

Aaron Sawyer  
04/18/08

SECURING WIRELESS NETWORKS: CLOSING THE BACK DOOR 1

Running head: A BRIEF GUIDE TO SECURING WIRELESS NETWORKS: CLOSING THE BACK DOOR

**A Brief Guide to Securing Wireless Networks: Closing the Back Door**

**in APA Style**

**Aaron Sawyer**

**East Carolina University**

## **ABSTRACT**

Wireless computer networks (WLANs) are being used in greater numbers now than ever before. Due to the unprecedented mobility, convenience, and flexibility that the technology offers, homes, businesses, and enterprises are deploying wireless networks in increasing numbers. Unfortunately, wireless networks may also act as an open door in the network security perimeter, allowing nearby attackers to eavesdrop on confidential communications, break into the wired network, or cause other serious problems. While the term "wireless security" has become an oxymoron for some in the face of recent wireless attacks, wireless networks can be made secure. This paper aims to give a brief history of wireless security, educate the WLAN administrator about the dangerous vulnerabilities of wireless networking, and make practical suggestions about how to close the door on potential intruders. Even though this paper focuses on the basic service and extended service set wireless architectures, many of the concepts can be applied to any wireless network.

## TABLE OF CONTENTS

<b>I. Introduction</b>	<b>Page 4</b>
<b>II. Brave New World – The dangers of wireless networks</b>	<b>Page 7</b>
<b>III. History of Wireless Security</b>	
<b>A. First Steps in Wireless Security – Wired Equivalent Privacy (WEP)</b>	<b>Page 10</b>
<b>B. It seemed like a good idea at the time – The Vulnerabilities of WEP</b>	<b>Page 14</b>
<b>C. The Dam Burst</b>	<b>Page 17</b>
<b>D. MAC filtering and Closed Networks have their own Issues</b>	<b>Page 20</b>
<b>E. Wi-Fi's WPA to the Rescue</b>	<b>Page 21</b>
<b>F. IEEE 802.11i &amp; WPA2 Finally Arrive</b>	<b>Page 25</b>
<b>IV. Common Wireless Attacks</b>	<b>Page 30</b>
<b>V. Wireless Networks used Today</b>	<b>Page 36</b>
<b>VI. Roads to Security – Commonsense Guidelines</b>	<b>Page 40</b>
<b>VII. The Battle Continues</b>	<b>Page 49</b>
<b>VIII. Works Cited</b>	<b>Page 50</b>

## **I. INTRODUCTION - WIRELESS LANs – THE BACK DOOR**

In July of 2005, outside of a Marshals store near St. Paul, Minn, a team of unknown attackers used a laptop computer along with what is believed to have been a telescopic antenna to lock onto, monitor, and eavesdrop on a wireless local area network (WLAN) used inside the store. After discovering that weak WEP (Wired Equivalent Privacy) encryption was being used, the team cracked the encryption scheme and began deciphering the wireless communications. As hand-held price checking devices, cash registers, and company computers communicated with one another, the attackers recorded their activities. The attackers also captured the usernames and passwords of employees as they logged in (Pereira, 2007).

After gleaning enough information from the wireless network traffic, the attackers focused their attacks on Marshal's parent company, TJX. Using the data that they had obtained, the group was able to break into TJX's central database, retrieving sensitive customer information, including Social Security numbers, driver's license numbers, military identification numbers, and credit card numbers. The stolen information was soon available for sale by the attackers on password-protected Websites for identity thieves (Pereira, 2007).

Signs of the heist first surfaced in November of 2005, when bogus credit card purchases began to appear. It wasn't until December 18 that an auditor discovered oddities in card data, indicating that something strange had taken place. Investigators were unable to catch the attackers since they used the IP addresses of private individuals and public locations. Forrester Research estimates that TJX's expenses from the breach could exceed \$1 billion in five years. These include expenses from

consultants, upgrades, attorney fees, and increased marketing, but not for possible lawsuit liabilities (Pereira, 2007).

The heist became known as the largest theft of credit-card numbers in history, with at least 45.7 million credit- and debit-card numbers being stolen. In addition, some 451,000 customers had private information stolen. Although the identity of the attackers is still unknown, security experts believe that the group may have been Romanian hackers or members of Russian crime groups. The attack has striking similarities to previous attacks perpetrated by these gangs; they are known for scoping out weak targets and methodically breaking into networks. Investigators blamed the success of their attacks in part on the weak wireless encryption scheme used (WEP). An auditor also later found that firewalls and data encryption were not implemented on a number of computers connected to the wireless network (Pereira, 2007).

While attacks of this scope and depth are relatively rare, the TJX case highlights the threats that computer networks face in the new wireless world. Marshals is not alone in its continued use of weak wireless security schemes. A study conducted by AirDefense Inc. in November of 2007 found that twenty-five percent of the wireless business networks scanned in retail outlets and malls around the world didn't use encryption of any kind. The same study found that another twenty-five percent of networks were using insecure WEP encryption, and that twelve percent used the name of the store as the SSID (Service Set Identification), giving potential attackers an instant "map" of the store. Other networks were found to be using access points (APs) with default passwords that could be easily broken into. In all, the study concluded that 85 percent of the wireless devices discovered would have been relatively easily to compromise or to eavesdrop on (AirDefense, 2007; Wilson, 2007).

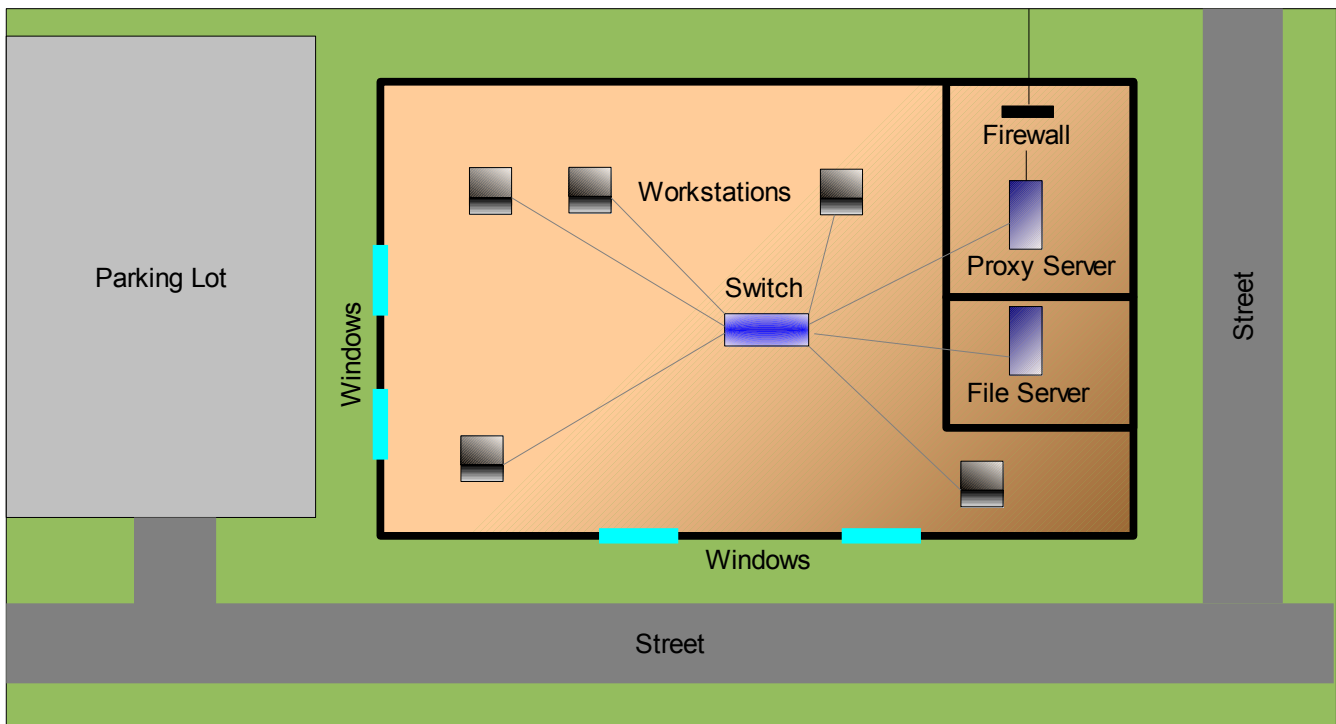
Wireless security is a widespread problem. Often, wireless networks open a back door in an otherwise secure computer network. This back door can form the weak point in the security perimeter that attackers are looking for. For homes, small businesses, and large enterprises, implementing effective wireless security is an absolute necessity. This paper will seek three major goals:

- 1) To give an historical background of wireless security,
- 2) To discuss the how each technology fairs against common attacks, and
- 3) To provide a list of ready-to-use wireless security practices that an organization can implement

There are three major wireless network architectures implemented today: the basic service set, the extended service set, and the independent service set. The basic service set (infrastructure mode) is a collection of wireless devices that are served by a single access point (AP). This configuration is used in small wireless network implementations. The extended service set is composed of two or more basic service set networks. It is able to cover a much broader area and can offer roaming services for wireless clients. This is frequently used in large wireless network implementations. Finally, the independent service set (ad-hoc mode) does not utilize an access point, but instead is completely peer-to-peer (Ciampa, 2006, pp. 154-156). Because most organizational wireless implementations utilize the basic service set and extended service set architectures, this paper will attempt to address them primarily, but the principles discussed could be applied to other topologies.

