Proceedings of the 2003 IEEE
Workshop on Information Assurance
United States Military Academy, West Point, NY June 2003

Wireless Security Threat Taxonomy

Donald Welch, *Senior Member, IEEE*, and Scott Lathrop

Several papers have published very specific threats to wireless networks—specifically in the area of attacks against the IEEE 802.11 Wired Equivalency Protocol (WEP). Other papers have addressed wireless attacks based on the attack models used in wired networks. However, the different characteristics of wireless networks require looking at the threat differently. We present a Wireless Threat Taxonomy that we used to build the security architecture for the Wireless Network at West Point.

Index terms – Wireless, Threat, Information Assurance, 802.11

I. 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. WLANs provide users a significant mobility advantage as users can access their information in many locations, some of which are more conducive to collaboration. The freedom and mobility that WLANs promise, however, also present some serious security challenges. In the military domain, the department of defense's (DoD) transition from industrial-age to network-centric warfare brings with it technical challenges that are highly dependent and revolve around the successful implementation of a robust and secure wireless network of systems. These networks must address the threats described here.

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. [1]

This paper addressees known security threats to IEEE 802.11 networks focusing specifically on 802.11a because that is the standard we implemented. 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 one of the possible flavors of 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. Most of the attack techniques highlighted here can be applied to other wireless network protocols, such as IEEE 802.15, a wireless personal area network specification similar to Bluetooth.

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, and certificates for both the wired network and WLAN.

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. We do not discuss availability attacks against a wireless network as they include techniques such as electronic jamming which goes beyond the scope of this paper.

When looking at confidentiality attacks we start with the least intrusive and work towards more intrusive attacks. Of the seven attack techniques in our taxonomy, three violate just the confidentiality or privacy of the session: traffic analysis, passive eavesdropping, and active eavesdropping. 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.

ISBN 555555555/$10.00 © 2003 IEEE

Proceedings of the 2003 IEEE
Workshop on Information Assurance
United States Military Academy, West Point, NY June 2003

II. THREATS

In this section we describe seven 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 know about, hence we do not feel it worth discussing here.

A. Traffic Analysis

Traffic analysis is a simple technique whereby the attacker determines the load on the communication medium by the number and size of packets being transmitted, the source and destination of the packets and the type of packets. The assumption is that the payload of the packets is encrypted and the attacker cannot decrypt the payload. This leaves only the header and any trailer information visible to the attacker. 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. It has been 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. [2]

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. 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 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, type 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.

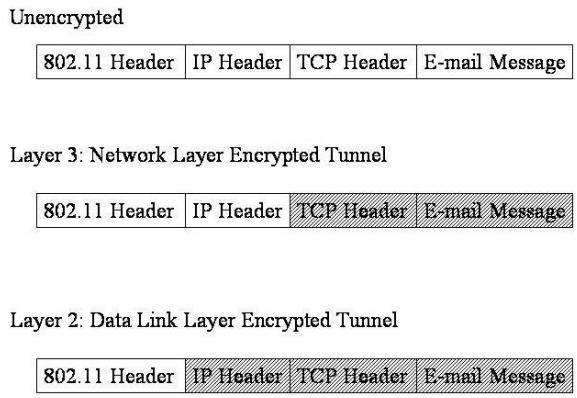

Figure 1: Layer Encryption

ISBN 555555555/$10.00 © 2003 IEEE

Most encrypted tunnels are implemented at layer 2 or layer 3. This leaves the header information exposed for the implementation layer and all lower layers as illustrated in Figure 1. The attacker can identify the source and destination by MAC address when layer 2 encryption is employed. Layer 3 encryption leaves the IP addresses of the sender and receiver open for viewing. In most cases the type of traffic is evident from reading the layer 3 header.

B. Passive Eavesdropping

In this attack the attacker passively monitors the wireless session (Figure 2) and the payload. If the payload is encrypted, this includes breaking the encryption to read the plaintext. The only precondition is that the attacker has access to the transmission. As described in the previous section, 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. [1]

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 that not only is the privacy of the information compromised, but the information gleaned is an important precondition for other, more damaging attacks.

