

VoIP Security



Presented at INTEROP
September 19, 2006
by Gary Audin
Delphi, Inc.

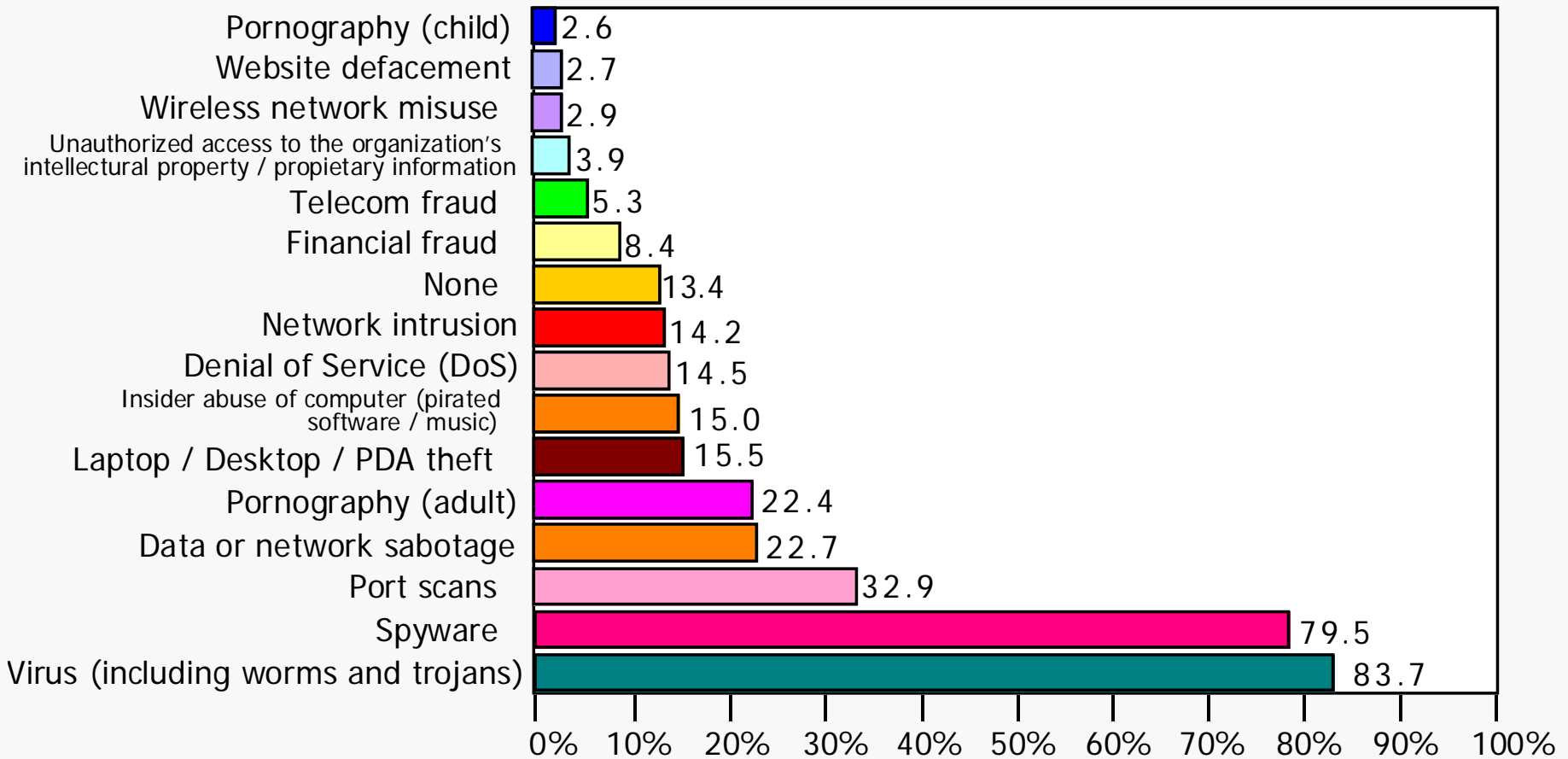
TDM-Based Voice Technology

- Smart centralized telephone switch
- Dumb telephones
- Identity = phone number
- Restricted administrative control access
- Strong physical security

