Security and Legal Implications of Wireless Networks, Protocols, and Devices

Jeff Bilger, Holly Cosand, Noor-E-Gagan Singh, Joe Xavier

1. Overview

Wireless networks have become common place in the past several years in homes and offices. Wireless networks have had a significant impact in our society by enabling:

- Individuals to transport laptops and other devices to and from meetings in office buildings, increasing employee productivity.
- Devices within close range to synchronize without a physical connection.
- Mobile users to receive email, text messages, etc. while on the move.
- Connection to the internet, throughout a home, without the time consuming and difficult task of running cable through the structure of the home.

There are several different sets of communication standards, enabling wireless networking in these different scenarios, for different types of devices. In the home and office, laptops utilize Wireless Local Area Network (WLAN) technologies to connect to wired networks, experiencing the full capabilities of network and internet access. Devices may synchronize themselves over very short ranges to other devices or networked desktops, using the Bluetooth standard. Mobile devices like smart phones and personal digital assistants (PDAs) communicate, using cellular technology. In this document, we have chosen to limit our discussion to the first type of wireless technology, the Wireless Local Area Network (WLAN) technologies.

We begin or discussion of WLAN technologies in Section 2 by discussing the functionality and current standards that apply to WLANs. Once this foundation has been laid, we describe the vulnerabilities of these networks in Section 3. In Section 4, we explain how, when a network is vulnerable, you can detect that it is under attack. In Section 5, the possible defenses for attacks

are discussed. In Section 6, legal implications, which may help mitigate attacks are explored. Finally, we close in Section 6, looking to the future of WLANs.

2. Introduction to Wireless Networking

Wireless networks (LANs) function in one of two ways: clients connect to a central access point (AP) which acts as a hub to other clients and to a wired network, or clients connect in an ad-hoc peer-to-peer mode. APs facilitate their ability to be located by broadcasting a Service Set Identifier (SSID) at a fixed interval, typically 10 times per second, but the broadcast time may be configurable by the administrator of the AP. The SSID is just the name of the AP which may be used by clients to connect to the wireless network. Clients, equipped with a wireless network interface card (NIC), will see a list of available AP's SSIDs. The client may then select from the list of APs. If the AP is unsecured, the client may connect to the network, allowing them to use the network resources supported by that AP without authentication, otherwise, authentication will be required. APs are typically left unsecured by default. Administrators of the AP must enable security when placing it on the network.

All of this has been made possible through the use of radio waves, used as a communication mechanism for approximately 100 years. Although the use of radio waves has been present for a long period of time, the broad adoption and standardization of the underlying devices, technologies and protocols are much more recent, beginning with the formation of the IEEE 802.11 committee in 1990[1]. The 802.11 committee was charged with the task of utilizing a set of available radio frequencies for wireless computer communication. Using these frequencies, they have defined a number of standards, enabling multiple vendors to interoperate. These standards can be segmented into two different categories: 1) basic communication standards and 2) security

[1] Fixed, nomadic, portable and mobile applications for 802.16-2004 and 802.16e WiMAX networks, Link

standards that help protect the exchange of information through the communication channel. The communication and security standards developed under the IEEE committee are described below.

2.1. Communication Standards

The 3 most popular communication standards, that have been supported by the 802.11 committee, are: 802.11a, 802.11b, and 802.11g[2]. Each of these standards is described below.

	802.11A	**802.11B**	**802.11**G
Year Released	1999	1999	2003
Communication Band	5GHz	2.4GHz	2.4GHz
Bandwidth	54Mbps	11Mbps	54Mbps
Communication Distance	50 meters	100 meters	100 meters
Channels	8	14	14
Compatibility	none	g	b

2.1.1. 802.11a and 802.11b

In 1999, the 802.11 committee ratified the 802.11a and 802.11b standards. The 802.11a and 802.11b standards, while ratified by the committee at the same time, are incompatible with each other.

The 802.11a standard enables 54Mbps of data in its communication. To transmit data, the 5GHz band was used, permitting 8 simultaneous channels over a maximum of 50 meters.

The 802.11b standard enables 11Mbps of data in its communication, using the 2.4 GHz band, permitting 14 communication channels over a maximum of 100 meters.

2.1.2. 802.11g

In 2003, the set of wireless communication standards was extended to include the 802.11g standard. The 802.11g standard enables 54Mbps of data communication, as does

[2] Intel, Understanding Wi-Fi and WiMAX as Metro-Access Solutions, Link

the 802.11a standard, however, utilizing the 2.4 GHz band as does the 802.11b standard. As with the 802.11b standard, 14 channels are available with a coverage range of up to 100 meters[3]. The 802.11g standard is compatible with the 802.11b standard, but incompatible with the 802.11a standard[4].

2.2. Security Standards

The 802.11 committee realized the importance of communication security, using the communication standards over open air waves, and therefore all 802.11 devices, included security protocols as part of their specification[5]. There are currently 3 security standards that have been ratified for devices that support the 802.11 standard[6]. Wired Equivalent Privacy (WEP), WiFi Protected Access (WPA)[7], and WiFi Protected Access 2 (WPA2 (802.11i). These standards are summarized and described below.

	WEP	**WPA**	**WPA2**
Year Ratified	1999	2003	2004
Key size	40 bit	128 bit	128, 192 or 256 bit
Key State	Static	Dynamic	Dynamic
Central Key Management	None	RADIUS	RADIUS
Authentication	WEP Key Challenge	802.1X authentication protocol with Extensible Authentication Protocol (EAP)	802.1X authentication protocol with Extensible Authentication Protocol (EAP)
Encryption Scheme		Temporal Key Integrity Protocol (TKIP)	Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES) for client-to-client
Device Compatibility	802.11a,b,g	802.11a,b,g	802.11a,b,g

[3] Kevin Suitor, What WiMAX Forum Certified products will bring to Wi-Fi, , Link
[4] Intel and WiMax: Accelerating Wireless Broadband, Link
[5] Trends in Telecom, Wireless Services for the Mainstream, Link
[6] Wi-Fi Alliance, Securing Wi-Fi Wireless Networks with Today's Technologies, Link
[7] Wi-Fi Alliance, Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks, Link

2.2.1. Wired Equivalent Privacy (WEP)

The Wired Equivalent Privacy (WEP) standard was introduced with the 802.11 standards, but by 2001 a number of weaknesses had been discovered in the standard, leading to the adoption of new standards (WPA). The cryptographic weakness in WEP was, in part, intentional. At the time of WEP's introduction, cryptographic keys for export to international markets was limited to 40 bit keys. To further compound the weakness presented by short keys, the WEP standard uses a single, static shared key without a dynamic key update method. Some WEP implementations include longer keys of 128, 152, or 256 bits, but these are non-standard and therefore incompatible.

2.2.2. WiFi Protected Access (WPA)

The WiFi Protected Access (WPA) standard, addresses all deficiencies found in the WEP standard. This standard was introduced by the WiFi Alliance in 2003 to bridge the security gaps of WEP[8], prior to the formal adoption of the 802.11i (WPA2) standard. WPA is a subset of the 802.11i standard (WPA2). The WPA security standard is designed to secure all versions of 802.11 devices, including 802.11a, 802.11b and 802.11g, described above.

WPA can frequently be installed on WiFi certified devices as a software upgrade. Access Points (AP) require a software upgrade. Client workstations require a software upgrade to their network interface card (NIC) and possibly an additional upgrade to their operating system (OS). Enterprises may choose to use a Remote Authentication Dial-In User Service (RADIUS) authentication server. In homes, by utilizing a shared password mode, users may avoid the additional setup and support of a RADIUS authentication server.

[8] Andrea Bittau, The Fragmentation Attack in Practice, Link

WPA supports a strong encryption algorithm and user authentication. The WPA standard employs Temporal Key Integrity Protocol (TKIP) for encryption, using 128 bit keys that are dynamically generated.

In a corporate environment, keys are generated leveraging the 802.1X authentication protocol with Extensible Authentication Protocol (EAP). The 802.1X protocol, adopted by the IEEE in August of 2001, is a network access control method used on both wired and wireless networks. The 802.1X protocol's use of EAP, enables the support of a variety of user credential types, including username/password, smart cards, secure IDs, or any other type of user identification. Clients and Access Points (AP) authenticate against the RADIUS server which validates client access to the network, as well as, enabling connected clients to know they are talking to valid APs once they are on the network.
In a home environment, "pre-shared keys" (PSK) or passwords are used to provide TKIP encryption.

In the WPA standard, if enterprise security is employed, a user supplies credentials to the RADIUS server which authenticates the user, or if enterprise security is NOT employed, supplies a manually entered password on the client device and Access Point. Once a user is authenticated, a unique master or "pair-wise" key is created for the session. TKIP distributes the key to the client and Access Point (AP), using the pair-wise key to generate unique data encryption keys to encrypt every data packet that is sent during the session. A Message Integrity Check (MIC), when enterprise security (RADIUS) is employed, prevents a "man in the middle" alteration of packets by requiring both the sender and receiver to compute and compare the MIC, assuming an attack and discarding the packet if the MIC doesn't match.

