IPCOMM2006

September 25-27 • Gaylord Opryland • Nashville, TN

All About IPT Security

Gary Audin

President

Delphi, Inc.

What Will Be Covered

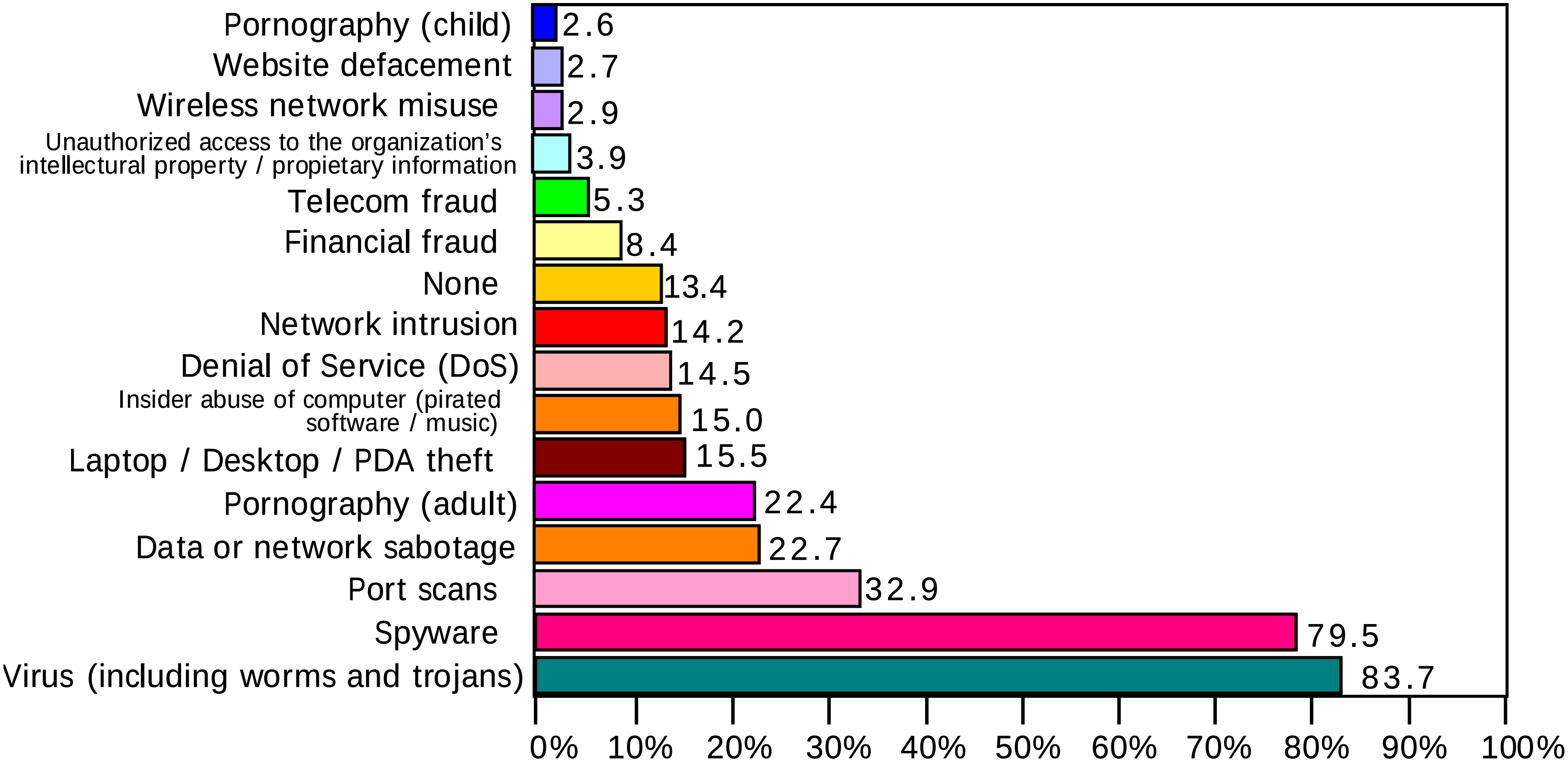
- Defining Security
- What to Worry About
- Systems for Security
- Securing Signaling and Speech
- Malicious Behaviors
- Recommendations
- VoIP/IPT Vendor Support
- Incident Response Team

Security Definition

The protection of resources requires constant vigilance.

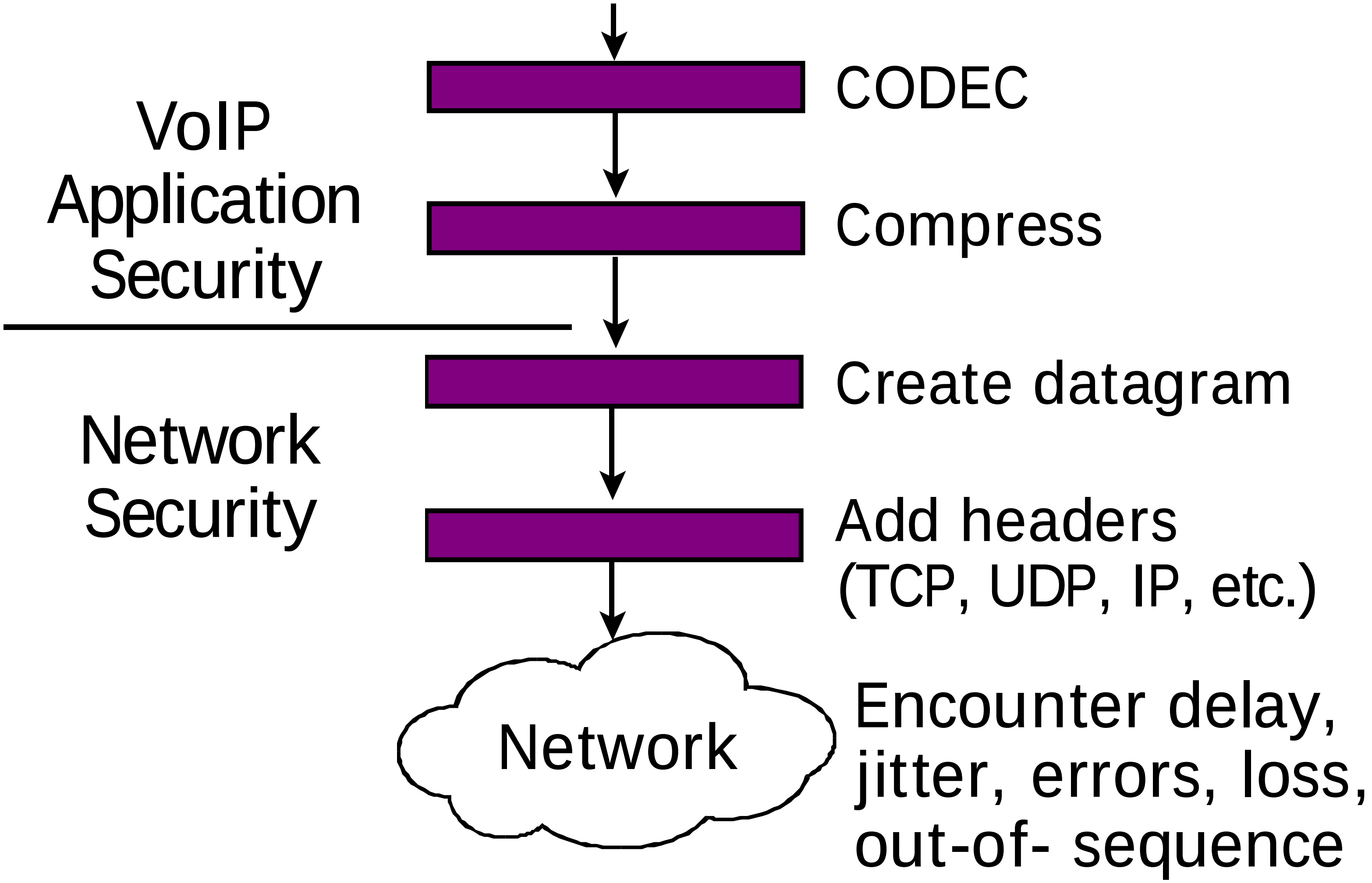
You are never finished.

Types of Computer Security Incidents

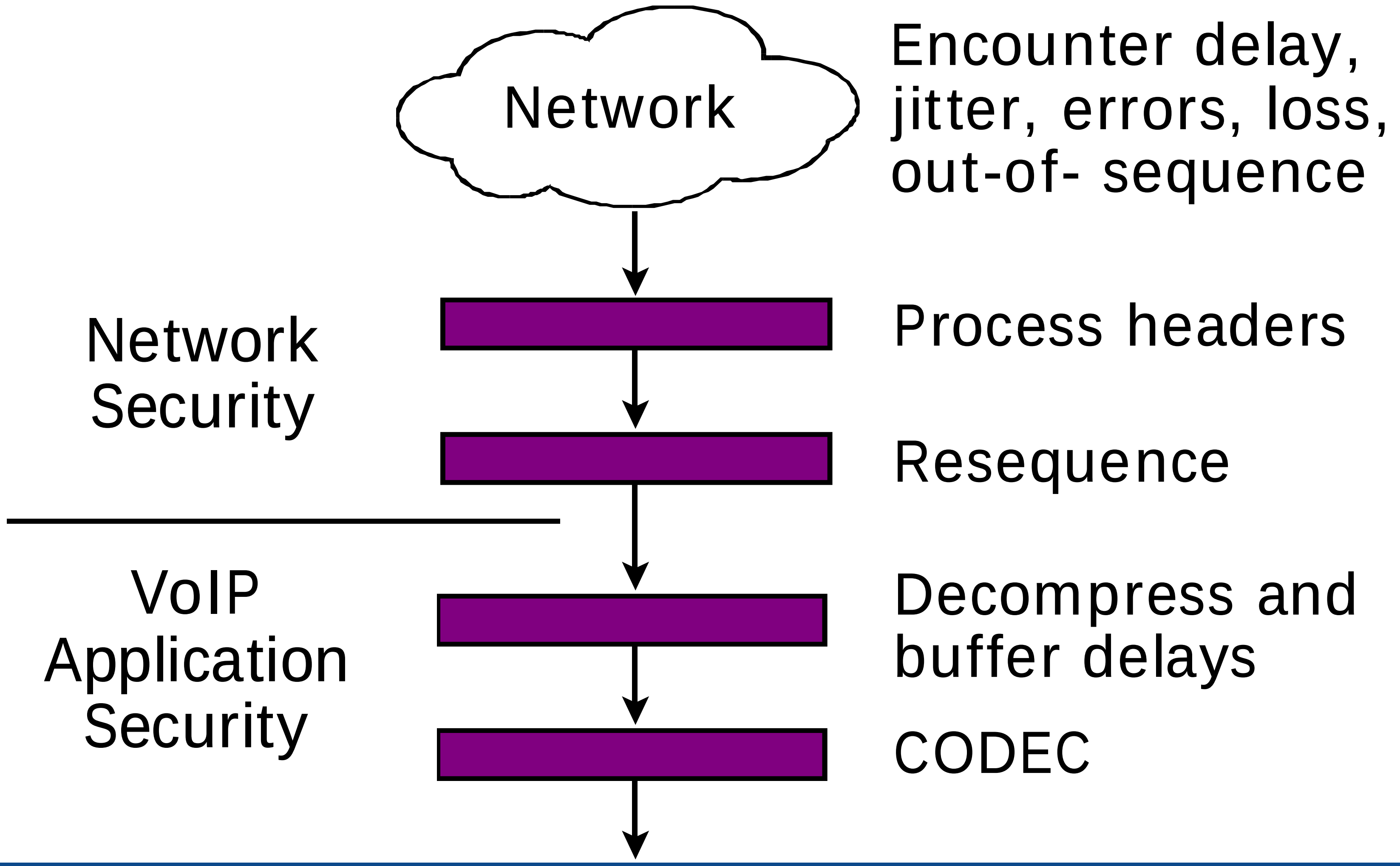


Source: 2005 FBI Computer Crime Survey

IP Network Security (part 1)



IP Network Security (part 2)



Network

Encounter delay, jitter, errors, loss, out-of- sequence

Network Security

Process headers

Resequence

VoIP Application Security

Decompress and buffer delays

CODEC

The Security Design Problem

- Ethernet and IP networks were not designed with integrated security
  - Ethernet, TCP, UDP, and IP Protocols are vulnerable
  - FTP, SMTP, Telnet, HTTP, etc. do not have built-in security features
  - All are peer-to-peer protocols

