

# Security Challenges in Wireless Network Communication

by: Greg M. Bednarski  
Janine Burbage  
Keith Eich

## Abstract:

We hear the word wireless so frequently that it has suddenly become a buzzword in our society. With the rush to adopt the mobility and freedom that wireless provides – access points (or hotspots) are coming on-line in homes, business, public facilities and government properties at an astounding rate. As with many emerging technologies, these networks are being designed and installed with little or no consideration for security. The proposed paper will present the reader with topics related to the booming 802.11 wireless technology, specifically: an introduction to the basics, some methods used to secure networks, known vulnerabilities to security, and an overview of Carnegie Mellon University's wireless network.

## Table of Contents:

I. Introduction to Wireless Fidelity (Wi-Fi)	Pages 2-7
II. Security & Wi-Fi Networks	Pages 7-15
III. Wi-Fi Vulnerabilities	Pages 15-24
IV. Wi-Fi at Carnegie Mellon University	Pages 24-28
V. Conclusion	Page 28

# I. Introduction to Wireless Fidelity (Wi-Fi)

Wireless Fidelity, another wise known as Wi-Fi, is a generic yet popular term for high frequency wireless local area networks (WLAN). One does not have to look too far to find a Wi-Fi network as they are increasingly replacing wired LANs in many organizations. Wi-Fi networks are creeping up in coffee shops and restaurants around the United States and are making their way into homes as a home network.

## **Wi-Fi Growth**

### **Laptops**

The increasing number of laptop owners has dramatically increased since 2001. Cahner's In-Stat Group<sup>1</sup> reports that by 2005, laptop computer use in USA will escalate to 60 million, while world wide usage is predicted reach over 150 million. Shipment of wireless enabled laptop computers, is expected to increase to over 15 million in 2005 as compared to 2.9 million in 2001. Are we soon reaching the point where laptops will become a commodity?

In-Stat/MDR<sup>2</sup> that claims that the two major forces transforming the business Wi-Fi market in 2003 are Intel's aggressive push of Centrino on the client side and the emergence of wireless switching on the infrastructure side. In-Stat/MDR expects that 16 million notebook PCs with embedded Wi-Fi will ship to businesses this year, and that by 2005, Wi-Fi will be included in 95% of notebooks as a standard feature with the extra cost of the Wi-Fi client basically transparent to the user. In-Stat/MDR analysts report that the anticipated rush of Wi-Fi clients has sparked an influx of vendors anxiously ready to design infrastructure needed to support the increasing number of Wi-Fi users. Start-ups and some traditional WLAN hardware vendors introduced the "AP/Switch" architecture as a way to ease the management, security, and configuration issues of large-scale WLAN roll-outs.

Cahner's In-Stat Group<sup>3</sup> also reports that Americans rely using their laptops for network connectivity when traveling: 86% use email, 85% are prepare documents, 74% are log into the Internet, 59% log into the corporate network, 48% schedule, 45% are prepare presentations, and 36% use their laptop for entertainment. How far are we from reaching the point where wireless will become a commodity?

---

<sup>1</sup> Wi-fi market information and statistics – February, 2003

<sup>2</sup> Business Wire. August 5, 2003 p(1)

Embedded Wi-Fi and Wireless Switching Promise to Further Facilitate Business WLAN Growth Reports In-Stat/MDR

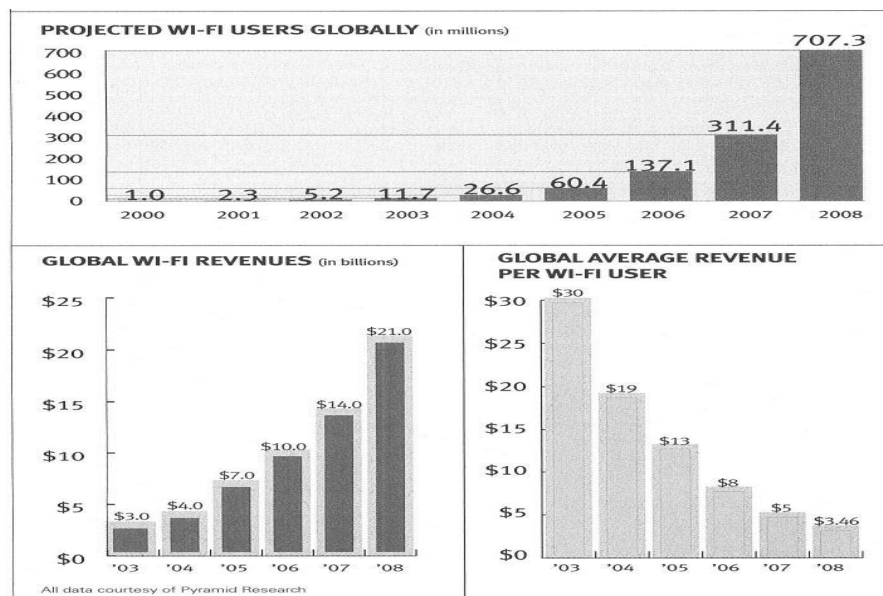
<sup>3</sup> Wi-fi market information and statistics – February, 2003

## US WLAN Market

According to Dell'Oro Group<sup>4</sup>, the Wireless LAN - 802.11 market will grow from \$1.5 B in 2002 to \$3.1 B in 2007, with all product categories continuing to drive revenue growth through the scope of the forecast. Analysys, a Telecommunications strategy, management and information consultancy<sup>5</sup>, predicts that the US mobile operators, wireless ISPs, roaming providers, and real estate owners will obtain their revenues from over 21 million wireless users. WLAN services are targeting the highly mobile business users that need a reliable, secure, fast, mobile connection enabling them to work anywhere in the world.

## Global WLAN Market

Pyramid Research<sup>6</sup> conducted a study that projects an estimated 700 million Wi-Fi users by 2008. This figure more than doubles most other research firm estimates, because other Wi-Fi studies assume that Wi-Fi will be popular mainly in the developed world. It is predicted that the majority of the world's Wi-Fi users will reside in developing countries such as China, where a lack of legacy telecom and data infrastructure will produce cheap and versatile Wi-Fi into all strata of daily use. Wi-Fi is not only exploited by the laptop, but it has more applications that developing countries are likely to exploit.



Projected Wi-Fi Users Globally – in millions

Global Wi-Fi Revenue – in billions

Global Average Revenue per Wi-Fi User

<sup>4</sup> Business Wire, July 30, 2003 p5439 Worldwide WLAN 802.11 Market to exceed \$3 Billion in 2007

<sup>5</sup> Wi-fi market information and statistics – February, 2003

<sup>6</sup> PRIMEDIA Business Magazines & Media Inc. Aug 18, 2003 INTELLIGENCE FROM THE BROADBAND ECONOMY

## Pricing

As far as WLAN pricing, Gartner analysts report that competition is forcing WLAN equipment and services prices down<sup>7</sup>. Although the 2002 global WLAN equipment purchases of 19.5 million units exceeded the forecast of 15.5 million units, revenues failed to reach the \$2.1 billion forecast because of falling equipment prices. This is because the WLAN market is attracting a large number of vendors.

Because Wi-Fi uses unlicensed radio frequencies, Wi-Fi is relatively easy and cheap to operate<sup>8</sup>. Many new laptop computers automatically detect Wi-Fi networks, while others do so by plugging in a wireless card. Many colleges, cities, coffee shops and restaurants offer Wi-Fi as a free service. This could lead to losses for those trying to profit from users paying for Wi-Fi at public hotspots. The entire idea of people paying for Wi-Fi in public could be a flop. The Grand Rapids Press states that there are 5,000 public hotspots in the United States, 2,700 are operated by the wireless phone carrier T-Mobile primarily offering service in Starbucks coffee shops and Borders bookstores. As of July 2003, T-Mobile charges 10 cents a minute, \$40 a month or \$360 a year. Allied Business Intelligence experts predict roughly 12,400 hot spots in the United States and Canada by 2003, and 78,000 hotspots 2008.

## WLAN Standards

The 802.11 is a family of specifications developed by the IEEE for Wireless LANs. The four family specifications include 802.11, 802.11a, 802.11b, and 802.11g. All four family members use Ethernet protocol and carrier sense multiple access with collision avoidance for path sharing.

