

# The Top Five VoIP Security Challenges:

..... And What You Can Do About Them



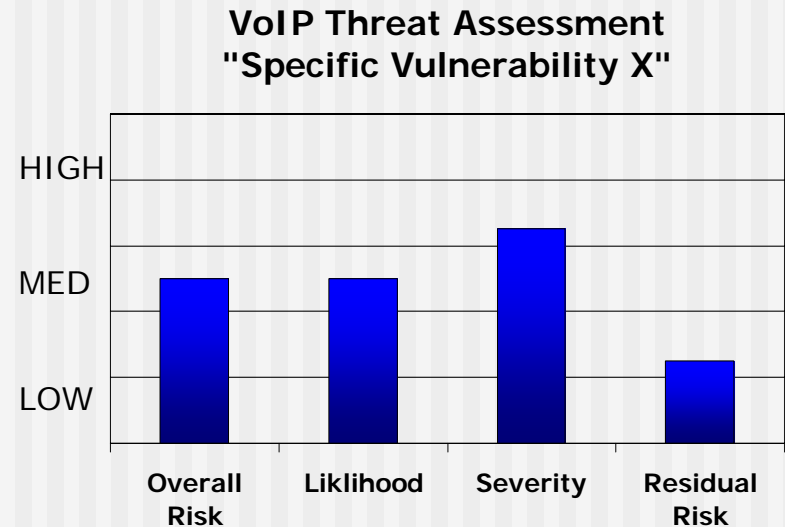
# Top Five VoIP Security Challenges

---

- **Inherent vulnerabilities of VoIP products and add on measures**
- **Sniffing eavesdropping**
- **Unauthorized resource usage**
- **Identity theft**
- **Distributed denial of service attacks**

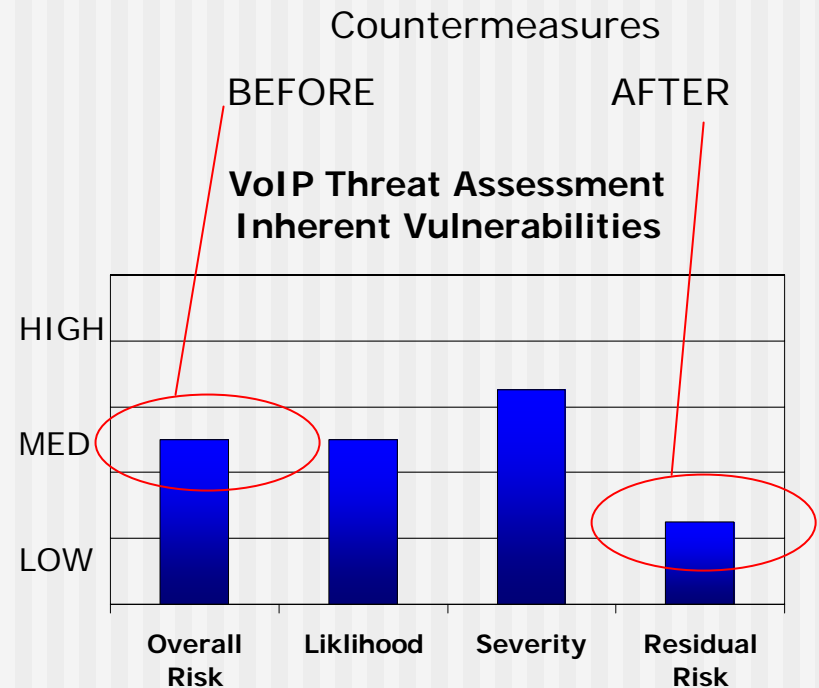
# VoIP Threat Assessment Model

- Overall Risk
- Likelihood
- Severity
- Residual Risk
  - mitigating factors



# Inherent vulnerabilities of VoIP products and add-on measures

- VoIP products inherent security (DoS and other vulnerabilities) differs by product; next slides will illustrate
- Mitigating factors
  - Effective countermeasures emplacement will reduce the risk; next slides will illustrate
  - Adopt a layered approach to security
  - Conduct pre- and post-deployment testing



# VoIP Product Inherent Security Compared (1 of 4)

Comparative results of DoS attacks on call controllers, media gateways, and IP phones

