

# Wavesight & *Wireless Security*

Wavesight

[www.wavesight.com](http://www.wavesight.com)

## Executive Summary

Wireless networking is growing faster than almost any IT infrastructure ever has, and the lure is irresistible to enterprises and consumers alike -- providing flexibility, cost savings, and extended communications. With this unbridled expansion comes a pocketful of very real & new security concerns.

This paper details the foundation concepts and technologies of wireless radio networking and in doing so, seeks to highlight the various and industry significant security options already embedded on Wavesight's array of outdoor transmission solutions. For its part, Wavesight takes wireless security very seriously! In fact, in the absence of the now ratified security standards; Wavesight had itself developed very many unique layers of data security for use on its previous generations of products such as **Aries & Gemini**.

Today, with the adoption and integration of the very latest Wi-Fi security features (as options) and the array of proprietary data handling protocols built in; Wavesight's radios are perhaps the most secure radios available on the market. This paper will outline and succinctly detail the security package available on all Wavesight radio solutions.

## Industry Specific Security Standards

The wireless industry's security standards as they have emerged to date are:

- **MAC (or *Medium Access Control*) address filtering**
- **64, 128 and 152 bit WEP (or *Wired Equivalent Privacy*)**
- **802.1x / Radius support**
- **TKIP (or *Temporal Key Integrity Protocol*)**
- **WPA (or *Wi-Fi Protected Access*)**
- **Hardware Encryption for WPA - 802.11i**
- **AES (or *Advanced Encryption Standard*) - Full rate 128bit encryption/decryption.**

## Security Standards – Explained

### **MAC (or *Medium Access Control*) address filtering**

MAC filtering gives the user control over which computers or devices can be part of a network based on a physical address number that is uniquely assigned to a device by the hardware manufacturer. In process terms, MAC address filters allow or disallow the forwarding of unicast and multicast packets either sent from or addressed to specific MAC addresses. In activating this option; the user may create a filter that passes traffic to all MAC addresses except those you specify or they can create a filter that blocks traffic to all MAC addresses except those they specify. Most wireless routers and access points today allow you to enter a list of MAC addresses that are allowed to communicate on the network.

The management nightmare of maintaining a list of MAC addresses might be considered a worthy price if MAC address filtering were 100% secure. That, however, is not the case. MAC address filtering is easy to defeat for someone who has the right tools. Using a wireless sniffer, an attacker can watch the wireless traffic of your network and easily pick MAC addresses of valid users out of the frames floating through the air, even if they are encrypted. Then, they can simply modify the MAC address their OS sends out to mimic one of the stolen ones and your security is beaten.

For small, less security conscious wireless implementations, MAC address filtering might be considered a viable option if nothing else were available, since the management aspect is not as difficult to deal with. For larger wireless networks, however, MAC address filtering simply does not offer the level of security that might justify its enormous management overhead.

**Whereas, in many products, MAC addresses are software based and can be altered, Wavesight radios have MAC addresses that are 'burnt-in' and thus, do not allow for rogue addresses to be entered.**

## **64, 128 and 152 bit WEP (or *Wired Equivalent Privacy*)**

A WEP key is a 'token' of hexadecimal characters (0 - F) that provides an encryption key for securing data on a wireless network. Most people forego the use of 64-bit encryption and opt for the more secure 128-bit or higher methods.

WEP was intended to give wireless users a level of security equivalent to being on a wired network. With WEP turned on, each packet transmitted from one radio to another is first encrypted by taking the packet's data payload and a secret 40 bit number and passing them through a shredding machine called RC4. The resulting encrypted packet is then transmitted across the airwaves. When the receiving station hears the packet it then uses the same 40-bit number to pass the encrypted data through RC4 backwards, resulting in the host receiving good, useable data.

There are problems, however, with WEP in its 802.11b-ratified form that keep it from being the definitive answer to wireless security. The main problem with WEP is that the RC4 stream cipher used to encrypt the data has often been proven insecure because of technological weakness in its encryption mechanism. While cracking WEP keys is not a simple task, those with the right tools, know-how and enough patience can achieve it. If the keys used are sufficiently strong, however, it is more likely than not that anyone wanting to snoop around will move on to a network that is less secure!

