



Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

How Things Work: WLAN Technologies and Security Mechanisms

This is the paper I wish I had before I was asked to start rolling out a WLAN at my corporate office. I was looking for a single source containing detailed explanation of how wireless technologies operate and how wireless security mechanisms are implemented. Skimming through tons of articles and some books on wireless subject, I was frustrated to realize that they, at best, address a specific issue or, at worst, offer an opinion not supported by any facts. Unlike them, the goal of this paper is ...

Copyright SANS Institute
Author Retains Full Rights

AD

An advertisement banner for Rational. On the left, the word "Rational." is in white on a blue background, with the IBM logo below it. In the center, the text reads "TAKE BACK CONTROL OF YOUR APPLICATION SECURITY" in bold, with "YOUR APPLICATION SECURITY" in a larger font. Below this, it says "»»» DOWNLOAD A TRIAL VERSION OF RATIONAL APPSCAN". On the right, there is a small image of a man in a white shirt and tie, holding a red object.

Rational.
IBM.
TAKE BACK CONTROL OF
YOUR APPLICATION SECURITY
»»» DOWNLOAD A TRIAL VERSION OF RATIONAL APPSCAN

How Things Work: WLAN Technologies and Security Mechanisms

Abstract

This is the paper I wish I had before I was asked to start rolling out a WLAN at my corporate office. I was looking for a single source containing detailed explanation of how wireless technologies operate and how wireless security mechanisms are implemented. Skimming through tons of articles and some books on wireless subject, I was frustrated to realize that they, at best, address a specific issue or, at worst, offer an opinion not supported by any facts. Unlike them, the goal of this paper is to use specific facts and details to illustrate the concepts of wireless communication and wireless security mechanisms.

This paper explains the concepts of wireless communications based on the electromagnetic theory and introduces wireless standards and elements. The central part of this paper is the detailed discussion of the wireless security mechanisms: WEP, 802.1x, and WPA. Rather than labeling either of them as weak, strong, secure, or vulnerable, it describes specific functions they perform by analyzing algorithms, protocols, and parameters involved in each mechanism.

Table Of Contents

| | |
|--|-----------|
| <u>WIRELESS MEDIA</u> | 3 |
| <u>ELECTROMAGNETIC WAVES</u> | 3 |
| <u>DATA TRANSMISSION</u> | 3 |
| <u>WIRELESS NETWORKING STANDARDS</u> | 4 |
| <u>WLAN COMPONENTS</u> | 5 |
| <u>ACCESS POINTS (APs)</u> | 6 |
| <u>WIRELESS CLIENTS</u> | 6 |
| <u>WIRELESS SECURITY FEATURES</u> | 6 |
| <u>DISABLING SSID BROADCASTING</u> | 6 |
| <u>MAC FILTERING</u> | 7 |
| <u>WIRED EQUIVALENT PRIVACY (WEP)</u> | 7 |
| <u>Dynamic WEP</u> | 8 |
| <u>802.1x</u> | 9 |
| <u>RADIUS Protocol (RFC 2865)</u> | 10 |
| <u>RADIUS Support for Extensible Authentication Protocol (EAP)</u> | 10 |
| <u>Common Authentication Mechanisms Used by EAP</u> | 10 |
| <u>Utilizing EAP-TLS Handshake</u> | 11 |
| <u>Proprietary 802.1x Authentication</u> | 12 |
| <u>Choosing 802.1x Authentication Methods</u> | 12 |
| <u>WI-FI PROTECTED ACCESS (WPA)</u> | 13 |
| <u>802.1x Authentication</u> | 13 |
| <u>TKIP</u> | 13 |
| <u>AES</u> | 14 |
| <u>WPA-Compatible?</u> | 14 |
| <u>CONCLUSION</u> | 15 |
| <u>REFERENCES</u> | 16 |

WIRELESS MEDIA

ELECTROMAGNETIC WAVES

In a wireless network, devices communicate with each other via electromagnetic waves. Radio waves, along with microwaves, infrared waves, visible light, ultraviolet rays, X-rays, and gamma-rays, are all types of electromagnetic waves (or electromagnetic radiation). What distinguishes these types of waves is frequency, which is inversely proportional to wavelength: $\lambda = c/f$, where λ is a wavelength, f is frequency, and c is the speed of light (3×10^8 m/sec) [1].

The above wave types are listed in the order of increasing frequency meaning that, among all electromagnetic waves, radio waves have the lowest frequency range (corresponding to the longest wavelength). The above formula also implies that all electromagnetic waves travel with the speed of light. (In fact, this statement applies to waves in a vacuum since waves travel through various substances, such as air, with slightly lower speeds.)