Device/Component	Version tested	Frag-mented UDP	TCP resource starvation	Random-ized ACK flood	Directed UDP flood
Alcatel OmniPCX Enterprise	R5.1Lx	Low	Low	Medium	Low
Alcatel Media Gateway	R5.1Lx	High	High	High	Low
Avaya S8700 Media Server	2.0	Low	Low	Low	Low
Avaya G650 Media Gateway	2.0	Low	High	High	High
Avaya S8300 Media Server	2.0	Low	High	Low	Low
Avaya G700 Media Gateway	2.0	Medium	Medium	Medium	Medium
Avaya IP Office 403	2.0	Medium	Medium	Medium	High
Cisco CallManager MCS 7835H	3.3(3)	Medium	Low	Low	Low
Cisco CallManager MCS 7825H	3.3(3)	Low	Medium	Medium	Low
Cisco 3725 Media Gateway	12.3(7)T	Low	Medium	Low	Low
Cisco Call Manager Express	3.1	High	High	High	Medium

Source: VoIP Security Assessment 2006 Copyright © 2006 Miercom



# VoIP Product Inherent Security Compared (2 of 4)

Comparative results of DoS attacks on call controllers, media gateways, and IP phones

Device/Component	Version tested	Frag-mented UDP	TCP resource starvation	Random-ized ACK flood	Directed UDP flood
Interactive Intelligence Enterprise Interaction Center	2.3	Low	Low	Low	Low
Mitel 3300 Integrated Communications Platform	4.1	High	Medium	High	Medium
Nortel Succession 1000M Signaling Server	3.0	High	Low	Low	Low
Nortel Media Gateway	3.0	High	Low	Low	Low
Nortel Gatekeeper	3.0	High	Low	Low	Low
Pingtel SIPxChange	2.2	Medium	Medium	Low	No Open Ports
Siemens ICN HiPath 3500	4.0	High	High	High	No Open Ports
SWYX International SwyxWare	4.21	Low	High	Low	Low
Vertical InstantOffice 3500	6.0	Low	Low	Low	Low

Source: VoIP Security Assessment 2006 Copyright © 2006 Miercom



# VoIP Product Inherent Security Compared (3 of 4)

Comparative results of vulnerability scan (open ports) on call controllers, Media Gateways, and IP Phones

Vendor/system	Version scanned	Total number of open ports (1)	High Severity (2)	Low Severity (3)
Alcatel/ OmniPCX Enterprise	R5.1Lx	18	4	10
Alcatel Media Gateway	R5.1Lx	65	1	4
Alcatel OmniPCX Enterprise Express	R5.1Lx	20	5	10
Avaya CLAN (Control LAN card) to S8700 Media Server	2.0	3	0	3
Avaya MedPro (Media Processor) module in G650 Media Gateway	2.0	1	1	4
Avaya IP Office 403	2.0	13	1	3
Cisco CallManager (7835H)	3.3(3)	46	11	25
Cisco CallManager Express	3.1	12	2	8
Cisco 3725 Media Gateway, IOS	12.3(7)T	4	0	1
EADS Telecom PointSpan M6501	E3FP	24	1	3
Interactive Intelligence, Enterprise Interaction Center (EIC)	2.3	10	6	24
Interactive Intelligence, Cisco Gateway [Cisco 1760]	Cisco IOS	4	1	5
Mitel 3300 Integrated Communications Platform	R4.1	26	28	20
Nortel Signaling Server (includes H.323 gatekeeper and gateway)	SSE 2.10.81	7	2	8

Source: VoIP Security Assessment 2006 Copyright © 2006 Miercom



# VoIP Product Inherent Security Compared (4 of 4)

Comparative results of vulnerability scan (open ports) on call controllers, Media Gateways, and IP Phones

Nortel Call Server/Media Gateway	R3.0	4	0	4
Pingtel SIPxChange	R2.2	7	1	11
Siemens ICN HiPath 3500	4.0	5	1	4
SWYX International SwyxWare	4.21	49	4	82
Vertical InstantOffice 3500	6.0	22	4	8

(1) Total unique TCP and UDP port numbers that Nessus determined were open.

(2) Possible high-severity vulnerabilities, involving services running on ports including these: 21/tcp(ftp), 23/tcp(telnet), 25/tcp(smtp), 80/tcp(www), 123/tcp(ntp), 139/tcp(netbios-ssn), 143/tcp(imap2), 389/tcp(ldap), 2000/tcp(SCCP), 2002/tcp(globe), 2565/tcp(coord-srv), 3571/tcp(megardsvr-port), 5800/tcp(unassigned), 8080/tcp(webcache), 8998/tcp(unassigned), 27444/udp(unassigned).

