

The Role of Security in Achieving Five Nines for VOIP



George Sullivan, CTO, Avaya Global Managed Services

IP Telephony

Contact Centers

Mobility

Services

Session Abstract

Assertions

- VoIP applications require more advanced network services than regular data applications
- Voice applications require a secured network environment to ensure a level of availability that satisfies the familiar "five nines" telephony performance metric

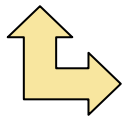
Responses

- This session will describe
 - New product, service and architectural best practices that can better protect IP telephony systems against threats
 - What is required to assure that VoIP satisfies critical infrastructure criteria

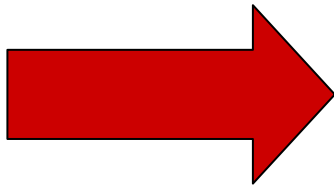
What does “Five Nines” refer to?

- A measure of availability (a system capable of delivering the services expected from it) or UPTIME
- Looking at the converse – how much un-availability (DOWNTIME) illustrates:

$$(1 - \underline{0.99999}) \times 365 \text{ days} \times 24 \text{ hrs/day} \times 60 \text{ min/hr} =$$



Note the 5 nines here



5.256 minutes of
DOWNTIME in a year

We are talking Business Communications

Communications for **competitive advantage**. An underused means for superior execution and deeper customer relationships by making

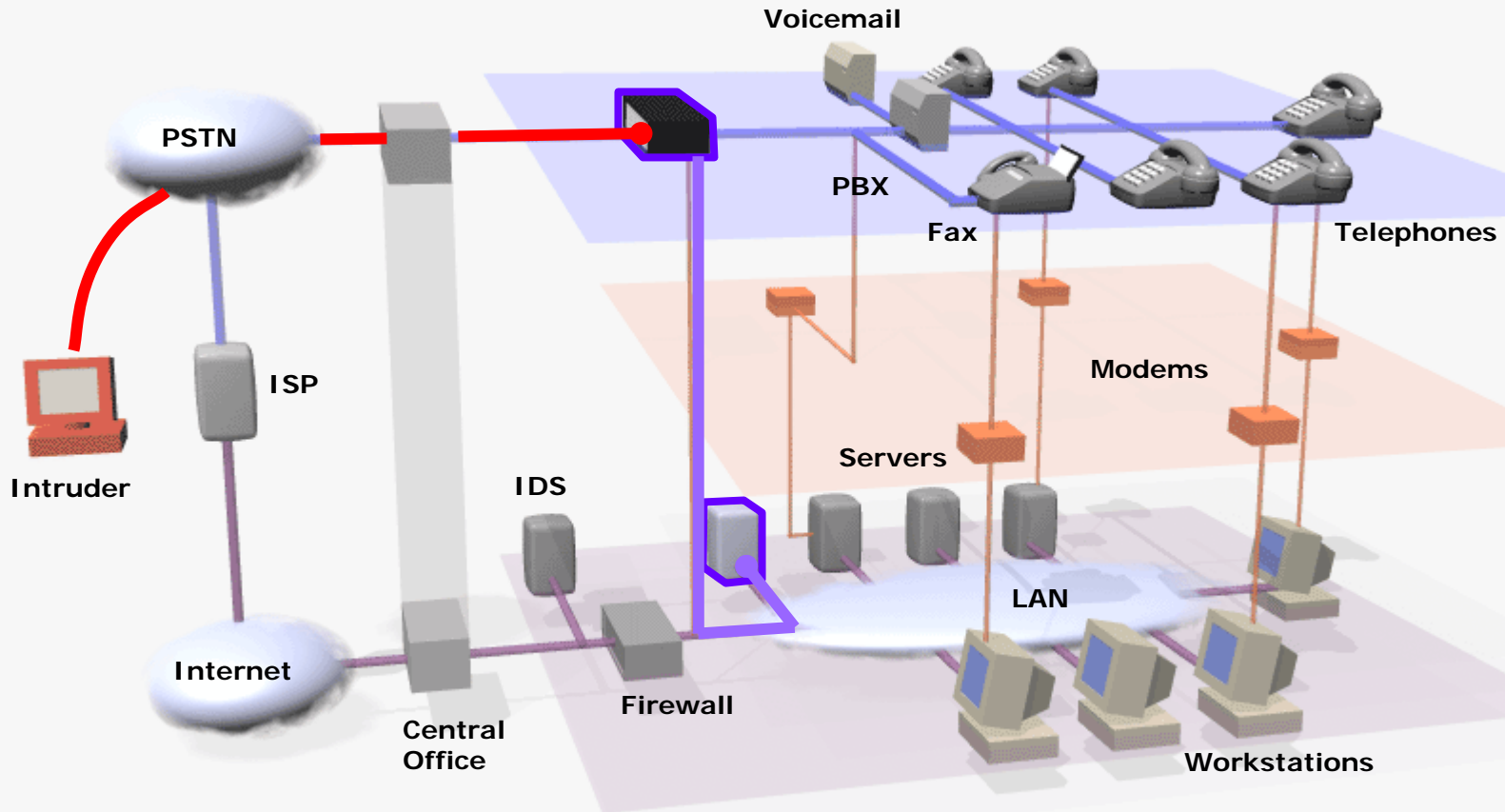
- ... **people** more **productive**
- ... **processes** more **intelligent**
- ... **customers** more **satisfied**

