

Ryan Kightlinger

May 5, 2005

Senior Project

Wireless Fidelity

During the last decade, Wireless Fidelity (Wi-Fi) has become a dominant force in society's technological arena. Throughout the course of history, wireless networks have evolved from the simple wireless LAN based ALOHANET into the more sophisticated Wireless Fidelity concept, developed by the Institute of Electrical and Electronic Engineers (IEEE). Despite these new and fascinating discoveries, wireless networking still poses numerous security risks to both the general public and corporate America. This article is intended to provide you with an in-depth analysis of the history of Wireless Fidelity, addressing the major security vulnerabilities contained inside the Wi-Fi (802.11) standard.

Although Wireless Fidelity is a relatively new technology, wireless networks have been around for quite some time, they even predate the wired LAN by just a few years. The University of Hawaii pioneered the way to wireless networking in their development of the ALOHANET in 1971. This network was originally designed to solve the university's dilemma of being able to transmit data to and from their four different sites scattered across the Hawaiian Islands. Wireless networking has evolved dramatically since that time, being incorporated into such devices as the Star 7, developed by Sun Microsystems in 1992. This unit was originally designed to serve as a handheld mini-tablet computer, which would incorporate a built in 900 MHz wireless network. Unfortunately for Sun Microsystems this unit was never marketed to the general public, leaving other corporations to profit from this technology.

Wireless networking has the ability to affect your everyday life in ways unimaginable in the past. Consider how society has benefited from the introduction of cellular networks into the economy during the 1980's. Similarly, wireless networks were created to improve upon past technological standards to make their uses more convenient to the general public. Wireless networking allows users within a corporation or a single household to share their data freely

from machine to machine, all without the necessity of placing wires through walls. These networks were engineered to eliminate the brutal constraints of wires, while incorporating all the features that made wired networks so popular in past years.

A wireless network is essentially made up of two basic units, a client adapter and an access point. The first of these devices, the client adapter, usually consists of a plug-in device of some variation that is connected directly to your main computer. This device holds the specification standards needed to establish a direct connection between your computer and a wireless access point. The access point acts as the Grand Central Station controlling all wireless activity between your networked computers. The data is able to be transported wirelessly through the use of radio waves, which are sent via small microwave transmitters embedded inside the wireless gear.

Wireless Fidelity underwent its development in the mid 1990's, being developed by research groups at the Institute of Electrical and Electronic Engineers. The goal was to develop a universal standard that would allow wireless devices from different vendors to communicate successfully with one another. The IEEE originally created the 802.11 working group to accomplish this task. This working group was the 11th group created under the IEEE's 802 networking standard, which governs the lowest level of networking functions contained inside the Open Systems Interconnection (OSI) Model. The 802.11 working group was finally completed and adopted as a standard by the IEEE in 1997. Shortly after its adoption, the IEEE created additional working groups to revise upon the 802.11 standard. These newly formed groups were given a corresponding letter, in alphabetical order, following the 802.11 standard (802.11a, 802.11b, etc.) to identify their primary task. The letters were assigned to each group according to their initial start date and have no relevance to their actual date of completion, as

some groups were able to finish more quickly than others. Currently the working groups for the 802.11 specification standard range from 802.11a to 802.11v.

Almost immediately after its adoption as a standard, 802.11 products began appearing on the open market. These products, however, were slow to catch on, since the 802.11 IEEE standard set in place a maximum data transfer rate of 2 Mbps (megabits per second), which traveled in the 2.4 GHz radio frequency range. When compared to the current speed of wired networks at the time (100 Mbps), these data rates were considered to be tremendously slow. Speed was not the only factor discouraging consumer purchases. These products were also priced so extremely high that few ordinary consumers could afford their purchase. In order to boost sales and increase interest worldwide, the IEEE convened and discussed improving the 802.11 standard, therefore creating several task groups to accomplish this goal. It wasn't until after the year 2000 when the Apple Airport wireless system finally brought Wi-Fi prices down to consumer levels.