(3) Possible low-severity vulnerabilities, involving services running on ports including these: 22/tcp(ssh), 53/tcp(domain), 135/tcp(epmap), 443/tcp(https), 513/tcp(login), 514/tcp(shell), 593/tcp(http-rpc-epmap), 1025/tcp(blackjack),

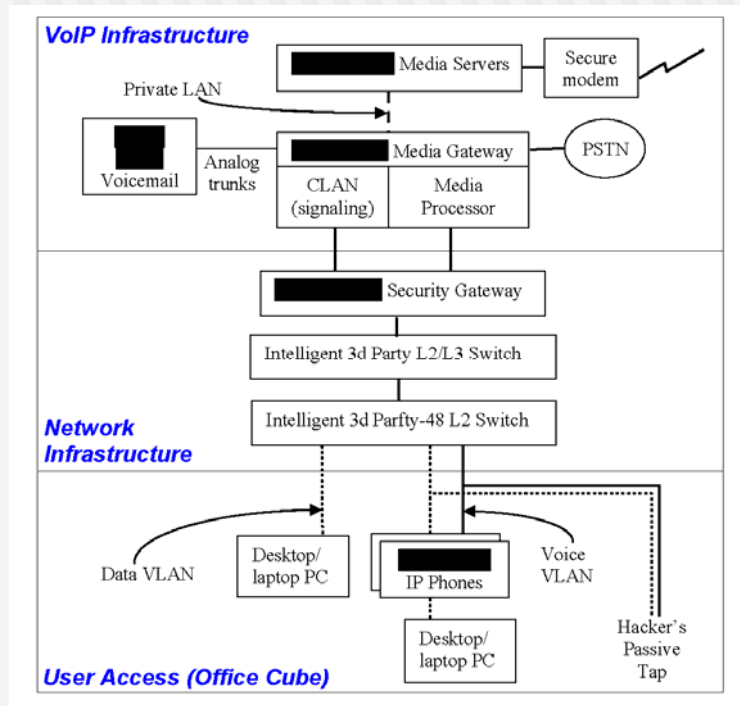
Source: VoIP Security Assessment 2006 Copyright © 2006 Miercom



# Composite Security Reviewed

## Test the complete solution!

Composite system security, we recheck all vulnerabilities previously exposed in the inherent security testing (FWs, IDS, IPF etc., employed of vendors preferred compliment)



Source: VoIP Security Assessment 2006 Copyright © 2006 Miercom

# Composite Security Reviewed

## Test the complete solution!

Composite and standalone security rated scorecard

Criteria	CertifiedSecure™	Stand alone	Composite
Overall Rating (see descriptions below)	<b>Secure</b>	<b>Vulnerable</b>	<b>Resistant</b>
Could insert passive tap cable into 10/100 powered IP phone connection	No	Yes	Yes
Could see, capture IP, MAC addresses, VLAN tag, identify key VoIP nodes	No	Yes	Yes
Could capture and record VoIP conversations (RTP streams)	Yes, but all data 128 bit encrypted	Yes, but all can be encrypted	Yes, but all can be encrypted
Could deliver traffic on Voice VLAN, contact key VoIP nodes, components	No	Yes	Yes
Could impersonate an IP phone (register and/or authenticate)	No	No	No
Could place unauthorized calls	No	No	No
Could effectively attack Call-control infrastructure	No	Yes	Yes
Could effectively attack other IP phones	No	Yes	No
Could effectively assault L2 infra-structure	No	No	No
Could effectively assault L3 infra-structure (including TFTP, DHCP)	No	N/A (no L3)	No

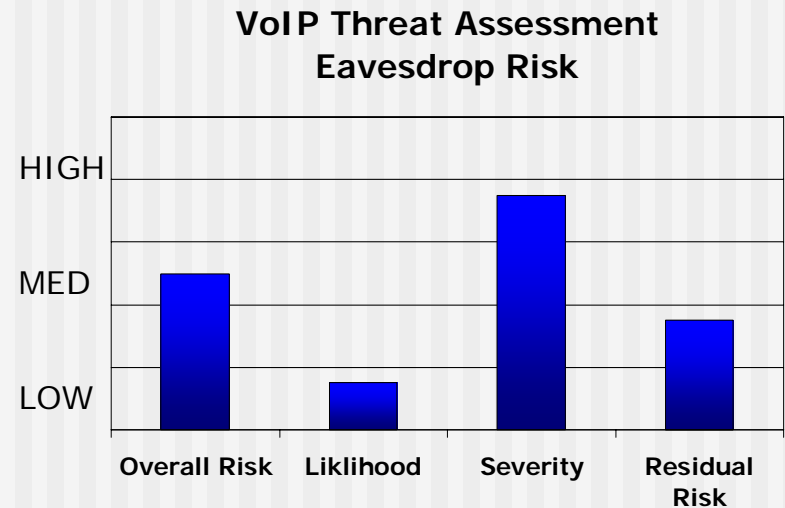
- **Secure** = No perceptible disruption to voice service could be achieved.
- **Resistant** = Attacks could yield only minor and/or temporary disturbance(s).