Wireless network technologies utilize radio waves, microwaves, and infrared waves. The table below lists the frequency and wavelength numbers of the three wave types used by wireless networking [2].

| Wave Type | Frequency (Hz) | Wavelength (m) |
|-----------|---------------------------------------|---------------------------------------|
| Radio | $< 1 \times 10^9$ | $> 1 \times 10^{-1}$ |
| Microwave | $3 \times 10^9 - 3 \times 10^{11}$ | $1 \times 10^{-3} - 1 \times 10^{-1}$ |
| Infrared | $3 \times 10^{11} - 4 \times 10^{14}$ | $7 \times 10^{-7} - 1 \times 10^{-3}$ |

While infrared technology is utilized mostly to connect computer peripherals (wireless mice and keyboards), typical wireless office networks utilize frequencies of several GHz which puts them on the border line between radio waves and microwaves, which is why they may be referred to as either high-frequency radio waves or low-frequency microwaves.

One of the most significant disadvantages of lower frequency waves is susceptibility to electromagnetic interference (EMI) – a phenomenon of increasing or diminishing (depending on the phase difference) of the wave's strength when it is combined with another wave of the same frequency. This implies that any electronic device emitting waves at the same frequency as the wireless network equipment will affect the wireless communication. Among such devices are microwave ovens and cordless phones.

DATA TRANSMISSION

In order for the electromagnetic waves to carry digital data (0s and 1s), the waves need to be modulated. Modulation is a procedure of altering amplitude, frequency, or phase of the wave. (The opposite process is called demodulation) [3]. A modem (modulator-demodulator) is an example of a device performing these functions. The basic modulation techniques are:

- Frequency-Shift Keying (FSK)
- Amplitude-Shift Keying (ASK)
- Phase Shift Keying (PSK)

Depending on the algorithm, there are several variations to these methods [4]. Among those used in wireless networking are:

- Binary Phase Shift Keying (BPSK)
- Quadrature Phase Shift Keying (QPSK)
- Quadrature Amplitude Modulation (QAM)

Prior to modulation, the process called encoding is used to transform the frequency of the digital signals (usually in MHz range) into much higher frequency of the radio waves (usually several GHz). Encoding greatly speeds up the data transfer and prevents “wasting” of the bandwidth. (Otherwise, simply modulating a digital signal with the frequency of several MHz, would result in a wavelength of hundreds of meters.) The two encoding techniques used in wireless networking are:

- Orthogonal Frequency Division Multiplexing (OFDM)
- Direct Sequence Spread Spectrum (DSSS)

OFDM divides the allocated frequency range into sub-ranges (a.k.a. sub-carriers) which simultaneously transmit the pieces of the data stream. The more channels we have, the more data can be transmitted in parallel, the greater bandwidth can be achieved.

Depending on the bandwidth requirements, OFDM may employ phase-shift or amplitude-shift modulation methods [5].

DSSS increases the frequency of the digital signal by combining it with another signal of a higher frequency (known as the chipping code). In fact, the chipping code adds some security to the communication as the receiving end must know this code in order to encode the original digital data. The length of the chipping code determines how much data will be transmitted over a unit of time (i.e. the bandwidth). Various algorithms are used to generate the chipping code. One of the most sophisticated and widely used algorithms is Complementary Code Keying (CCK). DSSS usually employs PSK modulation methods (BPSK and QPSK) [6].

WIRELESS NETWORKING STANDARDS

The wave nature of the signal makes it clear that the communicating devices must operate at the same frequency and utilize the same encoding methods. Below are the basic characteristics of the three widely used WLAN standards [7].

| Parameters | Standards | | |
|-----------------------|--------------------------|--------------------|---|
| | 802.11a (Wi-Fi5) | 802.11b (Wi-Fi) | 802.11g |
| Frequency Range (GHz) | 5.15-5.35 5.725-5.825 | 2.4000-2.4835 | 2.4000-2.4835 |
| Encoding Method | OFDM | DSSS | OFDM (and DSSS for 802.11b compatibility) |
| Max Bandwidth | 54 Mbps | 11 Mbps | 54 Mbps |

This table demonstrates that OFDM encoding is more efficient than DSSS: operating over the same frequency range (2.4000 – 2.4835 GHz), 802.11g provides up to 54 Mbps bandwidth with OFDM, while 802.11b allows only up to 11 Mbps with DSSS. With OFDM encoding, different modulation methods yield different data rates. For example, 802.11a standard mandates certain data rates (such as 6, 12, 24 Mbps) which are accomplished by employing a corresponding modulation method [9]. BPSK or QPSK modulations are used for transmitting data rates up to 18 Mbps, while variations of QAM (16-QAM, 32-QAM) are used to deliver higher data rates [5], [9].

