IPCOMM2006
September 25-27 • Gaylord Opryland • Nashville, TN

Software Maintenance: Patching and Version Control

Gary Audin
President
Delphi, Inc.

What Will Be Covered

- Managing Software for IP
- Software Procurement
- Patching Defined
- Security Vulnerabilities
- Distributing Software
- Applications with VoIP
- Job Description
- Recommendations

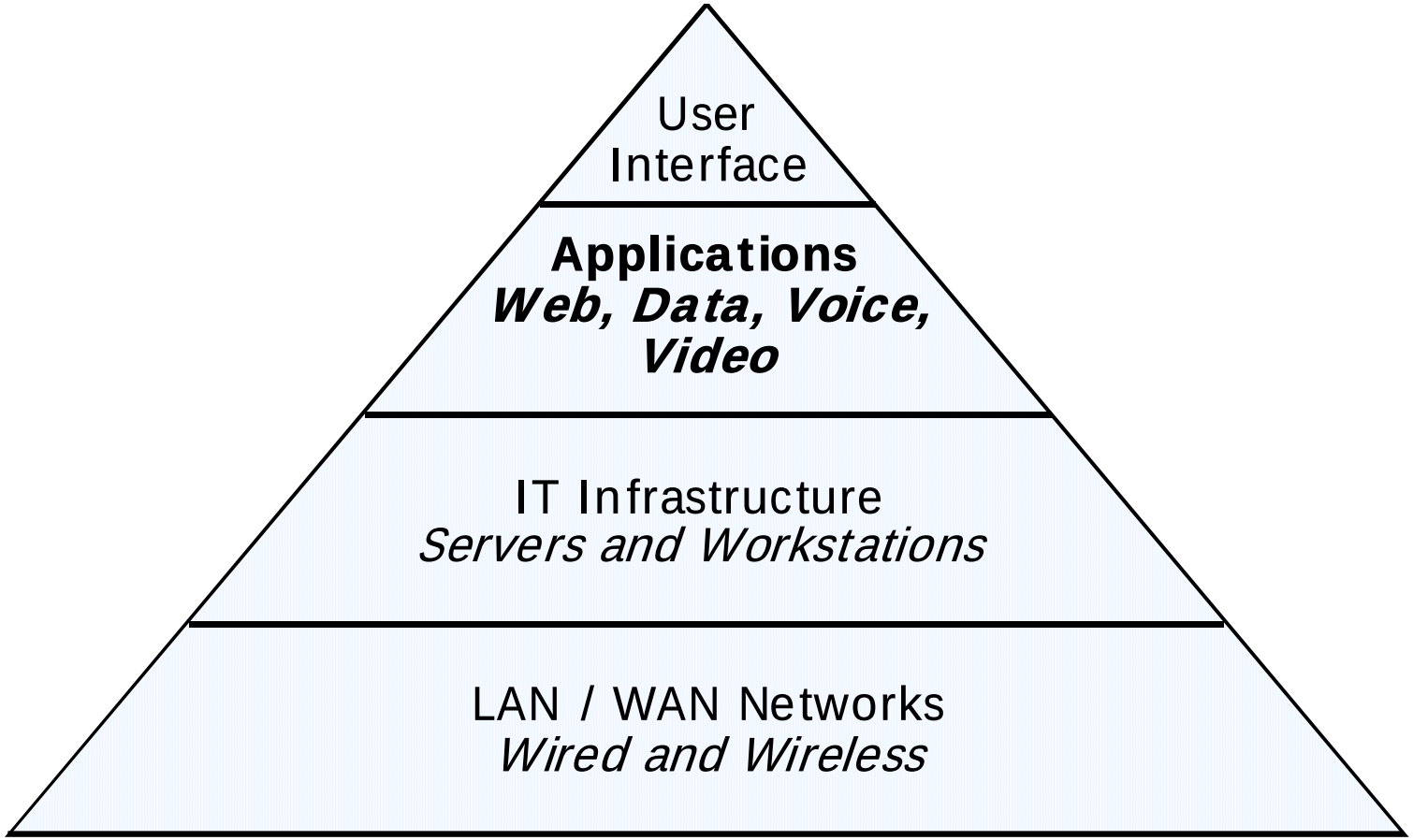
IP-Based Voice Technology

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

Managing Software Resources

- Status (network and devices)
- Configuration (hardware and software)
- Performance and QoS
- Usage and traffic
- Security (network and endpoints)

Convergence Pyramid



Software: Key or Achilles Heel?