## II. THE DANGERS OF WIRELESS NETWORKS – BRAVE NEW WORLD

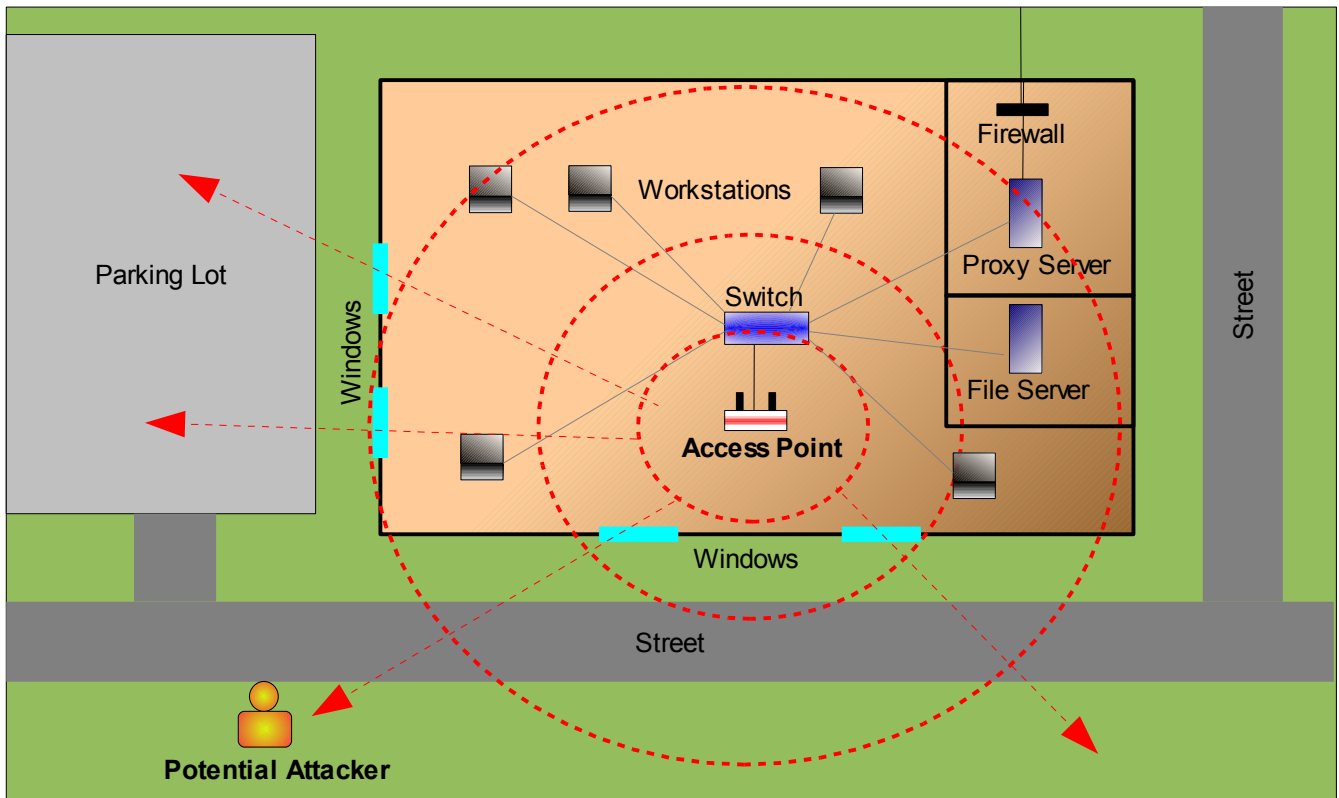
The fundamental characteristic of wireless networking is the ability to connect to a computer network without physical contact. Wireless networks broadcast data over publicly accessible radio frequencies instead of transmitting over private wires. In the past, businesses only dealt with wired networks. Such networks had few entry points and were generally harder to infiltrate from the outside. Attackers would have to connect to the physical LAN topology to infiltrate the network. Back-door attacks which penetrated a network from the inside were rare due to the feasibility of such an attack. See **Figure-1** for a simple example of a small business wired network.



**Figure-1.** A typical small business LAN.

With the introduction of wireless networks, the rules changed. No longer does an attacker have to connect to the physical network. Instead, an attacker can break into the network from across the parking lot. Today, attackers can scope out potentially vulnerable wireless networks from a moving vehicle, a popular practice known as wardriving.

Wireless networks open new doors into networks that previously did not exist, and can bring with them catastrophic consequences. As more and more small businesses and large enterprises implement wireless networks for increased productivity, mobility, and freedom, they often overlook the fact that they have just opened a gaping hole in their network's defenses. Refer to **Figure-2** for the small business network with a wireless connection. Notice that due to the wireless network broadcasting signals in all directions, the network is now accessible not only from within the intended building area, but also in the business's parking lot and even across the street. The wireless traffic travels even farther through unobstructed windows. This simple diagram does not show the additional wireless traffic emitted by clients.



**Figure-2.** A typical small business LAN with a wireless connection.

Due to these new vulnerabilities, wireless networks must be secured to protect the wireless data in transit as well as the internal wired network. As the TJX case demonstrates, wireless networks can form the stepping stone for an intrusion into the central network. The broadcast nature of wireless LANs makes security a particularly important subject.

### **III. THE HISTORY OF WIRELESS SECURITY**

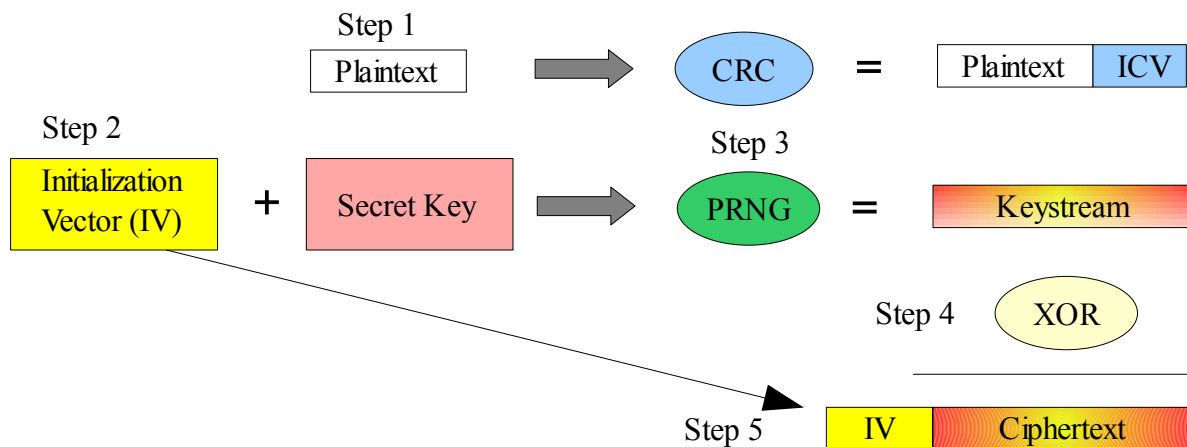
#### **A. FIRST STEPS IN WIRELESS SECURITY – WIRED EQUIVALENT PRIVACY (WEP)**

Even in its infancy, wireless network technology implemented a degree of security and privacy. The standard governing wireless networks is known as IEEE 802.11. As the original Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard was being developed, board members were aware of the new security challenges that broadcast communications brought with them. IEEE members saw that wireless networks needed to be protected from eavesdropping, unauthorized access, and data tampering. The team reasoned that because the confidentiality, access control, and data integrity of information is under increased threat over public airwaves, some mechanism was needed to bolster security to the level found in a wired network, at a minimum (Wong, 2003).

To provide data confidentiality in a wireless network, the IEEE decided that an encryption scheme was necessary to encrypt, or “scramble” the data as it traveled from one end point to another. If messages are encrypted before they hit the airwaves, they should be unreadable by unauthorized wireless users. Thus, encryption was proposed to prevent casual eavesdropping and provide data confidentiality (Brown, 2003).

The scheme developed by the IEEE group was WEP, Wired Equivalent Privacy. The system was meant to provide the “equivalent” amount of security thought to be present in a wired network. WEP was designed to implement the RC4 (Rivest Cipher 4) stream cipher, combining a 40-bit key with a 24-bit (theoretically) random number known as an Initialization Vector (IV) to encrypt messages (Wong, 2003). A stream cipher is an algorithm which replaces each character with another coded character.

Thus, each character is individually encoded (Ciampa., 2006, p. 270). Refer to **Figure-3** for a description of the WEP encryption process.



**Figure-3.** The WEP Encryption Process.  
Source: (Ciampa, 2006, p. 269)

In step 1, the unencrypted data (plaintext) to be encrypted is analyzed and a cyclic redundancy check (CRC) value is calculated. The CRC creates a unique checksum based on the plaintext message which verifies the contents of the message. WEP refers to this as the Integrity Check Value (ICV) and it is appended to the end of the plaintext message. In step 2, the secret WEP key is combined with a 24-bit value, known as the Initialization Vector (IV). The IV serves as a random value which changes with each packet. It helps to ensure that a random number will be generated in the next step. Without this random value, the keystream could be the same every time, and the encryption could be cracked. In step 3, the shared WEP key and the IV are entered into a pseudo-random number generator (PRNG) to create a random number: the keystream. The keystream is a series of 1's and 0's equal in size to the plaintext message and ICV. In step 4, the keystream, along with the plaintext message and ICV, are combined into a single message through an XOR operation. The result is ciphertext – the encrypted message. Finally in step 5, the IV value is added (without encryption) to the beginning of the ciphertext

because the message cannot be deciphered without it. At this point, the IV and ciphertext can be transmitted. A receiver can use its copy of the shared WEP key to backtrack through the process to produce the original message (Ciampa, 2006, p. 269).

To provide wireless authentication and access control, the IEEE team made two authentication types available:

1. Open system authentication
2. Shared key authentication

Open system authentication is not truly authentication at all. All a wireless user needs is the SSID, or name of the network to join. If the user knows the name of the network, he can join the network. Open system authentication is therefore an “open” system. WEP could still be used to encrypt messages, but it is not used to authenticate new devices wanting to join the network (Ciampa, 2006, pp. 270-271; Microsoft Technet, 2006)

In shared key authentication, the WEP key is used to provide data confidentiality and to restrict network access. If WEP-enabled wireless devices receive packets without proper WEP encryption, the packets can be ignored, thus theoretically limiting the secured wireless network to only those devices which have the WEP key (Brown, 2003).

Lastly, to provide data integrity, the 802.11 standard included an integrity checksum value, computed by both receiver and transmitter. If the checksum does not match, the packet is discarded. Thus, if any

packet happened to be manipulated, it would theoretically be ignored (Brown, 2003).

Outside of the IEEE 802.11 standard, two other notable access control mechanisms were soon developed by wireless device vendors:

1. MAC Filtering
2. Closed Networks

To help restrict unauthorized wireless access, vendors offered a MAC (Media Access Control) address filtering option for wireless access points. The MAC address is a unique number made up of 12-hexadecimal digits which are “burned” into all network interfaces. Because it is unique to each interface, an administrator can theoretically deny access to any wireless device not specifically allowed in a preconfigured list. Although this became a useful option in many small networks, it brought with it its share of disadvantages, most notable of which is the trouble of maintaining a list of static addresses.