2.2.3. WiFi Protected Access 2 (WPA2 (802.11i))

The WiFi Protected Access 2 (WPA2) standard, also known as 802.11i, is a superset of WPA. It includes the 802.1X/EAP authentication for corporate environments and PSK authentication for home environments. In addition, a new encryption scheme called Advanced Encryption Standard (AES) has been added. Its addition is to support ad hoc networking security between client workstations. It supports encryption, using keys of 128, 192 or 256 bits. The WPA2 standard is fully compatible with existing WiFi devices, including WPA devices. This standard was adopted in 2004.

3. Vulnerabilities of wireless networks, devices, and protocols.

There are a number of vulnerabilities in the security protocols listed above. We describe some of these vulnerabilities in the following sections.

3.1. Insertion attacks

Insertion attacks are based on deploying unauthorized devices or creating new wireless networks without going through security process and review.

- Unauthorized Clients – An attacker tries to connect a wireless client, typically a laptop or PDA, to an access point without authorization. Access points can be configured to require a password for client access. If there is no password, an intruder can connect to the internal network simply by enabling a wireless client to communicate with the access point.
- Unauthorized or Renegade Access Points – An organization may not be aware that internal employees have deployed wireless capabilities on their network in the form of an unauthorized access point, attached to the wired network.. This lack of awareness could lead to the previously described attack, with unauthorized clients gaining access to corporate resources through the rogue access point.

3.2. Interception and Monitoring of Wireless Traffic

As in wired networks, it is possible to intercept and monitor network traffic across a wireless LAN. The attacker needs to be within range of an access point (approximately 300 feet for 802.11b) for this attack to work, whereas a wired attacker can be anywhere there is a functioning network connection. The advantage for a wireless interception is that a wired attack requires the placement of a monitoring agent on a compromised system. All a wireless intruder needs is access to the network data stream traveling over public air waves.

There are two important considerations to keep in mind with the range of 802.11b access points. First, directional antennae can dramatically extend either the transmission or reception ranges of 802.11b devices. Therefore, the 300 foot maximum range attributed to 802.11b only applies to normal, as-designed installations. Enhanced equipment also enhances the risk. Second, access points transmit their signals in a circular pattern, which means that the 802.11b signal almost always extends beyond the physical boundaries of the work area it is intended to cover. This signal can be intercepted outside buildings, or even through floors in multistory buildings. Some of the monitoring techniques:

- Wireless Packet Analysis – Attacker captures wireless traffic using techniques similar to those employed on wired networks. Many of these tools capture the first part of the connection session, where the data would typically include the username and password. An intruder can then masquerade as a legitimate user by using this captured information to hijack the user session and issue unauthorized commands.
- Broadcast Monitoring – If an access point is connected to a hub rather than a switch, any network traffic across that hub can be potentially broadcast out over the wireless network. Because the Ethernet hub broadcasts all data packets to all

connected devices including the wireless access point, an attacker can monitor sensitive data on the wireless network, not even intended for any wireless clients.

- Access Point Clone (Evil Twin) Traffic Interception – The availability of WiFi in coffee shops, airports and other high-traffic areas led to the evolution of the Evil Twin Network[9]. The Evil Twin is essentially a wireless version of a phishing scam - users think they're connecting to a genuine hot spot but are actually connecting to a rogue access point set up by a phisher. Once connected, the attacker serves up pages mimicking actual websites. Banking, EBay or PayPal sites are the websites of choice. All the attacker needs is the hardware for an access point (with a higher signal strength than the target network) and off-the-shelf software tools like Karma[10] which is a set of wireless sniffing tools to discover clients and their preferred/trusted networks by passively listening for 802.11 Probe Request frames. Once identified, clients can be targeted by creating a Rogue AP for one of their probed networks (which they may join automatically) or using a custom driver that responds to probes and association requests for any SSID. Higher-level fake services can then capture credentials or exploit client-side vulnerabilities on the host.

3.3. Jamming

Denial of service attacks are also easily applied to wireless networks, where legitimate traffic can not reach clients or the access point because illegitimate traffic overwhelms the frequencies. An attacker with the proper equipment and tools can easily flood the 2.4 GHz frequency (or the other frequencies in which WiFi operates), corrupting the signal until the wireless network ceases to function. In addition, cordless phones, baby monitors and other

[9] Internet : http://news.bbc.co.uk/2/hi/technology/4190607.stm
[10] Available: http://www.theta44.org/karma/index.html

devices that operate on the 2.4 GHz band can disrupt a wireless network using this frequency. These denials of service attacks can originate from outside the work area serviced by the access point, or can inadvertently arrive from other WiFi devices installed in other work areas that degrade the overall signal.

3.4. Client-to-Client Attacks

Two wireless clients can talk directly to each other, bypassing the access point. Users therefore need to defend clients not just against an external threat but also against each other.

- File Sharing and Other TCP/IP Service Attacks – Wireless clients running TCP/IP services such as a Web server or file sharing are open to the same exploits and misconfigurations as any user on a wired network.
- DOS (Denial of Service) – A wireless device floods another wireless client with bogus packets, creating a denial of service attack. In addition, duplicate IP or MAC addresses, both intentional and accidental, can cause disruption on the network.

3.5. Brute Force Attacks Against Access Point Passwords

Most access points use a single key or password that is shared with all connecting wireless clients. Brute force dictionary attacks attempt to compromise this key by methodically testing every possible password. The intruder gains access to the access point once the password is guessed.

In addition, passwords can be compromised through less aggressive means. A compromised client can expose the access point. Not changing the keys on a frequent basis or when employees leave the organization also opens the access point to attack. Managing a large number of access points and clients only complicates this issue, encouraging lax security practices.

3.6. Attacks against Encryption

The 802.11, Wired Equivalent Privacy (WEP) standard, described above, was intended to make a WLAN as secure as an unsecured wired network.

Not long after WEP was developed, a series of independent research studies began to expose its cryptographic weaknesses. The first practical attack on WEP was identified by researchers[11] Scott Fluhrer, Itsik Mantin and Adi Shamir who found that, even with WEP enabled, third parties with a moderate amount of technical expertise and resources could breach WLAN security.

Three key difficulties were identified:

- WEP uses a single, static shared key. It remains the same unless a network administrator manually changes it on all devices in the WLAN, a task that becomes ever more daunting as the size of the WLAN increases.
- At the time of its introduction, WEP employed a necessarily short 40-bit encryption scheme. The scheme was the maximum allowed by US export standards at that time. In 1997, the US government deemed the export of data cryptography to be as threatening to national security as the export of weapons of mass destruction. By necessity, WiFi security had to be weak if the specification was to be adopted as an international standard and if products were to be freely exported.
- Other technical problems contributed to its vulnerability, including attacks that could lead to the recovery of the WEP key itself. Attacks based on Fluhrer, Mantin and Shamir's paper have come to be known as "FMS Attacks". Shortly after the FMS paper was released, the following tools to automate WEP cracking were developed:

[11] Scott Fluhrer, Itsik Mantin and Adi Shamir, Weaknesses in the Key Scheduling Algorithm of RC4. Link

- WEPCrack
- AirSnort

In response to the weaknesses in WEP new security mechanisms were developed.

- Cisco developed the Lightweight Extensible Authentication Protocol (LEAP)
- WiFi protected access (WPA) was developed to replace WEP. It had 2 sub-parts-
  - WPA-PSK (Pre-Shared key)
  - WPA-Radius

In March 2003, Joshua Wright[12] disclosed that LEAP was vulnerable to dictionary attack. A short time later Wright released ASLEAP, a tool to automate attacks against LEAP. Cisco released EAP-FAST as a replacement for LEAP about a year after Wright's initial disclosure to them.

In November 2003 Robert Moskowitz of ISCA Labs detailed potential problems with WPA when deployed using a Pre-Shared Key in his paper "Weakness in Passphrase Choice in WPA Interface".

In November 2004 Joshua Wright released CoWPAtty which could perform an automated dictionary attack process against WPA-PSK networks.

Despite excessive media outcry, WEP was still safe to use in some environments. Cracking a WEP key was so time consuming that it was often not feasible. Regular rotation of WEP keys could render FMS atttacks ineffective on most networks. However, that changed when h1kari of Dachboden Labs released a paper detailing ways to effectively crack WEP.

[12] ComputerWorld, Cisco Reiterates WLAN Threat, Link

In 2004 new tools such as Aircrac[13] and Weplab[14] based on a Chopping attack were released. Their methodology was to take a WEP packet and "chop" off the last byte to break the CRC/ICV. If the last byte was 0, the tools would XOR last the last 4 bytes with a certain value to make a valid CRC and then retransmit the packet. This attack methodology significantly reduced the amount of time required to crack WEP keys. It made a largely theoretical attack (FMS) very realistic.

Attacks against WEP

Even with chopping attacks, a large number of packets still need to be captured by an attacker. The easiest way to do this is by re-injecting packets back into the network to generate unique initialization vectors.

Attacks against WPA

WPA Pre shared keys with pass-phrases shorter than 21 characters is vulnerable to dictionary attacks. This is an offline attack and not as easy to identify in real time as attacks against WEP.

3.7. Misconfiguration

Many access points ship in an unsecured configuration in order to emphasize ease of use and rapid deployment. Unless administrators understand wireless security risks and properly configure each unit prior to deployment, these access points will remain at a high risk for attack or misuse. The following section examines three leading access points, one each from Cisco, Lucent and 3Com. Although each vendor has its own implementation of 802.11b, the underlying issues should be broadly applicable to products from other vendors.

