Wireless Security Hodgepodge

Glenn Royster
A+, Network+, A.A.S., B.S., M.S.

ABSTRACT

During the infancy of the wireless computing age, key defenses and deterrents to wireless attacks were the cost and complexity of methods required to partake in such activities. The current age of easily accessible, inexpensive tools have tilted the balance of price, complexity, and deterrence in favor of the novice wireless attacker. During year 2005, over a billion wireless users are projected (Lauter, 2004). As of this writing, the wireless security discussion is in escalation. This paper is a brief participant of the discussion, and concludes multiple security mechanisms (a hodgepodge, instead of a single solution) provide maximum wireless security.

INTRODUCTION

In terms of data transfer from device to device, wireless communication poses concerns that are common to wired devices. Such concerns include DoS, authentication of users, increased risk of intruders, human error of administrators, and unknowingly introduction of viruses by authorized users (Feil, 2003). Although both wired and wireless communications have security risks, wireless requires unique consideration because of its medium ("air"). Radio waves afford users increased mobility while at the same time providing attackers easier access. Depending upon location, environment, and facility construction, IEEE 802.11 signals can travel 150 to 1,000 feet. Unlike wired networks that route signals within the confines of physical properties such as cabling, NICs, and processors, wireless signals are present to everyone and everything that is within range. Not only did early IEEE standards not emphasize security, but also several design errors impact wireless security issues that have become prominent (Arbaugh, 2003). At the onset of the mobile computing phenomena, PDAs, smart phones, and other similar devices were developed without major consideration for security (Miller, 2001). As a result, this hurdle is still being overcome.

A BRIEF LOOK AT THE IEEE 802.11 FAMILY

802.11a wireless devices operate in the 5 GHz band. The orthogonal frequency-division multiplexing method is used to generate the signal. The prime difference between OFDM and frequency-division multiplexing (FDM) is each sub-band is used by one source at a given time in OFDM. In the case of OFDM, there are 52 sub-bands; 48 are dedicated to transmitting data and 4 are reserved for control information (Forouzan, 2004). There are 12 non-overlapping channels, 4 reserved for point to point and 8 reserved for indoor (Wikipedia, nd). OFDM employs quadrature amplitude modulation (QAM) to achieve a maximum data rate of 54 Mbps (Forouzan, 2004). The data rate is stepped down to 48, 36, 24, 18, 12, 9 or 6 Mbps, in correlation with device to device signal attenuation. The 5 GHz frequency of 802.11a provides signals that are less susceptible to interference than the 2.4 GHz band of 802.11b and 802.11g devices. However, the higher frequency of 802.11a limits signals to almost line of sight and requires more access points (Wikipedia, nd). The range for 54 Mbps throughput is about 30 to 50 feet; throughput at 6 Mbps can travel about 200 to 275 feet (Kapp, 2002).

The maximum data rate of **802.11b** is 11 Mbps, with step down rates of 5.5, 2, and 1 Mbps (Wikipedia, nd). The signal generation technique is high-rate direct sequence spread spectrum (HR-DSSS). Complementary code keying (CCK) is the component of HR-DSSS that distinguishes it from DSSS. In the CCK procedure, 4 or 8 bits are encoded to one CCK symbol. The 1 Mbps and 2 Mbps data rate modulations are compatible with DSSS. The bifurcation with DSSS comes when 4-bit and 8-bit CCK encodings are used to produce respective 5.5 Mbps and 11 Mbps data rates (Forouzan, 2004).

Both 802.11b and **802.11g** have 14 channels with center frequencies that are 5 MHz apart. Channels 1, 6, and 11 are non-overlapping and enable multiple networks to co-exist in close proximity without interference (Wikipedia, nd). 802.11g uses DSSS to produce 1, 2, 5.5, and 11 Mbps data rates.

To produce 6, 9, 12, 18, 24, 36, 48, and a maximum data rate of 54 Mbps, OFDM is used. The IEEE standard also specifies optional Packet Binary Convolutional Coding and a combination, DSSS-OFDM, signal generation technique (Vassis, Kormentzas, Rouskas, & Maglogiannis 2005).

The below table is a quick reference of other IEEE 802.11 standards. For more details, the reader is encouraged to reference http://ieee.org .

IEEE 802.11	Uses FHSS or DSSS and transmits at 1 or 2 Mbps in the 2.4 GHz RF and IR standard
IEEE 802.11d	International (country to country) roaming extensions
IEEE 802.11e	Enhancements: QoS, including packet bursting
IEEE 802.11f	Inter-Access Point Protocol (IAPP)
IEEE 802.11h	Spectrum and transmit power management extensions in the 5 GHz band in Europe
IEEE 802.11i	Enhanced security
IEEE 802.11j	4.9 GHz-5 GHz operation in Japan
IEEE 802.11k	Radio resource measurements
IEEE 802.11n	Higher throughput improvements (projected to be 4 to 5 times faster than 802.11g.
IEEE 802.11p	WAVE - Wireless Access for the Vehicular Environment (such as ambulances and passenger cars)
IEEE 802.11r	Fast roaming
IEEE 802.11s	Wireless mesh networking
IEEE 802.11t	Wireless Performance Prediction (WPP) - test methods and metrics
IEEE 802.11u	Inter-working with non 802 networks (e.g., cellular)
IEEE 802.11v	Wireless network management

