By Russ Housley and William Arbaugh

Security Problems in 802.11-Based Networks

Assessing inherent wireless network security deficiencies and seeking solutions.

Wireless local area networks (WLANs) have quickly become extremely popular. Enterprises and homeowners are avoiding the expenses and delays associated with installing wired networks. Travelers are enjoying high-speed Internet access in airports, hotels, and coffee shops worldwide. The number of these hotspots providing Internet connectivity is increasing, and many travelers are insisting on accommodations that provide WLAN services. The IEEE 802.11 series of standards define WLANs, and they are providing increasingly higher access speeds with each generation. Initially, wireless stations had a top speed of about 1Mbps; today, wireless stations have a top speed of 54Mbps. Draft standards are becoming stable that will allow even faster speeds.

Along with the increases in throughput, WLANs remain unlicensed and affordable. This combination of features has created exponential growth in the deployment of WLANs in businesses, homes, communities, and open spaces. This feature combination could allow WLAN technology to either replace 4G initiatives, or augment 4G with hotspot coverage.

Unlike wired networks, WLANs provide the transmitted data to anyone with a receiver that is in radio range. With the use of directional antennas, an adversary wanting to eavesdrop on communications can be quite far away. As a result, one must consider WLAN traffic as being delivered to the adversary as well as the intended party, and the adversary with a transmitter has the ability to inject or forge packets onto the network. This is a fundamental difference between wired and wireless network security.

Overview of Wireless LANs and WEP

An IEEE 802.11 WLAN is a group of stations (wireless network nodes) located within a limited physical area, where each station is capable of radio communication with a base station. There are two WLAN design structures: ad hoc and infrastructure networks. The vast majority of installations use infrastructure-based WLANs.

An ad hoc WLAN has no ability to communicate with external networks without using additional routing protocols. An ad hoc WLAN is normally created to permit multiple wireless stations to communicate directly with each other, requiring minimal hardware and management.

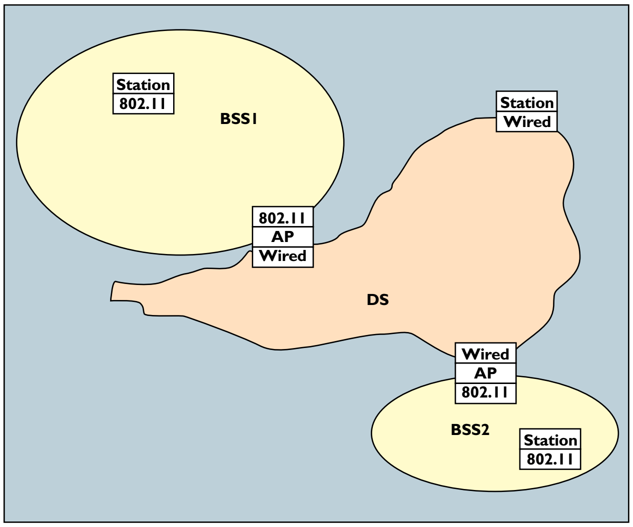

Figure 1. Typical WLAN configuration.

An infrastructure-based WLAN is composed of one or more Basic Service Set (BSS). Each station has exactly one BSS link connecting it to the infrastructure, the Distribution System (DS), which allows access to external networks. The station's attachment point to the DS, called the Access Point (AP), relays packets from the stations within the BSS to the DS as shown in Figure 1.

This relaying of traffic means that an adversary has additional opportunities to intercept traffic. In Figure 1, the traffic can be captured by radio receivers in BSS1 or BSS2, as well as by sniffers in the wired network. Stations communicate packets called media access control (MAC) service data units (MSDUs). When transmitting data, the MAC layer determines whether the data in the MSDU needs to be partitioned into smaller fragments or MAC protocol data units (MPDUs). When receiving data, the MAC layer determines whether the MPDU is a fragment that requires reassembly. Each MPDU includes a frame check sequence (FCS); a CRC-32 computed over the MPDU. The MAC uses the FCS to ensure the received frame arrived intact.

Prior to communicating, a station must associate with an AP. The IEEE 802.11 standard supports some optional authentication as part of association. Shared authentication uses a challenge and response exchange along with a shared secret to authenticate the station to the AP. Unfortunately, this authentication is easily compromised.

The IEEE 802.11 standard does not specify a means for obtaining the shared secret. The shared secret is typically a 40-bit key or a 104-bit key shared between many stations. A key shared between the AP and many stations is called a default key. A key shared between the AP and only one other station is called a key-mapping key. Both default keys and key-mapping keys are subsequently used to protect communications between associated stations.

The Wired Equivalent Privacy (WEP) protocol is used to protect MPDUs. WEP uses the default key or key-mapping key and the RC4 algorithm for encryption, and it uses CRC-32 to compute an Integrity Check Value (ICV) over the MPDU data. The resulting 32-bit ICV is appended to the MPDU prior to encryption. The RC4 key is composed of a 24-bit Initialization Vector (IV) value concatenated with the default key or key-mapping key to form a per-packet key. The MPDU data and ICV are then encrypted under the per-packet key. The IV and a key identifier are prepended to the encrypted MPDU data field, forming the complete WEP Protocol data unit as shown in Figure 2a.