Comparing the frequency ranges for 802.11a and 802.11b/g technologies, we notice that 802.11a operates over the range of $(5.35 - 5.15) + (5.825 - 5.725) = 0.30 \text{ GHz} = 300 \text{ MHz}$, while that later two technologies have only $2.4835 - 2.4000 = 0.0835 \text{ GHz} = 83.5 \text{ MHz}$.

A wider frequency channel makes 802.11a a good candidate for voice and video transmissions, while 802.11b/g technologies are more suitable for wireless office and home networks [8].

Bluetooth is another wireless technology. It is used to connect peripherals (cell phones, PDAs) within a short distance from a computer. This paper will discuss only 802.11 technologies.

WLAN COMPONENTS

There exist two modes of WLAN operation: *infrastructure* and *ad-hoc* (a.k.a. *peer-to-peer*). The later one, as the name implies, enables to quickly setup a small wireless workgroup, while the *infrastructure* mode is used to incorporate wireless clients into the existing wired LAN infrastructure [10]. This paper discusses the WLAN features when in the infrastructure mode, and, hereafter, all references to WLAN assume this mode of operation.

ACCESS POINTS (APs)

An AP links wireless clients to the traditional wired LAN [10]. Depending on the technology (802.11a/b/g) and its implementation, a single AP may handle up to several hundred wireless clients [8], [11].

An AP and a wireless client can talk to each other only if they use the same SSID (System Set Identifier) – an alphanumeric string of up to 32 characters. SSID is often referred to as Network Name [11]. Most APs, by default, broadcast their SSIDs to advertise themselves to wireless clients. This feature is analogous to Windows NetBIOS broadcasts which allow a Windows client to browse the network locating Windows domains and workgroups without knowing their names. While a Windows network is still functional without such broadcasts, a user would need to know the name of a given resource to be able to connect to it.

When a wireless client is being configured, it locates all available APs (i.e. wireless networks) and has an option of choosing to which one to connect.

WIRELESS CLIENTS

A wireless client is a desktop, laptop, or handheld device with a wireless network card able to communicate with an AP. As mentioned above, the client needs to be configured (automatically or manually) to use the same SSID as the AP to which it is connecting.

WIRELESS SECURITY FEATURES

My research revealed that wireless security is one of the most misunderstood aspects of wireless technologies. The biggest misconception is that a strong security mechanism is all that needed. The complexity is caused by the fact that many wireless security mechanisms rely on the existing security and/or authentication frameworks (such as Active Directory) and will be useless without it. This section shows how a WLAN can be protected using various mechanisms including those already built into wireless components.

DISABLING SSID BROADCASTING

As mentioned above, APs, by default, broadcast their SSIDs to advertise themselves to the wireless clients. As a result, when joining a wireless network, the client can see a list of all available APs (in fact, their SSIDs) and decide which one to join.

This implies that any wireless device, within a proper distance from the AP, would be able to join the AP (and become part of the network). Disabling SSID broadcasting makes APs harder to identify [12]. A client will have to manually enter the SSID to join a specific AP. This applies to all wireless technologies (802.11a/b/g).

This measure is the first and the easiest step toward securing a wireless network.

MAC FILTERING

Another feature available on most wireless APs is MAC (Media Access Control) Address Filtering. It allows the AP administrator to create an ACL (Access Control List) on the AP with the MAC addresses of the wireless clients allowed to connect to this AP. This measure requires more effort since the administrator would need to collect the list of MAC addresses for all authorized wireless devices [12]. While a useful security measure for a small office, this may not be feasible for large enterprises.

WIRED EQUIVALENT PRIVACY (WEP)

WEP is the optional security feature specified by the 802.11 standard (which applies to 802.11a/b/g products). WEP offers encryption and/or authentication mechanisms between the AP and the wireless client. Both WEP authentication and encryption are based on the secret key shared between the AP and the wireless client. The 802.11 standard specifies two types of shared secret keys: 40-bit and 104-bit [10].

The encryption key is derived from the shared secret key combined with the 24-bit parameter called Initialization Vector. The length of the resulting encryption key is 64-bit for the 40-bit shared secret key or 128-bit for the 104-bit shared secret key [13]. The IV changes with every message, thus causing the new encryption key to be generated every time. The 802.11 standard does not specify how the IV is generated, and different WEP implementations use different IV generation algorithms. For this reason, IV travels in clear text with the encrypted message (a.k.a. cipher text) since the recipient needs to know the IV in order to generate the encryption key, but does not know how the sender generated its IV [18]. Typically, the IV is implemented as a counter incremented with every consequent message. In fact, the 802.11 specification does not mandate changing the IV with every message, all it says is that “the IV may be changed as frequently as every MPDU [Management Protocol Data Unit]”.