(The IEEE, Inc. 3 Park Avenue, New York, NY 10016-5997, USA; Internet.com, nd; Wikipedia, nd)

WARDRIVING, WARFLYING, AND WARCHALKING

One of the early steps to intruding 802.11 signals is discovery. Whether done for fun, stolen Internet access, or identification of hacking targets, wardriving is a reconnaissance method that yields big dividends. During the early days of the phenomenon, wardrivers would roam in their automobiles in search of signals, using a laptop or other device that detects 802.11 broadcasts. Other tools of the trade included pencil/pen, pad, and/or map to record signal locations. Wardriving is now automated. The latest evolution involves a laptop, dedicated software, and GPS. Warflying is basically the same process as wardriving, the primary difference being the use of aircraft instead of automobile. However, warflying popularity is restricted by access to aircraft. Another obstacle to successful warflying is the limited range of current 802.11 signals, which requires low flying. Wardriving and warflying are significant enough to spawn dedicated Web sites; some sites are replete with maps that provide details such as SSIDs. The following are sites dedicated to warflying and wardriving: http://www.worldwidewardrive.org , http://www.wardriving.com , and http://www.wardrivingisnotacrime.com

Warchalking is similar to warflying and wardriving. The method of reconnaissance is the same. However, instead of electronic graphics or paper to display 802.11 locations, marks are place on buildings and sidewalks to indicate the presence of 802.11 signals. During the Great Depression, hobos used this form of communication to signal friendly homes. It is believed that chalk is the warchalker's preferred marking tool because it is temporary and may lessen the chances of being prosecuted for defacing property. (Lawrence & Lawrence, 2004; Thomas, 2004)

TOOLS: WIRELESS HACKING MADE EASY

Wireless stations must have a method to locate access points (APs) that are in range of communication. To facilitate this process, APs are required to constantly broadcast their capabilities. The location process that occurs between wireless stations and APs are impossible to mask. This is deemed an acceptable risk. And unfortunately, attackers can use these signals as a means to discover new victim targets (Feil, 2003). Popular tools of discovery include **NetStumbler** (Windows), **MacStumbler** (Mac), and **MiniStumbler** (Pocket PC). These programs learn the location, signal strength, MAC address, SSID, vendor, and channel of devices (Neilson, nd). As an added bonus, the software also detects whether WEP is enabled or disabled on devices. Both NetStumbler 0.4.0 and MiniStumbler 0.4.0 are free downloads and can be used to detect output from 802.11a, 802.11b, and 802.11g systems (NetStumbler, nd). MacStumbler 0.75b is also a free download, but can only display information about 802.11b and 802.112g systems (MacStumbler, nd). The xStumbler software is GPS friendly, which warrants it a must-have for the wardriver's arsenal.

Perhaps a method that somewhat mitigates signal cipher is limitation of signal strength. Higher-end APs such as Cisco 350, 1100, and 1200 series

allow wireless network administrators the capability to control the signal range, especially in effort to restrict signals extending beyond the perimeter of the organization (Thomas, 2004). However, to improve signal gathering, an intruder only needs about $5 worth of materials, 10 minutes of time, and easily accessible know-how to build **a big antenna** from cans. Such simple homemade accessories facilitate capture of low-powered 802.11 signals. An attacker may double the reception range by building a directional (sometimes called yagi) antenna of a Pringles can, steel rod, and washers. Also, a helical antenna constructed of PVC pipe and copper wire doubles the reception range. Within the right conditions, 802.11 signals can be captured miles away from the AP (Welch & Lathrop, 2003b). The reader can peruse the following site to ascertain the simplicity and low cost of wireless network antenna construction information: http://www.turnpoint.net/wireless/cantennahowto.html. The reader can also peruse the following site to ascertain how easy it is for the less construction savvy signal hunter to purchase powerful add-on wireless network antennas that are priced under $100 and as low as $30: http://antennasystems.com/broadband.html

Wired Equivalent Privacy (WEP) protocol was designed to give wireless networks an equivalent level of security as that realized by wired LANs (Internet.com, nd). The security protocol is based on the RC4 stream cipher, which uses the same key for both encrypting and decrypting data (Craiger, 2002). Borisov, Goldberg, and Wagner (2001) conveyed WEP was designed to achieve three security goals:

- *Confidentiality: The fundamental goal of WEP is to prevent casual eavesdropping.*
- *Access control: A second goal of the protocol is to protect access to a wireless network infrastructure. The 802.11 standard includes an optional feature to discard all packets that are not properly encrypted using WEP, and manufacturers advertise the ability of WEP to provide access control.*
- *Data integrity: A related goal is to prevent tampering with transmitted messages; the integrity checksum field is included for this purpose.*