[13] Download: http://www.cr0.net:8040/code/network/
[14] Download: http://weplab.sourceforge.net/

- **Server Set ID (SSID)** – SSID is a configurable identification that allows clients to communicate with an appropriate access point. With proper configuration, only clients with the correct SSID can communicate with access points. In effect, SSID acts as a single shared password between access points and clients. Access points come with default SSIDs. If not changed, these units are easily compromised. Here are common default SSID's:

Manufacturer	Default SSID
Cisco	tsunami
3Com	101
Lucent/Cabletron	Roam About Default Network Name
Addtron	WLAN
Intel	intel
Linksys	linksys

SSIDs go over the air as clear text if WEP is disabled, allowing the SSID to be captured by monitoring the network's traffic.

Another common vulnerability regarding the SSID is setting it to something meaningful such as the AP's location or department, or setting them to something easily guessable.

By default, the Access Point broadcasts the SSID every few seconds in what are known as 'Beacon Frames'. While this makes it easy for authorized users to find the correct network, it also makes it easy for unauthorized users to find the network name. This feature is what allows most wireless network detection software to find networks without having the SSID upfront.

- **Wired Equivalent Privacy (WEP)** – WEP can be typically configured as follows:
  - No encryption
  - 40 bit encryption

- 128 bit encryption

Most access points ship with WEP turned off. Although 128 bit encryption is more effective than 40 bit encryption, both key strengths are subject to WEP's known flaws.

- **SNMP Community Passwords** – Many wireless access points run SNMP agents. If the community word is not properly configured, an intruder can read and potentially write sensitive data on the access point. If SNMP agents are enabled on the wireless clients, the same risk applies to them as well.

  By default, many access points are read accessible by using the community word, "public". 3Com access points allow write access by using the community word, "comcomcom". Cisco and Lucent/Cabletron require the write community word to be configured by the user or administrator before the agent is enabled.

- **Client Side Security Risk** – Clients connected to an access point store sensitive information for authenticating and communicating to the access point. This information can be compromised if the client is not properly configured. Cisco client software stores the SSID in the Windows registry, and the WEP key in the firmware, where it is more difficult to access. Lucent/Cabletron client software stores the SSID in the Windows registry. The WEP key is stored in the Windows registry, but it is encrypted using an undocumented algorithm. 3Com client software stores the SSID in the Windows registry. The WEP key is stored in the Windows registry with no encryption.

- **Installation** – By default, all three access points are optimized to help build a useful network as quickly and as easily as possible. As a result, the default configurations minimize security.

3.8. Possible losses

The possible losses because of WiFi vulnerabilities are the same as in wired networking technologies plus the additional losses because of the wireless access. These include:

- Loss of network access, including email, Web, and other services that can cause business downtime.
- Loss of confidential information, including passwords, customer data, intellectual property, and more.
- Data interception and theft is difficult to detect and can lead to even more losses.
- Unauthorized access – the mobility of wireless devices means that they are far more susceptible to loss, which could result in the theft of information from the device. In addition, if authentication is weak at the device level, unauthorized individuals will gain access to sensitive information.
- Legal liabilities associated with unauthorized users.
- Loss of information integrity – wireless devices or data transmission methods may not have the capability to check data integrity, which could result in data being deleted or altered in transmission.
- Network Abuses – Since the speed of the wireless networks is still less compared to wired networks, any abuse on the wireless network could impact the performance of WLAN. For example, WLAN users will encounter network performance degradation due to network congestion when users are doing large file transfer across WLAN. The WLAN 802.11 standard is a shared media until after it gets onto the network. Additionally, the protocol requires large headers for each packet transferred.
- Cyber criminals have begun to use the unsecured WiFi networks of unsuspecting consumers and businesses to help cover their tracks in cyberspace.

4. Detection of attacks on wireless networks, devices, and protocols.

4.1. General Intrusion Detection Methods

An intrusion is defined[15] as any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource. The first line of defense in any network is intrusion prevention – using Firewalls and securing access using encryption and authentication. Firewalls are outward looking and limit access between networks to prevent an intrusion from happening. Authentication can range from passwords to biometric devices. However, it has to be assumed that this line of defense can and will be breached. The second line of defense is an Intrusion Detection System (IDS). Intrusion Detection Systems monitor traffic inside the network to detect an intrusion. The main purpose of an IDS is to protect a network system once an attack is detected by minimizing damages (cut off affected sub-nets) and gather evidence for prosecution.

Most security systems for wired networks examine only Layer 3[16] (network) or higher abstraction layers. The assumption is that the lower layers are protected by the physical security of the wires. This assumption doesn't hold for wireless networks. Signals from wireless networks are usually omni-directional and emanate beyond the intended coverage area. This makes the physical security of the network mostly impractical. Ideally, an intrusion detection system for wireless networks should function at Layer 2 even lower. One of the earliest research papers to focus on Intrusion Detection Systems was by Anderson[17]. His methods use data that are collected for other reasons (e.g., performance analysis) and were

[15] Richard Heady, George Luger, Arthur Maccabe, and Mark Servilla. The architecture of a network level intrusion detection system. Technical Report CS90-20, Department of Computer Science, University of New Mexico, August 1990.
[16] Webopedia, OSI Layers, Link www.webopedia.com/quick_ref/OSI_Layers.asp
[17] J. P. Anderson. Computer security threat monitoring and surveillance. Technical report, James P. Anderson Company, Fort Washington, Pennsylvania, April 1980.

designed for batch mode processing e.g. at the end of the day. A later paper by Dorothy Denning[18] lays out a detailed framework for building an IDS.

In general, Intrusion Detection involves recording audit data (traffic, connections) and analyzing the data to detect an intrusion. The key assumptions of an IDS are:

- User and program activity is observable
- Normal and intrusion activities have distinct behavior.

There are two main types of IDS. Host-based IDS systems audit data and monitor events generated by programs and users on the host system. A network-based IDS is usually installed at the gateways of a network and examines network packets that are routed through the hardware interfaces. Another distinction between the types of IDS is in what action it takes when it detects an intrusion. A Passive IDS logs the event and signals an alert. A reactive IDS will cut off the offending user or close down the Access Point.

The two main approaches to wireless intrusion detection are Signature Analysis and Anomaly Detection. Signature Analysis, also called Misuse Detection, identifies known intrusions by detecting patterns of known attacks. Signature Analysis is similar to how most virus scanners work – it's only as good as the signatures provided to it and relies on regular signature updates to keep abreast of known attacks. There are few false positives, when attacks are detected. STAT[19] is a system that uses Signature Analysis. Anomaly Detection works by detecting deviations from established normal usage patterns and flags these as anomalies. Anomaly Detection doesn't require prior knowledge of an attack signature so can detect new

[18] Dorothy E. Denning, An Intrusion-Detection Model, IEEE Transactions on Software Engineering, VOL. SE-13, No. 2, February 1987, 222-232. Link
[19] K. Ilgun, R. A. Kemmerer, and P. A. Porras. State transition analysis: A rule-based intrusion detection approach. IEEE Transactions on Software Engineering, 21(3):181-199, March 1995. Link

intrusion. However, since they rely on statistics of 'normal' usage patterns, they can have a high false positive rate. NIDES[20] is an IDS that uses Anomaly Detection.

While the basic principles of Intrusion Detection are similar for both Wired and Wireless Networks, Wireless Networks present a unique set of challenges.

- No clear separation between normalcy and anomaly. A node that sends out false routing information could be the one that has been compromised, or merely the one that is temporarily out of sync due to volatile physical movement.
- The physical layer is less secure than in fixed networks
- Ad-hoc networks do not have a fixed infrastructure
- There are no traffic concentration points, where packets can be monitored
- There is no clearly defined protected perimeter and no firewall
- Routing is based on trust and is cooperative in nature

4.2. Wireless Intrusion Methods

A number of attack vectors and vulnerabilities were covered in a previous section. This section on intrusion methods is only to provide a flavor of the various types of intrusions that a wireless IDS will have to contend with.

A really common intrusion method is "Wardriving". A "WarDriver" drives around neighborhoods (usually high-tech) with software that automatically detects and records IEEE 802.11 SSIDs on the street. The hardware usually only includes a laptop equipped with an 802.11 adaptor and an external antenna. Freely available software like Net Stumbler[21], that are built for Wardriving, can record positional information in conjunction with a GPS unit. Net Stumbler and other tools are covered in more detail later. WarDrivers are usually hobbyists who produce geographical maps of wireless networks including configuration information.

[20] Debra Anderson, Thane Frivold, Ann Tamaru, Alfonso Valdes, Next-generation Intrusion Detection Expert System (NIDES): A Summary, Computer Science Laboratory, SRI International. Link
[21] Download: http://www.stumbler.net

AirSnort[22] is a passive detector (doesn't emit signals) which collects wireless network traffic on the target network. Once enough frames have been collected AirSnort can detect the WEP key of the network by analyzing the "weak" frames. It might take a few hours to crack the key. Although firmware upgrades usually fix some of these issues, clients using outdated wireless network adapters leave the network vulnerable.