IP-Based Voice Technology

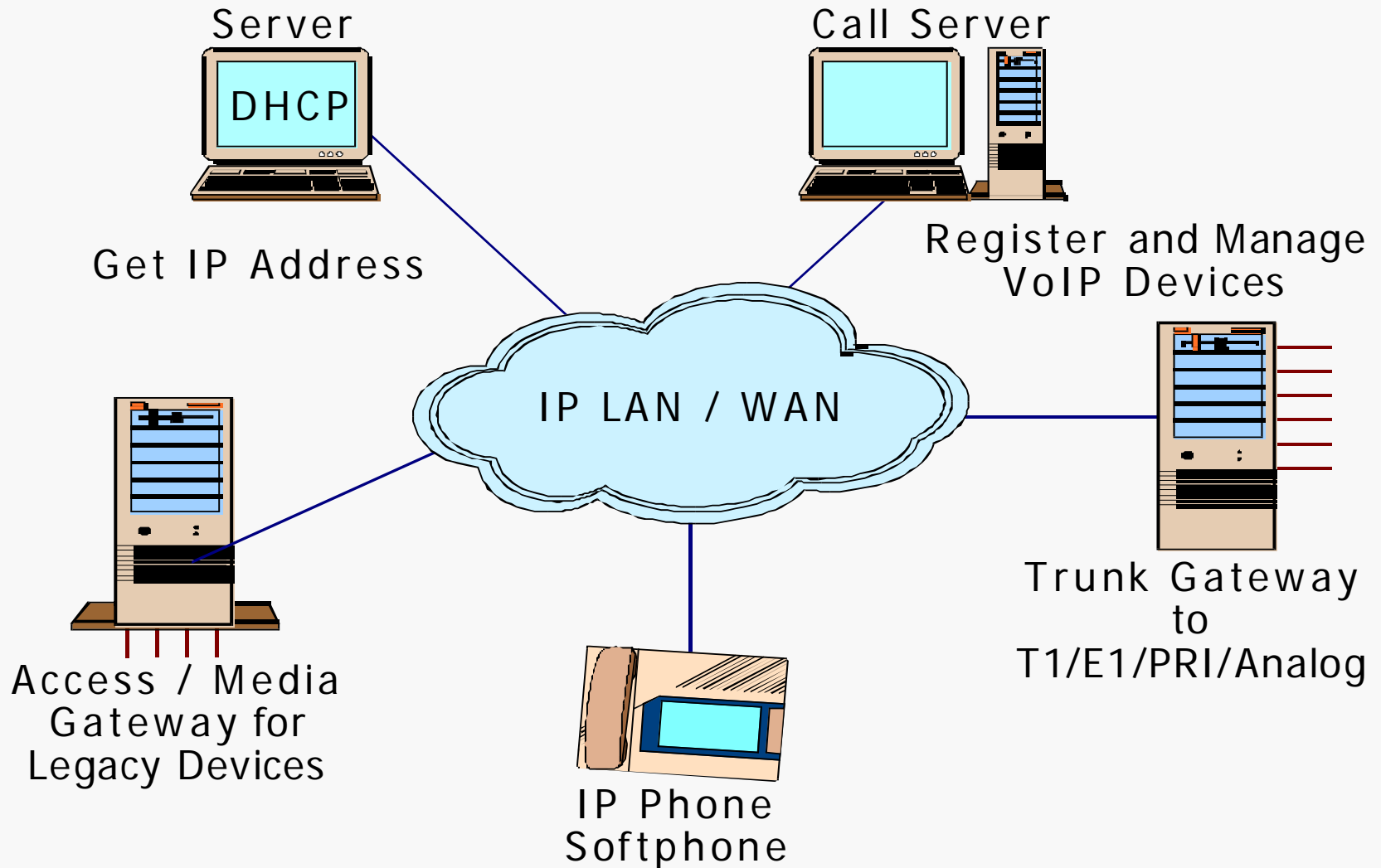
- Call server-based control
- Dumb LAN switch and router
- Distributed smart telephones
- Distributed smart gateways
- Identity = phone number + IP address
- Open control access through IP network