The first working group to improve upon the 802.11 wireless networking standard was the 802.11b committee, which accomplished its mission in 1999. This task group was created by the IEEE to develop a faster standard that would also be backwards compatible with past 802.11 technologies. Once finalized the 802.11b standard provided a new maximum data transfer rate of 11 Mbps that operated in the same 2.4 GHz radio spectrum as 802.11. Although many people still considered this speed to be relatively slow, it was able to compete successfully with the common 10-Base-T Ethernet system (10 Mbps). Since 802.11b was built to ensure backwards compatibility it was able to communicate with the older 802.11 hardware, though only at the slower data rates. The radio frequency that was designated to control 802.11b communication was the unlicensed 2.4 GHz Industrial Scientific and Medical (ISM) band. This same zone

shares space with such devices as microwave ovens, cordless telephones, Bluetooth equipped devices, and medical monitoring equipment. To eliminate the interference between devices spread-spectrum techniques were used. Up until the recent launch of 802.11g (2003), 802.11b was considered to be the dominant Wi-Fi standard.

	IEEE Standard				Proprietary	
	Wireless-A 802.11a	Wireless-B 802.11b	Wireless-G 802.11g	Wireless-N 802.11n	Texas Instruments 802.11b+	Atheros Super G
Year	2000	1999	2003	2006?	2001	2003
Top Bit Rate	54 Mbps	11 Mbps	54 Mbps	320 Mbps?	22 Mbps	108 Mbps
Compatible with	None	802.11g 802.11b+ Super G	802.11b 802.11b+ Super G	?	802.11b 802.11g Super G	802.11b 802.11b+ 802.11g
Pros:	Inference is rarely a problem as it works in the uncrowded 5 GHz band. Few network crackers have tools to sense and subvert it.	Cheap, esp. on used market. Shaken out and very reliable. As fast as any broad-band Net connection. Long range at top bit rate.	As fast as Wireless-A across greater range. Most gear has WPA support. Not a lot more expensive than Wireless-B.	Details are still thin; we'll know more by 2005.	Highly compatible with Wireless-B at Wireless-B bit rates. Cheap.	Highly compatible with Wireless-G and Wireless-B at their lower bit rates. Very high bit rates and throughput.
Cons:	Expensive. Antennas are not removable, by FCC rules. Highest bit rates are available only across a very short range. Won't connect to most public hotspots. May be abandoned now that Wireless-G is common.	Slow for moving large files around. Most gear will never support WPA. 2.4 GHz band is crowded and interference is a growing problem.	Network bit rate drops when Wireless-B clients associate with a Wireless-G AP. 2.4 GHz band is crowded and interference is a growing problem.	Unknown. May be expensive	22 Mbps bit rate only available for connections with other 802.11b+ gear. Most gear will never support WPA. May be abandoned now that Wireless-G and Super G are common.	108 Mbps bit rate only available for connections with other Super G gear. Operates only on channels 5 & 6. Uses wide swath of 2.4 GHz Wi-Fi band and has potential to interfere with other nearby networks.

Figure 4.2
Wireless Networking Technology Selection Matrix.

Table 1-1: 802.11 IEEE standards (Jeff Dauntemann's Wi-Fi Guide)

To ensure the compatibility between wireless products of different vendors, the IEEE handed over their control of product testing to the Wireless Ethernet Compatibility Alliance, otherwise known as WECA, established in August of 1999. This organization was in charge of creating a logo certification program that would test products for adherence to the newly approved 802.11b standard. This program was named Wi-Fi, which represented the longer phrase of Wireless Fidelity. Products that were able to pass this inspection were given the full authority to carry WECA's Wi-Fi certified logo. This logo was designed to quickly inform customers that products bearing the Wi-Fi certified logo were guaranteed to be compatible with the 802.11b standard. This certification process soon became something that few vendors could afford to live without. As time passed, WECA decided upon renaming its organization to the Wi-Fi Alliance, which is presently located on the World Wide Web at www.wi-fi.com. The Wi-Fi program also adopted the 802.11a and 802.11g standards as they became available and is expected to adopt future 802.11 technological standards as well.