**WEP is a standard feature today of all Wavesight radios and includes not only 64 and 128bit, but also an increased measure in 152bit encryption.**

## **802.1x / Radius support**

802.1x is a port-based network access control method for wired, as well as wireless, networks. The IEEE adopted it as a standard in August 2001. EAP handles the presentation of users' credentials, in the form of digital certificates (already widely used in Internet security), unique usernames and passwords, smart cards, secure IDs, or any other identity credential that the administrator is comfortable deploying. WPA allows flexibility in both the type of credentials that are used and in the selection of an EAP type. A wide number of standards-based EAP implementations are available for use, including AP Transport Layer Security (EAP-TLS), EAP-Tunneled Transport Layer Security (EAP-TTLS), and Protected Extensible Authentication Protocol (PEAP).

With EAP, 802.1x creates a framework in which devices mutually authenticate with the authentication server. This mutual authentication prevents users from accidentally connecting to "rogue" or unauthorized AP's on the wireless network and also ensures that users who access the network are the ones who are supposed to be there. When a user requests access to the network, the client sends the user's credentials to the authentication server via the AP. If the server accepts the user's credentials, the master TKIP key is sent to both the client and to the AP. A four-way handshake, a process in which the client and AP acknowledge one another and install the keys, completes the process.

For authentication to work, a user's transmission must get through to the back-end server performing the authentication. RADIUS (Remote Authentication Dial-in User Service) is a widely used authentication utility. The wireless client contacts the access point, which in turn communicates with the RADIUS server on the enterprise LAN. The RADIUS server then verifies the client's credentials to determine whether the device is authorised to connect or not. If the RADIUS server accepts the client device, the server sends data, including security keys, to the access point to enable a secure connection with the client.

**Radius support is a standard feature today of all Wavesight radios.**

## **TKIP (or *Temporal Key Integrity Protocol*)**

TKIP increases the size of the WEP key from 40 to 128 bits and replaces WEP's single static key with keys that are dynamically generated and distributed by the authentication server. TKIP uses a key hierarchy and key management methodology that removes the predictability which intruders relied upon to exploit the WEP key.

To do this, TKIP leverages 802.1x to produce a unique master, or "pair-wise" key for that computing session. TKIP uses this key and sets up a key hierarchy and management system, using the pair wise key to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated during that user's session. TKIP's key hierarchy exchanges WEP's single static key for some 500 trillion possible keys that can be used on a given data packet.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, the data is assumed to have been tampered with and the packet is dropped.

By greatly expanding the size of keys, the number of keys in use, and by creating an integrity checking mechanism, TKIP magnifies the complexity and difficulty involved in decoding data on a wireless network and thereby greatly increases the strength and complexity of wireless encryption, making it far more difficult — if not impossible — for a would-be intruder to break into a Wi-Fi network.

**TKIP is a standard feature today of all Wavesight radios.**

### **WPA (or *Wi-Fi Protected Access*)**

Designed to provide best-in-class enterprise security, WPA replaced WEP as the preferred Wi-Fi security solution and its emergence as a wireless standard represents a quantum leap forward in secure wireless transmission. WPA is built on standards-based interoperable security enhancements and not only provides exceptionally strong data encryption to correct WEP's weaknesses, it adds user authentication, thereby greatly increasing the level of over-the-air data protection and access control on both existing and future Wi-Fi networks. It is designed to secure all versions of 802.11 devices, including 802.11b, 802.11a, and 802.11g, multi-band and multi-mode. As a subset of 802.11i (also known as WPA2), WPA is both forward and backward compatible and is designed to run on existing Wi-Fi devices as a software download.

When properly installed, it provides users of wireless local area networks (WLANs) with a very high level of assurance that their data will remain protected and that only authorized users can access their networks. Cryptographers have reviewed Wi-Fi Protected Access and have verified that it meets its claims to close all known WEP vulnerabilities and provides an effective deterrent against known attacks. In the enterprise, WPA may be used in conjunction with an authentication server to provide centralised access control and management. Specifically, WPA uses the Temporal Key Integrity Protocol (TKIP) for encryption and employs 802.1x authentication with one of the Extensible Authentication Protocol (EAP) types available today.