Types of Computer Security Incidents



Source: 2005 FBI Computer Crime Survey

IP PBX Components to Secure



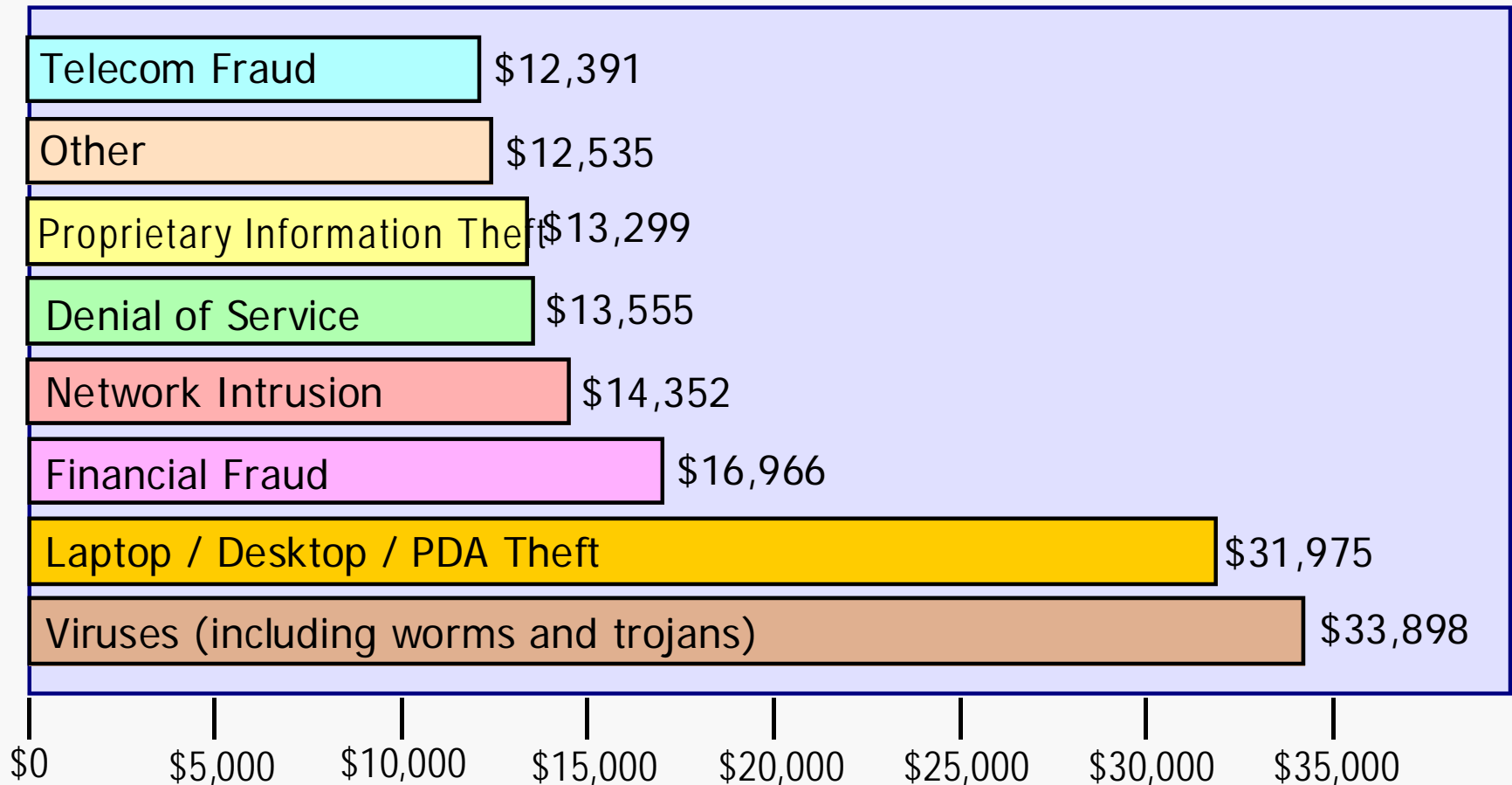
Security Issues

- Hacker (internal or external)
- Viruses/worms/trojan horses
- Spyware
- User authentication
- Access authorization
- Vulnerability during moves/adds
- Denial of service