- Software is less reliable than hardware.
- Rapid software changes **REDUCE** reliability and security.
- Stability is a goal.
- Old vs. new code: Is it obsolete or mature?

Request for Proposal Outline (1)

- Proposal Introduction
- Bidder Qualifications
- Legal and Insurance Requirements
- Proposal Conditions and Format
- Existing System Description
- *System Requirements (S)*
- *Endpoint Requirements (S)*
- *Maintenance and Support (S)*
- Training and Certification

(S) = software impact

Request for Proposal Outline (2)

- Installation and Cutover
- Optional Elements
- ***Software Licensing and Support (S)***
- ***Security (S)***
- ***Outsource Management and Administration (S)***
- ***Software Administration (S)***
- ***Use of Subcontractors***
- ***Non Disclosure Agreements***

Managing Software

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

Software Definitions

- Make sure you and the vendor agree on these definitions
- Version = A major set of upgrade software. May include new operating system, features, functions, fixes etc.
- Release = A modification to the version and probably includes additions
- Update = Modification to a release (not that common)
- Patch = Usually a problem fix with no new functions however one vendor also defines:
  - Firmware
  - Product improvement
  - Interoperability
  - Customized product improvement paid by customer
  - Diagnostic (to trap a specific event)

Definition of a Patch:

- Also called a *service patch*, is a fix to a program bug. A patch is an actual piece object code that is inserted into (*patched* into) an executable program. Patches typically are available as downloads.
- From www.webopedia.com

The Patching Decision

- Enterprises don't patch enough.
- Enterprises patch too much.
- Viruses infect faster than ever.
- Patches don't always work.
- Enterprises don't test the patches.
- Patches are necessary, but volume is out of control. Vendors avoid publicly stating the number of patches delivered.

Getting the Patch

- Through channel partners (mandatory or optional depends on vendor)
- Customer owned and maintained. Certified staff can access patch library, but may not be able to download (depends on vendor)
- Customer may not be allowed to even view the patch library
- Some patches are downloaded when the device registers to the server automatically

Verifying the Patch

- Do you have a test platform: server, gateway, phone?
- How well did the vendor perform software regression testing?
- Whose operating system patch should you install? Best with IP PBX vendor, not the operating system vendor.
- Vendors have their own security patch list

Common Vulnerabilities and Exposures (CVE)

- A dictionary of publicly known software security issues, 16,520 as of 04/01/06
- Maintained by Mitre for Homeland Security
- As of 04/01/06, there were 274 CVEs on IP Telephony, 33 on VoIP, 23 on SIP, 9 on H.323
- Accessible free at http://cve.mitre.org

National Vulnerability Database

- A list of publicly known software security issues
- Maintained by NIST for Homeland Security. Includes CVE dictionary
- As of 04/01/06, there were 3 on IP Telephony, 34 on VoIP, 42 on SIP, 14 on H.323 with security severity rating
- Accessible free at http://nvd.nist.gov

Distributing Software

- IT departments get 3000 to 4000 patches a year
- One Windows based vendor received 75 operating system patches in one year from Microsoft
- Software changes can come as frequently as every three weeks
- Two devices (servers) with different software may stop communicating with each other
- Outsource the software changes to IT, they do it now for data

Keeping Software Current

- Determine whether the software change is mandatory or optional and for how long (months, a year)
- When is the software no longer supported?
- Can you do a single total change or do you have to enter each piece of software separately?
- Have you budgeted the staff hours and system downtime?