The “closed network” concept is a proprietary access control method created by Lucent. In this scheme, the SSID of the network is kept a secret, and only those stations knowing the SSID may join the network. Thus, if the SSID is indeed secret, only authorized devices will be able to join the network (Arbaugh, Shankar, Wan, & Zhang, 2002). The option to disable SSID broadcasts has since been offered by many access point vendors (Ars Technica, 2002, p. 3).

The original wireless standard, which included WEP, became known as IEEE 802.11 and was adopted in 1997 (Wi-Fi Alliance, 2003). Unfortunately, the WEP encryption system was not subjected to

significant peer review before release, and it wasn't long until serious vulnerabilities were found (Wong, 2003).

## **B. IT SEEMED LIKE A GOOD IDEA AT THE TIME... - THE VULNERABILITIES OF WEP**

WEP seemed like a good idea at the time. At a time when encryption schemes were under tough scrutiny due to export restrictions and few users had gone wireless, revealing few vulnerabilities, WEP seemed like just the thing to make wireless networks secure, or at least as secure as their wired counterparts.

In 2001, WEP's first vulnerabilities were revealed. Two major papers by researchers at Berkley and the University of Maryland (UMD) found many vulnerabilities, including:

- Key reuse or “keystream attacks” due to “collisions”
- Weak message authentication
- Weak 802.11 access control mechanisms, including WEP cryptographic authentication
- Poor key management (the use of a single key by many users)

The Berkley team pointed out that the initialization vector (IV) used to make a random keystream for packets is too small. Because the IV is just 24 bits long, it provides only 16,777,216 possible values, and it will eventually repeat itself, creating an IV “collision.” Attackers could capture traffic on the network, wait for an IV collision to occur, and then use the identical keystream to help crack the

keystream (a keystream attack). With an identical IV, if the plaintext of one of the packets can be discovered, the keystream can be deduced (Borisov, Goldberg, & Wagner, 2001).

There are many possible ways to get the plaintext of the message. One can predict the IP headers used, perform a dictionary attack (guess), or even attempt to inject traffic across the network. This could be done by sending an email to a wireless user with known contents and waiting for the user to open it. At any rate, once a keystream has been isolated, messages encrypted with it can be deciphered. If an attacker can build a table of all of the keystreams used in the WEP network, the WEP key isn't even needed to decipher communications; the keystreams can be used (Borisov, Goldberg, & Wagner, 2001).

The Berkley team also found that due to weak message authentication, encrypted packets could be tampered with by having their ICV values modified. This could be accomplished by flipping the correct bit in the packet, and is possible because RC4 is a stream cipher, encrypting each character individually. Packets could then be injected back into the WLAN by using a previously used IV. Packets with reused IVs are perfectly acceptable in WEP (Borisov, Goldberg, & Wagner, 2001).

A very important finding of the Berkley team was that shared key authentication is inherently insecure. In shared key authentication, the device attempting to join the WLAN first requests to be authenticated by the AP. The AP then sends a challenge back, which is a random 128-byte fixed length string. The device requesting to be authenticated must respond by encrypting the challenge text with its WEP key and sending it back. If the response is validated by the AP, then the requesting device is authenticated and may join the network (Borisov, Goldberg, & Wagner, 2001).

The problem with the challenge-response method is that the challenge is sent in plaintext. An observer views the unencrypted data and then views that same data encrypted. By passive observation, an attacker can determine the keystream used and can use it to encrypt further messages and decrypt messages using that same IV and keystream. Furthermore, because WEP allows packets to be injected without the key (all one needs is the keystream and IV), an attacker can request to be authenticated and respond to the challenge text with the same keystream and IV that was observed. Since the length of challenge is always 128-bytes, the response will be valid. Thus, an attacker can become authenticated in a shared key authentication network by simple observation (Borisov, Goldberg, & Wagner, 2001). Even so, the attacker would still not be able to use the WEP-encrypted network without further attacks due to the presence of encryption (Arbaugh, Shankar, Wan, & Zhang, 2002).

Because the challenge-response method used in shared key authentication is so flawed, shared-key authentication is now considered to be worse than open authentication with WEP. In fact, Microsoft now recommends that organizations stuck with WEP disable shared-key authentication and use open-authentication with WEP data encryption enabled (Microsoft Technet, 2006).

Another issue arising out of weak authentication is the man-in-the-middle attack. Because authentication is one-way, with the client being authenticated but not the AP, nothing is stopping an attacker from setting up a fake AP (a rogue AP) and acting as a middle man for other users, passing their data along to the legitimate AP, but also recording and/or modifying their traffic. This is possible due to the cryptographic weaknesses of WEP and a lack of two-way authentication (Brown, 2003).

The Berkley researchers also noted that key management is often poorly implemented, and most organizations use the same key for all wireless users. WEP attacks are easier when the same key is used. Because of the hassle of reconfiguring the WEP key on every wireless client device, the WEP key is largely static (Arbaugh, Shankar, Wan, & Zhang, 2002).

These vulnerabilities formed substantial cracks in the security of WEP. The popular consensus was, however, that these flaws could be patched. Long-key length versions of WEP were created and released, but they did not address WEP's weaknesses. Deceptive advertising by vendors didn't help matters either. Vendors who advertised 64-bit WEP or 128-bit WEP encryption mislead consumers. 64-bit WEP is actually composed of a 40-bit key and a 24-bit IV. Likewise, 128-bit WEP is actually a 104-bit WEP key plus the IV. Even with longer encryption keys, WEP's problems remained.

### **C. THE DAM BURST**

The eventual “bursting of the dam” came in 2001 when Scott Fluhrer, Itsik Mantin, and Adi Shamir unveiled enormous flaws in the heart of WEP; in the Key Scheduling Algorithm (KSA) (Gast, 2002). Fluhrer, Mantin, and Shamir found that RC4, “the most widely used stream cipher in software applications,” had two significant weaknesses. First, it was found to have an “invariance weakness” in which a small part of the key determines a large portion of the KSA output. Second, a portion of the key input to the KSA was found to be “exposed to the attacker.” Fluhrer, Mantin, and Shamir found that because the same secret portion of a key is used with different exposed values, an attacker could reconstruct the secret portion by analyzing the first word of keystreams. In short, correlations were found to exist between the WEP key and the “random” keystream and these similarities were found to

be revealed to attackers (Fluhrer, S., Mantin, I., & Shamir, 2001).

By collecting encrypted packets with certain IVs (called “weak” IVs), an attacker could backtrack through the encryption process and crack the key (Hendrickson & Piotrowski, n.d., p. 4). By taking advantage of these leaked correlations, one could derive the WEP key by capturing enough encrypted traffic. Fluhrer, Mantin, and Shamir even formulated an attack that they proposed may crack the encryption scheme. A month later, Adam Stubblefield successfully implement the attack (AirSnort, 2004). Stubblefield stated that from 5,000,000 to 6,000,000 encrypted packets were needed to crack a 104-bit WEP key (Stubblefield, Ioannidis, & Rubin, 2001). The cracking utilities AirSnort and WEPCrack were soon released on the Internet, and became the first publicly available implementations of the FMS attack (AirSnort, 2004).

The findings of Fluhrer, Mantin, and Shamir changed everything. It was apparent now that WEP was fundamentally flawed (Gast, 2002). The attacks on WEP didn't stop, however. As time went on, new and better ways to crack WEP were discovered. In 2004, a hacker known as KoReK substantially improved upon the FMS attack, reducing the necessary number of captured packets to crack a 104-bit WEP key down to 500,000 to 2,000,000 packets. A year later, Andreas Klein demonstrated that there are even more correlations between the RC4 keystream and the key than Fluhrer, Mantin, and Shamir had found. Based on Klein's work, German researchers Andrei Pychkine, Erik Tews, and Ralf-Philipp Weinmann formed a new attack referred to as aircrack-PTW in April of 2007. Using this optimized attack, one can crack a 104-bit WEP key with 40,000 to 85,000 packets at a success rate of 50 to 95 percent, respectively. The authors of the attack claim that it takes a mere 3 seconds on a Pentium-M 1.7 GHz computer system to crack the key from captured packets (Tews, Pychkine, & Weinmann, 2007a).

The name of the team's paper revealing the new attack is “Breaking 104 bit WEP in less than 60 seconds,” (Tews, Pyshkin, & Weinmann, 2007b) Clearly, WEP is woefully inadequate and very broken.

Even to this day, new attacks are being formulated against WEP with great success. One example is the “Latté Attack” or “AP-less WEP cracking” found in October of 2007. In this attack, an attacker can take advantage of the Windows Wireless Stack and WEP flaws on a client system to obtain the WEP key from a corporate network (Phifer, 2007e).

The long and the short of these vulnerabilities is that WEP has broken encryption, flawed authentication methods, and a flawed message integrity system, making it vulnerable to a wide range of wireless attacks. It is ironic that the three main aims of the IEEE 802.11 group, confidentiality, access control, and data integrity, are all broken in WEP. In summary, WEP has many vulnerabilities, including:

- Brute force attacks (with a 40-bit key, such an attack is feasible)
- Dictionary attacks (the key can be guessed if weak)
- Keystream attacks (keystream cracking allows eavesdropping & message injections)
- Statistical correlation attacks (FSM, KoReK, and PTW attacks allow key cracking)
- Man-in-the-middle attacks (due to one-way authentication)
- Denial of service attacks (through disassociation frames)
- Weak message authentication (the ICV can be modified, packet injections possible)
- Flawed shared-key authentication (keystream exposed)
- Poor key management (the use of a single key by many users)

## **D. MAC FILTERING AND CLOSED NETWORKS HAVE THEIR OWN ISSUES**

While MAC filtering is a viable choice for many small businesses and home environments, its usefulness disappears in larger wireless deployments. It becomes overly cumbersome to keep static lists of every wireless device in use at a large organization. In addition, this method of access control can be easily faked, or “spoofed.” Simply looking at wireless packets provides attackers with valid MAC addresses. By typing two root commands on a LINUX system, an attacker can easily spoof a MAC address and can circumvent this access control method. On a Windows system, the registry can be modified to change the MAC address (Shimonski, 2003).

Lucent's proprietary “closed network” concept limits access to only those who know the SSID by disabling SSID beaconing on the access point. While this sounds like a good idea, it is well known that SSIDs are broadcast without encryption in many management messages. With a sniffer, anyone can determine the SSID and join a closed network. Thus, because the SSID is not truly a secret, closed networks are not really closed (Arbaugh, Shankar, Wan, & Zhang, 2002).