### 802.11b Standard

The 802.11b standard, often referred to Wi-Fi, is backward compatible with 802.11 and operates in the 2.4 GHz band. The modulation scheme is Direct Sequence Spread Spectrum with complementary code keying (CCK), which allows data speeds up to 11 Mbps and is less susceptible to multipath-propagation interference. The main advantages<sup>9</sup> to using 802.11b are price and compatibility. 802.11b hardware is widely available and significantly cheaper compared when compared to 802.11g or 802.11a hardware. The two well known disadvantages<sup>10</sup> to using 802.11b are security and performance. Because 802.11B is so prevalent, there are numerous hacking tools designed specifically for exploiting 802.11b environment. NetStumbler is a tool that uses a GPS to plot the location of each detected wireless access point onto a map. Radio interference is the biggest performance issue in 802.11b networks due to the high volume of

---

<sup>7</sup> Purchasing, July 17, 2003 v132 i11 p5(1) 2002 global wireless local area network (WLAN) equipment purchases.

<sup>8</sup> The Grand Rapids Press July 20, 2003 p(E2), Brian Bergstein AP

<sup>9</sup> *Evaluating the wireless networking options* <http://techrepublic.com/5100-6313-5054011.html?tag=sc>

<sup>10</sup> *Evaluating the wireless networking options* <http://techrepublic.com/5100-6313-5054011.html?tag=sc>

802.11b access points. Because 802.11b operates in the 2.4 GHz band, it is also susceptible to interference from microwave ovens and 2.4 GHz cordless phones.

## **802.11a Standard**

The 802.11a specification applies to wireless ATM systems and is used in access hubs. Operating at radio frequencies between 5 GHz and 6 GHz, 802.11a uses orthogonal frequency-division multiplexing (OFDM) modulation scheme. OFDM allows data speeds as high as 54 Mbps and multiple channels can be combined for even higher data rates. Although the high data rates are advantageous, the range at which 802.11a operates is less than 802.11b 802.11g (discussed below). The 802.11a standard allows 12 non-overlapping channels in the 5.8 GHz frequency range, thus users can co-locate up to 12 access points within a given area. Another motivator<sup>11</sup> to implementing 802.11a is that the signals are less susceptible to interference from other devices such as cordless phones, and less susceptible to interference from microwave ovens. This is because 802.11a operates in the 5.8 GHz frequency range while most cordless phones operate on a frequency of 2.4 GHz.

## **802.11g Standard**

The most recently approved standard, 802.11g, offers wireless transmission over relatively short distances with a data rate up to 54 Mbps operating in the 2.4 GHz range. 802.11g is an extension to 802.11b and is compatible with it. 802.11g uses the OFDM modulation in data rates above 20 Mbps, and DSSS with CCK modulation with data rates below 20 Mbps. The main advantages<sup>12</sup> to using 802.11g are compatibility and speed. 802.11g is completely backward compatible with 802.11b, so upgrading to the 802.11g network for better performance will be a smooth transition.

The primary reason for installing 802.11g networks will likely be speed, but with speed comes disadvantages<sup>13</sup>. An 802.11g signal requires 30 MHz of bandwidth while the entire 802.11g frequency range only consists of a total of 90 MHz of bandwidth. This limits the maximum number of access points to three that can be collocated within a certain area. Another disadvantage to using 802.11g is that the signal has a shorter range when compared to 802.11b. This disadvantage might actually be advantageous in some environments. For example, because an 802.11g signal can't travel very far, the number of access points in a building can increase, as long as no more than three access points are within range of each other at any given time.

---

<sup>11</sup> *Evaluating the wireless networking options* <http://techrepublic.com.com/5100-6313-5054011.html?tag=sc>

<sup>12</sup> *Evaluating the wireless networking options* <http://techrepublic.com.com/5100-6313-5054011.html?tag=sc>

<sup>13</sup> *Evaluating the wireless networking options* <http://techrepublic.com.com/5100-6313-5054011.html?tag=sc>

Dell'Oro Group's<sup>14</sup> recently published Report indicates that most Wi-Fi products will transition from 802.11b to 802.11g and then to 802.11 Multimode (802.11a/g), with the exception being Enterprise-class Access Points which will likely skip the transitions to 802.11g and move quickly to Multimode solutions.

## **WLAN Modulation Schemes**

The 802.11 standard uses the Frequency-Hopping Spread Spectrum (FHSS) modulation schemes. According to Webopedia.com<sup>15</sup>, FHSS is a transmission technology where digital signals are modulated with a narrowband carrier signal that hops in a random, predictable sequence from frequency to frequency as a function of time over a wide band of frequencies. 802.11 also use a transmission technology where the data signals at the sending station are combined with a higher data rate bit sequence that divides the user data according to a spreading ratio. This is known as the Direct-Sequence Spread Spectrum (DSSS) modulation scheme<sup>16</sup>.

The 802.11a and 802.11g differ from 802.11 in that it uses Orthogonal Frequency Division Multiplexing modulation scheme (OFDM). Webopedia.com<sup>17</sup> states that OFDM transmits large amounts of digital data over a radio wave by splitting the radio signal into multiple smaller sub-signals that are transmitted simultaneously at different frequencies to the receiver. A benefit to OFDM is that it reduces the amount of crosstalk in signal transmission

The 802.11b and 802.11g use the DSS S with Complementary Code Keying (CCK). Webopedia.com<sup>18</sup> states that CCK is a set of 64 eight bit code words that are used to encode data for 5.5 and 11 Mbps data rates in the 2.4 GHz band. Because the code words have unique math properties, they are distinguished from one another by a receiver despite large amounts of noise and multipath interference.

## **Business Decisions based on Standards**<sup>19</sup>

There are many options that need to be considered when making a business decision on implementing 802.11a, 802.11b or 802.11g.

You may consider the 802.11a specification if you need high bandwidth for streaming video or other dynamic multimedia content, you are a growing organization and need the greater capacity of more channels, or you are building a new network. Building a new network that requires better security than 802.11b and 802.11g will be the most influential reason for choosing 802.11a because most hackers focus

---

<sup>14</sup> *Business Wire*, July 30, 2003 p5439 Worldwide WLAN 802.11 Market to exceed \$3 Billion in 2007

<sup>15</sup> <http://www.webopedia.com/TERM/F/FHSS.html>

<sup>16</sup> <http://www.webopedia.com/TERM/D/DSSS.html>

<sup>17</sup> <http://www.webopedia.com/TERM/O/OFDM.html>

<sup>18</sup> <http://www.webopedia.com/TERM/C/CCK.html>

<sup>19</sup> *Evaluating the wireless networking options* <http://techrepublic.com.com/5100-6313-5054011.html?tag=sc>

on 802.11b and 802.11g networks. There are few hacking tools available for 802.11a networks because it is the least popular network choice. Because it uses the 5.8 GHz frequency range, 802.11a is also much less susceptible to radio interference than 802.11b or 802.11g.

You may opt for 802.11b if you are operating a transaction-intensive environment, your users travel a lot and need wireless access in other locations, you need to keep acquisition costs low, and you already have some 802.11b users.

If you already deploy 802.11b, and are looking to support more users, 802.11g<sup>20</sup> gives wireless networks based on 802.11b the ability to serve up to four to five times more users than they now do. It also opens the possibility for using IEEE 802.11 networks in more demanding applications, such as wireless multimedia video transmission and broadcast MPEG. Devices using 802.11b and IEEE 802.11g standards can coexist in the same network.

## **II. Security & Wi-Fi Networks**

### ***Network Security***

Physical network security has been a long standing problem. However, the majority of it is controllable due to physical security issues. You can control where ports are for connection to your network limiting a large amount of unnecessary security concerns. You can further place filters to only allow certain PCs on the network (MAC Address Filtering). The next step would be for Access Control to any server. Where you need a username and password to access information, share in pooled resources, or even gain admission to the network. However all of this assumes that your physical premises are secured and that a deviant individual is not working from the inside of your network. So encryption is another good layer of protection where you can encode data sent over the network so that other people can't monitor what is being said or shared over a connection. Soon there will be method of authentication from a hardware level that will allow more trusted connections to send information knowing who exactly is making the request, from what machine, running what OS, etc. Physical security is an issue with wireless networks since information does not just flow through wires locked behind doors but through the air where there are a lot of opportunities to intercept or block information sent between hosts and clients.