Source: VoIP Security Assessment 2006 Copyright © 2006 Miercom



# Sniffing Eavesdropping Vulnerability

- Encryption - most products evaluated support encryption (AES) but not call set up and other information
- Relatively easy to reassemble an unencrypted VoIP call
- Testing an AES rated product we were still able to capture key information after ongoing monitoring (see next slide)



# Information captured Eavesdrop from Man in the Middle Attack

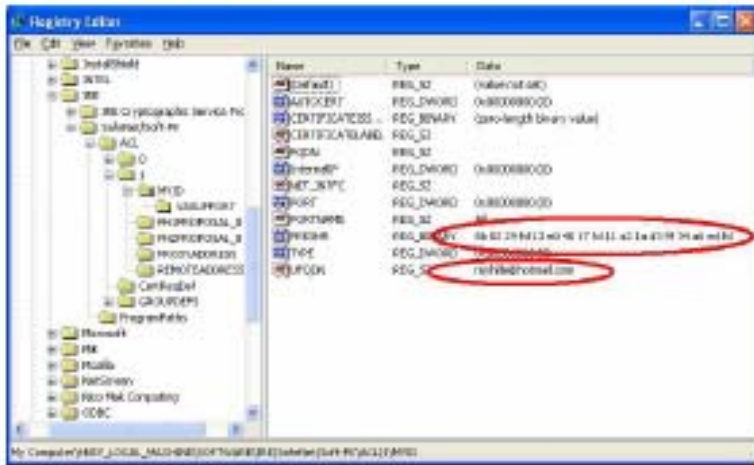


Figure 2: Username and Obfuscated Password Stored in Registry

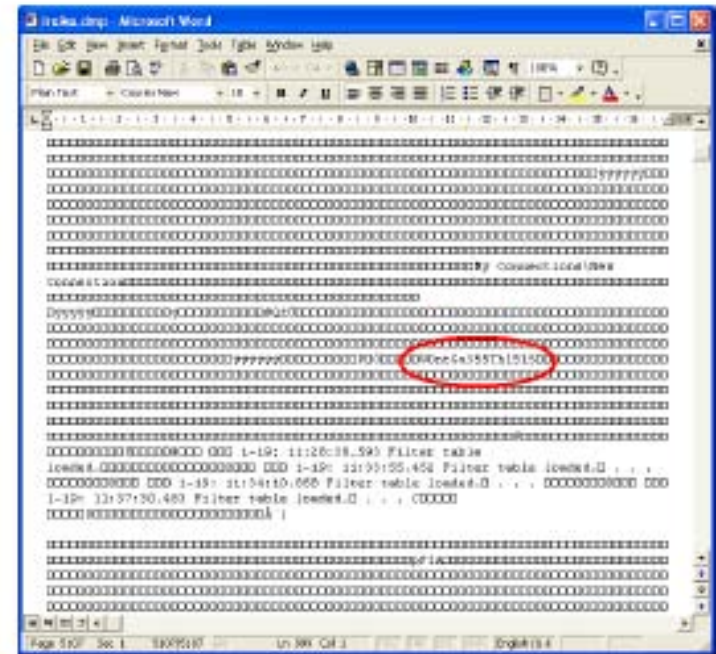
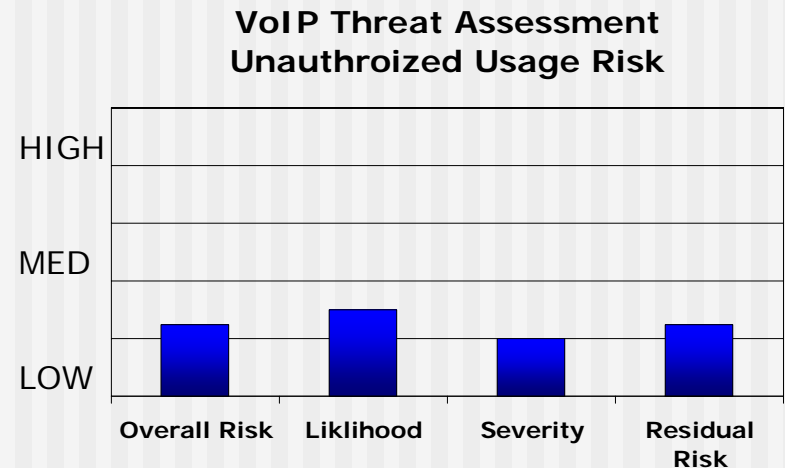


