X Authentication for Desktops
 - Support for Extensible Authentication Protocol (EAP)
 - EAP-MD5
 - Protected EAP (PEAP)
 - EAP-TTLS (Tunneled TLS)
 - EAP-TLS
 - EAP-FAST
 - Lightweight EAP (LEAP)
 - Support for authentication via EAP to a RADIUS (or other similar) server
 - Username and password entered through the phone interface or included certificate

Best Practices for VoIP Security

Best Practices for VoIP Security

→ General Network

- All voice streams and call signalling should be encrypted, ideally end-to-end.
 - Voice should be encrypted with Secure RTP (SRTP) using 128-bit AES. Signalling should use SSL/TLS wherever possible. (Alternative solutions use IPSec to encrypt everything.)
- Networks should be evaluated for readiness to carry VoIP traffic.
- Virtual LANs (VLANs) should be used to segment voice and data network.
- Secure mechanisms should be used for traversal of firewalls.

→ Management

- Remote management should only be performed over encrypted connections.
- Proper password management techniques should be used.
 - Any default passwords must be changed. Passwords need rotation.
- System actions should be logged with appropriate audit capabilities.
- Only secure connections should be used for web access, i.e. SSL/HTTPS.

→ Endpoint/Sets

- Set software loads should be encrypted and tamper-proof.
- Sets should run the minimum of services required.
- Connection of a set to the system must require an initial authentication and authorization.

Best Practices for VoIP Security, continued

→ Servers / ICPs

- Servers should be incorporated into appropriate patch management and anti-virus systems.
- All telephony equipment and servers should be located in an environment providing appropriate physical security.
- Sufficient backup power should be available to maintain operation of telephony devices (and necessary network infrastructure) in the event of a power failure.

→ Wireless

- All wireless devices should implement WPA and/or WPA2 versus WEP.

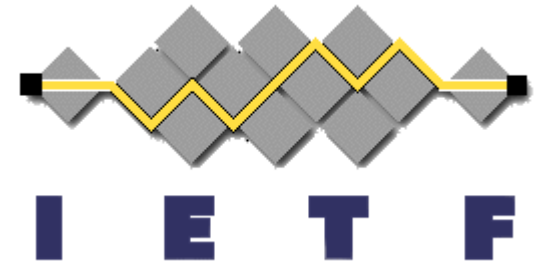
→ PSTN Threats

- Appropriate measures such as Class of Restriction should be in place to prevent toll fraud.
- Where there is high concern, accounts codes should be enabled to allow better tracking.
- SMDR records should be enabled and utilized to monitor call usage.