Unfortunately, when mentioning the key size, many publications do not specify whether they refer to the shared secret key or the encryption key and simply call it a “WEP key”. However, from my observations, most of the key sizes are given for the encryption keys. Another confusing fact is that some vendors support only one key size (for example, only 128-bit encryption keys, but not 64-bit encryption keys) or support additional key sizes (such as 152-bit extended encryption keys supported by NETGEAR 802.11a products [10]).

A typical WEP configuration, allows the AP to choose from the following three authentication modes:

- Open System (no authentication)
- Shared Key (hereafter is referred to as WEP Authentication)
- Both (any of the above)

WEP Authentication works as follows [10]:

- The client sends an authentication request to the AP.
- The AP sends a clear text message to the client.
- The client encrypts the message using its encryption key.
- The AP decrypts the message using its encryption key, compares it to the original text, and sends a success/failure response to the client.

In other words, WEP authentication may be described as the client's encryption test: only if the client has the same encryption key as the AP, will the client be authenticated. This, in turn, will happen only if the two share the same secret key.

If the AP is configured to use Shared Key Authentication, the clients must be configured to use the same authentication method, which implies that they have to be WEP-enabled. If the AP is configured to use any of the other two authentication methods, it will authenticate the client based on the client's preferred authentication method: (WEP) shared secret key or none (a.k.a. Open Authentication).

Similarly to authentication, the AP may or may not require encryption. WEP encryption uses the method called RC4 Cipher. Unfortunately, the RC4 Cipher can be cracked using some hacking tools available on the Internet, such as AirSnort [14].

Although WEP authentication and encryption are two independent functions, some implementations may not have an option of separating them. The typical AP WEP configuration options are [10]:

- Do not use WEP
- Use WEP for encryption
- Use WEP for Authentication and Encryption

While the last option lets us get the most out of WEP, the second option also makes sense given that WEP authentication utilizes WEP encryption. Some access points support authentication only option as well [10].

Dynamic WEP

The 802.11 standard does not specify several important aspects of the WEP mechanism:

- how the shared secret key is generated
- how it is distributed (it only suggests it is delivered "via a secure channel")

- the number of shared secret keys an AP can manage (it states that this number is “implementation-specific”)
- periodic key changes (a.k.a. key rotation or re-keying)

Due to the lack of standardization on these issues, various WEP implementations differ from each other based on how these procedures are handled. While some implementations assume the manual process for each of these steps, others automate one or more of these steps, thus, offering “Dynamic WEP”. Because these steps are independent and, hence, not all of them may be automated by a given implementation of WEP, the meaning of the “Dynamic WEP” term does not have a formal definition.

Typical Dynamic WEP automates at least key generation and distribution. Such automation usually relies on the 802.1x authentication discussed in the next section. The 802.1x authentication makes it possible because some of its authentication methods (such as EAP-TLS) generate the secret key for each client as the result of the authentication. With such implementation, the AP manages multiple shared keys – one for each client.

In addition to the key generation and distribution automation, some implementations automatically change the shared secret key and synchronize the change between the client(s) and the AP. Because there are no standards for this procedure, various algorithms and key timeout values are utilized.

Without automation, the WEP mechanism is referred to as “Static WEP”, and the shared secret keys are called “static keys” (vs. dynamic keys used by Dynamic WEP). Static WEP relies on manual key entry and distribution. The WEP configuration may also include an option to enter a text phrase from which the shared secret key will be derived [19]. Static WEP APs can usually handle only one or a few shared secret keys.

802.1x

The 802.1x specification defines the passing of authentication between a wireless client (supplicant), a wireless AP (authenticator, a.k.a. Network Access Server [NAS]), and a RADIUS Server (authentication server). As a result, the wireless client gets authenticated against the RADIUS server, and the AP plays the role of a pass-through device.

802.1x does not provide us with any authentication: all it does is gives the AP a capability to forward the client’s credentials to the RADIUS server and to forward the reply back to the wireless client. This functionality is accomplished by implementing the RADIUS and EAP protocols.

RADIUS Protocol (RFC 2865)

RADIUS (Remote Authentication Dial-In User Service) is a protocol which uses UDP packets to carry authentication and configuration information between the NAS and the RADIUS Server [15]. The authentication is based on the username, password, and, optionally, challenge-response. If the authentication is successful, the RADIUS server sends configuration information to the client including the necessary values to deliver the requested service, such as an IP address and subnet mask for PPP or a TCP port number for telnet [15].