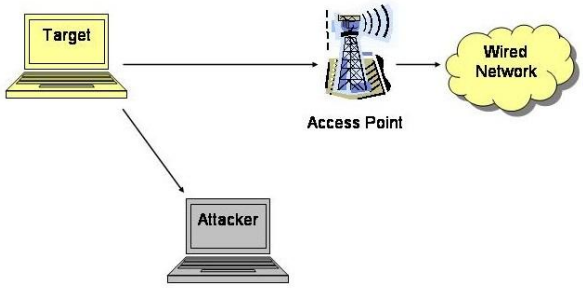

Figure 2: Passive Eavesdropping

If the session is encrypted at layer 2 or higher using a protocol such as Wired Equivalent Protocol (WEP) or the Advanced Encryption Standard (AES), then in order to read the data the attacker has to decrypt the packets. [3][4][5][6][1][7][8][9]

Passive eavesdropping requires reading the payload of the packets. Stream ciphers, like WEP are vulnerable to a number of passive attacks. WEP is particularly vulnerable because if its small Initialization Vector and poor stream cipher implementation. [10] [11] [5] Because of the finite number of initialization vector (IV) sequences, WEP's reuse of the IV makes it susceptible to attack. Rapid rekeying and other modifications make stream ciphers less vulnerable, but with a stream cipher it is always a race between the attacker and defender. Block ciphers such as AES or 3DES are a much stronger form of encryption. Currently there are not any public practical attacks on these encryption techniques. From a practical point of view passive eavesdropping is only possible against unencrypted and stream cipher encrypted packets.

C. Active Eavesdropping

The active eavesdropping technique involves the attacker injecting data into the communication to help decipher the payload. The attacker monitors the wireless session as described in passive eavesdropping. 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 her in determining the contents of messages. The preconditions for this attack are that the attacker has access to the transmission and has access to either part of plaintext such as a destination IP address or the contents of the entire payload.

Active eavesdropping attacks can take two forms: the attacker can modify a packet or can inject complete packets into the data stream. 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 she controls. The access point does the decryption prior to forwarding the altered packet on to the attacker's host. 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.

For more details on how the CRC-32 integrity checker is vulnerable see Borisov, Goldberg and Wagner's papers. [11] [9] [4] [5]

ISBN 555555555/$10.00 © 2003 IEEE

Using the weaknesses in WEP and other stream ciphers, the attacker can inject known traffic into the network in order to decrypt future packets sent by others. For example, if the attacker is an insider and sends an email message destined to their own computer on the wireless LAN or to the victim, 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 where C is ciphertext and P is plaintext,

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

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.

D. 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 on the WLAN. 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 based man-in-the-middle attacks.

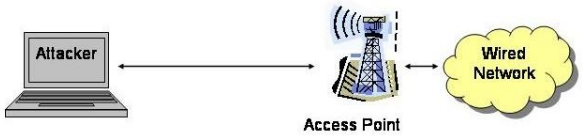

Figure 3: Unauthorized Access

Due to the physical properties of WLANs, attackers will always have access to the wireless component of the network (Figure 3). 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

E. Man-in-the-middle

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, or replay attacks.

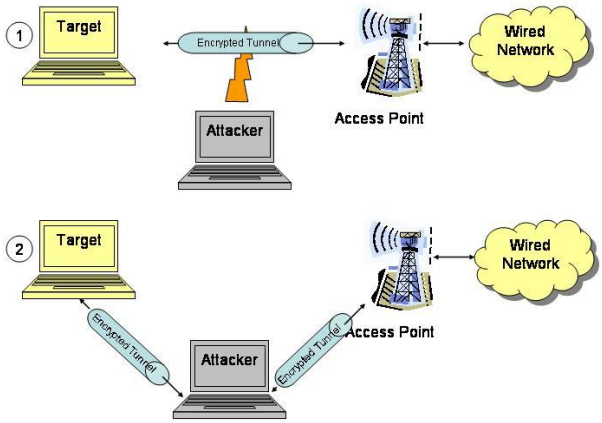

Figure 4: Man-in-the-middle Attack

A man-in-the-middle attack (Figure 4) 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 attacker will know the contents of the message prior to the intended recipient receiving it, or change the message en route.