Figure 1: VPN Client Process Memory Dump Showing Plain Text Password

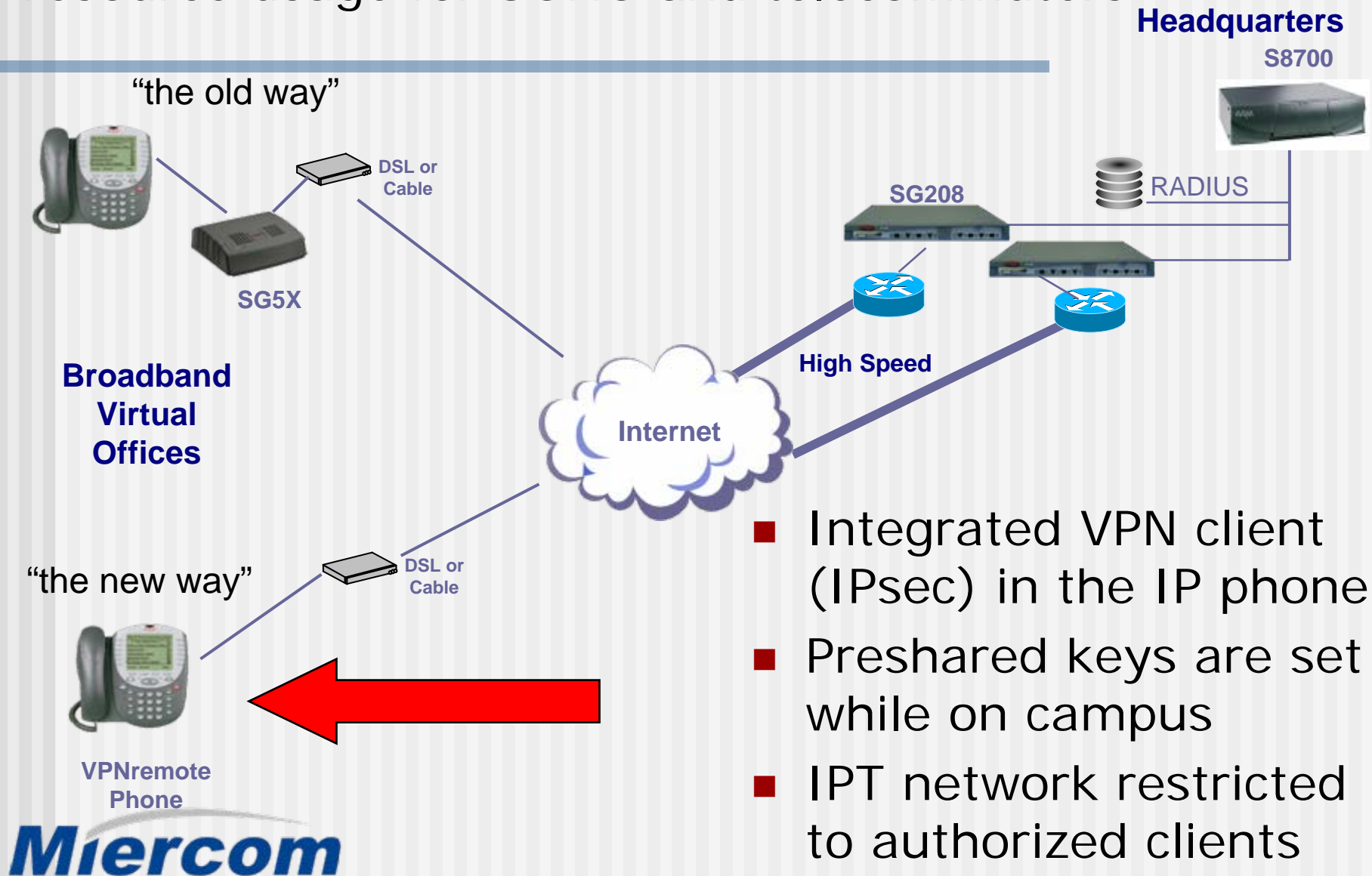
Password captured in the clear even though AES encryption was employed. A man in the middle attack allowed key info to be collected during connection setup