The next improvement made to the 802.11 networking standard came from the 802.11a working group in late 1999, shortly after the finalization of the 802.11b standard. This task group was created by the IEEE, alongside the 802.11b workgroup, to develop a faster wireless networking standard that would be more likely to compete with the 100-Base-T Ethernet system. In order to accomplish this goal, the 802.11a committee completely redesigned the physical network layer to operate in the 5 GHz radio spectrum, creating a new maximum data transfer rate of 54 Mbps. Due to this new frequency range, 802.11a products are incompatible with the past 802.11 standard, which utilized the 2.4 GHz spectrum. 802.11a achieves its best performance in the areas closest to the broadcast unit, as the quality of the signal degrades relatively faster with

distance than with a signal at a lower bit rate. This problem has more to do with the laws of physics, than with the engineering design of the standard. The obvious consequence of signal degradation is that the further you move your client adapter away from the broadcast signal, the lower the bit rate you will receive. You will most likely obtain your optimal bit rate speed from areas within the same room as your broadcast unit, free from any obstructions between the two devices. In addition to improving the bandwidth speed, the 5 GHz radio spectrum also provides for a much lower interference rate, since the spectrum does not have share its frequency with such devices as cell phones and microwave ovens, which are commonly located in 2.4 GHz zone. This 5 GHz band was designated by the United States Government to be part of the National Information Infrastructure Program, therefore providing a specialized zone for its device testing. Since its development 802.11a products were slow to catch on to the main stream market and gain wide spread public attention, and with the newly implemented 802.11g standard 802.11a is expected to fade into the past technological world.

The next 802.11 standard to be developed was 802.11g. This technological standard was initially set in motion by the IEEE in late 2000 to improve upon the 802.11b standard, while also maintaining backwards compatibility with the 802.11/b technology occupying the 2.4 GHz radio spectrum. The 802.11g standard was finalized by the IEEE in July of 2003. This standard provided a maximum data transfer rate identical to the 802.11a standard at 54 Mbps, nearly five times the speed of 802.11b. Since this standard occupies the 2.4 GHz spectrum, the data is able to maintain higher speeds at greater range when compared to 802.11a. When initially launched 802.11g equipment was priced surprisingly lower than 802.11a gear, which delivered speeds at similar levels. Due to this relatively low price, 802.11g was able to successfully compete with

the 802.11b standard, at prices of only 10 to 15 percent higher. In the nearby future the 802.11g standard is expected to fully replace the older Wi-Fi standards of 802.11b and 802.11a.

The latest 802.11 standard currently being underdevelopment by the IEEE is 802.11n. This task group was initially organized in September of 2003 and is anticipated to finalize its standard by the fourth quarter of 2006. When officially implemented this standard is expected to utilize the NII 5 GHz frequency band, avoiding the more crowded 2.4 GHz spectrum. 802.11n is also predicted to deliver an astonishing transmission rate of 250 Mbps. Since this standard is presently in the early stages of development, final details may vary.

In addition to the working groups devising the 802.11 standards, the IEEE has also organized several groups to work in correlation with one another. As mentioned previously, the 802.11 working groups currently range from 802.11a to 802.11v. The first working group to be developed after the 802.11b task group was assigned was 802.11c. This group was created with the initial task of developing a universal specification for wireless bridging. The next task group to be developed by the IEEE was 802.11d. This working group was formed to develop an international specification, mainly for wireless manufactures, that would enable wireless networking devices to interoperate with different networks worldwide. The following group, 802.11e, was formed to address the Quality of Service (QoS) of data transmission. The next group, 802.11f, was organized to develop the Extended Service Set (ESS), which is used in conjunction with multiple access points to enable the concept of roaming. Following the 802.11g wireless networking standard is the 802.11h working group, which was created to add European compatibility to the 802.11 standard. The next working group, 802.11i, was formed in March of 2001 to address the security vulnerabilities contained inside the 802.11 standard. Other

802.11 working groups are addressed in *Table 1-2*, shown below. Note that the IEEE 802.11 committee decided not to use the letters L, M, O, and Q for various reasons.