There are multiple ways to implement this attack. One example is when the target has an authenticated session underway. Figure 4**Error! Reference source not found.** illustrates this type of attack technique. In step one, the attacker breaks the session and does not allow the target to re-associate with the access point. In step two, the target machine attempts to re-associate 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. [12] [4] [8] [9]

Variations on this attack technique are based on the security mechanisms employed. The more security mechanisms in use the more security mechanisms that the

ISBN 555555555/$10.00 © 2003 IEEE

attacker will have to subvert when reestablishing the connection with both the target and the access point. 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. 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. Since 802.11 authentication is not mutual between the access point and the client, and the default encryption (WEP) is easy to crack, man-in-the-middle attacks are somewhat trivial on 802.11 networks.

Address Resolution Protocol (ARP) attacks are a particularly dangerous 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. The ARP attack differs from the other attack techniques in that the 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 analyzing authorization technologies. [12] [9] [13] [5] [14] [15]

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. [16] [17] [18]

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 below in Figure 5 where an attacker on a wireless client has access to sessions between two wired hosts.

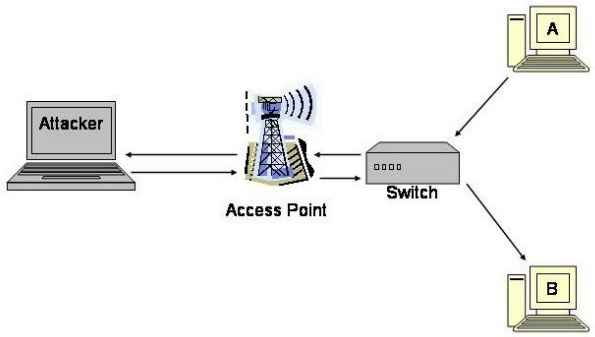

Figure 5: ARP Attack

Denying this attack technique is an absolutely vital step in designing the security architecture. Denying 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.

F. 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 6 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. [14] [13] [19]

ISBN 555555555/$10.00 © 2003 IEEE

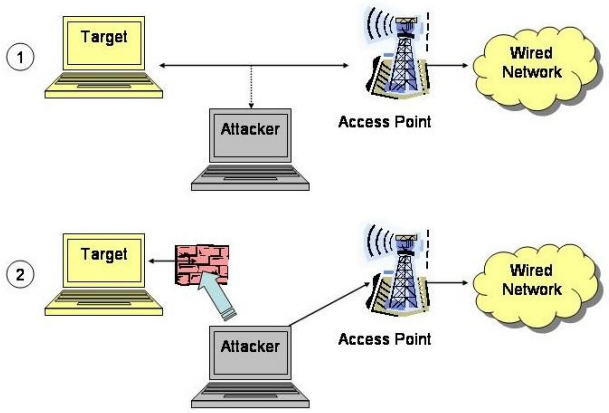

Figure 6: Session Hijacking

G. 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).

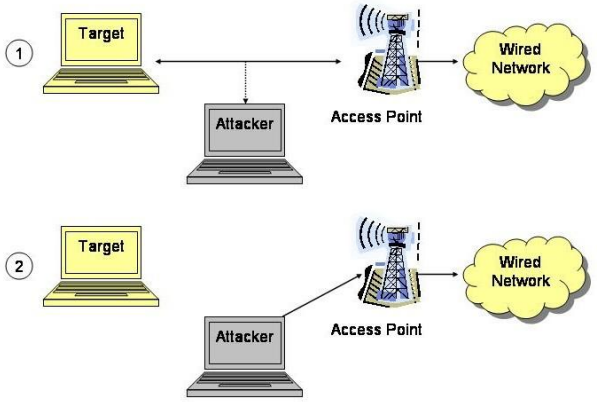

Figure 7: Replay Attack

In a replay attack (Figure 7), the attacker captures the authentication of a session or sessions. The attacker then either replays the authenticated session at a later time or uses multiple sessions to synthesize the authentication part of a session. Since the session was 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. [20] [5] [4] [7] [21]

III. Counter Measures

To mitigate the risks from these attack techniques a security architecture must have four components: mutual authentication, block cipher encryption of the payload, strong cryptographic integrity protection and a firewall between the wireless and wired components of the network. The absence of any one of these components leaves the WLAN open to attack through well-known attacks.