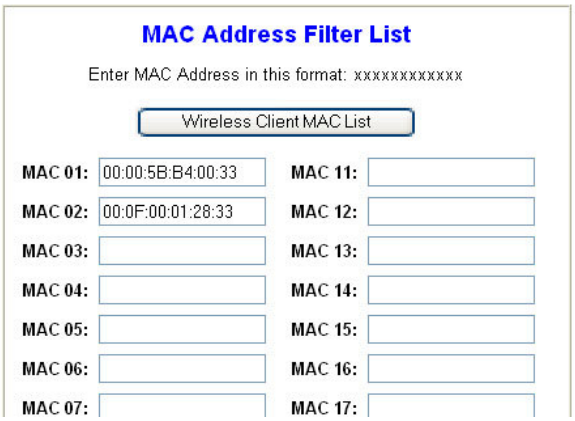
The basic framework of the WEP protocol centers on encrypting radio wave data between terminals (Internet.com, nd). A core component employed by WEP is the combining of the 40 or 104 bit secret key with a 24 bit Initialization Vector (IV) that is randomly generated. The combining of the secret key and IV provides 64 or 128-bit encryption. The small IV enables the WEP protocol to be easily compromised. Without going into greater detail, and in the interest of brevity, the reader should ascertain that 128-bit WEP is no more secure than 64 bit WEP (Thomas, 2004). The WEP protocol has inherent flaws which allow attackers to decrypt and/or add forged information to the supposedly protected transmissions. A major restriction to an attacker's ability to intrude transmissions wrapped by WEP is the attacker's capacity to capture transmissions and convert them to human readable form (Craiger, 2002). As will be discussed later, sniffing and converting transmissions are quite rudimentary tasks that require easily accessible low-cost or free resources.

WEP2 was developed to enhance the original WEP protocol. The major difference between WEP and WEP2 is the former does not include mandatory enforcement of 128-bit keys, nor does it support Kerberos 5. Yet, WEP2 is still problematic. It still has vulnerabilities, such as allowing IV replay attacks, not preventing plaintext attacks, and making the protocol susceptible to dictionary-based attacks because of mandatory support for Kerberos 5 (Craiger, 2002).

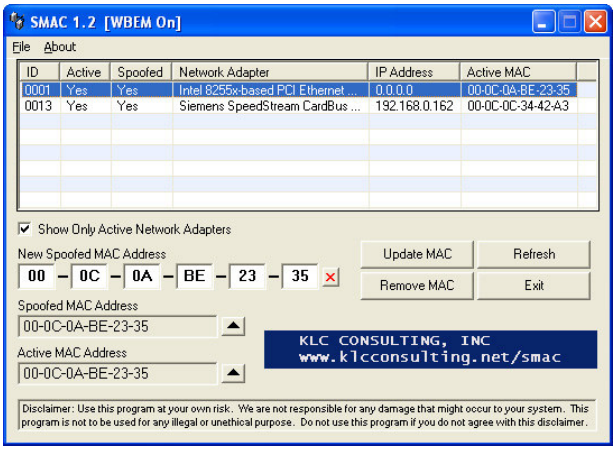
Traffic sniffing is made easy by interfacing a wireless NIC that supports raw (rf or promiscuous) mode with software such as **Kismet**. This Layer 2 tool offers 3-in-1 functions in relation to 802.11a, 802.11b, and 802.11g signals. Not only can it serve as an intrusion detection system for the good guys, but also it operates as a wireless network detector (well suited for wardriving), and it handles wireless transmission sniffing. Other notable features of Kismet are display of network IP range, hidden network SSID de-cloaking, manufacturer and model identification of access points and clients, and runtime decoding of WEP packets for known networks. (Kismet, nd)

Both **WEPCrack** and **AirSnort** are encryption cracking tools that exploit flaws in the RC4 algorithm, as outlined by Scott Fluhrer, Itsik Mantin, and Adi Shamir's paper titled Weaknesses in the Key Scheduling Algorithm of RC4. WEP encryption key cracking tools passively monitor communications. AirSnort, for example, can successfully compute the encryption key in less than one second, after it has been able to sniff approximately 5 to 10 million encrypted packets. The 5 to 10 million encrypted packet capture can transpire during a single session or multiple sessions separated by seconds or days. (Internet.com, nd; Rager, nd; Shmoo Group, nd-b)

Wireless device manufacturers provide administrators the ability to filter MAC addresses in effort to limit network participation to only devices with authorized MAC addresses. The below graphic is an example of a typical MAC filter interface.



After discovering a MAC address of an authorized device, an attacker is only limited by his ability to configure his unauthorized device to impersonate an authorized device. [In the interest of brevity, the reader is advised that the art of obtaining undisclosed MAC addresses is well documented in other sources and is beyond the scope of this text.] For less than $20, an attacker can download a program such as Spoof MAC (**SMAC**) from the Internet. This nifty tool and others allow their possessors the ability to virtually change MAC addresses to perhaps impersonate an authorized device during an attack.



