

# » Security Issues Around the Deployment of VoIP and Multimedia protocols in Wireless and Firewalled Environments «

A white paper by Matt Gordon-Smith,  
Siemens Insight Consulting



## Introduction

The recent increase of geographically dispersed users and telecommuting has given rise to greater requirements for better methods of collaboration and interaction between personnel. This has increased the prevalence of technologies such as Voice over Internet Protocol (VoIP) and multimedia protocols such as video-conferencing, web-casting and Instant Messaging. The capabilities of the Internet and many private networks have ensured that all these functions are able to run across existing infrastructure, encouraging network convergence and reducing costs. However, implementing these applications in firewalled environments and over wireless networks poses a number of security

issues, which need to be addressed as part of any such deployment.

The scope of this document is to identify and explore some of the issues that may affect organisations deploying this technology.

## Possible issues

### Privacy

For most applications not relying on real-time communication, the accepted way of protecting privacy is with the use of encryption. However, using application encryption for time-critical applications such as voice and multimedia services could add a significant overhead. This is because each packet of voice data would have to be individually encrypted by the application during sending and then decrypted at the other end, creating an unacceptable delay.

Encryption would not typically be deployed across trusted wired networks as the physical security of the network devices and connection points should be managed to mitigate the risk of traffic interception. This is not so easy with wireless networks, as a malicious party does not necessarily need physical access to the building or computer suites to access the network. In addition to this, wireless access points are typically less physically secure than wired network equipment, due to being placed outside of the secured environment of a data centre.

If running voice and multimedia services over a wireless network, then attempting to encrypt the traffic at an application level could cause the same severe delay as doing so over a wired network. To protect the traffic the entire communication between the user's wireless adapter and the wireless access point can be encrypted by various protocols at a much lower layer of the connection, which is transparent to the application. This bypasses the need for the encryption to be performed by the application and improving on the significant latency issue.

Earlier standards for wireless encryption such as the 64-bit and 128-bit Wireless Encryption Protocol (WEP) did not have much of a latency problem but were easily cracked and their use is no longer recommended. Wireless Protection Algorithm (WPA) is a more secure encryption standard with a similar low-latency. Another alternative is the later WEP2 encryption that uses the stronger Advanced Encryption Standard (AES), which although it provides more protection, increases the latency. Therefore, striking the correct balance between privacy and latency is essential.

As well as the risk of a third party being able to intercept voice and multimedia traffic over the wireless network there is also the risk that they could use those same wireless access points to connect to the wired network. By posing as a genuine user they can intercept the traffic once the wireless access point decrypts it. In order to help prevent this, wireless access points should not be configured to authenticate by only a traditional password.

Implementation of more advanced authentication systems such as the Extensible Authentication Protocol (EAP) would allow additional authentication methods such as Token Cards, Kerberos, Digital Certificates and PKI.

In addition to issues of third party interception of voice and multimedia traffic, there are also a number of legal issues regarding the extent to which the organisation is able to monitor the usage of these applications. This is discussed later

on in this document.

### **Bandwidth**

A key element of security is availability. If an application is not available to its users then the loss of that service could prevent the business from functioning. This is especially a concern when there are high availability requirements such as with health and emergency service organisations. Bandwidth is a key element in preventing Denial of Service (DoS) as many such attacks on the Internet work by removing the available bandwidth from the users. A DoS incident is not always the result of a malicious third party element, but can often be attributed to simply not having the required resources available in the first place. Therefore, attempting to run applications without the required bandwidth would constitute the organisation essentially performing a DoS attack on itself. VoIP needs to operate within a minimum guaranteed bandwidth to ensure that there is a minimal amount of delay in the voice traffic and that the quality of the sound is at the desired standard. The same applies to web conferences, video calls and many other multimedia applications where they not only require a minimum acceptable bandwidth, but also can make more significant demands on network capacity than many other applications.

Many local area networks have the available capacity for these applications and the functionality exists within the network devices to reserve bandwidth for specific applications such as VoIP. Provided that any wide-area connections have been suitably specified for these applications then they should also be able to meet the minimum requirements. However the overall performance of the network is only as good as its lowest capacity components.