There exist multiple RADIUS implementations – freeware as well as vendor-specific:

- Microsoft's IAS (Internet Access Service) which is included with Windows 2000 and Windows 2003 Server operating systems
- Cistron Radius Server for Linux, FreeBSD, OpenBSD, Solaris
- FreeRadius for UNIX-based systems

RADIUS Support for Extensible Authentication Protocol (EAP)

One of the RADIUS protocol limitations is that it can only implement password-based authentication: the password is transmitted either in the hash form (using MD5 hashing algorithm) or in the form of the response to a challenge (CHAP-password) [15]. The Extensible Authentication Protocol (EAP) gives RADIUS the ability to work with a variety of authentication schemes including Public Key, Kerberos, and smart cards [16].

The AP acts as the EAP-RADIUS translator between the wireless client and the RADIUS server. It uses the EAP protocol to communicate with the client and the RADIUS protocol to communicate with the RADIUS server. The AP encapsulates the information (such as a username or a public key) into the RADIUS packet and forwards it to the RADIUS server. When the server replies with Access-Accept/Reject/Challenge reply, the AP unpacks the RADIUS packet and forwards the reply back to the client in the EAP packet [16].

RFC 2869 (RADIUS Extensions) specifies the additional attributes set on the RADIUS packet to indicate to the RADIUS server that EAP protocol is being used. Since the EAP packet includes a field specifying what authentication method is to be used, the RADIUS server then acts on behalf of EAP and implements authentication by calling a designated routine [16].

Common Authentication Mechanisms Used by EAP

The two most widely used EAP authentication mechanisms are EAP-MD5 and EAP-TLS.

The EAP-MD5 algorithm consists of the following basic steps [17]:

1. The client sends the username to the server in clear text.
2. The server validates the username and sends the client a clear text message (called the challenge).
3. The client uses the MD5 hashing algorithm to produce a reply using the message text and the user password (so that the password itself isn't sent).
4. The server uses the same hashing algorithm (using the client's password stored on the server) to verify the reply.

As seen from these steps, although the password is not transmitted, it may be easy to crack since the entire conversation is in clear text. The EAP-MD5 authentication method is based on the previously existing CHAP (Challenge Handshake Authentication Protocol).

The EAP-TLS (Transport Layer Security) algorithm consists of the following steps [17]:

1. The client sends its identity (username or hostname) to the server in clear text.
2. The server validates the client's identity and sends the client the server's digital certificate (which includes the server's public key and the encryption cipher to be used).
3. The client verifies the server's certificate, generates a secret key and sends it to the server encrypted with the server's public key.
4. The server decrypts the message with its private key, derives the secret key, and sends the confirmation message back to the client encrypted with the secret key. This concludes the procedure known as the TLS Handshake [21]. (Because it closely resembles the SSL Handshake, these names are sometimes used interchangeably.) Along with this information, the server also requests the client's digital certificate.
5. The client sends its digital certificate to the server.
6. The server validates the client.

In order to implement EAP-TLS, all parties (the server as well as all clients) must obtain digital certificates. While it is possible to manually manage the certificates, large networks usually implement this with PKI (Public Key Infrastructure) servers.

While the two authentication algorithms above use different methodologies, they share one common step of transmitting the user identity in clear text from the client to the server. The obvious disadvantage of EAP-TLS is the need to manage client certificates. EAP-TTLS, discussed later, solves this problem.

Utilizing EAP-TLS Handshake

The first important use of the EAP-TLS authentication was briefly mentioned in the Dynamic WEP discussion: the authentication results in the generation of the secret key – the basis for WEP encryption. While this key is being transferred between the client and the RADIUS server, the AP gets hold of it, and now both, the AP and the wireless client, share the same secret key. Because EAP-TLS authentication is completely independent from WEP, there is no specification on how the key, generated by EAP-

TLS, becomes the WEP shared secret key. In fact, many articles refer to the dynamic distribution of WEP encryption (not shared secret) keys [17], [28]. According to the Orinoco Technical Bulletin, the AP uses the EAP-generated key (which it also refers to as the session key) to generate two encryption keys: for traffic from the clients to the AP and for traffic from the AP to the clients; these keys will be the same for all clients [17]. This implies that either the authors mistakenly refer to WEP shared secret keys as encryption keys, or that the WEP procedure of creating the encryption key (from the shared secret key and the IV) is not used.