(KLC Consulting, nd)

Rogue APs can be classified in primarily two categories: A friendly insider that brings in a personal AP from home and configures it to join the enterprise wireless system. This insider has no malicious intention to harm the organization's network. The other category is the attacker that employs his rogue AP to gain unauthorized access and/or attack the organization's wireless and/or wired network. Regardless of intention, an unauthorized or rogue AP, can be a gateway for attackers to gain easy access, especially considering low-end, home-use APs are generally not configured properly or offer higher-end security features as enterprise APs. A low-end AP with weak security capabilities that successfully joins an enterprise wireless network can become the link that potentially nullifies the entire wireless security policy and security of the enterprise. (Trapeze Networks, 2004)

From an attack perspective, rogue APs with more powerful transmitters can cause interference that slows throughput or cause complete DoS. Malicious APs can also broadcast data packets that overwhelm the spectrum and cause devices to repeatedly disconnect from authorized APs (Trapeze Networks, 2004). Usernames and passwords can be stolen by rogue APs by confusing legit users with DNS and HTTP redirects (Shmoo Group, nd-a). Or perhaps an attacker may configure a rogue AP to employ impersonation techniques to successfully connect to the network, attract legitimate users, tunnel Transport Layer Security (TLS) authentication exchange between the legit user and the authentication server; after the legit user is authenticated, the attacker gets additional data that enables him to disconnect the legit user and gain complete access to the wireless network, and possibly the wired network as well. The legit user is likely to reconnect successfully and consider the episode a normal glitch, while the server is unaware of the intrusion. (Trapeze Networks, 2004).

x(Net Admin) + Unchanged + Default EQUALS *y*(Bad Guy) + Easier + Access

Prior to unnecessarily expending additional resources to intrude a wireless network or device, often it makes sense for attackers to use defaults early in their attack quest. Since some wireless network administrators never exert effort to change device defaults, attackers may only need to expend less than a minute of effort to obtain manufacturer defaults and gain unauthorized access. For example, many password defaults can be obtained at a site such as http://www.cirt.net/cgi-bin/passwd.pl . Other defaults such as SSID, channel, and WEP keys can be gathered from a site similar to http://www.cirt.net/cgi-bin/ssids.pl .

EFFORTS TO MITIGATE HACKS

Passive eavesdropping consists of monitoring 802.11 communications to ascertain destination, source, size, number, and time of packet transmission. Information gleaned from the aforementioned data can be instrumental in more progressive attacks. Often such data is encrypted by stream ciphers such as WEP. The IV of WEP makes the protocol vulnerable to reuse and can be easily cracked. If the administrator can stay one step ahead of attacker by constantly re-keying the devices, perhaps WEP may provide sound encryption. Passive eavesdropping is best defending by using a block cipher such as Advanced Encryption Standard (**AES**) or Triple Data Encryption Standard (**3DES**). The difference between passive and **active eavesdropping** is the former does not involve injecting data into transmissions to decipher encrypted data. (Welch & Lathrop, 2003b)

Rogue APs have capability to levy much detriment. Beyond being a catalyst for attackers to implement DoS, access personal records, and/or steal intellectual property, Rogue APs can also facilitate unauthorized access to ISPs and the Internet that may develop into legal liabilities for the enterprise. (Trapeze Networks, 2004)

In defending against rogue APs the administrator should have a detailed map that includes location of enterprise APs and physical structures such as walls and other fixed objects. In combination with the AP map, the use of techniques employed by wardrivers should be used by the good guys to detect rogue APs. This requires administrators to routinely leave their network control centers on patrol duty to scan, capture, and analyze RF signals in quest to identify rogue APs. (Trapeze Networks, 2004) Aside from wardriving tools for rogue AP discover, there are tools such as HotSpotDK that alert administrators when changes in SSID, MAC address of the access point, MAC address of the default gateway, and signal strength occur (Shmoo Group, nd-a).

Another tier to prevent rogue AP attacks should be a combination of **802.1x authentication**, strong encryption such as Wi-Fi Protected Access (WPA), and authentication, authorization, and accounting (AAA) (Trapeze Networks, 2004). 802.1x was developed as a standard to pass Extensible Authentication Protocol (EAP) over wireless and wired networks. The beauty of EAP is its ability to deliver interoperability among various authentication systems. EAP is credited for allowing authentication factors such passwords, challenge-response tokens, and public-key infrastructure certificates to effortlessly work together (Snyder, 2002). Before being granted access to other network resources, 802.1x requires wireless devices to be authenticated. The reader is advised that EAP is only a transport protocol designed for authentication. The transport protocol can support multiple authentication schemes, such as one time passwords, smart cards, Kerberos, and public key (Strand, 2004. There are many authentication mechanisms supported by EAP (IANA.org, nd); they include EAP-MSCHAPv2, Lightweight EAP (LEAP), EAP-TLS, EAP-TTLS, Protected EAP (PEAP), and EAP-MD5 (Strand, 2004; Welch & Lathrop, 2003b).

WPA is the core implementation of 802.11i. WPA is a replacement for WEP and was developed primarily to eliminate the inherent vulnerabilities of WEP (Wikipedia, nd). 802.11i has three components; they are Temporary Key Integrity Protocol (TKIP), Counter Mode with CBC-MAC Protocol (CCMP), and 802.1x with TKIP or 802.1x with CCMP. TKIP was developed as short-term solution to eliminate weaknesses found in WEP prior to ratification of the 802.11i standard (Strand, 2004). In WPA, the IV is 48 bits. As the system is used, TKIP dynamically changes keys. The key recovery attacks available in WEP are restricted by WPA, which has a greater IV and changes keys. Also, WPA has a more secure Message Integrity Check (MIC) that limits alteration of payload; and the frame counter in MIC restricts replay attacks (Wikipedia, nd).