Tips From the Patchmaster (1)

- First step is to understand the patch files, functions and operation
- The patch should be tested in a simulated environment. If successful, then deploy the patch but be sure you can remove the patch if there is a problem.
- Change control is important during the pre-testing and deployment preparation

IP PBX Software Trends

- LINUX use is growing (Cisco's move)
- SIP signaling is spreading
- Performance is good and getting better
- Availability is improving 99.9% to 99.99%
- Security features and functions have been bolstered but still need work

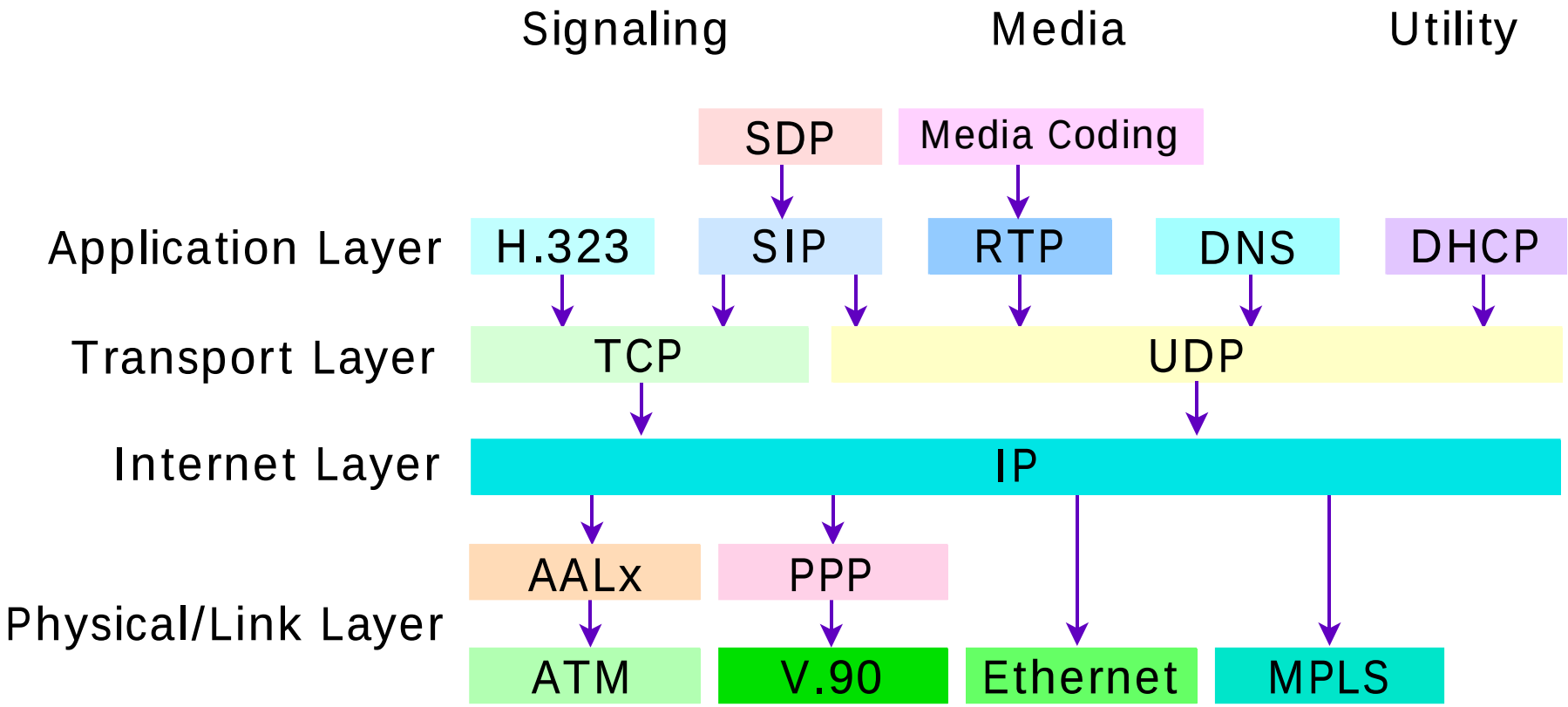
Reference: BCR, "High-End IP-PBXs", January 2006

Tips From the Patchmaster (2)

