# Wireless Network Security

*Partha Dasgupta and Tom Boyd*
Dept. of Computer Science and Engineering
Fulton School of Engineering
Arizona State University
partha@asu.edu, tboyd@asu.edu

## Abstract

Wireless networking is inherently insecure. From jamming to eavesdropping, from man-in-the middle to spoofing, there are a variety of attack methods that can be used against the users of wireless networks. Modern wireless data networks use a variety of cryptographic techniques such as encryption and authentication to provide barriers to such infiltrations. However, much of the commonly used security precautions are woefully inadequate. They seem to detract the casual sniffer, but are unable to stop the powerful adversary. In this article, we look into the technology and the security schemes in IEEE 802.11, cellular and Bluetooth wireless transport protocols. We conclude that the only reliable security measure for such networks is one hat is based on application level security such as using a VPN.

## 1. Introduction

The use of wireless communication for data networking has been around since the early 1990's, mostly using proprietary technologies. The Aloha network in Hawaii (circa 1970) was one of the first data communication networks without wires. The emergence and acceptance of standards around 2000 has exploded the use of wireless access and currently (2004) several forms of wireless communication is widely used by the mainstream computing community. These forms include, amongst others, the IEEE 802.11 series of wireless products, various forms of data access provided by cellular providers and an emerging technology for short-range communication called Bluetooth.

The barriers to wireless communication in the early 1990's were many. Spectrum was in short supply, which was later resolved by the FCC opening up several large bands in the 2GHz and 5GHz ranges for unlicensed use. The price of producing hardware that operates at the multi-gigahertz range fell sharply due to advances in miniaturization and innovative production techniques. Even with falling prices and availability of spectrum the barrier was interoperability, that is signaling protocols and frequencies used by a manufacturer of wireless hardware was not compatible with those used by another vendor, causing customers to get "locked-in" to a particular provider. This was enough of a customer disincentive to stifle the wireless market.

Several simultaneous occurrences finally pushed wireless access to the foreground of consumer products in the 2003 time frame. These are the decline in price of laptop computers and PDAs (personal digital assistants), the perceived need and allure of untethered Internet access and the emergence of standards notably IEEE 802.11b and which allowed products from any vendor to seamlessly interact with products of other vendors.

Along with the emergence of almost ubiquitous low-cost wireless access, we are now saddled with risks, vulnerabilities and a general lack of security at the network level when wireless communications are used. This paper discusses the vulnerabilities of wireless access and presents the industry standard solutions that can in some cases correct, mitigate or at least provide some level of confidence in wireless communication.

## 2. Vulnerabilities

A vulnerability is a flaw in any hardware or software system, that is the result of either oversight or poor design, or even the basic nature of the system that can be exploited to disrupt the intended operation of the system. The disruption may be in the form of the introduction of a malfunction or the gaining of unauthorized access as well as the theft of some or part of the information stored or in transit in the system. A complete description of vulnerabilities in computer systems and network systems is not within the scope of this article.

Until around the early 1990's vulnerabilities in computing and networking systems were not well understood and were generally ignored. There was a naïve and ultimately flawed assumption that operating systems are secure and computer users are largely honest. Any miscreants that exist lacked access to adequate equipment or technical knowledge to exploit any vulnerability that may exist in computer and networking systems. The emergence of the Internet spread the reach of computer networks into the mainstream and the above flawed assumption has given rise to a painful environment of exploits, hacks, spoofs, spam and many such destructive and often expensive intrusions upon the Internet infrastructure and to the hosts that are connected to the Internet.

Today we understand the nature and cause of a large number of these vulnerabilities (and many more are discovered almost daily). Today we are vastly cognizant of the need for identifying vulnerabilities and protecting the network and computers from them.