Besides this, the EAP-generated secret key, establishes the secure tunnel between the client and the authentication server. EAP-TTLS (Tunneled TLS) uses this tunnel to carry on the client authentication using any authentication method, specifically, the one which would not require the use of clients' digital certificates (which would greatly simplify the administration). Depending on the second EAP authentication used inside the tunnel, there are several types of EAP-TTLS. One of them is PEAP (Protected EAP) - Microsoft's implementation of EAP-TTLS. It uses MS-CHAP-v2 authentication inside the tunnel to authenticate the user based on the Active Directory or Windows Domain user ID and password. Since many vendors started adapting PEAP, it is now undergoing the evaluation of the IEEE committee aiming to become a standard.

It should be noted that the encryption of the authentication channel during the EAP-TTLS conversation between the wireless client and the RADIUS server is not related to the WEP encryption between the client and the AP, even though both encryptions are, in fact, based on the same key.

Proprietary 802.1x Authentication

LEAP (Lightweight EAP) is Cisco's proprietary extension of EAP which uses user ID and password-based authentication. The authentication algorithm is similar to EAP-MD5 described above. However, the MD4 hashing function used by LEAP is weaker than MD5 [20]. Another disadvantage of LEAP is its proprietary nature: it is a part of the Cisco (only) wireless card driver. While LEAP does generate WEP keys, it does not offer dynamic key changes, i.e. the WEP key changes only with each re-authentication [17].

Choosing 802.1x Authentication Methods

While the AP is unaware of the specific authentication method (EAP-TLS, EAP-TTLS, EAP-MD5) and merely passes through the authentication conversation, both the wireless client and the RADIUS server must support a chosen authentication method. For example, Microsoft's 802.1x client for Windows 2000 supports EAP-TLS, PEAP-MS-CHAP v2, or PEAP-EAP-TLS authentication types, but it doesn't support Cisco's LEAP or EAP-MD5.

WI-FI PROTECTED ACCESS (WPA)

The WPA can be expressed as:
802.1x Authentication + TKIP + (optional) AES.

802.1x Authentication

WPA relies on the 802.1x authentication described in the previous section for authenticating wireless clients via a RADIUS server and generating the secret keys which are then used to create encryption keys. This implies that 802.1x must use an authentication method resulting in the secret key generation (such as EAP-TLS or EAP-TTLS). Because shared secret keys, generated as the result of 802.1x authentication are unique for each client, WPA-enabled APs will handle multiple keys.

To make WPA usable by small businesses and home offices, which do not have RADIUS-based authentication environment, 802.1x authentication may be replaced with the shared key authentication which resembles WEP authentication. This mode of WPA authentication is known as Pre-Shared Key (PSK) mode (vs. Enterprise Mode used with the 802.1x authentication) [22].

TKIP

TKIP (Temporal Key Integrity Protocol) is responsible for generating the encryption key, encrypting the message and verifying its integrity. Although the actual encryption is performed using the same RC4 Cipher algorithm as WEP [26], specific enhancements are added to create stronger encryption key and ensure that it 1) changes with every packet and 2) is unique for every client.

TKIP encryption keys are stronger than those of WEP because they possess the following features:

- they are 256-bit long [27]
- they are generated using a more sophisticated procedure [23]

While WEP encryption keys are, according to the 802.11 standard, either 64 or 128-bit long, TKIP encryption keys are 256-bit long. WEP generates the encryption key using the shared secret key and the IV (Initialization Vector) as an input. TKIP adds the transmitter's MAC address to the list of the input parameters which implies that all senders will have different encryption keys [23]. Furthermore, TKIP increases the size of the IV from 24-bit (used by WEP) to 48-bit and mandates that it is used as a counter (also called TSC – TKIP Sequence Counter), which guarantees that it will only be reused once for every 281,474,976,710,656 (2^{48}) packets [23]. (Recalling from the WEP discussion, WEP did not specify an IV generation algorithm; while some vendors did implement it as a counter, others used less sophisticated procedures resulting in frequent IV repetitions, i.e. the same encryption keys.)

Like in WEP, the shared secret key is one of the input parameters for the encryption key generation, and WPA mandates its length to be 128 bits (vs. 40 or 104 bits in WEP) [23]. TKIP automatically changes this key, by default, every 10,000 packets [24]. The original shared secret key is called the Pairwise Master Key (PMK) or, simply, Master Key, while keys resulting from its periodic changes are called Temporal Keys [22], [24], [26].

AES

AES (Advanced Encryption Standard) is an optional WPA component. In 2002, AES replaced DES (Data Encryption Standard) as a part of the Federal Information Processing Standard which is mandatory for protection of sensitive unclassified federal information and may also be used by businesses in the US and world-wide.