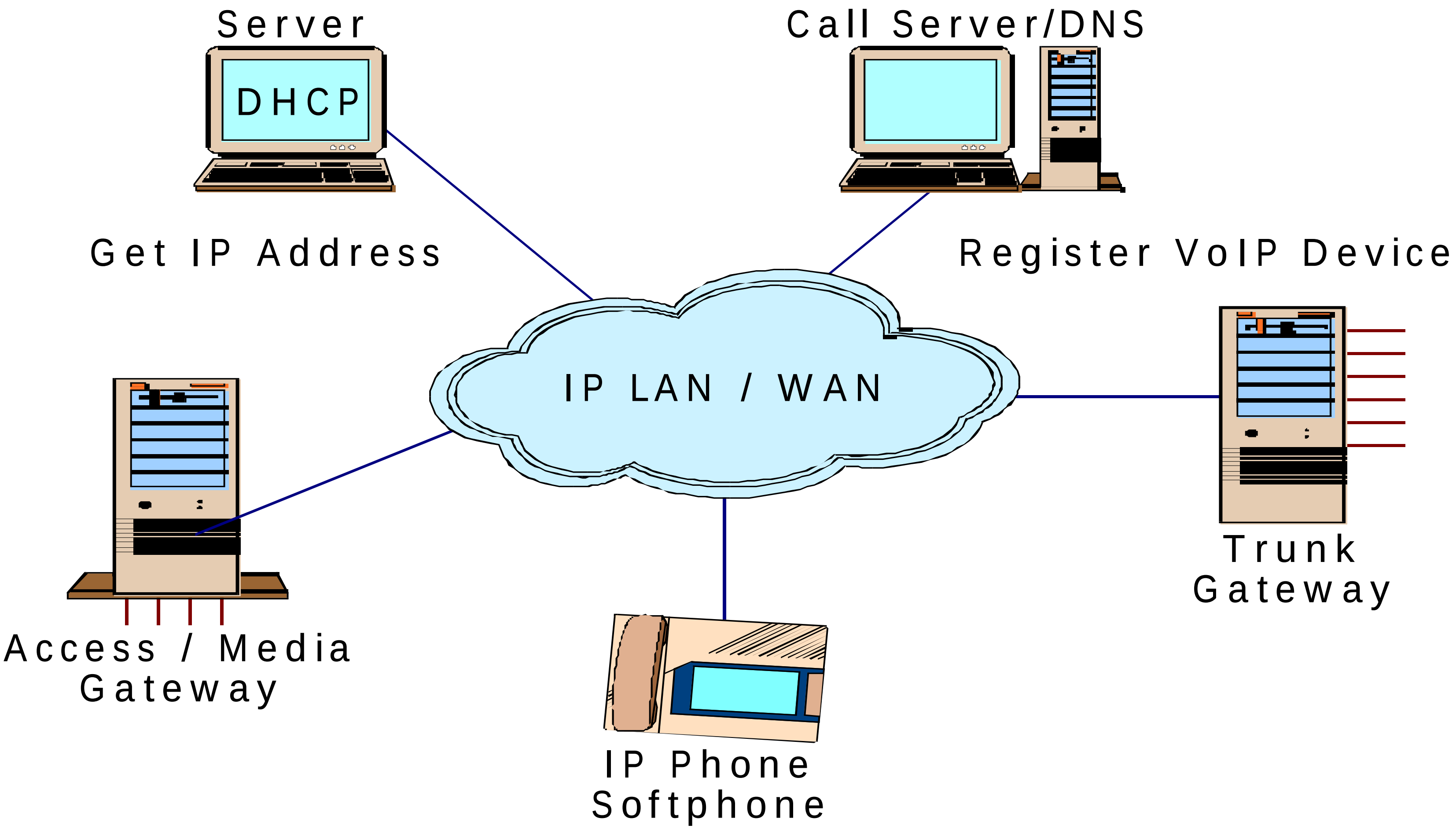
What to Worry About

- Access Control
  - Who can physically access the network?
    - Wired
    - Wireless
- Authentication
  - Knowing/identifying the accessing party
- Authorization
  - Is this party allowed to use the requested services?

More to Worry About

- Confidentiality
  - – Protesting the transmission
    - Signaling
    - Conversation
- Liabilities
  - – Financial
  - – Reputation
  - – Legal

