

CPNI VIEWPOINT 02/2007

ENTERPRISE VOICE OVER IP

AUGUST 2007

Abstract

Voice over IP (VoIP) is the term used for a set of technologies that enable real time voice or video conversations to take place across IP networks. VoIP devices and networks may interface with the Public Switched Telephone Network (PSTN). Enterprise VoIP, the subject of this Viewpoint, encompasses systems deployed by larger organisations that would traditionally run internal telephony services.

Other Viewpoints discuss Hosted VoIP 03/2007, in which an external provider hosts most of the control components, and Internet VoIP 01/2007, which involves peer-to-peer telephony via the public Internet.

CPNI Viewpoints

CPNI Viewpoints are intended to provide a management level overview of emerging risks. A Viewpoint may not necessarily offer mitigation advice; other CPNI products are available for this purpose.

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

KEY POINTS

- Using a shared medium will enable savings on the cost of infrastructure and operating charges but will bring new risks to business critical communications.
- Organisations considering VoIP should carry out a full risk assessment to understand the value of voice and data across the business.
- Risk mitigation measures need to be built in at the design stage and cannot easily be added later
- Involve the network and security teams for both voice and data in the planning to ensure a reliable and secure VoIP implementation
- If the business wishes to maintain the level of confidentiality available on current voice systems this will need to be built in by logical or physical separation of voice and data and measures to prevent interception between sites.
- Retaining an emergency telephony capability in the event of power loss will require planning and investment.
- Inbound VoIP calls from external organisations lack caller validation and may breach existing security measures.

INTRODUCTION

The traditional Public Switched Telephone Network (PSTN) infrastructure, and voice telephony in general, is in transition from a Time Division Multiplex (TDM) based, circuit-switched architecture; to an Internet Protocol (IP) based, packet-switched architecture, commonly referred to as Voice over IP (VoIP). One of the fundamental properties of the VoIP implementations is the use of common media for speech, signalling and control, and data.

The use of a common medium is seen as an advantage in that users and providers can make great savings on capital expenditure (capex) and operating charges (opex). However, the use of a common medium also brings a number of risks to business communications that should be balanced against the cost savings in any proposed or planned implementation, and actively managed.

Telephony networks are mission critical to an organisation and it is therefore vital to understand the potential vulnerabilities a move to VoIP could expose, and to ensure any implementation minimises the risks.

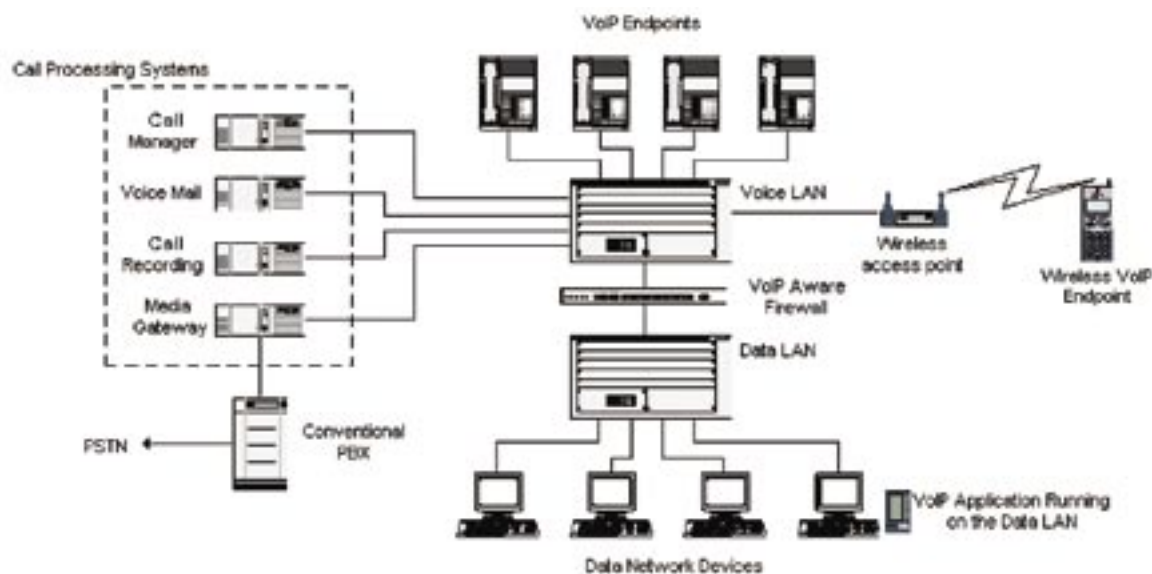
Enterprise VoIP solutions are developed for companies that would typically operate one or more telephony systems and utilise Private Branch Exchanges (PBX) to support a large number of users.

