

# CPNI VIEWPOINT 01/2007

## INTERNET 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). Internet VoIP, the subject of this Viewpoint, involves peer-to-peer telephony via the public Internet.

Other Viewpoints discuss Enterprise VoIP (02/2007), which describes systems deployed by larger organisations that would traditionally run internal telephony services, and Hosted VoIP (03/2007), in which an external provider hosts most of the control components.

### 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**

- The use of the Internet to carry VoIP traffic means there can be no guarantee of end-to-end network quality, and therefore no guarantee of call quality and reliability.
- There are two basic types of Internet VoIP client, each of which have differing security issues.
- Internet VoIP providers make little to no provision for handling emergency calls.
- There is currently no regulation of Internet VoIP providers in the UK.

## 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.

Internet VoIP describes services that provide IP-based telephony using the public Internet as a transport for voice, video and signalling or call set-up.

Internet VoIP can be split into two different types;

- Peer-to-peer based systems, often included as part of proprietary instant messenger type software (examples include Skype, Google Talk and MSN Messenger)
- Internet VoIP services based on open Session Initiation Protocol (SIP) standards, which can be used either from a PC soft-phone, or using specific VoIP hardware (examples include Vonage, SIPGate and BT Broadband Talk).

## GENERAL

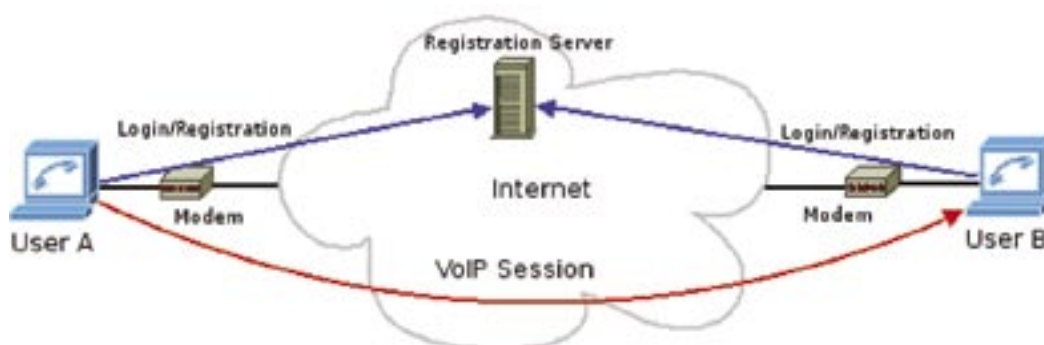
### Peer-to-Peer Systems

Figure 1 shows VoIP call setup with a peer-to-peer based system. When each user starts up their client software, it registers with a server on the Internet. This allows users to see each others status, and enables the software to initiate a direct VoIP connection with a peer based upon their current location.

Some peer-to-peer based systems may not interface with the PSTN at all, and only support calls between PC clients. Others have fee based PSTN interface services.

In addition to providing VoIP facilities, peer-to-peer PC based systems also provide instant messaging and file sharing services, which can have a detrimental effect on overall network performance and security.

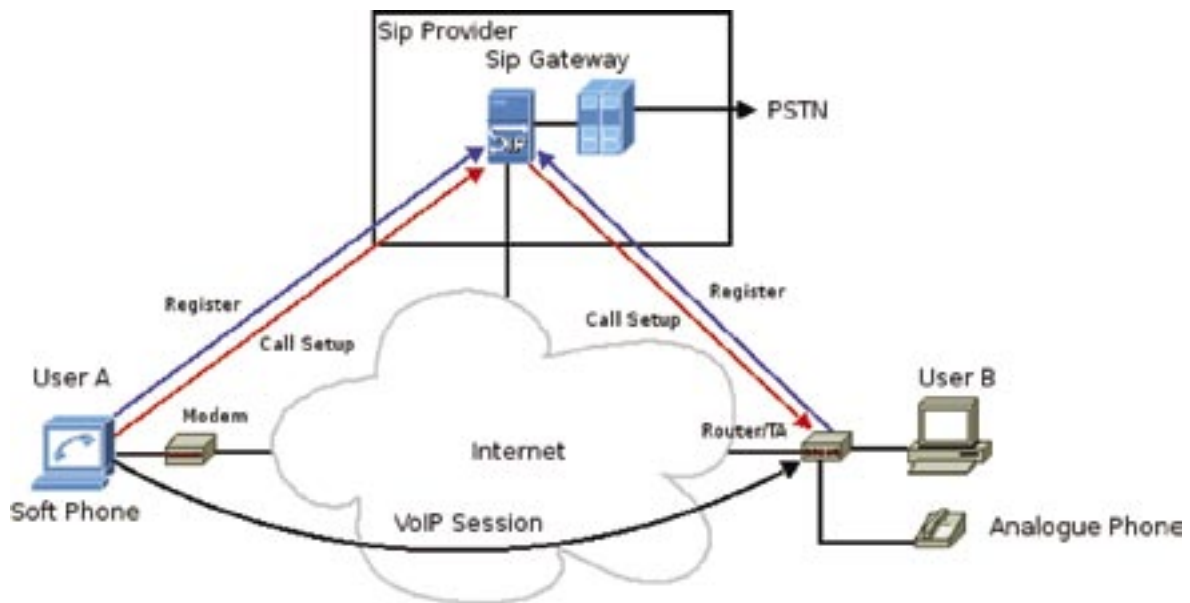
**Figure 1. Peer-to-peer VoIP call setup**