Old/New Security Threats

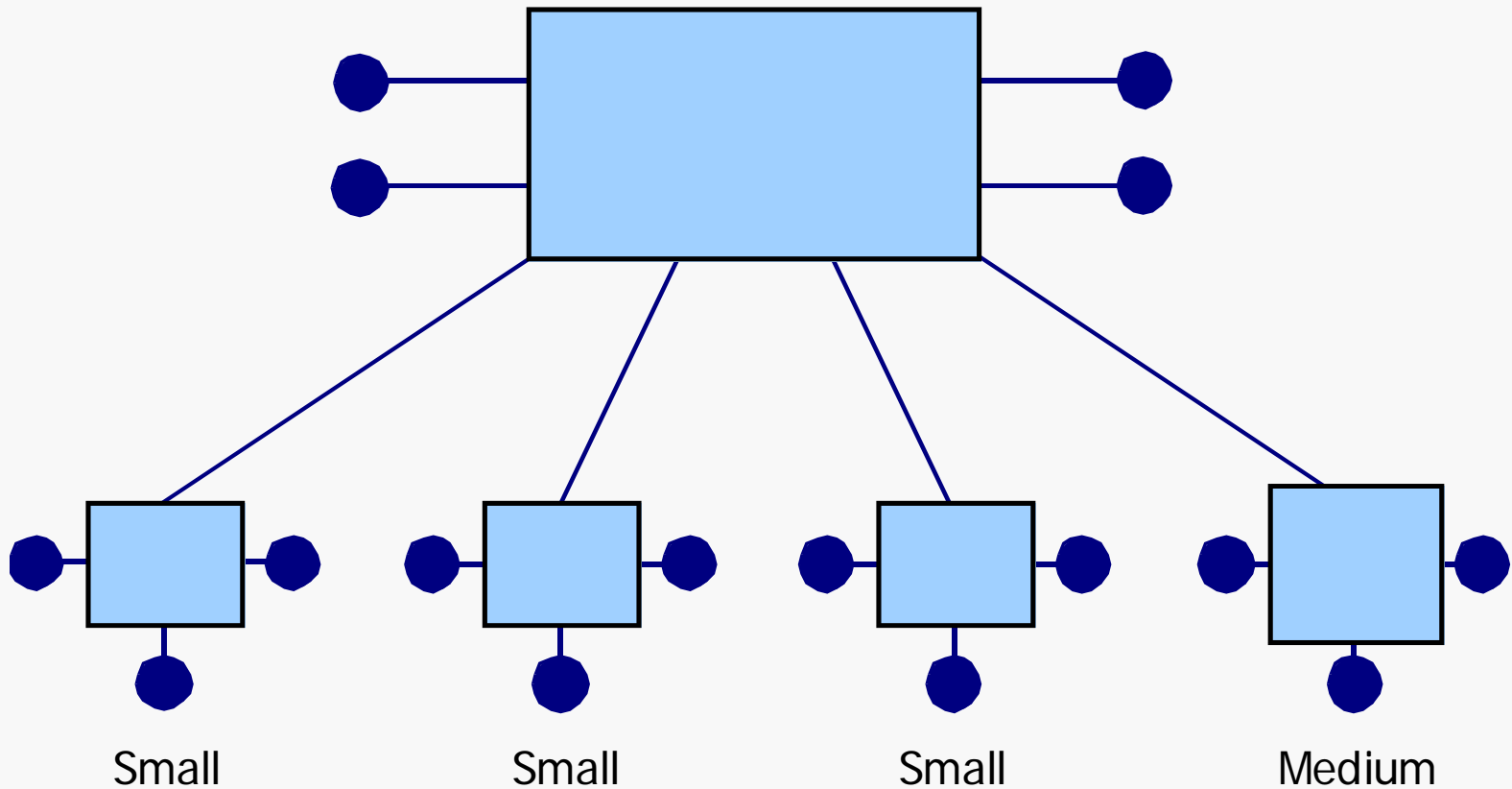
- Default password vulnerability (switch, phone)
- ARP cache poisoning and floods
- Web server interface
- IP phone netmask vulnerability
- Extension to IP address mapping vulnerability
- Insecure state (reset...)
- DHCP server insertion attack
- TFTP server insertion attack
- CPU resource consumption
- Account lockout

