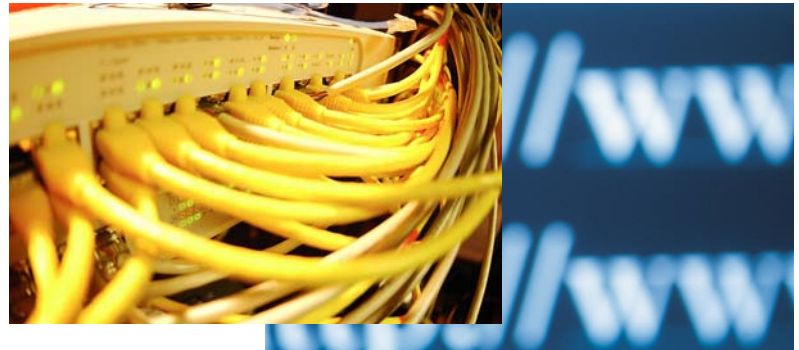


IP Telephony Security: Conducting A Vulnerability Assessment

Irwin Lazar
Principal Research Analyst
Nemertes Research, Inc.
August 23, 2006
Irwin.lazar@nemertes.com



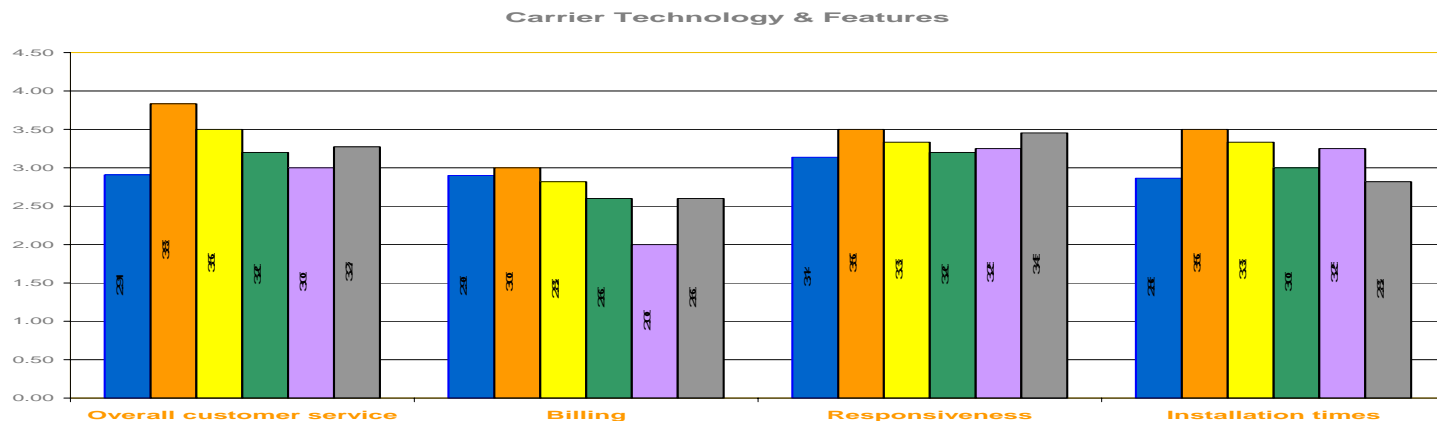
Agenda

- ⊕ Threats
- ⊕ Mitigation Techniques
- ⊕ Recommendations

Introductions

⊕ About Nemertes

- ⊕ Founded October 2002
- ⊕ Research data comes from network of 2,500 IT executives willing to discuss their issues and concerns at length
- ⊕ Principals all have 15-21 years industry experience, including operational
- ⊕ Focused on analyzing the business value of emerging technologies
- ⊕ Advise leading global enterprises, carriers, vendors, investment firms on emerging technologies.



IP Telephony Threats

⊕ The Sky Is Falling!!!

“Cisco Security Threats Serve as a VoIP Wake-Up Call”

Information Week, January 23, 2006

“Data and voice convergence brings host of new threats”

TechCentral, January 23, 2006

“Is VoIP The Cyber Criminal’s New Best Friend?”