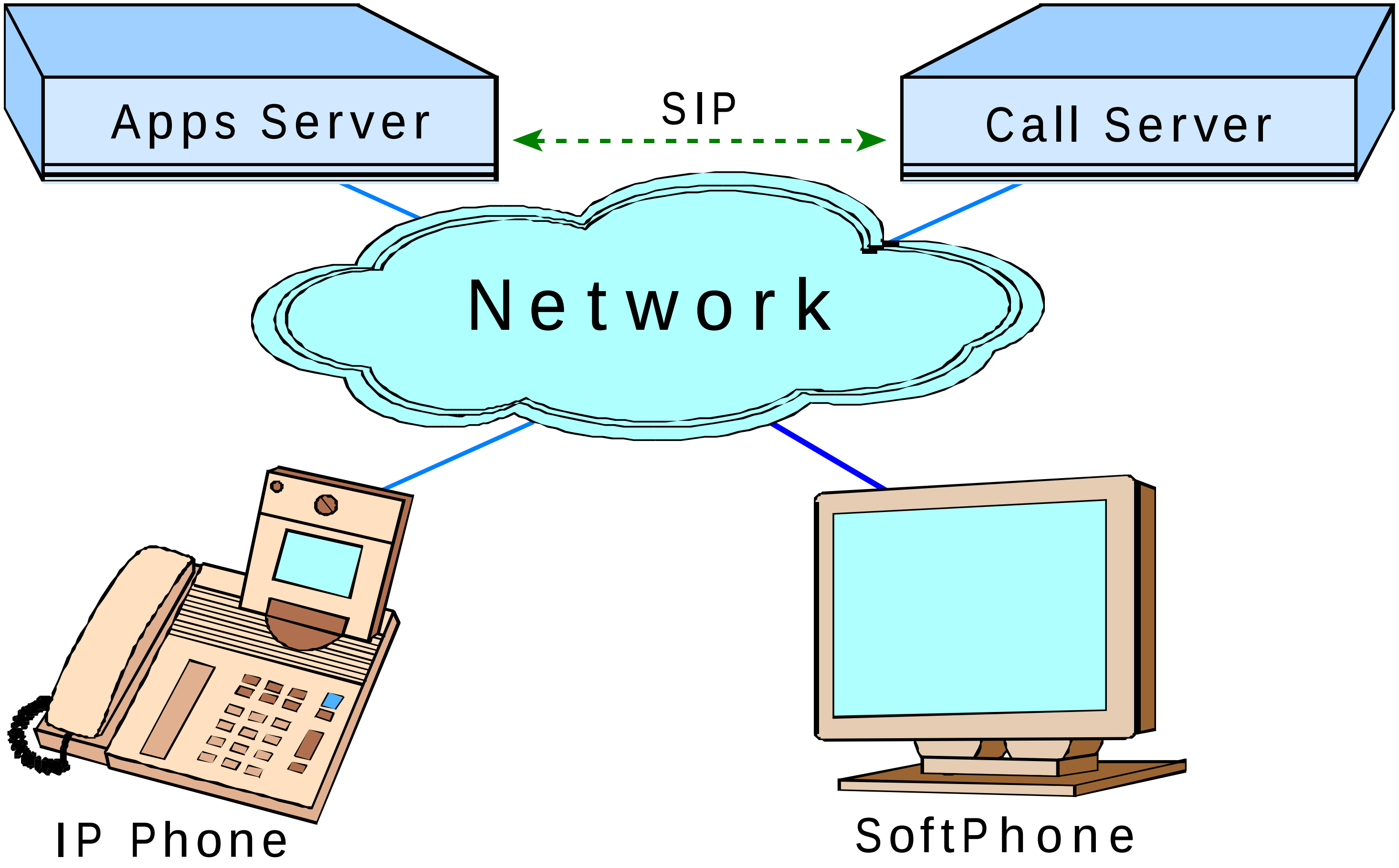
IP PBX Components



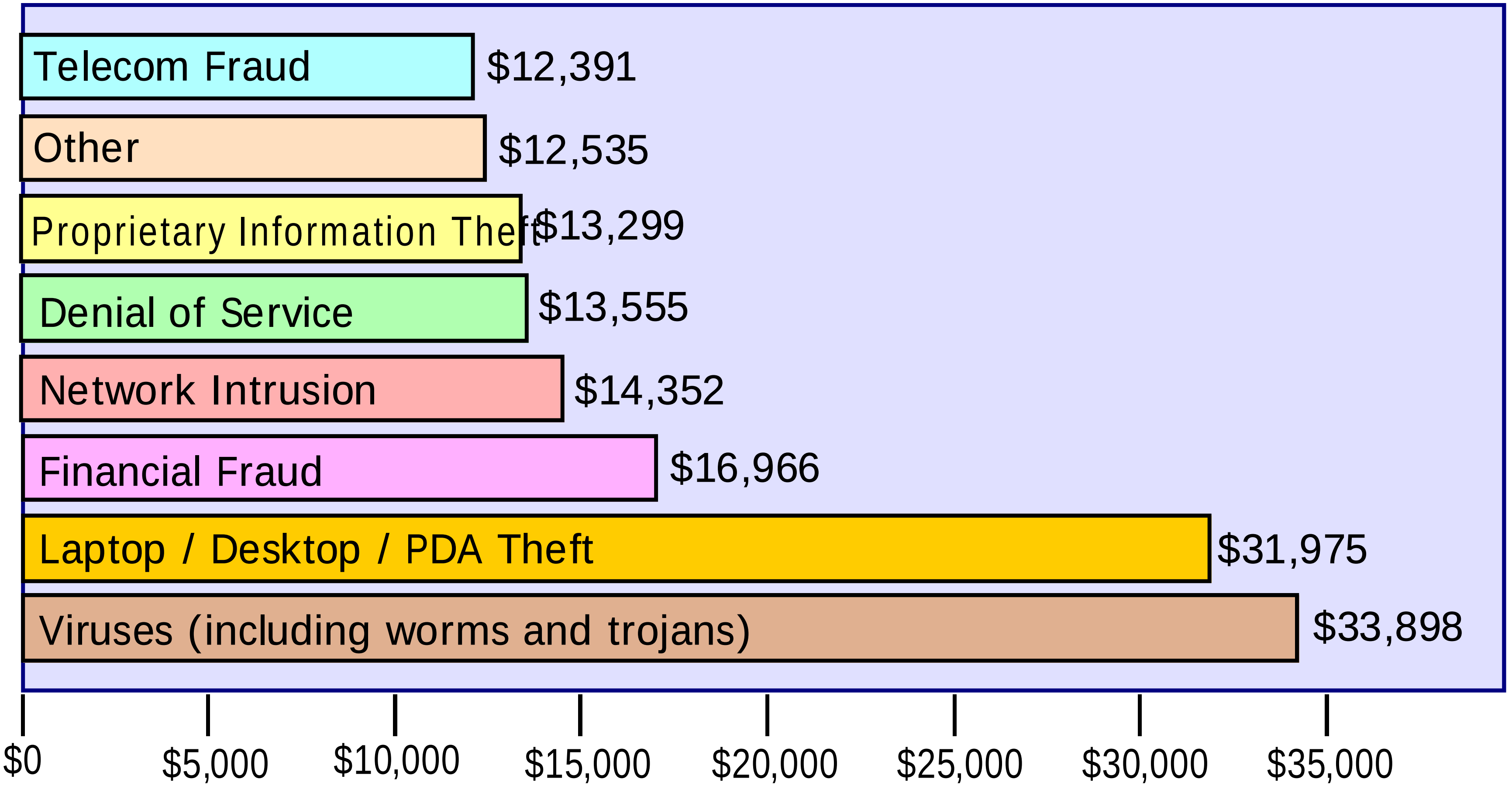
Old / New Security Threats

- 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

Application Residence



Average Losses



Source: 2005 FBI Computer Crime Survey

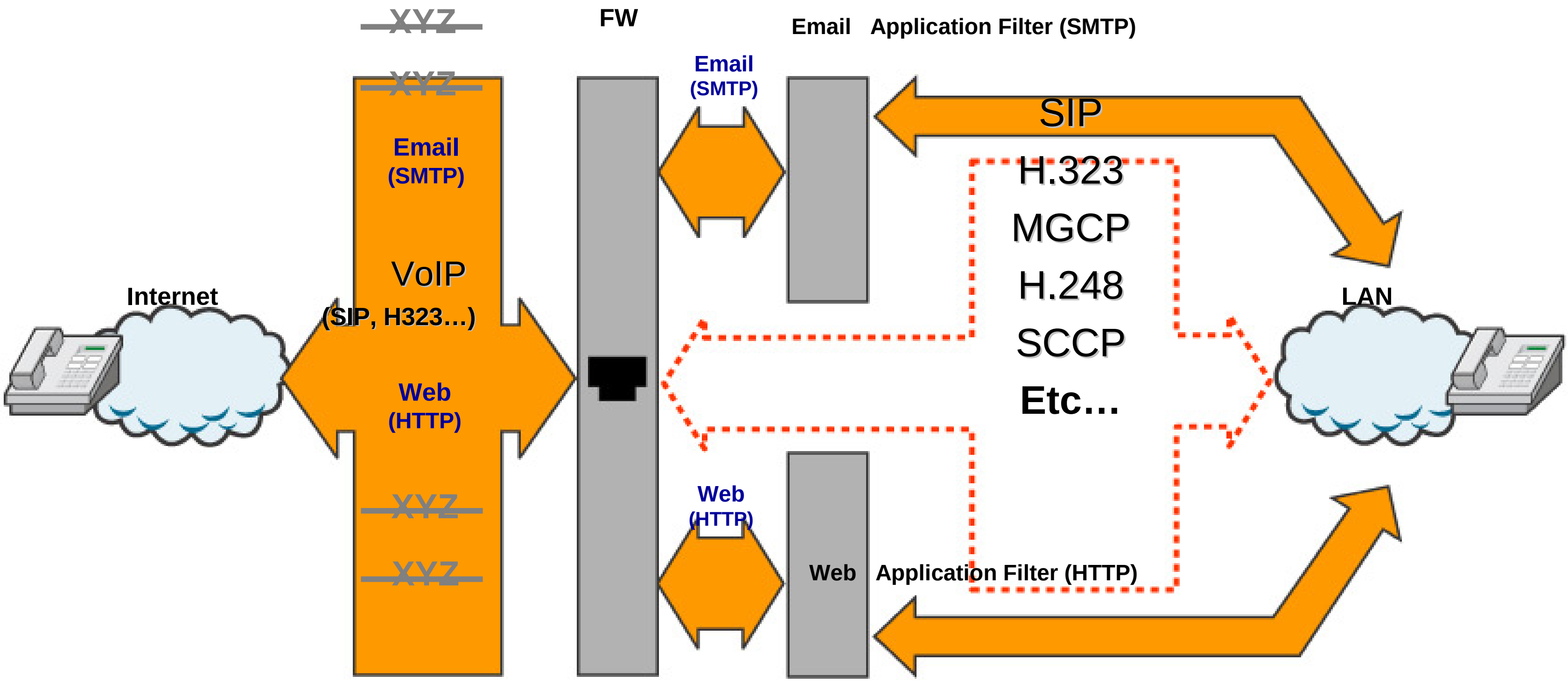
VoIP Security Challenges (part 1)

- Functions/features are installed in products first, then security
- Twice as many IP devices
- Denial of Service attacks disable calls
- Very reliable operation expected (911)
- QoS can conflict with security

VoIP Security Challenges (part 2)

- Multiple signaling standards
- Call quality important
- Network Address Translation (NAT) issues
- Longer call latency for encryption
- Dynamic UDP port assignment per call

Firewall Issues Courtesy of SecureLogix



- Must handle many protocols
- Application aware

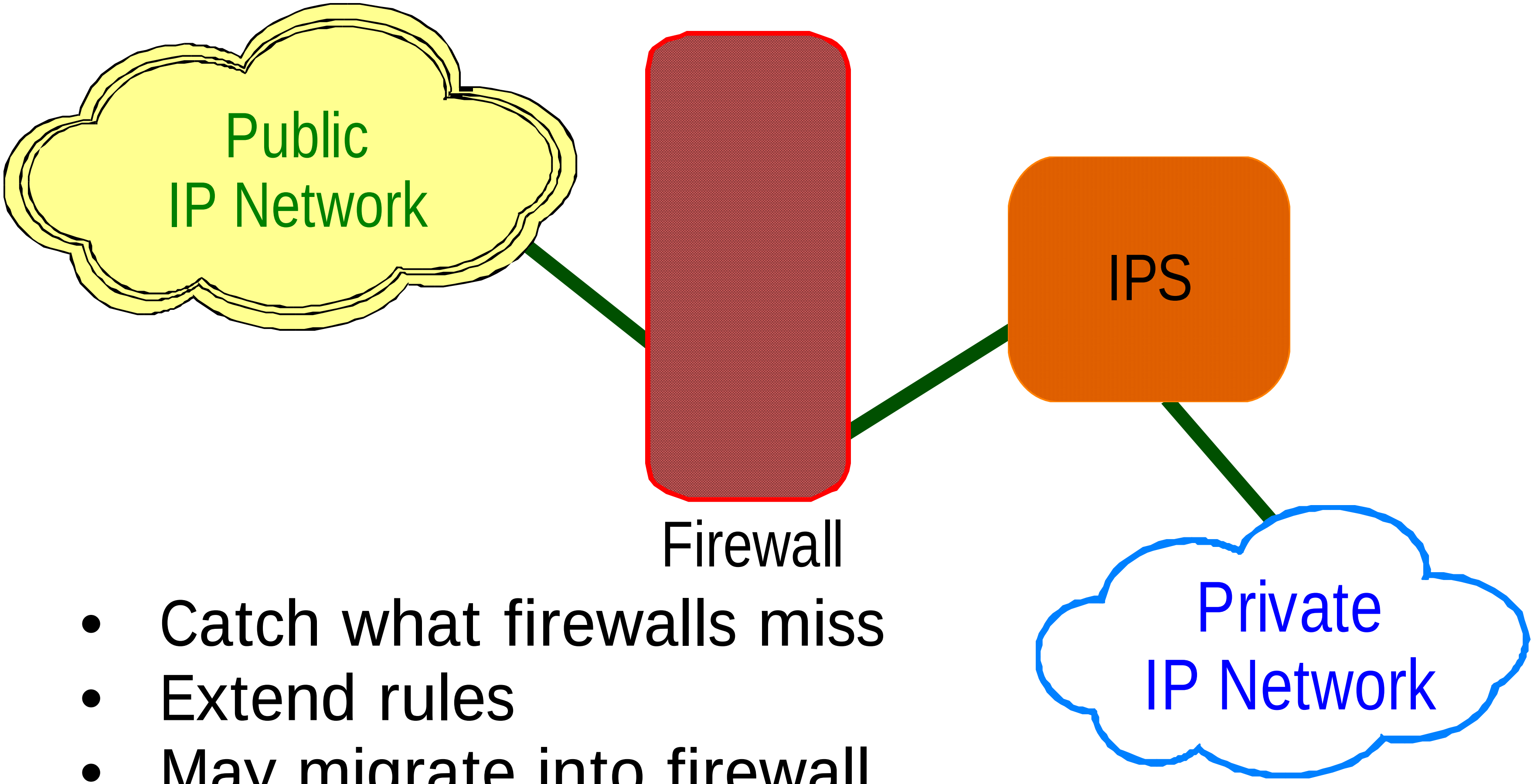
What Data Firewalls *Don't* Do

- Prevent toll fraud
- Prevent DTMF (touch-tone) attacks
- Shut down idle off-hook calls
- Inspect packet content for call type
- Monitor traffic types and report
  - Voice
  - Fax
  - Modem
  - Alarms
  - TDD
- Secure calls for the government
- Support Lifeline (at least one phone works with loss of power or equipment)
- Inspect packets for voice mail attacks and toll fraud signaling

Intrusion Detection

- Collects/Analyzes Network/Computer information for security breaches
- Covers intrusions (outside attacks) and misuse (inside attacks)
- Uses scanning (vulnerability assessment)
- Functions include:
  - Analyzing configurations and vulnerabilities
  - Assessing file and system integrity
  - Monitoring user and system activity
  - Recognizing attack patterns
  - Looking for abnormal activity
  - Tracking user policy violations

Intrusion Prevention Systems (IPS)

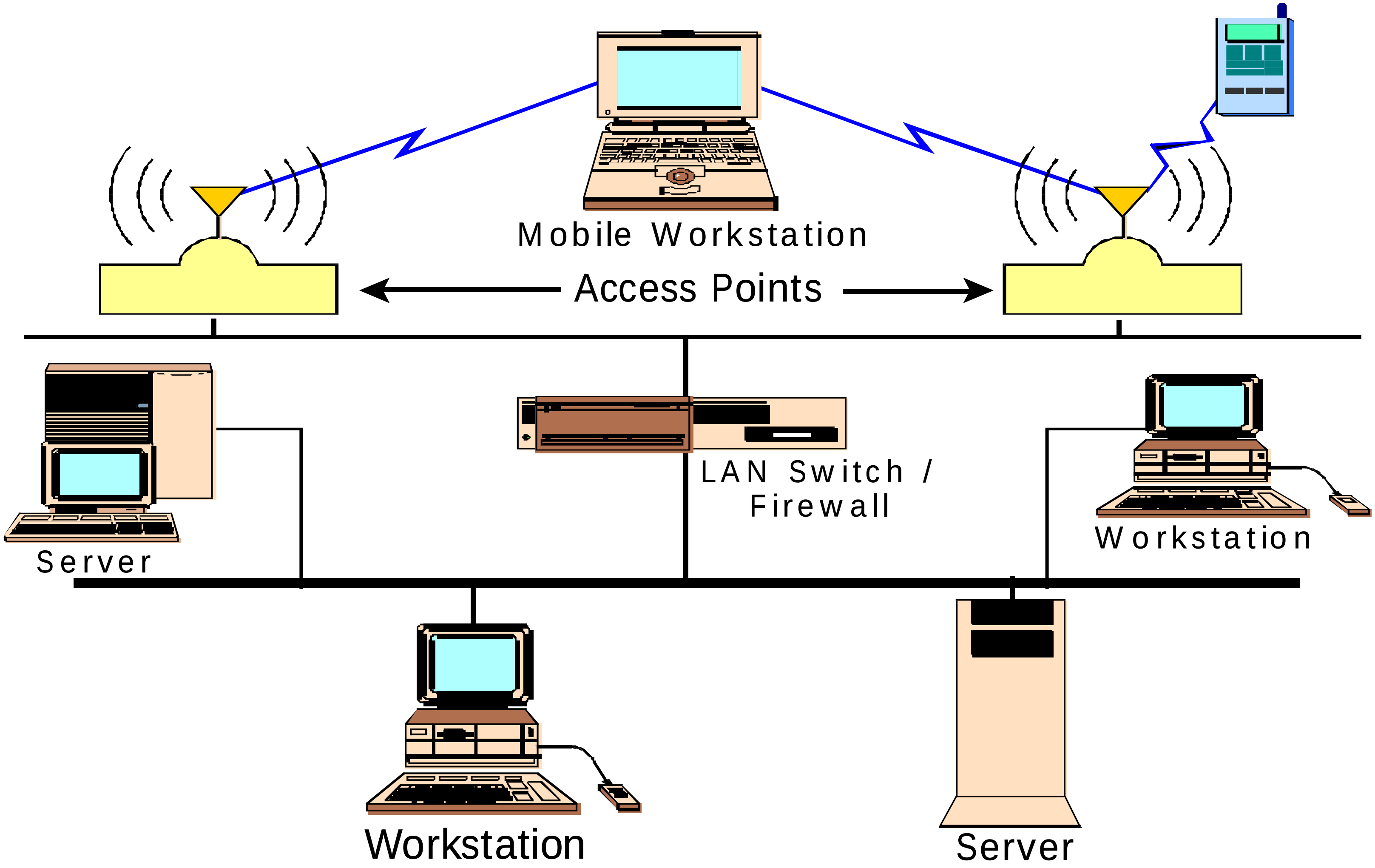


- Catch what firewalls miss
- Extend rules
- May migrate into firewall

LAN Switch Security

- Store configuration information and tables in a secure system
- Validate all changes ***BEFORE*** they are made
- Ensure that changes can only be sent from a very limited set of addresses
- Verify configurations and tables after a restart/reboot
- Add 802.1x to the LAN switch

Wireless Network



Top Ten WLAN Deployment Obstacles

1. Security concerns	68%
2. Interference / performance	26%
3. Waiting for market to settle	24%
4. Managing / troubleshooting	23%
5. Lack of budget	20%
6. Subnet roaming	19%
7. New vendor interoperability	18%
8. High prices	14%
9. Configuring / upgrading apps	14%
10. Too many standards	14%

Source: www.webtorials.com

Locking Down the WLAN

- Standardize NICs, register MAC addresses and turn on access control lists
- Do not use defaults for SSID
- At minimum use Wired Equivalent Privacy (WEP)
- Use Wi-Fi Protected Access (WPA)
- Use a VPN with IPsec or SSL encryption
- Plan for 802.1x
- Monitor the network