Because TKIP was developed under pressure as a quick fix to WEP, TKIP interfaces well with older 802.11 devices; the older devices may require only a firmware upgrade. CCMP provides improved integrity and confidentiality. However, since CCMP is a newly designed protocol and is CPU intensive, procurement of new or additional equipment may be required. 802.1x combined with TKIP is WPA, also referred to as short-term or Transition Security Network (TSN). The long-term solution is Robust Secure Network (RSN) or WPA2, which is the combination of 802.11x and CCMP (Strand, 2004).

Core devices of 802.1x are wireless node/s, AP/s that also serve as authenticator, and Remote Authentication Dial-In User Service (RADIUS) server (Snyder, 2002; Strand, 2004). The main processing power of 802.1x is needed in the wireless node/s and RADIUS server. This bodes well for the AP/s to handle the lightweight authentication tasks, since APs are generally not designed for robust processing (Snyder, 2002). WPA was intended to be used with an authentication server that assigns different keys to each user. However, in a SOHO or

ad-hoc environment, a less secure pre-shared key (PSK) can be used; but the full protection of 802.1x will be negated (Wikipedia, nd). Use of a PSK is considered *WPA-Personal*. Use of EAP and RADIUS is considered *WPA-Enterprise* (Strand, 2004). When configuring **AAA**, the RADIUS server can be standalone or homogenized with a directory services system such as Microsoft's Active Directory. Proper implementation of 802.1x authentication and AAA is likely to halt rogue AP attacks. For more details about 802.1x, the reader is encouraged to examine Snyder (2002) and Strand's (2004) works.

This is a good point in the text to pit stop to examine encryption and integrity. **Encryption** protocols are necessary to provide virtual tunnels; they enhance the privacy of transmissions. Providing encryption to the lowest possible OSI layer is optimum. In essence, each layer above it is protected. As the below graphs indicate, Layer 3 encryption is not as potent as Layer 2; Layer 3 encryption leaves the IP address exposed in clear text and renders the packet susceptible to IP spoofing (Welch & Lathrop, 2003a). IP spoofing can be a means to breach transmissions and inject data (Welch & Lathrop, 2003b). Examples of Layer 2 tunnels are WEP or AES. Layer 3 tunnels include IPSec or VPN. Tunnels that operated at Layer 4 include SSL. Assigning encryption to the lowest possible layer has a downside. It creates a longer tunnel; this decreases system performance. Yet, the alternative must be upgrade of equipment, not the sacrifice of security. (Welch & Lathrop, 2003a)

Unencrypted			
802.11 Header	IP Header	TCP Header	E-mail Message

Layer 3 Encrypted Tunnel			
802.11 Header	IP Header	TCP Header	E-mail Message

Layer 2 Encrypted Tunnel			
802.11 Header	IP Header	TCP Header	E-mail Message

Integrity and encryption are not necessarily one and the same. While encryption is responsible for privacy, **integrity** mechanisms verify the message has not fallen victim to modification by a malicious or imposture transmission participant. Examples of good data integrity protocols are Secure Hash Algorithm (SHA-1) [used in TLS, SSL, PGP, SSH, S/MIME, and IPSec (Wikipedia, nd)], RACE Integrity Primitives Evaluation Message Digest 160-bit (RIPEMD-160), and keyed-hash message authentication code (HMAC). Examples of known vulnerable protocols are Cyclic Redundancy Check 32 (CRC-32) [used in WEP], Message-Digest algorithm 4 (MD4), and Message-Digest algorithm 5 (MD5). (Welch & Lathrop, 2003a)

Hodgepodge Wireless Security Checklist

Depending upon capabilities, the maximum security options listed below should be implemented.

802.1x – use for key management and authentication (Thomas, 2004)
AAA (Trapeze Networks, 2004)
Anti-virus and personal firewall software on client devices (Craiger, 2002; Karygiannis & Owens, 2002)
AP – change default channel (Thornton, 2003)
AP – decrease RF footprint by limiting RF propagation to only required areas/range (Thornton, 2003); use empirical means to test signal range (Karygiannis & Owens, 2002)
AP – disable DHCP and use static IP addresses if fixed number of nodes access AP (Thornton, 2003)
AP – disable insecure and nonessential management protocols (Karygiannis & Owens, 2002)
AP – establishment authentication for management interfaces (Karygiannis & Owens, 2002)
AP – implement proactive measures that include IDS components (Karygiannis & Owens, 2002; Thomas, 2004)
AP – Layer 2 switch instead of hub for AP connectivity (Karygiannis & Owens, 2002)
AP – limit DHCP pool; do allow 50 addresses if only 5 are needed (Thornton, 2003)
AP – mutual authentication of client and access point to limit man-in-the-middle, replay and session-high jacking (Welch & Lathrop, 2003a; Welch & Lathrop, 2003b)
AP – password protect management interfaces (Craiger, 2002)
AP – Patrol, at regular and random intervals, to scan and analyze RF signals to detect rogues (Karygiannis & Owens, 2002; Trapeze Networks, 2004)
AP – physical security to prevent access that can allow undetected configuration changes (Thomas, 2004)
AP – place near center of facility, away from perimeter (Karygiannis & Owens, 2002)