To guarantee the integrity of the VoIP connection, a function called Quality of Service (QoS) can be used to give priority to voice traffic over any other. QoS guarantees are given based on the percentage of network packets lost and the percentage that have to be discarded due to late arrival. Additional QoS guarantees are required for VoIP over Wireless (VoIPoW or VoWiFi) because of the potential increase in packet loss and latency when users are roaming between wireless base stations. There is also the key issue of the signal degradation present when users are further away from a base station, which in turn affects the quality of the traffic. The quality of VoIP communication is judged via a Mean Opinion Score (MOS) test where the rating is graded from 5 for excellent quality similar to perfect AM radio reception, down to 1 for bad quality which would constitute a communications breakdown.

Organisations should ensure that their MOS score for VoIP does not drop below an acceptable standard when used over a wireless network.

Bandwidth can also be an issue through firewalls. Although many modern firewalls have a large capacity for traffic, many older implementations are more restrictive. No matter what the bandwidth potential of a firewall, if it is highly utilised, then there may not be significant enough resources available to pass VoIP and multimedia traffic through without experiencing a delay.

## Firewall Configuration

The basic principle of a firewall is that you use it to deny access to all traffic and then only allow through that communication which you have explicitly permitted within the firewall rulebase. Therefore, the more connections that are permitted to pass through the firewall and the larger the range of addresses that can communicate through, the weaker the security provided by the firewall.

A number of problems can arise from the implementation of VoIP through a firewall. Many existing enterprise firewalls are unable to distinguish between voice and data traffic in order to prioritise the voice communication and avoid latency as discussed previously. Configuring numerous User Datagram Protocol (UDP) ports to be constantly open can enable some firewalls to overcome this latency, but this would seriously weaken the overall effectiveness of the firewall. Issues can also stem from the fact that connections cannot be initiated into a secure firewalled environment without the originating address and destination network port already being configured in the rulebase. Potentially, this could open up the firewalled environment to a significant number of addresses. Using a peer-to-peer connection initiated from inside the firewalled environment would solve this, but once open, there is a permanent hole in the firewall and the person on the other end of the connection, or someone posing as them, could take advantage of this to access the firewalled environment without authorisation.

## Network Resilience

With separate data and voice networks and with multimedia services provided through television, video or satellite, the failure of one element would not normally have an impact on another. Although the failure of the phone network could affect the use of the videoconferencing suite, the overall impact would not be the total loss of all communication.

With voice services being integrated into data networks, videoconferencing merging in the same way and audio/video downloads and streaming also available by the same medium, a failure of that medium would have a significant impact on the ability of the network users to continue working.

Not only are there the possible outage risks to consider, but also additional support costs would be incurred for managing these extra services and the additional helpdesk calls for when they go wrong. If someone loses their network connection and that network also carries their voice traffic, how do they call the helpdesk? Increased resilience and component redundancy need to be carefully considered as networks converge.

## Legal considerations

Network and application monitoring is an essential part of managing and maintaining the health of any network and the systems that run across it.

Monitoring tools may be used which not only take a high level view of the network but which could potentially read the data being sent across it. If the network is carrying VoIP traffic and the monitoring software were able to reproduce the voice output then this could be considered an illegal act.

The Regulation of Investigatory Powers Act 2000 (RIPA) is a framework for the lawful interception of all postal, telecommunications and digital communications. It replaces the Interception of Communications Act 1985 and all other prior legislation in this area. Under the Interception of Communications Act 1985 it was illegal to tap into any public telecommunications network without a warrant from the Home Secretary.

However, private telecommunications networks, such as internal systems or office networks, were excluded and were not covered by any other law in this way.

This meant that organisations could do what they wanted with the information on their own networks with relative impunity. By monitoring within a firewalled environment, it would have been simple to claim immunity through the operation of a private network.