- Hotfixes can be chained, that is several hotfixes can be installed without a reboot.
- Even if the patch fixes an application with no known exploit, install it within 48 hours.
- Insure deployed patches are:
  - Consistent
  - Have status tracking
  - Have error logging

Software Stack

Applications

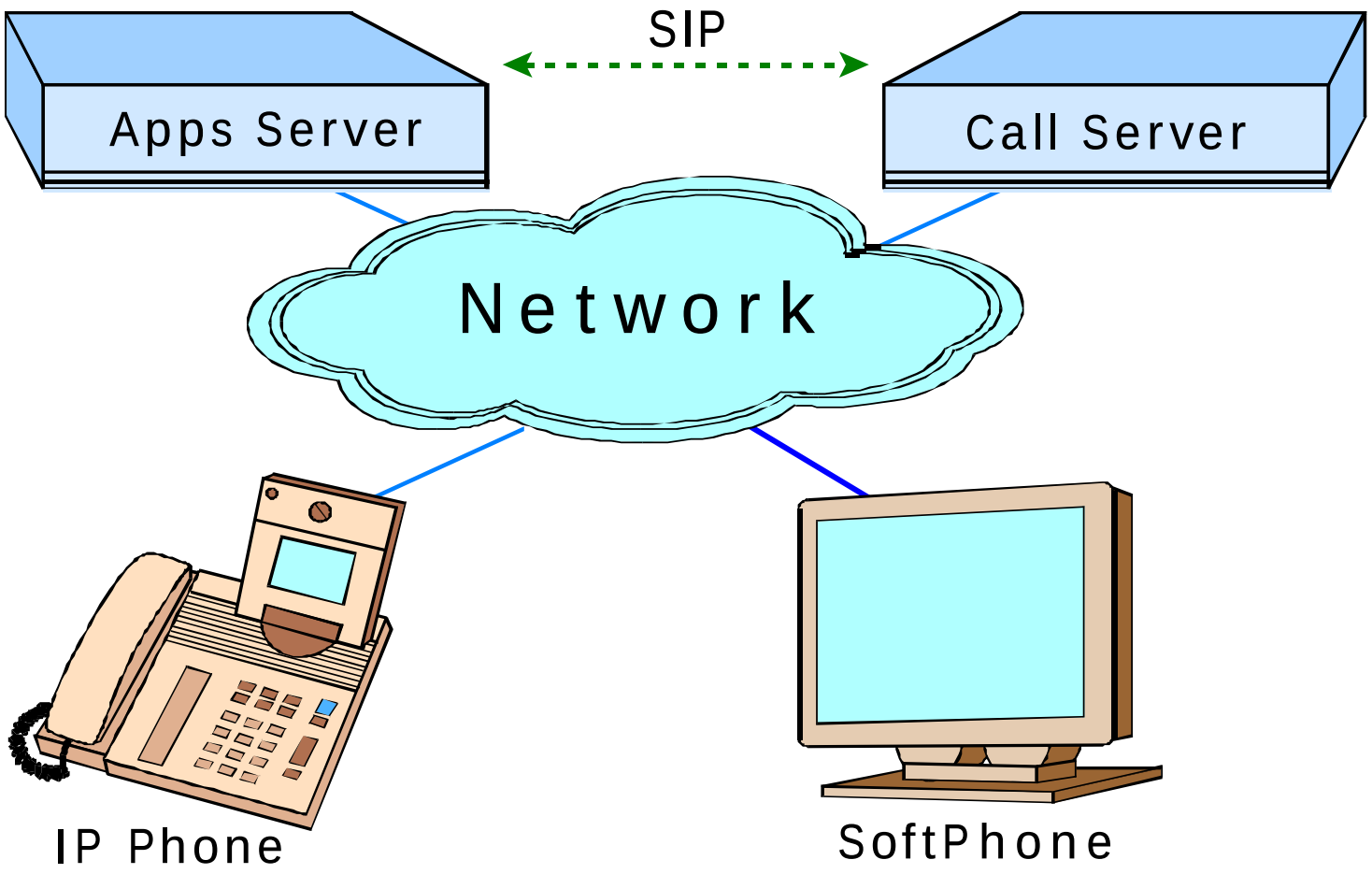


- Secure SIP and RTP

Calling Configurations

- Keep the software in all devices coordinated
- SIP, H.323, proprietary signaling
- Phone to phone (peer-to-peer)
- With one call server
- With multiple call servers
- What configurations are allowed?