This Viewpoint examines Enterprise VoIP security issues as they apply to the planning, deployment and operational phases of an implementation.

GENERAL

Enterprise VoIP deployment

Figure 1. Enterprise VoIP deployment components



The diagram above illustrates some of the components that may appear in an Enterprise VoIP deployment. The precise terms and systems used vary depending upon the vendor used, but generally the components that are commonly used fall into one of three categories.

Table 1. Enterprise VoIP Components

Endpoints	IP Phones; Soft phones etc.
Call Processing Systems	Servers and interface systems that setup calls, link VoIP calls with the PSTN, provide voice mail and voice recording etc.
Network Infrastructure	Switches, routers, firewalls etc.

Enterprise VoIP solutions can be used to interface with traditional PBX systems, which may continue to offer PSTN connectivity in the transition to NGN. Pure VoIP communication will generally be limited to calls both originated and terminated within the same organisation. However, while Service Providers provide services to link VoIP 'islands' using a VoIP interconnection, the PSTN will continue to be used by many for calls that cross an organisation's boundaries.

The convergence of voice and data into IP based communications allows Enterprise VoIP adopters to implement applications (for example contact centres) that integrate voice and data in a very flexible manner.

Enterprise VoIP products are sold on the benefits of cost savings that may be achieved by converging voice and data networks, alongside efficiency savings that greater flexibility in the voice network could provide. However, not all data networks can easily accommodate the particular requirements of voice content and control data. Any potential savings should accurately reflect the additional investment in data networks that is invariably required to deploy Enterprise VoIP in a reliable and secure manner.

Security cannot be layered onto an Enterprise VoIP deployment as effectively or efficiently post-implementation as it would be at the design stage. Organisations considering the transition to VoIP should not be tempted to leave security issues for a 'second phase' as it is invariably more expensive and more difficult to 'bolt-on' later, and leaves the business at significant risk.

PLANNING

It is essential to involve the right teams when planning an Enterprise VoIP deployment. Within many organisations voice support, whilst part of the general network and IT support functions, tends to operate autonomously. When deploying VoIP, it is important to involve the network and security teams for both voice and data to ensure a reliable and secure deployment.

If selecting an external company or integrator to deliver Enterprise VoIP, it is important to ensure they provide details of the security measures they intend to employ. It is possible to deploy VoIP systems 'out of the box' without truly understanding the security implications for the business, and this can lead to problems in the future. Check to see if a potential supplier addresses the security concerns outlined in this document as part of their submission.

A formal risk assessment of an Enterprise VoIP deployment is strongly advised. To facilitate such a risk assessment, the importance of the use of voice across the business with regards to confidentiality, integrity and availability should be understood.

Separate data networks, such as voice data, corporate data, and management data, can exist on the same physical network, or they can be physically separate networks, each optimised to the specific characteristics of the data. In a conventional PBX system, voice is transported on a physically

separate network to corporate data, with entirely different electrical characteristics and signalling. Due to the fundamental changes involved in convergence, good network design is critical.

The physical separation of traditional telephony makes call interception difficult, and insulates voice operations from any attacks or problems being experienced on the data network. Thus, the traditional voice network is generally considered 'safe' and 'trusted'.

In VoIP systems, access to the data network can be all that is required to achieve call interception. For example, with the right circumstances and skills, it would be possible to cause the IP packets that are supporting a VoIP call to be routed via a rogue computing device on the same network, giving the opportunity to record or disrupt the call.

In order to mitigate against the risk of VoIP call interception, there are three techniques that can be used by the corporate VoIP user to ensure VoIP traffic remains separated from data traffic, and is therefore less prone to attack and diversion.

