Spectralink Technical Bulletin

CS-15-06 - Understanding Wireless Security

Spectralink's 84-Series wireless phones meet the highest security requirements. By the time you deploy your 84-Series wireless phones, most of your basic security issues have already been ironed out by AP vendors and security servers to conform to federal regulations in place to protect personal privacy. Medical information, for example, is protected by HIPPA (Health Insurance Portability and Accountability Act) or PCI (Payment Card Industry). If you have general security questions after the deployment of your 84-Series phone, this best practices document should have the answers, or at least point you in the right direction.

System Affected

84-Series Handsets

Some Basics About Encryption and Authentication

On Wi-Fi networks there can be a trade-off between good security and good audio. The most rigorous enterprise-level security can protect against eavesdropping and unauthorized toll calls, but it can also increase server demand, resulting in latency and audio packet loss. Implementing less robust, personal-level security measures will reduce server processing demands, ease configuration, and smooth audio flow through your network, but may not provide adequate security for many enterprise Wi-Fi networks. The good news: Proper configuration of 84-Series phones offers the best of both worlds, ensuring excellent audio in the most robust security environments.

Table 1 highlights the correlation between security and audio relating to various Wi-Fi encryption and authentication techniques, with considerations for configuring the phones for the best security and audio.

Table 1: Enterprise Environment Security Trade-Offs

Wireless Security Method	*Security in Enterprise Environments*	*Audio*	*Ease of Configuration and Other General Information*
WEP	Poor	Excellent	Easy to administer, little processing overhead, adequate security for many home wi-fi networks. Easily compromised with hacking tools readily available on the internet. Every phone can decrypt every other phone's data. Still in use on some older enterprise networks.
WPA-PSK	Acceptable	Excellent to Good	Acceptable security for many small business wi-fi networks. Each phone negotiates a key (see TKIP below) with the AP so phones can't decrypt each other's data, although a sophisticated hacking device that knows the PSK can decode anyone's traffic. The problem can be minimized with periodic rotation of long, hard-to-hack passwords.
WPA2-PSK	Acceptable to Good	Excellent to Good	Good security for most small business wi-fi networks. Similar to WPA with the addition of AES/CCMP, one of the most secure encryption algorithms available. The PSK limitation is still an issue, however.
WPA2-Enterprise[1]	Excellent	Excellent to Poor	Excellent security for enterprise wi-fi network. PSK is replaced by some form of EAP and a RADIUS server, and each phone is configured with its own username and password, making the conversation between phone and AP completely private. The processing requirements of a RADIUS server, however, can compromise handoffs, so a fast-roaming technique such as OKC or CCKM must be employed.

[1]WPA2-Enterprise variables:

84-Series phones use three authentication types: EAP-FAST, PEAPv0 with MSCHAPv2 or EAP-TLS. EAP-FAST is used by products of Cisco, its creator, and by a growing number of other WLAN vendors. It uses a PAC file, which is similar to a certificate. PEAPv0 with MSCHAPv2 is the most common form of PEAP, which uses a certificate to authenticate the server. EAP-TLS is the most comprehensive EAP type by requiring client's to have their own certificates with which to authenticate to the network.

84-Series phones use either of two fast-handoff techniques as they roam among APs: CCKM or OKC. CCKM is used exclusively by Cisco APs. OKC is used by most non-Cisco APs.

Other Basic Security Concerns

Be aware of these basic security considerations while deploying 84-Series phones.

VLANs Robust, processing-intensive security methods disrupt voice, but not data. Voice and data traffic can be separated by dividing a physical WLAN into virtual networks (VLANs). Separate VLANs for data and for voice can alleviate the problem.

MAC filtering APs can be configured to allow or deny access to clients based on clients' MAC addresses. This technique can degrade AP performance and is discouraged for voice traffic on a WLAN, so it is discouraged when delploying 84-Series phones.

Firewalls Traffic-filtering abilities of firewalls can enhance security, but firewalls create jitter in audio and are likewise discouraged when deploying 84-Series phones.