Although it has long been recommended in security circles to disable SSID beaconing wherever possible, today it is recommended to *leave SSID beaconing enabled*. With SSID beaconing disabled, all clients are forced to constantly send out probe requests as they attempt to locate the hidden network. These probe requests contain the SSID and are sent out from clients wherever they are - even at remote locations. This is a potential security threat as an attacker could capture these probes, determine the SSID, and then set up a rogue access point with the captured SSID (creating an “evil twin”). From here,

the client may attempt to connect to the fake network, and the attacker can capture the authentication traffic for use in future attacks (Ou, 2008). Microsoft now “strongly” recommends leaving SSID beaconing enabled so that clients will not automatically send out these probe requests (Microsoft Technet, 2006). In addition, disabling SSID beaconing will increase the traffic overhead of the network and can degrade performance (Phifer, 2003; Moskowitz, 2003, p. 3). In summary, closed networks are more trouble than they are worth.

On the other hand, disabling SSID beaconing will stop many casual snoopers from discovering the network. Disabling SSID beaconing may be desirable for small home-based wireless networks with clients that are connected for short periods and do not leave the immediate area (Phifer, 2003). Many IT experts argue, however, that the threat posed by probe requests broadcast by clients negates any benefit gained by “hiding” the SSID (Ou, 2008).

### **E. WI-FI'S WPA TO THE RESCUE**

After serious WEP vulnerabilities were discovered in 2001, the wireless world was looking for a solution that would address WEP's shortcomings. WEP2 and Dynamic WEP are two of these attempted fixes. WEP2 attempted to address WEP's problems in two ways: by increasing the WEP key to 128 bits instead of 64 and by implementing a new authentication scheme known as Kerberos. Unfortunately, these two steps did not substantially improve the security of WEP. Because WEP2 had its own share of weaknesses it was rarely implemented (Ciampa, 2006, p. 293).

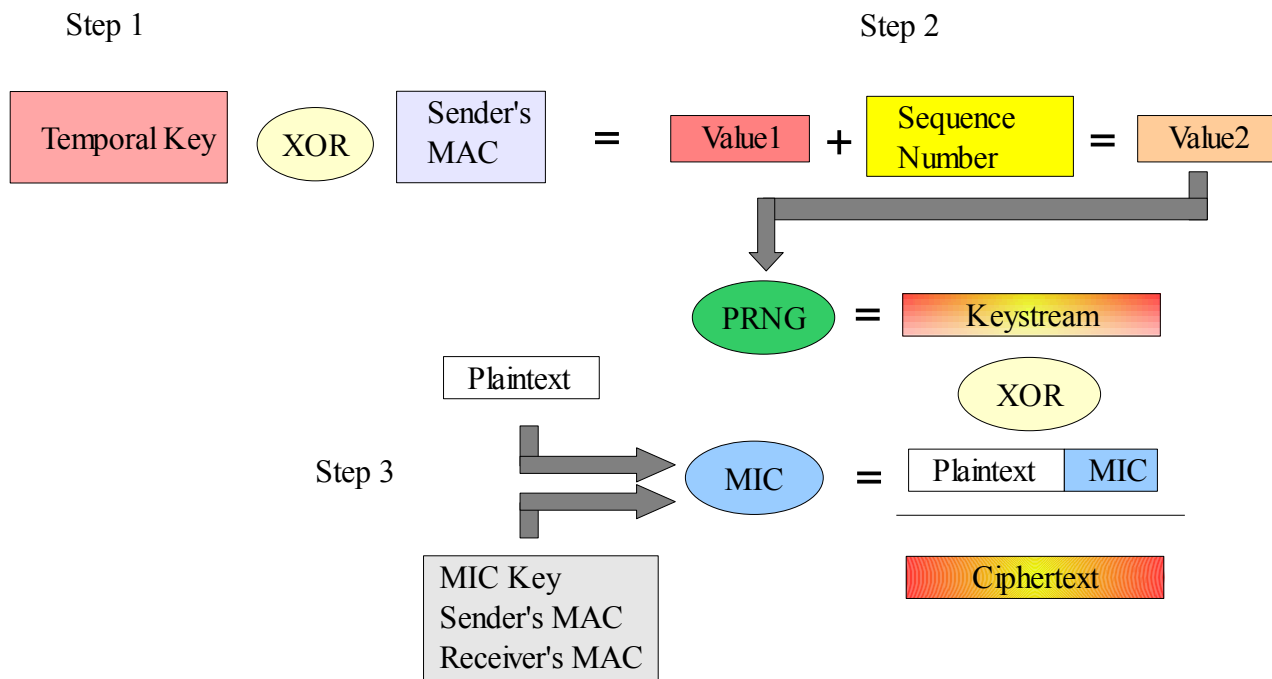
Dynamic WEP was another proposed solution. Dynamic WEP frequently rotates keys, making packets harder to crack. Keys can be set to rotate at a specified period, such as every 15 minutes. While Dynamic WEP largely overcomes the weaknesses of WEP's weak IV's, it is not a total security solution and is still susceptible to man-in-the-middle and denial-of-service attacks. Because of this, it was not widely implemented either (Ciampa, 2006, pp.293-294).

In March of 2001, IEEE TG1 split into two groups, one of which would create a new wireless security scheme. It was three years until IEEE 802.11i, the new wireless security model, was finally ratified. During this time, the Wi-Fi Alliance, a consortium of equipment manufacturers and software providers, decided that wireless security could wait no longer and developed Wi-Fi Protected Access (WPA). WPA was introduced in October of 2003 with the goal of providing security for present and future wireless devices. WPA is a subset of the 802.11i standard and implements security through encryption and authentication (Ciampa, 2006, pp. 49, 295, & 297)

WPA was designed to replace WEP and was designed to fit within the WEP procedure with a minimal amount of change (Ciampa, 2006, p. 305). WPA uses the Temporal Key Integrity Protocol (TKIP) rather than a static encryption key. Instead of using a pre-shared key which creates a keystream, WPA uses a pre-shared key to serve as the seed for generating the encryption keys. WPA increases the IV space to 48 bits (now called the “sequence number”) and uses a long, 128-bit per-packet key to dynamically encrypt each packet with a different key (Ciampa, 2006, pp. 304, 306, & 297). This solves the IV collision problem and eliminates the correlation weaknesses of WEP.

WPA also eliminates the Cyclic Redundancy Check (CRC) function and replaces it with Message

Integrity Check (MIC). WEP's CRC system does not adequately protect the integrity of data, as one can alter both the packet and the CRC value and craft a valid packet. WPA's MIC implements a strong mathematical function computed by the transmitter and receiver. If the computed MIC value does not match the packet's MIC value, the packet is discarded. This makes packet modification extremely difficult, if not impossible (Ciampa, 2006, p. 298). Refer to **Figure-4** for a description of the WPA encryption process.



**Figure-4.** The WPA Encryption Process.  
Source: (Ciampa, p. 305)

In step 1, a temporary key is generated and is XORed with the sender's MAC address, creating Value1. In step 2, Value 1 is mixed with a sequence number (which replaces the IV) to produce Value2, the per-packet key. Value2 is then run through a Pseudo Random Number Generator (PRNG), as in WEP. The output of the PRNG is the keystream, which is used for encryption. In step 3, instead of inputting the plaintext message into a CRC function, the MIC Key and the sender's and receiver's MAC addresses

are all entered into a MIC function. The result is the plaintext message with a MIC key appended.

Finally, the plaintext message and the MIC key are XORed with the keystream, producing the ciphertext. The receiver uses its copy of the pre-shared key to backtrack through the encryption process and produce the original plaintext message (Ciampa, 2006, p. 305).

TKIP in WPA is composed of three major components:

- 1) the MIC, which protects against packet forgeries
- 2) an IV sequence, which protects against replay attacks by sequencing each packet, and
- 3) TKIP key mixing, which uses temporary per-packet keys with limited lifespans

TKIP forms the heart of WPA. Compared with WEP, WPA requires similar computational effort and superior security (Ciampa, 2006, p. 306). Because the encryption process is so similar to WEP, implementing WPA can be as simple as upgrading client software and updating the firmware of older access points (Ciampa, 2006, p. 299).

WPA offers two authentication modes: 1) pre-shared key (PSK) authentication based on a secret key shared among devices, and 2) authentication via a dedicated authentication server. The pre-shared key mode is intended for personal and small home /office environments (SOHO) whereas authentication via an authentication server is designed for enterprise networks. The IEEE 802.1x standard defines how authentication takes place with an authentication server, and is discussed in more detail in the next section (Ciampa, 2006, pp. 304, 308).

Although WPA provides comprehensive and robust security in a small home /office environment and adequate security in an enterprise environment, it is not immune to attack. Brute-force dictionary attacks are possible in WPA-PSK (Pre-Shared Key) networks. The popular hacker's tool “coWPAtty” can be used to launch dictionary attacks against WPA-PSK networks (Wirelessdefence.org, 2006). To avoid a successful dictionary attack, it is important to enter either a random sequence of at least 20 ASCII characters or a random sequence of at least 24 random hexadecimal digits as the passphrase (the passphrase is used to create the shared secret) (Ciampa, 2006, p. 307). Words, which are not random, should never be used in a passphrase.

WPA was meant to fit within the confines of the WEP structure. Because WPA was not created from scratch, security vulnerabilities may be discovered in the future (Ciampa, 2006, p. 311). Today, it is recommended to use WPA2 (discussed shortly) instead of WPA whenever possible.