- i) Building them using separate network hardware, with only the VoIP network being linked to the service provider, can physically separate the VoIP and data networks.
- ii) Network switch configuration options can be used to keep voice data logically separate from normal LAN data. This can be achieved by configuring separate Virtual LANs (VLANs) for VoIP and data, and by ensuring that VoIP and data devices are connected to switch ports that are configured to use the appropriate VLAN.
- iii) The VoIP devices can encrypt VoIP traffic before it is transmitted on the network. Encryption on its own does not prevent the diversion or disruption of VoIP data packets, but does prevent eavesdropping.

Logical separation should be coupled with controls such as port based network access authentication to ensure that the correct physical devices are connected to the correct ports. Without such controls it may be possible to connect PC devices to the voice LAN, compromising separation.

Separate IP networks should be used for voice and data services; this means that voice and data devices should be allocated logically separate IP addresses.

VoIP endpoints are usually reliant upon network support services such as DHCP*, TFTP* and DNS servers to provide configuration information. Dedicated support services should be considered for VoIP networks, rather than risk compromising separation by using existing systems for these tasks.

The use of shared physical media for VoIP and data services means an attack against data devices (e.g. a worm attempting to spread through the network) could result in voice services being affected. Network Quality of Service (QoS) techniques should be used to provide VoIP traffic some priority over normal data.

IP phones are actually low powered computing devices, and generally run embedded versions of standard operating systems. As such IP phones can contain vulnerabilities that may be exploited, and require software updates and patches on a regular basis. Generally IP phones will download their software from the call processing systems or TFTP servers when switched on. It is anticipated that as VoIP matures and its use becomes more widespread that more effort will be put into finding vulnerabilities associated with them.

* see Glossary

The use of 'soft' phones on desktop computers can cause the rule regarding the separation of the voice and data networks to be broken, as calls to and from the soft phone will have to traverse the data network and enter the voice network for call processing and routing. Firewalls able to inspect the VoIP traffic should be implemented between the two networks to ensure that only valid traffic crosses between the networks.

Networks carrying VoIP sessions must be able to guarantee acceptable levels of latency, packet loss and jitter otherwise call quality may suffer, ultimately making the service unusable.

Once live it will be extremely difficult to negotiate down time on a voice system. However Enterprise VoIP systems tend to run on commodity operating systems and hardware, which will require patching and maintenance more often than a traditional PBX. Sufficient network resilience and good network design can accommodate this.

If you cannot take down the call processing systems of a VoIP implementation to apply critical security patches in a timely manner, you may leave your organisation exposed to vulnerabilities for extended periods of time.

An organisation could choose to use the Internet as a low cost alternative to PSTN connectivity between sites. In such circumstances this traffic should be secured to ensure confidentiality, for example by using Virtual Private Network (VPN) technologies. Latency may be difficult to guarantee, and should be carefully tested. For a detailed discussion of VPN technology, see NISCC Viewpoint 03/06.

Inbound Internet VoIP could open the organisation to attacks such as SPAM over Internet Telephony (SPIT) or denial of service, and potentially provide an avenue over which perimeter security could be breached. The potential low cost of Internet VoIP should therefore be balanced against the increased risk of attack. (See Viewpoint 01/2007 "Internet VoIP".)

EMERGENCY CALL HANDLING

Typically large organisations have their own emergency number, which will be directed to switchboard staff. PBX systems can associate extension numbers with a physical location, ensuring that the source of an emergency call can be identified. The flexibility that an Enterprise VoIP solution provides with regards to easy relocation of extensions may make location information hard to provide. Procedures should be examined and updated to allow for this.

Gaining emergency assistance in the event of conditions such as power failure may be difficult via VoIP systems, as network-switching equipment is not always resilient to power failure. It may be necessary to invest heavily to ensure the entire required infrastructure is as resilient as possible. Alternatively emergency procedures may need to change, with external exchange lines being provided for emergency use, and staff being made aware which telephones can be used in emergency or power loss situations.

CONCLUSION

The inherent separation from the data network that a traditional PBX based telephony system provides has desirable security properties that can be emulated using Enterprise VoIP with careful design. While most vendors do provide the features required to achieve equivalent security, care should be taken to ensure that these features are implemented correctly.

Enterprise VoIP is potentially more susceptible to call interception and modification than a traditional PBX based-system, unless steps are taken to ensure that the VoIP signalling and media connections are secured.

As the take up of Enterprise VoIP accelerates, the amount of effort concentrated on finding vulnerabilities will also increase. The standards are also still evolving. It will be important to keep up to date with future developments and to analyse their impact on the security position of an Enterprise VoIP deployment.