### **Network Transmission & Protocol Stack <sup>21</sup>**

OSI (Open Systems Interconnection) is a standard model/reference for how information should be transmitted between any two points on a network. Its purpose is to allow developers to focus on one layer

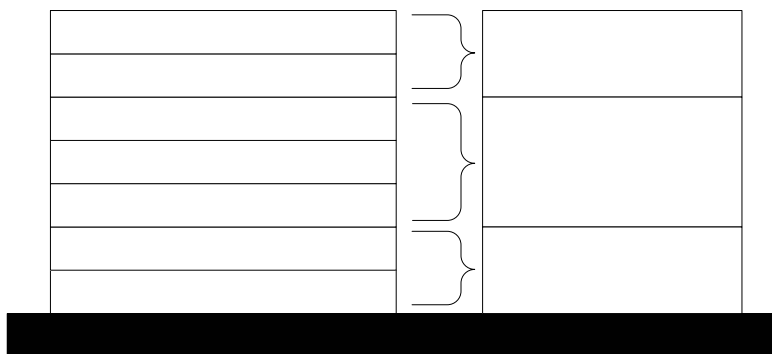
---

<sup>20</sup> <http://standards.ieee.org/announcements/80211gfinal.html>

<sup>21</sup> <http://computer.howstuffworks.com/osi.htm> & <http://www.cisco.com/warp/public/535/2.html>

independent of the others so there is a guarantee of interfacing. The model defines seven layers of functions that take place between end-to-end communications. It is generally simplified into three layers shown below. The main idea behind OSI is that the communication process can be divided into layers, with each layer adding its own set of special, related functions. The Network Access Layer can be thought of as physical connections, the medium through which information is sent, and any physical devices used in communication. The Transport Layer is where routing and destination information is present – it is generally referred to as the IP (Internet Protocol) Suite where packets and connections exist. Lastly the Application Layer is where the format of the user data and information is held.

One of the main differences between physical and wireless networks with regards to the OSI Network Protocol Stack is the Network Access Layer. In wireless networks the physical connection is not as secure because it is relatively impossible to limit air waves to stay behind locked doors. This makes wireless security a difficult obstacle because the foundation of the entire communication is open.



## Access Control and Authentication

Access Control is a form of security where a user makes a request to use or access an object on the network. The reference monitor then grants or denies this request. Often times this is done through groups or individual permissions where the default is deny-all except on what is stated by the administrator of the system.

Authentication is the method by which the reference monitor determines who actually made the request. Each request arrives on some channel. For example this can be done on a single machine when the kernel is called from a user process or when a network connection is activated. The reference monitor must authenticate the channel and determine who the request is from. This is trivial in a centralized system such as an Operating System where all the channels are known but it is much harder in a distributed system such as a network. On a distributed system the request may transverse non-trusted points or

been directed through parts of the system which are faulty or broken. Therefore it is important to understand that each of these problems are unique in administration and difficulty.

## **Applied Firewalls: MAC Address Filtering & SSID**

A firewall is a component (or set of components) that restrict communication service between two networks. Often firewalls are used between the Internet and an internal network. A firewall has the ability to filter packets based on information encoded into the Transport Layer of a packet. In a traditional sense this is a good idea to keep information secure on two different networks but it isn't directly applicable to wireless networks.

The idea of packet filtering can be applied to a network security scheme known as MAC Address Filtering. This method can be used on wireless or wired networks since every NIC (Network Interface Card) is given a unique serial number - a MAC (Media Access Control). Most network connection points have the ability to restrict access to a list of certain MACs. This is useful so that information cannot be sent through wireless Access Points without having a proper MAC address. The downfall to this security scheme is that it is possible to sniff the network for a useable address or even guess a MAC address thus obtaining access to the network.<sup>22</sup>

The SSID (Service Set Identifier) is a token which identifies an 802.11 network. The SSID is a secret key which is set by the network administrator. You must know the SSID to join an 802.11 network; however, the SSID can be discovered by network sniffing.<sup>23</sup> The fact that the SSID is a secret key instead of a public key creates a management problem for the network administrator. Every user of the network must configure the SSID into their system. If the network administrator seeks to lock a user out of the network, the administrator must change the SSID of the network, which requires reconfiguration of every network node. Some 802.11 NICs allow you to configure several SSIDs at one time. And most 802.11 access point vendors allow the use of an SSID of "any" to enable an 802.11 NIC to connect to any 802.11 network. Therefore the idea of solely using SSID as a security mechanism is not advisable.

## **Encryption**

Encryption is often a good way to securely transmit information. Using encryption can help keep adversaries from knowing who are communicating, what they communicating, modifying what is being communicated or impersonating communication. Below will serve as an introduction on how encryption can work on either the network access or application layer; and how it is applied to create mechanisms to secure Wi-Fi networks.

---

<sup>22</sup> [http://www.hackfaq.org/wireless\\_networks-13.shtml](http://www.hackfaq.org/wireless_networks-13.shtml)

<sup>23</sup> [http://www.hackfaq.org/wireless\\_networks-11.shtml](http://www.hackfaq.org/wireless_networks-11.shtml)

Most forms of encryption can be broken down given enough time or understanding of the mathematics behind it. But generally, well chosen algorithms and key-bases will keep adversaries away. Some of the considerations to take into account are replay attacks, type flaw attacks, and freshness (man-in-the-middle) attacks. In the third section of this paper you will see how these attacks occur.

## ***WLAN Security Protocols***

<sup>24</sup>According to Meta Group Inc, security reigns as the number one inhibitor to enterprise adoption of WLAN technologies. Securing a WLAN is complex and costly due to the immature standards and lack of interoperability of these standards. Vendors are interested in pushing their own technologies with proprietary standards forcing companies to adopt a single-vendor solution or use third party wireless gateways. As a result, total revenues from enterprise WLAN sales have recently declined although there has been continued growth in the consumer WLAN market.

To enhance the security of WLANs, the 802.1X standard<sup>25</sup> was developed as an authentication framework for wireless LANs, allowing a user to be authenticated by a central authority. The algorithm that is used to authenticate a user is left open and multiple algorithms are possible. 802.1X uses an existing protocol, the Extensible Authentication Protocol that works directly over the link layer protocols for message exchange during the authentication process.

EAP<sup>26</sup> is a transport layer protocol that can be used by a variety of different EAP methods.

The EAP authentication methods were designed with to handle wireless security requirements. These include "mutual authentication" meaning, the authenticator must authenticate the user and the user must authenticate the authenticator. The methods are "self protecting" to guard against eavesdropping on the insecure physical medium. The method must also be immune to online or offline dictionary attacks. The method must also produce session keys that can be used to provide authentication, confidentiality, and integrity protection for the session the user wants to establish. Wi-Fi authentication methods should also forward secrecy so that the password or secret key is never compromised, work with all access points that support 802.1x with EAP authentication, be quick and efficient, cheap to maintain, and convenient for users.

---

<sup>24</sup> *Africa News Service* Oct 21, 2003 *Wireless LAN Security Falls Short of Expectations*

<sup>25</sup> [http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40\\_gci787174,00.html](http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci787174,00.html)

<sup>26</sup> *EAP Methods for 802.11 Wireless LAN Security*

[http://www.iec.org/online/tutorials/eap\\_methods/topic03.html?Next.x=28&Next.y=24](http://www.iec.org/online/tutorials/eap_methods/topic03.html?Next.x=28&Next.y=24)

## Certificate Based Protocols

EAP Tunneled Layer Security Protocol (EAP-TLS), EAP-TTLS, and PEAP were developed specifically for the Wi-Fi network and are based on public key certificates and the Transport Layer Security protocol<sup>27</sup>. EAP-TLS<sup>28</sup> is a public key certificate authentication method providing mutual authentication of client to server and server to client. Both the client and the server must be assigned a digital certificate signed by a Certificate Authority that is trusted by both. EAP-TLS uses includes mutual authentication, key exchange to establish dynamic WEP or TKIP keys, fragmentation and reassembly of long EAP messages, and Fast reconnect.

EAP-TTLS<sup>29</sup> is a more easily managed security method over EAP-TLS and offers the benefit of not requiring the set up and management of client certificates on each WLAN user's device. Rather, the user is authenticated using password-based credentials enclosed in the TLS security wrapper. This helps prevent against active and passive attack.