### 2.1 Vulnerabilities in Wired Networks

In a wired network, data packets traverse from one host (sender) to another (receiver) over a collection of wires, terminated by switches, routers and gateways. In the majority of the current Internet the data travels as "cleartext" that is the data packets contain the data in native form. Anyone with physical access to the wire or the switches and routers, can physically siphon off the data and record, look and analyze the contents. In addition, the intruder may change, tamper or destroy the data. In the extreme, the intruder may simply cut the cable or disable the router.

Thus, we classify the vulnerabilities into several loose classes:

**Eavesdropping:** Anytime two (or more) computers communicate over a network the data packets can be intercepted, copied, stored or analyzed. This is a passive form of a security vulnerability that does not disrupt the communication, and is almost always undetectable but may cause leakage of data and activity information. Since every packet has source and destination addresses, the attacker can gain information about who communicates with whom and how much data is being exchanged. The content of the data is also visible if the data is sent unencrypted. Encryption converts the data into a no readable form the requires effort to reconvert to its readable form. If encryption is used properly, the contents may remain secret, but the routing and the size of communication still remains detectable.

**Man-in-the-middle (MITM):** The MITM attack is one step beyond the eavesdropping attack and is an active form of the attack. In this form, the attacker intercepts the data traveling from Alice to Bob and alters the contents, intelligently. The intruder may drop packets, replay packets, modify packets or even completely change the contents. For example, if Alice is surfing *www.cnn.com*, the intruder might keep most of the CNN site's look and feel intact, but insert spurious or false news stories. If Alice is downloading a security patch from Microsoft.com, the intruder may substitute the downloaded file, with an executable of his own, that infects Alice's computer with a virus. Some forms of MITM attacks can use even more nefarious tactics to convince Alice to part with sensitive or damaging information. The assumption in the analysis of MITM attacks is that the intruder has computers with unbounded power and ample time to attack, spoof and fool Alice for any gain or purpose. Making MITM attacks infeasible on communication networks, is one the harder problems in network security.

**Denial of Service (DoS):** The DoS attack is a generalization of a large number of different attacks, which essentially leads to one participant in a communication link unable to communicate. Cutting the wire between a client and a server is a physical DoS attack. Similarly sending a large number of fake but complex queries to a server, causing the server to spend an inordinate amount of time performing useless computations and not being able to do genuine work is a form of a host based DoS attack. In a well-designed network, attacking the network via DoS is not feasible, but the DDoS attack is a form of DoS that is quite effective on the Internet backbone (next section).

**Distributed Denial of Service (DDoS):** The DDoS attack is a variant of the DoS where the attacker floods the network fabric with traffic, causing congestion that essentially stops major parts of the network from operating properly. The Internet has many backbone links, which are links that carry rather large quantities of data between very heavily accessed sites. Saturating one or more such backbones has the effect of crippling the Internet. Such attacks are launched by first recruiting a very large number of zombies—i.e. random machines scattered around the Internet, which are programmed via a virus to become non-consensual accomplishes. Then these zombies send data to selected attack targets such that the aggregate traffic congests the Internet backbones. The DDoS attack is particularly nasty as it is almost impossible to prevent or contain and has been used very effectively to cripple the Internet.

**Buffer Overflows:** The Buffer Overflow attack is a technically sophisticated attack and exploits unknown bugs in network software to attack a victim computer. Simply put, an attacker sends a large amount of data that is non-conforming to the data format expected by the receiver. This data is crafted in some very particular and ingenious way that the receiving software, in the process of copying the data to its internal buffers, overwrites some key address elements in the stack or heap of the receiving machine. Then there is a snowball effect where the receiving computer actually starts executing some code that was part of the message it received, in effect, executable object code provided by the attacker. This object code opens up listening ports, installs backdoors and makes the victim a slave of the attacker. Due to the difficulties in designing a good Buffer Overflow attack, these are not too common, but still there have been plenty of such attacks in the past that have caused significant damage (e.g. MSBlaster) and new ones are continuously being discovered.