# Unauthorized Resource Usage Vulnerability

- Much hype for this vulnerability, potential concern but not yet observed prevalent
- Vulnerability tests have proven it is possible however
- Recent increase in concern for this vulnerability as IPT providers extending service to remote and SOHO users

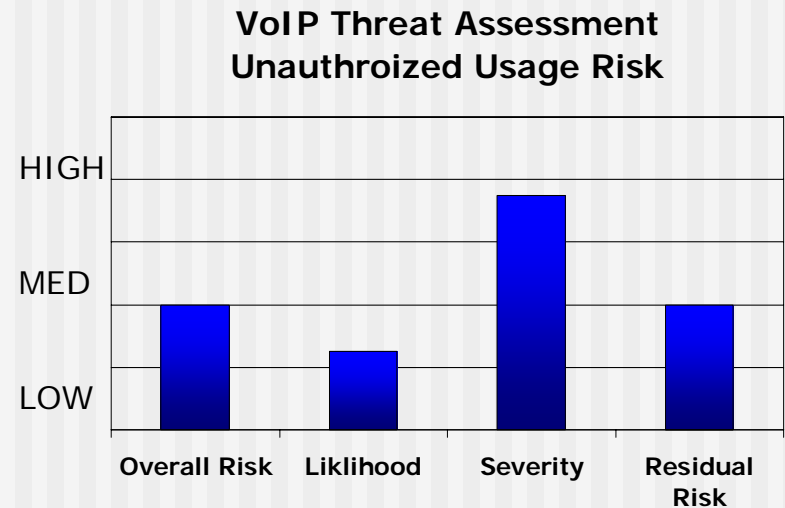


# Example on how to thwart unauthorized resource usage for SOHO and telecommuters



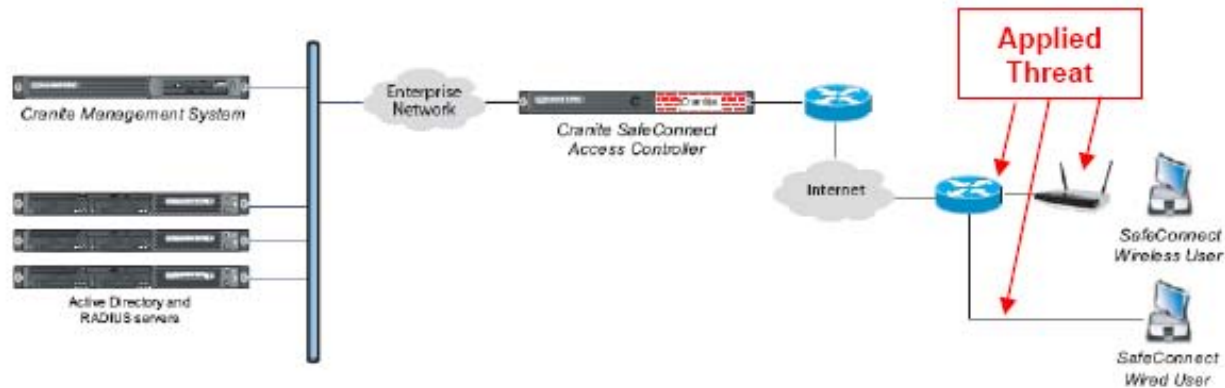
# Identity Theft Vulnerability

- Not observed any documented cases of this using IPT, however vulnerability tests have proven it is possible
- Recent increase in concern for this vulnerability as IPT providers extending service to remote and SOHO users



