Wireless VoIP Security Fundamentals

Written by Mark Collier

Wireless access, based upon various IEEE 802.11 standards, is commonly used in enterprise (and home) networks. Wireless access offers huge advantages, especially for mobile users, both within the office and when traveling outside the office. Geographically mobile users take advantage of wireless access to maintain connectivity while traveling through airports, at hotels, conferences, etc. This allows continual access to email, messaging, network services, Internet access, and now, VoIP. Wireless VoIP allows you to do many things, including:

Use a wireless handset and be able to take it with you as you move around the office. This offers great advantages in certain industries, such as retail, where users are mobile.

Use fixed mobile convergence (FMC) phones, which use 802.11 access when you are in the office and cellular access when you are outside the office.

Use a softphone on your laptop, so your office phone is available when you are online.

From a security point of view, security issues presented in wired VoIP are also present in wireless VoIP. The main difference is the need to secure the wireless link. Because wireless is broadcast over the air, depending upon the physical properties of the office, communications can be easily intercepted by attackers. Attackers can also attach themselves to the network, allowing illegitimate access and possible attacks. Additionally, attackers can masquerade as legitimate access points, tricking users into connecting to a rogue access point. Lastly, some users who do not have access to enterprise wireless can easily set up their own “rogue” access points.

Wireless VoIP security should include the same measures used to secure wired VoIP. In addition, it is essential to secure the wireless link, which is very vulnerable. Fortunately, there are wireless security standards available to secure this link.

The Wireless Threat

Wireless networks differ from their wired counterparts in that they are virtually impossible to physically secure. In a physically secure enterprise, it is difficult for an external attacker to enter the office and covertly connect a laptop to the network. With wireless, the signals are broadcast over the air, and can be easily intercepted by an attacker who is within range of the signals.

A common practice is for attackers to “war drive,” which involves an attacker driving around, using a standard wireless NIC, perhaps with a custom antenna, to detect available wireless networks. There are numerous tools, such as “netstumbler,” which make it trivial to identify and exploit poorly secured wireless networks. If you do not secure your enterprise wireless network, you have effectively installed an Ethernet switch in your parking lot, allowing anyone to connect and monitor your network.

Despite the availability of standards-based security, many enterprise wireless networks are completely unprotected. Simple countermeasures are available, such as hiding the network’s service set identifier (SSID), or locating wireless access points outside the corporate firewall, but these steps are not commonly employed.

The IEEE 802.11 specification includes wired equivalent privacy (WEP). Despite its availability for years, WEP is still not used by many enterprises. Furthermore, WEP has been proven to be weak, and tools are readily available to exploit its use.

An attacker who has access to unsecured traffic will be able to observe sessions, including VoIP signaling and audio. There are many available tools, including Ethereal, VOMIT, VoIPong, etc., which can be used to observe and record call signaling and audio.

If an attacker can gain access to the network through a non-secure wireless access point, they can use other tools to launch denial of service (DoS) attacks against the VoIP network. This is greatly simplified if softphones are allowed on, and VoIP signaling is allowed from, the virtual LAN (VLAN) on which the devices are located.

An attacker may also use a non-secure wireless network to gain access to the Internet. This may simply waste bandwidth, or the attacker may access objectionable material. Alternatively, the attacker may use the network to generate SPAM, launch DoS attacks, or with VoIP, make toll calls. The attacker may even use this access to allow others to make multiple toll calls.

In addition, any of the security issues described in previous columns are possible with wireless VoIP. If you use wireless handsets—and do not secure them—you are at great risk of eavesdropping and DoS attacks. If you allow softphones on laptops (or any wireless device)—and do not secure them—you likewise greatly increase the threat of attacks, such as DoS.

Wired Equivalent Privacy

WEP is part of the 802.11 standard, and is an early attempt at providing “link”-level security. Link-level security involves securing the over the air traffic between the wireless access point and device. It is not a substitute for other security measures, such as signaling or media encryption, which should still be considered.

WEP uses a secret key, shared between the communicating devices. WEP was designed to prevent eavesdropping, to provide a degree of access control, and data integrity. “Classic” WEP uses the RC4 cipher (encryption algorithm) with a 40-bit shared secret key. Many vendors have implemented later versions of WEP that support larger length keys.

Not long after its implementation, WEP was determined to be non-secure. Using readily available software, an attacker can collect a large sample of packets and recover the key. Once a key is recovered, it can be used to decrypt any and all traffic. The message integrity capability of WEP is also weak and easily exploited.

While WEP provides some security, and when coupled with larger keys and other technologies like 802.1X authentication is certainly better than no security at all, it is not recommended for enterprises, including those using wireless VoIP.

802.1X/Extensible Authentication Protocol

802.1X is an IEEE standard that allows authentication and key management for wireless (and wired) networks. 802.1X is used to control access to a network at the port level, and prevent

unauthenticated/unauthorized devices from gaining access to a network. 802.1X is not a cipher (encryption algorithm, like WEP, AES, etc.), but rather, it focuses on authentication. 802.1X provides a framework, referred to as the extensible authentication protocol (EAP), to allow different types of authentication to be used. This allows 802.1X-enabled clients, access points, and switches to support a variety of authentication methods, including passwords, tokens, smartcards, certificates, etc. 802.1X is generally integrated with a backend authentication/authorization/accounting server, such as a RADIUS server.