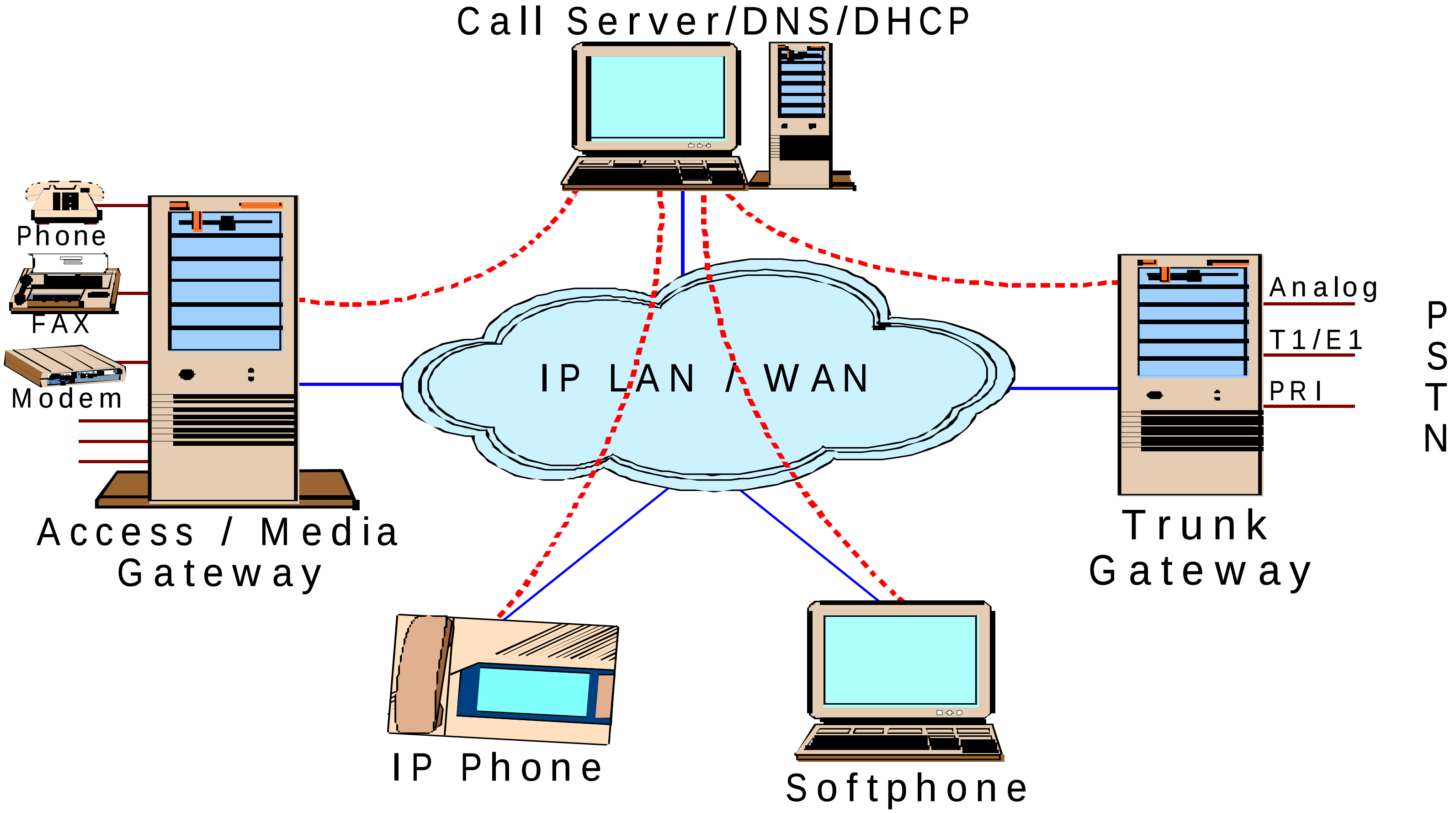
Managing Software

- Operating system
- Applications (features and functions)
- Non telephony applications
- Versions, releases and patches
- Keeping OS and applications coordinated among many sites

Where Do I Start?

- Assume an attack will occur and probably be successful
- Start looking at the core: storage, applications, servers, network
- Look for the most valuable and sensitive resources
- Evaluate risk to these resources
- Protect these resources first
- Work outward to less valuable, less sensitive resources

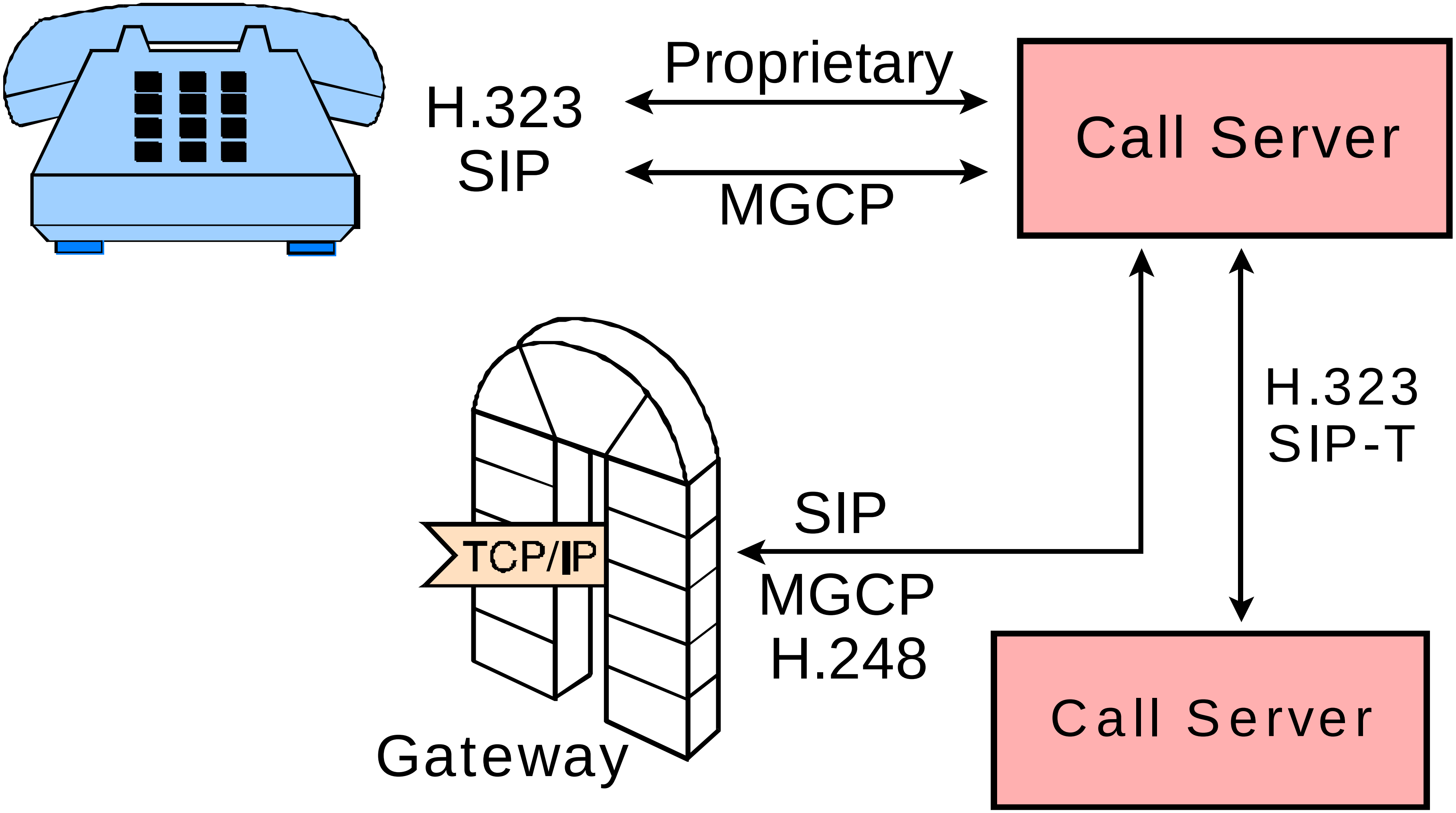
H.323 and SIP Signaling Paths



Calling Configurations

- SIP and H.323 signaling
- Phone to phone (peer-to-peer)
- With one call server
- With multiple call servers