**Trojans, viruses and other hacks**: All of these are variants on a basic attack—download executable code to a victim computer in order to use the computer to launch other attacks, or to steal information on the victim computer. The techniques range from emailed attachments, social engineering, doctored web pages, phony advertisements and a grab bag of other tricks that form the hacker's playground. Informed and educated users can "almost always" ensure that he or she does not fall prey to these tricks. However, since the majority of the computer users of today are relatively unsophisticated, Trojans and viruses are a significant source of concern. These hacks can utilize unsuspecting victim's computers to perform DDoS attacks, generate SPAM and other misdeeds that affect the networked community as a whole.

### 2.2 Vulnerabilities in Wireless networks

Vulnerabilities that exist in wired networks also exist in wireless networks. However, due to physical limitations of access to wired networks, the attack probability is somewhat lower. Consider the typical home computer user. She connects to the Internet via an ISP using dialup, cable modem or DSL, all of which are physical connections. In each of these cases, she is using the ISP owned (or Telco owned) equipment to connect to a corporate access point. Thus, her communications into the Internet is "almost always" safe from eavesdropping and MITM attacks. Similarly, an office user is protected from random sniffing or hijacking attacks. This is not the case when wireless access is used.

The attacks on wireless networks that exploit the "over air" characteristics of the wireless signal use the abovementioned eavesdropping and MITM attacks. In addition, there is the ability to acquire unauthorized wireless access from a wireless service point. We briefly describe the techniques that can be used.

**Rogue Access Points:** The Rogue Access Point is a simple, but effective technique to steal credentials and perform a variety of attacks on a wireless network, particularly 802.11b networks. Consider a coffee shop that provides wireless service to its customers. Valid users have a username and password. An intruder, Ivan, sets up another access point near the shop with the same SSID as the coffee shop. When a customer, Alice, tries to connect to the coffee shop's network, she inadvertently connects to Ivan's network, which retrieves her username and password, and using her account logs on to the coffee shop's network and provides Internet access to Alice. However, Ivan can not only steal Alice's credentials, but can be a MITM for all customers of the coffee shop who stray into Ivan's wireless signal. From this point, Ivan can launch all kinds of MITM attacks on unsuspecting users (who will not see anything amiss) with impunity.

**Rogue Clients:** A wireless client can gain unauthorized access to a wireless network by stealing credentials, sniffing the wireless signals, cloning MAC addresses and such.

**Open Access Points:** Many wireless networks are set up as "open", that is without keys or authentication mechanisms, as this is often the factory default. For such networks, anyone with a wireless client can gain access to the Internet. Not only that, the intruder can gain access to the network (often inside a firewall) and can access data and other resources available on the network.

**WEP Key Attack:** The encryption used in WEP (Wireless Equivalence Privacy), that is the standard encryption system for 802.11b (later sections) is particularly weak and can be compromised by eveasdropping. Attacks against the WEP protocol allow intruders to gain access to the network and steal encrypted traffic.

**Jamming:** All wireless networks are prone to jamming, that is emission of radio signals in the frequencies used by the network, making communications impossible. This is a form of the Denial of Service attack, but it is easier to launch on wireless networks. Jamming is illegal, but so are most attacks.

**High Gain Antennas:** Low power wireless networks such as the 802.11b network seems to be secure from any intruder not in the vicinity. However, this has been shown not to be true. It has been demonstrated, that using high-gain antennas, an intruder can access a 802.11b network from up to 15 miles away, even though the network is designed for a maximum operational range of about 300 feet.

### 2.3 Countermeasures

Much of the countermeasures for attack avoidance on wireless networks is the same as that in wired networks. Encryption, when used properly, defeats all eavesdropping attacks. However the protocols for encryption and key exchange are often flawed and provide holes that an intruder can exploit. Digitally signed certificates, if used by the client and the server provide immunity from MITM attacks. Digital certificates are, however, not often used. Running a Virtual Private Network from the wireless client to some trusted wired internet proxy is the most secure form of wireless communication and should be used for all Internet communications (even casual web browsing). This provides guarantees to the wireless clients that data will not be stolen and MITM attacks will not be launched.