# Man in the Middle Attack

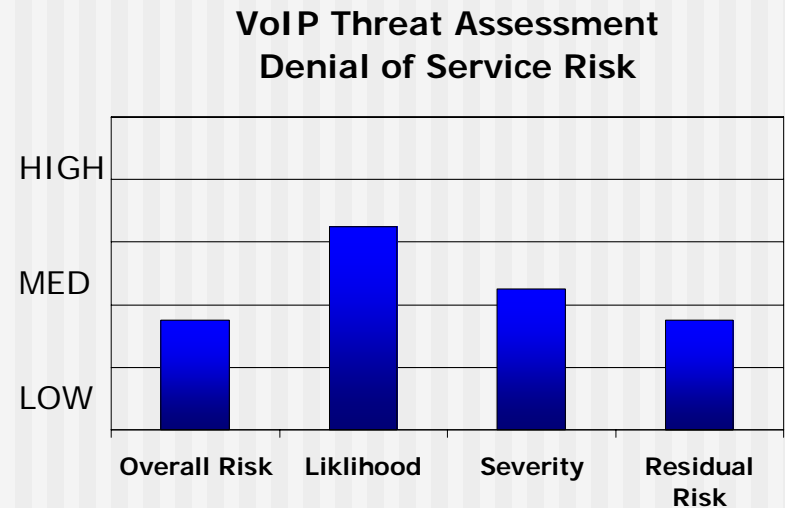
## Test Bed Setup



In this particular test, we redirected secure IPsec tunnels and captured information on call setup up for remote users. Passwords and other key information were found vulnerable after we successfully inserted ourselves into the remote users connection to home office.

# Denial of Service Vulnerability

- Very common and occurrences at large VoIP deployments today
- Can be malicious (targeted), can also be due to an error in deployment
- Many possible sources, predominant is virus propagation
- Instances of VoIP specific attacks documented



# DoS Outages are most significant threat today on customers' networks for converged networks

---

## **Virus and DoS Attack (Nov 05)**

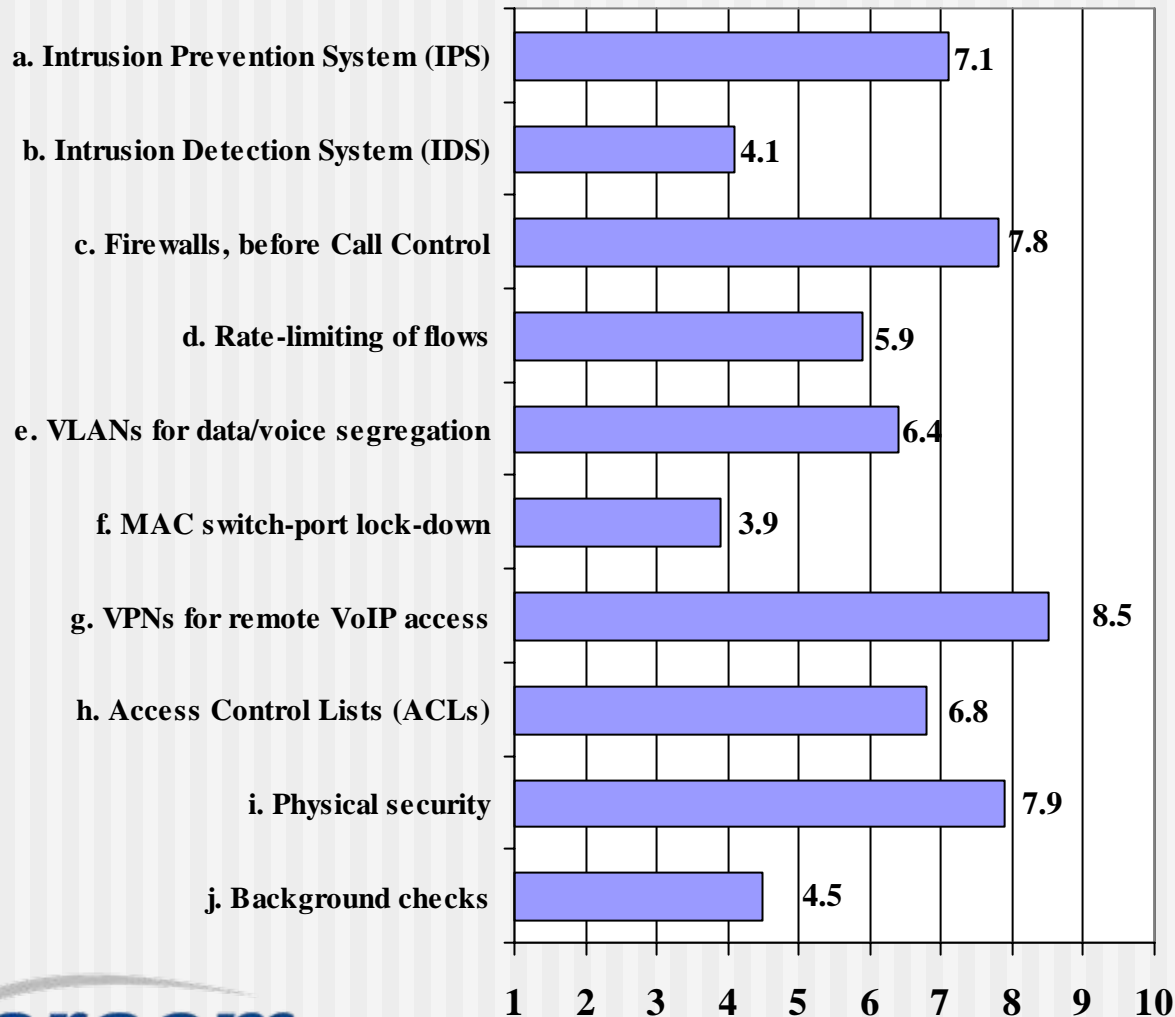
West Cost municipality, virus entry via email bypassed virus scanning products employed for 24 hours. Virus propagated a DoS attack – network utilization peaked. **Networked applications and VoIP rendered ineffective. Over 2,000 VoIP phones disabled for 6 hours.**

