

## Security for VoIP and Voice over Wireless

Author: Bob Cushing, Broadband Vantage Ltd

### About this document

This paper is one of a set of papers focused on technical topics (called the Technical Thread) which in turn forms part of a series of papers produced by Samsung Telecom UK. It is not designed to be a comprehensive analysis of all aspects of security and seeks only to highlight some of the key issues.

### Introduction

The rapid growth in popularity of VoIP, and the emerging nature of Voice over Wireless, has meant that attention has been turned to security. Some of this attention has been caused by concerns fanned by the security software industry itself and some is justified, particularly in the light of the imperfect history of security in the Wireless LAN market.

### Security is security is security

At one level the criticisms levelled at VoIP and wireless technologies are nothing new. There is an argument that the problem is not that these technologies are inherently insecure (or at least any more insecure than other IP networks) but that they have been poorly implemented. Like many other technologies early in their cycle they have often been set up as trials and as such have not come under the realm of normal, operational deployment. For wireless in particular, the technology has been so easy to install that many users have been installing networks in direct contravention of corporate policies designed to protect corporate network assets. As a result they have created a back door to main systems and increased their vulnerability to attack. Adding voice to a wireless network does not automatically make it insecure, it is the network itself and how it is implemented that defines the overall security envelope.

In the home and small business sector the problem has been compounded because many users without a network specialist to call on are incapable of configuring advanced levels of security functionality. They often have weak password implementations and leave the equipment with its "out of the box" naming conventions. Many Linksys wireless hubs can be found with the name still set to "linksys" or Cisco set to "tsunami". When combined with a password that complies with merely the minimum required to get the thing working, and access set to open it is not surprising that many of these networks are so easy to get on to.

## **“Warchalking” et al.**

With wireless networks so easy to access (you would hardly call it hacking), it was inevitable that users, keen to find a free method of access to the Internet on the move, would start to publicise these open doors. Thus the start of the practice known as “warchalking”, whereby the location of an open access point is “chalked” on a pavement or otherwise publicised. Software applications have also sprung open which help users find vulnerable networks and simplify the process of getting access to them.

## **Wireless Security**

The history of wireless security is effectively covered by two acronyms: WEP and WPA. Wired Equivalent Security (WEP) as its name suggested sought to provide an encryption equivalent to the security offered by the physical nature of wired LANs. However, it is possible to change the payload in WEP without knowing the key and a standards body was convened (802.11i) to address the issues. As this took longer than anticipated (4 years) the Wi Fi Alliance introduced an interim scheme, Wi Fi Protected Access (WPA). This implemented much of the 802.11i standard but was also backwardly compatible with early 802.11b adaptors. The key improvement from WEP was the use of Temporal Key Integrity Protocol (TKIP) which governs the change of keys while the system is in use.

## **Generic Security**

As with any IP network there are a whole set of sanctions available to the user to secure access to wireless systems.

## **Policy and passwords**

Clearly a security policy is only as good as its implementation and if staff deliberately contravene it organisations will need to consider their actions. Poor personal security and default usernames and passwords are an invitation for amateurs to access free resources, irrespective of any intent to cause damage.

## **Physical and MAC level security**

It makes sense to start from the physical network and work up when setting security standards. The standard for MAC level security is 802.1ae. The advantage of working at this level is that the same structure can be applied across a whole variety of different scenarios although it generally viewed as complex.

## **Firewalls and NAT**

While many users are protected within the boundaries of the corporate network, these levels of security are compromised as soon as they attempt to access central resources remotely. Personal firewalls in addition to network level firewalls are a sensible precaution as is using Network Address Translation to provide some level of protection of the internal IP address

structure. It should be noted that these precautions are far from infallible; they may only deter the casual intruder

### **DNS, DHCP and VLANs**

The standard methods of managing an IP address structure are Domain Name System (DNS) and Distributed Host Configuration Protocol (DHCP). DNS controls how a domain name (such as [www.broadbandvantage.com](http://www.broadbandvantage.com)) is translated to its underlying IP address and DHCP allocates IP addresses dynamically to users, meaning that you could have a different address every time you access the network. However once you are on the network DHCP will allocate you an address. These technologies are therefore not a guarantee of security - they are just part of the structure.

Virtual Local Area Networks (VLANs) are becoming increasingly popular as a way of securing networks when accessed from the Internet. Most VLANs employ some form of tunnelling technology to create a “private” pipe across the Internet and then encrypt the traffic passing through those pipes. From a VoIP perspective they also have the advantage of partitioning traffic so that different priority and Quality of Service (QoS) schemes can be implemented. There are both proprietary (viz, Cisco’s MPLS technology) and standards based implementations (802.1p and q)

### **Authentication and 802.11i**

The evolution of the various Wireless security schemes towards 802.11i, highlight the central need for authentication services. Authentication, the process by which someone’s identity is established on a network is the key first step in a process often called “AAA” which stands for Authentication, Authorisation and Accounting. As has already been identified User Names and Password schemes are only as useful as they are sophisticated; simple schemes are an open invitation. Much focus has been placed on the development of various security “Key” systems which provide electronic keys from a central secure resource. These keys change dynamically and provide a much more secure infrastructure for all IP services (not just VoIP) whether provided over a wired or wireless infrastructure.

The full 802.11i standard was agreed in June 2004.

### **Conclusion**

VoIP and Wireless security have to be considered in context of overall network security. Whilst Wireless LANs can be considered to be inherently insecure there are adequate tools available to deliver the appropriate level of security. VoIP is as secure as any other IP application given the provisos discussed in this paper.

## About the Author

### **Bob Cushing**

Bob combines 20 years experience in the IT and Telecoms industry with a keen interest in how technology changes the way we do things, especially at a personal and SME level. In demand as a public speaker and conference chairman, he has written a number of papers on the impact of technology on working practices. His company, Broadband Vantage provides consultancy in the Broadband marketplace and on marketing to SMEs. He is currently employed as CEO of Wired Workplace.