Application Residence

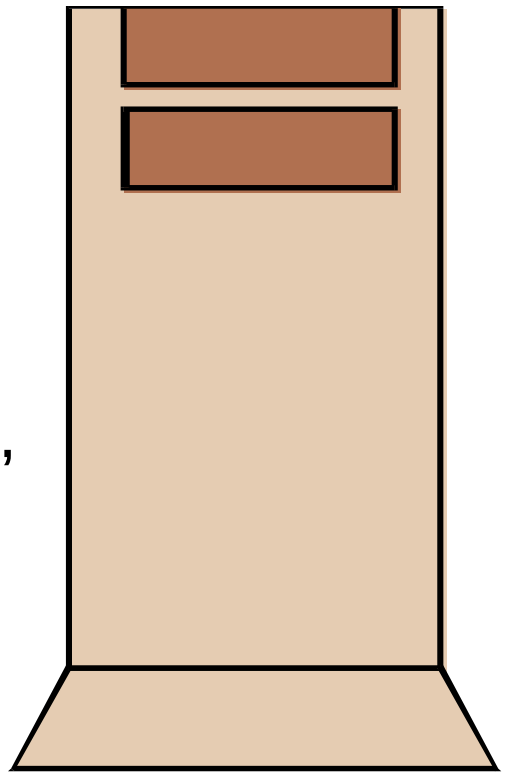


Applications on Top of VoIP

- Common functions and features of a PBX are not the applications that will be used to justify an IP PBX
- IP PBX vendors are offering new features like Presence and call center functions under the user's control
- New applications will be server based and will probably reside outside the call server
- New applications will probably be produced by third-party software vendors and enterprise organizations
- Applications will be specific to vertical markets

Microsoft LCS
(Office Communicator)

- Instant messaging
- Buddy list
- Collaboration
- Outlook address books
- Interface with Outlook, WORD, PowerPoint, Excel, SharePoint, OneNote
- Built on desktop / laptop



Compliance Issues

- Once VoIP/IPT devices can access IT data servers, then multiple regulations will apply
- Sarbanes-Oxley for public enterprises and some not-for-profit
- HIPAA and Graham-Leach
- VoIP/IPT systems and networks will be audited