Silicon.com, January 26, 2006

“IP Telephony Is Inherently Insecure, and since its operations depend on the Internet, all cyber vulnerabilities on the Internet threaten to knock out phone systems that use VoIP”

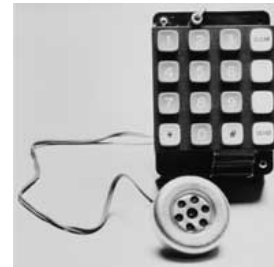
Cyber Security Industry Alliance, May 2005



Threats

⊕ Let's Remember, The PSTN Isn't Secure Either

- ⊕ Phones & trunks can be tapped
- ⊕ Toll fraud is still a concern



⊕ Voice Security Is As Much A Social Problem As A Technical Problem

- ⊕ Hang out in a coffee shop or airport and you're likely to hear sensitive topics being discussed in the open
- ⊕ Modern office cube farms are inherently insecure

Threats

- ⊕ What are the real threats?
 - ⊕ Denial of Service Attacks
 - ⊕ Against calls servers, gateways and end-points
 - ⊕ Eavesdropping
 - ⊕ Unauthorized call capture, either internally or externally
 - ⊕ Could also include remote speakerphone activation
 - ⊕ Toll Fraud
 - ⊕ Internal misuse or external access to call services
 - ⊕ Rogue phone placement