PEAP<sup>30</sup> is a protocol proposed by Microsoft, Cisco, and RSA security. Like EAP-TTLS, PEAP authenticates WLAN clients without requiring them to have certificates and adds a TLS layer on top of EAP, but it differs from TTLS because it uses the resulting TLS session as a carrier to protect other legacy EAP methods. PEAP uses TLS to authenticate the server to the client but not the client to the server requiring only the server to have a public key certificate. The client and server exchange a sequence of EAP messages encapsulated within TLS messages, and the TLS messages are authenticated and encrypted using TLS session keys negotiated by the client and the server.

### **Security Issues and other concerns with Certificate Based Authentication Methods:** <sup>31</sup>

1. Cost of Administration: Certificates have to be created (or purchased), distributed, and securely installed on each user device.
2. Lengthy Protocol Exchange: Requiring many protocol exchanges lengthens the authentication delay for the user and uses more computing resources on the authenticator.
3. Authentication of the Device not the User: Certificates must be stored on the user device or on a smart card that the user carries. It is often the case that the device is authenticated not the actual user, and this is unacceptable when there are many individual users or when the device can't be secured.

<sup>27</sup> [http://www.iec.org/online/tutorials/eap\\_methods/topic03.html?Next.x=28&Next.y=24](http://www.iec.org/online/tutorials/eap_methods/topic03.html?Next.x=28&Next.y=24)  
*EAP Methods for 802.11 Wireless LAN Security*

<sup>28</sup> [http://www.iec.org/online/tutorials/eap\\_methods/topic03.html?Next.x=28&Next.y=24](http://www.iec.org/online/tutorials/eap_methods/topic03.html?Next.x=28&Next.y=24)  
*EAP Methods for 802.11 Wireless LAN Security*

<sup>29</sup> [http://www.whitehatinc.com/funk/odyssey/ody\\_ds.html](http://www.whitehatinc.com/funk/odyssey/ody_ds.html)

<sup>30</sup> [http://www.iec.org/online/tutorials/eap\\_methods/topic03.html?Next.x=28&Next.y=24](http://www.iec.org/online/tutorials/eap_methods/topic03.html?Next.x=28&Next.y=24)  
*EAP Methods for 802.11 Wireless LAN Security*

<sup>31</sup> [http://www.iec.org/online/tutorials/eap\\_methods/topic03.html?Next.x=28&Next.y=24](http://www.iec.org/online/tutorials/eap_methods/topic03.html?Next.x=28&Next.y=24)  
*EAP Methods for 802.11 Wireless LAN Security*

## Password Authentication Methods

<sup>32</sup>LEAP was developed by Cisco in 2001 as an improved version of Extensible Authentication Protocol-MD5 and it was released as an IEEE 802.1X Extensible Authentication Protocol (EAP) authentication type. LEAP is a mutual EAP authentication algorithm that supports dynamic derivation of session keys in wireless networks. The wireless client associates to an access point and blocks all user requests for LAN access until the mutual authentication takes place. Once the user enters the shared secret – the user's logon password – the access point will send the authentication request to the Remote Authentication Dial-In User Service (RADIUS) server. If access is authenticated, the RADIUS server will derive a WEP key used transmission of information. LEAP was released before it received full ratification by IEEE to prevent a growing Wi-Fi market from withering due to flaws in security.

### **Security Issues and other concerns with LEAP:**

1. Dictionary Attacks: LEAP transmits Challenge-Handshake Authentication Protocol (CHAP) negotiations in the open without the benefit of an encrypted tunnel. Thus, LEAP is prone to offline dictionary and brute force attacks. If hackers break into the network, they have the username/passwords to get in to the servers.
2. Proprietary: Because LEAP is proprietary to Cisco, it can only be used with Cisco access points.

## 802.11 Security Algorithms

### WEP

Wired Equivalent Privacy (WEP)<sup>33</sup> algorithm is a security protocol for wireless LANs that encrypts data over radio waves so that data is protected when it is transmitted from one point to another. WEP also functions as a means to prevent unauthorized access to Wi-Fi networks. WEP relies on a secret key shared between the Wi-Fi device and an access point. The key encrypts packets before they are they are transmitted, and an integrity check ensures that the packets were not modified as they traveled the network.

WEP uses RC4 encryption, stream cipher, which expands a short key into an infinite pseudo-random key. "The sender XORs the key stream with the plaintext to produce ciphertext. The receiver has a copy of the same key, and uses it to generate identical key stream. XORing the key stream with the ciphertext yields the original plaintext."<sup>34</sup>

### **Security Issues with WEP:**

---

<sup>32</sup> *TechRepublic*, May 6, 2003 *Cisco's Leap provides superior WLAN security*

<sup>33</sup> <http://www.webopedia.com/TERM/W/WEP.html>

<sup>34</sup> WEP Security Problems <http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>

1. Stream ciphers: Stream ciphers are vulnerable to attacks because if an attacker flips a bit in the ciphertext, then the corresponding bit in the plaintext will be flipped when it is decrypted.
2. Eavesdropping: If an eavesdropper obtains the XOR for two plaintexts, the XOR can enable statistical attacks to recover the plaintext.
3. WEP's defenses against the attacks described above are an Integrity Check (IC) to ensure that packets have not been modified while in transit, and Integrity Vector (IV) to augment the shared secret key to produce a different RC4 key for each packet. Unfortunately, these defenses have been implemented incorrectly resulting in poor security.

## WPA

Because WEP is not as secure as it was intended and believed to be, the Wi-Fi Protected Access (WPA) security protocols was introduced<sup>35</sup>. WPA was developed to improve upon the security pieces of WEP by improving the data encryption. User authentication does not usually exist in WEP, but it is implemented in WPA. WPA can provide enterprise-level authentication via 802.1x and the extensible authentication protocol (EAP). WEP regulates access to wireless networks based on a system's MAC address, which is easy to be sniffed out and captured. EAP is built on a more secure-public key encryption mechanism help guarantee only authorized network users can access the network.

WPA uses a Temporal Key Integrated Protocol (TKIP) as well as user authentication. TKIP scrambles the keys using hashing algorithms and appends an integrity-checking feature to reassure the user that the keys have not been tampered with. TKIP<sup>36</sup> uses a 48-bit initialization vector, per-packet key mixing, a message integrity code named "Michael" and a key distribution mechanism. WEP uses a 24-bit initialization vector, while a 48-bit initialization vector significantly increases the number of possible shared keys that can be dynamically generated. WEP is vulnerable to replay and initialization vector collision attacks, but TKIP can protect against this because of the new sequencing rules and extended IV. Using a per-packet key mixing, the key hierarchy structure and 128-bit based keys will be stronger. Per-packet mixing protects against key recovery attacks using tools like "AirSnort", which are used to crack weak WEP keys. The Michael checksum algorithm protects against forgery attacks.

## WPA Version 2

WPA is a temporary fix for WEP until WPA Version 2 (802.11i) is introduced in the second quarter of 2004<sup>37</sup>. Below is a chart from 3e Technologies International White Paper<sup>38</sup> comparing WPA with WPA v2 (802.11i) standard.

---

<sup>35</sup> <http://www.webopedia.com/TERM/W/WPA.html>

<sup>36</sup> "WPA should wipe out some WEP worries" <http://www.eweek.com/article2/0,3959,813619,00.asp>

<sup>37</sup> "3e Technologies International White Paper"  
[http://en1.endiva.net/3eti/files/literature/3010.5503\\_WLAN\\_White\\_Paper\\_8page\\_lores.pdf](http://en1.endiva.net/3eti/files/literature/3010.5503_WLAN_White_Paper_8page_lores.pdf)

Feature	Currently Implemented	Proposed 802.11i Implementation
802.1x	X	X
Basic Service Set	X	X
Independent Service Set		X
Pre-authentication		X
Key hierarchy	X	X
Key management	X	X
Cipher and Authentication Negotiation	X	X
TKIP	X	X
CCMP		X

As shown in the chart, the interim solution uses a subset of the 802.11i features, but as implemented today, it has a major flaw for enterprise environments: it doesn't support roaming. WPA doesn't support Independent Basic Service which is needed for operating in Ad Hoc mode. Pre-authentication which feeds the transfer session keys between access points when a user is roaming is also not implemented in the current WPA algorithm.

WPA v2 uses the AES-based CCMP protocol to establish an 802.11 Robust Security Network (RSN). It is designed to offer cryptographic security over the air equivalent to IPsec. It includes both RC4-based encryption which is the collection of protocol mechanisms that make up WPA and the AES-based algorithm called the Counter Mode CBC-MAC Protocol (CCMP). CCMP is based on a Federal Information Processing Standard-approved cipher, and is thought to be the future of wireless security at the link layer<sup>39</sup>. Currently, CCMP cannot become FIPS-approved because it uses an unapproved mode.