AP – put the wireless network behind a separate routed interface to enable a quick, single shut off point (Thomas, 2004)
AP – should have its own firewall interface (Thornton, 2003)
AP – turn on logging and review logs on a regular basis (Karygiannis & Owens, 2002)
AP – use SNMPv3 and/or SSL/TLS for management via HTTP (Karygiannis & Owens, 2002)
Assume – anyone within signal range can access the network (Craiger, 2002)
Authentication – biometrics, smart cards, 2-factor authentication, PKI (Karygiannis & Owens, 2002)
Clear all configurations on unused devices (Karygiannis & Owens, 2002)
Defaults – change them all (Karygiannis & Owens, 2002)
Dynamic session keys (Craiger, 2002)
EAP – decide which authentication protocol best fits the environment (Thomas, 2004)
Firewall – between wireless LAN and wired LAN (Karygiannis & Owens, 2002)
Firewall – configure to block unauthenticated traffic to limit ARP attacks (Welch & Lathrop, 2003b)
Firewall – features combined with IPSec, SSH, and/or SSL to limit eavesdropping and access by unauthenticated devices (Craiger, 2002)
Identify authorized wireless devices users (Karygiannis & Owens, 2002)
Integrity – sound cryptographic verification to limit eavesdropping, replay and session high-jacking (Welch & Lathrop, 2003b)
Layer 2 – use a block cipher such as AES or 3DES to limit eavesdropping (Welch & Lathrop, 2003b)
MAC address filtering [also block MAC addresses of lost or stolen NICs] (Craiger, 2002)
NIC – audit wireless NIC inventory to ensure accountability (Craiger, 2002)
Packet Authentication – this requires an attacker that is able to high-jack a session to also be able to authenticate individual packets in order to trick the receiving device (Welch & Lathrop, 2003a)
Passwords – change regularly (Karygiannis & Owens, 2002)
Passwords – strong [at least 8 characters long that include uppercase and lowercase letters, numbers, and special characters] (Roland, 2004)
Policies – appoint individuals to be accountable for 802.11 standards implementation, threats, and mitigation tracking (Karygiannis & Owens, 2002)
Policies – define were (what location) wireless devices can be used (Karygiannis & Owens, 2002)
Policies – define what data is authorized for wireless transmission (Karygiannis & Owens, 2002)
Policies – enforce them (Thomas, 2004)
Policies – provide guidelines on reporting losses of wireless devices and security incidents (Karygiannis & Owens, 2002)
Power off devices when not required for use (Karygiannis & Owens, 2002)
RADIUS server (Karygiannis & Owens, 2002; Snyder, 2002; Strand, 2004)
Session – timeout set for 10 minutes or less (Thomas, 2004)
Shared-key authentication instead of open authentication (Craiger, 2002)
Software – test and deploy patches (Karygiannis & Owens, 2002)
SSID – disable active broadcasting (Thomas, 2004); makes AP less susceptible to casual discovery (Thornton, 2003)
SSID – replace the default with a long and random sequence of characters (Craiger, 2002)
TCP/UDP – restrict wireless transmission to only required ports (Thornton, 2003)
VPN (Craiger, 2002) IPSec-based for wireless (Karygiannis & Owens, 2002) – such tunnels enhance the privacy and integrity of transmission (Welch & Lathrop, 2003a)
WEP – in the absence of WPA, enable WEP and frequently change the keys to limit eavesdropping (Craiger, 2002)
WPA – use it instead of WEP if it is available (Wikipedia, nd); may require firmware upgrade
WTLS – be aware this transport protocol has three operating modes/classes. Class 1 provides no security; class 2 is susceptible to man-in-the-middle and session high-jacking; use class 3 (Welch & Lathrop, 2003a)

EVOLUTION: LOCATION ENABLED WIRELESS SECURITY

Malaney (2004) outlined a security system that employs GPS and the signals generated by the network devices. This system is applicable to ad hoc, mesh, WLAN, or 3G networks. This system is termed Location Enhanced Security Service (LESS).

It is not intended to be an additional security layer to existing encryption techniques. The basic premise is the use of network device signals in conjunction with GPS to determine the location of authorized devices with a high degree of certainty. When a new device requests permission to participate in the network, the claimed location and GPS tracked information of the device must fall within an acceptable range as determined by LESS before access is granted. If the locations are not reconciled, personnel can be dispatched to investigate the location of the suspected malicious device. Although LESS can be applicable for a mobile environment, ease of use and practicality seem more reasonable for static or fixed systems since the best degree of certainty is established by participation of easily reconcilable device locations. Reconciliation of device location may be difficult in a dynamic or mobile environment. Hence, the LESS concept is due refinement.

DON'T WORRY ABOUT BLUETOOTH. IT IS SECURE! SURE?

Bluetooth (802.15) and Wi-Fi (802.11b and 802.11g) use the 2.4 GHz frequencies, known as the unlicensed/unregulated industrial, scientific, and medical (ISM) bands (Chaudhry & Sheikh, 2002; ITU, 2005). And, some may draw comparison between Bluetooth and Wi-Fi. However, the two should not really be considered true competitors or the same because they transmit differently and satisfy different needs. Although both technologies allow mobility, one should think of Wi-Fi as a radio frequency replacement for CAT 5 cables and Bluetooth as a radio frequency replacement for USB cables. Bluetooth's limited range and speed prevent it from handling full-function network tasks.