## 3. Wireless Technologies

This section will discuss the actual specifications and standards for the 802.11 family, CDMA, GPRS and Bluetooth. There are numerous vendor specific extensions to many of these standards but those extensions are not included here. We discuss the protocols, their operational properties and provide insights into the relative security of each of these technologies.

### 3.1 802.11

The IEEE 802.11 consists of a group or family of Wireless LAN (WLAN) standards. They are designed for use with wireless data access devices such as laptops and PDAs. Each member of the family builds upon the 802.11 base and is identified by a single letter suffix to the standard. This leads to an alphabet soup of protocols (802.11a, 802.11b, 802.11c, 802.11d and so on).

The 802.11 base or legacy standard set specifies the lower portion of the Data Link Layer's Medium Access Control (MAC) and the Physical Layer's (PHY) operations. Since WLAN operation requires everyone to use the same set of frequencies, the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol, which is similar to Ethernet, is used. However, there is an added problem in that the wireless stations cannot detect a collision as reliably as in a wired environment. To remedy this issue, Collision Avoidance is used. To do this the protocol defines a window of time between frame transmissions that can be used to make a determination as to the medium's usage. This space is referred to as the Interframe Space (IFS) and is defined within the basic standard with several variants that allow for simple request prioritization. The station that wishes to transmit avoids, at least initially, any potential collisions by listening for any stations that may already be transmitting. If it detects another station transmitting, it waits until the next IFS then attempts to transmit. If a collision is detected, a transmission in progress is detected or the station has just finished transmitting, then an Exponential Backoff Algorithm is used to determine when to try again.

In the lower, physical layer, there are three specifications defined for the transmission of the data, Frequency-Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS) and Infrared (IR). Most vendors choose to use the DSSS method, which uses two different "phase shift keying" or modulation approaches to achieve 1 Mbps (Differential Binary Phase Shift Keying DBPSK) or 2 Mbps (Differential Quadrature Phase Shift Keying DQPSK) data transmission rates. The data sent using these methods is first "modulated" using a specific pattern of ones and zeros referred to as the "chipping sequence".

One of the issues that arises with this standard is the usage of the 2.4GHz band. Many other devices such as microwaves and cordless phones are also using this same band. In congested areas such as a large city with a large number of closely packed and tall buildings, the signals may not be clear and there is the possibility that differing signal types and strengths may cause wireless stations to select an access point other than the desired target.

### 3.1.1 The Family of Protocols

**802.11a:** This is a recently developed standard and is beginning to appear in the market. It is specified as using the unlicensed 5 GHz band and operating at data rates of 6, 9, 12, 18, 24, 36, 48 and 54 Mbps. However, interestingly, to meet the standard, data rates of only 6, 12 and 24 are required. It introduces a new Physical Layer protocol, Orthogonal Frequency Division Multiplexing (OFDM). By using the 5GHz band, it is assumed that interference with other devices would be less of an issue. However, the tradeoff is that the signal travels less distance or attenuates more quickly than the 2.4GHz band.

OFDM uses a form of spread spectrum in that it transmits signals separated by a set of precise frequencies, alternately transmitting on these frequencies in a set order or pattern. The spacing of the frequencies and the modulation of the signal within these frequencies is what provides the "orthogonality". This approach is touted as having benefits including a high spectral efficiency, resilience to RF interference and a lower multipath interference.