Quality of Service (QoS) QoS is sometimes disabled to overcome a minor security flaw inherent in TKIP, a protocol used exclusively in WPA and optionally in WPA2. However, 84-Series phones and other latency-sensitive devices need QoS, which lets APs prioritize traffic and optimize the way shared network resources are allocated among different applications. Without QoS, all applications running on different devices have equal opportunity to transmit data frames. That works well for web browsers, file transfers, or email, but audio and video streaming are sensitive to latency increases and throughput reductions, and so require QoS.

A typical scenario While security deployment on a wi-fi network can be quite complex (assigning multiple SSIDs for different security types, or different security for remote users than for office users, or higher security levels for people in more sensitive positions…), a typical facility simply selects an optimum security method and applies it to all users. WPA-PSK and WPA2-PSK are easier to deploy and administer than WPA2-Enterpise and provide security that is good but not optimum. Someone outside the company who knows the network pass key (an ex-employee, for example) could hack into the network. In the most secure environments (WPA2-Enterprise), each 84-Series user has a username and password that are authenticated by a RADIUS server before the phone is allowed on the network. It is easy, then, for the adminstrator to revoke the credentials to restore seamless security, for example, when an employee leaves the company.

Administrators' Security Tips

Security settings on the 84-Series phone can be configured in several ways, but only one way is recommended.

Recommended: Load configuration files into the phone from the Wireless Configuration Station (WCS) computer via USB connection. (See Spectralink 84-Series Admin Guide)

Discouraged: Change security settings globally with configuration files broadcast to all phones from the Central Provisioning Server over a secure channel set up by with the WCS.

Discouraged: Change security settings on an individual phone either through the phone's menus or with the Web Configuration Utility (WCU).

Figure 2: Configuring 84-Series Series Phones for Security

Configuring all phones for security

Wireless Configuration Station (WCS)

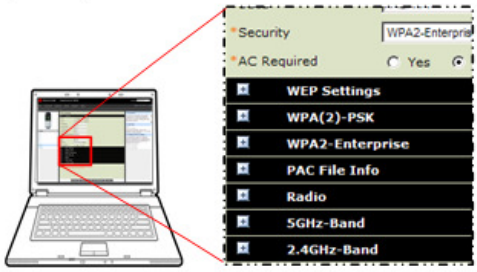
- ❑ Enable each phone for the wireless network (via USB).
- ❑ Create config files to define security for all phones on the network.
- ❑ Load the security information into each phone.
- ❑ Establish a secure communication channel for over-the-air provisioning by the Central Provisioning Server* (Not pictured)

Configuring a single phone for security (not recommended)

8400 phone

- ❑ Adjust security settings through the phone's Administration menus.

or…



Web Configuration Utility (WCU)

- ❑ Adjust a phone's security settings through a PC running the Web Configuration Utility. Choose **Settings > Network > Wi-Fi**

*Security settings are typically set only in the initial provisioning files loaded into the phone from the WCS via USB. Security settings could be included in the files that are broadcast to all phones over a secure channel from the Central Provisioning Server, but it is generally discouraged.

Which Tools to Use?

The wireless configuration station (WCS) and provisioning server are used to deploy a security system on the entire network initially, and then to change global settings in all phones from time to time, for example:

- When it's time to change network passwords or keys, such as the preshared key (PSK) in personal Wi-Fi Protected Access (WPA) networks.
- When upgrading security, for example, from WPA2-PSK to WPA2-Enterprise.

Such global security changes are made by configuration files containing configuration parameters such as

- device.wifi.wep.key1
- device.sec.TLS.profile.deviceCert1 or

- sec.TLS.customCACert.1

For more information about configuration parameters, refer to the *Spectralink 84-Series Deployment Guide*.

Admin Tip: Making Global Changes to Your Wireless Security System Network

To make global changes to your your wireless security system network, follow these steps:
1. Set up the APs to support two different security modes or keys (the old and the new),
2. Set the config files to change everything to the new mode or keys,
3. Wait awhile for all the phones to get the config update.
4. Disable the old settings on the APs.

The phone's administrative menus and the Web Configuration Utility (WCU) are rarely used for security changes on a phone. However, they might be used to troubleshoot a phone with improperly set security settings, or to try out several phones under different security settings. Under normal conditions, the phone's crucial security settings have already been defined for all phones by the config parameters and should not be changed on individual phones.