Bluetooth uses the frequency hopping spread spectrum (FHSS) transmission technique. The "frequency hopping" component of FHSS employed by Bluetooth consists of 79 channels divided into 625 micro second time slots (Cordeiro, Abhyankar, Toshiwal, & Agrawal, 2003; Tutorial Reports, nd). A device modulates 625 μs at a specific frequency and then uses a different frequency (Forouzan, 2004). Hence, data hops 1,600 times per second, among the 79 channels.

The communicating devices use a pseudorandom sequence to align and synchronize data flow. The pseudorandom number seems to be random; however, it is known and shared among the communicating devices (Wikipedia, nd). In essence, the receiver must know the hopping code, plus listen to the incoming signal at the right time and frequency (Internet.com, nd). Because of the required pseudorandom sequence, transmission occurs on a small portion of the spread-frequency at any given time; the chance of interference from non-Bluetooth devices is remote. (Wikipedia, nd)

In terms of privacy, the seemingly random frequency hops through the spectrum decreases the probability of eavesdropping and jamming. However, adept attackers are able to not only eavesdrop, but also actually seize control of Bluetooth devices, even when security features are enabled (Biever, 2005). An attacker can go beyond the realm of just listening to phone conversations. Without physical control of the victim's phone, the attacker can place calls through the victim's phone that will be charged accordingly.

Bluetooth becomes vulnerable during pairing, the initial communication between devices in which the secret key, frequency hopping pattern, and synchronization are established. The vulnerability created during pairing is minimized when pairing occurs in an isolated area. Yet, users must be aware that Bluetooth sniffers can be employed to relay Bluetooth communications to software that decodes the algorithm and disclose the secret key. Additionally, Bluetooth devices automatically broadcast their personal IDs to other Bluetooth devices. An attacker can spoof one of the personal IDs, causing his device to impersonate one of the legitimate devices. The impersonating device can send a message claiming to have forgotten the secret key. This forces the other device to discard the key and start a new pairing session, allowing the attacker access to the Bluetooth network (Biever, 2005).

The Bluetooth exploit is quite rudimentary, provided the right tools are in place. The vulnerability is a fairly recent discovery, and the average Bluetooth user is probably more likely to be hacked large metropolitan areas where there are condensed users and hackers. Also, wireless attackers may not consider Bluetooth devices to be as practical or as challenging as other hackings, unless there is a high probability that critical, or personal identification data intelligence will be gained. Additionally, Wikipedia (nd) notes that the timing required in Bluetooth hacking may require custom hardware, since most current commercial devices cannot support the timing required for successful attacks. In the absence of an IEEE standard and implementation that address the aforementioned vulnerability, users should definitely not link or transmit any critical or personal data with Bluetooth technology.

CONCLUSION

Almost any given single security mechanism (such as MAC filtering) alone may be easily overcome by attackers. However, proper configuration and implementation of the maximum possible security mechanisms must be used to form a hodgepodge of multiple security layers, in effort to provide the best possible wireless protection.

The IEEE 802.11n standard is under development, slated to operate at speeds 4 to 5 times faster than 802.11g and with greater range (Wikipedia, nd); wireless is making a serious run to replace wired LANs. The wireless industry has crested the billion-dollar mark (Feil, 2003), and wireless popularity and demand for the technology show no sign of near-term decrease. By 2010, wireless technology will be a critical element in the majority of Fortune 2000 companies (Thomas, 2004). Therefore, the wireless security discussion will continue to be prevalent.

REFERENCES

Arbaugh, W.A. (2003). Wireless Security is Different. *Computer, 36(8)*, 99-101.

Biever, C. (2005). *New Hack Cracks 'Secure' Bluetooth Devices*. Retrieved July 10, 2005, from http://www.newscientist.com/article.ns?id=dn7461

Borisov, N., Goldberg, I., & Wagner, D. (2001). *Intercepting Mobile Communications: The Insecurity of 802.11*. Retrieved June 28, 2005 from http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf,

Chaudhry, M.A.R. & Sheikh, M.I. (2002). Protocols stack & connection establishment in Bluetooth radio. *Students Conference, ISCON '02, 16-17 Aug. Proceedings. IEEE, 1*, 48 – 55.

Cordeiro, C.D.M., Abhyankar, S., Toshiwal, R., Agrawal, D.P., (2003). A Novel Architecture and Coexistence Method to Provide Global Access to/from Bluetooth WPANs by IEEE 802.11 WLANs**.** *Performance, Computing, and Communications Conference, 2003. Conference Proceedings of the 2003 IEEE International, 9-11 April*, 23-30.

Craiger, J.P. (2002). 802.11, 802.1x, and Wireless Security. Retrieved July 6, 2005, from http://www.giac.org/certified_professionals/practicals/gsec/2010.php

Feil, H. (2003). 802.11 Wireless Network Policy Recommendation for Usage within Unclassified Government Networks. *Military Communications Conference, 2003. MILCOM 2003. IEEE, 2*, 832-838.

Forouzan, B. A. (2004). *Data Communications and Networking*. New York: McGraw-Hill.