802.1X enables mutual authentication, which prevents a rogue device from connecting to the wireless network, and prevents a rogue access point from tricking a device into connecting to it.

WPA, WPA2, and 802.11i

Due to deficiencies in WEP, enterprises and vendors began to supplement WEP with third-party solutions, some of which are proprietary. Around the same time, the IEEE began work on 802.11i, which defines strong security for wireless networks.

In order to try to maintain compatibility among the various solutions, the Wi-Fi Alliance (a group of wireless vendors) defined WiFi protected access (WPA). WPA was defined as a forward-compatible standard, which includes portions of the 802.11i standard, particularly those portions which would run on existing wireless access point and device hardware.

WPA replaces WEP with a strong encryption technology called temporal key integrity protocol (TKIP). TKIP provides enhanced data encryption, including a per-packet key mixing function. TKIP also provides a message integrity check (MIC), extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA also uses the 802.1X/EAP standard for authentication, employing different authentication schemes for enterprise and home users. Home users generally use shared secret keys, whereas enterprises generally use a stronger authentication technology aided by a central server based on RADIUS.

WPA2 is now available, and reflects the full 802.11i specification. WPA2 is very similar to WPA, but includes support for the advanced encryption standard (AES), which offers stronger encryption suitable for use in the U.S. Government. Note that AES is more computationally intensive than other kinds of encryption, and may require various access points and devices to be upgraded.

As of today, most wireless access points and devices support WPA, and support for WPA2/full 802.11i is increasing. These standards, along with a strong 802.1X/EAP authentication method, should be used for enterprise-class security, especially when such a critical service as wireless VoIP is made available. Unfortunately, this type of security requires set up and configuration, and even though it is available, it isn’t widely used by enterprises.

Other Security Approaches

In addition to the link-level security offered by WEP, 802.1X/EAP, WPA, and WPA2/802.11i, other security approaches can also be used:

Virtual private networks (VPNs): connect wireless devices to the enterprise and provide authentication and encryption.

Signaling/audio authentication/encryption: protect communications between the IP phone/softphone, the IP PBX, and other IP phones/ softphones.

VoIP firewall: provides an additional layer of protection for the IP PBX, in response to the increased threat of rogue devices entering the network when wireless VoIP is available.

These approaches can be combined to offer "security embedded within security," where for example, the IP phone encrypts its audio and a standard such as 802.11i is used to authenticate and encrypt the wireless link. Such combinations may offer the best security, but due to multiple authentication and encryption operations, may introduce excessive latency for the audio.

Authentication can also be an issue when roaming between access points, resulting in temporary loss of audio (or in some cases, dropped calls). Standards are being developed to enable "fast handoff" and authentication when roaming across access points.

Conclusion

Wireless VoIP offers great advantages to mobile users. Mobile phone users in certain industries, such as retail, can reap significant benefits from wireless VoIP, as can geographically mobile users, such as sales personnel, whose softphone allows them to "travel" with their office phone.

Unfortunately, since wireless is broadcast over the air, it is difficult to secure and easily intercepted by attackers. Fortunately, there are now standards that allow the wireless link to be secured.

The recommended course of action is to secure your VoIP application—just as you would if it was wired—and use link-level security such as WPA or WPA2/802.11i.

Mark Collier is the CTO for SecureLogix. He has been developing voice/VoIP technology for over 10 years and is currently focused on VoIP vulnerability research and defining future technology for SecureLogix. He can be reached at mark.collier@securelogix.com.

Wireless VoIP security is the use of one or more protective strategies implemented by a company that uses VoIP technology for business-sensitive communications.Â Wireless VoIP security works to protect a company's network voice communications by preventing attacks before they happen and, in the event that an attack happens, being able to detect it and defend the network. If VoIP communications become compromised, voice quality can degrade, making a user's voice unintelligible and the system useless. Protecting a business's IT infrastructure from threats such as Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks is crucial to maintaining a working, efficient communication system. Voice over IP â€“ the transmission of voice over packet-switched IP networks â€“ is one of the most important emerging trends in telecommunications. As with many new technologies, VOIP introduces both security risks and opportunities. VOIP has a very different architecture than traditional circuit-based telephony, and these differences result in significant security issues. Lower cost and greater flexibility are among the promises of VOIP for the enterprise, but VOIP should not be installed without careful consideration of the security problems introduced. Administrators may mistakenly assume that... VoIP security threats. Choosing a secure VoIP provider. Healthcare VoIP security. Best practices for optimal VoIP security. The future of VoIP security. Final thoughts. Why VoIP security matters. Security is essential to every business. It doesnâ€™t matter if you have a large organization or a small business.Â Require Wi-Fi encryption. Activate WPA2 on your companyâ€™s wireless networks. Instruct employees also use this encryption for their Wi-Fi network. As a best practice, update your Wi-Fi password every year.