Average Losses

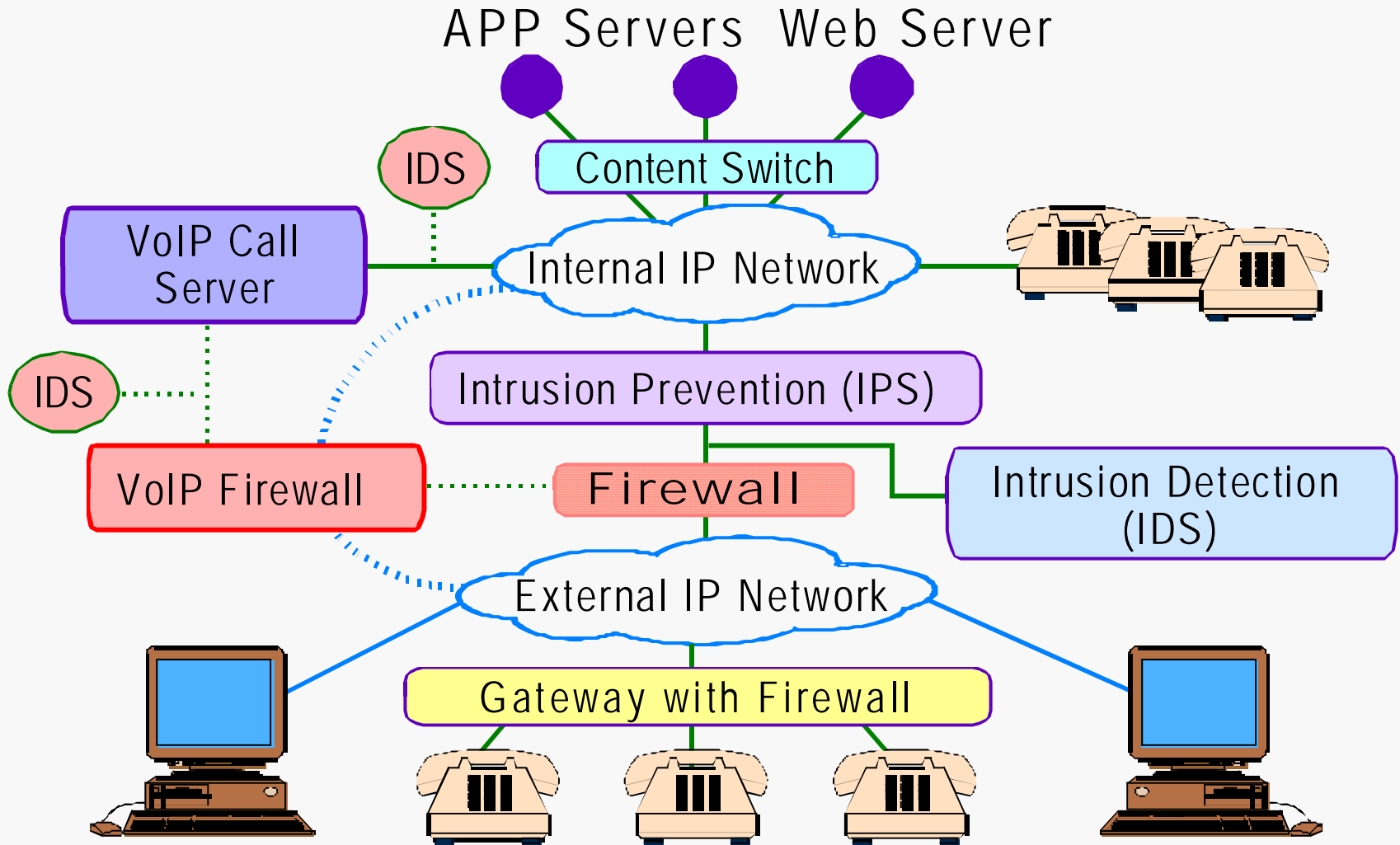


Source: 2005 FBI Computer Crime Survey

Distributed Security Management



Security Positions



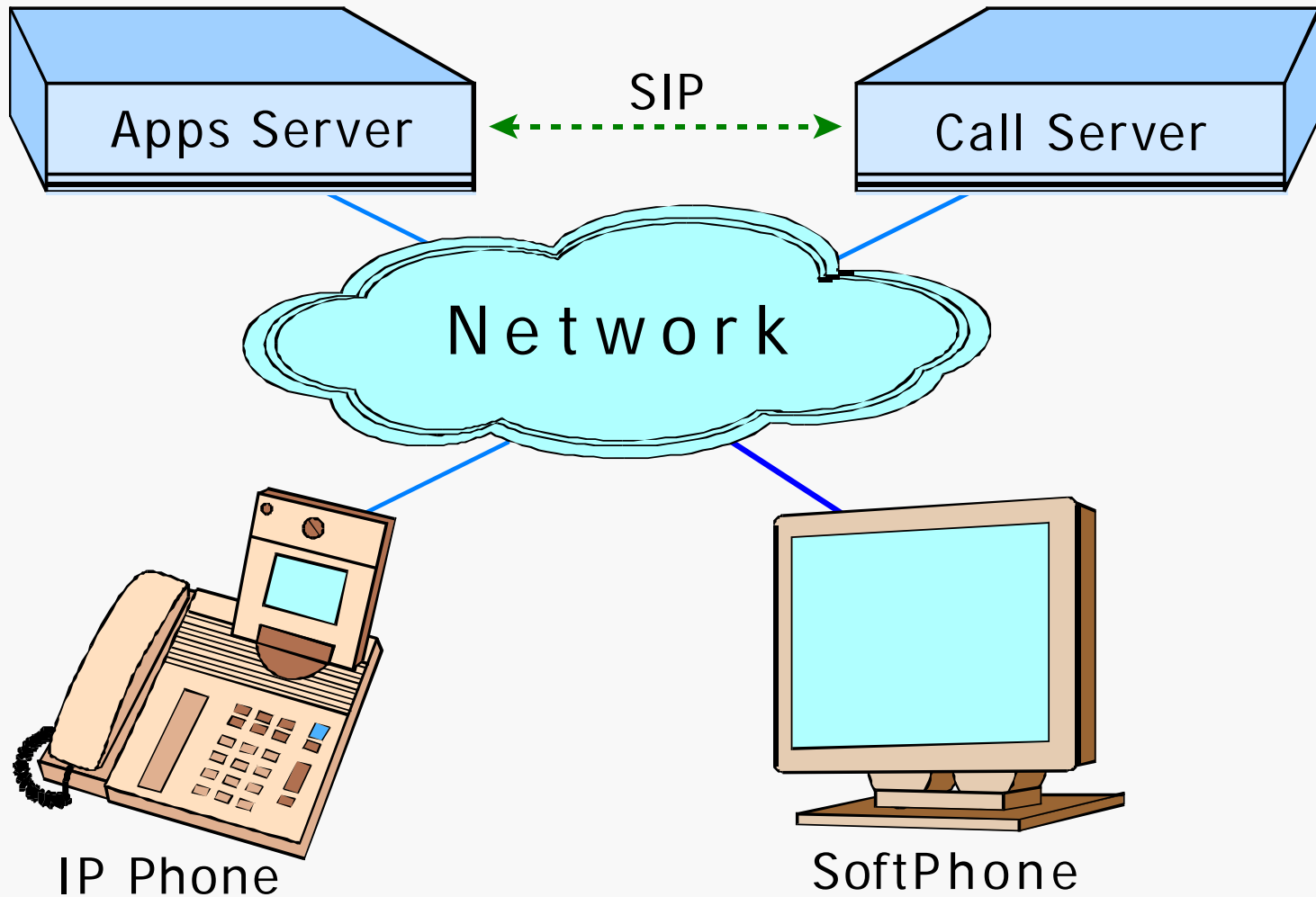
Server Vulnerabilities

- Issues:
 - Operating system/support software issues
 - Application implementation
 - Application manipulation (toll fraud)
 - Unauthorized administrative access
 - Protocol attacks
 - Denial of Service
- Example:
 - See www.ee.oulu.fi/research/ouspg/protos/testing/c07/sip/

Function/Feature Tampering

- Can be enabled without authorization
- Blockage against caller(s)
- Eliminated for call destination
- Application server blockage
- Spoofing Caller ID

Application Residence



Gateway Vulnerabilities

- DoS against phone gateways
- DoS against trunk gateways
- Toll fraud
- Signaling delays
- Internal/external call blocking
- Viruses, Trojan horses, malware

Recommendations for Servers and Gateways

- Try to use secure platforms (remove services)
- Secure the operating system/services
- Maintain patches
- Use strong authentication for access
- Separate LAN/VLAN for access
- Control access by IP Phones and softphones
- Consider using host-based security