Lauter, K. (2004). The Advantages of Elliptic Curve Cryptography for Wireless Security. *Wireless Communications, IEEE, 11(1)*, 62-67.

IANA.org. (nd). Extensible Authentication Protocol (EAP) Registry. Retrieved June 21, 2005, from http://www.iana.org/assignments/eap-numbers

International Telecommunication Union (ITU). (2005). Frequently Asked Questions. Retrieved April 13, 2005 from the ITU Web site: http://www.itu.int/ITU-R/terrestrial /faq/index.html#g013

Internet.com (nd). Webopedia: Online Computer Dictionary for Computer and Internet Terms and Definitions. Retrieved from the Web site: http://www.webopedia.com/

Lauter, K. (2004). The Advantages of Elliptic Curve Cryptography for Wireless Security. *IEEE Wireless Communications, 11(1)*, 62 - 67

Lawrence, E., & Lawrence, J. (2004). Threats to the Mobile Enterprise: Jurisprudence Analysis of Wardriving and Warchalking. *International Conference on Information Technology: Coding and Computing, Proceedings, 2(5-7 April 2004)*, 268-273

Kapp, S. (2002). 802.11a. More Bandwidth without the Wires. *IEEE Internet Computing, 6(4)*, 75- 79

Karygiannis, T. & Owens, L. (2002). *Wireless Network Security: 802.11, Bluetooth and Handheld Devices*. Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology

Kismet. (nd). Kismet. Retrieved July 9, 2005, from http://www.kismetwireless.net/

KLC Consulting. (nd). SMAC Official Website. Retrieved July 10, 2005, from http://www.klcconsulting.net/smac/

MacStumbler. (nd). MacStumbler 0.75b. Retrieved July 8, 2005, from http://www.macstumbler.com/

Malaney, R.A. (2004). A location enabled wireless security system. *Global Telecommunications Conference, 2004. GLOBECOM '04, IEEE, 4(29)*, 2196-2200.

Miller, S.K. (2001). Facing the Challenge of Wireless Security. *Computer, 34*(7), 16-18

Neilson, B. (nd). Wireless Networks and Security. Retrieved July 9, 2005, from the Information Systems Security Assurance Web site: http://issa-northtexas.org/files/04-03-16%20Wireless%20Security%20-%20Brett%20Neilson.pdf#search='brett%20l%20neilson'

NetStumbler. (nd). MiniStumbler v0.4.0. Release Notes. Retrieved July 8, 2005, from http://www.netstumbler.com/downloads/ministumbler_v0.4.0_release_notes.pdf

NetStumbler. (nd). NetStumbler v0.4.0. Release Notes. Retrieved July 8, 2005, from http://www.netstumbler.com/downloads/netstumbler_v0.4.0_release_notes.pdf

Rager, A. (nd). WEPCrack. Retrieved July 11, 2005, from http://wepcrack.sourceforge.net/

Roland, J.F. (2004). *CCSP Self-Study: Securing Cisco IOS Networks (SECUR)*. Indianapolis, IN: Cisco Press.

Shmoo Group. (nd-a) AirSnarf. Retrieved June 23, 2005, from http://airsnarf.shmoo.com/

Shmoo Group. (nd-b). AirSnort Retrieved July 11, 2005, from http://airsnort.shmoo.com/

Snyder, J. (2002). What is 802.1x? Retrieved June 22, 2005, from http://www.networkworld.com/research/2002/0506whatisit.html

Strand, L. (2004). 802.1X Port-Based Authentication How To. Retrieved June 29, 2005 from http://tldp.org/HOWTO/html_single/8021X-HOWTO/#what8021x

Thomas, T.M. (2004). *Network Security: First-Step*. Indianapolis, IN: Cisco Press.

Thornton, F. (2003). Wireless Networking Basic Security Checklist, Small Business Version. Retrieved July 5, 2005 from http://www.wardrivercentral.org/WLAN_Sec_v3.pdf# search='wireless%20security%20checklist'

Trapeze Networks. (2004). Detecting Rogue Users and APs in a Wireless LAN. Retrieved Jun 27, 2005, from http://www.trapezenetworks.com/technology/whitepapers/detectingrogue/detectingrogue.pdf#search='rogue%20ap'

Tutorial Reports. (nd). Bluetooth Technology. Retrieved April 10, 2005, from the Web site: http://www.tutorial-reports.com/wireless/bluetooth/technology.php

Vassis, D., Kormentzas, G., Rouskas, A., & Maglogiannis, I. (2005). The IEEE 802.11g Standard for High Data Rate WLANs, *IEEE Network, 19(3)*, 21- 26.

Welch, D., & Lathrop, S. (2003a) *A Survey of 802.11a Wireless Security Threats and Security Mechanisms*. Technical Report ITOC-TR-2003-101. New York: Information Technology and Operations Center, Department of Electrical Engineering and Computer Science, United States Military Academy, West Point.

Welch, D., & Lathrop, S. (2003b). Wireless Security Threat Taxonomy. *Proceedings of the 2003 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY, June 2003, 76-83.*

Wikipedia (nd). The Free Encyclopedia. Retrieved from http://en.wikipedia.org/wiki/Main_Page