### III. Wi-Fi Vulnerabilities

#### *Insecurities Overview*

The most obvious drawback to using a Wi-Fi network concerns the method of data transfer itself. Whereas on a traditional LAN all data is passed between network elements via a physical cable, wireless LANs broadcast data between base stations and end users' computers via radio frequencies. As long as a

<sup>38</sup> "3e Technologies International White Paper" [http://en1.endiva.net/3eti/files/literature/3010.5503\\_WLAN\\_White\\_Paper\\_8page\\_lores.pdf](http://en1.endiva.net/3eti/files/literature/3010.5503_WLAN_White_Paper_8page_lores.pdf)

<sup>39</sup> "Draft 802.11i approved by NIST" <http://www.oreillynet.com/pub/wlg/3821>

person is within broadcast range of a base station (or other wireless user's computer in an ad-hoc network setup) they have the ability to cause mischief on that network. In general, attacks on wireless networks fall into four basic categories: passive attacks, active attacks, man-in-the middle attacks, and jamming attacks.<sup>40</sup>

## Passive Attacks

A passive attack can be easily accomplished by simply listening in on network traffic. That is, traffic that is not intended for your computer's address. This activity is commonly referred to as *packet sniffing*. Some claim that this activity is not illegal, and may be correct considering WiFi networks operate at an unlicensed spectrum of frequency. Regardless of the snooper's intent, the contents of packets of data passed between other senders and receivers can be captured, analyzed, and read; without anyone knowing the better. WEP, the Wired Equivalency Protection encryption, is one method used to keep wireless data private, but has its flaws. A common tool used to find and detail wireless networks (but not capture traffic) is Network Stumbler<sup>41</sup>. A useful piece of free software, this suite simply details signal strength, encryption types, names, and locations of wireless network access points. More detail is provided on Network Stumbler, WEP, and other tools below.

## Active Attacks

Wireless and wired networks share many commonalities, including methods of active attacks. Once a WiFi network is compromised, a malicious individual could introduce *malware*<sup>42</sup>, root kits (designed to give the cracker administrative access at a later time), theft and destruction of data, or perform other activities commonly associated with wired networks. One type of attack specific to wireless networks is bandwidth stealing, sometimes referred to as *spoofing*. In this attack an individual accesses shared WAN resources via the unsecured (or cracked) wireless network. If someone's private 802.11 router is connected to a DSL or cable modem, and serves this access to all on that network, the intruder would be able to use this high-speed access anonymously. Any further malicious activities initiated by this person could not be specifically traced back to him or her. Although MAC addresses can be filtered to allow only authorized users to access the network, there are fairly simple methods around this, detailed later in this discussion, as well as use of the WEP encryption algorithm and its weaknesses.

## Man-in-the-middle Attacks

Another type of attack that is gaining in popularity is the man-in-the-middle attack. This wireless variation on a standard man in the middle attack is implemented by placing an access point within range

---

<sup>40</sup> Shimonski, Robert. "Wireless Attacks Primer" [http://www.windowsecurity.com/articles/Wireless\\_Attacks\\_Primer.html](http://www.windowsecurity.com/articles/Wireless_Attacks_Primer.html)

<sup>41</sup> <http://www.netstumbler.com>

<sup>42</sup> *Malware*: Short for **malicious software**. Software designed specifically to damage or disrupt a system, such as a virus or Trojan horse.

of a legitimate network and copying that network's SSID (*Service Set ID* - which is readily available via Wi-Fi network administration utilities like Network Stumbler). WiFi networks aren't the only wireless networks vulnerable to this type of attack; indeed any communication made over the air is able to intercepted, analyzed, and retransmitted. An excellent example would be wireless keyboard and mice used commonly - their communications are not encrypted and can therefore be read and recorded<sup>43</sup>. While this attack is very similar to simple *sniffing* and *spoofing*, the difference lies in the fact that normal users' connections may be initialized via this inserted access point. All traffic, including passwords, secret keys, and data are passed through this point before being forwarded to the legitimate network. In this case, the use of the Network Stumbler tool can easily detect unauthorized access points by surveying active points in an area, alerting the network administrators to their existence.

## Jamming Attacks

Finally, jamming attacks, although not common, are used to disrupt Wi-Fi network communications. Similar to flooding a server with requests in a DOS attack, this attack floods the Wi-Fi spectrum with powerful signals on the same frequency, thereby cutting communications between the access points and their users. Although a signal is not technically 'jammed', it is interfered with enough to reduce the quality of the signal so it is unusable. Many drawbacks to this technique arise: Ståhlberg states that the fact that WLAN uses a very high frequency with a low output power makes it very difficult, if not impossible, for the attacker to jam a network within a building from outside.<sup>44</sup> The equipment is expensive, the result is very temporary, and therefore not a very tractable method of long-term network disruption.

With the framework provided by the above understanding of common types of attacks, this discussion will further focus on the methods and tools used to attack a network, and resulting impacts on Wi-Fi as a telecommunications medium.

## War Driving

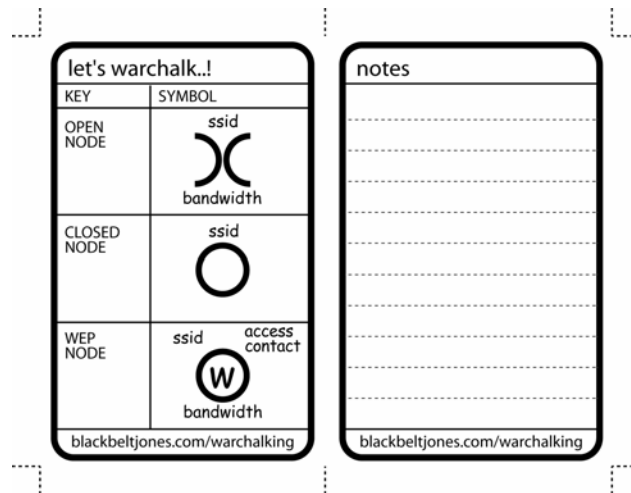
Although "War Driving" in itself is beyond the scope of this paper, it deserves some attention as a potential gateway into compromising a Wi-Fi network. We say potential because War Driving in itself is not illegal (this is also why it is considered beyond our scope for this discussion). Whether it is considered a heinous activity is more a function of the reader's ethics than a function of the law. Winn Schwartau describes War Driving as "[Driving] up and down streets, NetStumbler will identify the hundreds of networks in businesses, government offices and homes. The screen will display the kind of wireless

---

<sup>43</sup> "Logitech Wireless Devices are Vulnerable to Man-in-the-Middle Attacks", <http://www.securiteam.com/securitynews/5HP0Q004AM.html>

<sup>44</sup> Ståhlberg, Mika. *Radio Jamming Attacks Against Two Popular Mobile Networks*, Helsinki University of Technology

network access point, the manufacturer and the signal strength of the network you have detected. Most importantly, the network will broadcast its SSID (Service Set Identification) and the unique network media access control (MAC) address.”<sup>45</sup> The areas where Wi-Fi networks are found are marked by chalk (“war chalking”) on the streets to signify to others that a wireless network exists in that location.



*War Driving chalk-marks formatted for a wallet-size reference card*

The fact that Wi-Fi equipment is readily available (and cheap) has led to a grassroots movement of users allowing others to freely use their access points when in the area. Commonly called Free Nets, this allows travelers the ability to check email and access the internet. The potential malicious end of this comes in the form of others trying to attack these open networks. War Driving doesn’t just seek Free Nets – it seeks all networks. A malicious War Driver may see a closed network as a challenge, an open network as easy prey.

