Information Technology and Operations Center

Department of Electrical Engineering and Computer Science

United States Military Academy

West Point, New York 10996

TECHNICAL REPORT

ITOC-TR-2003-101

A Survey of 802.11a Wireless Security Threats and Security Mechanisms

A Technical Report to the

Army G6

Investigators

Colonel Donald J. Welch, Ph.D.

Major Scott D. Lathrop

Directed By

Colonel Donald J. Welch, Ph.D.

Approved by

Executive Summary

High bandwidth wireless local area networks are gaining popularity. Along with this popularity has come a well publicized series of vulnerabilities in the IEEE standard implementations. In response, a number of standards from wired networking (e.g. 802.1x and IPsec) are being adopted to wireless. Vendors are also developing and selling proprietary security solutions. The normal security risk assessment/risk mitigation process can be complicated by a misunderstanding of the range of available options and the strengths and weaknesses of each. However, the nature of wireless technology raises the stakes in performing a proper risk assessment and deploying a wireless network that meets local security requirements.

This white paper first describes taxonomy of wireless LAN attack techniques. We then describe the generic mechanisms available for authentication of users and the protection of the privacy and integrity of the data. We conduct a basic analysis of each security countermeasure by looking at the attack techniques addressed by the mechanism. Our analysis takes into account the perspective of both insiders and outsiders. We conclude by stating our recommendations for WLANs. These recommendations include:

- Mutual Authentication
- Layer two encrypted tunnel
- Strong cryptographic integrity verification

Without these features, not only is a WLAN vulnerable, but the entire information infrastructure of which it is a part is at risk. We also recommend per-packet authentication although we would not go so far as to make it a requirement.

1. Introduction

Wireless Local Area Networks (WLAN) are increasing in popularity. They are being installed by businesses of all types, educational institutions, governments and the military. The reason is that WLANs provide users the access to their information in many locations, some of which are more conducive to collaboration. Furthermore, the concepts and technical challenges associated with the department of defense's (DoD) transition from industrial-age to network-centric warfare are highly dependent and revolve around the successful implementation of a secure, wireless network of systems. The freedom and mobility that WLANs promise also present some serious security challenges.

WLANs are not limited by network jacks nor are they limited by geography. WLANs provide unprecedented flexibility in that an area not originally intended as a collaborative workspace can accommodate a large number of wireless clients. Auditoriums now accommodate hundreds of networked computers just by plugging a few Wireless Access Points (WAPs) into the network. The radio waves used for WLAN propagate quite well. The advertised ranges for wireless network interface cards range up to 300 feet. In reality, 802.11b networks can be accessed over one-half mile away in an urban environment. [Ell02]

By most estimates a significant portion of these networks have no security mechanisms whatsoever. [Ell02] According to Ellison's informal study of four U.S. cities only 38% of the wireless LANs that they could find while merely driving on public highways had the default standard security mechanism called Wired Equivalent Privacy (WEP) enabled. WEP provides very little effective security, and this figure shows that most administrators are not even attempting to secure their WLAN let alone succeeding. Insecure WLANs are not just a problem for WLAN users, but through Address Resolution Protocol (ARP) attacks, every system on the same side of the router as the WLAN in an organization's network is vulnerable to attack.

The military and education domains are no exception. Here at the United States Military Academy (USMA), a high-bandwidth secure wireless network is a key component of our vision for educating and developing leaders. We believe that the best environment for learning is an information rich environment. Hence our vision is to convert ever learning space at West Point into an information-rich environment through portable computers and wireless networks. The use of the network in the classroom facilitates active learning. The professor can act more as a mentor than a lecturer as the student thinks more deeply about problems during active learning activities. USMA has a rich and robust information infrastructure that the cadets and faculty currently use in computer laboratories, offices and the barracks. With a WLAN, every classroom, study hall and laboratory will in effect become an information-rich, computer laboratory. This will provide the Army with officers better able to lead and meet the challenges of a changing technological, social, political and economic world.

At USMA we are dedicated to providing a secure high-speed WLAN that does not pose a greater risk to our information than the current, completely wired network. To do so we have conducted a study of the available WLAN security technology. This white paper is a summary of that work and should be useful to those planning a secure WLAN implementation.

We have addressed known security threats to IEEE 802.11 networks focusing specifically on 802.11a because that is the standard we are implementing. However, the difference between 802.11a and other protocols in the 802.11 family is trivial with respect to security. 802.11 WLANs all use the same layer 2 packets; the difference is in the physical layer. 802.11a uses a higher frequency than 802.11b or 802.11g. This higher frequency means that the radio transmission will not travel as far and will not propagate through solid objects as well the low frequency standard. This tends to help limit eavesdropping, but in no way eliminates the threat. Also 802.11a has about 5 times the bandwidth that 802.11b does. This higher bandwidth means that attacks that require data collection can be executed faster on an 802.11a WLAN than on an 802.11b WLAN.

To limit the scope of this paper we have decided to choose representative techniques rather than try and assemble and discuss a complete list of WLAN attacks. Specific attacks are normally focused on vulnerabilities that are design and implementation specific. However, there are classes of attack techniques that apply across different technologies. Through our choices we hope to achieve a fair comparison of the different WLAN security technologies. We will also not discuss attacks that are either stopped or defeated by the technologies we discuss in this paper. Our discussion of the threats can be found in Section 2.

We look at the threat from two points of view: the insider and the outsider. The outsider has access to the wireless network and the software and hardware that can be purchased or otherwise obtained publicly. The insider is a valid user of the wireless network whose goal is to obtain access to information which she would not otherwise be entitled. The insider has valid software/hardware/certificates for both the wired network and WLAN.

We then discuss the generic security technologies. What the technologies are, how they work, the types of attacks they protect against, and those attacks to which they are vulnerable. Generally, each security product employs security technologies to authenticate a network session, to protect the confidentiality of the session, and to insure information integrity. The products on the market mix and match these techniques so we have found it useful to examine them separately.

The goal of this paper is not to determine “the best” wireless security architecture but to provide information for the Information Assurance (IA) planner to use while designing a WLAN. IA planners must inventory their information assets and determine the motivation, capabilities, and resources of the adversaries that threaten their information. Planners can then begin a risk assessment and develop their risk mitigation strategies. This paper will help planners develop courses of action using various security architectures and write policies from those strategies by providing information about the theoretical effectiveness of the technologies. This paper does not replace the extensive risk analysis IA planners must perform.

2. Threats

In this section we describe eight attack techniques that we use to compare the security technologies available. We chose these attack techniques to be generic enough so that they can be used to evaluate representative security technologies. We also strove to make them complete, in that any well-known attack can be decomposed and the components can all be classified into one of these attack techniques.

A complete information assurance risk assessment requires a focus on the threats against the three key components of assuring information. That is, the information system should protect against confidentiality, integrity, and availability (CIA) attacks. We chose not to discuss attacks on the WLAN availability, otherwise known as denial of service attacks. Denial of Service attacks against layer 1 or layer 2 cannot be defeated by any of the security technologies that we are analyzing. However, this is a serious consideration in any type of future tactical system’s employment of a wireless network.

We start by examining attacks against the confidentiality of communication on the network. We then move into those attacks that actually alter the network traffic, hence destroying the integrity of the information on the network. When looking at confidentiality attacks we start with the least intrusive and work towards more intrusive attacks.

Of the eight attack techniques in our taxonomy, four violate just the confidentiality or privacy of the session: traffic analysis, passive eavesdropping, active eavesdropping with partial known plaintext, and active eavesdropping with known plaintext. One technique can be used to violate confidentiality and/or integrity -- the man-in-the-middle attack. Three attack techniques violate the integrity of the network traffic: unauthorized access, session high jacking, and the replay attack.

The integrity attack techniques generally require successful use of one or more of the confidentiality attack techniques in order to meet the necessary preconditions of these attacks.

2.1.Traffic Analysis

Traffic analysis is a simple technique whereby the attacker can determine the load on the communication medium by the number and size of packets being transmitted. The attacker only needs a wireless card operating in promiscuous (i.e listening) mode and software to count the number and size of the packets being transmitted. A simple yagi or helical directional antenna provides an increased range at which the attacker may analyze traffic. A yagi antenna is a simple directional antenna consisting of a horizontal conductor with several insulated dipoles parallel to and in the plane of the conductor. We have shown that making a simple yagi antenna out of a “Pringles” can, a steel rod, and some washers, an attacker may double the range at which they are receiving transmissions. A helical, or spiral antenna, built for less than $100 out of PVC plumbing pipe and copper wire, increases the range by more than double the original distance. [Leo02]

Traffic analysis allows the attacker to obtain three forms of information. The attack primarily identifies that there is activity on the network. Similar to standard radio communications, a significant increase in the amount of network activity serves as an indicator for the occurrence of a large event.

The identification and physical location of wireless access points (APs) in the surrounding area is a second form of information acquired from traffic analysis. Unless explicitly turned off, access points broadcast their Service Set Identifiers (SSIDs) in order to identify themselves to wireless nodes desiring access to the network (see also section 3.1.2). The SSID is a parameter that must be configured in the wireless card's driver software for any wireless station desiring access to a wireless LAN. By broadcasting this information, access points allow anyone to identify in their area to identify them with simple locator software.

If a directional antenna is used along with a Global Positioning System (GPS), an attacker may know not only that there is an AP(s) in the area, but may also obtain the physical location of the access point or the center of the wireless network. From a military standpoint, this is the same technique used in triangulating radio communications or field artillery batteries for the purpose of counterfire.

The third piece of information that an attacker may learn of through traffic analysis is the type of protocols being used in the transmissions. This knowledge is obtained based on the size and the number of packets in transmission over a period of time. A simple example of this attack is the analysis of a Transmission Control Protocol (TCP) three-way handshake. TCP synchronizes the communication between two end nodes by transmitting a series of three packets. The sender transmits a synchronize (SYN) packet to let the receiver know it wants to communicate, to provide it with the sender's initial sequence number, and to pass other parameters used in the protocol. The receiver then replies with its initial sequence number an acknowledgement of the original sender's sequence number (SYNACK). Finally, the original sender transmits an acknowledgement of the receiver's initial sequence number (ACK) and then the transmission of application data between the two nodes may commence. Each packet used in the three way handshake is a fixed size in terms of the number of bytes transmitted. Based on the relatively small, easily identifiable size of a SYN/SYNACK/ACK packet sequence followed by a sequence of several large packets would serve as an indicator that the network stations are communicating using TCP/IP as their underlying protocol. This information can then be used further to assist in carrying out attacks that exploit the knowledge of TCP/IP header information. Such attacks are described later.