Procedures for Setting up a Default Wi-Fi Network Security Configuration Through the WCS

Security for the 84-Series phones on the Wi-Fi network is disabled by default until the administrator enables and defines it by changing configuration parameters while building configuration files for the Wi-Fi network. Use one of the following three procedures as you build your configuration files, depending on whether you are using WEP, WPA-PSK /WPA2-PSK, or WPA2-Enterprise.

Enter a WEP key

Some small legacy Wi-Fi networks employ WEP security, in which case the 84-Series phone's security feature can use up to 4 pre-shared encryption keys. These keys can be either 40 or 104 bits in length and must consist of only hexadecimal characters. The 84-Series phones do not support key rotation. During operation, only one key can be used by the phone.

Enter a PSK in WPA-PSK or WPA2-PSK mode

Most personal and small business Wi-Fi networks, and some enterprise networks, employ either WPA-PSK or WPA2-PSK security. For encryption, WPA-Personal uses TKIP, and WPA2-PSK uses AES/CCMP. In both cases, authentication is done with a PSK, which is a 64-character hexadecimal key. To make the key easier to configure, a password (sometimes called a

passphrase) 8-63 characters long and the SSID are used to create the PSK. The 84-Series phones can use either the PSK or passphrase form in the configuration.

Enter the EAP parameters in WPA2-Enterprise mode

Administering WPA2-Enterprise mode on the 84-Series phones involves not only selecting a fast-roaming handoff technique (OKC or CCKM), setting up an enterprise security name and password, but also selecting one of the three most common forms of EAP protocols— EAP-TLS (which requires client certificates), PEAPv0 with MSCHAPv2 (which requires a CA Certificate), or else EAP-FAST (which may require a PAC file to be manually loaded if it wasn't provisioned over the air). EAP-TLS requires that each client have a certificate that will be used to present itself to the authentication server as a valid user. PEAPv0 with MSCHAPv2 requires the provisioning of a root certificate. EAP-FAST requires a selection of either in-band or out-of-band provisioning. If out-of-band, then a PAC file needs to be provisioned, either through the configuration file or manually. Typically, Cisco networks use EAP and CCKM, while non-Cisco networks use PEAP and OKC.

Understanding Wireless Security Terminology

- **AAA** Authentication, Authorization and Accounting (see RADIUS).
- **AES** Advanced Encryption Standard is a cipher (encryption algorithm) used by WPA2 that uses the same key to encrypt and decrypt data. (see CCMP)
- **AP** Access Point is a receive-transmit device that facilitates data flow among wireless devices like the 84-Series phones in Wi-Fi networks.
- **CA** Certificate Authorities, used in WPA2-Enterprise security, issue digital certificates to establish a defined relationship of trust between the certificate creator (root CA) and the certificate users. Public CAs such as Verisign issue certificates to many enterprises, and some large enterprises create and issue certificates of their own, for exclusive use within the enterprise. In either case, the trust relationship is verified by validating the contents of all of the certificates in the certificate chain up to the root CA. The CA certificate is critical to defining the certificate path and usage restrictions for all end entity certificates issued for use in the PKI (see PKI).
- **CCKM** Cisco Centralized Key Management is a fast-roaming handoff technique (a proprietary version of OKC) used by Cisco APs that can reduce the need for a RADIUS server by authenticating the client without perceptible delay in voice or other time-sensitive applications. (see OKC and RADIUS)
- **CCMP** Counter-mode with Cipher-block-chaining Message-authentication-code Protocol (or Counter-Mode with CBC-MAC Protocol) is an encryption protocol used by AES for WPA2. AES/CCMP supersedes TKIP. CCMP uses CCM that combines CTR (Counter) for data confidentiality and CBC-MAC for authentication and integrity.
- **EAP** Extensible Authentication Protocol is an authentication framework used in WPA2-Enterprise that lets each protocol determine how to encapsulate messages. Some 40 EAP methods have been defined. Three of those methods—EAP-TLS (using client side certificates), EAP-FAST (using a PAC and proposed by Cisco to replace LEAP) and PEAPv0 with MSCHAPv2—are among the three most common and are supported by the 84-Series phones. EAP-TLS requires that the client have a unique certificate used to authenticate it to the network, PEAPv0 requires a server-side CA certificate, and EAP-FAST requires a PAC file, which is similar. (see CA and PAC)
- **MIC** Message Integrity Check in WPA/TKIP replaces WEP's CRC to insure integrity of each data packet sent on a Wi-Fi network.
- **OKC** Opportunistic Key Caching "opportunistically" shares cached PMKs with other APs so that as a client roams a PMK is already present on the target AP, and the client simply references the PMK ID in the reassociation request frame. This limits the involvement of the RADIUS server that can inherently retard the hand-off process. (see CCKM and RADIUS.)
- **PAC** Protected Access Credential, used in EAP-FAST, creates a TLS tunnel to verify client credentials.