**WPA is a standard feature today of all Wavesight radios.**

### **Hardware Encryption for 802.11i (WPA2)**

Like WPA, WPA2 uses the 802.1x/EAP framework as part of the infrastructure that ensures centralised mutual authentication and dynamic key management. Just like WPA, WPA2 is also designed to secure all versions of 802.11 devices, including 802.11b, 802.11a, and 802.11g, multi-band and multi-mode.

Additionally, however, WPA2 provides a new, encryption scheme, the Advanced Encryption Standard (AES) and uses Counter-Mode/CBC-Mac Protocols (CCMP). CCMP is a block cipher that encrypts 128-bit blocks of data at a time with a 128-bit encryption key (not to be confused with 128-bit WEP encryption). Like WPA, WPA2 relies on Pre-Shared Keys (PSK) to provide encryption.

**WPA2 is a standard feature today of all Wavesight radios.**

### **AES (or *Advanced Encryption Standard*) - Full rate 128bit encryption/decryption.**

AES has emerged as the encryption standard that is used globally to protect sensitive information. The U.S. Department of Commerce and the National Institute of Standards and Technology (NIST) have already formally adopted AES as the official US government standard. In fact, recent updates from the US National Security Agency, suggest that (as of Dec 2005) no successful attacks against AES have been recognised.

AES is defined by its counter cipher-block chaining mode (CCM) and supports the Independent Basic Service Set (IBSS) to enable security between client workstations operating in ad hoc mode. AES uses a mathematical ciphering algorithm that employs variable key sizes of 128-, 192- or 256-bits. Enterprises building new WLANs will without doubt find AES essential.

AES is by far the strongest commercial encryption standard available today and provides an unbeatable encrypted in-air data path.

**AES is a standard feature today of all Wavesight radios.**

## Wavesight Specific Security Layers

In addition to Wavesight's adoption of the very latest Wi-Fi security features (as options); two key feature sets, among an array of data handling protocols, have been integrated as standard on all Wavesight radios; the combination of which delivers unrivalled performance and super secure transmission. These protocols are:

### Super AG Mode

This mode brings into play, three key features of a Wavesight radio. Its origin lies in previous product developments and the functions incorporated in our chipsets by the largest silicon manufacturer of 802.11 radio devices, Atheros.

#### 1. Fast Frames

Fast Frames restructures the content of every frame by extending away from 802.3 frame constraints and variable characteristics. Gaps are removed giving a longer (super packet), which in turn provides for increased bandwidth performance and greater security. The structure of the super packet can only be read by another Wavesight device.

#### 2. Fast Frame Bursting

This co-exists with Fast Frames and provides contiguous Frames. Here, master frame header is set, which not only holds the details of individual frames, but also allows for contiguous frame transmissions without individual (FF) headers. The total number of Burst Frames is 8. Bursting in this way ensures the transmit time is kept to a very short interval while maintaining the minimum acknowledge request which, on conventional systems, will inevitably limit available bandwidth. Because bursting can only be detected and recognised by another Wavesight device, a high level of data security and resilience is therefore maintained.

#### 3. Compression

Before data is encapsulated into Fast Frames, it is compressed using LZ77 coding technique. This provides an additional layer to data security whilst transmitting on air.

## Unit Identification

Within Wavesight's control programme utility, (RFA), whilst in FWA mode, the Base unit can have its static tables adjusted to only communicate with identified stations. This is done within the MAC layer id process. When operating in AP mode, a similar method can be implemented on the client devices. Such security, as used in previous products, ensures that even if the various codes and SSID's are known, rogue units cannot connect or operate within the network.

## Conclusion

As a function of the world we live in today, all wireless infrastructures are vulnerable to insider curiosity, outsider attack, and attempted eavesdropping. Surprisingly, however, wireless infrastructures can be in fact, more secure than their wired counterparts! All wireless data security standards as defined are now fully implemented in the current firmware releases available for Wavesight's radios.



**Ronan Smith**  
Chief Executive



**Stephen Jordan**  
Chief Technology Officer