Mutual authentication means that both the client and the access point authenticate each other. The access point knows that it is opening a session with an authorized client and the client knows that it is opening a session with a legitimate access point. Authenticating the access point stops man-in-the-middle attacks. Strongly authenticating the client makes replay and session high-jacking attacks more difficult.

Block cipher encryption of the payload stops passive eavesdropping attacks. Depending on the implementation it also makes many other attacks more difficult. Another important aspect of the encryption is the layer at which the packets are encrypted. Layer 2 encryption limits traffic analysis while layer 3 is more flexible. Layer 2 encryption also makes active eavesdropping attacks much more difficult. If the implementation and configuration is sound, replay and session high-jacking attacks become very difficult.

Strong cryptographic integrity verification is the key to stopping active eavesdropping. It also plays an important role, along with payload encryption, in stopping replay and session high-jacking attacks.

A firewall that stops all network traffic from unauthenticated clients from reaching the wired network is absolutely critical to a secure architecture. By not stopping unauthorized access ARP attacks are possible all the way back to the first router in the wired network. ARP attacks are a form of man-in-the-middle attacks; as such they can affect the integrity of the information and are devastating.

These components, properly implemented and configured, will result in a wireless network component that offers little to no additional threat to the network as a whole. Neglecting any one of these components exposes the network to a significant increase in risk.

ISBN 555555555/$10.00 © 2003 IEEE

IV. Conclusion

In this paper we did not address denial of service attacks on wireless networks. Interfering with a wireless transmission is very easy to do and difficult to stop. An attacker with a stronger transmitter or advantageous location can cause significant availability problems. Mitigating these risks is far beyond the scope of this paper. Because management packets in 802.11 are not authenticated, even a weak transmitter can broadcast forged *disassociate* packets and keep legitimate users off the network.

Another key aspect that we did not address is key distribution. The encryption keys for the authentication and the payload as well as the actual authentication keys themselves must be available to all participants. Problems with key distribution can undo all the security effort put into designing a secure architecture.

That said, we have described a simple taxonomy for attack techniques that can be used to construct all the well-known wireless attacks. By understanding these seven attack techniques and using them to analyze a wireless security architecture, the network designer can understand the risk and take the proper mitigation steps.

By using this taxonomy we determined that the minimum components of a secure WLAN architecture include at firewall between the wireless and wired components of the network, private mutual authentication, block cipher encrypted payloads (preferably at layer 2), and strong cryptographic integrity checking. We used this taxonomy in designing the West Point wireless network component. The wireless component first phase includes seven buildings, 369 access points and will eventually grown to 5,000 users. It meets the DoD policy for secure unclassified wireless networks.

V. References

[1] 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.
[2] 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.
[3] 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.
[4] Moioli, Fabio, Security in Public Access Wireless LAN Networks, Masters Thesis, Department of Teleinformatics, Royal Institute of Technology, Stockholm, Sweden. 12 June 2000.
[5] 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.
[6] 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.
[7] Chickinsky, Alan, Wireless LAN Security Threats. Document IEEE 802.11-01/258
[8] 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.
[9] 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.
[10] 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.
[11] 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.
[12] 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.
[13] 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.
[14] 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.

ISBN 555555555/$10.00 © 2003 IEEE

[15] 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.
[16] 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.
[17] 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.
[18] Carey, Allan, Wireless Security Vulnerabilities continue to Surface: Cigital Identifies the Latest. White Paper by Cigital, Inc. http://www.cigital.com. October 2001.
[19] 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.

[20] 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.
[21] 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.

ISBN 555555555/$10.00 © 2003 IEEE