4.3. WLAN Scanners

Two tools that appear to be most commonly used by hobbyists and WarDrivers are Net Stumbler and Kismet[23]. Net Stumbler appears to be the most popular scanner used on Microsoft Windows. Net Stumbler works by sending 802.11 probes that actively scan by sending out requests every second and reporting on the responses. AP's by default, respond to these probes, but can be configured not to and to stay silent. We installed Net Stumbler on a Windows XP machine and captured signal strengths at a coffee shop in Seattle.

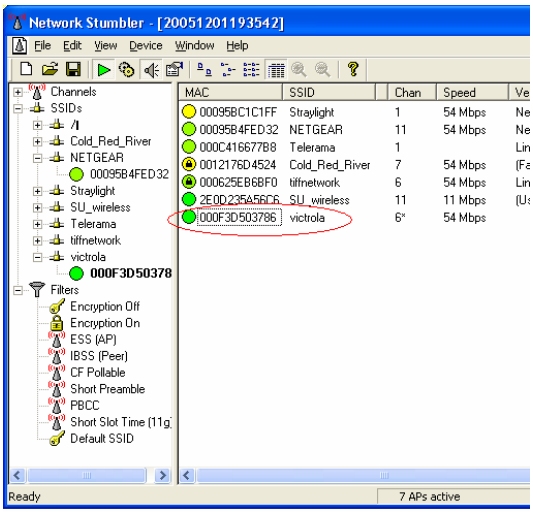

Figure 1: Available Networks in range

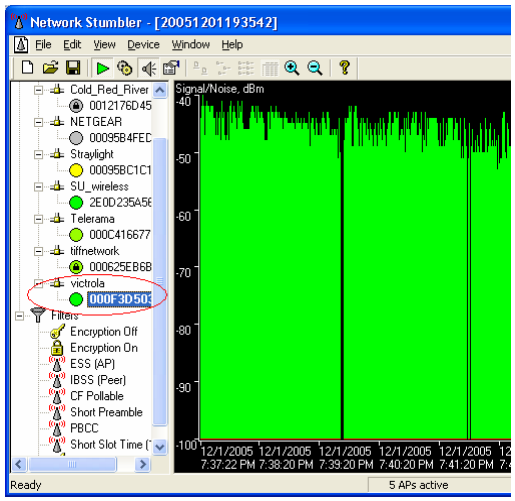

Figure 2: Signal Strength for the "victrola" network

Net Stumbler also has integrated support for a GPS unit allowing a WarDriver to easily build a wireless hot-spot map. As a bit of a social experiment we drove about the Capitol Hill

[22] Download: http://airsnort.shmoo.com
[23] Download : http://www.kismetwireless.net

neighborhood in Seattle mapping wireless access points using Net Stumbler. A partial result set is in Table 1. In all we detected 191 distinct wireless Access Points after approximately 2 miles of driving. Capitol Hill is a technologically advanced neighborhood and a lot of the residents are employed by high-tech companies and it followed that a majority of the networks were secured using WEP.

Latitude	Longitude	SSID	(BSSID)	[SNR Sig Noise]	WEP
N 47.6218117	W 122.3114700	Loop of Henley	(00:11:24:0c:92:e1)	[15 64 49]	No
N 47.6218117	W 122.3114700	AEGEAN	(00:0f:3d:5c:a9:b0)	[21 70 49]	Yes
N 47.6218117	W 122.3114700	ACTIONTEC	(00:0f:b3:49:d6:bb)	[26 75 49]	Yes
N 47.6218117	W 122.3114700	Ladro	(00:50:e8:02:2d:27)	[22 71 49]	No
N 47.6218117	W 122.3114700	Hicks	(00:12:17:f0:52:39)	[26 75 49]	Yes
N 47.6218117	W 122.3114700	ACTIONTEC	(00:0f:b3:3a:35:55)	[31 80 49]	Yes
N 47.6218117	W 122.3114700	seahome	(00:0d:88:44:97:97)	[17 66 49]	Yes
N 47.6218117	W 122.3114700	default	(00:0f:3d:06:81:1b)	[20 69 49]	Yes

Table 1: Some Results from WarDriving in Seattle

Kismet is another popular 802.11a/b/g network sniffer that can monitor networks using almost any card supported in LINUX and Mac OSX operating systems. Kismet is a passive sniffer and listens for network traffic as opposed to actively sending out probe requests. Over time, it can detect hidden networks by analyzing data traffic and building up a 'picture' of data movement.

4.4. Commercial Wireless IDS Products

AirDefense[24] is a complete hardware and software system comprising of sensors deployed throughout the network which are interfaced to a management appliance. It provides a management console for administration. AirDefense detects intruders and attacks and can also diagnose potential vulnerabilities in the network like misconfigurations. After an intruder

[24] Available : http://www.airdefense.net/products/

or attack is detected connecting to an access point, AirDefense can terminate the wireless connection from the intruder to the access point.

AirMagnet[25] runs on laptops or handhelds. For intrusions, AirMagnet detects unauthorized APs and clients and DoS attacks by flooding. It also performs real-time network audits to inventory all hardware, tracks all wireless LAN activity and enforces WLAN policies for security and management. Lastly, it monitors the health of the network to identify and respond to hardware failures, network interferences and performance degradation. The manufacturer claims that their latest version – Version 6.0, completely automates configuration, detection, analysis, mitigation, notification, security and management of the system.

Hot Spot Defence Kit[26] is a free, non-enterprise, host-based defence kit developed by the Shmoo Group to assist users in detecting wireless attackers. HotSpotDK which is available for Mac OS X and Windows XP, checks for changes in the Extended Service Set Identification (ESSID) in an infrastructure wireless network, MAC address of the access point, MAC address of the default gateway, and radical signal strength fluctuations. A change in signal strength is a good indicator for an Evil Twin Network. We installed the system on a Windows XP box. The source code (C#) is included in the download. The HSDK provides just enough information for a user to get suspicious about an obvious rogue Access Point. Trusted Access Point MACs can be specified along with thresholds for Signal Strength changes which are usually indicative of an Evil Twin Network.

[25] Download: http://www.airmagnet.com/
[26] Download: http://airsnarf.shmoo.com/hotspotdk.zip

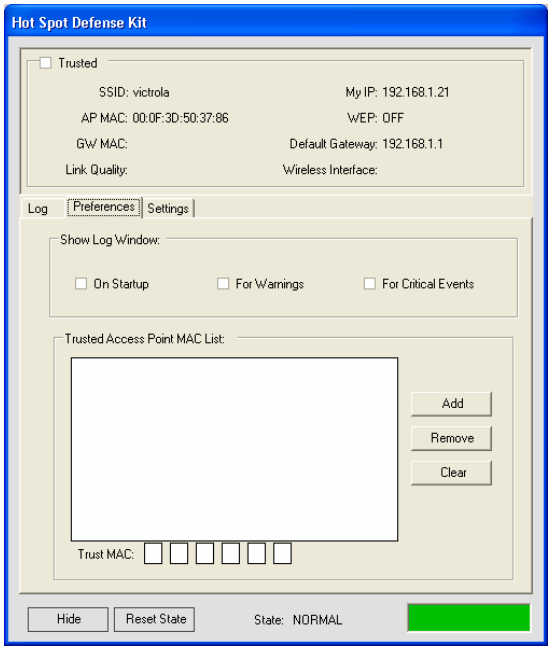

Figure 3: Specify a list of Trusted Access Points MACs

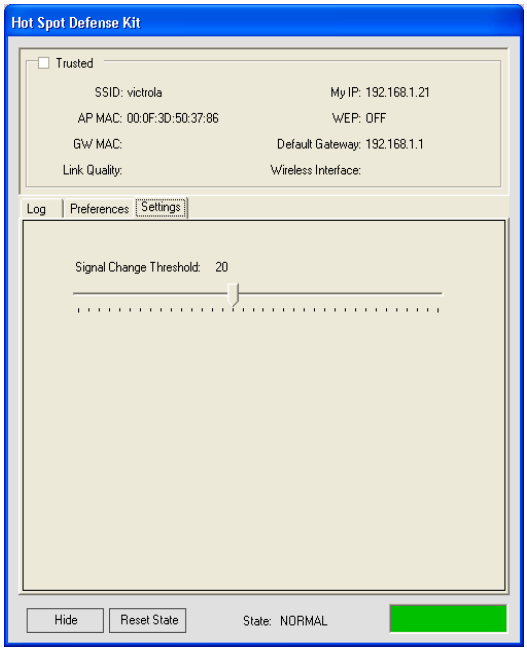

Figure 4: Set threshold for signal strength

AirSnare[27] is a free program (non-commercial license) for Windows that detects DHCP requests or unauthorized MAC addresses attempting to connect to an AP. The software can be configured to send an alert to the administrator and an optional message is sent to the intruder via Windows netmessage.

4.5. Academic Research

There are a number of research efforts into the area of Wireless Intrusion Detection and we attempt to review some of the more interesting ideas.