## **Wi-Fi (In)Security Statistics**

Although solid statistics regarding wireless or wired network security compromises are hard to come by, a number independent network enthusiasts have published their own findings on wireless access points. Although the trend to encrypt wireless access points with WEP seems to be increasing, a large number of insecure points still exist. Most statistics regarding secured Wi-Fi access points come from our War Driving friends, as mentioned above. The first “World Wide War Drive” took place between Aug. 31-Sept. 1, 2002, with a hundred people in six countries and two continents driving through twenty-two unique areas. War Drivers discovered 9,300 access points with a paltry thirty percent having turned on WEP encryption.<sup>46</sup> Great interest was generated by the statistics of this activity, and more World Wide War Drives have been conducted since, in October 2002, and most recently July 2003. A total of 122,454

<sup>45</sup> Schwartau, Winn. “War-Driving Lessons”, <http://www.nwfusion.com/columnists/2002/0902schwartau.html>

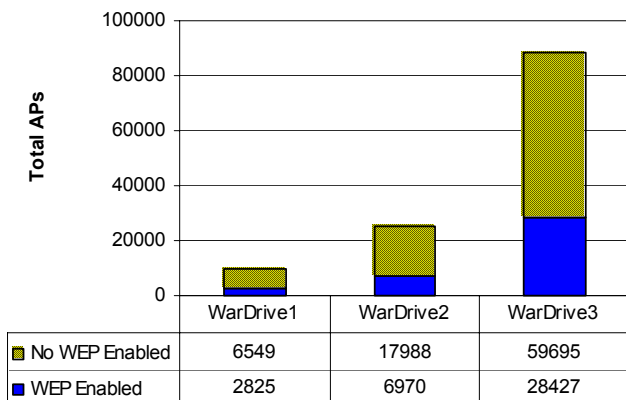
<sup>46</sup> D. Mohney, “WiFi War Driving”, [http://www.synchrologic.com/2003/09/23/eng-primemedia/eng-primemedia\\_112118\\_5773960666571695083.html](http://www.synchrologic.com/2003/09/23/eng-primemedia/eng-primemedia_112118_5773960666571695083.html)

access points have been cataloged via these efforts across four continents and fifty-two countries. An alarming number running unencrypted and using default settings, these points present little to no challenge for the casual attacker to take advantage.

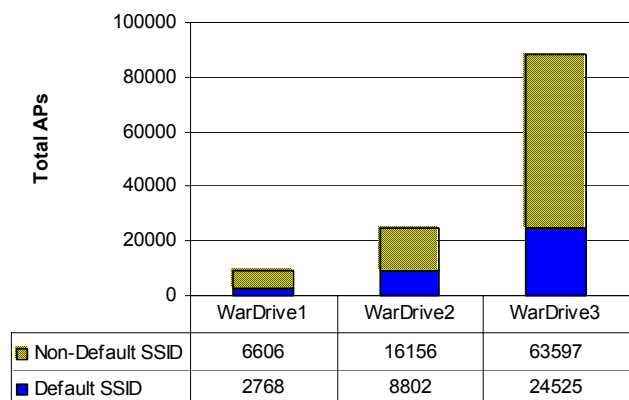
Furthermore, professional organizations, such as AirDefense, a WiFi security consulting company, have conducted their own surveys to confirm the above findings. Targeting Atlanta, Chicago, and San Francisco, and expanding their research to include most commercially available forms of WiFi encryption, the following was found of 1,136 access points<sup>47</sup>:

- 650 - 57 percent - did not utilize any form of encryption, such as WEP, WPA, LEAP, PEAP or other proprietary solutions
- 104 access points - 9 percent of the total - were rogue access points because they were in complete default settings for their SSID, channel, IP addressing and broadcasting of their SSIDs

World Wide War Drive WEP Statistics



World Wide War Drive SSID Statistics



Source: WorldWideWarDrive.org

**Compiled Stats of Atlanta, Chicago, and San Francisco**

Total Access Points Detected	1,136
Access Points without Encryption	650 (57%)
Rogue APs (100% default settings)	104 (9%)
Access Points Broadcasting SSID	876 (77%)
Consumer-Grade Access Points	331 (29%)
Ad Hoc Networks	45 (32 unencrypted)

Source: AirDefense Corporation <sup>48</sup>

<sup>47</sup> AirDefense, "War Drive Survey: 57% of Enterprise Wireless LANs not Encrypted", [http://www.airdefense.net/newsandpress/09\\_24\\_03.shtm](http://www.airdefense.net/newsandpress/09_24_03.shtm)

<sup>48</sup> AirDefense Corporation, [www.AirDefense.net](http://www.AirDefense.net)

This data leads us to one simple conclusion: the quick adoption of 802.11 wireless computer networks has resulted in insecure deployment in personal, business, and government use. In general, attacks on computer networks have increased as the number of world-wide computer users increases, and Wi-Fi will offer an additional target for denial of service, theft of data, and total compromise of computer networks.

## ***Tools and Methods***

Now that we have a basic understanding of the types of attacks Wi-Fi networks are susceptible to, and understand the insecure environment in which many are operating, we can more readily discuss the various tools and methods used in compromising these telecommunications networks. With compromise comes impact to the users, reactions from the keepers of the network, and more impacts to the users and Wi-Fi society as a result of those reactions. With a proper understanding of the tools and methods available, you can better secure your network. The following section aims to discuss these tools, methods, and user impacts.

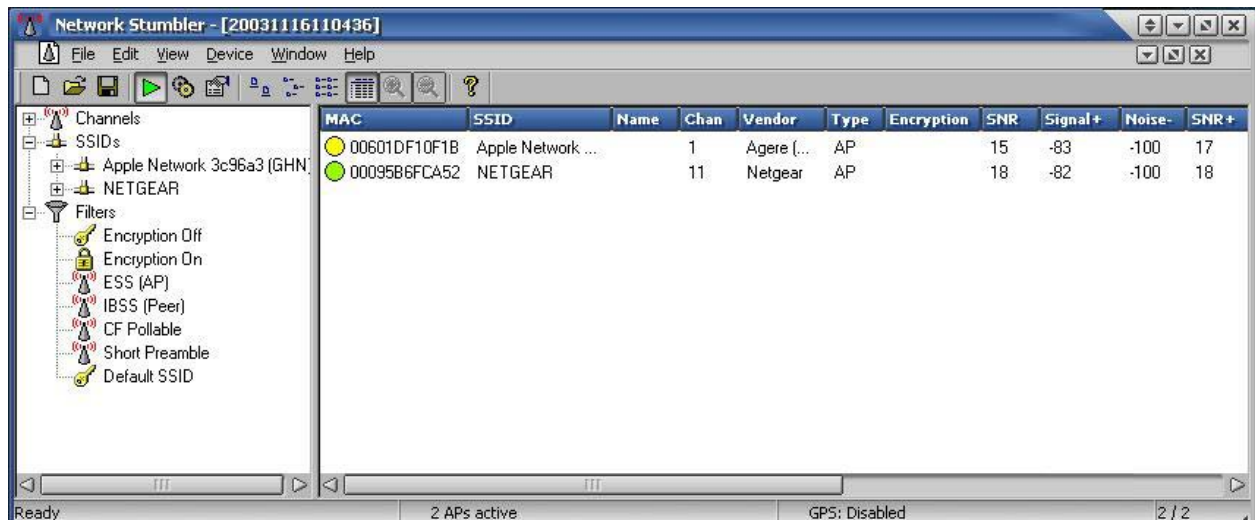
### **Network Stumbler**

A very useful tool for the wireless network engineer, Network Stumbler is a simple Wi-Fi access point discovery program. This software allows a user to not only identify where access points are located, but also grade the signal strength, identify the hardware vendor, examine encryption method used (or not used), and save a log of these findings. You can easily see the legitimate uses for this, as wandering your Wi-Fi campus testing access points and finding potential rogue points is a necessity. On the other hand, using this tool, or those with similar functionality, is the first step in discovering potentially insecure networks.

To further illustrate this point, KPMG consulting has been running a Honneypot network in London to gauge exactly how frequent security incidents are on an *unsecured* Wi-Fi network. According to VNUNET, "the company discovered that the five most common applications used by unauthorized users to connect were NetStumbler, ApSniff, GTKSKAN, WarDrive and Wellenreiter, which identify unsecured systems and attempt to gain access."<sup>49</sup> The data gleaned from a quick survey of existing Wi-Fi networks speaks volumes regarding the owner/operator's knowledge of or commitment to securing their network.

---

<sup>49</sup> VNUNET, "Securing Your Wireless Networks", <http://www.vnunet.com/Analysis/1148634>



*A sample of Wi-Fi networks in the Pittsburgh area provided by NetStumbler*

In the figure above, NetStumbler quickly shows us a survey of networks operating in a small neighborhood in Pittsburgh, PA. Two networks, identified by their SSID as “NETGEAR” and “Apple Network” are currently operating with no encryption. NetStumbler allows the would-be intruder to filter networks by the type of encryption used, if any, by SSIDs, and by channels which the access points are broadcasting on. By connecting a GPS device to the PC, NetStumbler will also log the exact coordinates of each network for future use and mapping.