## **Slammer (July 05)**

### **and other types of attacks**

Triggers an overflow in memory within a critical NT based CallManager process. This can result in a denial-of-service condition, which will cause the CallManager server to shut down and reboot. **Attacker could redirect calls and eavesdrop on calls**

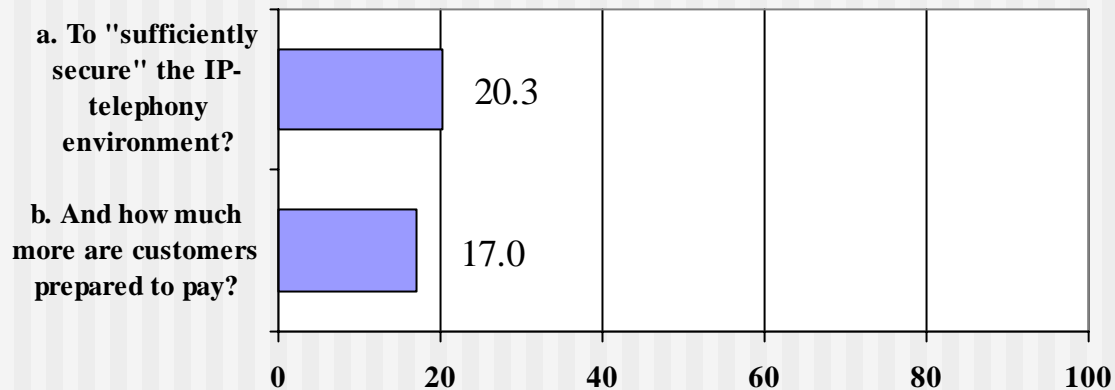
# Top 10 Most Effective VoIP Security Measures



Source: VoIP Security Assessment 2006  
Copyright © 2006 Miercom

# Cost for Effective VoIP Security Measures

Fig. 4-6: How Much More Should Adequate Security Cost? (percent) \*



Source: VoIP Security Assessment 2006  
Copyright © 2006 Miercom

# VoIP Security – Encryption and Authentication

	<b>Alcatel</b>	<b>Avaya</b>	<b>ShoreTel</b>	<b>Siemens</b>	<b>3Com</b>
<b>VoIP RTP voice stream (media) encryption</b>	Yes, supported on gateways and Alcatel IP Touch hard phones. NOT (yet) supported on softphones	Yes, on all links (including to/from gateways) and phones including softphones	Yes, on vendor's IP phones (MGCP) and gateways; NOT on softphone or any supported SIP phones	Yes, on vendor's IP phones and gateways; being added to softphone (not yet supported when tested)	No, none
<b>Media encryption</b>	Secure RTP, 128-bit AES	Uses 128-bit AES	Proprietary 64-bit	Secure RTP, 128-bit AES	No, none
<b>Call set-up and call control encryption</b>	Key call-control values are encrypted, including by softphones	To some extent (between gateways and server); generally, we could not readily extract useful info from captured call-control Packets	No, none	Yes, per Secure RTCP specification; 128-bit AES.	Registration pw is hashed in transmission via MD5 algorithm
<b>Endpoint/caller authentication</b>	802.1x (external RADIUS) and EAP/MD5 authentication are supported	Encrypted key exchange at phone registration (HMAC-SHA1), which is used for each call; no 802.1x external authentication; 8-digit PIN passwords	UserID and password (up to 25 digits) wireless SIP phone (only) supports 802.1x/ RADIUS	802.1x (external RADIUS) authentication supported by all IP endpoints; also, mechanisms preclude message spoofing	Variable-length Password required for initial phone registration