A Word on Standards

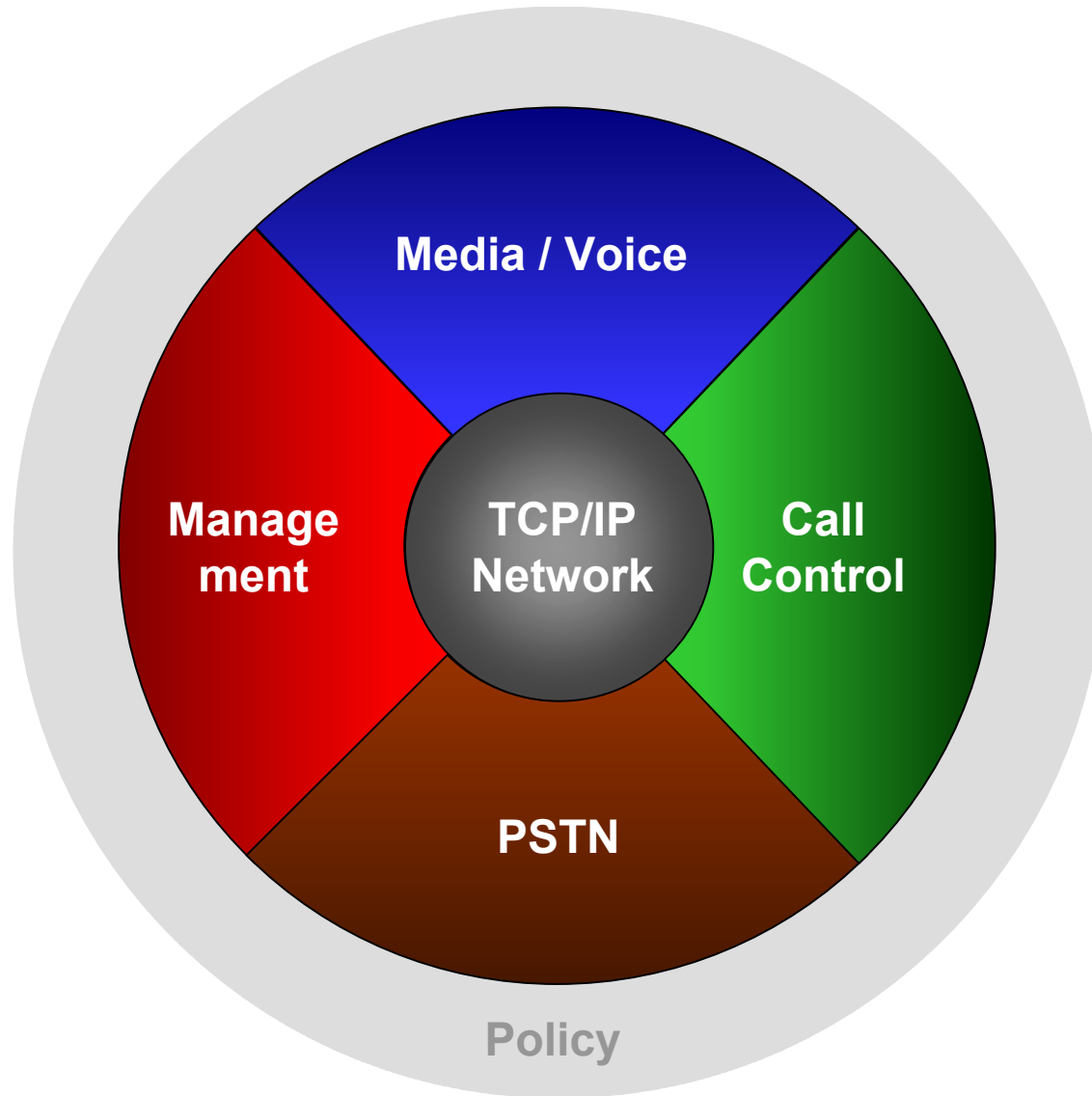
VoIP Standards

- Most VoIP deployments today are still with proprietary protocols
- However, industry future focused around:
 - SIP – Session Initiation Protocol
 - SRTP – Secure RTP
- Most VoIP Standards are under the IETF:
 - Working Groups: SIP, SIPPING, SIMPLE, MMUSIC, BEHAVE, ECRIT, SPEER
- Some of the major VoIP security issues before the IETF:
 - How do you securely exchange the keys to enable SRTP between vendors?
 - How do you know the identity of the caller? (i.e. to combat SPIT)
 - How do you address emergency calling? (i.e. E-911)
 - How do you find another number over the Internet without using the PSTN? (ENUM)
 - How do we improve NAT/firewall traversal?
 - How do connections between “peers” authenticate? (i.e. SIP trunking for PSTN bypass)
- New Real-time Applications and Infrastructure (RAI) “area” within IETF to add focus
- Additional standards in IEEE (802.1x, 802.11), ECMA (CSTA), ISO and TIA (LLDP-MED).