Standards

- IEEE 802.11 - The original 1 Mbit/s and 2 Mbit/s, 2.4 GHz RF and IR standard
- IEEE 802.11a - 54 Mbit/s, 5 GHz standard (1999, shipping products in 2001)
- IEEE 802.11b - Enhancements to 802.11 to support 5.5 and 11 Mbit/s (1999)
- IEEE 802.11d - international (country-to-country) roaming extensions New countries
- [IEEE 802.11e](#) - Enhancements: [QoS](#), including packet bursting
- IEEE 802.11F - [Inter-Access Point Protocol](#) (IAPP)
- IEEE 802.11g - 54 Mbit/s, 2.4 GHz standard (backwards compatible with b) (2003)
- IEEE 802.11h - 5 GHz spectrum, [Dynamic Channel/Frequency Selection](#) (DCS/DFS) and [Transmit Power Control](#) (TPC) for European compatibility
- [IEEE 802.11i](#) (ratified [24 June 2004](#)) - Enhanced security
- IEEE 802.11j - Extensions for Japan
- IEEE 802.11k - Radio resource measurements
- IEEE 802.11n - Higher throughput improvements
- 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 - Interworking with non-802 networks (e.g., cellular)
- IEEE 802.11v - Wireless [network management](#)

Table 1-2: 802.11 working groups (wikipedia.org)

When initially designing the 802.11 wireless networking standard, the IEEE chose to implement a variety of security protocols to protect its users against the threat of wireless attacks. These security protocols were needed since wireless networking in its most basic form is an insecure technology. Regardless of whether a network is composed of wires or utilizes wireless technology, a network will always be vulnerable to attack. This has more to do with the human factor in implementing a network, than with the technology aspect itself. As you may be aware of, humans will always be susceptible to performing ill-advised actions, even when they know it

goes against their best interest to do so. In order to achieve a successfully secured network, you must be able to balance the issues of trust and risk.

For a security system to be considered effective, it requires trusting people and trusting technology. If for any reason one of these two issues of trust fails the system may be compromised, opening a potential hole for attack. Trusting people is considered to be problematic for several reasons. The most significant reason for this trust violation is that humans have the natural tendency of deviating from their respective protocols, often through careless activity. Along with trusting individuals, you must also be able to trust yourself, by following your own policies and procedures. Failure to do so will weaken even the strongest security systems. Throughout this issue of trust, the education of your workers plays an important role in their ability to fully comprehend their assigned tasks and corporate responsibilities. By providing your workers with the appropriate education, you will undoubtedly achieve their maximum productivity in securing your local business surroundings. Similarly to the task of trusting your employees, trusting the technology around you is of equal, if not greater, importance. This task is also considered to be a problematic issue for reasons quite different from the human trust factor. First of all, we do not always have a sufficient understanding of the technology that “we are called upon to trust”. This may result in our ability of trusting the technology to perform tasks that it was never designed to handle, therefore creating a false sense of security. Secondly, technology, as it was initially developed, will always contain flaws. These may be hidden even from the leading experts in the field, until someone finds and exploits the vulnerability. Lastly, newer technology will always be developed, rendering the older technology useless and ineffective.

In addressing these issues of security the IEEE chose to design their own security protocol, which they implemented inside their 802.11 wireless networking standard. This newly created protocol was deemed Wired Equivalent Privacy (WEP). WEP was intended to provide wireless users with a form of protection that would limit outside interference and secure their data over network travel. In order to utilize this technology WEP must be installed inside the firmware of wireless devices, including access points and client adapters. When enabled WEP establishes a 64 bit data encryption rate between access point and client adapter. In recent years this encryption rate has been improved upon to reach areas up to 124 bit in encryption, although at unofficial levels. Many of the problems with WEP encryption arise from people's misconception of what the standard is actually capable of achieving. In reality WEP was not designed for anything other than monitoring your network traffic and preventing outsiders from accessing your private network.