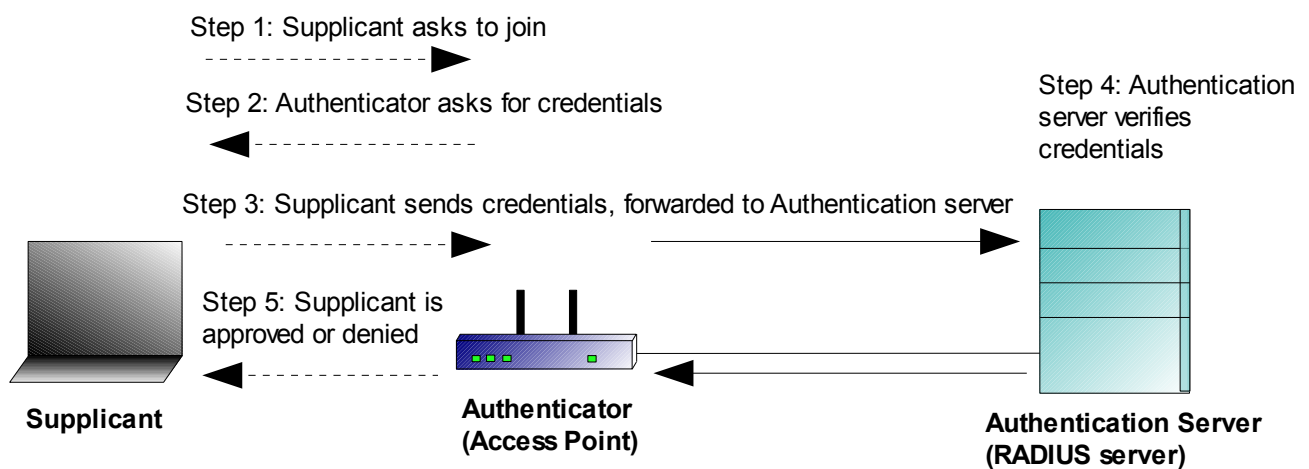
## **F. IEEE 802.11i & WPA2 FINALLY ARRIVE**

A year after WPA was introduced, the IEEE 802.11i standard was finally ratified. Also referred to as Robust Security Network (RSN), IEEE 802.11i is considered to be a solid security model, providing a high level of wireless security. Instead of a stream cipher such as RC4, IEEE 802.11i uses the block cipher Advanced Encryption Standard (AES) for encryption. AES breaks the plaintext down into blocks of 8 to 16 bytes and manipulates these blocks. Through a series of iterations, or rounds, the bytes are rearranged and substituted. Multiplication is then performed on the changes. The result is a much stronger encryption scheme, practically immune from modern brute-force attacks (Ciampa, 2006, p.

295).

Authentication and key management in IEEE 802.11i are provided by the IEEE 802.1x standard. IEEE 802.1x was originally designed for wired networks, and operates using port security. A particular device requesting access to the network is restricted from doing so or receiving any traffic from that network until its credentials are verified. IEEE 802.1x blocks all ports to a device until it is authenticated by an authentication server. An authentication server is a server which verifies the identity and privileges of requesting devices (Ciampa, 2006, p. 296). This could be a dedicated server or an integrated module in the access point (Chen, Jiang, & Liu, 2005).

An example of an authentication server would be a RADIUS (Remote Authentication Dial-In User Service) server. Refer to **Figure-5** for a simple description of the authentication process in a RADIUS-based IEEE 802.1x system.



**Figure-5.** IEEE 802.1x authentication  
Source: (Ciampa, p. 297)

First, the requesting device, the supplicant, associates with the access point, often called the authenticator. The authenticator acts as a proxy for the user's authentication, and completely blocks off the protected network from the supplicant. In fact, it only opens a single port to the supplicant with itself. The supplicant begins by asking for network access. The authenticator asks for its credentials, and receives them from the supplicant. The authenticator then forwards on the request and credentials to the authentication server, which in this case is the RADIUS server. The authentication server first evaluates if the access point is allowed to make such requests. If it is, the RADIUS server looks up the user's credentials and determines if the user is in fact permitted the access that is being requested. Depending on the authentication method and the credentials used, challenge text may be sent back to the supplicant, which the supplicant must answer with the correct value. Once the authentication server has decided whether or not the supplicant should be granted access, it sends its answer to the authenticator, which is relayed to the supplicant (Ciampa, 2006, pp. 296-297 & 309-310; Fleishman, 2003). Using this method, the authentication server is never directly contacted. This affords a greater degree of security for the authentication server, which contains the valuable database of user credentials.

IEEE 802.1x uses the Extensible Authentication Protocol (EAP) to handle the presentation of user credentials, which may be digital certificates, usernames and passwords, smartcards, or secure IDs. Many EAP types are available for implementation. Common EAP types that are used include EAP-Transport Layer Security (EAP-TLS), EAP-Tunneled Transport Layer Security (EAP-TTLS), and Protected Extensible Authentication Protocol (PEAP) (Chen, Jiang, & Liu, 2005, p. 28; Wi-Fi Alliance, 2003, p. 5).

Using an authentication server makes user administration easier and can thwart man-in-the-middle attacks due to two-way authentication. By using an EAP implementation such as EAP-TLS, EAP-TTLS, or PEAP, for example, both the client and server will mutually authenticate each other and man-in-the-middle attacks become much harder to wage (Intel Corporation, 2007).

In September of 2004, the Wi-Fi Alliance introduced Wi-Fi Protected Access 2 (WPA2), based on the IEEE 802.11i standard. WPA2 implements AES encryption and provides an even stronger security system for WLANs than WPA. WPA2 is similar to 802.11i, but it allows for greater interoperability with WPA (Ciampa, 2006, p. 299). Encryption under WPA2 uses the AES-CCMP (Counter Mode CBC-MAC Protocol) protocol. The AES algorithm deals with blocks of 128 bits, but the length of the cipher keys and rounds of encryption can be changed. In the IEEE 802.11i/WPA2 implementation of AES, a 128-bit key is used, with each round iterated 10 times (Ciampa, 2006, p. 307).

Like WPA, WPA2 offers two security modes: 1) pre-shared key authentication based on a shared secret, and 2) authentication by an authentication server (IEEE 802.1x). Pre-shared key authentication is intended for personal and small office (SOHO) use where an authentication server is unavailable. (Ciampa, 2006, pp. 306, 311). Like WPA, WPA2 networks using a pre-shared key are vulnerable to dictionary attacks (Phifer, 2007b). It is important to make the secret passphrase as long and as random as possible (at least 20 characters long), with a healthy mix of various random characters (Ciampa, 2006, pp. 306,307, & 311).

The authentication method recommended for enterprise use is IEEE 802.1x - currently the strongest authentication method available. IEEE 802.1x is currently very attractive to enterprise environments in

which many distinct wireless users must access the network. IEEE 802.1x allows for centralized wireless access management (Ciampa, 2006, pp. 306 & 311).

In summary, wireless security has been a bumpy road. First there was WEP, but it had serious vulnerabilities. This was followed by a more secure WPA, and finally, a very secure WPA2. With a basic understanding of these security systems, we can now focus on how each of these systems holds up against common wireless attacks.

## **IV.COMMON WIRELESS ATTACKS**

The following section lists some common wireless attacks and how network security solutions handle these attacks. Best-selling author Robert Shimonski (2003) classifies wireless attacks into four main categories:

1. Passive Attacks (eavesdropping packets)
  - a. Brute force attacks
  - b. Brute force dictionary attacks
  - c. Statistical correlation attacks
2. Active Attacks
  - a. Unauthorized Access (unwanted file sharing, adding/changing/deleting data)
  - b. Spoofing
  - c. Denial of Service attacks
3. Man-In-The-Middle attacks
4. Jamming attacks (also Denial of Service)

Passive attacks are performed by passively capturing wireless traffic. Thus, passive attacks use eavesdropping to further their purpose. If the network is already open, eavesdropping could be considered an attack in and of itself. If valuable information is transmitted over an open wireless connection, for example, an attacker's eavesdropping would have already achieved the purpose of capturing that information (Shimonski, 2003).

The freeware program “Netstumbler” is a popular wireless program that is commonly used to locate wireless networks. It can identify the Service Set Identifier (SSID), determine the encryption used, and even determine the manufacturer of the access point. If the SSID of the access point is hidden, other programs such as “Ethereal,” WildPacket’s “AiroPeek,” or “Kismet” can be used to locate a WLAN and determine the SSID (Kismet, n.d.; Shimonski, 2003).

Often, the capturing of wireless network traffic is but the first step in an attack. Brute force attacks are attacks which attempt to break the encryption of captured traffic through brute force, trying every possible key combination. At lower bit strengths, such as WEP's original 56-bit encryption, such attacks become feasible with modern equipment. Higher bit strengths, such as 128-bit encryption, make these attacks less feasible.

A particularly popular kind of brute-force attack is the dictionary attack, also called the “offline” dictionary attack. It differs from the raw brute force method in that it uses a dictionary of commonly used words to attempt to break the encryption key. Such attacks can be very effective if a weak passphrase is used. For example, if the secret passphrase is “secret,” a dictionary attack would attempt different commonly used words in encryption and compare the result with the captured traffic. When there is a match (in this case, “secret”), the passphrase (key) is cracked. WPA/WPA2 networks using a pre-shared key are vulnerable to this attack. As a matter of fact, the dictionary attack is the only known cryptographic vulnerability of WPA/WPA2-PSK networks (Aircrack-ng, 2008; Shimonski, 2003).

Statistical correlation attacks exploit flaws in the encryption scheme to crack the key from captured traffic. The most widely known correlation attacks are the WEP attacks FMS, KoReK, and PTW. Flaws

in WEP reveal correlations between the key and the keystream, and from these correlations, attackers can eventually crack the key. WPA and WPA2 networks are currently believed to be immune from these attacks (Aircrack-ng, 2008).

Active attacks are attacks which not only receive wireless traffic but also transmit wireless traffic, taking an active role in the targeted wireless network. After gleaning information from a passive attack, an active attack can be waged. Unauthorized access, spoofing, and denial of service attacks can be considered to be active attacks (Shimonski, 2003).

Unauthorized access is the use of resources by unauthorized parties. If a wireless network is open, with no encryption, attackers may be able to access file shares, add or delete files, and introduce malware onto connected computer systems. The TJX break-in in our introduction is an example of the unauthorized use of data. WEP has known flaws that enable attackers to crack the key and gain entry into the wireless network. WEP's shared-key authentication system is also flawed, and through eavesdropping, an attacker can observe the authentication sequence and spoof an authenticated connection (Shimonski, 2003).

Because the goal of many wireless attacks is the unauthorized access of resources, sound security practices are needed to protect resources from wireless attack. This includes setting the proper file and folder permissions on computers connected to the wireless network as well as implementing sound wireless security, such as WPA/WPA2. In addition, a firewall between the access point and the wired network will help to protect the internal network from possible intrusions. Installing software firewalls on wireless clients helps to protect them from unauthorized wireless access.

Spoofing is the impersonation of an authorized station to gain unauthorized access to a wireless network. This is commonly done to circumvent MAC filtering. By changing a registry entry on a Windows system or by entering two root commands on a LINUX system, an attacker's MAC address can be spoofed to match that of a valid user. This is a known weakness of MAC filtering (Shimonski, 2003).