2.2. Passive Eavesdropping

In this attack the attacker passively monitors the wireless session (Figure 1). The only precondition is that the attacker has access to the transmission. As described previously, we have hypothesized that a directional antenna can detect 802.11 transmissions under the right conditions miles away. Therefore this is an attack that cannot easily be stopped by using physical security measures.

One would believe that wireless network users would configure their wireless access points to include some form of encryption; however, studies have shown that less than half of the wireless access points in use even have the vulnerable 802.11 wireless security standard, the wired equivalent privacy (WEP) protocol, properly configured and running. [Ell02]

Assuming that the session is not encrypted, the attacker can gain two types of information from passive eavesdropping. The attacker can read the data transmitted in the session and can also gather information indirectly by examining the packets in the session, specifically their source, destination, size, number, and time of transmission. The impact of this type of attack is not just based on the importance of the privacy of the information. The information gleaned from this attack is an important precondition for other, more damaging attacks.

If the session is encrypted at layer 2 or higher using a protocol such as WEP or the Advanced Encryption Standard (AES), then in order to read the data the attacker has to decrypt the packets. [Fra01][Moi00][Bor01][ISS][Ell02][Chi][Col02a][Col02b] In our analysis of security mechanisms described later in the paper, we look at the effect of the encryption and not the particular mechanism to help compare across different technologies.

There is a lot of documentation and negative press describing the vulnerabilities associated with the WEP protocol [Arb01] [Bar02] [Bor01] [Bor02] [Wal00]. Because of the finite number of initialization vector (IV) sequences, WEP's reuse of the IV makes it susceptible to attack. We believe that AES implementation is a much stronger form of encryption at layer 2 and that there is currently no practical method of cracking it; therefore, we will focus our eavesdropping category of attacks on the WEP protocol.

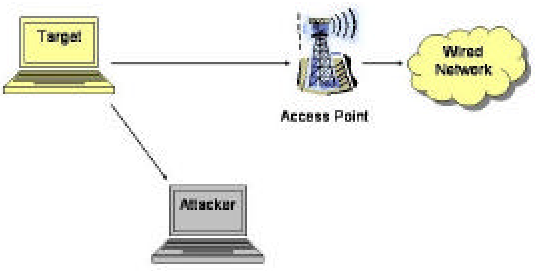

Figure 1 Illustration of passive eavesdropping. The attacker simply listens in on the radio broadcasts of the target and wireless LAN.

WEP was designed to insure the confidentiality of the data at the network layer (layer 3 of the OSI model) and higher layers, but it is inadequate because it uses an encryption algorithm ill-suited for the wireless domain. WEP uses the RC-4 encryption algorithm that has a key size of 40 or 128 bits (104 in actual vendor implementation). The problem with WEP, however, is not the size of the key; it is the fact that the initialization vector's (IV) address space is too small. The IV is the "seed" that generates a unique key stream for every packet generated. Together the IV and the 40 or 128 bit key are inputs to the RC4 algorithm. The algorithm's output is the key stream used to encrypt the original data using a basic XOR function (Figure 2). Mathematically this can be represented as

$$C = P \oplus RC4(IV, k)$$

where P is the plaintext, C is the resulting ciphertext, *k* is the static WEP key, and *IV* is the public initialization vector.

Figure 3 shows what portion of a packet is encrypted when WEP is applied prior to the transmission. Since it is a layer 2 encryption method, the IP headers, TCP headers, and application data (in this case an email message) are encrypted. Notice that the IV, along with other information in the 802.11 header, such as the source and destination MAC addressees are transmitted in the clear. The reason why the IV is transmitted in the clear is because the receiving node must know that piece of information in order to decrypt the received packet. Mathematically, the receiving end must determine (*plaintext*, *P*) where

$$P = C \oplus RC4(IV, k)$$

In this case the shared secret or private key is K--the WEP encryption key.

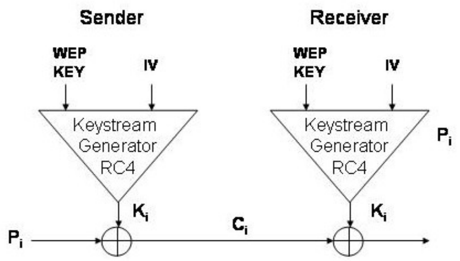

Figure 2 Illustration of the RC4 process used to create an encrypted message at the sender node and a decrypted message at the receiving node. The plaintext is encrypted using the key stream, K. The key stream is created from the static WEP key and the initialization vector. The encrypted message is decrypted using the same key stream used to encrypt the message. The receiver creates this key stream the same way the sender did, by using the static WEP key and IV. The result is the original plaintext message.

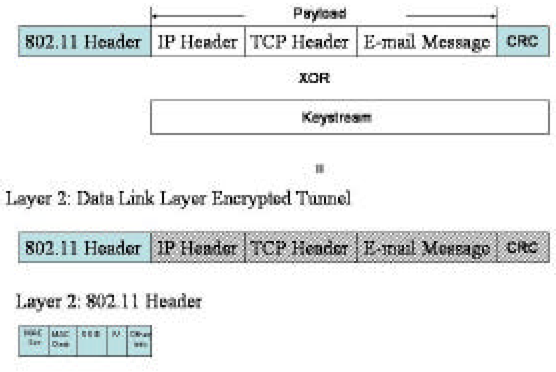

Figure 3 The construction of a wireless network packet and the layer 2 tunnel used in WEP. The payload and the checksum are encrypted while the 802.11 header is not. 802.11a and 802.11b headers are identical. The 802.11 header contains the IV in plaintext.

The encryption is very difficult to break as long as a different IV is used per packet. The problem arises in that the IV is only 24 bits yielding $2^{24} = 16,777,216$ unique key streams. Table 1 shows the results of turning on a network monitoring tool, and passively “sniffing” packets on a wireless network. The table shows that within a 10 minute period, an average of 11,362 packets is being generated between one laptop and an 802.11b wireless access point. This translates into an average of 19 packets being transmitted per second. Calculated in days, it would theoretically take approximately 10 days to exhaust the address space before IV reuse would occur. Practically, however, the amount of time is drastically reduced when one takes into account the generation of more packets through the use of application software (i.e. web browser or email client), the use of the 802.11a protocol (which has five times higher bandwidth), more than one user accessing the wireless network, the birthday paradox, and the fact that most vendors implementation of the IV starts the number at either 0 or some fixed constant rather than at a random number. [Bar02] [Wal00]

The birthday paradox states that when there are a group of 23 people in a room, there is greater than a 50% chance that two or more people have the same birthday. The percentage increases to 97% when there are 50 people in a room and increases to almost 100% when there are 100 people in the room. [Ros98]

Applying the birthday paradox to the wireless realm, where the number of people in the room equates to the number of packets transmitted, indicates that there is a 50% chance of collision among IVs after only 4823 frames (approximately four minutes) and a 99% chance of duplicate IVs with 12,430 frames (approximately 11 minutes). It is safe to say that within 10 minutes an attacker could capture enough packets to see re-used IVs.

Layer 4 Protocol Type	Number of Packets Generated
TCP	7637
UDP	1459
OTHER	2266
TOTAL	11362
AVG PACKETS/Sec	~19

Table 1 Number of packets captured from a wireless network interface card (NIC) within a 10 minute period.

A viable technique for an attacker to passively eavesdrop against WEP is to gather several packets through sniffing software in order to capture duplicate IVs and then exploit the fact that all TCP/IP packets have known information in their headers at fixed locations. For example, the IP header always has a source and destination IP address at a fixed length from the start of the packet. TCP header information, such as the source and destination ports, is similar. Application level header information (i.e. Email header information) is also located within the packet at a fixed interval from the start. Therefore, given known plaintext and the IV the attacker can infer the key stream sequence for specific portions of the packet. They can then build a database of (IV, key stream) pairs that allow them to decipher portions and/or modify any future packets given an IV.

As a simple example, lets assume that the IP address is a four-bit number (0000 – 1111). Based on previous reconnaissance of the internal network, lets assume that the attacker knows that IP address 0001 is a heavily visited machine (perhaps a domain controller, web server, or Email server). The attacker eavesdrops on the wireless connection and sniffs a packet with an encrypted field of 1011 at the same location in the packet where the IP address is stored. Given this information, the attacker can infer that for the given IV, the key stream sequence for the IP portion of the packet is $P \oplus C = K$ or $0001 \oplus 1011 = 1010$. Now for any other packet transmitted using this IV we can decipher the IP address because we have the keystream (1010) for that segment of the packet.

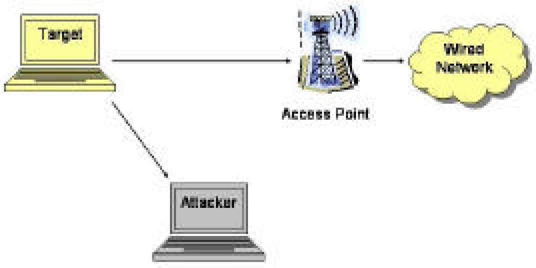

Figure 4 Illustration of passive eavesdropping. The attacker simpl y listens in on the radio broadcasts of the target and wireless LAN.