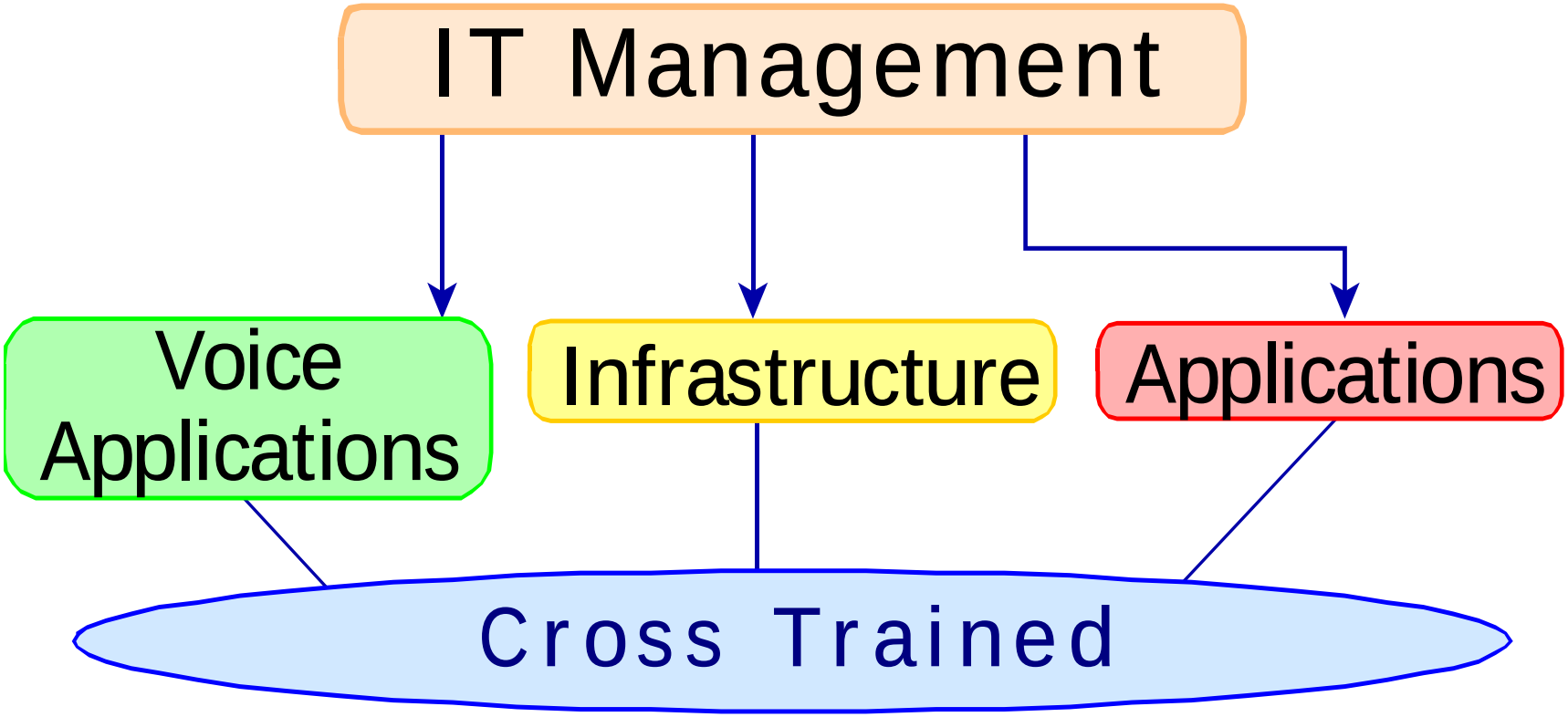
Third-Party Vendors

- Applications working with or on top of LCS
- LCS connection via SIP/SIMPLE and XMPP (Extensible Messaging and Presence Control) - Jabber
- Specific to vertical markets
- Competitors may also provide interfaces

The Software Licensing Scene

- Endpoint (phone, gateway) or user licensing
- Trunk license
- System licensing for the box software
- Seat licensing for messaging, ACD
- Right to use (RTU) licensing for features, functions — survivability, protocols, applications

True Staff Convergence



Certifications

- Applications
- Operating systems
- Infrastructure
- IP Telephony
- Costly to educate, who pays
- Higher salaries, 10% to 30%
- Usually vendor specific