The upcoming 802.1i security specification (which WPA is part of), will introduce new encryption algorithms: Wireless Robust Authentication Protocol (WRAP) and Counter with Cipher Block Chaining Message Authentication Code Protocol (CCMP) [25].

WPA-Compatible?

Although this paper aims to provide an un-biased view, I could not keep from adding this paragraph. It is not about how to make devices WPA-compatible. (Numerous articles cover this subject.) It is about the meaning of the WPA-compatibility. Apparently, some wireless devices marked as WPA-compatible (such as Microsoft's Wireless Base Station MN-700) provide only 256-bit WPA encryption in PSK authentication mode, i.e. they do not support 802.1x authentication. (Be aware.)

CONCLUSION

The number of bibliography entries at the end of this paper is a good proof of the lack of information sources encompassing all wireless concepts and features in one place. This paper aims to be one of such sources. The author attempted to help a reader build a framework of knowledge – a necessary ground for successful completion of any project (whether technical or not). As many companies are preparing to roll out wireless networks, a lot of decisions are to be made about which technologies to choose and how to make the networks secure. The author hopes that, combined with practical skills and experiences, this knowledge framework will help the readers to correctly interpret technical specifications, ask the right questions, and make informed decisions. (Needless to say, these qualities make the author extremely unpopular in the sales community.)

© SANS Institute 2004, Author retains full rights.

REFERENCES

- [1] The Imagine Team. "Electromagnetic Spectrum." High Energy Astrophysics Science Archive Research Center.
URL: http://imagine.gsfc.nasa.gov/docs/science/known_1/emspectrum.html
(7 Nov. 2003)
- [2] The Imagine Team. "Regions of the Electromagnetic Spectrum." High Energy Astrophysics Science Archive Research Center.
URL: http://imagine.gsfc.nasa.gov/docs/science/known_1/spectrum_chart.html
(7 Nov. 2003)
- [3] "Data Communications Technology." Understanding Networking Technologies. Course Manual. Chapter 5. Atrium Technical, Inc.
URL: <http://www.netguru.net/courses/ntc/NTCC5.htm> (7 Nov. 2003)
- [4] "Wireless Technologies." Internetworking Technologies Handbook. Chapter 20. Cisco Systems, Inc.
URL: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/wireless.pdf
(7 Nov. 2003)
- [5] "Wireless Technology." Allied Telesyn International Corp.
URL: <http://www.alliedtelesyn.com/allied/marketing/wireless/technological.htm>
(7 Nov. 2003)
- [6] "80211b Modulation." Vocal Technologies, Ltd. 22 October 2003.
URL: http://www.vocal.com/data_sheets/80211b_mod.html (7 Nov. 2003)
- [7] "High-Speed Wireless LAN Options." Wireless LAN Association.
URL: <http://www.wlana.org/pdf/highspeed.pdf> (7 Nov. 2003)
- [8] "Wireless Comparison Information." NETGEAR, Inc.
URL: http://www.netgear.com/pdf_docs/WirelessInfoev4.pdf (7 Nov. 2003)
- [9] "802.11a Technology Overview." Stanford University Communication and Networking Services.
URL: <http://www.stanford.edu/group/networking/NetConsult/wireless/80211a.html>
(7 Nov. 2003)
- [10] "Wireless Networking Basics." NETGEAR, Inc.
URL: <http://www.netgear.com/docs/refdocs/Wireless/wirelessBasics.htm>
(7 Nov. 2003)
- [11] "Wireless Ethernet." Intel Corporation.
URL: <http://www.intel.com/english/home/trends/wireless/info/ethernet.htm>
(7 Nov. 2003)
- [12] Farshchi, Jamil. "The Essential Components of a Wireless Policy." Wireless Network Policy Development. Part Two. Symantec Corp. 10 October 2003.
URL: <http://www.securityfocus.com/printable/infocus/1735> (7 Nov. 2003)
- [13] Schenk, Rob. Garcia, Andrew. Iwanchuk, Russ. "Wireless LAN Deployment and Security Basics." ExtremeTech.com.
URL: <http://www.extremetech.com/article2/0,3973,1073,00.asp> (7 Nov. 2003)
- [14] Townsend, Kevin. "Management Guide to Securing Your Wireless LAN." BlueSocket, Inc. 2003