Protocol Usage



H.323
SIP

Proprietary

MGCP

Call Server

H.323
SIP-T

TCP/IP

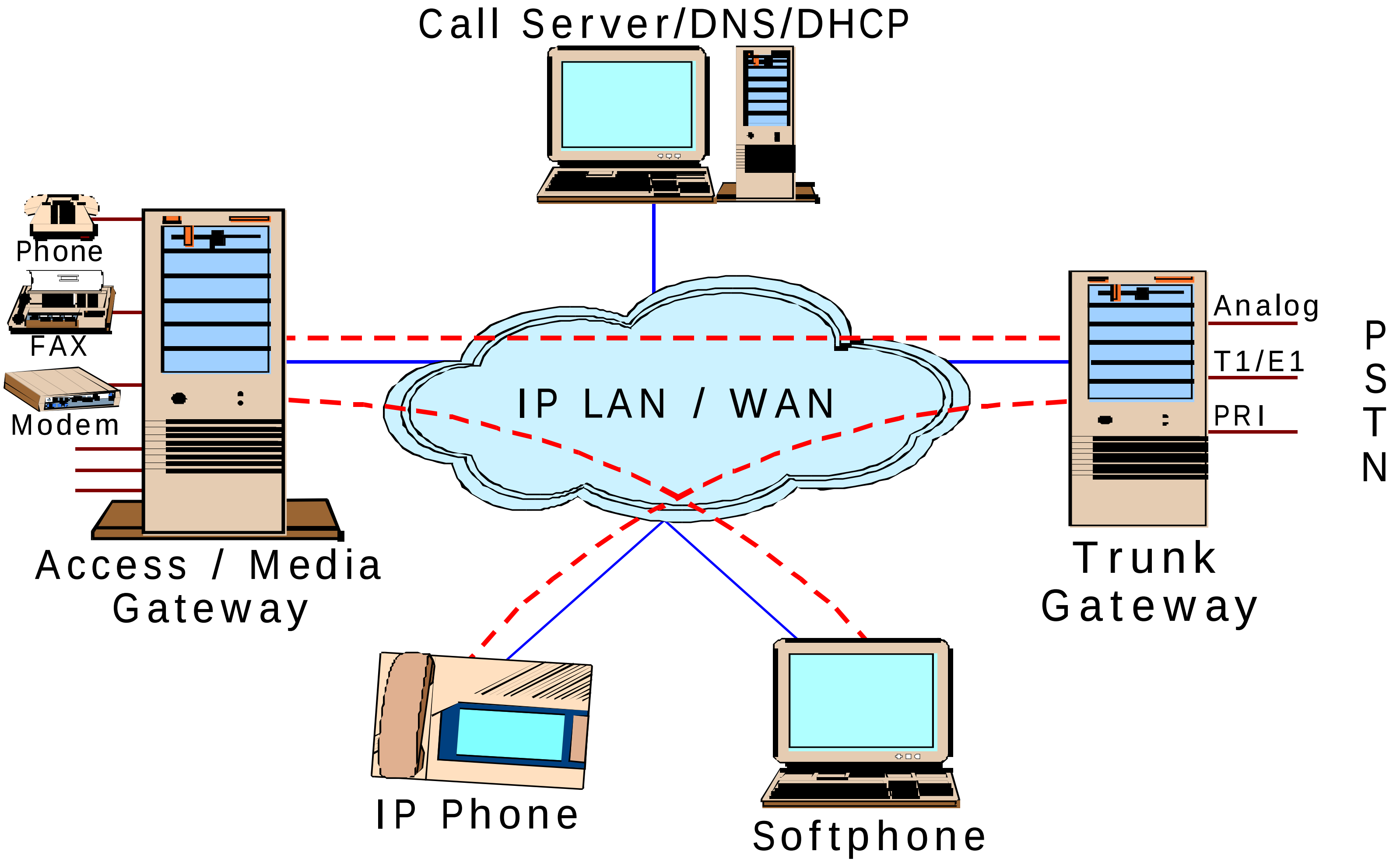
SIP

MGCP
H.248

Gateway

Call Server

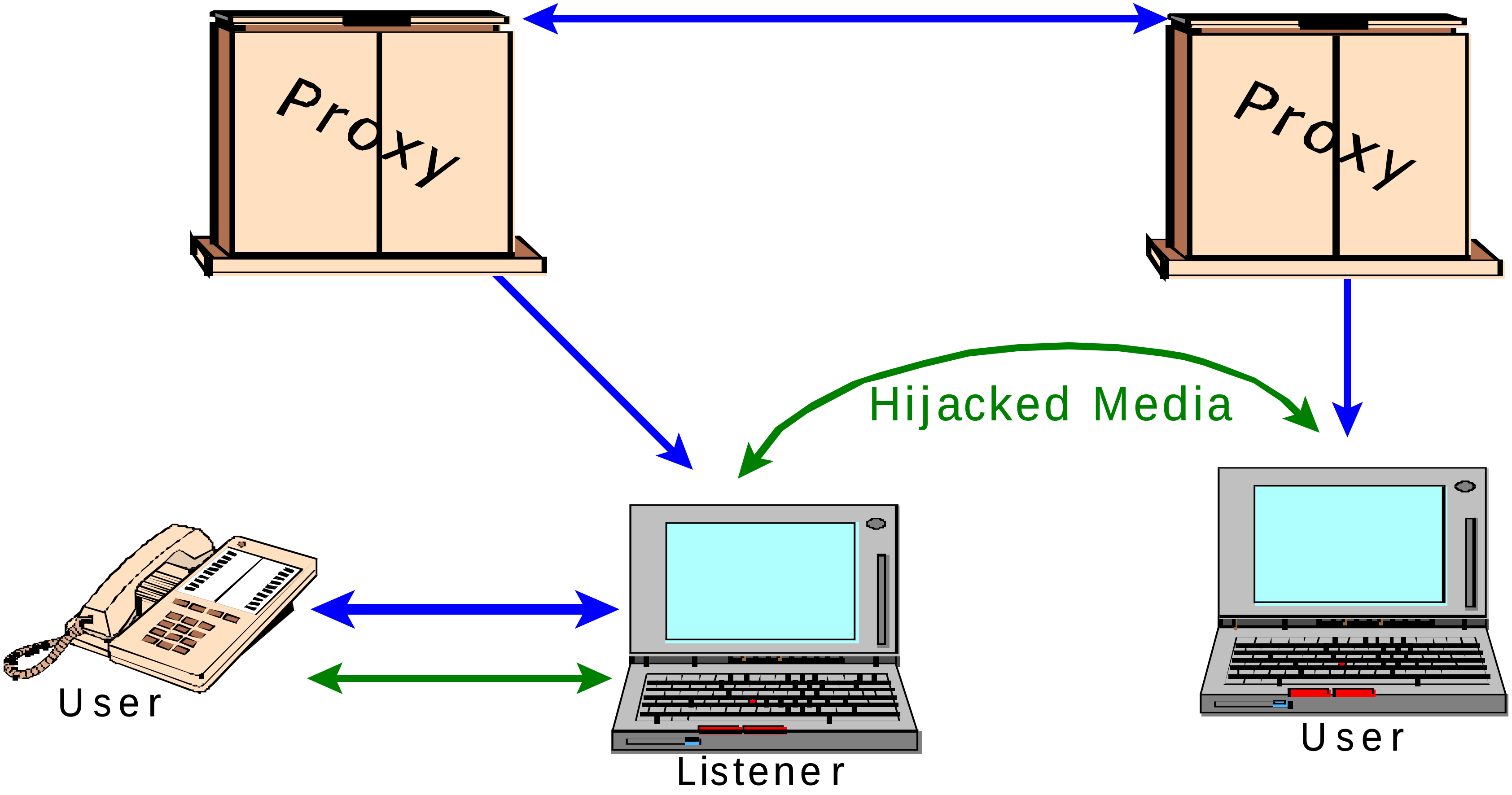
RTP Speech Paths



Call Server Bypass

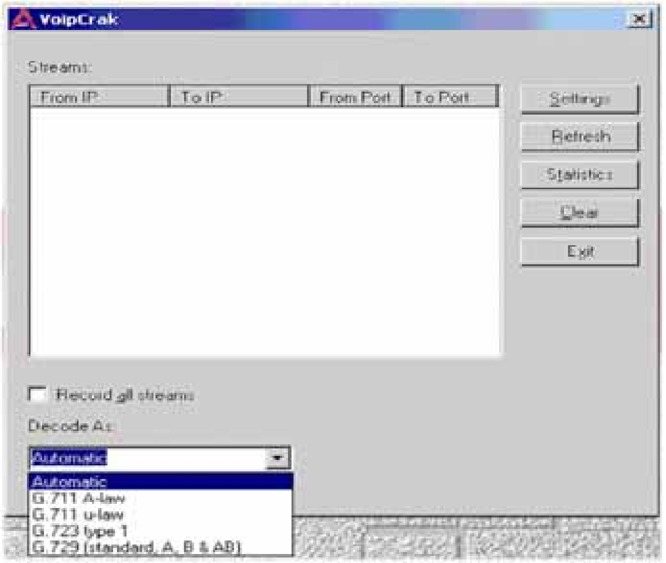
- Internal peer-to-peer (P2P) calls
- External gateway calls billed to enterprise
- Some VoIP/IPT vendors offer P2P calling without server intervention
- Skype is an example

Eavesdropping

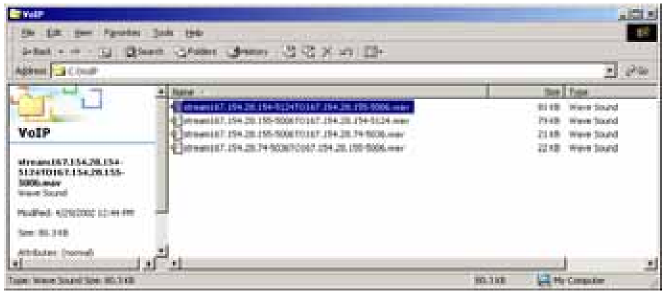


Eavesdropping on RTP Media

- Vomit/VoIPong/Oreka
  - Publicly available
  - Decodes G.711 into .WAV
- VoIPCrack
  - Not public
  - Decodes multiple Codecs



Decode As: Automatic

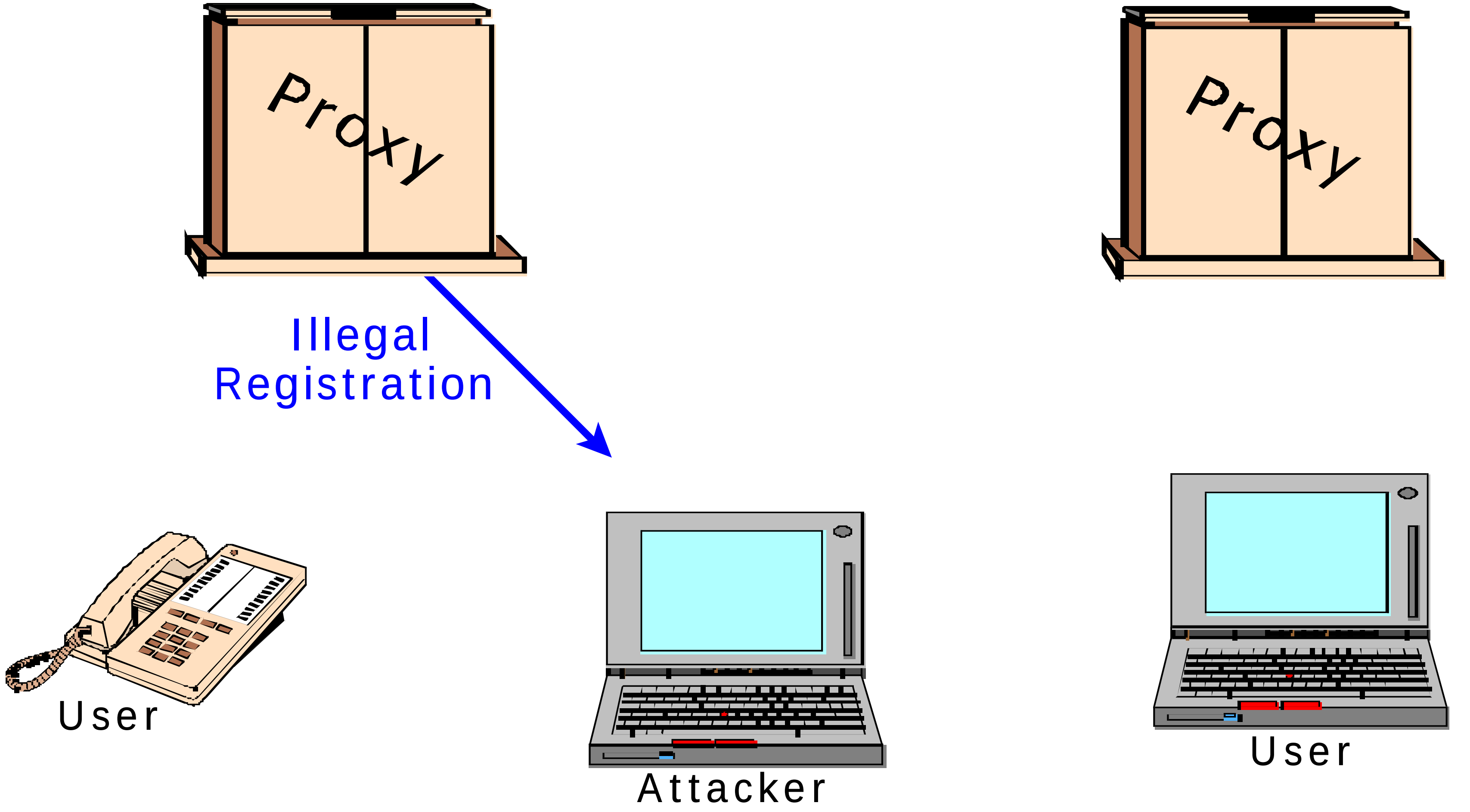

VoIP
File Edit View Favorites Tools Help
Back Search Folders History
Address C:\VoIP
Go
My Computer

Name	Size	Type
stream167.154.28.154-5124TO167.154.28.155-5006.wav	81 KB	Wave Sound
stream167.154.28.155-5006TO167.154.28.154-5124.wav	79 KB	Wave Sound
stream167.154.28.155-5006TO167.154.28.74-5006.wav	21 KB	Wave Sound
stream167.154.28.74-5036TO167.154.28.155-5006.wav	22 KB	Wave Sound

stream167.154.28.154-5124TO167.154.28.155-5006.wav
Wave Sound
Modified: 4/29/2002 12:44 PM
Size: 80.3 KB
Attributes: (normal)