In another attack using passive eavesdropping, the attacker can simply exploit the 802.11 authentication protocol. The 802.11 authentication protocol uses a standard challenge/response sequence. First, a wireless client desiring access sends a message to the access point informing it that it desires access to the wireless network. The access point replies with a frame containing a random 128 byte frame representing the *challenge*. This challenge is not encrypted. The wireless device then encrypts the challenge using WEP and sends the encrypted challenge as its *response* to the access point. The access point decrypts the response and verifies that it matches the initial challenge. If the response matches the challenge then the process is reversed and the access point authenticates itself to the wireless client in order to provide mutual authentication. [Arb01]

In order to successfully attack this protocol, the attacker first captures the unencrypted challenge and the WEP encrypted response. Because the attacker knows the unencrypted random challenge, the WEP encrypted challenge, and the public IV used to encrypt the challenge, the attacker can derive the key stream produced by WEP using the associated IV. That is,

$$RC4(IV, k) = C \oplus P$$

Using the key stream, RC4(IV, k) associated with that particular IV, the attacker now has all of the information necessary to authenticate to the wireless access point without having to know the shared WEP key, k. [Arb01]

The final passive attack against the WEP protocol requires simply eavesdropping and building a database of $(IV, C_1 \oplus C_2)$ pairs. Given any two messages encrypted with same key stream, you can determine the XOR of those two messages. The attacker can then use techniques such as frequency analysis and dragging cribs to recover both original messages. [Sin00] The more packets using the same key stream, the easier it is to decrypt all the packets using that key stream.

2.3. Active Eavesdropping with Partially Known Plaintext

In this attack the attacker monitors the wireless session as described in passive eavesdropping (Figure 1). Unlike passive eavesdropping, however, during active eavesdropping, the attacker not only listens to the wireless connection, but also actively injects messages into the communication medium in order to assist them in determining the contents of messages. The preconditions for this attack are that the attacker has access to the transmission and has access to partially known plaintext such as a destination IP address.

Since WEP uses a cyclic redundancy check (CRC) to verify the integrity of the data in the packet, an attacker can modify messages (even in encrypted form) so that changing data in the packet (i.e. the destination IP address or destination TCP port) cannot be detected. The attacker's only requirement is to determine the bit difference between the data they want to inject and the original data.

An example of active eavesdropping with partially known plaintext is *IP Spoofing*. The attacker changes the destination IP address of the packet to the IP address of a host he or she controls. In the case of a modified packet, the authentic receiving node will request a resend of the packet and so the attack will not be apparent. Another approach is to resend the packet with the modified header. Since the receiver judges whether a packet is valid, the resend should not cause any response from the access point or access controller which kindly decrypts the packet before sending it to the attack receiver, thus violating the confidentiality of the communication (Figure 5).

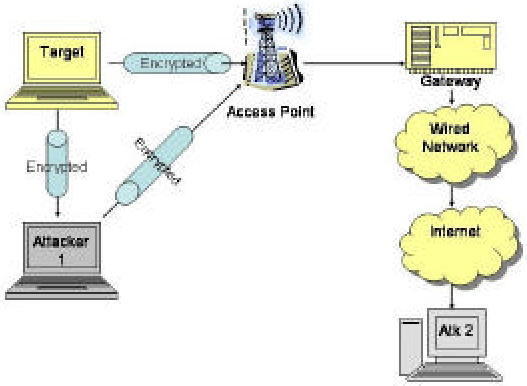

Figure 5 IP Spoofing. In this attack, Attacker 1 intercepts and modifies the packets in the message. Attacker 1 changes the destination IP address and nothing else. The packets then continue through the access point and to the gateway where they are decrypted. The plaintext packets then continue to the Atk 2 machine where they are collected and read by the attacker.

Expanding our example from the previous section, let's assume the attacker controls a machine at IP address 1111 (again, assuming four-bit IP addresses for simplicity). This machine could be anywhere in the world, not necessarily within the geographic vicinity of the wireless access point. The attacker's desired end state is to decrypt the WEP encrypted message by sending it through the wireless access point (which kindly decrypts the WEP encrypted message) to a pre-determined IP address controlled by the attacker. The original sender of the message never knows that their messages are being recreated and sent to another machine for analysis.

Through eavesdropping, the attacker captures a packet containing a previously recorded (IV, key stream) pair and WEP encrypted cipher text of 1011 located in the IP destination field. Using the previously recorded key stream for this IV (1010), the attacker can infer the packet's destination IP address as being 1011 XOR 1010 = 0001. The attacker can then send the same message to her target machine (IP address 1111) by simply modifying the original message through XOR math. Mathematically, the attacker XOR the desired destination IP address with the key stream for this IV to get the encrypted IP address (0101).

$$IP_{spoofed} \oplus keystream = encrypted_{spoofedIP}$$

$$1111 \oplus 1010 = 0101$$

Because the CRC is a linear function of the message, the cipher text sent by the attacker is just the XOR of the original cipher text and the delta between the original IP and the new IP plus the new checksum. [Bor01]

This attack can successfully thwart an encrypted tunnel if the tunnel ends at a gateway, like a VPN concentrator. The packet is decrypted by the VPN concentrator and sent to the destination (attacker) in decrypted form. If the IP header is encrypted then just modifying the IP address while keeping a valid integrity check is an easier problem because the attacker only has to guess the contents of the header correctly and not the payload. [Bor02] [Col02b] [Moi01] [Bor01]

2.4. Active Eavesdropping with Known Plaintext

Using the weaknesses in WEP described above, the attacker can inject known traffic into the network in order to decrypt future packets sent by others. For example, if the attacker sends an email message destined to their computer on the wireless LAN from another computer, the IV associated with that message now enables the attacker to decrypt packets in the future using the same IV. Mathematically, when the same IV is used,

$$C_1 \oplus C_2 = P_1 \oplus P_2$$

If you know P_1 and can acquire C_1 and C_2 by eavesdropping then it is trivial to compute P_2. The same type of attack can occur by sending web traffic or knowing where the user is browsing. One could quickly build a database of (IV, P_1) in order to decrypt any layer 2 encryption using WEP. The only defense against this attack is to frequently change the WEP key so as to guarantee that you will have unique (IV, key) pairs. The successful implementation of frequently changing WEP keys depends on the initial authentication method, the exchange of the private key, and the frequency at which the WEP key is updated. Such implementations are complicated, only guarantee to slow an attacker, and do not necessarily preclude previously described WEP attacks.

2.5. Unauthorized Access

Unauthorized Access is different from any of the previous attack types that we have discussed in that it is not directed at any individual user or set of users. It is directed against the network as a whole. Once an attacker has access to the network, she can then launch additional attacks or just enjoy free network use. Although free network use may not be a significant threat to many networks, access is a key step in ARP attacks (Section 2.6.1).

Due to the physical properties of WLANs, attackers will always have access to the wireless component of the network. In some wireless security architectures this will also grant the attacker access to the wired component of the network. In other architectures, the attacker must use some technique like MAC address spoofing to gain access to the wired component of the network.

2.6. Man-In-The-Middle Attack

If the packets being transmitted are encrypted only at the network layer, or layer 3, then the attacker can obtain the header information from the data link layer (layer 2) and layer 3. A VPN or IPsec security solution entails such a countermeasure. Although these solutions protect the users from a direct confidentiality attack against the application data, it does not deny indirect confidentiality attacks such as man-in-the-middle, session hijacking (Section 2.7), or replay attacks (Section 2.8).

A man-in-the-middle attack can be used to read private data from a session or to modify the packets thus violating the integrity of a session.

This is a real-time attack, meaning that the attack occurs during a target machine's session. The data may be read or the session modified as it occurs. The attack will know the contents of the message prior to the intended recipient receiving it, or the message is changed en route.

There are multiple ways to implement this attack. One example is when the target has an authenticated session underway. Figure 6 below illustrates this type of attack technique. In step one, the attacker breaks the session and does not allow the target to reassociate with the access point. In step two, the target machine attempts to reassociate with the wireless network through the access point and is only able to associate with the attacker's machine which is mimicking the access point. Also in step two, the attacker associates and authenticates with the access point on behalf of the target. If an encrypted tunnel is in place the attacker establishes two encrypted tunnels between it and the target and it and the access point. [Lyn02] [Moi00] [Col02a] [Col02b]

Variations on this attack technique can are based on the security environment. Without encryption or authentication in use the attacker establishes a rogue access point. The target unwittingly associates to the rogue which acts as a proxy to the actual wireless network.

This attack can be simple or quite complicated depending on the security mechanisms in place. The more security mechanisms in use the more security mechanisms that the attacker will have to subvert when reestablishing the connection with both the target and the access point. If authentication is in place the attacker must defeat the authentication mechanism to establish new connections between herself and the target and herself and the access point. If encryption is in use, the attacker must also subvert the encryption to either read or modify the message contents.

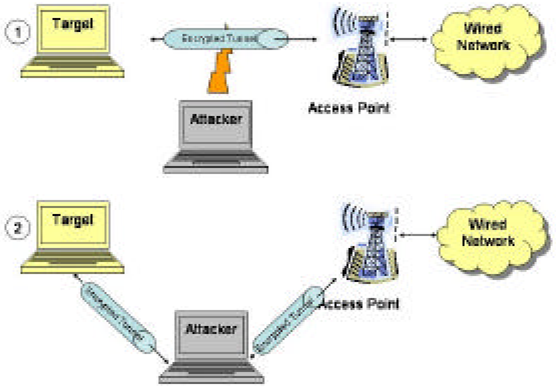

Figure 6 Man-In-The-Middle Attack. The attacker first breaks the connection between the target and the access point. Then the attacker presents herself as an access point and allows the target to associate and authenticate with her machine. The target believes that he is interacting with the legitimate access point because the attacker has established a valid session with the access point using her own credentials. She passes all traffic between the target and access point either only reading it or modifying it depending on her objective.

2.6.1. ARP Attacks

ARP attacks are a particularly dangers subset of man-in-the-middle attacks because these attacks can be directed against targets on the wired component of the network, not just wireless clients. The attack can involve either circumventing the authorization mechanism if it exists, or providing false credentials. This differs from the other attack techniques in that the false credentials may in fact belong to a valid user. The attacker is only gaining access to the network and is not masquerading as the target. This may be an ambiguous distinction but we find it useful when discussing authorization technologies below. [Lyn02] [Col02b] [Sch02] [Bor01] [Mis02] [Pot02]

Denying this attack technique is an absolutely vital step in designing security architecture. Not having access to the WLAN limits the attacker's possibilities for further attack. Defending against unauthorized access will make successful attack on the integrity of the WLAN much more difficult.

We have separated ARP redirection attacks from Man-In-The-Middle attacks because ARP redirection does not require that the attacker establish sessions with the target and the network. ARP attacks can be a way of performing traffic analysis or passive eavesdropping.