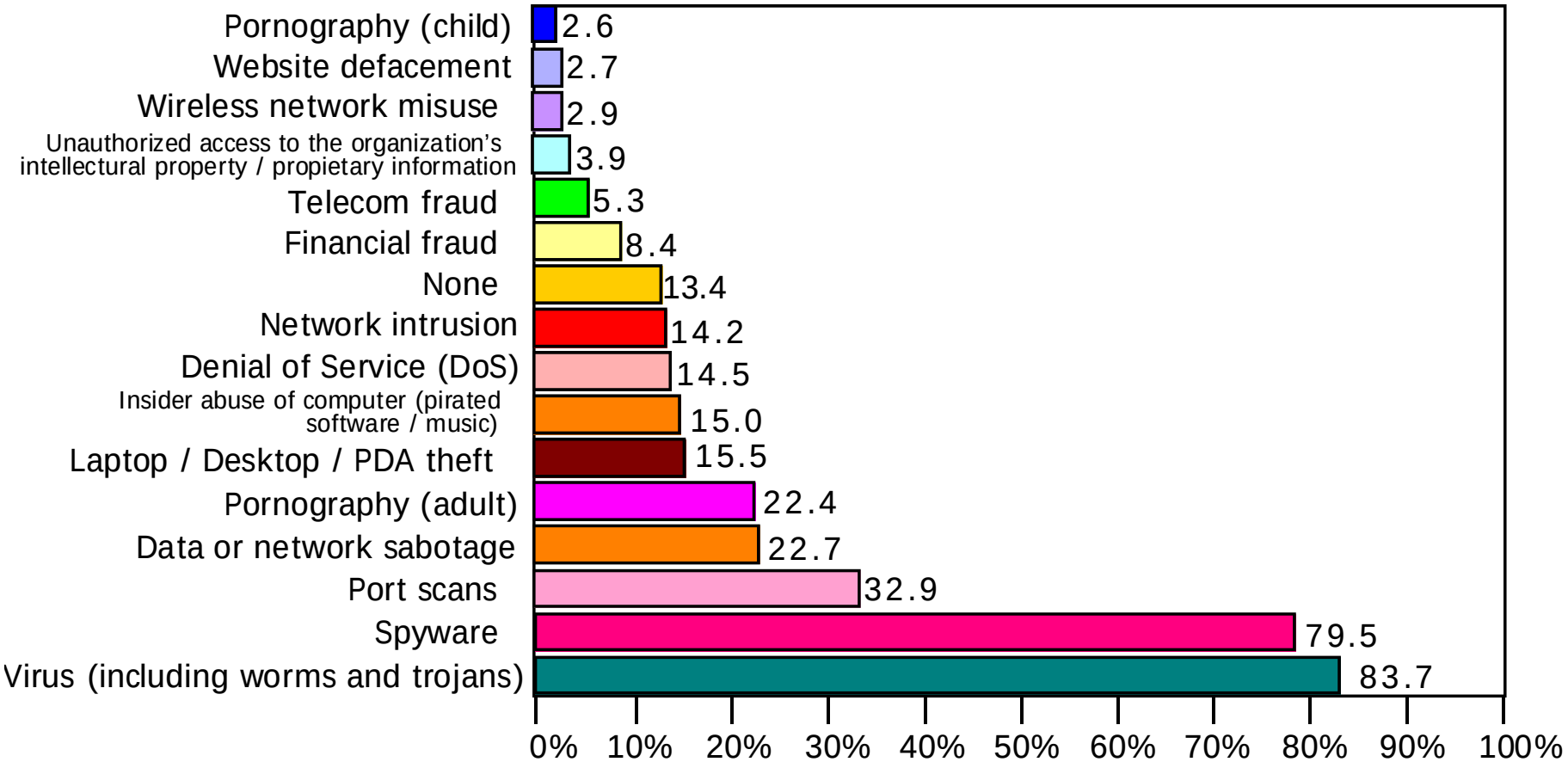
Voice Application Specialist (1)

- Manage all servers (call, **V-mail**, apps)
- Manage call center (ACD, CTI, VRU)
- ***Support hard IP phones***
- ***Support softphones***
- ***Provide all PBX features and functions***
- ***Support VoIP gateways***

Voice Application Specialist (2)

- ***Produce and manage VXML and SALT enabled applications***
- ***Call quality monitoring and reporting***
- ***Support extension mobility and hoteling***
- ***Integrate application servers (Microsoft LCS, IBM and….)***

Types of Computer Security Incidents



Source: 2005 FBI Computer Crime Survey

Hardening a VoIP Operating System

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

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

Security Recommendations (1)

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

Security Recommendations (2)

- 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 encrypting phones

Safe Softphones

- As vulnerable as any desktop 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

Key Points to Take Home

- Software is constantly changing
- The VoIP/IPT customer has all the problems that IT has had for years
- Don’t assume a patch works
- Set up a patching control and installation procedure and adhere to the procedure
- Define the right job description
- You will be patching servers, gateways, IP phones and applications

IPCOMM2006
September 25-27 • Gaylord Opryland • Nashville, TN

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

IPCOMM2006
September 26-27 • Gaylord Opryland • Nashville, TN

QUESTIONS?

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