- ⊕ Attacks can come from inside or out

Threats

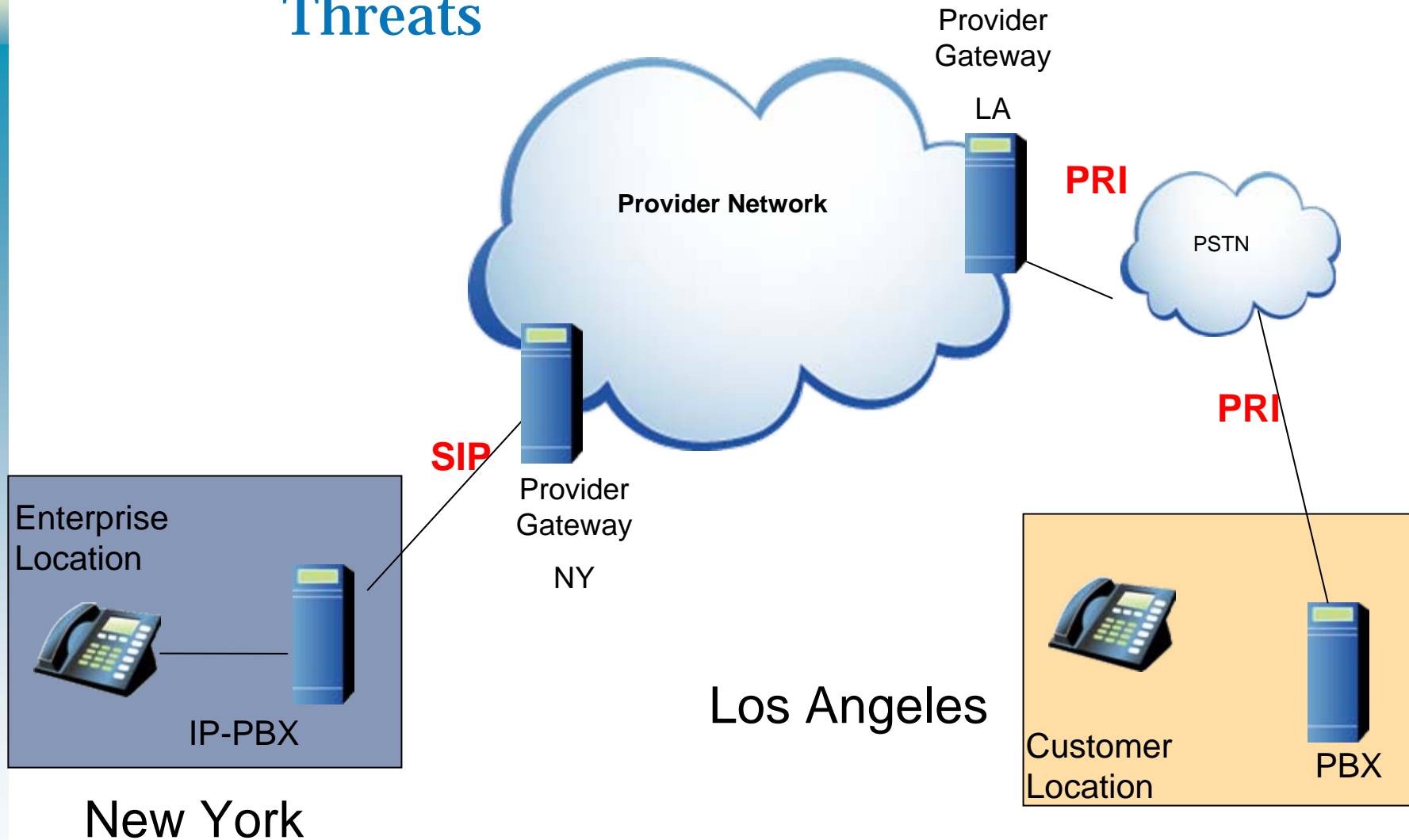
⊕ The Reality

- ⊕ Many threats are overblown, current VoIP deployments are small, and are generally isolated from the Internet
 - ⊕ PSTN provides a “firebreak”
 - ⊕ SPIT isn’t a real threat (yet)

⊕ But, this is changing

- ⊕ Increasing use of public services
- ⊕ Softphones
- ⊕ Increasing IP-to-IP peering

Threats



Mitigation Techniques

- ⊕ Operational
 - ⊕ Risk assessment
 - ⊕ Security audits
 - ⊕ Use of tools such as VoIP Shield's "VoIP Audit" or open-source test kits to detect potential flaws
 - ⊕ User training
 - ⊕ Patch management