**802.11b:** Most of the current wireless networks and network infrastructure is based on this standard. 802.11b uses the original 802.11 defined 2.4 GHz frequency range along with a fast DSSS encoding scheme. This standard is what the Wireless-Fidelity (Wi-Fi) Alliance has chosen as their initial standard. It uses a 1, 2, 5.5 and 11 Mbps transmission rate set. The speed of transmission selected determines the type of modulation used. The 802.11 standard uses the 11 bit Bark code to create chips, but this code does not lend itself to supporting the higher data rate of this standard. To achieve this, Complementary Code Keying (CCK) is utilized in replacement for the Barker code. CCK has 64 unique code words, so it can encode up to 6 bits in a chip rather than 1 bit per chip that 802.11 defines. Security is provided in 802.11b using WEP, which is a shared key system and is, as we will below, weak.

**802.11c/d/e/f:** These variants are essentially variants of 802.11b with some changes. The "c" variant provides procedures for network access points, the "d" variant can use other frequencies in countries where spectrum allocation is different. The "e" variant provides QoS optimizations. The "f" variant supports roaming between access points of different vendors.

**802.11g:** This is a recently ratified standard (June 2003) that is a high speed super-set of 802.11b. This standard achieves the higher data rates attributed to 802.11a only using the 2.4GHz band rather than 5GHz. This standard allows for an intermixing of both 802.11b and 802.11g stations accessing the same Access Points. The 802.11g specification allows for the specification of data rate values that exceed the defined performance specification and allowances within the software control structures and fields. So there are a number of vendor developed and available extensions to the 802.11g that utilizes these field options to allow for speeds that exceed the 802.11g specification limits.

**802.11h:** This is a supplement to the MAC layer to support European compliance with 5GHz wireless LANS.

**802.11i:** Due to the security issues identified below relating to the security of the 802.11 WLAN protocols, this standard attempts to address these problems. It adds new encryption key protocols such as Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES). 802.11i also defines additional standards such as secure IBSS, secure fast handoff and secure de-authentication and disassociation. Whereas some of the standards proposed are considered easy, software upgrades to existing products, some of these new standards will require hardware changes to support them.

### 3.2 GPRS

General Packet Radio Service (GPRS) is a standard for a value added service to be used with the cellular telephone infrastructure using GSM and TDMA. It augments the voice capability of cellular phones, providing digital wireless communication data rates of up to 171.2 kbps theoretically and 114 kbps practically. GPRS works by using a Gateway GPRS Support Node (GGSN) to interface to other networks such as the Internet. The mobile device communicates with a Serving GPRS Support Node (SGSN). The GGSN and SGSN work together to maintain the virtual connections and to deliver the data. The SGSN acts to maintain an attached state for the mobile device as it moves through the network.

Though GPRS seems to provide a good match for other packet based backbones, it also brings with it a few downsides. One of the issues is that GPRS must share the bandwidth with the GSM/TDMA voice channel. This means the data and voice transmissions interfere with each other (quality and bandwidth tradeoffs occur). There is no inherently defined security protocol built into the GPRS standards, so other existing protocols must be used. For example, in order to securely send data between two GPRS stations over the Internet, Virtual Private Network (VPN) could be employed at the higher layers to provide data encryption at the very least.

### 3.3 CDMA

After the success of digital cellular systems such as GSM in most parts of the world and TDMA in the US, Qualcomm developed a competing standard, the Code Division Multiple Access (CDMA) protocol. This original definition is currently also known as cdmaOne and is defined as the IS-95B standard. CDMA works by transmitting a digitally encoded analog signal using spread-spectrum technology combined with a special coding scheme over a 1.25 MHz channel. It encodes the data using a set of 64 bit Walsh Codes. In theory at least, up to 64 users could use the same channel. The coding used in CDMA is used at the wireless transmission level and making it difficult for a receiver, not having the correct code, to even receive any intelligible signal (the signal is equivalent to noise).