Achieved by deeply embedding best-in-breed communications technology into the fabric of the enterprise, using software, services and systems that layer seamlessly on any network

Converged Networks: the Basis for Business Communications

**Converged networks
result from design and implementation
of a common networking infrastructure
that accommodates data, voice and
multimedia communications.**

Converged Networks – is this it?



Is this your network? Have you checked?

If It's Converging - Then It Must Be Good



- **Convergence is that fantastic state brought to you by purveyors of The Next Big Thing (including Avaya)**
 - Seems to be part of the new technology marketing playbook
 - Beyond the marketing hype, real breakthroughs may exist

- **But what exactly is converging? Examples:**
 - Voice, video, and data services (circuit/packet convergence)
 - Phones, cameras, PDAs, GPS devices and other gadgets
 - Computers and business or consumer electronics
 - Collaboration, workflow, messaging (email and instant messaging), telecom systems and business applications

Converged Networks: The Promise

- **We may actually lower costs after all**
- **Simplified network infrastructure (potentially)**
- **Rapid Feature/Application deployment**
- **IP Telephony utilizes the Internet architecture, similar to the World Wide Web**
 - **Intelligent clients utilizing services within the network**
- **Applications and Services can be distributed throughout the network**
 - **With intelligence in the clients or in the application on the network <- New Security Implications**

Converged Networking Requirements

A successful deployment of VoIP means addressing infrastructure and management issues **BEFORE** implementation

Performance must be guaranteed

Availability must be guaranteed

A New and Blurry World

- Facts
- Access to network services is now more important than ever
- The network perimeter is becoming impossible to define
- Intranets, extranets, VPNs, & other Remote Access Services (RAS) blur the definition of a trusted internal user
- Critical corporate data may be located on handhelds, laptops, thumbdrives, phones – anywhere...
- Network/application/human weaknesses *will* be exploited

Common Concerns from Customers about Security for Converged Networks

- Confidentiality of voice conversations
- Call interception and eavesdropping
- Invasion of data privacy and integrity through signal protocol tampering
- Spoofing or presence theft
- Theft of service and toll fraud
- Call quality and integrity
- Availability of services
- Compliance issues with International, Federal and State privacy/security regulations
- New vector for the delivery of malicious information

Converged Networks = Old Risks + New Issues/Threats

Old Risks

- All of IP protocol's security weaknesses are inherited
 - Sniffing
 - Spoofing
 - Denial of service
 - Replay attacks
 - Message integrity, etc.
- Legacy application servers
- Well-known operating systems

Plus

New Issues/Threats

- Unique performance requirements
 - Speed
 - Availability
- Increased network points of access
- Increased network complexity
- Concerns about application maturity
- Reversal of traditional security model
 - Intelligence is moved to the edge

Threats and Fears

- VoIP technology can be abused to introduce security and availability issues
 - Delay/Latency
 - Jitter
 - Packet Loss
 - Speech Coding techniques
 - Network Availability
 - Managing Access and Prioritizing Traffic
- Intercept/hijack your IP-based telephony traffic
- Hack your voicemail system or IVR
- Use your customer network/servers to attack other sites (port scanners can be installed on HP printers now (www.phenoelit.de)). Why not an IP phone?

Devices at Risk

● New

- IP Endpoints (IP phones, softphones, etc)
- Media Gateways
- Media Controllers
- SIP proxies
- Gatekeepers
- Location Servers
- VoIP Firewalls
- “Communication Enabled” Applications and Servers

● Old (but related)

- Routers
- Switches
- Servers (DNS, DHCP, TFTP, DBMS, Email, Directory, etc.)

Converged Networks: Applications

- Voice over IP (VoIP) or better ... IP Telephony
- Customer Relationship Management (CRM)
- Unified Messaging
- Distance Learning
- 802.11a/b Wireless
- Collaborative Video
- Time-critical applications like process control, services delivery and supply chain management
- What application cannot converge?