Type: Wave Sound Size: 80.3 KB 80.3 KB

Registration Hijacking



Proxy

Proxy

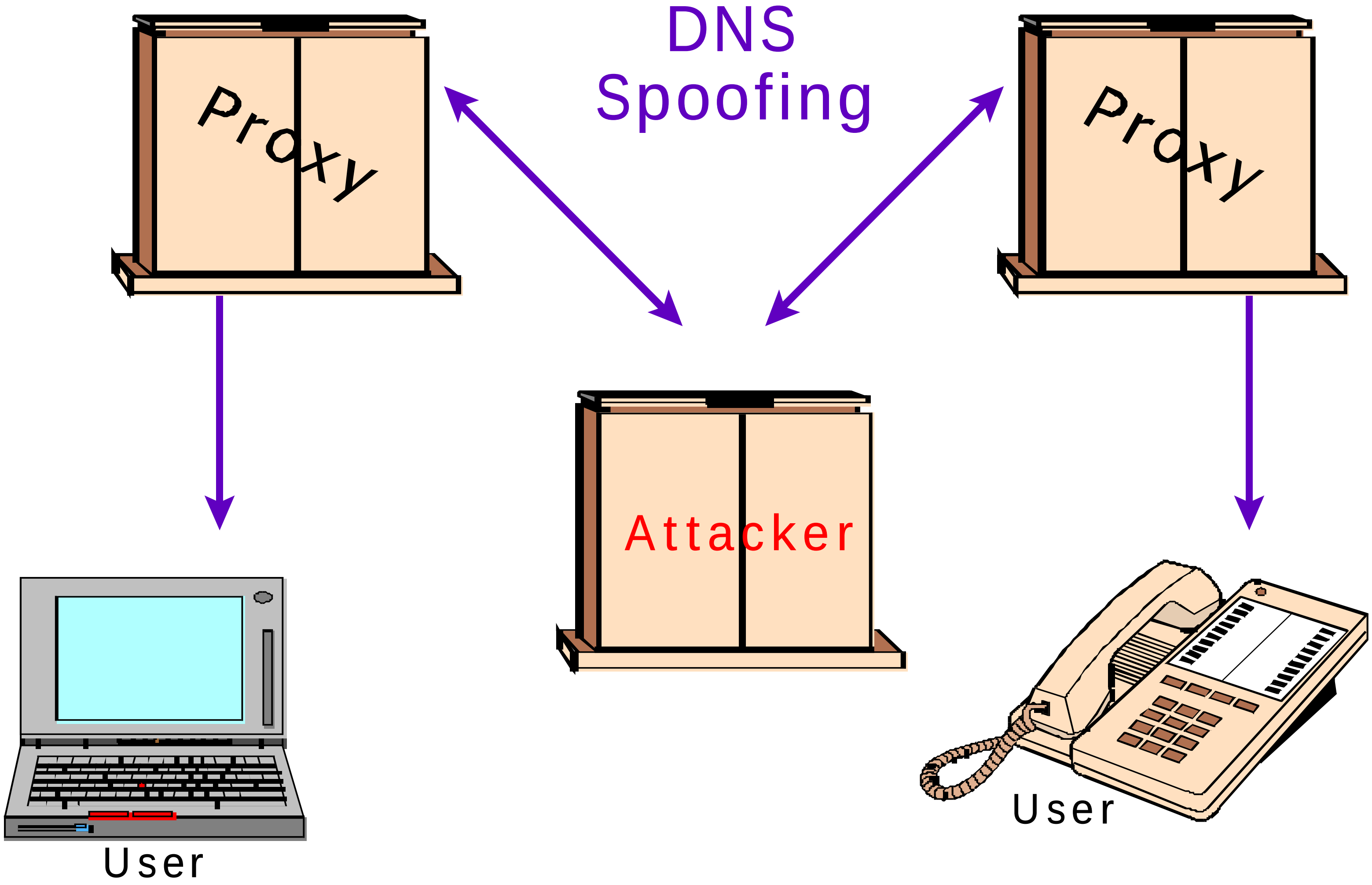
Illegal
Registration

User

Attacker

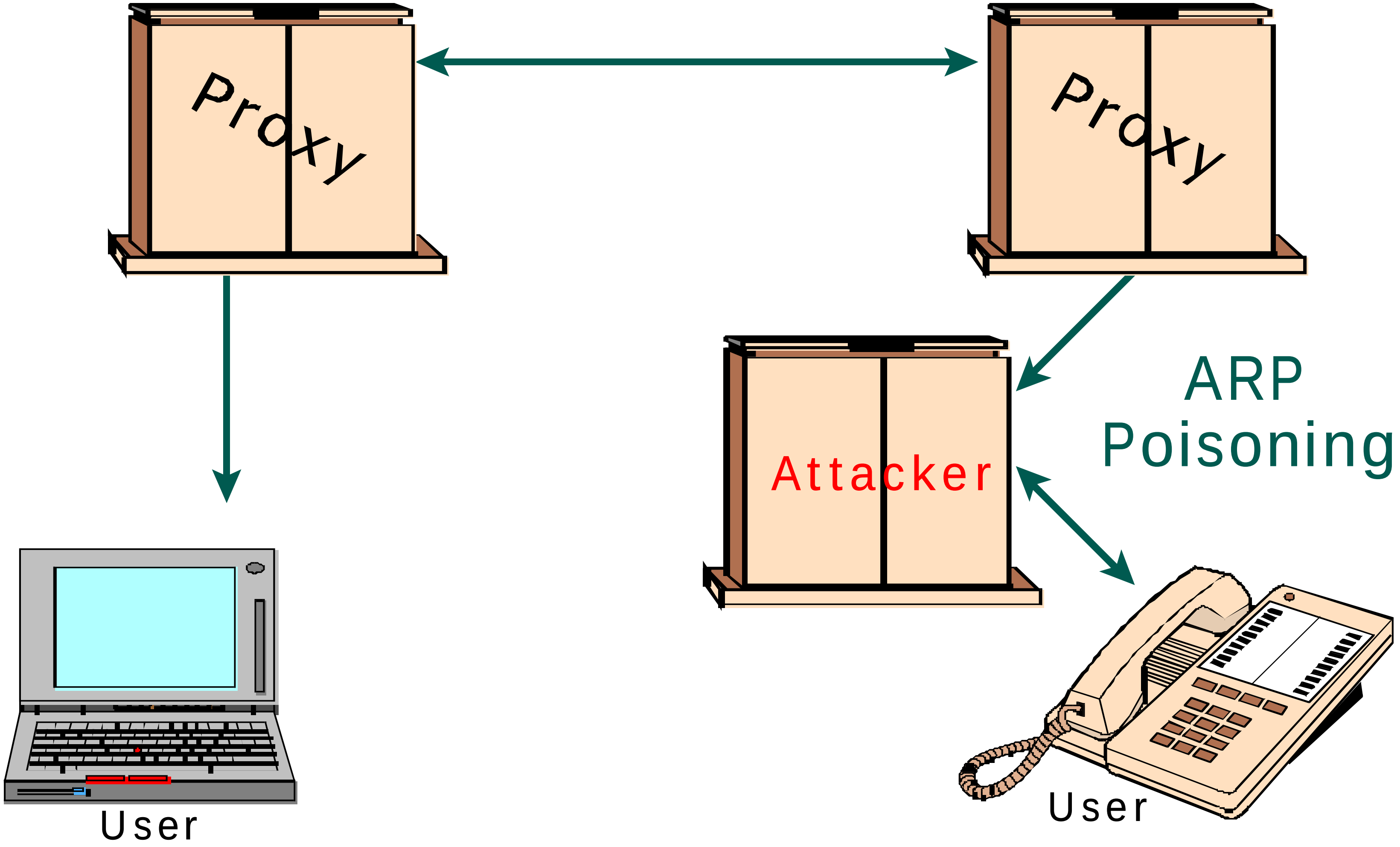
User

Call Server Impersonation (1)



DNS Spoofing

Call Server Impersonation (2)



Proxy

Proxy

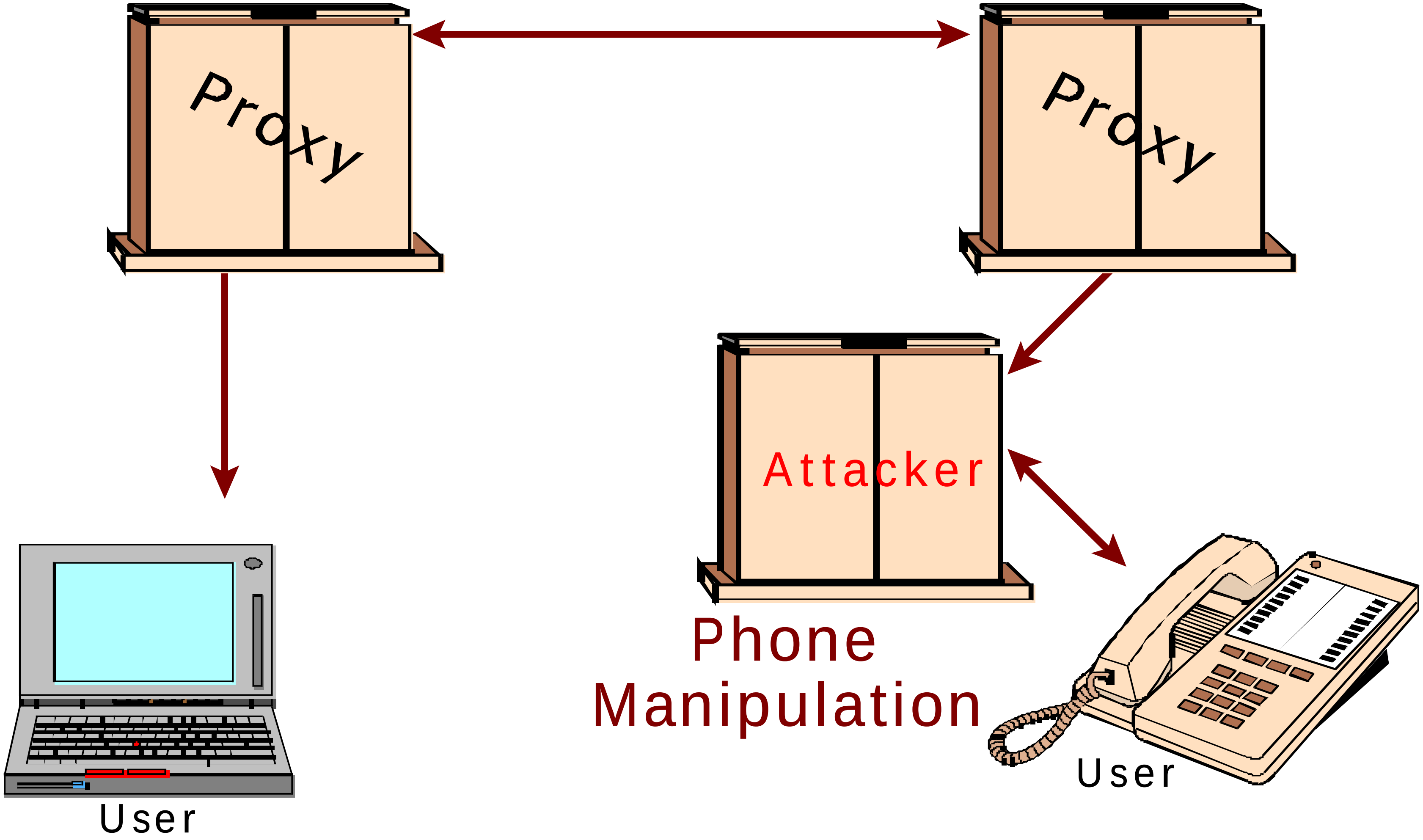
Attacker

ARP Poisoning

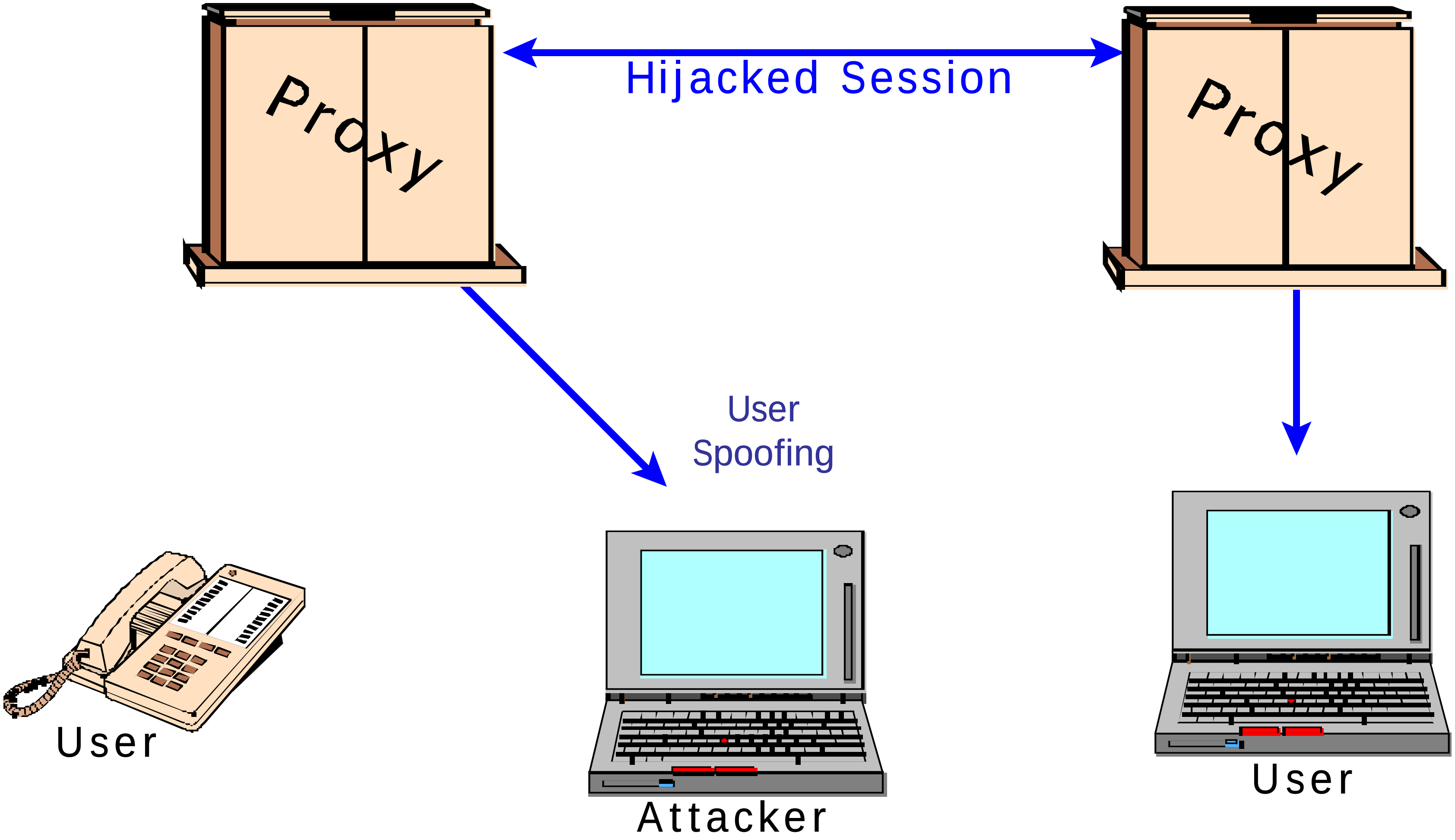
User

User

Call Server Impersonation (3)