- [15] Network Working Group. "RFC 2865 – Remote Authentication Dial In User Service (RADIUS)." Internet RFC/STD/FYI/BCP Archives. Request for Comments 2865. June 2000. URL: <http://www.faqs.org/rfcs/rfc2865.html> (7 Nov. 2003)
- [16] Network Working Group. "RFC 2869 – RADIUS Extensions." Internet RFC/STD/FYI/BCP Archives. Request for Comments 2869. June 2000. URL: <http://www.faqs.org/rfcs/rfc2869.html> (7 Nov. 2003)
- [17] "Principles of 802.1x Security." ORiNOCO Technical Bulletin 048/B. Agere Systems Inc. April 2002.
- [18] "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications." ANSI/IEEE Std. 802.11. 1999 Edition.
- [19] "WUA-400 AeroPad Manual for PC." User Manual. Xsense Connectivity, Inc. 2002.
- [20] "What Are MD2, MD4, and MD5?" Techniques in Cryptography. RSA Laboratories' Frequently Asked Questions about Today's Cryptography 4.1. Chapter 3. RSA Security Inc. URL: <http://www.rsasecurity.com/rsalabs/faq/3-6-6.html> (7 Nov. 2003)
- [21] "How TLS Provides Security." Product Documentation. IONA Technologies. 2003. URL: <http://www.iona.com/support/docs/orbix2000/2.0/tls/html/Intro3.html> (7 Nov. 2003)
- [22] "Wi-Fi Protected Access." Overview. Wi-Fi Alliance. 2002.
- [23] Leira, Jardar. "TKIP and MIC." UNINETT. URL: http://www.uninett.no/wlan/kip_mic.html (7 Nov. 2003)
- [24] Edwards, Mark. "Increasing Wireless Security with TKIP." Security Administrator. Windows & .NET Magazine. 23 October 2002. URL: www.secadministrator.com/Articles/Index.cfm?ArticleID=27064 (7 Nov. 2003)
- [25] Lawson, Stephen. "Wi-Fi Group Lays out Better Wireless Security." InfoWorld. 31 October 2002. URL: <http://archive.infoworld.com/articles/hn/xml/02/10/31/021031hnwifi.xml> (7 Nov. 2003)
- [26] LaRosa, John. "WPA: A Key Step Forward in Enterpriser-class Wireless LAN (WLAN) Security." White Paper. Meetinghouse Data Communications, Inc. 26 May 2003. URL: http://www.mtghouse.com/MDC_WP_052603.pdf (7 Nov. 2003)
- [27] Loeb, Larry. "Roaming Charges: Out with the WEP, in with the WPA." IBM Corp. 18 June 2003. URL: <http://www-106.ibm.com/developerworks/wireless/library/wi-roam11/> (7 Nov. 2003)
- [28] "Cisco Aironet 350 Series Access Points." Data Sheet. Cisco Systems. 2001.



Upcoming SANS Training

[Click Here for a full list of all Upcoming SANS Events by Location](#)

| | | | |
|---|------------------------|-----------------------------|------------|
| SANS SOS London 2009 | London, United Kingdom | Jul 13, 2009 - Jul 18, 2009 | Live Event |
| SANS Future Visions 2009 Tokyo | Tokyo, Japan | Jul 15, 2009 - Jul 17, 2009 | Live Event |
| SANS IMPACT 2009 | Kuala Lumpur, Malaysia | Jul 27, 2009 - Aug 01, 2009 | Live Event |
| SANS SEC563: Mobile Device Forensics Debut | Baltimore, MD | Jul 27, 2009 - Jul 31, 2009 | Live Event |
| SANS Boston 2009 | Boston, MA | Aug 02, 2009 - Aug 09, 2009 | Live Event |
| SANS WhatWorks in Virtualization and Cloud Computing Security Summit 2009 | Washington, DC | Aug 17, 2009 - Aug 21, 2009 | Live Event |
| SANS Atlanta 2009 | Atlanta, GA | Aug 17, 2009 - Aug 28, 2009 | Live Event |
| SANS Virginia Beach 2009 | Virginia Beach, VA | Aug 28, 2009 - Sep 04, 2009 | Live Event |
| SANS SCDP SEC556: Comprehensive Packet Analysis - Sept. 2009 | Ottawa, ON | Sep 09, 2009 - Sep 10, 2009 | Live Event |
| SANS Critical Infrastructure Protection at Oceania CACS2009 | Canberra, Australia | Sep 10, 2009 - Sep 11, 2009 | Live Event |
| SANS Network Security 2009 | San Diego, CA | Sep 14, 2009 - Sep 22, 2009 | Live Event |
| SANS SCDP Cutting Edge Hacking Techniques - June 2009 | Ottawa, ON | Sep 15, 2009 - Sep 15, 2009 | Live Event |
| SANS Rocky Mountain 2009 | OnlineCO | Jul 07, 2009 - Jul 13, 2009 | Live Event |
| SANS OnDemand | Books & MP3s Only | Anytime | Self Paced |