Enterprise VoIP components are all based upon standard hardware and software, and will therefore require careful patch and upgrade management to maintain security.

Use of VoIP systems may compromise the ability to make emergency 999 calls, and adequate provision must be made to compensate for this.

USEFUL LINKS

<p>www.voipsa.org</p>	<p>VoIP Security Alliance: A collaboration between vendors, service providers and industry leaders that aims to promote the adoption of VoIP by improving security research, education and awareness. In particular, see the 'VOIPSA Threat Taxonomy' dated 24 October 2005.</p>
<p>www.hackingvoip.com/sec_tools.html</p>	<p>An illustration that risk mitigation is an important activity during Enterprise VoIP implementation, this web page lists currently available tools discussed in a forth-coming book that can be used to compromise VoIP if sufficient controls are not implemented.</p>
<p>www.blueboxpodcast.com</p>	<p>A weekly roundup of VoIP security related issues produced by VOIPSA member Dan York.</p>
<p>www.cpni.gov.uk</p>	<p>A number of products giving advice on related subjects including: NISCC Technical Note 01/07 IPsec VPN Security Guide dated 4 January 2007 CPNI Viewpoint 01/2007 'Internet VoIP' dated August 2007 UK NSIE 'VOIP Security Considerations for Service Providers' dated July 2007</p>
<p>www.ofcom.org.uk</p>	<p>The telecommunications industry regulator: The Ofcom website contains a description of the telecommunications marketplace, including details of the Authorisation Regime.</p>

GLOSSARY

802.1Q	An IEEE standard that defines the use of Virtual LANs (VLANs)
802.1X	An IEEE standard that defines port based network access control.
ACL	Access Control List: In networking an access control list defines the communications permitted between specific source and destination locations.
Circuit switched	A circuit switched network is one that establishes a dedicated circuit between endpoints before any communication occurs. Each circuit created cannot be used by other callers until the circuit is released and a new connection is set up.
DHCP	Dynamic Host Configuration Protocol: Defined by the IETF standard RFC 2131, DHCP is used by networked systems to obtain IP addresses and other parameters to allow network operation.
DLE	Digital Local Exchange
DTMF	Dual-tone Multi-frequency: A line code used for signalling to and from the traditional telephone instrument.
DNS	Domain Name System: Defined in the IETF standards RFC 1034 and 1035, DNS provides a mechanism to resolve host names to IP address information.
Endpoint	Within this document the term 'Endpoint' is used to describe any device that initiates or terminates a VoIP session.
ETSI	European Telecommunications Standards Institute
Firewall	A logical barrier designed to prevent unauthorised or unwanted communications between sections of a computer network
H248	H.248, also known as the "Megaco" protocol, is the international standard for media gateway control.
H323	H.323 is an international standard defined by the ITU for multimedia communication over packet-switched networks.
IETF	Internet Engineering Task Force: The standards body for Internet protocols.
IP	Internet Protocol: a data-oriented protocol used for communicating data across a packet-switched network.
IP Address	Internet Protocol Address: a unique address that devices use in order to identify and communicate with each other on a computer network utilising the Internet Protocol standard (IP).
IP Phone	A VoIP endpoint that looks and works like a conventional analogue telephone, but usually with additional capabilities like video display.
ITU	International Telecommunication Union
Jitter	In packet-based networks jitter is the measure of variation in delay experienced by consecutive packets as they travel from source to destination. VoIP devices include buffers to smooth out the effects of jitter, but ultimately call quality will suffer if jitter becomes too high.
LAN	Local Area Network