Summary

Security Aspects of IP Telephony



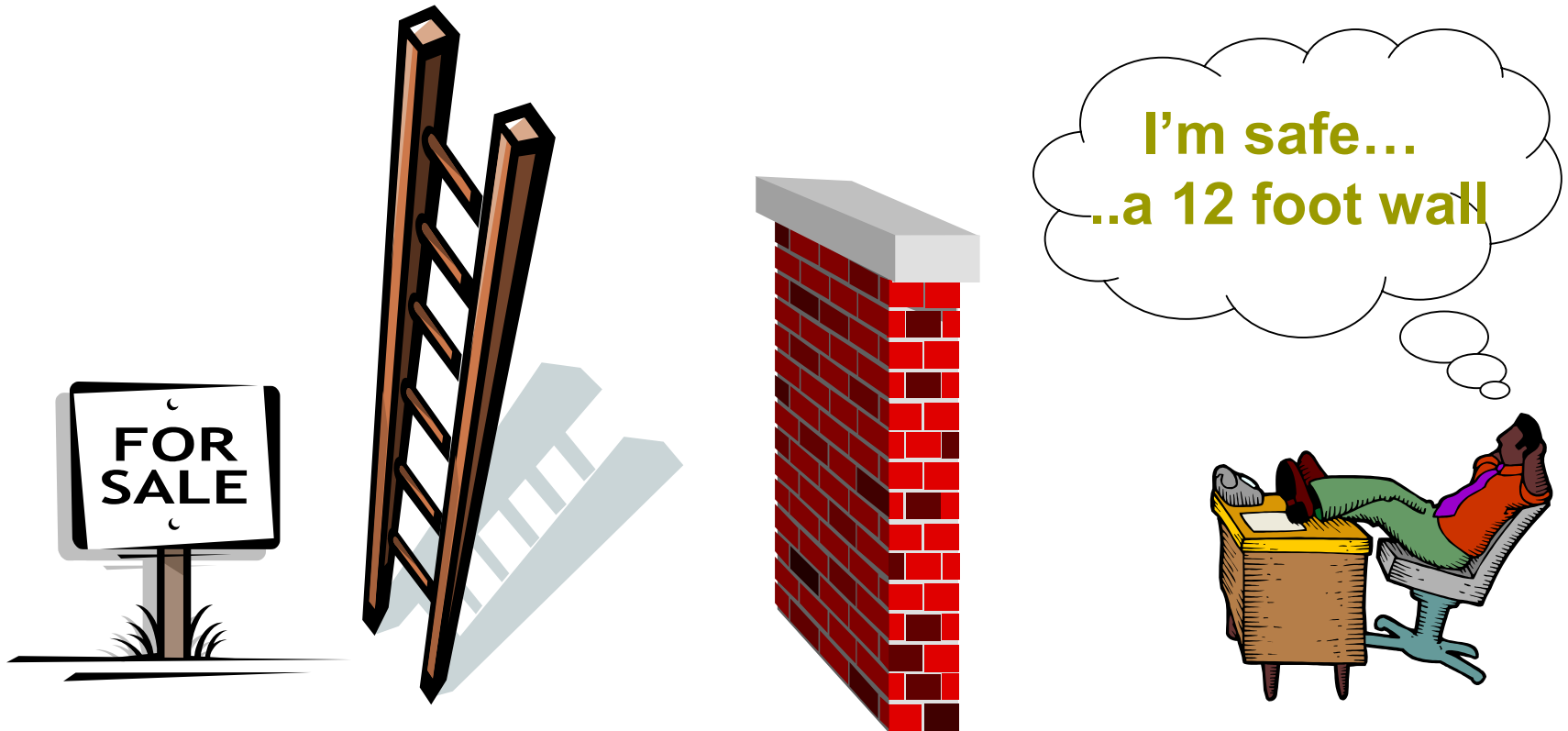
Security Links

- VoIP Security Alliance <http://www.voipsa.org>
 - Threat Taxonomy - <http://www.voipsa.org/Activities/taxonomy.php>
 - VOIPSEC mailing list - <http://www.voipsa.org/VOIPSEC/>
- Blue Box: The VoIP Security Podcast - <http://www.blueboxpodcast.com/>
- Computer Emergency Response Team (CERT) <http://www.cert.org/>
- U.S. Computer Emergency Readiness Team – <http://www.us-cert.gov/>
- U.K.'s National Infrastructure Security Coordination Center (NISCC)
<http://www.niscc.gov.uk>
- AUS-CERT – <http://www.auscert.org.au/>
- Internet Storm Center – <http://isc.sans.org/>

The Paradox of VoIP: One could argue that VoIP is already far more secure than the PSTN ever was



And Remember....



.....13 foot ladders

It's a question of vigilance

Thank you



it's about **YOU**

Dan York, CISSP

Director of IP Technology, Office of the CTO

Chair, Mitel Product Security Team

Member, Board of Directors, VoIP Security Alliance

dan_york@mitel.com

Report security issues to security@mitel.com