Active denial-of-service attacks attempt to deny service to authorized parties. Over a wireless network, these attacks can be identical to their wired counterparts and include *ping floods*, *SYN attacks*, *fragment attacks*, and *Distributed DoS (DDoS)* attacks. Open networks are vulnerable to these denial-of-service attacks, and because WEP is easily cracked, it too is vulnerable (Shimonski, 2003).

Fortunately, due to strong encryption and authentication, WPA/WPA2 based networks are protected from these classic attacks. However, WPA networks can be vulnerable to a sly version of the DoS attack. WPA access points have the option of stopping all transmissions (disassociating all devices and preventing new associations) for one minute if two packets with malformed MICs are detected within one minute. Therefore, if this option is enabled, an attacker could craft malformed packets with bad MICs for the sole purpose of shutting down the network; a denial of service attack. Since this MIC countermeasure is optional, it can be disabled, preventing this particular DoS attack. (Ciampa, 2006, p. 298; Maufer, 2003, p. 281).

One wireless form of a denial of service attack is the kicking off of legitimate users by sending false disassociation frames. When the access point receives these frames, it will disconnect the (supposed)

sender from the network. WEP and WPA/WPA2 networks are vulnerable to these attacks, and they can be very difficult to identify and defend against. Special RF scanners can be used to detect and pinpoint unauthorized wireless devices that may send out these frames (Ciampa, 2006, p. 383).

Man-in-the-middle attacks are a class of attacks that set up rogue (illegitimate) access points within range of wireless clients for the purpose of acting as a “middle man” for clients. When clients see the rogue access point (also called an “evil twin”), the SSID matches the legitimate access point and they mistakenly join it instead of the true access point. From here, the attacker can forward on their requests to the true access point, but he can monitor or change their traffic. It has been common in the past for attackers to use two network cards in their laptops, one serving as the phony access point, and the other forwarding on traffic to the real access point. Attackers may hide their rogue access points in closets or under desks near the true access point (Shimonski, 2003).

Historically speaking, man-in-the-middle attacks have always been a problem with wireless networks. WEP-based networks are very vulnerable to man-in-the-middle attacks. WPA and WPA2-based PSK networks are not immune to man-in-the-middle attacks because of their lack of mutual authentication (Phifer, 2007a). WPA and WPA2-based networks using IEEE 802.1x enterprise authentication are protected from man-in-the middle attacks if an EAP type supporting mutual authentication is used (Intel Corporation, 2007).

Rogue access points themselves are a major security threat for wireless networks, even if they are not set up by attackers for a man-in-the-middle attack. Rogue (unauthorized) access points can be set up by employees to make networking easier. Because unauthorized access points connected to the LAN open

a new door into the internal network, they effectively bypass established security mechanisms and present a clear danger. WPA/WPA2 clients are not inherently protected from joining unauthorized access points, but employing IEEE 802.1x authentication can prevent users from mistakenly joining phony access points (Bulk, 2006; Phifer, 2007a).

To protect against rogue access points, employees should be banned from setting up their own access points and the organization's airwaves should be periodically scanned for unknown access points (Cisco Systems, Inc., 2007). A Wireless Intrusion Prevention System, which continuously scans for such activity, can be very useful in detecting unauthorized access points (Phifer, 2007a).

Finally, jamming attacks use RF transmissions to flood the airwaves with noise and block wireless network transmissions. This is an inherent problem in wireless networks because traffic collisions are avoided by transmitting devices. If wireless traffic (or a traffic-like transmission) is detected, stations must wait until the airwaves are clear again before they can transmit. Cordless phones and microwave ovens are known to interfere with wireless LANs. In addition, Bluetooth devices and other wireless hardware can cause wireless jamming. Jamming may be intentional or unintentional and is relatively rare. To prevent jamming, policies must be made banning the use of interfering equipment near the wireless network (Ciampa, 2006, p. 280; Shimonski, 2003).

## V. WIRELESS NETWORKS USED TODAY

With an understanding of the different wireless security mechanisms available and the common wireless attacks waged on wireless networks, we can now turn our attention to examining the wireless networks used today. There are many variants of wireless networking security in use today. The most prevalent systems found in operational use are:

1. No Security
2. WEP
3. WPA/WPA2-PSK
4. WPA/WPA2 with RADIUS
5. VPN (IPSEC, SSH, or TLS / SSL over WLAN)

Wireless LANs with no security are the most vulnerable to attack. They are in effect “wide open.” There is no authentication of users, no encryption of transmissions, and no security measures in place. This is a wireless attacker's dream. With no security measures, an attacker is free to eavesdrop, use the Internet connection (if available), access any file shares, or perform other malicious actions.

There are many reasons why wireless networks are left unsecured - one is ignorance. Because wireless networks are so easy to install, many people just plug them in and use them. While the networks do “work,” they also form a soft spot that is just waiting to be taken advantage of.

As we have seen, WEP – secured wireless LANs are not truly secure. While WEP's vulnerabilities have been known for years, a large percentage of current companies still use WEP (Phifer, 2007d). For many, the reason comes down to cost. More efficient security mechanisms such as WPA must be implemented within the device itself. While the firmware on most WEP-based access points and wireless network interface cards can be upgraded to support WPA, some devices cannot be upgraded to support WPA. If the device does not support WPA, the administrator must replace the device to implement WPA (Wi-Fi Alliance, 2003, p. 2).

Many early point-of-sale retail computer systems and scanners only support WEP (Fleishman, 2007). The cost of replacing wireless network devices is a heavy burden to many small businesses who cannot invest in more expensive equipment. Other organizations are simply ignorant of the security vulnerabilities of WEP. It is also easier to setup a wireless network the way it comes; without upgrades. For these reasons, a number of organizations still use WEP in their wireless networks. While WEP is insecure, it is definitely better than no security at all.

Before WPA became available, the conventional wisdom for securing wireless networks was to treat them as insecure, placing access points outside of a firewall and then tunneling VPN connections through to the wired network. Any other traffic would be insecure (Fleishman, 2003). While it certainly is more secure to treat a wireless connection as untrusted, and organizational firewalls are extremely important, WPA has allowed many organizations to treat wireless networks with increased trust. If properly configured, WPA – based wireless LANs are relatively safe from wireless attacks. The symmetric keys used in WPA-PSK cannot be easily cracked if a strong passphrase (which is used to create the pre-shared key) is used. Attackers are currently limited to dictionary attacks in WPA. The

security of the symmetric key depends on the strength of the passphrase used; if it is easy to guess, the key may be easily cracked. This is why a strong passphrase is so important.

WPA – based wireless LANs using IEEE 802.1x authentication are also relatively secure from wireless attacks. It is important to remember, however, that WPA was not built from the ground up and does not offer the highest security protection possible.

WPA2 – based WLANs are highly secure networks, fit for enterprise-level adoption. The AES-CCMP encryption standard ensures that encrypted packets cannot be cracked. Just as in WPA, however, in personal security / pre-shared key mode, a symmetric key could also be cracked if it is easy to guess.

WPA2 is the most secure wireless network configuration in use today.

In enterprise environments, WPA/WPA2 networks utilize IEEE 802.1x authentication and use an authentication server, such as a RADIUS server, to authenticate clients. This allows administrators to place all wireless users into a database and configure their access rights from a central location. Central management makes security easier to implement, makes network usage easier to track, and increases security because a network-wide policy can be applied at a central server (Ciampa, 2006, p. 310).

VPNs over WLANs are not as common as the other types of wireless security mentioned, but they are used by many organizations for increased security over a WLAN (Intel Corporation, 2007). A secure tunnel allows for private communications over an insecure medium. As an example, one could use SSH server and the SSH client “PUTTY” to establish a secure tunnel over a wireless network. Traffic could then be securely sent through this encrypted tunnel. One must be cautious in implementing a VPN over

a wireless link, however. VPNs do not solve all WLAN security problems. User error in a VPN application could have catastrophic consequences, and could result in sensitive data not being enclosed in the tunnel. In addition, the cost of the equipment and continued management can be high and the complexity of the network increases, making things harder for the administrator (Intel Corporation, 2007).

## **VI. ROADS TO SECURITY – COMMONSENSE GUIDELINES**

Depending on the current wireless network, security needs, and the available budget, there are different roads to improving wireless security. An organization must decide, based on its security policy, how to implement an effective balance between operating needs and security. The following recommendations are for organizations who want to secure their WLANs which are connected to a private network (basic and extended service sets). Wireless hotspots and ad-hoc networks require different security and operational needs.

1. Basic Security Measures
2. Interim Security Measures (for little to no resources)
3. WPA/WPA2-PSK
4. WPA/WPA2-Enterprise
5. VPN, SSL over WLAN
6. High Security WLAN Precautions

## Basic Security Measures

First among the steps to securing a wireless network are basic security measures, which should be implemented regardless of the security system in place.

1. First scan the area for conflicting access points. This will prevent Denial of Service issues down the road (Dowler, 2007, p. 9).
2. Place the access point in a favorable location. The access point should be placed where the transmissions will be broadcast in the desired location and range (Cox, 2003). By reducing the power of the access point or by using a directional antenna, one can reduce the range of the wireless network.
3. Change the default SSID of the access point to an abstract and random name. Naming a wireless network after a business or a family name is a bad idea. Attackers could use the SSID to determine who the network belongs to, and with more effort, could determine possible weaknesses (Dowler, 2007, p. 10).
4. Change the default username/password of the access point. Follow strong password creation procedures by using various characters and making the password as long as possible (Dowler, 2007, p. 9).
5. Leave SSID beaconing enabled, as this will prevent clients from constantly sending out probe requests with the SSID (Microsoft Technet, 2006). On clients, be sure to configure the network as a broadcast network so that probe requests will not be sent out (Rubens, 2007). If you do decide to disable SSID beaconing, set the access point to respond only to probe requests with the SSID, if possible (Macaulay, 2002, p. 11). Disabling SSID beaconing may not be possible

on WLANs with roaming users (Ciampa, 2006, p. 302).

6. Enable MAC filtering, if possible. This may not be feasible in large deployments or possible in roaming networks ( Macaulay, 2002, p. 8; Phifer, 2007c).
7. Disable unused network shares on clients and disable peer-to-peer wireless connections on clients if an access point is used. Ensure that only trusted connections are listed on the client's wireless connection profile (AirTight Networks, Inc., 2007).
8. Ensure clients are properly protected with software firewalls.
9. Update the drivers of wireless network interface cards (NICs) in clients and update the firmware of access points. Keep the drivers and firmware up to date.
10. Regularly check device logs for unusual activity.
11. Periodically perform site surveys, or “sweeps” for rogue access points or other banned wireless devices (Cisco Systems, Inc., 2007).
12. Turn off access points when the wireless network is not in use.