Anjum, Subhadrabandhu and Sarkar[28] appear to be the first to study the ease of using Signature-based intrusion detection with different routing protocols. The protocols considered

[27] Download : http://www.softpedia.com/get/Network-Tools/Network-Monitoring/AirSnare.shtml
[28] Farooq Anjum, Dhanant Subhadrabandhu, Saswati Sarkar. Intrusion Detection for Wireless Adhoc Networks. Proceedings of Vehicular Technology Conference, Wireless Security Symposium, Orlando, Florida, October 2003

were AODV[29], TORA[30], DSDV[31] and DSR[32]. They noted that signature based detection techniques are not likely to be completely effective in ad-hoc networks on account of the different path taken by various packets. By ensuring that malicious packets all take different paths, an intruder could evade leaving a "telltale" signature. Their conclusion was that this weakness will ensure that signature based attack detection will have incomplete information to work with in an ad-hoc network. They also observed that reactive routing protocols (AODV, TORA, DSDV) are less effective than proactive routing protocols (DSR) in facilitating the detection of intrusions.

Zhang and Lee[33] concluded in their study that an effective intrusion detection system for ad-hoc networks would need to be distributed and cooperative. They proposed an architecture where every node participates in intrusion detection by trying to detect anomalies. Individual IDS agents are placed on each node and monitors local activities. If anomalies are detected in local data or if the data is inconclusive then the IDS agents collectively participate in global intrusion detection actions.

Pietro and Molva[34] proposed a distributed IDS similar to [19] that consists of local observations that are combined and distributed to calculate a reputation value for each node. In their "Collaborative Reputation Mechanism" nodes are allowed to participate in the network or are excluded based on reputation. In their work, the authors specify in detail how the different nodes should cooperate to combine the local reputation values to a global reputation and how they should react to negative reputations of nodes.

---

[29] Definition - AODV : Ad Hoc On-Demand Distance Vector
[30] Definition - TORA : Temporally-Ordered Routing Algorithm
[31] Definition - DSDV : Destination Sequenced Distance Vector
[32] Definition - DSR : Dynamic Source Routing
[33] Yongguang Zhang, Wenke Lee. Intrusion Detection in Wireless AdHoc Networks. Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking MobiCom'2000), August 6–11, 2000, Boston, Massachussetts.
[34] Pietro Michiardi and Refik Molva. Prevention of Denial of Service attacks and Selfishness in Mobile Ad Hoc Networks.

Although [29] concluded that signature based attack detection will have limitations, it appears from surveying the literature that a distributed, signature based intrusion detection system like the one proposed in [29] has the most chances of being successful. The low occurrence of false positives and the ease of deploying signatures in a corporate environment (Systems Management Servers or auto-update from a central location) make this the most likely to succeed at the scale required by a large corporation.

5. Defense options: What can be done to make wireless networks more secure?

5.1. Introduction

Based on the known threats affecting WiFi networks it is possible to make pragmatic decisions regarding effective defense options. However, no single defense is sufficient to mitigate all threats; instead a multilayered approach is required. Yet, the very nature of a multilayered approach introduces complexities and it is important that security be easy to implement, use, and manage. Although defense measures are important, they are only one piece of a good security framework. This is because a good security framework is based on risks, defense, and deterrence[35]. This chapter will describe defense options in detail while other chapters will cover risks and deterrence.

5.2. Securing wireless networks today[36]

Although many wireless networks are unsecured or utilize faulty security, there exist many technologies and procedures that can make wireless networks less susceptible to successful attacks. These technologies range from the very easy to implement, such as requiring a password or key to access a wireless access point, to the extreme, such as surrounding your

[35] Butler Lampson, Microsoft, "Accountability and Freedom.", Link
[36] It is assumed that Red-Team penetration attacks are used to constantly assess threats.

office or home with radio dampening materials in order to keep the wireless signal from transmitting to the outside.

Despite the risks, the existing defense options are effective in mitigating threats from most sources. However, each wireless network owner and user must decide if the cost of defense is more than the expected cost due to loss[37].

5.2.1. Protect the access point

Most access points are configured with security *disabled*, a default administrator password and a default Service Set ID (SSID)[38]. Users normally do not change these default settings. This combination allows hackers to easily hijack the wireless network and possibly gain access to the administration of the access point as well.

In order to protect the access point, the following actions should be taken by the administrator of the access point:

- Require an administrator password to manage the access point.
- Change the administrator password on a regular basis.
- Change the default SSID to something innocuous (i.e. something that does not identify the make and model of the access point or the name of the company).
- If possible, configure the access point so that it does not broadcast its SSID.
- Change the encryption keys on a monthly or yearly basis and choose a longer key.

5.2.2. Enable authentication and encryption over the wireless channel

Unless authentication and encryption protocols are used over the wireless network, all data transmitted over the wireless network can be passively monitored and unauthorized

[37] Expected cost due to loss is calculated as (probability of attack) x (cost due to attack)
[38] PCMag, SSID Definition, Link

users can access the wireless network to launch other attacks or to steal bandwidth. The protocols should be chosen with care since not all authentication and encryption protocols are secure.

5.2.2.1. Try to avoid using WEP

Wired Equivalent Privacy (WEP)[39] is the authentication and encryption mechanism that is part of the IEEE 802.11 standard released in 1997. Even though WEP was known to have limitations, it was chosen in order to ensure efficient implementations[40]. However, after WEP supported wireless devices flooded the market, researchers showed that it had serious weaknesses and that it could be compromised[41].

Although WEP is better than nothing and may keep most people from exploiting a wireless network, any competent hacker can compromise a WEP enabled network. Additionally, automated tools[42] exist that allow even unskilled people crack WEP enabled networks in about 3 minutes[43].

Most wireless network cards can be upgraded with new firmware so that they will support stronger encryption using WiFi Protected Access (WPA) [44]. Unfortunately, most 802.11 access points purchased prior to 2003 will need to be replaced with ones that supports WPA.

---

[39] PCMag, WEP Definition, Link
[40] 802.11 WEP: Concepts and Vulnerability http://www.wi-fiplanet.com/tutorials/article.php/1368661
[41] SR Fluhrer, I Mantin, A Shamir, Weaknesses in the Key Scheduling Algorithm of RC4, Lecture Notes in Computer Science, Link
[42] Download: http://www.cr0.net:8040/code/network
[43] Compliancepipeline, FBI Teaches Lesson In How To Break Into WiFi Networks, Link
[44] PCMag, WPA Definition, Link

5.2.2.2. WPA

In 2002, the WiFi Alliance proposed an improved security protocol called WiFi Protected Access (WPA). This protocol implements a subset of the 802.11i security standard and was intended as an interim solution until the 802.11i standard was approved. Although WPA provides better security than WEP, a security researcher found a flaw[45] if short text only keys are used. Although the flaw has nothing to do with the protocol itself, many WPA enabled products allow users to define short keys that can be easily hacked.

Effective WPA keys should consist of more than 21 alphanumeric characters that form nonsensical words in order to be immune to brute force dictionary attacks.

Additionally, since WPA is based on RC4 encryption, it is susceptible to a packet forgery attack. However, WPA should be considered more than adequate security for most users.

5.2.2.3. WPA2

Although WPA provides sufficient security for most users, WPA2 is the official security protocol that implements the complete 802.11i security standard. Released in 2004, it provides enterprise and government grade security by utilizing Advanced Encryption Standard (AES)[46] and is not susceptible to a packet forgery attack like WPA is.

5.2.2.4. 802.11x

Enterprises should consider implementing full 802.11x solutions in order to protect their data. 802.11x supports mutual authentication as well as dynamic WEP between

[45] Slashdot, New Wireless Security Standard Has Old Problem?, Link
[46] PCMag, AES Definition, Link

a client and a back end RADIUS server. This provides more robust and secure access verification than MAC addressing and, if mutual authentication is used, it will eliminate susceptibility to man in the middle attacks.

5.2.3. Additional authentication and encryption for end-to-end encryption

Encryption and authentication protocols such as WEP, WPA, and WPA2 only encrypt and authenticate data traveling over the wireless connection. However, if a hacker accesses the wireless network without authorization and the wireless network connects to a wired network, sensitive data on the wired network could be exposed. To mitigate this threat, additional authentication and encryption such as that provided by Secure Sockets Layer (SSL)[47], Transport Layer Security (TLS)[48], and/or Virtual Private Networks (VPN's) should be used to encrypt the data from end-to-end[49].

5.2.4. Define and enforce security policies

Well defined policies for allowing or restricting wireless access can be used to reduce the likelihood of successful attacks on wireless networks. Some possible policies include:

- Turn off wireless access during off hours or when not at home.
- Use the strongest WEP, WPA, or WPA2 keys possible.
- Provide a separate wireless network for visitors to the office. Such a wireless network would not interface with the wired network.
- Only allow connections from devices with strong signals. Since the signal strength of a wireless connection is inversely proportional to the distance of the

[47] PCMag, SSL Definition, Link
[48] PCMag, TLS Definition, Link
[49] Note: Technologies such as VPN only encrypt data in the network layer and above. Also, broadcast traffic is not protected by VPN (IPSec). Thus wireless encryption such as WEP and WPA should be used as well in order to provide complete protection over the wireless connection.

device to the access point, a weak signal implies that the device attempting to access the wireless connection is far away and likely not in the physical building.

- Ad hoc networks (such as those providing wireless peer-to-peer connectivity between devices) should not be allowed.
- Unauthorized access points should be prohibited from being deployed on the network without approval.
- Devices should be configured to only allow connections to approved wireless networks and not to the wireless network with the strongest signal.
- Do not allow dual-homed devices (devices with both a wireless card and an Ethernet card) to exist on the network.