### 3.4 Bluetooth

Bluetooth is a standard that describes a short range wireless link between devices. The maximum link distance is about 10 meters (33 feet). The transmitter operates on the 2.4GHz

ISM band and uses a fast acknowledgement frequency hopping which improves the robustness of the signal in a noisy frequency environment. The technology changes hops (changes frequency) faster or more frequently due in part to its use of smaller data packets than any other device that uses the band such as 802.11b. Since it also uses less power for its transmissions, it also is intended for the Bluetooth units to be relatively close to each other. Bluetooth is intended for use as a communications link between small potentially cheap devices. It is not intended for both mobility and distance. It has a data rate of between 300-400 kbps. That is to say a mouse can communicate with a PC or some other mouse driven devices, wirelessly.

## 4. Security in 802.11

Wireless LANs are significantly less secure than wired LANs. Signals can be more easily captured from a number of stations by the simple choice of capture location. In order to prevent this type of data capture from being successful, the wireless LAN standards have included a set of protocols and facilities. However, like anything new and interesting, it turns out that the initial protocols were not as robust in performing their task as was to be hoped.

### 4.1 SSID, WEP and WPA

Optionally, security for 802.11, 802.11a, b and g was initially defined to be based on the use of the Service Set Identifier (SSID) and the Wired Equivalent Protocol (WEP) to provide for both authentication and privacy through the encryption of data over the radio waves. Each wireless LAN has the option of specifying a SSID that can be exchanged at the initiation of communication between a system and an Access Point. The SSID in use must be the same between both sides before further communications can commence. Unfortunately, this exchange is in clear text, so it is relatively easy to capture the SSID of the network thus rendering the SSID to little more than a convenient label for the Access Point.

WEP is a key based security protocol intended to prevent "casual eavesdropping" of the data being transmitted over the wireless network. The key is used to encrypt/decrypt the data portion of a packet. The key that is defined in the original standards is a single 40-bit key although larger keys, up to 128 bits, are defined by a follow on standard often referred to as WEP2. The key is defined at and for each of the stations that communicate over the wireless LAN. The entire key is never exchanged over the wireless network, so it is not directly captured. In principle, the WEP methodology is strong, however, the implementation is flawed and allows the key to be determined relatively easily. Another problem with the WEP approach is that it is a shared key, shared by all users of the network, and hence the key is subject to be leaked manually.

The WEP key generation is based on the RC4 stream cipher algorithm. The algorithm depends upon a permutation of all the possible n bit words, a pair of indices and the initial value of a variable key. RC4 defines the output of a Key Scheduling Algorithm (KSA) which uses the variable key as input to drive the subsequent permutations of the algorithm. As it turns out, the keys used for this initial value, can be based on a series of "weak" keys, which are keys that for a small number of bits, the remaining bits can be easily generated given the original key generation methodology. This makes generating certain keys easy to do in a short period. Since time is a code breakers enemy, any reduction in time improves the ability to break into the key and data [1].

The second WEP key vulnerability is the ability to analyze the exposed or available portion of the encryption key, the initialization vector (IV), and data portion of the packet to determine a pattern that an attacker can readily use to generate the unseen or private portion of the key. This weakness relates to analyzing the exposed data, a pattern can be spotted that can be concatenated with a guess about the secret part and provide a relatively quick and small set of choices to try and guess the key.

This WEP weakness has been well documented and exploited. In general, in an environment with large quantities of data in the air, all of the keys can be captured with in a matter of a few hours. In a home network, with little or small bursts of airborne data, the time to capture the key is significantly longer, but still relatively easy. Larger key sized tend to increase the key cracking time, but in most cases this appears to only be on the order of twice or less the time required to derive the 40 bit key.

To resolve this security issue, a new replacement standard was developed called WiFi Protected Access (WPA). This was developed as a cooperative effort between the WiFi Alliance and the IEEE. This standard is derived from the 802.11i standard and is considered to be "forward compatible" with this standard. WPA is a software replacement for the WEP standard, so no hardware changes are required. It replaces the existing key operation with the Temporal Key Integrity Protocol (TKIP), which is defined in the 802.11i standard. Specifically WPA improves encryption by including a per packet key mixing function, a message integrity check (MIC), an extended initialization vector (IV) with sequencing rules and a re-keying mechanism. It is believed that these changes will address the WEP weaknesses.