Latency	Latency, or delays in the traffic paths, can cause voice quality degradation if it is excessive. The goal commonly used in designing networks to support VoIP is the target specified by ITU standard G.114 which states that less than 150 ms of one-way, end-to-end (from mouth to ear) delay provides user satisfaction for telephony applications. Delay is typically experienced through various components that make up VoIP connections, including encoding/decoding, network transport and routing and encryption/decryption.
Layer 2	The Data Link Layer. Ethernet is the most common data link protocol.
Layer 3	The Network Layer. IP operates at the Network Layer of the OSI seven-layer protocol stack.
MAC Address	Media Access Control Address: A 48-bit address used to uniquely identify systems on an Ethernet.
Media Gateways	Media Gateways provide conversion between traditional telephone circuits and voice content carried on VoIP networks. Gateway control protocols such as MGCP and H.248 (Megaco) are used to control set up of calls on Media Gateways in response to call management requests received in signalling messages.
MGCP	Media Gateway Control Protocol: Defined by the IETF in standard RFC 3435, MGCP is used between call processing systems and Media Gateways that link VoIP to the PSTN.
NIDS:	Network Intrusion Detection System: a system that tries to detect malicious activity by monitoring network traffic.
Packet Loss	Packet loss causes voice clipping and dropouts in conversation. Many codecs incorporate packet loss concealment techniques to mask the effects of lost or discarded VoIP packets. The packetisation interval determines the size of samples contained within a single packet. For a 20ms packetisation interval, the loss of two or more consecutive packets results in a noticeable degradation of voice quality. VoIP networks should be designed for zero packet loss in normal operation.
Packet switched	A data communications system in which packets (units of information carriage) are routed between nodes over data links shared with other traffic.
Patch	An update to a piece of software that fixes a defect in a formal release. Most often used in reference to operating systems.
PBX	Private Branch eXchange
Peer to Peer	A peer-to-peer system is a distributed system whose component nodes participate in similar roles, and are therefore peers to each other. There is usually some form of structure placed on peer-to-peer networks to enable individual nodes to locate each other.
Proxy	A proxy is a server that acts as an intermediary between a workstation user or local service and the Internet or remote service, so that an enterprise can control and administer security and provide a caching service.
PSTN	Public Switched Telephone Network
QoS	Quality of Service

Router	A router is a communications device that forwards data packets across a network toward their destinations, through a process known as routing. Routing occurs at Layer 3 (the network layer i.e. Internet Protocol (IP)) of the OSI seven-layer protocol stack.
RTP	Real-time Transport Protocol: Defined by the IETF standard RFC 3550, RTP is a standardised packet format for delivering audio and video over internet networks.
Signalling	Signalling protocols are used to manage all aspects of call set-up, acceptance and termination, as well as in call operations such as handling DTMF signalling to remote call systems. The signalling protocols also provide a transport for text based instant messaging functionality.
SIP	Session Initiation Protocol: Defined by the IETF standard RFC 3261, SIP is an application-layer control protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include VoIP telephone calls, multimedia distribution, and multimedia conferences.
Soft Phone	A piece of software for making VoIP calls using a general-purpose computer, rather than using dedicated hardware.
SPIT	Spam over Internet Telephony: A theoretical method of exploiting the SIP protocol to distribute unsolicited voice messages and calls to VoIP users.
SRTP	Secure Real-time Transport Protocol: Defined by the IETF standard RFC 3711, SRTP provides encryption, message authentication and integrity, and replay protection to the RTP data.
Stateful Inspection	A method for keeping track of the state of network connections (such as TCP streams) travelling through a routing TCP/IP device (usually a firewall). The system is programmed to distinguish legitimate packets for different types of connections. Only packets matching a known connection state will be allowed to pass.
Switch	A network switch is a networking device that performs transparent bridging (connection of multiple network segments with forwarding based on MAC addresses) at full wire speed in hardware.
TDM	Time Division Multiplexing: A transmission technique whereby several low speed channels are multiplexed into a high speed channel for transmission. Each low speed channel is allocated a specific position based on time.
TFTP	Trivial File Transfer Protocol: Defined by the IETF standard RFC 1350, TFTP is a very simple file transfer protocol which is useful for providing image and configuration data to relatively low powered network devices.
Toll Fraud	Any technique that allows a third party to make fraudulent calls by exploiting configuration weaknesses in telephony systems.
TLS	Transport Layer Security: A cryptographic protocol that provides secure communications on the Internet for such things as web browsing, e-mail, VoIP, and other data transfers.
VLAN	Virtual LAN: A method of creating independent logical networks within a physical network.
VoIP	Voice over Internet Protocol

VPN	Virtual Private Network: A VPN is a private communications network often used within an organisation, or shared by several organisations, to communicate confidentially over a publicly accessible network.
Wi-Fi	A brand originally licensed by the Wi-Fi Alliance to describe the underlying technology of wireless local area networks based on the IEEE 802.11 specifications.
Wire Tapping	The monitoring of telephone conversations by a third party, often by covert means.