## Session initiation protocol (SIP) based VoIP

Figure 2 shows call setup with a SIP based system. In this case either a PC based soft phone program can be used (User A), or a router with a built-in telephone adapter that supports SIP (User B). On start-up each registers with the SIP provider, which identifies the client with a PSTN number and current Internet location. When a new call is initiated it is setup via the SIP provider, but the VoIP session is made directly with the called party, unless it is to a PSTN number.

**Figure 2. SIP Internet VoIP call setup**



## OPERATION

Networks carrying voice traffic must be able to guarantee acceptable quality of service. Levels of packet latency, packet loss and jitter all have to be maintained within defined limits or call quality may suffer, ultimately making the service unusable. When using the Internet as a transport, there are no guarantees possible regarding end-to-end network performance, and hence it is not possible to guarantee service availability.

Unencrypted VoIP traffic can be intercepted without the knowledge of the user by anyone with access to the data path between source and destination. As the transport network used is the public Internet, without the use of encryption techniques it is therefore impossible to guarantee call confidentiality and integrity.

In the UK, Internet VoIP services are not currently subject to telecommunication regulations applied to Publicly Accessible Telephony Services (PATS). This means that the standards a customer would expect with regards to facilities, availability and billing from a PSTN service may not be in place on an Internet VoIP service.

Where there is a requirement or policy to log or record all calls for example for regulatory purposes, Internet VoIP systems can circumvent the logging process and breach the policy.

It is important to understand why peer-to-peer VoIP based systems are required to be used for business operations. Given that calls are only free between like PC clients, the scope for call cost savings are likely to be minimal, and could be discounted by the increased security risks posed by the additional instant messaging and file sharing capabilities.

Peer-to-peer PC clients have many features that can lead to the inadvertent leaking of information. For example, some record online status, and will automatically update a central server when a user is online or logged out.

Peer-to-peer PC based systems have proven to be very adept at circumventing firewall access controls. It is difficult to restrict or block their use. These systems may or may not encrypt VoIP communications; potential users should investigate the encryption capabilities of a particular client before using it.

SIP based Internet VoIP services do not routinely employ any voice encryption. Signalling encryption is usually also minimal, being restricted to only the credentials used by the client device to login to the SIP gateway.

SIP based Internet VoIP services will permit inbound SIP calls from any location, and are therefore theoretically vulnerable to denial of service attacks by simple random call creation, and SPAM over Internet Telephony (SPIT).

## **EMERGENCY CALL HANDLING**

In general Internet VoIP services are not considered as PATS, and are therefore not required to provide 999 services, although the regulator is encouraging them to do so. It is therefore important to understand whether or not a particular Internet VoIP provider will permit calls to the emergency services.

As access to Internet VoIP services rely upon the availability of power, and proprietary hardware or software solutions, they should not be considered as a primary method of access to the emergency services, even if the provider permits emergency calls.

## **CONCLUSION**

The use of Internet VoIP solutions for CNII applications should be examined carefully before adoption. Historically Internet VoIP has been developed for individual users, who wish to take advantage of toll free calling; security and service quality have therefore not featured as a high priority. As a result, Internet VoIP is not considered suitable for corporate use or in business-critical applications.

The additional instant messaging and file sharing capabilities of peer-to-peer Internet VoIP systems have potentially serious security implications.

Internet VoIP services should not be considered as a primary method of access to the emergency services.

## USEFUL LINKS

|  |   |
|--|---|
| <a href="http://www.voippsa.org">www.voippsa.org</a>               | 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.                   |
| <a href="http://www.blueboxpodcast.com">www.blueboxpodcast.com</a> | A weekly roundup of VoIP security related issues produced by VOIPSA member Dan York.  |
| <a href="http://www.cpni.gov.uk">www.cpni.gov.uk</a>               | A number of products giving advice on related subjects including:<br>NISCC Technical Note 01/07 IPsec VPN Security Guide dated 4 January 2007<br>CPNI Viewpoint 02/2007 'Enterprise VoIP' dated August 2007<br>UK NSIE 'VOIP Security Considerations for Service Providers' dated July 2007 |
| <a href="http://www.ofcom.org.uk">www.ofcom.org.uk</a>             | The telecommunications industry regulator: The Ofcom website contains a description of the telecommunications marketplace, including details of the Authorisation Regime.   |

## 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.  |