

Voice over Wireless LAN Security

Ensuring Voice Quality in a Secure, Converged Wireless Network

Wireless LAN security presents a serious challenge: how to make wireless LANs secure without compromising application performance. Because wireless LAN security is a primary concern industry-wide, new standard and proprietary mechanisms for authentication, data encryption, and key management are being developed to address these concerns. However, these additional security measures may unintentionally affect performance for time-sensitive applications such as voice.

The security concern for voice applications has typically been low for two primary reasons: voice and data applications were on separate networks, and voice information is transient and not stored. For voice over wireless LAN applications, the first of these concerns is no longer valid. Installing a wireless LAN – even if it only to support voice clients – opens a network to potential unauthorized wireless access.

The wireless security mechanism defined in the original IEEE 802.11 wireless LAN specification is Wired Equivalent Privacy (WEP), which encrypts wireless data packets using a fixed key. The management limitations of a fixed encryption key, combined with well-publicized weaknesses in the WEP implementation, have led to near-term proprietary security enhancements and long-term security standards development.

Most proprietary security implementations add some form of authentication and key management to the existing WEP encryption to reduce the risks of unauthorized access and compromised encryption keys. Proprietary implementations that are designed around wireless data applications are usually not compatible with wireless voice devices for two reasons. First, they typically utilize special application software on the wireless client devices that requires an MS Windows-based operating system, which NetLink Wireless Telephones do not support. Second, proprietary security implementations require re-authentication each time the client device associates with a different access point. This re-authentication process takes from one half second to several seconds depending on network design. Because wireless telephone users frequently moving between access point coverage areas, they will experience significant breaks in the audio stream as the handset re-authenticates, severely degrading overall voice quality.

Security measures recently adopted by industry through the Wi-Fi Alliance, namely Wi-Fi Protected Access (WPA), and in-progress within IEEE Task Group I (802.11i), will also require re-authentication before handoff between access points and likely create unacceptable delays for voice applications. In order to make enhanced security features usable to voice handsets, a simpler handoff technique will be required when using these approaches.

SpectraLink is a significant contributor in both the IEEE 802.11 and Wi-Fi Alliance organizations. SpectraLink will implement enhanced security features as they are adopted by major industry players and the overall market, while encouraging the adoption of fast handoff mechanisms within the 802.11i standard. In the meantime, SpectraLink will implement WPA in NetLink Wireless Telephones to ensure interoperability with Wi-Fi certified access points, and work with WLAN infrastructure vendors to ensure access point handoff meets the low latency requirements of voice.

In addition, SpectraLink recommends increasing security by using policy-based solutions that allow for different levels of security by application type, such as edge controllers and VLANs. Third-party products on the market today, such as those from ReefEdge and Bluesoft, offer both enhanced network security and management capabilities for Wi-Fi networks.

As the market leader in voice over wireless LAN, SpectraLink is building awareness of the performance requirements of voice applications throughout the industry. Together with other application providers SpectraLink will grow the overall Wi-Fi market, creating new opportunities for wireless voice applications over secure, low-latency wireless networks.