RIPA which repeals this older legislation, making allowances for private networks and defining them as any private telecommunications system that is attached to a public telecommunications system, such as an internal phone system linked into the public phone network. It also expands on the definition of "public telecommunication systems" as not just those granted a licence under the Telecommunications Act 1984, but any telecommunications service offered to the public in the UK. This would include both private VoIP & multimedia systems linked in to external ones as well as private VoIP and multimedia systems on a private network connected to an Internet Service Provider (ISP).

Under RIPA some legitimate private interceptions are permitted, including monitoring for regulatory practices and standards, to detect crime and unauthorised use and in the interests of national security. All these permitted interceptions have requirements and provisions within RIPA that need to be applied and adhered to. Organisations affected by this act also need to be aware it intersects with the Data Protection Act (1998) and the Human Rights Act (1998) against which any action must be balanced.

# Security Issues Around the Deployment of VoIP and Multimedia Protocols in wireless and Firewalled Environments

## Recommendations

Based on the possible issues outlined within this document, the following are recommendations for organisations wishing to deploy VoIP and multimedia protocols in wireless and firewalled environments. As the scope of this document is only to identify the issues with these implementations, rather than to detail possible mitigations, this section is a very high level summary of suggested actions in the form of a conclusion:

- Implement encryption on all wireless connections that will provide the best balance between privacy and latency. In addition, use a stronger wireless authentication method than the traditional password. All wireless access points should be physically placed out of site and reach.
- Ensure all network equipment can handle the required bandwidth, including increasing the capacity of Wide Area Network (WAN) links if applicable. Consider the use of Internet Virtual Private Network (VPN) connections to replace leased lines for greater bandwidth, as well as flexibility and cost savings. Ensure that there are no bottlenecks and that time-critical traffic, such as voice and multimedia, is given priority. Ensure that appropriate QoS is implemented on all wireless, as well as wired networks.
- Ensure that all existing firewalls are able to prioritise voice traffic over data traffic. Upgrade or replace those that can not.
- Protect Internet gateways by implementing either voice-aware firewalls or an application gateway server within the Internet Demilitarised Zone (DMZ) to allow incoming VoIP calls and multimedia traffic initiated from external parties without compromising the security of the gateway firewall.
- Build resilience into the network in terms of dual switches, routers, firewalls and system/application servers. Also configure diverse routing and backup connections with

automatic fail over. Don't let a small network failure disrupt all communication. Ensure that appropriate technical support is available for any additional services being run across the network.

- Seek legal advice about what is and what is not permitted under the law regarding the monitoring of network communication.



## Author's biography

**Matt Gordon-Smith** is a Senior Consultant with Siemens Insight Consulting, leading the Security Architecture & Design team. Matt has an honours Bachelors degree in Information & Computer Science and is a Certified Information Systems Security Professional (CISSP).

Matt started his career in IBM, initially as a Network Architect. His interest in security started early on, as he designed and implemented network and firewall solutions. He became acutely aware of the issues surrounding security perimeters and the importance of access control and logical and physical network separation between networks of differing trust. Matt's work as network custodian, responsible for the configuration management, user controls and patch management of network devices also gave him a firm grasp of these important security elements.

Matt soon moved within IBM from this role to a position as a Security Architect, using the security knowledge developed in his previous role and specialising in the implementation and management of security around networks. This role allowed him to explore the greater realms of security and to develop knowledge in the other security domains. Matt's work as a Security Architect has taken him to different business sectors and has involved creating solutions up to enterprise architectures.

Insight Consulting is the specialist Security, Compliance, Continuity and Identity Management unit of Siemens Communications and offers a complete, end-to-end portfolio encompassing:

- Security
- Compliance
- Continuity
- Identity Management
- Managed Services
- Training

Siemens Insight Consulting subscribes to the CESA Listed Advisor Scheme (CLAS) and CHECK services. We're also certified against BS 7799 and are a preferred supplier of services to the UK Government and are an accredited Catalyst supplier.

If you'd like to find out more about how we can help you manage risk in your organisation, visit our web site at [www.siemens.co.uk/insight](http://www.siemens.co.uk/insight)  
Siemens Insight Consulting  
Tel: +44 (0)1932 241000  
Fax: +44 (0)1932 236868

[www.siemens.co.uk/insight](http://www.siemens.co.uk/insight)