## **Interim Security Measures**

If WEP is the only option, interim security measures can be used until the network is upgraded. Interim security measures, also called a “transitional” security system by author Mark Ciampa (2006), operates on the idea that it is best to implement as many security measures as possible. Even if one by one these measures could be evaded, together they make life more difficult for attackers and will turn away most undetermined snoopers. At any rate, it is important to consider these steps as temporary until a more secure wireless system can be installed. Even after taking these security measures for WEP, WEP is still open to attack. It is imperative to replace WEP in your organization. Until WEP can be replaced:

1. Implement Basic Security Measures (discussed previously).
2. Enable a minimum of 104-bit WEP encryption, using a key made with random hexadecimal characters. Avoid passphrase generators, as the keys they produce may not be truly random (Ciampa, 2006, p. 303; Phifer, 2007c).
3. Rotate shared WEP keys at frequent intervals, such as quarterly (Phifer, 2007c).
4. Disable shared-key authentication; use open authentication. Shared key authentication is so flawed that Microsoft now recommends disabling it, opting instead for open authentication with WEP encryption (Microsoft Technet, 2006).
5. Treat the wireless network segment as insecure and place a firewall between the access point and the protected network (Macaulay, 2002, p. 8). Any data sent over the wireless network with only WEP encryption for protection is not to be trusted.
6. Seriously consider implementing a VPN; see **VPN Security Measures**.

### **WPA/WPA2-PSK Measures**

Implementing WPA instead of WEP brings a substantial boost in security. If wireless devices do not support WPA2, WPA is the best wireless security option available. WPA/WPA2 networks can use a shared secret (a secret passphrase) in pre-shared key mode (PSK). This mode is intended for small home/office (SOHO) use of 10 devices or less (Ciampa, 2006, p. 304).

1. Implement Basic Security Measures (discussed previously)
2. Use a strong passphrase. Either use a random sequence of at least 20 ASCII characters or a random sequence of at least 24 hexadecimal digits (Ciampa, 2006, p. 307). Make the passphrase as long and random as possible. If using ASCII characters, use numbers, letters with case changes, and other ASCII characters. WPA/WPA2 are vulnerable to dictionary attacks (Phifer, 2007b). The longer and more random the passphrase, the better.
3. Ensure the SSID is a unique, uncommon name, different than the default. The SSID is mixed with the shared secret to create the key. Hackers use tables of common SSIDs to speed up the cracking process (Phifer, 2007b).

### **WPA/WPA2-Enterprise Measures**

1. Implement Basic Security Measures (discussed previously).
2. Use a robust EAP implementation that supports mutual authentication, such as EAP-TTLS, EAP-FAST, or PEAP (Intel Corporation, 2007).
3. Disable unused EAP types on the RADIUS server (Wright, 2007).
4. Ensure that clients properly identify and authenticate the authentication server. The default operating system settings may accept all root certificate authorities. Clients should only accept digital certificates from the approved authentication server. These settings can be set through group policy objects in Windows (Wright, 2007).
5. Avoid using EAP types that are vulnerable to brute force dictionary attacks, such as EAP MD5, EAP GSS with Kerberos V, or Cisco LEAP (Aboba, 2006).

### **VPN Security Measures**

1. Implement Basic Security Measures (discussed previously).
2. Ensure that the VPN software is being correctly implemented.
3. Educate users how to properly use the tunneling software.
4. Place a firewall between the access point and the protected network, allowing only traffic over tunneled ports.
5. Place software firewalls on wireless clients that block traffic not traveling over tunneled ports.
6. Keep tunneling applications up to date.
7. Routinely check the VPN logs for attempted break-ins or unsuccessful logins.
8. Consider implementing a NIDS (Network-based Intrusion Detection System) behind the firewall. A network-based IDS can detect attack patterns or unusual traffic patterns and sound an alert (Whitman & Mattord, 2004, p. 289).
9. Periodically perform checks on the VPN system.

## High Security WLAN Security Precautions

In addition to using a WPA/WPA2 secured network, the following measures can be implemented in networks that require increased security. Enterprises handling sensitive information and organizations especially concerned about security may require additional security measures.

1. Treat the wireless network as being insecure. Traffic flowing over the wireless medium is potentially vulnerable to attack, and the wireless medium may serve as an entry point for attacks.
2. Place a firewall between the access point and the protected network and only allow required traffic to pass.
3. Place an IDS behind the firewall to monitor for wireless intrusions. Wireless break-ins may cause anomalous traffic patterns. Installing a network-based IDS will detect these patterns and sound an alert. Implementing an IDS can take considerable effort, however, so be warned (Whitman & Mattord, 2004, p. 289).
4. Consider implementing a WIDS (Wireless Intrusion Detection System) / WIPS (Wireless Intrusion Prevention System). Such a system is composed of wireless sensors which scan the airwaves for rogue access points, known attack patterns, or odd wireless behavior (Ciampa, 2006, p. 315). A WIDS / WIPS continually monitors the security of a wireless network and can take appropriate actions under specific conditions (DigitalAir Wireless Networks, 2006).
5. Consider installing network access control software on clients. A system such as **SpectraGuard<sup>®</sup> SAFE** from AirTight Networks will allow clients to create a profile for trusted

zones and will stop clients from accidentally connecting to foreign wireless devices (AirTight Networks, Inc., 2007).

6. Frequently check device logs for unusual activity.
7. Regularly perform site surveys, or “sweeps” for rogue access points or other banned wireless devices.
8. For wireless networks transmitting especially sensitive data, implement a VPN on top of the WPA/WPA2 architecture; see **VPN Security Measures**.

## VII. THE BATTLE CONTINUES

While security for wireless networks has come a long way since the original IEEE 802.11 standard was adopted in 1997, it is important to remember that wireless security is an ongoing concern. One of the most recently discovered wireless vulnerabilities has been the disclosure that certain wireless NIC drivers can be compromised by bombarding the wireless NIC with floods of wireless packets. This attack technique, called “fuzzing,” floods the wireless card with so much traffic that it can cause programs to crash or even allow malicious software to execute. It also doesn't require the wireless NICs to be connected to a network; the wireless NIC need only be turned on and functioning. Although fuzzing is a technically tedious attack, with the proliferation of new attack scripts it is now an emerging threat. This attack was demonstrated during Black Hat USA 2006, and is yet another reason to keep wireless NIC drivers up to date (McMillan, 2006).

In the wireless arena, the battle for security is ongoing. The truth is, as long as a wireless network broadcasts traffic on publicly available frequencies, it will be attacked. TJX was attacked and its defenses failed because they were woefully inadequate. To keep such attacks from becoming successful, it is important that the wireless administrator lock down the wireless network by following the steps detailed in this paper. By tightening down wireless networks, would-be-attackers can be put out of business, and your organization can be kept safe.

## VIII. WORKS CITED

Aboba, B. (2006, June 13). *The Unofficial 802.11 Security Web Page*.

Retrieved April 5, 2008, from

<http://www.drizzle.com/~aboba/IEEE/>

Aircrack-ng. (2008, March 27). *faq [Aircrack-ng]*

Retrieved April 4, 2008, from

<http://www.aircrack-ng.org/doku.php?id=faq>

AirDefense. (2007, November 15). *AirDefense's Comprehensive Survey of 3,000 Retail Stores Finds Many Wireless Data Security Vulnerabilities as Holiday Shopping Season Nears*.

Retrieved April 4, 2008, from

[http://www.airdefense.net/newsandpress/11\\_15\\_07.php](http://www.airdefense.net/newsandpress/11_15_07.php)

AirSnort. (2004, December 31). *AirSnort Homepage: Introduction Section*.

Retrieved April 4, 2008, from

<http://airsnort.shmoo.com/>

AirTight Networks, Inc. (2007, October 21). *Caffe Latte Vulnerability Discovered by AirTight:*

*Underscores Urgent Need for Wireless Road Warriors to Adopt Best Practices*

Retrieved April 5, 2008, from

[http://www.airtightnetworks.net/news/pressrelease/news\\_company100.html](http://www.airtightnetworks.net/news/pressrelease/news_company100.html)

\*Arbaugh, W.A., Shankar, N., Wan, Y.C.J., & Zhang, K. "Your 80211 wireless network has no clothes,"

*Wireless Communications, IEEE [see also IEEE Personal Communications]* , vol.9, no.6, pp.

44-51, Dec. 2002

Retrieved April 4, 2008, from

[http://ieeexplore.ieee.org/iel5/7742/26001/01160080.pdf?isnumber=26001\[\]=STD&arnumber=1160080&arnumber=1160080&arSt=+44&ared=+51&arAuthor=Arbaugh%2C+W.A.%3B+Shankar%2C+N.%3B+Wan%2C+Y.C.J.%3B+Kan+Zhang](http://ieeexplore.ieee.org/iel5/7742/26001/01160080.pdf?isnumber=26001[]=STD&arnumber=1160080&arnumber=1160080&arSt=+44&ared=+51&arAuthor=Arbaugh%2C+W.A.%3B+Shankar%2C+N.%3B+Wan%2C+Y.C.J.%3B+Kan+Zhang)

Ars Technica. (2002, July 17). *Wireless Security Blackpaper.*

Retrieved April 4, 2008, from

<http://arstechnica.com/articles/paedia/security.ars/3>

Borisov, N., Goldberg, I., & Wagner, D. *Intercepting mobile communications: The insecurity of 802.11.*

In Proceedings of MOBICOM 2001, 2001.

Retrieved April 4, 2008, from

<http://citeseer.ist.psu.edu/borisov01intercepting.html>

\*Brown, B., "802.11: the security differences between b and i," *Potentials, IEEE* , vol.22, no.4, pp. 23-27, Oct.-Nov. 2003

Retrieved April 4, 2008, from

[http://ieeexplore.ieee.org/iel5/45/27781/01238689.pdf?isnumber=27781\[\]=JNL&arnumber=1238689&arnumber=1238689&arSt=+23&ared=+27&arAuthor=Brown%2C+B.](http://ieeexplore.ieee.org/iel5/45/27781/01238689.pdf?isnumber=27781[]=JNL&arnumber=1238689&arnumber=1238689&arSt=+23&ared=+27&arAuthor=Brown%2C+B.)