A Plethora of Protocols for VoIP/IP Telephony

- **Signaling Protocols:**
Protocols in which Establish, Locate, Setup, Modify and Teardown sessions
- **Media Transport Protocols:**
Protocols which transmit the voice samples
- **Supporting Protocols:**
DNS, Location Servers, QoS, Routing Protocols, AAA...

Protocol Breakdown

- Signaling
 - SIP
 - H.323
- Media Transport
 - RTP & RTCP
 - SCTP
- Supporting Protocols
 - Routing - TRIP (Telephony Routing over IP)
 - Quality of Service – RSVP, 802.1q
 - DNS, tftp, SNMP, etc

Signaling Protocols

● SIP

- A signaling protocol for Internet conferencing, telephony, presence, events notification and instant messaging.
- Based on HTTP
- Native support in Windows XP
- IETF

● H.323

- A signaling protocol for Internet conferencing, telephony, presence, events notification and instant messaging.
- Based on SS7
- ITU

Comparable features – but not interoperable
H.323 is the market leader, but SIP is gaining

Transport & Supporting Protocols

- **RTP:** Real Time Transfer Protocol to packetize various media streams, such as voice, text, video,
- **RTP/AVP:** Real Time Transfer Protocol Audio Video Profiles,
- **RTSP:** Real Time Streaming Protocol for media play-out control,
- **RSVP:** Resource Reservation Protocol
- **SDP:** Session Description Protocol to convey the parameters for a session,
- **TRIP:** for routing IP calls to desired gateways to the PSTN,
- **SMIL:** Synchronized Multimedia Integration Language to insert other media such as text, graphics and URLs in audio/video streams for synchronized display,
- **SOAP:** XML over SIP, A system for making requests for different services,
- Protocols for Presence and Instant Messaging are in the IETF standards process
- Many more in progress

Transport & Supporting Protocols

Many new protocols have
been proposed

Hackers love new protocols
:-)

Protocol-enabled Tricks with VoIP

- DNS/DHCP queries can be spoofed
- Tftp download of image can be abused.
- RTCP uses source description RTCP packets that contain a source identifier, basically a 32 bit random number, and a description of the source. These identifiers are exchanged and piggy-backed while opening the media channel. We are interested in how random this number might be.
- H.323 v3 allows SNMP set commands: version info is in H225 header protocol field
- Legacy IP protocol security weaknesses (Voipcrack, vomit, spoofing, replay attacks, MITM attacks, DNS poisoning)
- IIS5, SQL, tftp services, OS's (linux, Win2000)

What Types of Damage are we Talking About?

Direct Losses

- Theft
 - Money
 - Trade secrets and company information
 - Digital assets
 - Consumer information
 - Computer resources
- Productivity Loss
 - Corruption of data
 - Diversion of funds
 - Recovery and continuity expenses

Indirect Losses

- Secondary Loss
 - Loss of potential sales
 - Loss of competitive advantage
 - Negative brand impact
 - Loss of goodwill
- Legal Exposure
 - Failure to meet contracts
 - Failure to meet privacy regulations
 - Illegal user activity
 - Officer liability

Ensuring your Equipment Meets New Demands

● Security Products

- Firewalls, Intrusion Detection & Prevention, Access Control and Authentication
 - Plethora of vendors and products
 - Market forces drive requirements and features to address them

● Protocols embedded/used in products

- Big issue

● Applications and platforms

- PC's & Servers
 - Market forces drive requirements and features to address them nicely
- Applications
 - Big issue

Equipment for New Demands, cont'd

- As more intelligence and function moves to the end-points (Enterprise perimeter and beyond)
 - Intrusion detection & prevention and other security related protection must be **embedded in the products** themselves (rather than the “surround”)
 - Example:
 - Caller-ID spoofing
 - This problem will force the bigger players -- mainly banks and telcos -- to enforce accuracy in both caller ID and call routing
 - VoIP technology leaders such as Avaya, will start putting sender authentication controls at the interfaces to the traditional phone systems -- thereby signaling the end of both spam and phishing while giving themselves a significant, if short term, competitive advantage in routing and related products

Tapping Services to Meet New Demands

- The complexity of managing IP Telephony stems from the fact that it is a cross-vertical service that spans applications (including call management, voice mail messaging and conferencing), system components (including servers, databases and middleware) and core network resources (including routers, gatekeepers and gateways).
- Managing such a complex ensemble of service infrastructure demands an automated, top-down (service to infrastructure) performance and availability management perspective.
 - Since the service level can be only as good as the weakest link in the service delivery chain, bi-directional smart navigation from both top-down service views and bottom-up resource views are critical to achieve accurate risk assessment and mitigation.