As mentioned before, NetStumbler and other network discovery applications by themselves offer many legitimate uses. Other tools, skills, and motives are required to turn these applications to a devious nature.

## **WEPCrack**

As discussed earlier, one of the best methods for the casual user to protect their network is to enable the Wired Equivalent Protection (WEP) encryption algorithm available on most popular access points. Although this creates some processing overhead resulting in a drop in transfer rate, it is effective in preventing less-determined intruders from accessing your network. If you have a greater need to secure your network, though, WEP is far from the best choice to solely rely upon.

According to research conducted by Nikita Borisov, Ian Goldberg, and David Wagner at the University of California, Berkeley, WEP is vulnerable to four specific types of attacks:

- **Passive Attack to Decrypt Traffic:** this results from an improper implementation of integrity checks of encrypted data, and use of a small initialization vector (24 bits) to create new RC4 keys for

encryption. Such a small vector size almost guarantees the reuse of the same key. After capturing enough encrypted messages with the same key stream, statistical analysis will eventually yield an unencrypted message.

- Active Attack to Inject Traffic: If an attacker has knowledge of the plaintext for an encrypted message, he can use this information to construct correct encrypted messages, and insert them into the data stream.
- Active Attack from Both Ends: Extending the above attack, an attacker needs not know about the contents of a message, only its header. Specifically the destination IP address for encrypted packets. He can then flip bits to redirect these packets to a machine he controls.
- Table-Based Attack: Again, as a result of the small space of the initialization vector, with enough messages captured, an attacker can build a dictionary of initialization vectors and their corresponding key streams. Although almost 15GB of data needs to be intercepted, once the analysis is done, an attacker can decrypt every packet sent over the network.<sup>50</sup>

The underpinnings of RC4 and other encryption are well beyond the scope of this paper, so for more technical information regarding the weaknesses of RC4, refer to "Weaknesses in the Scheduling of the RC4 Algorithm" by Fluhrer, Mantin, and Shamir of Cisco Systems and The Weizmann Institute.<sup>51</sup>

Granted, the above attacks seem to require a fair amount of technical savvy and knowledge of cryptographic analysis. This is where software such as *WEPCrack* comes in. *WEPCrack* is developed for the Linux operating system, and is freely available under the GNU General Public License, and programmed in PERL scripting language. It automatically uses the known vulnerabilities of the RC4 key scheduling (described above).

*WEPCrack* first emulates encrypted data one may see on a WEP enabled network. It uses this pseudo-data to generate initialization vector combinations that can be used to weaken the secret key used on an actual WEP network. Secondly, it uses actual captured encrypted traffic to scan for weakened keys as generated in the first step. As it does this, it builds a dictionary of its findings. Finally, the script uses the data collected to attempt to determine the secret key being used on the network.

Another tool used exclusively for obtaining WEP encryption keys is *AirSnort*. *AirSnort* passively monitors encrypted transmissions and computes the secret key once enough packets have been captured. This package also runs on the Linux operating system, is freely available under the GNU General Public License, and is created in C.

---

<sup>50</sup> N. Borisov, I. Goldberg, D. Wagner, "Security of the WEP Algorithm", <http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>

<sup>51</sup> S. Fluhrer, I. Mantin, A. Shamir, "Weaknesses in the Scheduling of the RC4 Algorithm", [http://www.drizzle.com/~aboba/IEEE/rc4\\_ksaproc.pdf](http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf), Cisco Systems, The Weizmann Institute

According to the creator's web site, "AirSnort requires approximately 5-10 million encrypted packets to be gathered. Once enough packets have been gathered, AirSnort can guess the encryption password in under a second."<sup>52</sup> For anyone relying solely on WEP to protect their network access, this is a frightening statement. After capturing enough information to build a dictionary large enough, the secret key needed to access a WEP encrypted network simply pops out.

## Ethereal

Another very useful tool for network engineers is *Ethereal*. According to the maker's website, Ethereal, "...allows you to examine data from a live network or from a capture file on disk. You can interactively browse the capture data, viewing summary and detail information for each packet..."<sup>53</sup> Ethereal itself doesn't capture data from a network, but allows for easy graphical analysis of the protocols, data paths, and actual data being transmitted.

For the aspiring network intruder, this is the essence of snooping, or network sniffing. The implications are obvious: any unencrypted data sent across a network, including web page requests, email, documents, and passwords are easily readable. Using the advanced filtering features, a user can focus on the conversation between two IP addresses, and recreate the entire session. Wi-Fi exasperates this problem as the airwaves are a shared medium, and not contained to communication directly from a computer to a switch.

*A note on laws:* Unauthorized interception of data on a network is a serious offense. For this reason, the authors will not capture and network data, nor will examples of actual data be provided in this paper. In Pennsylvania specifically, Chapter 76, Subchapter B provides provisions defining computer offenses and grading of such crimes. Section 7611, defining unlawful use of computer and other computer systems, part (a), paragraph 2 states a person commits the offense of unlawful use of a computer if he "intentionally and without authorization accesses or exceeds authorization to access... any computer, computer system, computer network, computer software, program, database, world wide web site or telecommunication device or any part thereof..."<sup>54</sup>. An offense under this section constitutes a 3<sup>rd</sup> degree felony. Depending upon what the intruder does while sniffing the network they may be prosecuted under additional sections of Chapter 76.

---

<sup>52</sup> <http://airsnort.shmoo.com>

<sup>53</sup> <http://www.ethereal.com>

<sup>54</sup> Pennsylvania Code, Chapter 76, §7611(a)(2)

## **Wi-Fi Jamming**

As with any other radio waves, Wi-Fi is susceptible to attenuation over distance, limited by its broadcast power, and can be degraded due to environmental factors such as walls and interference. Since the 2.4GHz and 5GHz spectrums in which 802.11 run in are unlicensed by the FCC, anyone can run a transmitter without oversight. Licensed amateurs, on the other hand, can broadcast at much higher power levels than Wi-Fi Access Points.

Although neither inexpensive nor easy to accomplish, jamming of a Wi-Fi signal is possible. A Marconi Noise Generator used in conjunction with a powerful enough transmitter could create enough spread-spectrum noise to effectively sever communications between a Wi-Fi point and the computers it serves. For this type of denial attack to occur, an attacker must have this equipment set up relatively close to the point they'd like to jam, which further reduces the potential effectiveness.

## **IV. Wi-Fi at Carnegie Mellon University**

In 1994, CMU was awarded a \$500,000 grant from the NSF to build an experimental high-speed wireless network that was intended to support research and educational projects.<sup>55</sup> This wireless research project provided the foundation for CMU's wireless network today. In 1995, there were no 802.11 standards so a number of proprietary solutions were evaluated. These solutions were broadcasted in the unlicensed ISM band. CMU opted with AT&T's 915-MHz solution because of the shared vision between customer and supplier. AT&T used CMU as a test bed to learn network scalability.

### ***Deployment***

CMU deployed research wireless networks in five buildings with 75 access points to server 150 users. The idea was to allow a user or a robot to seamlessly connect and stay connected. At the time, wireless cards ran about \$800 per card with data rates at only 1-2 Mbps. By 1998, the IEEE launched the 802.11 standard and CMU considered a production wireless network. Agere (formerly AT&T/Lucent) extended its wireless commitment with CMU by funding a grant fro \$625,000 for 400 WaveLAN 802.11 compliant APs and network cards. Thus, in 2000, CMU had 30 buildings running wireless, with 24x7 support. By 2001, wireless was expanded into the 30 dormitories. In 2001, there were around 620 APs covering 60 buildings over 4 million square feet. Dorms constitute about half the wireless network. Currently, CMU's wireless network covers almost 100 percent of the campus and there are approximately 750 APs.

---

<sup>55</sup> ECAR, Case Study 6: Wireless Networking at Carnegie Mellon University, 2002

## ***Installation of Access Points (AP)***

The method of installing the AP was trial and error because every building is uniquely designed. Age, architecture, and building materials influenced the AP placement. CMU designed the network for coverage not capacity. CMU's residential halls had more fire doors, porcelain and ceramic fixtures resulting in 100 more APs installed than originally expected. The newer buildings only required about 12 APs. Dr. Alex Hills used a "Rollabout" which uses a computer on a cart. As it is moved around the room, it automatically creates a coverage map suggesting ways to install the APs. For channel allocation, CMU picked the 1, 6, and 11 which have the minimum overlap.