In Jeff Duntemann's (Wi-Fi Guide) own words, "WEP is not an end to end encryption mechanism. WEP does not distribute or manage network keys. WEP does not hide traffic sent by one legitimate user of a wireless network from other legitimate users of the same network. WEP does not authenticate users except by checking encryption keys". (Page 294 – 295)

The underlying foundation behind WEP encryption is the RC4 stream cipher, which was developed in 1987 by Dr. Ron Rivest of RSA Security. The RC4 cipher was chosen due to its simple design and its extremely efficient algorithm used to encrypt data. From a user's standpoint, WEP encryption is a relatively easy feature to implement inside of a wireless

network. The first step is to launch your access point's configuration panel and select four unique encryption keys that will be passed on to each of your networked devices. These keys are composed of hexadecimal numbers, ranging from the digits 0-9 and the letters A-F. For the basic 64 bit encryption, each key will be composed of 10 hexadecimal numbers. After you have defined your initial key values, the next step is to perform key distribution. This process involves manually entering in your key values into each of your client adapters that you would like to connect to your wireless network. To simplify this process of key distribution, many modern access points have added the ability to generate these key values automatically using a simple pass-phrase, composed of a string of characters ("Pittsburgh Steelers"). In order for a network connection to be established, all key values must be identical. Once the process of key distribution is finished, WEP encryption can now be enabled, encrypting your network traffic between client adapter and access point.

In recent years, WEP encryption has been under attack by a serious flaw found in the RC4 cipher. WEP uses this cipher to perform its encryption technique by combining a block of clear text (unencrypted data) with a string of pseudorandom numbers, the same size as the clear text message. The string of pseudorandom numbers, which the cipher generates, is called the *keystream*. The keystream and the clear text message are combined into a single block of data called the *frame*. This frame is transmitted over the airwaves inside of units of data called *packets*. It is the utmost in importance that each frame should be encrypted using a unique keystream. Failure to do so will weaken the RC4 system, allowing the secret key to be easily cracked. The main problem with the RC4 cipher is that it uses a random 24 bit number seed called an initialization vector (IV). Since this vector is sent with every encrypted frame, it allows an outsider to identify if two frames were encrypted with the same initialization vector. By

gathering enough data with similar IV values, a hacker can easily crack the secret key and gain access to a wireless network. With the 24 bit number seed used in the RC4 cipher, there are presently 16,777,216 different IV values. This may appear as an overwhelming number, but with a large network in constant use, you will likely exhaust all the possible IV values in just six hours. This allows a hacker to gather enough information to crack your wireless network in a little over a day's time. Depending on the size of your network and its rate of usage, this may result from a non-threatening to a severe security vulnerability. It should be noted that WEP is also vulnerable to attacks using brute force. This is a dictionary style type of attack, which constantly throws passwords at the network until the user is able to crack the secret key.

Perhaps one of WEP's biggest drawbacks is simply that users don't realize the potential benefits that WEP has to offer and therefore fail to enable the security mechanism. In addition, the media has made WEP appear as a useless technology, not worth utilizing. Although WEP has its security vulnerabilities, for a small home network WEP offers a more than adequate amount of protection. By just activating the system, intruders will more than likely pass your network by for one that falls prey to an easier attack. Regardless of whether or not you're using a corporate or home network, you should do your very best to secure your wireless connection. You will be the one responsible if intruders decide to use your network for illegal activity, such as mass spamming.

