VoIP Security and Mitel IP Telephony Solutions

Dan York
Chair, Mitel Product Security Team
February 2006
Agenda

The Challenge of Security
Understanding VoIP Security Threats
Mitel Security Solutions
Tools, Contacts, Help
Summary
Questions / Answers
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

→ 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.K.’s National Infrastructure Security Coordination Center (NISCC) http://www.niscc.gov.uk

→ 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 Mitel Doing Specifically?

→ Extensive portfolio of secure solutions available for you today
→ Member of VoIP Security Alliance
→ Connected to industry security groups including:
  – CERT and US-CERT
  – NISCC (National Infrastructure Security Co-ordination Center)
→ Security portal:
  – Mitel Online – Technical Support -> “Security at Work”
→ Ongoing security vigilance
What is the Industry Doing to Help?

→ “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


→ 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”
  – http://www.voipsa.org/

→ So what are the actual threats to IP Telephony?
Understanding IP Telephony Security Threats
Before We Begin …

→ Nobody is 100 percent secure and never has been!
→ Employ “best practices” from an organization perspective …
→ Be sensitive to operation and cost
→ Security concerns are not new: Mitel offers extensive TDM defenses
Security Challenges … CIA

➔ **Confidentiality**
  – Protect the voice and data stream including call control signaling
  – Prevent eavesdropping on conversations, toll fraud, impersonation

➔ **Integrity**
  – Ensure that information is protected from unauthorized modification
  – Prevent discovery of a user, system or application password

➔ **Availability**
  – Ensure that communication services are available to users
  – Avoid any adverse effects resulting from a denial of service (DoS) attack or computer worm
Security Aspects of IP Telephony

- Media / Voice
- Call Control
- Management
- PSTN
- Policy
- TCP/IP Network
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
The Signalling Path

**Threats:**
- Denial of Service
- Impersonation
- Snooping account codes
- Toll fraud

**Defense Strategies:**
- Signalling path encryption
- Encrypted desktop load on 3300 ICP
- Proper system programming
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)
PSTN and Legacy Devices

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
Mitel Security Today

✓ Secure Voice / Media
✓ Secure Call Control / Signalling
✓ Secure Management Interfaces
✓ Secure against legacy PSTN threats
✓ Secure against common network attacks
Mitel 3300 ICP Encryption

- Encryption across full Mitel desktop portfolio
  - Voice Stream: Secure RTP using 128 bit Advanced Encryption Standard (AES)
  - Call control encrypted using Mitel’s Secure MiNet (AES)
  - Full support for all current and recent sets
    - Mitel 5201, 5207, 5010, 5020, 5212, 5215, 5220, 5224, 5230, 5235, 5240, Navigator IP Phones
    - Mitel Your Assistant Softphone

- Encryption of signaling and media path between multiple ICPs (clusters)
Secure Management Interfaces

- Web management interfaces for systems and applications implement SSL
- Authenticated access to provisioning, administrative user interfaces
  - Different levels of access with different passwords
- Mitel 7100 Management Access Point:
  - Secure remote admin for VPN or Dial-up access
- XML APIs
  - All traffic encrypted using standard SSL
  - Strong certificate-based authentication required
- Live Business Gateway
  - Uses SSL/TLS-encrypted SIP for communication to Microsoft Live Communication Server
Secure against legacy/PSTN threats

- Extensive Class of Restriction avoids misuse of communications resources
- Well-proven toll fraud restrictions:
  - Traditional TDM COS/COR
  - Account codes
  - Restrictions on trunk-to-trunk connections
  - SMDR records
- Ability to flag calls as malicious
- Feature access restrictions

PSTN
Secure against common network attacks

→ Denial of Service protection within 3300 ICP and desktops
  – Performance may be reduced but system doesn’t shut down
→ Sets include micro-firewall and rate throttling to fend off DoS attacks
→ Support for VLANs to segregate voice and data traffic
→ Core Platform OS, VxWorks, is not susceptible to Windows OS viruses / attacks
→ Application operating systems hardened against attack
→ Mitel is IP infrastructure agnostic giving our customers choice
  – HP, Foundry, Cisco, or others
→ Set authentication requires unique association of MAC address, IP and user entered PIN registration number
→ Set software downloads are encrypted and tamper-proof to ensure sets cannot be spoofed
→ Sets in MiNet mode do not include a web browser or other services that can be attacked
Support for 802.1x

→ How do you know who is plugging into your network jacks?
→ Network device must be authenticated before switch port is opened
→ 802.1x Authentication for Desktops
  – Support for Extensible Authentication Protocol (EAP) EAP-MD5 challenge
  – Support for authentication via EAP to a RADIUS (or other similar) server
  – Username and password entered through the phone interface
  – Supported on dual mode 5212, 5215, 5220, 5224, 5235 and Navigator IP Phones
Wireless Security

- Encryption and enhanced authentication for SpectraLink Telephones using Wi-Fi Protected Access (WPA) and WPA2
- WLAN Stand supports WPA, WPA2
- IP-DECT sets (EMEA & AP) include native DECT encryption
Secure traversal of firewalls