5.2.5. Utilize devices that are easy to configure

Many security exploits are caused by incorrectly configured wireless networks and devices. This is a direct result of the difficulty for the average user to configure their systems correctly. Products such as Linksys routers supporting SecureEasySetup[50] and the Buffalo AirStation[51] can be used to secure access points and devices at the push of a button.

5.2.6. Utilize Intrusion Detection solutions

In order to detect inappropriate or anomalous activity on the wireless network, intrusion detection solutions (as covered in Section 4) can be employed. Products such as those offered by AirDefense[52], Red-M[53], and AirMagnet[54] protect against accidental associations, rogue AP's, wireless phishing such as Evil Twin attacks as well as other

[50] Download: http://tinyurl.com/9abw7
[51] Download:. http://www.buffalotech.com/wireless/products/AOSS.html
[52] Download: http://www.airdefense.net/
[53] Download: http://www.red-m.com/

known and unknown threats. Moreover, most Intrusion Detection (ID) solutions support centralized management, support endpoint control and detection of risky configurations.

5.2.7. Define who can utilize the access points

Most access points support Media Access and Control (MAC)[55] address based filtering which specifies which devices can utilize that access point. As mentioned earlier, no single defense is sufficient; instead a combination of defenses should be utilized. As such, MAC address based filtering should be used in combination with wireless encryption and authentication such as WPA. Otherwise, and attacker could easily sniff the allowed MAC addresses and impersonate one of them in order to gain access to the network.

5.2.8. Segment all access points from your wired networks

As an additional defense measure, all access points should not simply bridge your wired network. Instead, every access point should be segmented behind a firewall in order to provide the best possible protection.

5.2.9. Define Protocol Filters

Protocol filters can be used to disallow or restrict traffic that is deemed unwanted or anomalous. Specifically, many Denial of Service (DoS)[56] attacks use uncharacteristically large Internet Control Message Protocol (ICMP) packets and these could be disallowed by defining a protocol filter.

5.2.10. Limit the broadcast range of the access point

If an access point is broadcasting its signal outside a home of office, a hacker can easily detect and perform reconnaissance on the network in order to mount an attack. However,

[55] PCMag, MAC Address Definition, Link
[56] CERT, Denial of Service Attacks, Link

if the access point is not broadcasting its signal outside the building then it is much more difficult to detect and attack such a network.

Some access points allow the power level of the radio signal to be adjusted, which in turn will increase or decrease the radius of the broadcast signal. Directional antennas can also be used to restrict the direction of the signal.

In other circumstances, special radio dampening paint and window shields from Force Field Wireless[57] or wall paper[58] can be used to contain the broadcast signal of the access point to the interior of the building. These two technologies also have the added benefit of protecting your wireless network from denial of service attacks from the outside since they also keep external radio signals out.

5.2.11. Educate end users

All the technology available is worthless unless the users of the system buy in and understand the rationale for the defense measures. Additionally, educating the end users on proper procedures and disclosure of sensitive information will make them less susceptible to social engineering[59] attacks.

5.2.12. Bait and confuse attackers

Certain defense options involve baiting or enticing hackers to attack an easy target. According to the contrast principle, if two wireless networks are available and one seems much easier to hack than the other, chances are the more secure wireless network will be left alone.

[57] Download: http://www.forcefieldwireless.com/products.html
[58] The Register, UK scientists roll out WiFi proof wallpaper, Link
[59] Internet Search for “social engineering”, Link

5.2.12.1. Fake access points

Fake access points allow legitimate wireless networks to hide in plain sight. This is achieved by literally generating thousands of fake access point beacon frames in order to confuse a would-be attacker. FakeAP[60] and Raw Fake AP[61] are two such tools that generate fake access point beacon frames and both are available for free.

5.2.12.2. WiFi Honeypots

In order to occupy would-be attackers as well as to gain an insight on new attack methods, WiFi honeypots[62] can be employed. WiFi honeypots are wireless networks consisting of vulnerable access points and computers that exist only to entice an attacker to probe and exploit that wireless network.

5.3. Cost-Effectiveness Analysis of current defense options

Even though valuation measures are not easily obtainable, we can use cost-effectiveness analysis to relate cost to a *measure* of outcome. To simplify the analysis, we will use a scale of 1-5 for cost (with 1 being no cost) and a scale of 0-5 for efficacy (with 0 being ineffective). Additionally, since most defense options available for WiFi networks and devices are not mutually exclusive, we will compare those alternatives separately from the alternatives that are mutually exclusive.

Protecting the access point

	Protect the access point	**Do nothing**
Efficacy	5	0
Cost	2	1
Cost-effectiveness ratio	2.5	0

[60] Download: http://www.blackalchemy.to/project/fakeap/
[61] Download: http://rfakeap.tuxfamily.org/
[62] SecurityFocus, Wireless Honeypot Trickery, Link

Compared to the alternative of doing nothing, protecting the access point is very cost effective.

Enabling authentication and encryption over the WiFi channel

	WEP	WPA	WPA2	802.11x	Do nothing
Efficacy	2	3	4	5	0
Cost	3	3	3	4	1
Cost-effectiveness ratio	0.6	1	1.3	1.25	0

For users who only have WEP enabled devices, using WEP is better than the alternative of doing nothing. For home users, it is most effective to use WPA2. For enterprises, 802.11x provides the best security option.

Using additional authentication and encryption for end-to-end encryption

	SSL/TLS	VPN	Do nothing
Efficacy	5	5	0
Cost	1	4	1
Cost-effectiveness ratio	5	1.25	0

Although SSL/TLS provide a high level of security and are extremely cost-effective, they are only utilized when visiting specific websites. VPN's are cost-effective, but only practical for enterprise users.

Define and enforce security policies

	Utilizing security policies	Do nothing
Efficacy	3	0
Cost	3	1
Cost-effectiveness ratio	1	0

Compared to the alternative of doing nothing, utilizing security policies in an effort to mitigate WiFi-related threats is cost-effective.

Utilize devices that are easy to configure

	Using an easy to configure device	Not using an easy to configure device
Efficacy	3	3
Cost	2	3
Cost-effectiveness ratio	1.5	1

Assuming the protection (efficacy) afforded by devices is relatively the same, the most cost-effective solution is the device that has less cost (easier to configure).

Utilize Intrusion Detection solutions

	Using an IDS	Do nothing
Efficacy	5	0
Cost	5	1
Cost-effectiveness ratio	1	0

Although ID solutions provide exceptional security benefits, their costs are prohibitively high for home users and most small businesses. For enterprises that require a heightened level of security, ID solutions are a cost-effective option.

Define who can utilize the access points

	Using MAC filtering	Do nothing
Efficacy	3	0
Cost	2	1
Cost-effectiveness ratio	1.5	0

Compared to the alternative, MAC address filtering is a cost-effective option.

Segment all access points from the wired network

	Segmenting access points	Do nothing
Efficacy	5	0
Cost	4	1
Cost-effectiveness ratio	1.25	0

Although segmenting all access points from the wired network affords exceptional security benefits, their costs are prohibitively high for home users. For enterprises, segmenting is a cost-effective option.

Define protocol filters

	Defining protocol filters	Do nothing
Efficacy	5	0
Cost	4	1
Cost-effectiveness ratio	1.25	0

Defining protocol filters is prohibitively high for home users, but it is cost-effective for enterprises.

Limit the broadcast range of the access point

	Reduce power level of the AP	Utilize special paint or wall paper	Do nothing
Efficacy	4	5	0
Cost	2	4	1
Cost-effectiveness ratio	2	1.25	0

It may be prohibitive for many home users it utilize special paint or wallpaper to limit the broadcast range of their access points. However, compared to the alternative of doing nothing, reducing the power level of their access point is cost-effective. For enterprise users, both options are cost-effective when compared to the alternative of doing nothing.

Educate end users

	Educate end users	Do nothing
Efficacy	3	0
Cost	3	1
Cost-effectiveness ratio	1	0

Compared to the alternative, educating end users is cost-effective for enterprises.

Utilize fake access points

	Using fake AP's	Do nothing
Efficacy	4	0
Cost	3	1
Cost-effectiveness ratio	1.3	0

This defense option is normally not applicable to home users. However it is cost-effective for enterprises.

Utilize WiFi Honeypots

	Using WiFi Honeypots	Do nothing
Efficacy	3	0
Cost	5	1
Cost-effectiveness ratio	0.5	0

This defense option is not applicable to home users. Some enterprises could consider it cost-effective compared to the alternative, but configuring and managing honeypots have a high cost.

5.4. Securing wireless networks for the future

Although many defense options are available to secure existing wireless networks, most are used to compensate for flaws that are part of the fundamental building blocks of the networks themselves such as protocol faults or weak encryption and authentication schemes. In order to

truly secure future wireless networks, decisive action and long range commitments must be taken today.

5.4.1. Support for long term fundamental research

Many of the problems of existing wireless networks cannot be solved without investing in fundamental research. Unfortunately, for the last 10 years funding for basic research has flat-lined[63]. Additionally, the research should not be classified since that would only benefit military and certain governmental entities.

5.4.2. Increase the cyber security research community

Currently, the cyber security research community is too small to effectively address all security issues with existing wireless networks, let alone perform basic research that could benefit future wireless networks. The government and universities should provide incentives to retain current researchers as well as attract new researchers to the field.