The Address Resolution Protocol (ARP) maps the Media Address Controller (MAC) address (Layer 2) of a network node to the Internet Protocol address (Layer 3). Altering the mapping of the MAC address to IP address allows an attacker to reroute network traffic through her machine. With the session passing through the attacker's computer the attacker can read plaintext, collect encrypted packets for later decryption, or modify the packets in the session. ARP cache poison attacks are contained by routers but a great deal of damage can be done with a successful ARP Cache Poisoning attack. [Wha01] [Fle] [Car01]

To carry out a successful attack the attacker must have access to the network but nothing else. The attacker sends a forged ARP reply message that changes the mapping of the IP address to the given MAC address. The MAC address is not changed just the mapping. Once the cache has been modified the attacker can act as a Man-In-The-Middle between any two hosts in the broadcast domain. This is illustrated in Figure 7 below where an attacker on a wireless client has access to sessions between two wired hosts.

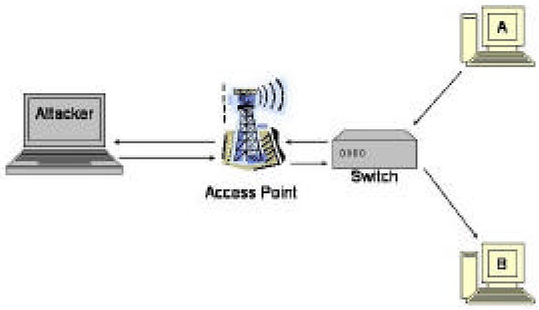

Figure 7 APR Cache Poison Attack. The attacker has placed herself "in between" two computers (A & B) that are on the wired network. The targets do not realize that they are victims of a wireless attack because the do not think that are part of a wireless network.

2.7. Session High-Jacking

Session High Jacking is an attack against the integrity of a session. The attacker takes an authorized and authenticated session away from its proper owner. The target knows that it no longer has access to the session but may not be aware that the session has been taken over by an attacker. The target may attribute the session loss to a normal malfunction of the WLAN. Once the attacker owns a valid session she may use the session for whatever purposes she wants and maintain the session for an extended time. This attack occurs in real-time but can continue long after the victim thinks the session is over.

To successfully execute Session High Jacking the attacker must accomplish two tasks. First she must masquerade as the target to the wireless network. This includes crafting the higher-level packets to maintain the session, using any persistent authentication tokens and employing any protective encryption. This requires successful eavesdropping on the target's communication to gather the necessary information as shown in step one of Figure 8 below. The second task the attacker must perform is to stop the target from continuing the session. The attacker normally will use a sequence of spoofed disassociate packets to keep the target out of the session as depicted in step two below. [Mis02] [Sch02] [Sko02]

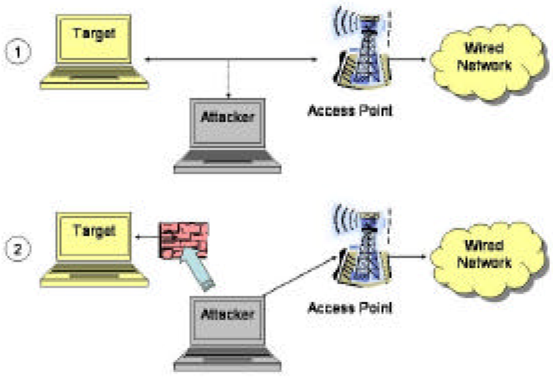

Figure 8 Session High-Jacking. The target first establishes a valid session. The attacker collects enough information from the session to conduct the attack. In step 2, the attacker blocks access from the target to the access point and continues the authenticated session masquerading as the target to the access point.

2.8. Replay

Replay attacks are also aimed at the integrity of the information on the network if not necessarily the integrity of a specific session. Replay attacks are used to gain access to the network with the authorizations of the target, but the actual session or sessions that are attacked are not altered or interfered with in anyway. This attack is not a real-time attack; the successful attacker will have access to the network sometime after the original session(s).

In a replay attack (illustrated in Figure 9) the attacker captures the authentication of a session or sessions as shown in step one below. The attacker then either replays the session at a later time or uses multiple sessions to synthesize the authentication part of a session for replay in step two. Since the session was a valid, the attacker establishes an authenticated session without being privy to any shared secrets used in authentication. Without further security mechanisms the attacker may interact with the network using the target's authorizations and credentials. If the WLAN employs encryption that the attacker cannot defeat the attacker may still be able to manipulate the WLAN by selectively modifying parts of the packet to achieve a desired outcome. [Kri02] [Bor01] [Moi01] [Chi] [Kar02]

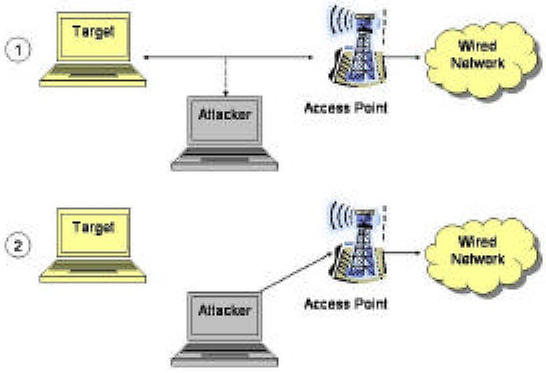

Figure 9 Replay Attack. This attack is similar to session high-jacking except for timing. At some time after a valid session between the target and the access point the attacker replays the authorization to create an authorized session.

3. Security Mechanisms and Technologies

In this section we discuss the different security technologies generally available on the marketplace. We describe how these technologies work and the attack techniques they are intended to stop or restrict. We also comment on the effectiveness of these technologies and the attack techniques for defeating them. This section represents no new discoveries, but relies on published attacks.

We break wireless security technology into three broad categories. Based on our research most vendors use a combination of technologies from these categories to build a secure system. The first category is authorization. This includes the mechanisms for determining whether or not a client is an authorized user of the WLAN and which authorizations the user should have. It also includes the mechanisms for stopping an unauthorized user from using the WLAN. The second category includes those mechanisms for maintaining the privacy of the session once a user is authenticated into the WLAN. Normally, the privacy is maintained by some use of encryption. The final category contains those mechanisms that verify the integrity of the information.

When we discuss these security mechanisms we do so from two points of view. The first is from that of an outsider. This is an attacker who has no special knowledge of the WLAN other than what she can gather from open-source reconnaissance tools and a wireless device capable of physically accessing the WLAN, like a laptop with 802.11a card. The second is from that of an insider. This attacker may be a member of the organization and have a laptop with the software, hardware, certificates, etc. that authorized users have. It may be an attacker who steals a laptop from an authorized user or an attacker who purchases the hardware and software used by the target WLAN to aide the attack. Both are threats and both must be considered when designing a WLAN security architecture.

When examining these security mechanisms we will keep in mind what we call the "Blazing Saddles Principle." In the film Blazing Saddles, a posse was pursuing the main characters across a wide flat expanse of desert. The bad guys came upon a toll booth and waited while a member went back for dimes. Meanwhile, the posse caught up with the guys who were waiting for a couple of dimes. The good guys did not have a well integrated defense in depth, but the humor was their "toll booth" defense worked!

Unfortunately, we cannot expect attackers to act like the characters in a film. When we build a security system we must cover all possible attacks; we cannot depend on our adversaries to attack our strong points. Making an attack more difficult in any way is a worthy feature of a security mechanism even if it does not provide perfect protection. Security mechanisms as a rule do not provide perfect security. When properly integrated into a defense in depth they can raise the cost required to defeat them high enough to make the attack impractical. As stated by Ferguson and Schneier, "Partial countermeasures only make sense if they make attacks harder to perform. Protecting against difficult attacks makes no sense if there is no protection against the easy forms of attack." [Fer99]

3.1. Authentication

These are the technologies used to authenticate an individual client into the WLAN. Once authenticated, the client usually owns an authenticated session that continues until the client or WLAN terminate the session.

3.1.1. IEEE 802.11 Standard or Wired Equivalent Privacy (WEP)

The 802.11 standard provides a number of options for authentication. Here we discuss the two that provide the most protection from unauthorized users.

3.1.2. Closed System Authentication (Service Set Identifier (SSID))

This is the most basic security authentication mechanism for 802.11 networks. The SSID can be used as a shared secret; however, as a security mechanism it is virtually worthless. In its most secure configuration the access point will not respond to probe requests. This gives the illusion of maintaining the SSID as a shared secret. In reality, the SSID is transmitted unencrypted. An attacker can use passive eavesdropping to discover the SSID, or if she is impatient, she can use an active attack. To actively attack a WLAN using SSID as a shared secret the attacker sends a forged disassociate message to the target and then eavesdrops as the target automatically begins to reassociate with an authentication transaction. [Lyn02].

We mention this security mechanism only for completeness. There is some indication that some administrators have used this in an attempt to restrict unauthorized users but it is only effective against the most unskilled attacker.

3.1.3. Media Access Card (MAC) Access List

Access Points can be programmed to allow access to the WLAN by MAC address. This security mechanism is designed to deny access to all clients except those explicitly authorized to use the WLAN. The effort required to implement and maintain access lists is large. This mechanism does not scale well and is only useful for small WLANs.

Access Lists can easily be defeated by an attacker with minimal tools. It provides no protection from the insider, who is an authorized user of the network. An outsider who obtains a wireless network access card (WNIC) that is authorized entry into the WLAN is effectively an insider. An outsider can also sniff the traffic between the AP and the client collecting a valid MAC address. She can then craft packets with a forged MAC address for easy access to the WLAN.

Although not a scalable security measure, this mechanism will stop an attacker without any specialized attack tools. It effectively *raises the bar*, albeit only a small amount, and therefore meets the Blazing Saddles Principle described earlier.

3.1.4. Shared RC4 key Authentication

As described in section 2.2, WEP's implementation of shared RC4 Authentication does not offer a high degree of security. Defeating WEP authentication has been published by both Borisov et. al. [Bor01] and Arbaugh et al. [Arb] An attacker that intercepts a single authentication sequence can then authenticate into the WLAN at will using this key. Many WLANs employ a single key for all users. Regardless, WEP only allows for four total keys, making this vulnerability serious.