### 4.2 802.1X

The IEEE appears to recognize that the security standards introduced in the original and subsequent 802.11 standards were not as robust as they should be for an effective deployment. To this end, working committees have been formed to propose a variety of extensions, enhancements and replacements. In addition to the work on the 802.11i standards, there is a Robust Security Network (RSN) proposal, focused on a long-term solution to the 802.11 problems, referred to as 802.1X.

RSN provide security by adding a third party, authentication server service to the authentication process. The way this works is that the station, referred to as the Supplicant, that wishes to connect to the network by way of the Access Point, referred to as the Authenticator, makes a connection request. The Authenticator then contacts an Authentication Server, usually a RADIUS type server, which either validates or rejects the request. The Extensible Authentication Protocol (EAP) is used to make the authentication request. In this way a high degree of secure, flexibility exists as to the actual service that can be deployed. EAP is considered to be secure in that is a *challenge-response* model.

Like in all new protocol proposals, Mishra and Arbaugh [2] believe that they have identified weaknesses that allow for both a Man-In-Middle attack and to allow a Session Hijacking to occur. The first attack focuses on the relationship between the Authenticator and the Authenticating Server. No explicit mutual authentication is specified in the standard and thus someone sitting between these two entities could gain access and assume either role. The second attack relies on the wireless operational environment and the ability for an attacker to use certain management frames to change the Supplicants and Authenticators connection to a different Supplicant while remaining in an Authenticated state. Proposals are made by Mishra et.al. as how to correct this issue. In addition, Cisco makes proposals for how to resolve these security problems [3]. This dialogue is not complete, however but when it is, it normally results in a much stronger standard.

### 4.3 MAC Filtering

Another approach to resolving the issues with WEP security is to use a list of valid MAC addresses (also known as a White List) at the Access Point control access. If your MAC address is not listed on the Access Point you are not granted access. This sounds good in theory, but in actuality, valid or acceptable MACs can be capture or sniffed using standard wireless cards and software. Once this information is obtained, it is relatively easy for the wireless card to be set to use the valid MAC. Once this occurs, the Access Point is no longer involved with the network security.

The converse of the White List is the Black List, which is a list of those who can not access the network is kept. This approach suffers from the same type of attack as that of the White List. All this is required is a valid or Access Point acceptable MAC address. This can be obtained using the same tools and procedure as that of the White List. Once a valid MAC is obtained it the attacker simply changes the MAC address of his station's card and then gains access to the network by way of the Access Point.

### 4.4 Virtual Private Networks

VPN can be employed over the WLAN to provide the data level encryption and end to end authentication depending upon what services are provide at the wired network side. The use of VPN can be used to augment the existing protocols such as WEP and WPA and can be used in lieu of the availability of the 802.11i or 802.1X standards. VPN uses IPsec with encryption and L2TP inside of IPsec. The VPN environment is considered by most to be very secure and a variety of standard are being codified in support of a more widespread interoperability. There are no defined vulnerabilities with VPN. Most of the problems arise with either vendor implementations or access to data and security information from either end of the VPN connection. This latter problem exists in any setting and certainly is not solvable through the usage of VPN.

## 5. Security in Cellular networks

The security of cellular networks has been studied, but not as rigorously as other forms of wireless networks. This is because, today the usage of cellular networks for critical data transmission has not been popular. Cellular networks are used for small messages, quick web browsing and sending pictures. Hackers have not been interested in eavesdropping on such activities. Thus much of what is known of these vulnerabilities (or lack thereof) is somewhat speculative.