Translation of Previous Slide ☺

- Solutions (IP Telephony, Communication Applications, Business Applications, etc.) and the infrastructure they depend on must be managed holistically
 - Systems Management
 - Network Management
 - Security Management
 - etc.

Must exist simultaneously and MUST BE INTEGRATED!

- Rare given the IT Department + Network Management Service Providers (MSP) and Managed Security Service Providers (MSSP) are at the table as different entities more often than not and integration of same is generally a dream

Services (a.k.a. Managed Services), cont'd

- Differentiating IP Telephony services rests not only on the ability to deliver acceptable call quality and performance, but also on the right level of visibility and interaction in terms of customer-facing service level reporting (a.k.a. Management Systems as well as platform facilities)
- Vendors
 - Your products must support it!
- Customers
 - You must demand it!
- Service Providers
 - You Must deliver it!

Architecture

Increased network points of access equals increased network complexity, and complexity is the bane of security engineers. In addition, SIP may become a particularly attractive as hacking target, due its HTTP based underpinnings, and the ease with which ASCII encoded packets can be manipulated

- Payload or data encryption is an important piece of the VoIP security puzzle, but in most cases, the ability of an attacker to access the signaling channel will yield information about a call that is almost as valuable as the data content
 - Answer (perhaps – authenticate/encrypt the signaling channel
- No amount of encryption can protect against a single bad password, naïve system administrators, or poor protocol implementations.
- Converged networks, regardless whether based upon H.323 or SIP, require a different way of thinking about security

Principles for Approaching Converged Security

- **Emerging technologies when coupled with administrators not yet trained on the technology, lax security practices, insufficient controls, and poor understanding of the risks form an especially challenging security environment.**
- **One of the first keys to securing VOIP is to use and enforce the security mechanisms already deployed in data networks (firewalls, encryption, etc.) to emulate the security level currently enjoyed by PSTN network users.**

Specifics

- **Enforce physical security - Unless the VOIP network is encrypted, anyone with physical access to the office LAN could potentially connect network monitoring tools and tap into telephone conversations. Even if encryption is used, physical access to VOIP servers and gateways may allow an attacker to monitor network traffic.**
- **VOIP-ready firewalls and other appropriate protection mechanisms should be employed. Use firewalls designed for VOIP traffic. Stateful packet filters can track the state of connections, denying packets that not part of a properly originated call.**
- **Separate voice and data on logically different networks. Different subnets with separate RFC 1918 address blocks should be used for voice and data traffic, probably should use separate DHCP servers for each.**

Specifics cont'd

- **Use strong authentication and access control on the voice gateway system, as with any other critical network management component.**
- **Use IPSec or Secure Shell (SSH) for all remote management and auditing access. If practical, avoid using remote management (WAN) at all and access IP PBX's and related components from a physically secure system (inside the perimeter).**
- **Special consideration should be given to E-911 emergency services communications, because E-911 automatic location service is not available with VOIP in some cases.**

VoIP Specific

● Encryption

- IPSec or SSL: Both use the same type of negotiation to set up tunnels
 - IPSec usually functions at Layer 3 to encrypt the entire packet.
 - SSL functions between application and TCP to encrypt only application payload of packet. Retains addressing

● Network Segmentation

- Vlans
- Firewalls

● Strong Authentication

- PKI
- Token-based Access

Call to Action

- Customers
 - Educate yourselves on threats, what can be done and **DEMAND** of product and services vendors that it gets done!
- Communication/Application Product Vendors
 - Listen to your customers
 - Directly secure your products (do not wait on surround)
- Infrastructure Vendors
 - Listen to your customers
 - Consolidate management mechanisms
- Service Vendors
 - Listen to your customers
 - Manage holistically

Change How We Think about Security

- Old

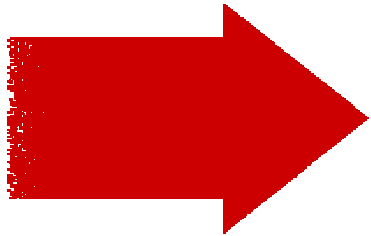
- Trust Internal Users
- Authenticate External Users - Maybe
- Firewall Internal Data & Users

Change How We Think about Security

- New

- Trust No One
- Authenticate Everyone
- Protect Important Data Wherever it is

Change How We Think about Security



Trust No One

**But trust
yourself to
identify solid
support that's
available**



AVAYA

OFFICIAL
PARTNER

**Official Convergence Communication Provider
for the 2002 and 2006 FIFA World Cup™
FIFA Women's World Cup USA 2003**