This security technology offers no protection from a malicious insider. An insider or an attacker masquerading as an insider can authenticate and associate to the WLAN by virtue of their owning the shared secret (key). With access to the WLAN, the attacker has met a necessary precondition for most attacks.

As described previously, an outsider attacker can easily defeat WEP authentication. The attacker will need special tools, but those tools are easily available in the public domain. The skill required to use these tools are minimal. The problems with WEP security are well documented but we include them for completeness.

3.1.5. 802.1x

IEEE 802.1x is a specification for port-based authentication for wired networks. It has been extended for use in wireless networks. It provides user-based authentication, access control and key transport. 802.1x is designed to be flexible and extensible. It relies on Extensible Authentication Protocol (EAP) for authentication, which was originally designed for Point-to-Point Protocol (PPP) but was reused in 802.1x. 802.1x uses three types of entities: the client, the access controller and the authentication server[1]. Typically, the

[1] Not 802.1x terminology. 802.1x calls the nodes the supplicant, Authenticator and Authentication Server. We chose keep our terminology consistent

authentication server is a Remote Authentication Dial-In User Service (RADIUS) server which is coupled to the wired network authentication. The access point may also serve as the Access Appliance. EAP is extensible; hence it can use any authentication mechanism. It operates at the network layer (layer 3) rather than the data link (layer 2) which contributes to the flexibility of the protocol.

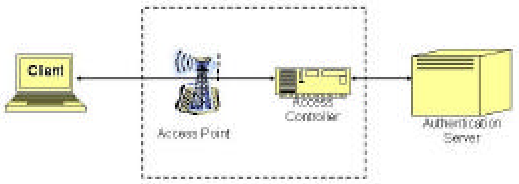

Figure 10 In 802.1X the Access Point has an Access Controller function that may or may not be incorporated into the access point. Regardless, the access controller uses the authentication server (normally RADIUS) to determine whether or not to authenticate the client.

802.1x has some serious shortcomings for a wireless network. These come from the reuse of good security mechanisms in an environment for which they were not designed. Reused protocols have been examined more closely than newly developed protocols and therefore are normally more secure. The problem in 802.1x is not the quality of the reused protocols, but the imperfect fit of the wired protocols to a wireless network.

For 802.1x to work in a wireless setting, the access point/access controller must allow traffic to the authentication server prior to authentication. Both 802.11a WLAN protocol and 802.1x use state machines to function correctly. The adaptation of 802.1x to 802.11a left the two state machines loosely coupled. Due to the loose coupling between the state machine in the two protocols 802.1x is subject to session high-jacking attack from an outsider. [Mis02]

The problem of a rogue network connection is much smaller in wired networks than in WLANs. 802.1x also is designed to provide authentication of only the client and not the access point. Mutual authentication is vital to protecting against man-in-the-middle attacks. Client-only authentication leaves an opening for an attacker to spoof the target into thinking that her machine is the access point, thus establishing a rogue access point a component of a man-in-the-middle attack. [Mis02] [Pot02]

When RADIUS is used to actually perform the authentication it relies on a shared secret with the authenticator. Depending on the scale of the WLAN, key distribution can be problematic. Poor key distribution makes it easier for an outside attacker to mimic an insider with all the associated vulnerabilities.

The insider may not have much of an advantage with 802.1x over the outside attacker. Since 802.1x is coupled to wired network authentication (normally through RADIUS) the insider will only have access to their normal resources. If the 802.1x is not coupled to a mechanism for blocking network access like inline authentication then 802.1x only protects network resources from the honest user. The attacker, whether an insider or outsider, has a platform for launching attacks. Implementing 802.1x security must be coupled with a blocking mechanism so that unauthenticated clients cannot access the network..

Using 802.1x to authenticate sessions stops the casual unauthorized user from accessing the WLAN. However, it does not prevent a moderately skilled attacker with few resources from successfully attacking the network.

3.1.6. Extensible Authentication Protocol - Transport Layer Security (EAP-TLS)

The EAP has a number of different modes of operation, hence the moniker extensible. The most promising is the use of TLS as the authentication mechanism in the EAP. The TLS is the newest version of Secure Socket Layer 3.0 or SSL.

EAP-TLS supports mutual authentication and dynamic keying. Key differences in implementation are key management. EAP-TLS can use a shared secret which is only as secure as the secret. It can also use a Public Key Infrastructure (PKI) to distribute keys. However, this adds significant complexity and overhead to a system along with a host of new potential vulnerabilities that must be addressed. Attacking PKI systems is beyond the scope of this paper. [Cis02]

Mutual authentication is comprised of two separate authentications. The client authenticates the wireless access point and the wireless access point authenticates the server. The TLS handshake is

throughout this paper.

the basis for authentication. The server gives a certificate to the client and the client validates the certificate. Once the client is confident of the server's identity it sends its certificate to the server. One weakness is that the identification occurs in the clear so an attacker can eavesdrop on the exchange. [Gas02] Both parties in wireless transactions are certain that the party with whom they are exchanging information is who they think they are. We discuss mutual authentication in the generic sense here because it is a vital concept to network security and is incorporated into most proprietary security solutions and is also part of some standard security systems.

Mutual authentication can be implemented using numerous techniques. If the implementation is vulnerable, then the system is vulnerable. Besides assuring he identity of the two end points, the authentication scheme must also assure the confidentiality of the authentication transmissions to protect against replay (Section 2.8) and session high-jacking (Section 2.7) attacks.

Mutual authentication can use secret keys or a public key infrastructure with a central certificate authority. Each has their strengths and weaknesses. The key aspect is that neither party implicitly trusts the other.

Mutual authentication stops man-in-the-middle attacks (Section 2.6). An attacker cannot fool the client into thinking that he is authenticated into the access point because the client authenticates the access point. Mutual authentication may not stop session high-jacking. If each individual packet is authenticated, then it will increase security of the transmission, but at an obvious performance cost. We discuss per packet authentication separately. Many replay attacks can be thwarted by mutual authentication. If the authentication includes time or sequence numbers replay attacks will be much more difficult, if not impossible.

3.1.7. Tunneled Transport Layer Security (TTLS)

It is not clear whether or not EAP-TLS can be implemented without a public key infrastructure for certificate exchange. We believe that it is possible to install the certificates on the client and server without using a PKI but we are not absolutely certain that this is the case. But there is no doubt that TTLS does not require a PKI. TTLS differs from EAP-TLS in that it is a two stage protocol. In the first stage an encrypted tunnel is established between the client and server. In doing so, the server presents its certificate to the client and thus the client is confident of the server's identity. In the second phase the client's credentials are given to the server for validation. These credentials are in the form of attribute-value pairs and not digital certificates. [Gas02] All EAP authentication protocols meet this criterion. Because the credentials are passed in an encrypted tunnel a digital certificate is not necessary.

3.1.8. Protected Extensible Authentication Protocol (PEAP)

PEAP is very similar to TTLS. It is really just a different flavor of TTLS. It is also a two phase protocol. The first phase is used to authenticate the server and establish an encrypted tunnel between the client and the server. Then instead of using the older attribute-value pair to authenticate the client, authentication is limited to any EAP method. Since EAP includes a wide array of authentication protocols this is not a severe restriction, but it does allow less flexibility than TTLS. [Gas02]

3.1.9. Wireless Transport Layer Security (WTLS)

WTLS has three operating modes, only one is secure. Class 1 authentication is anonymous authentication and offers no security. It is important that an implementation never allow class 1 authentication or an attacker may be able to "negotiate down" to a class 1 authentication. That is, the attacker may create a session whereby the authenticator grants anonymous access rights. This situation is not warranted in most organizations.

Class 2 is server authentication only, while class three calls for authentication of both the client and the server. The keys for both the client and server may be either private or public. Public keys require a secure key management infrastructure while private keys require secure key distribution and storage.

WTLS when implemented properly provides a good level of security. A class 2 authentication is vulnerable to man-in-the-middle attacks as well as session high-jacking, while a class 3 authentication is not. It is important that the implementers not allow the system to be "negotiated down" to class 2 – thus circumventing mutual authentication.

3.1.10. Packet Authentication

Packet Authentication is different from the session authentication that the previous paragraphs address. Once an authenticated session is established and the keys are exchanged most schemes rely on the privacy of an encrypted tunnel and integrity checking on the payload to imply the identity of the sender. This is an effective scheme, however, the addition of packet authentication adds an additional mechanism that an attacker must defeat. We do not believe replay, session high-jacking and man-in-the-middle attacks are possible when packet authentication is added to strong session authentication.

The individual packets that are transmitted as part of an authenticated session must all come from the sender and arrive at the intended recipient. The receiver must be sure that the individual packets of a session did in fact come from the sender or else the session is subject to man-in-the-middle, replay or session high-jacking attacks. These attacks all can succeed because the attacker fools the receiver into believing the packets sent by the attacker are from the target, hence destroying the session integrity of the system. These all rely on breaking an authenticated session. Per-packet authentication adds another layer of defense that an attacker must defeat. She cannot just take over an authenticated session without the ability to authenticate the packets that she generates or modifies. By itself packet authentication does not offer much defense; however, when combined with mutual session authentication it is very effective. This is an example of how properly integrated partial security mechanisms can form a defense-in-depth.

3.1.11. Summary

The table below is a summary of session authentication security mechanisms and the effectiveness of those mechanisms against the four attack techniques that require circumventing the authentication scheme. We rate each mechanism as poor, marginal or good from the point of view of an insider and an outsider. A poor rating means that the mechanism is easy to defeat with widely available tools. A poor security mechanism will basically protect against inadvertent attacks or errors but will not stop an attacker. Marginal ratings indicate that defeating the mechanism requires either resources (like time) or significant skill. A marginal security mechanism is susceptible to an attacker with skill and experience and the resources required to devote to such an attack. Mechanisms that we rate *good* may stop a skilled attacker or may slow an attacker enough that she cannot achieve her objective. We expect that good mechanisms are vulnerable only to the most skilled professionals that are determined to succeed because the reward for success is high enough.