5.4.3. Provide incentives or mandates to upgrade

Although the first generation of wireless networks and devices were easily exploitable, interim improvements to these protocols now exist. Yet, this introduces some backward compatibility issues which makes existing networks and devices less secure than they could be. Future wireless networks and devices will suffer from this same problem because in order for devices and wireless networks to interoperate, they must use a lowest common denominator of authentication and encryption. To break this cycle, incentives or rebates could be provided by the government, manufacturers, or insurance companies that encourage (or even mandate) a user to upgrade their networks and devices to the most secure versions.

[63] NITRD, Cyber Security: A Crisis of Prioritization, Link

5.4.4. Devise incentives to force manufacturers to focus on security usability

Until securing a wireless device is as easy as locking a door, many WiFi systems will continue to be exploited. Economic theory[64] tells us that incentives are required to get the manufacturers to invest their resources in solving the security usability problem. In order to provide the appropriate incentive, manufacturers should be held liable if their products can not be secured with reasonable effort due to faulty or unintuitive user interfaces.

Although products that make configuration of security easier such as SecureEasySetup[65] by Broadcom do exist, many manufactures have opted not to utilize them.

5.4.5. Wireless standards should be driven by security

When wireless standards are driven by market pressures, politics, and export laws, disaster ensues. The canonical example is the initial 802.11 standard in which the WEP protocol was chosen (due to political issues, export laws, and market pressure) despite known vulnerabilities. The end result was catastrophic. Insecure wireless networks are ubiquitous, years of standardization work was required just to address the introduced security vulnerabilities, and backward compatibility issues continue to undermine security to this day. If the standards are driven by and designed around security, then this could be avoided.

5.4.6. Enforce standards compliance

Unlike the telecommunication industry, which is based on standards[66]; the computing industry is driven by the concept of being "first to market", usually at the detriment of security. Some companies even develop their own standards and hope for consensus after

[64] Hal Varion, UC Berkeley, "Economics and Computer Security.", Link
[65] Download: http://www.broadcom.com/products/secureeasysetup.php
[66] ITU, Homepage, Link

the fact. The end result is that multiple competing standards exists which introduce confusion, insecurity, interoperability issues, and backward compatibility issues. First to market and security are usually orthogonal goals and the government should enforce standards compliance in the computing industry in order to provide more secure wireless networks and devices.

5.4.7. Out of the box, non-default security

Today, many wireless access points do not have security enabled out of the box. They also use defaults for sensitive information such as the SSID and administrator password. These conditions make most access points easily exploitable. Additionally, many network cards are configured to connect to the strongest signal by default which can result in unintended associations with rogue networks occur automatically.

The government should apply pressure on manufacturers in the form of laws or liability in order to reverse the trend of disabled security by default.

A concerted, long term effort should be undertaken to educate manufacturers, standards bodies, and consumers about the need for out of the box security. As little as 2 years ago, the Chairman of the WiFi Alliance stated:

> *"Networking can still be a complicated process, and what we're trying to do first is make it as easy as possible for consumers to set up the networking. Then they can work on enabling security."*

This comment underscores the fact that many people believe security to be an afterthought. Only constant, long term education on the importance of security centric design will change this trend.

5.4.8. Seamless and automatic update technologies

Wireless protocols, encryption and authentication standards evolve due to constantly changing threat models and technologies. As such, improved technologies to enable seamless and automatic updates need to be developed in order to ensure that future wireless networks and devices can evolve with the changing security landscape.

Companies such as Microsoft should be encouraged to share their knowledge of such systems as Automatic Update[67] with the entire industry for the greater good.

5.4.9. Act on existing recommendations

In February of 2003, the National Infrastructure Advisory Council (NIAC)[68] released the National Strategy to Secure Cyberspace[69] report which contains many recommendations that address cyber security issues. These recommendations should be fully supported and acted upon by the Department of Homeland Security (DHS).

5.4.10. One international standards body for wireless security

Until one definitive standards body to oversee wireless security exists, there will be confusion and inefficiencies. Today there are numerous standards bodies such as ISO[70], ITU-T[71], IEEE[72], ETSI[73], NCITS[74], and alliances such as the WiFi Alliance[75] and WiMax Forum[76] that have some stake in wireless security.

---

[67] Microsoft update, Link
[68] The National Infrastructure Advisory Council, Link
[69] The National Strategy to Secure Cyberspace, Link
[70] International Organization for Standardization, Link
[71] International Telecommunication Union, Link
[72] Institute of Electrical and Electronics Engineers, Link
[73] European Telecommunications Standards Institute, Link
[74] International Committee for Information Technology Standards, Link
[75] The WiFi Alliance, Link.
[76] WiMax Forum, Link

Governments, under the auspices of the United Nations, should agree on designating one standards body responsible for overseeing and coordinating wireless security in an effort to minimize duplication of work.

5.4.11. Overhaul the legal system and pass laws that have real consequences

Security also depends on deterrence and current laws are either too vague or have little in the way of deterrence due to the light punishment if convicted. Furthermore, the current legal system is unprepared and inadequate to handle complex technical cases involving issues such as wireless security.

Some possible solutions are:

- Governments should encourage lawmakers to collaborate with security experts in an effort to pass laws that effectively address the issues of wireless security. Specifically, laws should be passed that do not provide a legal grey area and updates to laws should be fast-tracked by special committees so that they can keep up with technology.
- Judges that oversee such cases should be trained in the technical aspects and implications of wireless security in order to gain a better understanding of the crimes involved.
- Amend current law to account for wireless technologies.

Until more strict and less vague laws are passed, criminals will continue to exploit wireless technologies. Moreover, until a system is developed by which laws can be updated to reflect changing technology in a timely matter, legal loopholes provided by these grey areas will continue to be exploited.

6. Legal implications of wireless networks and devices.

6.1. Introduction

Technology always outpaces the law, thus producing legal grey areas. While the law rushes to catch up with technology, inconsistencies in federal, state, and local laws are inevitable which cause further confusion. WiFi technology presents interesting issues regarding what should and should not be legal, liability, negligence, and culpability. Moreover, since WiFi uses radio waves which, in certain instances, can propagate across local, state, or international borders, questions regarding jurisdiction are relevant as well. For companies that are bound to ensure compliance with laws such as the Health Insurance Portability and Accountability Act (HIPPA)[77], the Gramm-Leach Bliley Act (GLBA)[78], and the Sarbanes-Oxley Act (SOX)[79], WiFi technology introduces added complexity to an already complex threat landscape.

The current laws are wholly inadequate to address the security and privacy concerns of WiFi. Historically, applying antiquated laws to new technology issues has resulted in unintended legal consequences[80]. To fix the system, local, state, and federal governments and technology experts need to work together with the international community in order to craft new and effective laws that address the legal issues caused by wireless networks, limit unintended legal consequences and loopholes and most importantly, protect the innocent and deter criminal activity.

[77] Health Insurance Portability and Accountability Act of 1996, Link
[78] Gramm-Leach Bliley Act of 1999, Link
[79] Sarbanes-Oxley Act of 2002, Link
[80] EFF Analysis of trespass of Chattels Legal Theory, Link

6.2. Legal grey areas

New technology introduces new paradigms of social behavior and can result in unintended consequences. To mitigate these consequences, time is needed to develop new laws or apply existing laws to these issues. Until this occurs, many legal grey areas will exist.

With WiFi, some of the most important questions are related to connecting to open (non-password protected) WiFi networks without the express consent of the owner, operating open WiFi networks, accountability of operators of commercial WiFi networks, and jurisdiction when criminal activity occurs.

6.2.1. Connecting to open WiFi networks

Is connecting to an open WiFi network a crime? Although it may border on illegal, the general consensus is that in most situations, such as infrequently connecting to an open WiFi network only to obtain limited access to the Internet, you would not be prosecuted under laws such as the Computer Fraud and Abuse Act (CFAA)[81], Electronic Communications Privacy Act (ECPA)[82] or common law tort of trespass to chattels[83].

However, certain instances could be considered intentional and disruptive and would likely be prosecuted under existing laws:

- Frequent use of an open WiFi network.
- Saturating the available bandwidth of the open WiFi network.
- Accessing the open WiFi network in order to observe the data transmitted over the network (sniffing or eavesdropping).

[81] The Computer Fraud and Abuse Act of 1986, Link
[82] The Electronic Communications Privacy Act of 1986, Link
[83] Wikipedia, Tresspass to chattels, Link

- Informing other people of open WiFi networks (war driving, war chalking, and war flying results).
- Engaging in criminal activity while connected to an open WiFi network.

Although the CFAA could be used to interpret that the very act of "choosing" an open WiFi network as proof of "intentional access", it could be argued that many wireless access points use the same default SSID (such as "linksys"). Thus someone could connect to an open WiFi network by mistake. Also, the default behavior of many wireless cards is to automatically connect to the access point with the strongest signal without any user intervention. Another defense would be to argue "apparent consent" since the open WiFi network did not have any security enabled to access the network. Additionally, it could be argued that since WiFi networks operate in unlicensed radio frequencies, they belong in the public domain. Hence any unsecured WiFi network is fair game.

In rebuttal to these defense claims, Zefer[84] could be cited which says that the trespassers default status remains unauthorized in the absence of an explicit consent from the owner of the wireless network.