The security of GPRS networks depend upon the A3, A5 and A8 algorithms used by the GSM system to authenticate the user and the base station and to cipher all data and voice traffic between them. While on the surface GPRS seems to be secure many security holes have been discovered. The smartcard used in the GSM system uses an authentication system in which a challenge response is performed with the mobile units ESN (electronic serial number). The encoding used in this challenge response scheme has been shown to be vulnerable and smartcards can be thus cloned.

The A5 cipher is used to encrypt all the data communications. Researchers believe that A5 is not as strong as its 114 bit key length but can be broken using hardware based cryptanalysis. However, such attacks are not prevalent as the importance of user data transmitted by GPRS networks is still quite small.

The CDMA systems are believed to be more secure than the GPRS network, mainly due to the nature of the radio frequency signaling. While it is possible to listen in on a GPRS transmission using TDMA receivers, such is not possible with CDMA. A CDMA receiver has to be coded with the correct 64-bit code to receive a channel of CDMA traffic, and without this code, or with a wrong code, the received signal is noise. A brute force attack to find a correct code is not feasible. The code is exchanged between the sender and the receiver at the handshake, which happens over an encrypted channel.

IN spite of the difficulty in "tuning" into a CDMA transmission, the data (or voice) transmission is further encrypted. This double layer of ciphering makes CDMA security, possibly quite strong.

All cellular networks are however vulnerable to location finding by triangulation or directional antennas. That is, an attacker can find the location of a mobile station with the use of radio monitoring equipment. This does not compromise the privacy of the data, but the privacy of the operators location.

## 6. Security in Bluetooth

There are four entities in Bluetooth devices that are used to maintain link level security. The first is the Bluetooth device address, which is a 48-bit value, unique to each Bluetooth device and defined by IEEE. The second is a private authentication key, which is a 128 bit random number. Thirdly, there is an 8 to 128-bit private encryption key. Lastly is a pseudo randomly generated, 128-bit number that the device generates. These entities are used to one degree or another depending upon the mode of security level setting (mode) of the Bluetooth device.

The choices for Modes are 1 to 3; where Mode 1 is the non-secure mode, Mode 2 is "service level enforced" and Mode 3 is "link level enforced". Mode 3 security begins the security prior to a communications channel being established. Devices can also be tagged as trusted and untrusted with service levels tat include requiring both authorization and authentication, authentication only and open to all.

The vulnerabilities of Bluetooth security mechanisms are have not yet been thoroughly investigated. Since the market penetration of Bluetooth is yet low, these devices have not been subject to severe scrutiny. Hence, the security level provided by the native mechanisms built into Bluetooth is unknown.

## 7. Conclusions

As wireless devices are gaining popularity, their built in security systems are beginning to show definable and exploitable weaknesses. The 802.11b and WEP scheme is the most popular and the most maligned due to its inadvertently poor design. Other systems are most probably better or else their weaknesses are not yet discovered.

All wireless (and wired) systems are capable of supporting application level security methods such as VPN, SSL, SSH and so on. Conventional wisdom states that the security provided by these higher level protocols is much superior. Baring implementation flaws, these protocols provide as close to guaranteed security as we can achieve today. Since the underlying transport level security does not affect the security of VPN-like protocols, they can be safely used over insecure wireless networks.

## 8. References

[1] Weaknesses in the Key Scheduling Algorithm of RC4, Scott R, Fluher, Itsik Mantin, Adi Shamir, Lecture Notes in Computer Science, Revised Papers from the 8th Annual Internation Workshop on Selected Areas in Cryptography, Springer-Verlag, 2001, ISBN 3-540-43066-0

[2] “An Initial Security Analysis of the IEEE 802.1X Standard", with William A. Arbaugh, Technical Report, University of Maryland, Department of Computer Science CS-TR-4328, UMIACS-TR-2002-10, Feburary 2001

[3] http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1680_pp.htm, Accessed February 29, 2004, Posted Thu Aug 22 06:32:08 PDT 2002, Cisco Systems, Inc.