Table 2 Summary of Authentication Effectiveness

	Man-in-the-Middle	***Session High-Jacking***	***Replay***	***Unauthorized Access***
SSID	Insider: Poor Outsider: Poor	Insider: Poor Outsider: Poor	Insider: Poor Outsider: Poor	Insider: None Outsider: Poor
WEP RC4	Insider: Poor Outsider: Poor	Insider: Poor Outsider: Poor	Insider: Poor Outsider: Poor	Insider: None Outsider: Poor
MAC Access List	Insider: Poor Outsider: Poor	Insider: Poor Outsider: Poor	Insider: Poor Outsider: Poor	Insider: None Outsider: Poor
802.1X	Insider: Poor Outsider: Poor	Insider: Poor Outsider: Poor	Insider: Poor Outsider: Poor	Insider: None Outsider: Marginal[†]
WTLS Class 3	Insider: Good Outsider: Good	Insider: Good Outsider: Good	Insider: Poor Outsider: Poor	Insider: None Outsider: Good†
EAP-TLS	Insider: Good Outsider: Good	Insider: Good Outsider: Good	Insider: Poor Outsider: Poor	Insider: None Outsider: Good†
Packet Authentication	Insider: Poor Outsider: Poor	Insider: Poor Outsider: Poor	Insider: Poor Outsider: Poor	Insider: None Outsider: Good†

[†] Only if combined with a mechanism to block access to unauthorized users

3.2. Encrypted Tunnel or Virtual Private Network (VPN)

Packets are kept private by the use of encryption. Encryption systems are designed to provide a virtual tunnel that the data passes through as it traverses the protected part of the network. If the system is properly designed and correctly implemented, the contents of the payload will be unreadable to those without the proper decryption key. The contents that the receiver decrypts must not only be private, but exactly as the sender intended. In other words correct tunnel will not only keep the contents private, but also free from modification. This requires the use of a cryptographic integrity checker or checksum.

3.2.1. OSI Network Layer and Endpoints

Two of the key design parameters of VPN are the OSI network layer that is encrypted and the endpoints of the tunnel. Generally, the lower the layer that is encrypted the more secure. Also the longer the tunnel, generally the more secure the tunnel. The drawback is that the more secure these mechanisms the higher the reliance on vendor specific components and the decrease in system performance. Integration with your existing architecture is beyond the scope of this paper but is useful in understanding the array of options.

3.2.1.1. Endpoints

Encrypted tunnels can have three possible sets of endpoints. The first illustration in Figure 11 shows a tunnel that runs from client to access point. The second runs through the access point but only to an access controller appliance that separates the wired and wireless components of the network. Finally end-to-end encrypted tunnels run from the client to the server passing through the wired and wireless network segment in the encrypted state. They are decrypted at the destination. These may be used together to form a defense-in-depth.

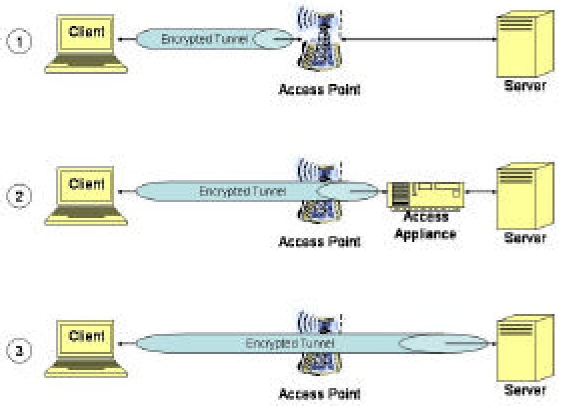

Figure 11 Endpoint Options for Encrypted Tunnels.

3.2.1.2. Encryption Layer

Besides the length of the encrypted tunnel, the other attribute that determines the security of the encryption is the implementation layer. Encrypted tunnels may be implemented at layer 4 (i.e. secure sockets or SSL), the layer 3 (i.e. IPSec or VPN solutions), and/or at the layer 2 (i.e. WEP or AES. Figure 12 demonstrates what portion of a packet is actually encrypted given a specific implementation layer. Layer 3 tunnels encrypt layers 4 and higher leaving the layer 3 header exposed. Likewise, a layer 2 tunnel encrypts layer 3 data and higher protecting information like the source and destination IP address of the packet.

The security of an encrypted tunnel increases when encryption is applied at a lower layer. Thus, a layer 3 tunnel is not as secure as a layer 2 tunnel. For example, spoofing an IP is easier to achieve when a layer 3 tunnel rather than a layer 2 tunnel is implemented because the IP address of the recipient is transmitted in the clear. A layer 2 tunnel decreases the risk of an IP spoofing attack but does nothing to prevent an ARP spoofing attack as the MAC address is still transmitted in plaintext.

The rule of thumb for encrypted tunnels is, "when you own a level, you can break security implemented on all the higher levels." This provides a good guide but only when examined in isolation. Combinations of other security mechanisms with encrypted tunnels will increase security.

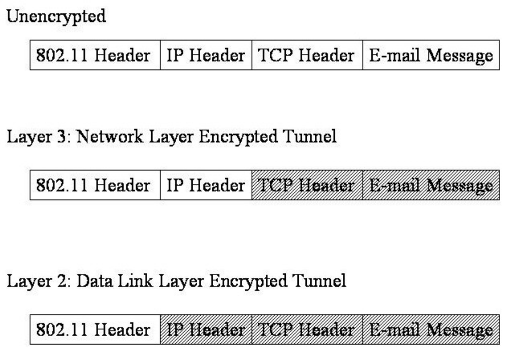

Figure 12 Encryption implementation at layer 2 and layer 3.

3.2.2. Encryption Algorithm and Key Size

Another major design feature is the type of encryption to use. In theory, the algorithm and key length combine to make the packets difficult to read. The implementation however, is a key aspect that cannot be ignored. Flaws in implementation can drastically alter the effort required to break the encrypted message negating any theoretical advantage a scheme may have. WEP encryption is a perfect example of how implementation flaws negate the theoretical advantages of the algorithm. While WEP encryption provides minimal protection, triple-DES (Data Encryption Standard) is the current standard and if properly implemented provides adequate security for most applications. The Advanced Encryption Standard (AES) is the newly approved standard which provides a higher level of assurance while requiring less processor power.

3.2.2.1. IEEE 802.11 Standard or WEP (40 and 104 bit keys)

WEP is a layer 2 encryption scheme based on the RC4 stream cipher. It relies on a secret key that is shared by the client and server. WEP uses a non-cryptographic checksum of the plaintext to insure integrity. The plaintext and the checksum are encrypted using an initialization vector, the secret key and the RC4 algorithm. The initialization vector and the encrypted payload are then sent to the recipient.[Bor01]

As discussed in section 2, the WEP 40 bit key size can be attacked by brute force. The 104 bit keys are not currently vulnerable to brute force attacks but regardless of key size WEP is vulnerable to both passive and active eavesdropping. WEP encryption can be defeated passively when the key stream is reused. Because the WEP initialization Vector (IV) is only 24 bits, reuse can occur quite frequently even in a well implemented version of WEP. The use of 802.11a with a potential for a fivefold increase in bandwidth decreases the time needed to passively defeat WEP to minutes. Active eavesdropping with partially or fully known plaintext are relatively simple attacks to carry out on WEP WLANs. A determined attacker could build a decryption dictionary in a relatively short period of time and thus have real-time access to all message traffic on the WLAN. WEP WLANs that start the IV at 0 when reinitialized or don't change the key stream after every packet make this task simpler still.[Bor01]

Attackers can modify a WEP encrypted packet, or create a new packet that meets the WEP authentication standards violating the integrity of WEP sessions. This allows man-in-the-middle and session high-jacking attacks to be successful.

WEP security is flawed, but does provide some security. WEP provides almost no protection from insiders. With only four keys available, multiple users using the same key are inevitable. Even though WEP can be broken relatively easily by outsiders, the attacker must use special tools and may have to invest days of effort to do so. Neither of these requirements presents much of a hurdle, but discourage the casual attacker looking for an easy target.

3.2.2.2. Layer 2 Block Cipher Encrypted Tunnel

Strongly Encrypted Tunnels include those tunnels encrypted with triple-DES and AES block cipher encryption.

Layer two tunnels hide the IP header data from the passive eavesdropper. In a properly implemented system this can eliminate an IP redirection attack and make man-in-the-middle (Section 2.6) and session high-jacking (Section 2.7) attacks much more difficult. WEP is a layer 2 encrypted tunnels with all the advantages of a layer 2 tunnel, but because of the flaws in the algorithm and implementation it provides little security. Layer 2 tunnels that are encrypted with better algorithms provide security from passive eavesdropping.

Layer Two Tunnels protect against IP Spoofing (Section 2.3) attacks from outsiders. Insiders, who own the secret key, can eavesdrop on the session, and armed with that information, they may conduct other attacks. Key management is the major vulnerability for layer two tunnels.

3.2.2.3. Layer 3 Virtual Private network (VPN) or Strongly Encrypted Tunnel

Strongly Encrypted Layer 3 VPNs leave the IP header data between the VPN client and the VPN concentrator unencrypted while protecting the payload and header information for layers 4 and up. Layer 3 VPNs tend to be more vender independent and can be configured to protect sessions over the portions of the wired network as well as the WLAN.

Layer 3 Strongly encrypted Virtual Private Networks (VPN) can provide strong protection against outsider's access to private sessions. Like Layer 2 tunnels, key management is important. The owner of the secret key can eavesdrop on protected sessions. If combined with a public key infrastructure (PKI) this risk can be mitigated. However, PKI increases the complexity of the infrastructure and can introduce other vulnerabilities to the system. Even without the key, Layer 3 VPNs are more vulnerable than layer 2 tunnels. In 802.11a WLANs, management packets are not authenticated and an attacker can easily break the connection between the target and the wireless access point. Without per packet authentication the attacker can then launch a man-in-the-middle or session high-jacking attack.

3.2.3. Summary

To summarize, to protect the privacy of the session we can choose criteria for three major design parameters: layer, topology, and encryption. Most encryption for WLAN takes place at layer 2 or layer 3. Most topologies just include the wireless portion of the network. Normally, an appliance located between the wireless portion of the network and the remainder of the wired network is the endpoint of the encrypted tunnel. There are tunnels that extend from the wireless client to the server, like the security architecture provided by IBM, but they are vendor specific.