- Teleworker Solution allows secure use of remote extension anywhere there is an IP address
- Works with standard Mitel IP sets – no special sets to purchase

![Diagram of Teleworker Solution](image)
SIP Security

- Mitel SIP desktops support Secure RTP
  - Today: dual mode 5212, 5215, 5220, 5224, 5235, Navigator IP Phone
- SIP sets satisfy challenging PROTOS test suite for CERT advisory CA-2003-06
  - (http://www.cert.org/advisories/CA-2003-06.html)
- Support for traversal of firewalls including STUN
- SSL/TLS-encrypted SIP planned for calendar Q2, 2006
  - Also will support HTTPS and SSL-encrypted telnet
- SIP sets support 802.1x
- SIP trunking in 3300 Rel 7.0 will support SSL/TLS for signaling
- Mitel continually monitors evolving SIP security standards
Protection Beyond Product to Process

→ Mitel focus on security

→ Broad based internal security team encompassing R&D, test, product management, product support, product verification

→ Internal process to ensure compliance with vendor security bulletins (such as Microsoft)

→ Escalation process for reported security vulnerabilities
  – Email sent to security@mitel.com
  – Triage by product security team
  – Escalation to appropriate product groups as necessary
  – As needed security advisories posted to www.mitel.com/security

→ Ongoing vigilance throughout customer / product lifecycle
Where to Go for More Information

  – Advisories, Security white papers, FAQ

→ Mitel OnLine
  – “Security at Work” portal
  – Webinar and customer presentations
  – Security Technology Brief
  – 3300 ICP Security White Paper
  – 3300 ICP Security FAQ
  – 3300 Engineering Guidelines
  – More documents coming soon…

→ If you have more questions:
  – Engage your SE
  – To report a suspected security vulnerability email [security@mitel.com](mailto:security@mitel.com)
Security Links

→ VoIP Security Alliance http://www.voipsa.org
→ Computer Emergency Response Team (CERT) http://www.cert.org/
→ U.K.’s National Infrastructure Security Coordination Center (NISCC) http://www.niscc.gov.uk
→ Internet Storm Center – http://isc.sans.org/
Mitel Security Solutions Summary
Mitel Security Today

✔ Secure Voice / Media
✔ Secure Call Control / Signalling
✔ Secure Management Interfaces
✔ Secure against legacy PSTN threats
✔ Secure against common network threats

Thank you

Dan York
Chair, Mitel Product Security Team
dan_york@mitel.com

Report security issues to security@mitel.com
Backup Slides
Addressing Security Threats

**Attack Points**
1) Denial Of Service
2) Password Sniffing
3) Eavesdropping
4) Spoofing, Assuming Identity
5) Spoofing, APIs

**Security Implementations**
1) Hardening of Call Control and OS
2) Implement Secure Socket Layer
3) Employ Encryption of Media Streams
4) Implement SSL on Signaling Streams
5) Authentication with Policy Based Access
Security Threats ... Confidentiality

→ 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 – fraudulent use of telephony resources – toll fraud, impersonation
  – Consequences – increased costs 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

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

➔ Defense Strategies:
  – Change default password, minimum length, enforce periodic change
  – Never exchange passwords in clear text
  – Password maintenance, delete ex-employees, security codes
  – Use SSL for secure communications
Security Threats ... Availability

➔ 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
802.1X handshake

Set, PC, endpoint → LAN Switch → RADIUS Server

Supplicant

- Identity
- Request Credentials
- Credentials
- Authentication Key

Authenticator

- Challenge
- Identity
- Request Credentials
- Credentials

Authenticating Server

- Authentication Key

Uncontrolled Port

Controlled Port

LAN Resources

Exact format unique to each Extensible Authentication Protocol (EAP) method

- EAP-MD5
- EAP-TLS
- EAP-TTLS
- PEAP
- EAP-FAST, others
How Can VLANs Solve My Security Problems?

- Green VLAN – data VLAN
- Black VLAN aka Voice VLAN
- Virus permeates network
A Few Security Terms

→ Denial of Service (DoS)
  – Repetitive attacks that limit normal access to services

→ Spam for Internet Telephony (SPIT)

→ Worm
  – Move through a network quickly from device to device
  – Both intranet and Internet

→ Virus
  – Attached to a program and propagates when that program is executed
  – Replication and activation

→ Trojan horse
  – Viruses and worms hide in other programs – hence the name

→ Spoofing
  – Changing your MAC or IP address to impersonate another device

→ Phishing
Security Considerations of CX vs CXi Platforms

→ CXi provides internal switch and firewall
  – Integrated package
  – VLAN support upon initial release Mitel 3300 CXi Controller
    – (SX-200 ICP VLAN support will follow)
  – Can use either internal firewall or firewall of choice
  – Position for smaller organizations or standalone sites

→ CX Controller package requires external switch
  – Add switch and firewall to suit architecture requirements
  – Position for organizations with strong security focus