Due to architectural and security concerns, CMU decided to add external range antennas to each AP. The external antennas allow Computing Services to add new antennas as needed to address issues such as transmitting into a corner.

## ***Costs***

The original installation in the academic buildings would have been \$2000 per AP- \$1000 for an AP which was donated by Agere/AT&T/Lucent, and \$1000 for installation of power, data, wired network port, and labor cost. The price dropped when expanding the wireless to dorms: \$500 for an AP; \$600 to run power and data, including \$500 for the data cable, and another \$100 to power it over Ethernet; design and labor costs for two FTE's including three FTEs, plus \$55,000 for outside assistance. CMU also spent \$170,000 to upgrade the wired network infrastructure in the dorms. Russel Yount from CMU's Network Development Group estimates that roughly 60-70% of the cost of installing an Access Point is in the labor. He postulates that with the current trend the price of the devices themselves will no longer be an issue.

## ***Carnegie Mellon's Wireless Security***

Carnegie Mellon chooses to have an open system where the only mechanism to gain access to the actual network is through MAC address filtering. This means that a user needs to register their computer's MAC address with a protected database of allowed machines. The administrators felt it was too difficult to protect a single WEP (or similar) key for authorization. Likewise protecting the SSID seems difficult; therefore the SSID of the entire network is plainly named CMU.

Carnegie Mellon also allows for unregistered machines to access the network through a proxy. The proxy allows for all communication from Access Points through a heavily protected and secure Linux box where all wireless network communication passes. In this box there is essentially the equivalent of a switch where if the machine is registered it is allowed to access CMU's entire network and also the internet.

However, if the machine is unregistered, it is allowed to temporarily register through a CMU account and access software vulnerability patching websites.

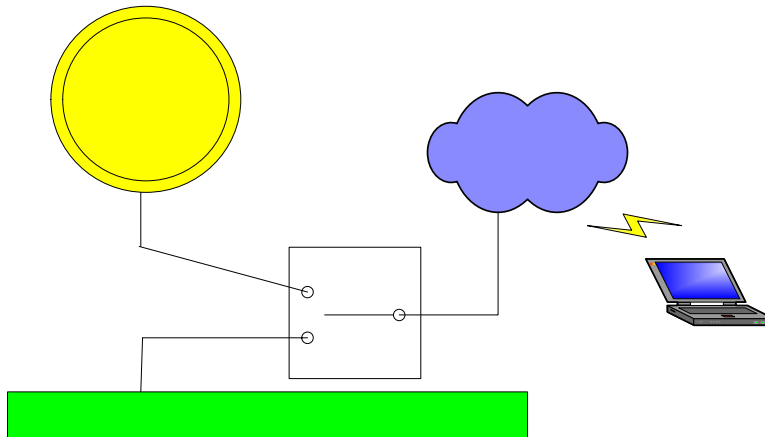


Diagram depicting CMU's Wireless Gateway

Computing Services also uses the unregistered access for problem computers on the network. They are allowed to access certain websites. This helps keep virus infected or vulnerable machines off the CMU network while giving them access to fix their problems.

## ***The Future of Wireless at Carnegie Mellon***

Wireless technology continues to grow at a fast pace and Carnegie Mellon is constantly evaluating new technologies as they emerge. The current plan is for Carnegie Mellon to implement 802.11a.<sup>56</sup> This will enable faster speeds on the wireless network and will suppress some of the current disturbances from other devices operating in the 2.4GHz spectrum.

As of July 2003, Carnegie Mellon had just over 10,000 registered wireless devices. With the current infrastructure there is a lack of ability to scale beyond approximately 1000 nodes.<sup>57</sup> Carnegie Mellon is planning on moving their network architecture to more of a flat backbone giving more subnet space for the wireless portion of the network. Their other hope is that Mobile IP will be an answer to help them in the future. If not the propagation of IPv6 which creates more IP address space will hopefully give Carnegie Mellon some more network IP room with which to play.

There are some technical obstacles that must be overcome before true mobile computing can become widespread. The most fundamental of these is how IP (the Internet Protocol) routes packets. The original system was designed with the notion of a fixed network location much similar to traditional home based phones and phone numbers. But since wireless networking gives the ability for a node to bounce around, a

<sup>56</sup> <http://www.cmu.edu/computing/wireless>

<sup>57</sup> [http://www.cmu.edu/computing/documentation/faq\\_wireless\\_tech/WireTechFAQ.html](http://www.cmu.edu/computing/documentation/faq_wireless_tech/WireTechFAQ.html)

packet's destination then becomes a moving target. Mobile IP (RFC 2002) is a new standard proposed to solve this dilemma. It specifically allows mobile devices to have two IP addresses: a fixed home address and a "care-of" address that will change with each new point of network attachment.<sup>58</sup> This new standard could alleviate some of Carnegie Mellon's current support issues in addition to assisting in the need of clearing up network address space.

## ***Carnegie Mellon as a Target***

We now understand some of the most common types of attacks and tools useful in breaching a wireless network. At Carnegie Mellon, we pride ourselves in having one of the earliest and largest-coverage Wi-Fi networks amongst higher-education institutions. But knowing what we do, the obvious question arises: how secure is our network, and how secure are the individuals using it?

Carnegie Mellon's Computing Service group does not publish statistics on wireless network security incidents, nor general network security incidents, out of fear someone may use that as a primer to gauge the network's vulnerabilities. Luckily, the Educause Center for Applied Research's recent paper "Wireless Networking at Carnegie Mellon University" can give us some insights on the security at hand.

## **Physical Security**

According to Lawrence Gallagher, manager of data communications at CMU, states "Due to campus architectural and security concerns, we use an external range antenna... we can hide the [access points] above the ceiling or inside a room"<sup>59</sup>. CMU clearly understands that an exposed access point is a vulnerable access point. By securing the actual access point hardware CMU ensures equipment cannot be tampered with or stolen.

## **Authentication**

The 'Wireless Andrew' system contains a single user authentication system: before a new user can access the network, they are presented with a web-based form used to register their MAC address. To complete access, they must provide their Andrew account and password. This is an excellent method to keep casual bandwidth thieves away, but has a crippling flaw: after this initial registration of the user's MAC address, the network is freely available to them without re-registration. During future sessions, the MAC address is transmitted automatically, verified by CMU's servers and the user again has access, without need for re-authentication. Transmitting the MAC address as the sole method of authentication means it can be snooped out of the air as it is transmitted and saved by an intruder.

---

<sup>58</sup> <http://www.computer.org/internet/v2n1/perkins.htm>

<sup>59</sup> ECAR, "Wireless Networking at Carnegie Mellon University", p.5

Using a method called **MAC Address Cloning** this intruder could transmit this authorized MAC address as his own to gain unfettered access to Wireless Andrew when he pleases. MAC addresses are typically contained in a serial EEPROM (electronically erasable programmable read-only memory) integrated circuit physically soldered into a computer's network card. With some know-how and the proper off-the-shelf tools, this integrated circuit can be reprogrammed to reflect whatever address one chooses.<sup>60</sup>

## Encryption

As previously discussed, encrypting the data flowing across your Wi-Fi network is essentially the easiest method to protect your data from snoopers. As we also know, encryption adds overhead to the data transmission, resulting in a significant drop in data-rate. CMU opts to not use WEP encryption due to this and other constraints it would place on the network. WEP does not lend itself to such a large user base, either, having to broadcast the encryption key to the thousands of users, as well as frequent key changes would make management a nightmare.

Instead, CMU relies on application-level encryption. Students are urged to use secure FTP, secure Telnet, and encrypted web pages when transferring sensitive data over the network. Any sensitive data – passwords, email, and social security numbers – are otherwise transmitted clearly across the network, and susceptible to sniffing.

## V. Conclusion

Wi-Fi networks are inherently insecure due to their broadcast nature and unfortunate reliance on WEP as the encryption *dú-jour*. This paper has explored the most common ways in which wireless networks are compromised – and gives the reader the ability to take action to secure a wireless network.

Don't forget: if it's easy for you to access, chances are it's easy for others to access, too!

---

<sup>60</sup> Kingpin, "MAC Address Cloning", [http://www.atstake.com/research/reports/acrobat/mac\\_address\\_cloning.pdf](http://www.atstake.com/research/reports/acrobat/mac_address_cloning.pdf)