The final parameter is the choice of encryption algorithm and key size. WEP and enhanced WEP are common. Lengthened key size and dynamic rekeying are common enhancements. Most solutions that do not use WEP use 3DES which is FIPS-140 compliant. Vendors have chosen 3DES due to its long record of secure use and compliance with government standards. This allows them to sell to government clients. AES is the new government standard, which although not as well tested as 3DES, promises to remain secure for a longer period of time into the foreseeable future and gives the added bonus of being less computationally intensive.

Table 3 Summary of Encrypted Tunnel Analysis

	Traffic Analysis	Passive Eavesdropping	Active Eavesdropping with Partial Known Plaintext	Active Eavesdropping with Known Plaintext
Layer 3	Insider: Key Distribution Dependent Outsider: Marginal	Encryption Algorithm Dependent[‡]	Insider and Outsider: Marginal	Encryption Algorithm Dependent‡
Layer 2	Insider: Good Outsider: Good	Encryption Algorithm Dependent‡	Insider and Outsider: Good	Encryption Algorithm Dependent‡
End-to-End	Layer and Algorithm	Encryption	Encryption	Encryption

[‡] With poor key distribution the insider can read the authentication messages because she has the key. In the case where each client has a separate key the insider has no advantage over the outsider.

	Dependent	Algorithm Dependent‡	Algorithm Dependent‡	Algorithm Dependent‡
Wireless Only	Layer and Algorithm Dependent	Encryption Algorithm Dependent‡	Encryption Algorithm Dependent‡	Encryption Algorithm Dependent‡
WEP	Insider: Marginal Outsider: Marginal	Insider: Poor Outsider: Poor	Insider: Poor Outsider: Poor	Insider: Poor Outsider: Poor
Strong Encryption	Layer and Algorithm Dependent	Insider: Good‡ Outsider: Good	Insider: Good‡ Outsider: Good	Insider: Good‡ Outsider: Good

3.3. Integrity Checking

Another aspect that must be considered is integrity checking. Integrity is normally implemented separately from the encryption and indicates whether or not the packet has been altered from when the sender created it. A cryptographic checksum is a necessity. The question is whether to protect the message itself or the meaning of the message. The integrity check mechanism can encrypt the message and authenticate the encrypted message or it can authenticate the plaintext message and encrypt the authentication and the message. Ferguson and Schneier advocate authenticating the actual meaning or message before encryption while the people who developed IPsec advocate authenticating the encrypted message. Authenticating the encrypted message leaves the session vulnerable to potential attack as documented by Ferguson and Schneier. [Fer98]

3.3.1. WEP CRC-32 Checksum

The WEP Checksum is a linear function of the message. Taking the plaintext as input the CRC-32 checksum calculates a 32 bit number based on the content of the message. Any modification of the message should result in a different checksum when the CRC-32 function is used. This would indicate to the receiver that the message has been modified. The function does not map just one message to each of the 429 million possible values. There are far more than 429 million possible messages, so each value actually has many possible messages that can have the CRC-32 function applied to result in that value. A clever attacker can modify the message and leave the checksum unchanged. Because both the RC4 stream cipher and the CRC-32 checksum are linear the attacker can actually modify the message without even knowing the entire contents of the message, just the change she wants to make.

3.3.2. Cryptographic Checksum or Message Integrity Codes (MIC)

When encrypting the message a technique called Cipher Block Chaining (CBC) can be part of the encryption algorithm. In fact it is used in most modern algorithms. CBC calculations result in a residual value that does not have to be transmitted to decrypt the message; however, the residue can only be computed by using the secret key. Hence it insures the message is intact. This technique does not work when the message is encrypted. [Kau95]

3.3.3. Secure Hash Algorithm SHA-1

SHA-1 is an algorithm for computing a condensed representation of a message. The SHA-1 algorithm computes a 160-bit output called a message digest from the original message. It is virtually impossible to find a message to match a given digest or two separate messages that produce the same digest; therefore, a modified message will be detectable as such by the receiver, thus maintaining the integrity of the message. [NIS95]

3.3.4. Others

There are other cryptographic hash algorithms that provide message integrity. MD4 and MD5 are older algorithms that have demonstrated vulnerabilities with published attacks. RIPEMD-160 and HMAC are two less popular algorithms that also do not appear vulnerable at this time. [Sta99]

3.3.5. Summary

To summarize, multiple encryption as found in 3DES and AES provides cryptographic assurance of a message’s integrity. MIC can do the same but only at the expense of not using encryption to protect the message privacy. The WEP CRC is linear and does not provide much protection. The advantage that insiders have over outsiders is key distribution dependent. If the inside attacker does not have the key used by the target then she does not have an advantage over the outsider. If, however, she has the key used by the target, then she can create packets that have a matching integrity check.

3.4. Summary

These design parameters combined with the quality of the implementation determine the security of the sessions on your WLAN. Most attacks are automated, so while they are arcane and require skill in cryptography, they are quickly packaged for use by even the mathematically inept.

4. Conclusion

Security is not absolute. There is no "secure" or "non-secure" technical solution. Security includes the entire environment. The three major components of security are the technology, the policies, and the people. They are all legs of a three-legged stool. In the way that a three-legged stool is not stable without all three legs; a system will not be secure without the right technology, policy, *and* people. Security technology is only one component, albeit a very critical component.

Another attribute of security to keep in mind is that security is not a state, but a process of risk management. To develop, run, and maintain a secure network, the administrators and responsible leaders must know the value of the information assets and the threats against them. They must then consider the functionality their organizations need for mission accomplishment and the resources they have at their disposal. They then use risk mitigation strategies (technologies, policies, user training, etc.) to reduce the risks appropriately.

This paper identifies current classes of threats to WLANs. Understanding these threats is a critical task in the security process. We have not found as comprehensive and detailed WLAN threat analysis anywhere in the literature, and felt it was necessary for our own analysis to fully understand the threat before we could examine security technologies. We have also described and investigated the current security mechanisms commonly available for WLAN authentication, privacy, and integrity. Once again, we have drawn from extensive writings on these mechanisms and put them into one document for the ease of the reader.

As a result we have derived the attributes of a secure architecture for our environment. This analysis may not apply to other environments but by following our reasoning you should be able to better understand your own situation.

We believe that a WLAN security architecture must have the following attributes: mutual authentication; a strongly encrypted layer 2 tunnel; and strong cryptographic integrity verification. Without these features, not only is a WLAN vulnerable, but the entire information infrastructure of which it is a part is at risk. We also recommend per-packet authentication although we would not go so far as to make it a requirement.

Mutual authentication requires that the client authenticate itself to the network and that the network also authenticate itself to the wireless client. Man-in-the-middle, session high-jacking, and replay attacks are enabled by only requiring the wireless client to authenticate itself to the network. The authentication scheme used for each authentication must be strong enough to resist the current state of practical attacks. This is not currently the case with WEP since there are many published attacks against it. EAP-TLS is the strongest authentication scheme that we analyzed and we highly recommend it. 802.1x is vulnerable to a number of published attacks and because of its loose coupling with the 802.11 wireless state machine appears to have a fatally flawed design for wireless network implementations that will be difficult to fix. WTLS should provide sufficient security if properly implemented and configured. Like IPSec it is complicated and complication is the bane of security. IPSec allows different implementation and configuration choices. Either the vendor must provide secure configurations or the administrator must configure the system properly to provide a secure configuration. It is possible, but requires a lot of training and education on the system administrator's part.

Client authentication should have two parts: the client and the user. In this way, a lost or stolen wireless client gives only partial access to the network. This partial access may be enough for an attacker if the link between client authentication and user authentication is not strong. Blocking access from an authenticated wireless client but unauthenticated user to any part of the network other then the authentication server is mandatory to combat ARP cache attacks.

Another aspect of authentication is packet authentication. Once an authenticated session is established and the keys are exchanged, most schemes reply on the privacy of an encrypted tunnel and integrity checking on the payload to imply the identity of the sender. This is an effective scheme; however, the addition of packet authentication adds an additional layer of security that an attacker must defeat. We do not believe replay, session high-jacking and man-in-the-middle attacks are possible when packet authentication is added to strong session authentication.

In most organizations the privacy of the message is important. Even organizations that do not care about the privacy of the message should strongly consider encrypted tunnels for integrity protection. Knowing the content of a message is very helpful to an attacker in carrying out a number of attacks on the integrity of the message. The tunnel must be encrypted using a modern block-cipher like AES or 3DES. Stream ciphers such as RC4 that is used in WEP are susceptible to many attacks in a wireless environment. Although the WEP implementation can be considerably strengthened with some simple steps this breaks interoperability with the standard implementations of WEP. As long as the product does not follow a standard, it might as well be as strong as practical. In our opinion AES is the best choice due to its efficiency. The theoretical attacks against AES are not yet practical in the foreseeable future and until they are we believe AES provides sufficient protection.

Combining strong mutual authentication with a strongly encrypted layer 3 tunnel provides a good level of protection and it might be adequate for many organizations. If an organization must protect information as it travels through the wired network then a client to server layer 3 tunnel is a good solution. For those organizations that are more focused on the threats to the wireless component of the infrastructure layer 2 tunnels provide a better choice. By hiding the network layer header, attacks that manipulate the IP address are much more difficult. Traffic analysis is also severely hindered by this approach. Client-to-server encryption can also be overlaid on a layer 2 encrypted tunnel to provide a very high level of protection.

Finally, it is important to protect the integrity of the message. WEP's CRC-32 has numerous attacks against it both published and demonstrated. We do not recommend its use. MD4 and MD5 also have published vulnerabilities although carrying out successful attacks still remains difficult. We are not aware of any published practical attacks against SHA-1, which is the NIST approved standard. Although other cryptographic integrity checks may meet the specific needs of an organization, we recommend using SHA-1.

Key management is the one significant area that we have not addressed in detail. For those organizations that choose--or are forced to use--public key encryption, the proper choice of the mechanisms, policies and people are vital and beyond the scope of this paper. PKI is complex and must be properly administered and configured. PKI has its own threats which must be mitigated. The alternative is using a shared secret. The more entities that possess the shared secret, the less secret it is. Distributing and managing secret keys is once again beyond the scope of this paper. Our advice is to choose an approach carefully and devote significant resources to the issue of key management or else risk spending resources on security that does not pass the "Blazing Saddles" principle.