Bulk, F. ( 2006, January 27). Crash Course: The ABCs of WPA2 Security. *Network Computing*.

Retrieved April 5, 2008, from

<http://www.networkcomputing.com/showArticle.jhtml?articleId=177103376>

\*Chen, J-C., Jiang, M-C., & Liu, Y-w. "Wireless LAN security and IEEE 802.11i," *Wireless Communications, IEEE [see also IEEE Personal Communications]* , vol.12, no.1, pp. 27-36, Feb. 2005

Retrieved April 4, 2008, from

[http://ieeexplore.ieee.org/iel5/7742/30466/01404570.pdf?isnumber=30466\[\]=JNL&arnumber=1404570&arnumber=1404570&arSt=+27&ared=+36&arAuthor=Jyh-Cheng+Chen%3B+Ming-Chia+Jiang%3B+Yi-wen+Liu](http://ieeexplore.ieee.org/iel5/7742/30466/01404570.pdf?isnumber=30466[]=JNL&arnumber=1404570&arnumber=1404570&arSt=+27&ared=+36&arAuthor=Jyh-Cheng+Chen%3B+Ming-Chia+Jiang%3B+Yi-wen+Liu)

Ciampa, M. (2006). *CWNA Guide to Wireless LANs* (Second Edition).

Boston, Massachusetts: Thompson Course Technology.

Cisco Systems, Inc. (2007). *Addressing Wireless Threats with Integrated Wireless IDS and IPS*.

Retrieved April 5, 2008, from

[http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6521/prod\\_white\\_paper0900aecd804f155b\\_ns386\\_Networking\\_Solutions\\_White\\_Paper.html](http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6521/prod_white_paper0900aecd804f155b_ns386_Networking_Solutions_White_Paper.html)

Cox, J. (2003, December 1). Build a secure enterprise WLAN. *Network World*.

Retrieved April 5, 2008, from

<http://www.techworld.com/mobility/features/index.cfm?featureid=221>

DigitalAir Wireless Networks. (2006). *Wireless Intrusion Prevention Systems*.

Retrieved April 5, 2008, from

[http://www.digitalairwireless.com/wireless\\_intrusion\\_prevention\\_system.asp](http://www.digitalairwireless.com/wireless_intrusion_prevention_system.asp)

Dowler, M. (2007, July 30). Beginners Guides: Securing A Wireless Network – PCSTATS.com.

In *Beginners Guides*.

Retrieved April 5, 2008, from

<http://www.pcstats.com/articleview.cfm?articleid=1489&page=9>

Fleishman, G. (2003, January 10). Key to Wi-Fi security. *InfoWorld*

Retrieved April 5, 2008, from

<http://www.infoworld.com/articles/ne/xml/03/01/13/030113newifisec.html>

Fleishman, G. (2007, October 17). New WEP Attack: Caffe Latte Hits Client, Not Access Point.

*Wi-Fi Networking News*.

Retrieved April 5, 2008, from

<http://wifinetnews.com/archives/007993.html>

Fluhrer, S., Mantin, I., & Shamir, A. "Weaknesses in the Key Scheduling Algorithm of RC4."

Presented to the Eighth Annual Workshop on Selected Areas in Cryptography, August 2001.

Retrieved April 4, 2008, from

[http://www.crypto.com/papers/others/rc4\\_ksaproc.ps](http://www.crypto.com/papers/others/rc4_ksaproc.ps)

Gast, M. (2002, April 19). *Wireless LAN Security: A Short History*. O'Reilly Media, Inc.

Retrieved April 4, 2008, from

<http://www.oreillynet.com/pub/a/wireless/2002/04/19/security.html>

Hendrickson, L. & Piotrowski, V. (n.d.). *Wireless Security: from WEP to 802.11i*.

Retrieved April 4, 2008, from

[http://www.micsymposium.org/mics\\_2004/Hendrick.pdf](http://www.micsymposium.org/mics_2004/Hendrick.pdf)

Intel Corporation. (2007, October 25). *Wireless security - 802.1x and EAP types*.

Retrieved April 4, 2008, from

<http://www.intel.com/support/wireless/wlan/sb/cs-008413.htm>

Kismet. (n.d.) *Kismet*.

Retrieved April 6, 2008, from

<http://www.kismetwireless.net/>

Macaulay, T. (2002, February 18). *Hardening IEEE 802.11 wireless networks*.

Retrieved April 5, 2008, from

[http://www.mosteiro.hpg.ig.com.br/Material/Wireless/Others/Hardening\\_802.11.pdf](http://www.mosteiro.hpg.ig.com.br/Material/Wireless/Others/Hardening_802.11.pdf)

Maufer, T. A. (2003, October 17). *A Field Guide to Wireless LANs for Administrators and Power Users*. Prentice Hall PTR.

McMillan, R. (2006, June 21). Researchers hack Wi-Fi driver to breach laptop. *InfoWorld*.

Retrieved April 5, 2008, from

[http://www.infoworld.com/article/06/06/21/79536\\_HNwifibreach\\_1.html](http://www.infoworld.com/article/06/06/21/79536_HNwifibreach_1.html)

Microsoft Technet. (2006, December 6). *Recommendations for Small Office or Home Office Wireless Networks*.

Retrieved April 4, 2008, from

<http://technet.microsoft.com/en-us/library/bb727047.aspx>

Moskowitz, R. (2003, December 1). *WLAN Testing Reports: "Debunking the Myth of SSID Hiding"*

Retrieved April 6, 2008, from

[http://www.icsalabs.com/icsa/docs/html/communities/WLAN/wp\\_ssid\\_hiding.pdf](http://www.icsalabs.com/icsa/docs/html/communities/WLAN/wp_ssid_hiding.pdf)

Ou, G. (2008, March 11). PCI security standard endangers wireless LANs. *ZDNet*

Retrieved April 6, 2008, from

<http://blogs.zdnet.com/security/?p=941>

Pereira, J. (2007, May 4). BREAKING THE CODE. How Credit-Card Data

Went Out Wireless Door. *The Wall Street Journal Online*.

Retrieved April 4, 2008, from

<http://online.wsj.com/article/SB117824446226991797.html>

Phifer, L. (2003, June 30). 10 Common questions (and answers) on WLAN security.

*SearchSecurity.com*

Retrieved April 6, 2008, from

[http://searchsecurity.techtarget.com/tip/0,289483,sid14\\_gci912555,00.html](http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci912555,00.html)

Phifer, L. (2007a, January 29). Getting Phished: Why SSID Spoofing (Still) Matters

*Wi-Fi Planet*.

Retrieved: April 4, 2008, from

<http://www.wi-fiplanet.com/tutorials/article.php/3656661>

Phifer, L. (2007b, March 23). WPA PSK Crackers: Loose Lips Sink Ships

*Wi-Fi Planet*.

Retrieved: April 4, 2008, from

[http://www.wi-fiplanet.com/tutorials/article.php/10724\\_3667586\\_2](http://www.wi-fiplanet.com/tutorials/article.php/10724_3667586_2)

Phifer, L. (2007c, September 6). WLAN Security Service Aims to Boost PCI Compliance

*eSecurityPlanet.com*

Retrieved: April 5, 2008, from

[http://www.esecurityplanet.com/best\\_practices/article.php/3698111](http://www.esecurityplanet.com/best_practices/article.php/3698111)

Phifer, L. (2007d, October 5). WLAN Security Blamed for TJX Payment Card Breach

*Wi-Fi Planet.*

Retrieved: April 5, 2008, from

<http://www.wi-fiplanet.com/news/article.php/3703636>

Phifer, L. (2007e, December 12). The Caffe Latte Attack: How It Works—and How to Block It.

*Wi-Fi Planet.*

Retrieved: February 21, 2008, from

<http://www.wi-fiplanet.com/tutorials/article.php/3716241>

Rubens, P. (2007, April 5). The Critical XP Wi-Fi Patch You Need Today.

*Enterprise IT Planet.com*

Retrieved April 6, 2008, from

<http://www.enterpriseitplanet.com/networking/features/article.php/3669941>

Shimonski, R. J. (2003, February 24). Wireless Attacks Primer. *WindowSecurity.com*

Retrieved April 4, 2008, from

[http://www.windowsecurity.com/articles/Wireless\\_Attacks\\_Primer.html](http://www.windowsecurity.com/articles/Wireless_Attacks_Primer.html)

Stubblefield, A., Ioannidis, J., & Rubin., A.(2001, August 21) "Using the Fluhrer, Mantin, and Shamir

Attack to Break WEP", ATT Labs Technical Report, TD4ZCPZZ, Revision 2.

Retrieved April 4, 2008, from

<http://citeseer.ist.psu.edu/stubblefield01using.html>

Tews, E., Pychkine, A., & Weinmann, R-P. (2007a, April 5). *aircrack-ptw*

Retrieved April 4, 2008, from

<http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/>

Tews, E., Pyshkin, A., & Weinmann, R-P. (2007b, September 16). *Breaking 104 bit WEP in less than 60 seconds*. Cryptology ePrint Archive, Report 2007/120.

<http://eprint.iacr.org/2007/120>

Whitman, M. E. & Mattord, H. J. (2004, November 23) *Principles of Information Security*. Second Edition. Thompson Course Technology.

Wi-Fi Alliance. (2003, April 29). *Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks*.

Retrieved April 4, 2008, from

[http://www.wi-fi.org/files/wp\\_8\\_WPA%20Security\\_4-29-03.pdf](http://www.wi-fi.org/files/wp_8_WPA%20Security_4-29-03.pdf)

Wilson, T. (2007, November 15). Many Retailers Open to Wireless Attacks. *Dark Reading*.

Retrieved April 4, 2008, from

[http://www.darkreading.com/document.asp?doc\\_id=139291](http://www.darkreading.com/document.asp?doc_id=139291)

Wirelessdefence.org. (2006). *coWPAtty Main Page*.

Retrieved April 4, 2008, from

<http://www.wirelessdefence.org/Contents/coWPAttyMain.htm>

Wong, Stanley. (2003, May 20). *The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards*. SANS Institute.

Retrieved April 4, 2008, from

<http://cnscenter.future.co.kr/resource/hot-topic/wlan/1109.pdf>

Wright, J. (2007, April 23). Using PEAP for wireless authentication. *Network World*

Retrieved April 5, 2008, from

<http://www.networkworld.com/columnists/2007/042307-wireless-security.html>