Hijacking Session



Proxy

Hijacked Session

Proxy

User
Spoofing

User

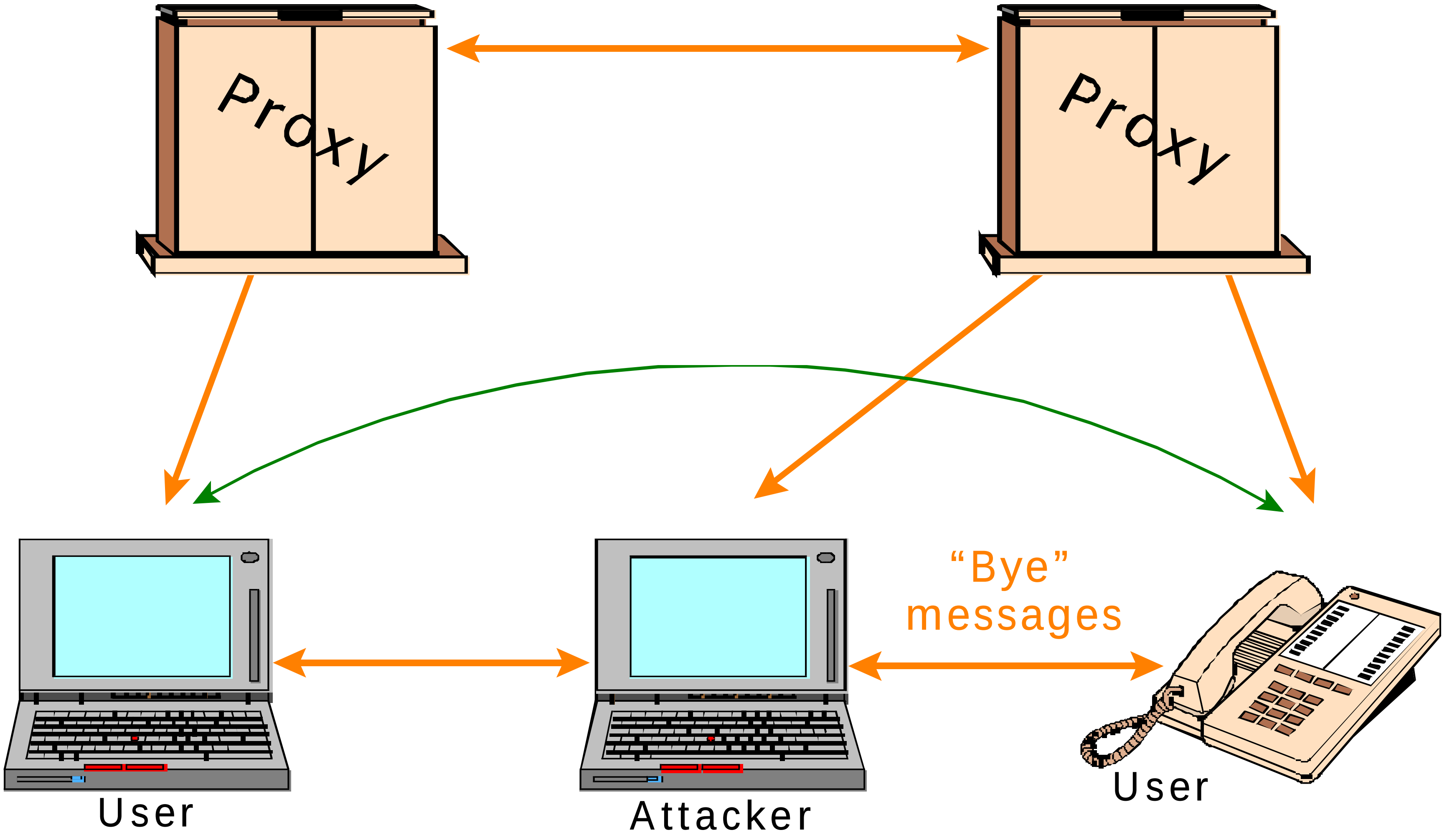
Attacker

User

Directory Tampering

- Call redirect
- Call blocking
- False E911 location information
- DID and DOD redirect

Session Teardown Flood



Function/Feature Tampering

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

Spoofing Caller ID

- Caller ID as an IP address is not verified by routers
- Caller ID is carried in a data field and can be tampered with in transmission
- Caller ID in VoIP may not be valid

Call Redirecting

- Delivering the call to another destination without the knowledge of the caller
- Can be performed by illegal proxy
- Can be implemented in the call server directory
- Modified router table can be used

Coming to an IP Phone Near You

Voice Spam!

SPIT

VoIP Recommendations

- Deploy VoIP-optimized firewalls:
  - Maintain application-level security
  - Interface with existing data firewall
  - Deploy a ‘5 nines’ solution
  - Integrate with TDM firewalls for migration
  - Perform high speed processing of the media
  - Perform protocol-aware NAT
  - Open and close ports for media sessions
  - Inspect media for tunneling/flow/DoS
  - Provide IDP functions
  - Preserve QoS markings

Encryption Considerations

- Key assignment; static vs. dynamic
- Key length (long = delay + strength)
- Per registration or per call
- Processing delay extended
- Does not go through gateways
- Standard or proprietary
- Must be resident in the server, gateway and phone

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/

IP PBX Call Server Reports (from some vendors)

- Locate open/unused trunks and lines
- Observe and report user misuse
- Determine trunk utilization and efficiency
- Monitor and report QoS
- Locate unauthorized modems/faxes
- Detect toll fraud

Hardening a VoIP Operating System

- Select an operating that can be hardened
- Remove all:
  - Utilities
  - Unused drivers and applications
  - Development software
  - Diagnostic software

Call Detail Recording (Ideal)

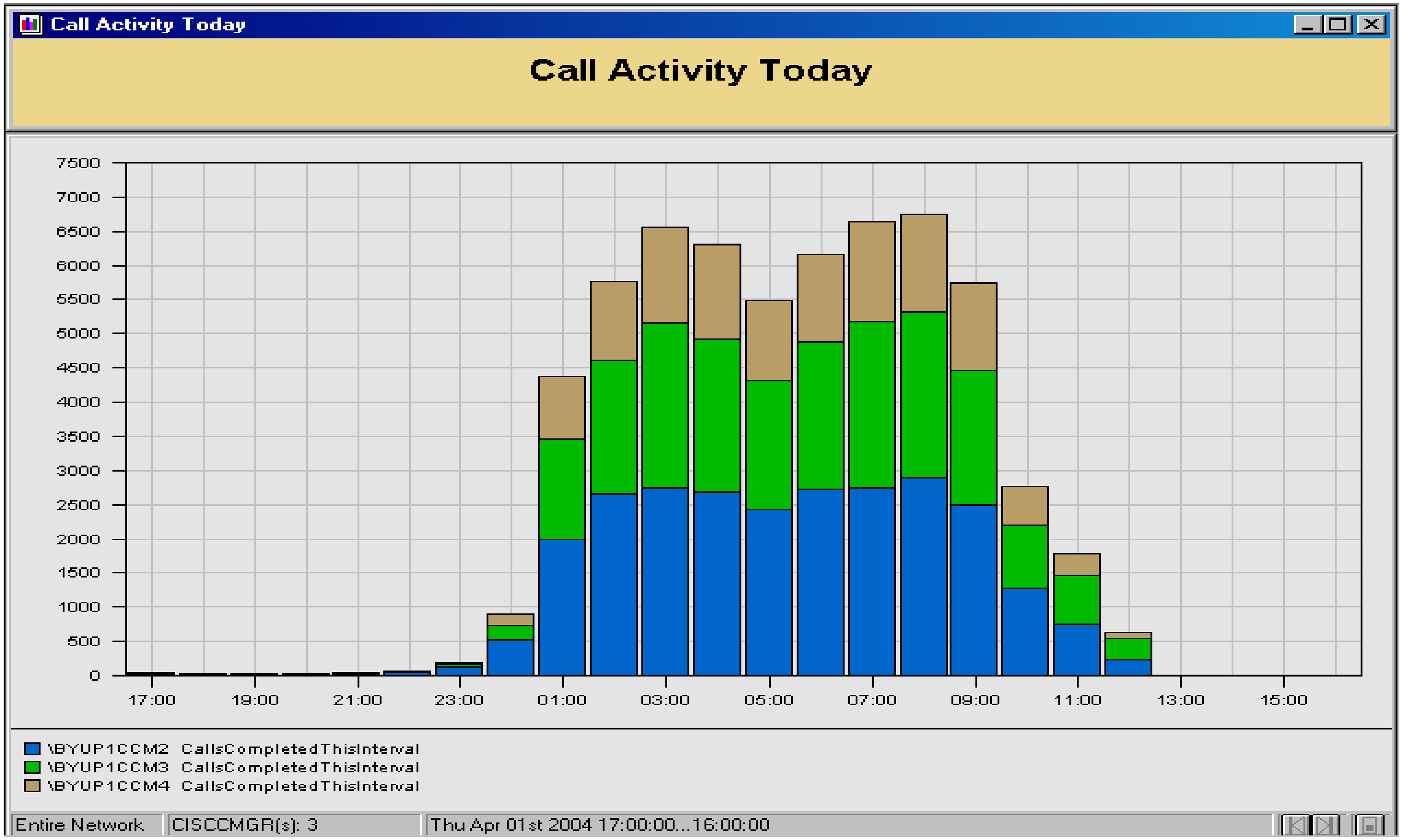
- New Elements
  - RTCP performance per call and per direction
  - Both IP addresses used
  - Both UDP port numbers used
  - Call setup and tear down time
  - Current calls in process
  - Call success rate
  - Average call duration
  - Call Server ID(s) and IP address
  - Error messages (ICMP)
  - Applications used
  - Encryption in use

IP-PBX Call Server Reports for Security

- Locate open/unused trunks and lines
- Observe and report user misuse, abuse and negligence
- Determine trunk utilization and efficiency
- Locate unauthorized modems/faxes
- Detect toll fraud
- Capture unauthorized Internet access

Courtesy of Integrated Research

Call Activity Report



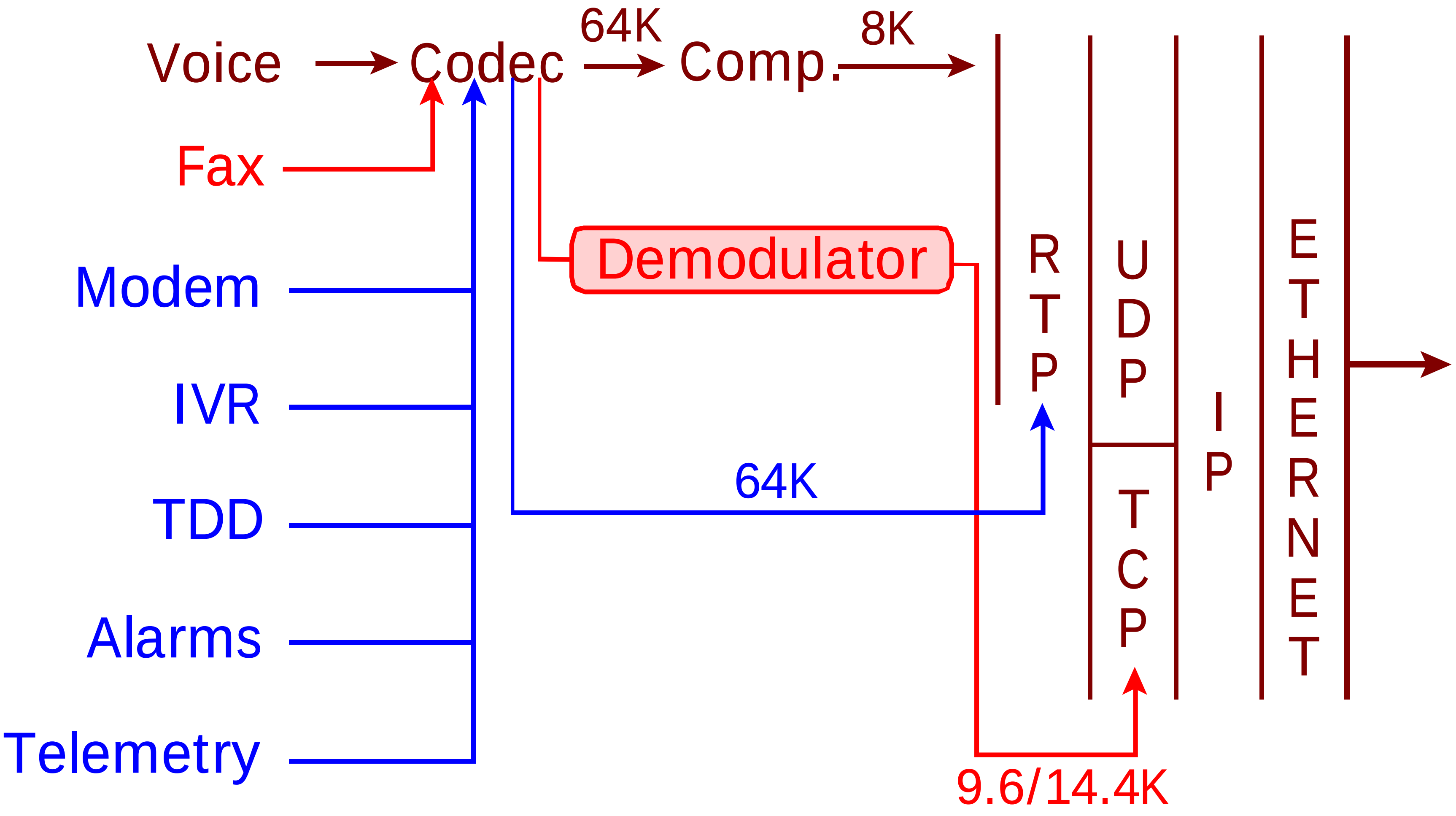
🟦 \BYUP1CCM2 CallsCompletedThisInterval
🟩 \BYUP1CCM3 CallsCompletedThisInterval
🟫 \BYUP1CCM4 CallsCompletedThisInterval