The simplest way to combat the threat against wireless attacks is to enable the WEP security mechanism. Although this security standard is still vulnerable to attacks made through the passing of IV values, inside each data packet, there are ways to potentially slow down the attack. By rotating your keys on a daily, weekly, or even monthly basis, you prevent the attacker from gathering enough data to successfully crack your network key. In addition to enabling

WEP protection, there are other precautions that you may take to deter wireless hackers. It is recommended that once you enable WEP, you should change your default SSID (Service Set Identifier). This ID assigns a name to your network and is broadcasted from your wireless access point. By leaving your SSID on its default name hackers will likely be drawn to your network, assuming that it may be vulnerable to an easy attack. It is advised that you should avoid using personal information, such as your family or business name, when renaming your network's SSID. The best recommendation is to use a somewhat general and boring name (flora or fauna), while avoiding random numbers and characters. Another way to protect your wireless network is to lower your access point's broadcasting signal, if your device supports this feature. By lowering your broadcasting range, hackers will be less likely to detect your wireless network. The next form of protection that you may take is to simply turn off your broadband modem and computer when not in use. If your devices are disabled, then hackers won't be able to utilize any of your network's resources. Perhaps the best recommendation that I can provide you with is to use the strongest encryption password that your security system can support. If you choose to use an easily guessable password then even the best security systems will fail.

In an attempt to correctify the vulnerabilities contained inside the WEP security protocol, the IEEE began working on its newest security standard in late 2001, entitled Wi-Fi Protected Access (WPA). Upon its completion in 2002, WPA was able to address and solve every known security issue involved in WEP. In addition, WPA raised the standard encryption key from 40 to 128 bits in length, making brute force attacks nearly impossible. WPA also enlarged the Initialization Vector (IV) from 24 to 48 bits. By doubling this vector it would now take a total of 281 trillion packets before exhausting the total number of unique IV values. Gathering enough packets to successfully crack the WPA system would take well over a thousand years with

today's current technology. A new feature that WPA added to the Wi-Fi standard is the ability to automatically generate and pass new encryption keys to all networked devices. This eliminates the time consuming process of manually transferring keys on a regular basis. WPA also added the new ability of mutual authentication between access point and client adapter. This new feature was added to prevent "man in the middle" attacks. This type of attack refers to placing a rogue access point in the middle of a wireless network in an attempt to gather encrypted data. Another important feature that the IEEE decided to implement into the WPA security protocol was the Message Integrity Code (MIC). This feature was designed to determine whether or not a network packet had been tampered with during its course of travel.

Like all current technology, WPA is still vulnerable to certain types of attacks. The most notorious being the Denial of Service (DoS) attack. This attack occurs in part because of WPA's Message Integrity Code. Since WPA automatically shuts down an access point when two or more packets fail the MIC test, a hacker can use this ability to shut down a wireless network for an extended period of time. The only way to stop this attack from happening is to disable the MIC feature. Similarly to WEP, WPA's security depends heavily on the length of the original pass-phrase used to generate the shared secret key. Simply put, the shorter the key, the greater the chance that the system will be compromised.

It is currently estimated that well over half of the world's wireless networks will continue to be installed without utilizing a form of protection. In most cases enabling a security mechanism, such as WEP or WPA, is as easy as clicking a few buttons and typing in your pre-shared key. For more information on enabling WEP or WPA a user should consult their wireless access point's instruction manual. It is important to remember that if a user fails to protect their

wireless network, they will be the ones ultimately held responsible, if their network falls prey to illegal activity.

Works Cited

Duntemann, Jeff. Wi-Fi Guide. Scottsdale: Paraglyph Press, 2004.

Hurley, Chris, et al. Wardriving: Drive, Detect, Defend. Rockland: Syngress Publishing, 2004.

"IEEE 802.11" Wikipedia. 2005. 05 March. 2005 <<http://en.wikipedia.org/wiki/802.11>>.

"Unwired Pioneers" Computer World. 2005. 12 March. 2005
<<http://www.computerworld.com/mobiletopics/mobile/story/0,10801,63894,00.html>>.