Migration Techniques

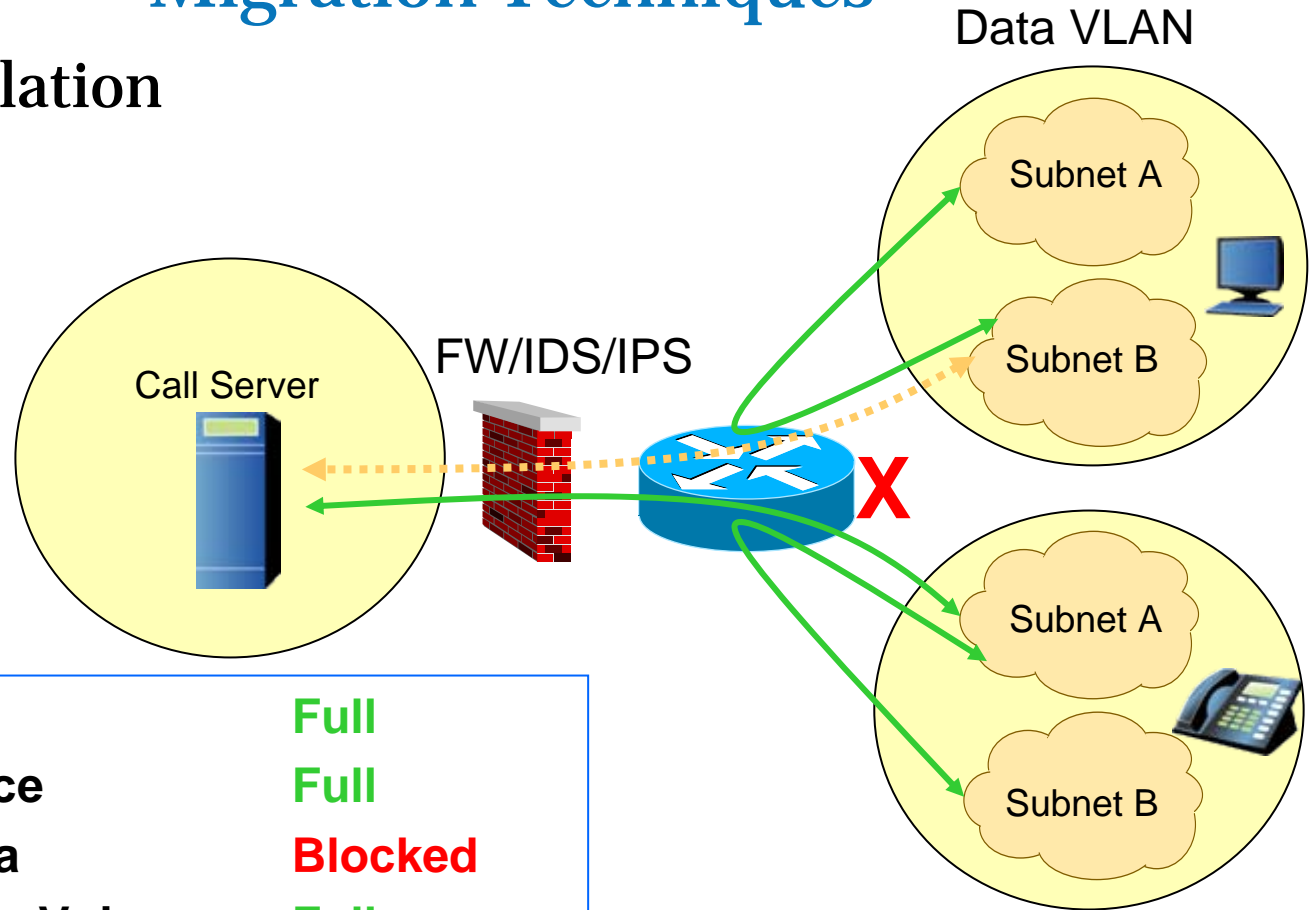
⊕ Technical

- ⊕ Network isolation
 - ⊕ Voice and Data on separate VLANs
- ⊕ Encryption
 - ⊕ Both signaling and media
- ⊕ Hardening of call servers
 - ⊕ Host-based intrusion detection
 - ⊕ Closing unnecessary ports
- ⊕ Hardening of end-points
 - ⊕ Signed software loads
 - ⊕ Access controls (802.1x)
- ⊕ Hardening of network
 - ⊕ Intrusion detection
 - ⊕ Voice-aware firewalls



Migration Techniques

V-LAN Isolation



Data to Data	Full
Voice to Voice	Full
Voice to Data	Blocked
Call Server to Voice	Full
Call Server to Data	Limited

Recommendations

- ⊕ Risk assessment
- ⊕ Technical best practices
 - ⊕ TLS/SSL for signaling
 - ⊕ SRTP for media
 - ⊕ IDS/IPS on all servers and at network connection points
 - ⊕ VoIP-aware firewalls to protect network zones
 - ⊕ Authentication of network devices
- ⊕ Operational best practices
 - ⊕ Training
 - ⊕ Vulnerability testing
 - ⊕ Patch management



Recommendations

⊕ For Further Study

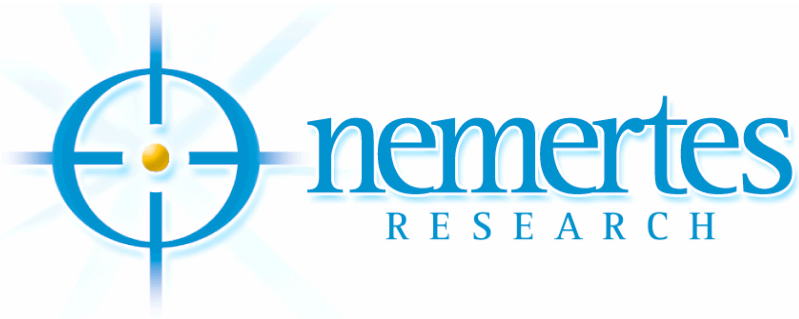
⊕ Follow security developments/discussions

⊕ VoIPSA Mailing List - <http://www.voipsa.org/>

⊕ Blue Box VoIPSEC Podcast -
<http://www.blueboxpodcast.com/>

⊕ US National Institute of Technologies and Standards (NIST)
“Security Considerations for Voice over IP Systems”

⊕ <http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf>



Thank you!