Although some cases are currently in the courts, there are no real legal precedents. As Neal Katyal, a professor of criminal law at Georgetown University stated in response to the legality of WiFi mooching, he responded, "Nobody really knows. It's a totally open question in the law. There are arguments on both sides"[85].

6.2.2. Operating an open WiFi network

Is operating an open WiFi network a crime? The general consensus is that as long as you do not have a premeditated plan to commit or assist in criminal activities, or you are not

[84] WiFi Liability: Potential Legal risks in Accessing and Operating Wireless Internet, Link
[85] News.com, WiFi mooching and the law, Link

in violation of your Internet Service Providers (ISP's) terms of service, then you would not be prosecuted under existing laws.

Many ISP's such as Time Warner Cable, and Verizon Online DSL state that open WiFi networks are in violation of their terms of service and constitute theft[86]. Many states such as Maryland, Delaware, Florida, and Michigan have laws that enforce these claims. In contrast, Speakeasy believes that "shared wireless networks are in keeping with our core values of disseminating knowledge, access to information and fostering community..."[87]

One of the problems of open WiFi networks is that it provides near anonymity to anyone using the wireless network. If criminal activity does occur, it would be traced back to the operator's network and the operator would bear the burden of proving their innocence. In contrast, many black hat hackers prefer operating open WiFi networks since they could cite plausible deniability if they are caught.

Additionally, the operator of an open WiFi network could be held liable for providing access that could facilitate activities that damage others. This argument is based on the precedent of *A&M Records, Inc. v. Napster, Inc.* in which the operator has the right and ability to monitor the infringing activity. However, most commercial WiFi network devices do not have these features and, even if they did, the average user would not know how to configure them correctly.

Although criminal liability is difficult to prove, the following activities would most likely constitute criminal activity[88]:

- Intentionally setting up an open WiFi network to facilitate a crime.

[86] Cable companies cracking down on WiFi, Link
[87] Speakeasy WiFi NetShare Service, Terms of Service, Link
[88] TechTarget, Could WiFi send you to jail?, Link

- Being aware that your open WiFi network is being used for questionable activities and doing nothing to stop it.

In contrast, negligence is not as difficult to prove. If a business fails to protect sensitive data as required by law then they could be held negligent under such laws as HIPPA, GLBA, and SOX.

6.2.3. Commercial WiFi Networks

It is currently unclear if commercial operators, such as T-mobile, Sprint and Starbucks could be held accountable if criminal activity occurs on their wireless networks. However, the end user usually agrees to a terms of service[89] that may indemnify the operator from any harm caused. The terms of service may also define what is considered legal activity and any deviation from this is in violation of the terms of service.

6.2.4. Jurisdiction

Radio signals, which wireless networks utilize to provide connectivity, do not recognize borders. This can complicate the question of jurisdiction in the following situations:

- An open WiFi network located in one county is accessible in a bordering county that has outlawed unsecured WiFi access
- A WiFi network in Ciudad Juarez, Mexico is utilized by someone in El Paso, Texas for criminal activity
- An open WiFi network in an embassy used by criminals operating in a sovereign nation

In order to provide clarity to this situation, local, state, and federal governments need to work together with the international community and agree who has jurisdiction.

[89] Sprint WiFi, Terms of Use, Link

6.3. Should existing law be changed?

When new technologies are introduced, they usually produce legal loopholes because existing law could not foresee their consequences. Since our legal system is based on the common law tradition of precedents, it takes time to develop precedents applicable to the new technology. New precedents should be required since applying existing precedents to decide the legality of these unforeseen consequences can result in an awkward and inconsistent legal process.

Unfortunately, with respect to cases regarding WiFi technology, the courts are attempting to apply existing laws such as CFAA, ECPA, and CAN-SPAM[90]. These laws were passed to address other issues and result in ambiguity when they are applied to WiFi cases. This ambiguity causes rulings to be based on the details of each case, which in turn produces inconsistent precedents.

To alleviate these problems, existing law must be updated in order to provide unambiguous application and consistent precedents with respect to WiFi case law.

6.3.1. The Federal Computer Fraud and Abuse Act (CFAA)

This law was enacted in 1986 and was intended to address computer hacking and should be amended in the following ways in order to address issues related to using a WiFi connection without explicit prior consent:

- Section 1030 (a)(2) should be amended to indicate that someone using a WiFi connection without explicit prior consent for criminal purposes or for any purpose that adversely affects the ability of the wireless network to function normally (i.e. saturate bandwidth) is illegal.

[90] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM), Link

- Section 1030 (a)(2) should be amended to indicate that passively viewing data transmitted over a WiFi network without explicit prior consent is illegal.
- Section 1030 (c)(2) should be amended to provide appropriate punishment to deter someone from using a WiFi connection without explicit prior consent as outlined above.

Using a WiFi network without prior consent for non-criminal activity in a way that does not adversely affect the normal operation of the network should be legal.

6.3.2. The Electronic Communications Privacy Act (ECPA)

This law was enacted in 1986 in an attempt to compensate for the shortcomings of the Federal wiretap statute in regards to modern computer transmission technologies. The main purpose of this law is to prohibit unlawful access or surveillance as well as some disclosures of electronic communication without proper procedure.

- Title 18, part I, chapter 119, section 2510 (16)(a) should be amended to add "password protected" to account for the fact that many WiFi networks support the use of passwords for access.
- Title 18, part I, chapter 119, section 2511 (2)(g) should be amended such that using a communication network without prior consent for non-criminal activity in a way that does not adversely affect the normal operation of the network is legal.
- Title 18, part I, chapter 119, section 2511 (1) should be amended to indicate that passively viewing data transmitted over a communications network without explicit prior consent is illegal.

7. Closing Words

The future of wireless networking appears to be heading in two directions. There are future standards of 802.11. The next version has already begun, referred to as 802.11n. In addition, new standards are evolving that provide much broader area coverage for wireless networks. This new standard is 802.16, commonly referred to as WiMax.

These standards are actually expected to augment each other. WiMax will provide broad area coverage. For instance: college campuses, downtown areas, rural/remote areas without cable infrastructure, etc. While the WiFi standard will continue to cover a shorter range aimed at increasing overall network bandwidth.

7.1. Communication Standards

The communication standards that are currently being worked on by their respective committees are summarized in the table below and then further discussed in the sections that follow:

	802.11n	**802.16-2004**	**802.16e**
Year Released	2006 to 2007	End of 2005	2006 to 2007
Communication Band	5GHz or 2.4GHz	3.5GHz and 5.8GHz	2.3GHz and 2.5 GHz
Bandwidth	200+Mbps	15Mbps at 5MHz channel or 35Mbps at 10MHz channel z	15Mbps at 5MHz channel
Communication Distance	100 meters	Up to 30 miles	Up to 30 miles
Channels	24-40MHz or 3-20MHz		
Compatibility	a in 5GHz/40MHz and b,g in 2.4GHz/20MHz	802.16e	802.16d
Client Mobility	Fixed	Fixed	Mobile

7.1.1. 802.11n

There is a new 802.11 standard that is underway. This standard is the 802.11n standard. It utilizes the 5GHz band, using multiple, 20-40 MHz channels simultaneously, enabling 100-200Mbps of data. This standard will replace while still remaining compatible with the 802.11a, 802.11b, and 802.11g standards. This standard is expected to be finalized in late 2006 or 2007 with devices becoming available in that time frame. This standard is designed to support the increased WLAN bandwidth required by next generation wireless applications.

7.1.2. 802.16-2004 (802.16d) WiMAX

This standard supports fixed client wireless access. This standard uses the 3.5GHz and 5.8GHz frequency bands and is expected to become certified in the end of 2005 time frame. Coverage will range from a base station to 50 kilometers with throughput of 15Mbps when using a 5MHz channel to 35Mbps when using a 10MHz channel. This standard is fully forward compatible with the 802.16e standard.

7.1.3. 802.16e WiMAX

This standard supports mobile client wireless access, in addition to fixed client wireless access. This standard is expected to use 2.3GHz and 2.5GHz bands and is expected to become certified in the 2006 to 2007 time frame. As with the fixed standard, coverage will range from a base station to 50 kilometers with throughput of 15Mbps when using a 5MHz channel to 35Mbps when using a 10MHz channel. This standard is fully backward compatible with the 802.16d standard.

7.2. Security Standards

As WiMAX is adopted, securing these communications becomes that much more imperative as the communication distance goes from 100 meters where the perimeter may be secured, to 50 kilometers, making it near impossible to secure potential receivers.

On WiMAX networks, due to their increased accessibility, security standards are very stringent. The standard requires a dedicated security processor on base stations and has a high minimum standard encryption and authentication requirement. For encryption, two standards are supported DES3 and AES (as with WPA2). All traffic is encrypted using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) with AES for transmission and data integrity. For authentication, the baseline privacy interface (BPI+) security protocol is required, using PKM-EAP (Extensible Authentication Protocol) (as with WPA/WPA2).

For WiFi networks, the improved security standard of WPA(2) helps mitigate some of the network's vulnerability, however, even using the improved WPA standards, wireless networks are still vulnerable to DOS attacks. In addition, the ever increasing prevalence of wireless devices opens up networks to an increasing number of attackers.