Entire Network | CISCCMGR(s): 3 | Thu Apr 01st 2004 17:00:00...16:00:00

Recommendations for Servers

- Secure Voice Servers:
  - 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 or IDS/IPS

Gateway Connections



Gateway Vulnerabilities

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

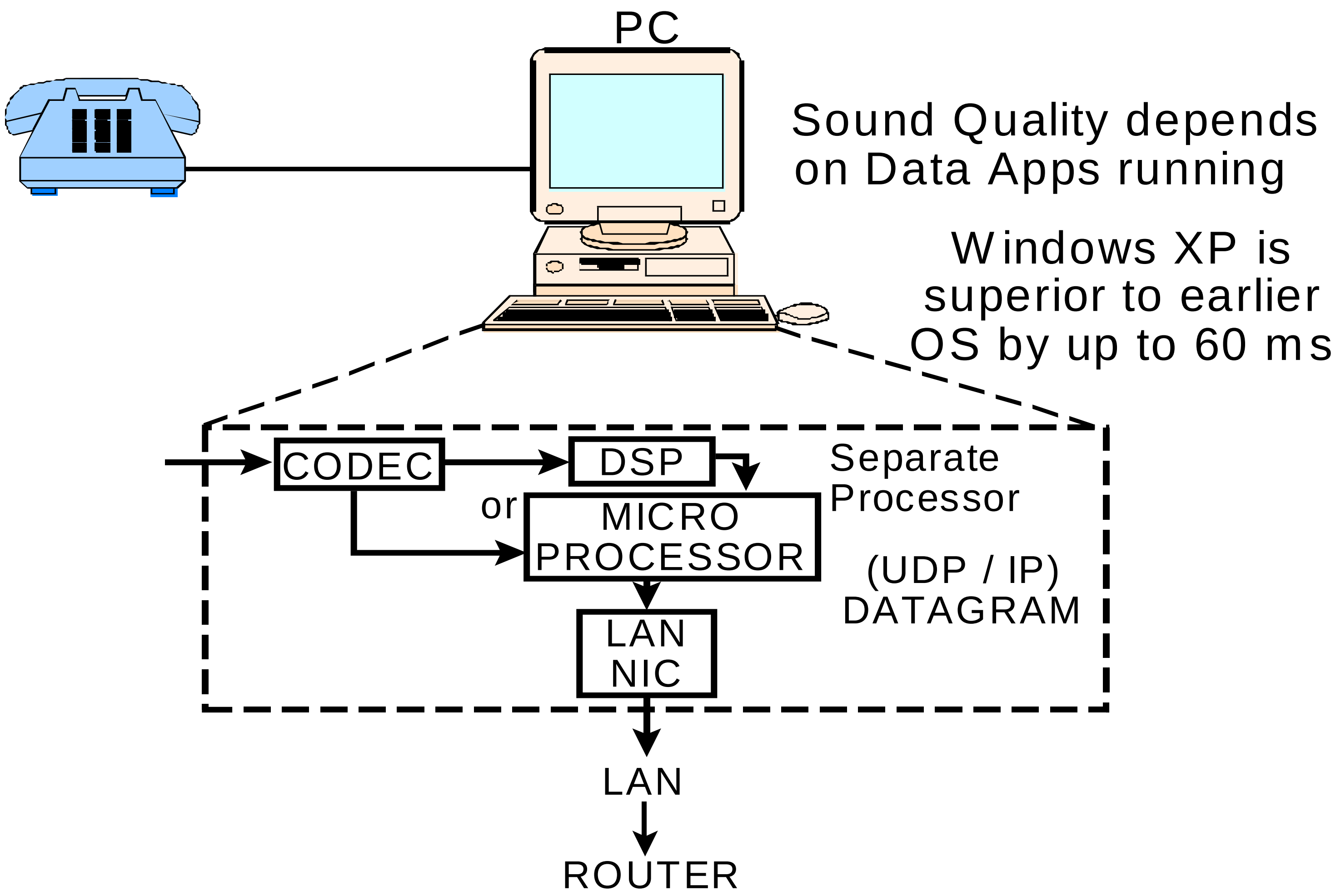
IP Phone Vulnerabilities

- Issues:
  - Rogue “softphones”
  - Implementation attacks (DoS and access)
  - Simplistic remote access attacks
  - Local access attacks
  - Unauthorized firmware/applications
  - Protocol attacks
  - IP phones are cheap and easy to work with
- For examples:
  - See www.sys-security.com

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, if possible.
  - Secure IP softphones

IP Softphone



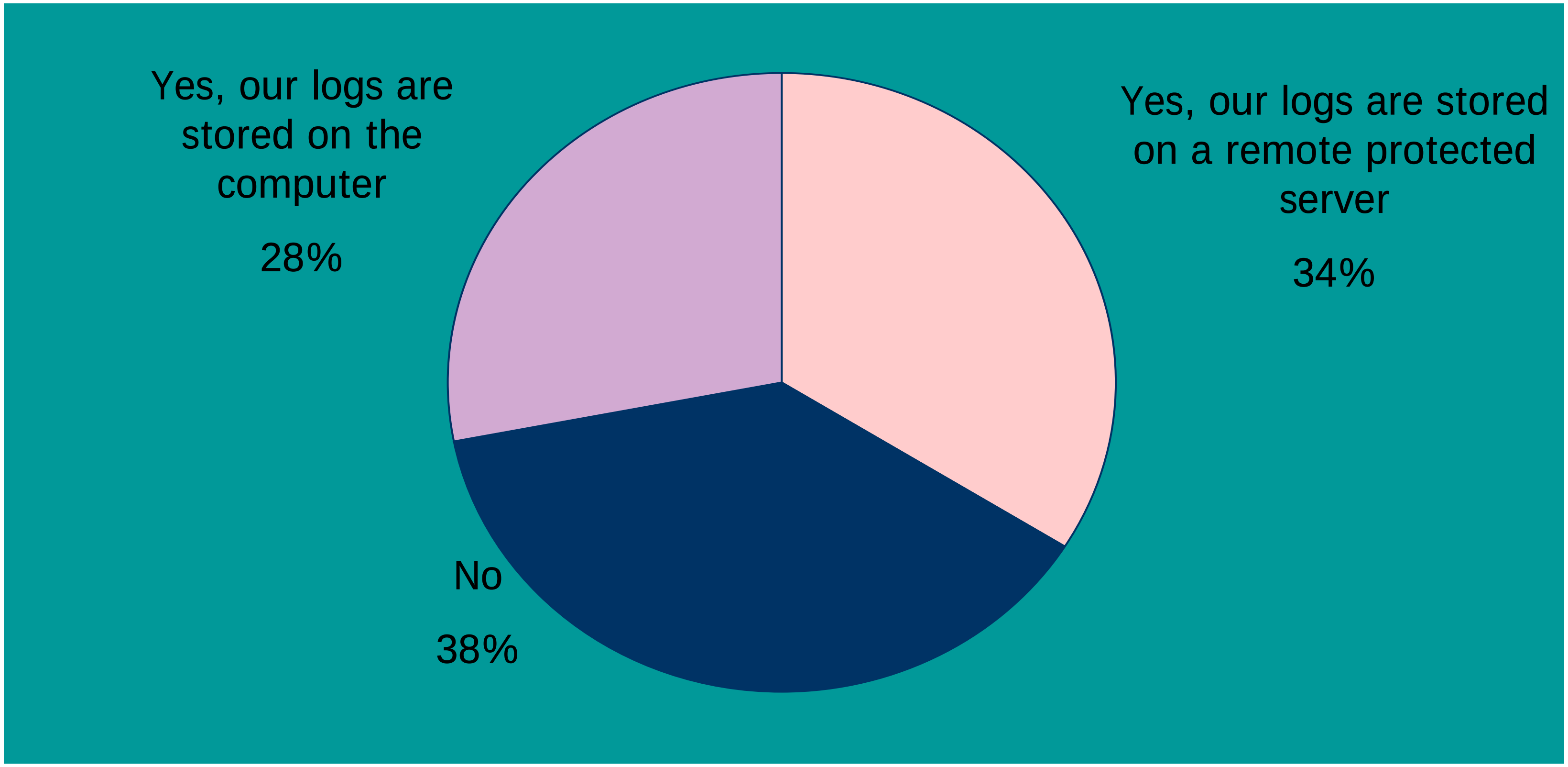
Sound Quality depends on Data Apps running

Windows XP is superior to earlier OS by up to 60 ms

Softphones are PCs

- 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 Gatekeeper for P2P calls (NetMeeting)
- Can spoof other devices

Has Your Organization Activated Computer Security Logging?



Source: 2005 FBI Computer Crime Survey

Vendor Security:

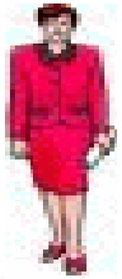
- Encrypted call control
- Endpoint and caller authentication
- RTP/VoIP-stream encryption
- Secure management access
- Documented security policies
- Support for specific security infrastructure environments

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”

Incident Response Team (IRT)



- At least two members who are not friends
- Always involved in planning and design meetings
- Perform vulnerability assessments
- Need to document everything

Incident Response Landscape

- Who owns what?
- What is an incident and how is it counted?
- IRT services and functions
- Proactive, reactive, local, remote support
- On-line or on-site
- IRT report, storage and tracking
- Law enforcement interface
- IRT measurement and security statistics

Network Forensics

- What you collect is what you have to work with.
- Always keep the original raw data on “read only” storage and use a copy for forensics.
- Do not destroy the raw data.
- Have two or more members of the IRT validate the accuracy of the raw data.
- Filter information as you investigate.

Network Recommendations

- Engineer the Network for Security:
  - Build a switched network
  - Make use of VLANs
  - Secure network components
  - Configure perimeter firewalls to block VoIP
  - Limit the number of calls over media gateways
  - Use encryption over untrusted networks
  - Consider the use of firewalls and NIDS
  - Consider the use of encrypting phones

Key Points for Security (1)

- Think security constantly
- There are new VoIP vulnerabilities that are different than data vulnerabilities
- The VoIP security issues deal with the VoIP applications
- There are many new forms of malicious behavior

Key Points for Security (2)

- Securing the IP and softphones is mandatory
- You must enhance LAN security
- VoIP security must be constructed on top of data security
- You need to create an Incident Response Team that understands VoIP

Information Resources

www.voiploop.com - weekly BLOG on communications subjects

www.webtorials.com - 15 articles on VoIP and IP Telephony

www.voipsa.org - VoIP Security Alliance

www.cve.mitre.org and www.nvd.nist.gov for vulnerability lists

Delphi, Inc.

delphi-inc@att.net

- Consulting and analysis firm
- 28 Years as an independent consultant
- Contributor to major publications, such as Business Communications Review and the ACUTA Journal
- Speaker at many user conferences
- International experience with enterprises, vendors, educational institutions and government agencies

QUESTIONS?

Contact:

Gary Audin
delphi-inc@att.net
703 908 0965