There is a very wide range of proprietary security technologies on the market and we have examined many of them. We require a WLAN that addresses the threats against our information, meets DoD and Army standards, and has a reasonable total cost of ownership. We have only found two products that meet our needs. The most common shortcomings that we found are the use of Layer 3 encrypted tunnels and weak session authentication.

References

[Air02] AirDefense, Wireless LANs: Risks and Defenses. White Paper available at http://www.airdefense.net/company/whitepaper/Risks_Defenses_0802.pdf last accessed 20 September 2002. 2002 AirDefence, Inc.

[And01] Andersson, H., S. Josefsson, G.Zorn and B. Aboba, Protected Extensible Authentication Protocol (PEAP) Internet Engineering Task Force Internet-Draft, web page online available at http://globecom.net/ietf/draft/draft-josefsson-pppext-eap-01.html last assessed 5 December 2002.

[And02] Andersson, H., S. Josefsson, Glen Zorn, D. Simon and Ashwin Palekar, Protected EAP Protocol (PEAP) Internet Engineering Task Force Internet-Draft, web page online available at http://globecom.net/ietf/draft/draft-josefsson-pppext-eap-tls-eap-02.html last assessed 5 December 2002.

[Arb01] Arbaugh, William, Narendar Shankar and Y.C. Justin Wan, Your 802.11 Wireless Network has No Clothes. Department of Computer Science University of Maryland. Web page online available at http://www.cs.umd.edu/~waa/wireless.pdf last accessed 20 September 2002.

[Bar02] Barnes, Christian, Tony Bautts, Donald Lloyd, Eric Ouellet, Jeffrey Posluns, David M. Zendzian, and Neal O'Farrell, Hack Proofing Your Wireless Network. Syngress Publishing Inc, Rockland, MA, 2002, pp 201 – 237.

[Bor01] Borisov, Nikita, Ian Goldberg and David Wagner, Intercepting Mobile Communications: The Insecurity of 802.11, in the Proceedings of the Seventh International Conference on Mobile Computing and Networking, July 16-21, 2001.

[Bor02] Borisov, Nikita, Ian Goldberg and David Wagner, Security of the WEP Algorithm. Webpage online available at http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html last assessed 26 September 2002.

[Car01] Carey, Allan, Wireless Security Vulnerabilities continue to Surface: Cigital Identifies the Latest. White Paper by Cigital, Inc. http://www.cigital.com. October 2001.

[Chi] Chickinsky, Alan, Wireless LAN Security Threats. Document IEEE 802.11-01/258

[Cis02a] Cisco Systems. Extensible Authentication Protocol Transport Layer Security Deployment Guide for Wireless LAN Networks. Webpage on line available from www.cisco.com last accesses 22 October 2002.

[Cis02b] Cisco Systems. Wireless LAN Enterprise Campus with Multi-Site Branch Offices. Webpage on line available from www.cisco.com last accesses 22 October 2002.

[Col02a] Colubris Networks, Inc. Comparing Colubris IPSEC Wireless Access Point Solutions with Wireless Middleware Gateways. 2002 Webpage online available at http://download.colubris.com/library/whitepapers/WP-020912-EN-02-00.pdf last accessed 20 September 2002.

[Col02b] Colubris Networks, Inc. Comparing Colubris IPSEC Wireless Access Point Solutions with Cisco Safe for Wireless LANs. 2002 Webpage online available at http://download.colubris.com/library/whitepapers/WP-020912-EN-01-00.pdf last accessed 20 September 2002.

[Ell02] Ellison, Craig, Exploiting and Protecting 802.11b Wireless Networks, 4 September 2001, webpage online http://www.extremetech.com/print_article/0,3998,a=13880,00.asp ExtremeTech.com last accessed 20 September 2002.

[Fer99] Ferguson, Niels and Bruce Schneier, " A Cryptographic Evaluation of IPsec." Counterpane Internet Security White Paper, 1999. Webpage online available at http://www.counterpane.com/ipsec.html last accessed 3 October 2002.

[Fle] Fleck, Bob and Jordan Dimov, Wireless Access Points and ARP Poisoning: Wireless vulnerabilities that expose the wired network. White Paper by Cigital, Inc. http://www.cigital.com.

[Flu] Fluher, Scott, Itsik Mantin and Adii Shamir, Weaknesses in the Key Scheduling Algorithm of RC4 webpage online available at http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf last accessed 4 October 2002.

[Fra01] Fratto, Mike, Mobile & Wireless Technology Tutorial: Wireless Security in Network Computing, 22 January 2001, CMP United Business Media, webpage online http://www.nwc.com/shared/printArticle.jhtml?article=/1202/1202f1dfull.html&pub=nwc accessed 20 September 2002.

[Gas02] Gast, Matthew, A Technical Comparison of TTLS and PEAP, The O'Reilly Network White Paper, 17 October 2002, web page on line last accessed 5 December 2002, available at http:// www.oreillynet.com/pub/a/wireless/2002/10/17/peap.html

[ISS] Internet Security Systems, Wireless LAN Security: 802.11b and Corporate Networks. ISS Technical White Paper. Webpage online available at http://documents.iss.net/whitepapers/wireless_LAN_security.pdf last accessed 20 September 2002.

[Kar] Karygiannis, Tom and Les Owens, Wireless Network Security: 802.11, Bluetooth and Handheld Devices (Draft), National Institute of Standards and Technology Special Publication 800-48.

[Kau95] Kaufman, Charlie, Radia Perlman and Mike Speciner, Network Security: Private Communication in a Public World. PTR Prentice Hall, Englewood Cliffs, NJ. 1995.

[Kri02] Krishnamurthy, Prashnt, Joseph Kabara, Tanapat Anusas-amornkul, Security in Wireless Residential Networks, IEEE Transactions on Consumer Electronics, Vol 48, No 1, February 2002. pp 157-166.

[Leo02] Leoutre, Marc, Edward Post, Mark Reigner, and Scott Lathrop, Wireless Security: Wireless Antennas and Footprint Analysis, Unpublished Research Paper. United States Military Academy, West Point, NY, May 2002.

[Lyn02] Lynn, Mike and Robert Baird, Advanced 802.11 Attack, presentation to Black Hat 2002 Conference, Las Vegas, NV 31 July 2002. Available at http://www.blackhat.com/presentations/bh-usa-02/baird-lynn/bh-us-02-lynn-802.11attack.ppt last accessed 20 September 2002.

[Max02] Maxim, Merritt and David Pollino, Wireless Security. RSA Press, McGraw-Hill/Osbome, Berkeley, CA. 2002.

[Mis02] Mishra, Arunesh and William Arbaugh, An Initial Security Analysis of The IEE 802.1X Standard. University of Maryland, Department of Computer Science and University of Maryland Institute for Advanced Computer Studies Techniacal Report CS-TR-4328 and UMIACS-TR-2002-10 6 February 2002.

[Moi00] Moioli, Fabio, Security in Public Access Wireless LAN Networks, Masters Thesis, Department of Teleinformatics, Royal Institute of Technology, Stockholm, Sweden. 12 June 2000.

[NIS95] National Institute of Standards and Technology, Secure Hash Standard Federal Information Processing Standards Publication 180-1, 17 April 1996. Web page online available at http://www.itl.nist.gov/fipspubs/fip180-1.htm last accessed 18 October 2002.

[Pot02] Potter, Bruce, 802.1x: What it is, How it's broken, and How to fix it. presentation to Black Hat 2002 Conference, Las Vegas, NV 31 July 2002. Available at http://www.blackhat.com/html/bh-usa-02/bh-usa-02-speakers.html#Bruce%20Potter last accessed 20 September 2002.

[Ros98] Ross, Sheldon M. A First Course in Probability. Prentice Hall, Upper Saddle River, NJ, 1998, pp 40 – 41.

[Sch02] Schwartz, Ephraim, Researcher crack new wireless security spec. InfoWorld. 14 February 02. Webpage online available at http://staging.infoworld.com/articles/hn/xml/02/02/14/020214hnwifispec.xml, last accessed 1 Oct 02.

[Sim00] Simon, D., Ba Aboba and T. Moore. IEEE 802.11 security and 802.1x. IEEE Document 802.11-00/034r1, March 2000 webpage online available at http://www.ieee802.org/1/mirror/8021/docs2000/8021xSecurity.PDF last accessed 4 October 2002.

[Sin00] Singh, Simon. The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. Doubleday, New York, NY, USA 1999.

[Sko02] Skoudis, Ed, Counter Hack: A Step-by-Step Guide t Computer Attacks and Effective Defenses. Prentice Hall, Upper Saddle River, New Jersey, 2002. pp 351-358.

[Sta99] Stallings, William, Cryptography and Network Security: Principles and Practice, 2e, Prentice Hall, Upper Saddle River, NJ 1999,

[Sym02] Symantec Corp. Wireless LAN Security Enabling and Protecting the Enterprise, White Paper. May 2002 Web Page online available at http://www.symantec.com/avcenter/reference/symantec.wlan.security.pdf last assessed 27 September 2002.

[Tru01] Trudeau, Pierre, Building Secure Wireless Local Area Networks. White Paper by Colubris Networks, Inc. 2001. Webpage online available at http://download.colubris.com/library/whitepapers/WP-010712-EN-01-00.pdf last accessed 20 September 2002.

[Wag96] Wagner, D. and B. Schneier, "Analysis of the SSL 3.0 Protocol, The Second USENIX Workshop on Electronic Commerce Proceedings, USENIX Press, 1996, pages 29.40. USENIX Press, 1996. Revised version available from http://www.counterpane.com

[Wal00] Walker, Jesse, Unsafe at any key size: an analysis of the WEP encapsulation. IEEE Document 802.11-00/362, Oct 2000. Web page online available at http://www.drizzle.com/~aboba/IEEE/ last accessed 4 October 2002.

[Wha01] Whalen, Sean, An Introduction to Arp Spoofing, April 2001 webpage online available at http://packetstormsecurity.nl/papers/protocols/intro_to_arp_spoofing.pdf last accessed 20 September 2002.