- **PEAP with MSCHAPv2** Protected EAP with Microsoft's Challenge Handshake Authentication Protocol (version 2) is the most common form of PEAP and the only one supported by Cisco. (see EAP)
- **PKI** Public Key Infrastructure is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA). The user identity must be unique within each CA domain. The binding is established through the registration and issuance process, which, depending on the level of assurance the binding has, may be carried out by software at a CA, or under human supervision. (see CA)
- **PSK** Pre-Shared Key is a secret shared by two parties on a secure channel and is used in WEP and WPA-Personal standards so that all APs and their clients share the same key (a secret password or passphrase or hex string). Security from PSK can be effective (if it remains secret) or ineffective (if the PSK becomes known by hackers). WPA-PSK is superseded by WPA-EAP in enterprise environments. (see EAP)
- **QoS** Quality of Service lets APs prioritize traffic and optimize the way shared network resources are allocated among different applications. QoS is vital in deploying 84-Series phones, giving audio a high priority to avoid latency and lost packets. (see TKIP)
- **RADIUS** Remote Authentication Dial In User Service is a protocol used by a server to provide AAA functionality. A RADIUS server, especially if located in a remote location, can drastically slow down the handoff process, causing a loss of audio as an 84-Series phone moves among APs, a problem that is overcome with OKC or CCKM.
- **TKIP** Temporal Key Integrity Protocol is a security protocol used in WPA to supersede WEP and was superseded in turn by AES/CCMP used in WPA2. WPA uses TKIP, while WPA2 can use TKIP (for WPA2-Personal) or AES/CCMP (for WPA2-Enterprise). TKIP dynamically generates a new key for each packet (unlike the WEP key that remains static for the entire network), but has security flaws that can be overcome by disabling QoS and by using long, hard-to-hack, easy-to-remember passwords such as "!LovePar!$!n7he$pr!ng7!me." But QoS is required for audio, video, and other latency-sensitive applications, making TKIP a poor security choice when deploying the 84-Series in a large enterprise setting.
- **TLS** Transport Layer Security is a network protocol that supersedes Secure Sockets Layer (SSL).
- **WEP** Wired Equivalent Privacy is the first IEEE wireless LAN security standard, now easily hacked and being phased out. A WEP key is a 10-, 26-, or 58-hex-digit security code (e.g. 1B657D8FE3) chosen by the administrator and set on each Wi-Fi network device to allow devices to exchange encoded messages with each other while hiding the contents of the messages from easy viewing by outsiders. (see TKIP)
- **WPA** Wi-Fi Protected Access is a set of security standards newer and better than WEP. (Technically, WPA is a certification rather than a standard.) WPA2 using CCMP/AES encryption instead of TKIP is very secure. A WPA and WPA2 network can operate either in Personal mode, using a single network password (PSK), or in Enterprise mode (requiring a different password for each user).

Copyright Notice

Notice

Warranty

The *Product Warranty and Software License and Warranty* and other support documents are available at http://support.spectralink.com.

Contact Information

US Location
800-775-5330

Spectralink Corporation
2560 55th Street
Boulder, CO 80301

info@spectralink.com

Denmark Location
+45 7560 2850

Spectralink Europe ApS
Langmarksvej 34
8700 Horsens

infodk@spectralink.com