- Consider deploying a firewall and IDS/IPS

IP Phone Recommendations

- Implementation:
 - Update default administrator passwords
 - Disable unnecessary remote access feature
 - Prevent casual local configuration of the IP phone
 - Secure the firmware upgrade process
 - Use IP Phones that support security features
 - Limit use of the web server
 - Enable logging

Securing Softphones

- As vulnerable as any PC
- Require virus protection
- Must be patched as often as a data PC
- Softphone software has little or no security
- Can be programmed to bypass the call server for P2P calls
- Can spoof other devices

Vendor Security Features

	Alcatel	Avaya	ShoreTel	Siemens	3Com
RTP Encryption	Yes (except Softphones)	All	Yes (except Softphones)	Yes	None
Encryption Type for Media	SRTP 128-bit AES	128-bit AES	Proprietary 64-bit	SRTP 128-bit AES	None
Call Control Encryption	Yes	Partial	None	Yes Secure RTCP	Registration Password
Caller Authentication	802.1x and EAP/MD5	HMAC – SHA1 8-digit pin	User ID Password 802.1x	802.1x	Variable Length Password

Source: BCR Magazine, January 2006, "High-end IP PBXs: VoIP Powerhouses"

THE END

Delphi, Inc.
delphi-inc@att.net
703.908.0965