WEP has critical security flaws, as published in [3] and [4]. The flaws are the result of incorrectly using the RC4 stream cipher and poor choice of CRC-32 as a data integrity algorithm. These flaws and remedies for them are discussed in the article "Security Flaws in 802.11 Data Link Protocols" in this section.

Wireless LAN Problems

One of the goals of the current WLAN standard was to provide security and privacy that was "wired equivalent," and to meet this goal the designers implemented several security mechanisms to provide for confidentiality, authentication, and access control. Unfortunately, all of these mechanisms were demonstrably broken [1–3, 4, 6].

Identity in WLANs. An essential element in any security architecture is a robust and non-malleable identity. Without a reliable form of identity, malicious outsiders can potentially masquerade as valid users. In WLANs, the MAC address of the WLAN card is used as the only form of identity for both devices and users. In the early versions of the device drivers for WLAN cards, the MAC address was not changeable by the user (even though the card contained the capability to change its address). But, most open source device drivers now allow the user to change the MAC address.

Access Control. Access control is the process that limits those that can utilize a system resource. As such, a good access control mechanism is like a reliable doorman who only lets the occupants (and their visitors) into a building, preventing all others from entering. There are two major forms of access control used in current WLAN equipment: access control lists, and a proprietary "closed network" mechanism.

While the WLAN standard does not include an access control mechanism, most vendors have embraced the use of a MAC-address-based access control list (ACL). An ACL is essentially a lookup table based on the identity (in this case the MAC address) that indicates what resources the specific identity is permitted to use. In a WLAN, the only resource is use of the network. Thus, the MAC ACL lists the MAC addresses with permission to use the network. If the MAC address does not appear in the list, then the unlisted station is not permitted to use the network.

This is one of the places where a malleable identity creates a problem. Since the MAC address can be changed at will, an attacker need only eavesdrop or sniff the wireless network to identify those MAC addresses that are permitted access (the MAC address is always transmitted in an unencrypted form, even if WEP is used). Once an authorized MAC address is identified, the attacker need simply change their card to the same address—now the attacker's traffic will be permitted by the ACL of the access point.

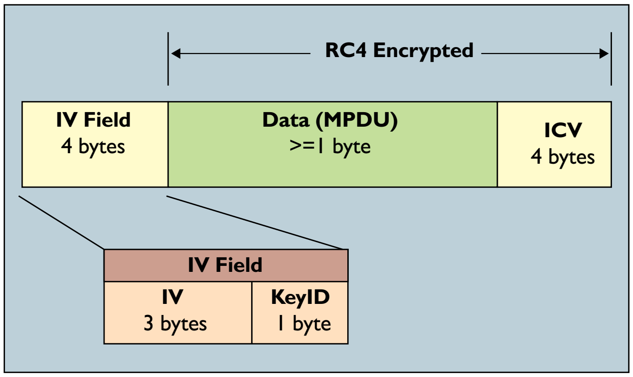

Figure 2a. WEP Protocol data unit.

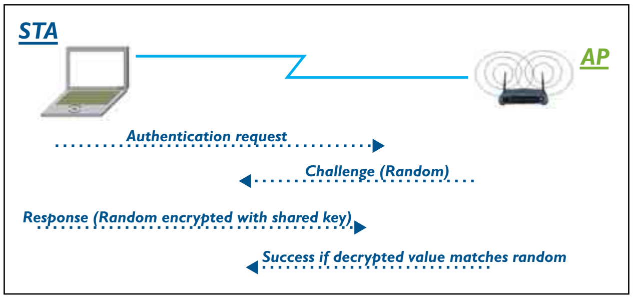
STA
AP
Authentication request
Challenge (Random)
Response (Random encrypted with shared key)
Success if decrypted value matches random

Figure 2b. Shared key authentication.

The second form of widely used access control is the "closed network" approach. In this case, the user must present a secret to the access point to gain access—generally a reasonable method of access control—provided the secret remains so. Unfortunately in the closed network approach, this is not the case. The string used as the shared secret is actually the BSS or network name, and this name is broadcast in the clear in several management frames during the course of normal WLAN operation. As a result, once again the attacker need only "sniff" the network to gain enough information to use the network resources. Note that even disabling the broadcasting of the network name in the "beacon" management frame does not prevent an adversary from learning the network name as it also appears in the "probe request" and "probe response" management frames.

Authentication. The current WLAN standard includes two forms of authentication: open system and shared key. The open system authentication is a null authentication process where the station, or client, always successfully authenticates with the access point, that is, the access point permits everyone to authenticate successfully.

The second authentication method utilizes a shared key with a challenge and a response. The authentication process uses four messages as shown in Figure 2b. The station requests authentication using a shared key, and the access point responds with a 128-byte randomly generated challenge. This value is sent back to the requesting station. Upon receiving the challenge, the station encrypts it using the shared key and the RC4 encryption algorithm, returning it to the access point. The access point decrypts, using RC4 and the shared key, the encrypted response from the station, and then checks to see if the decrypted value matches the random value sent in the second message. If it does, the station is authenticated; otherwise, authentication fails.

The problem is that an attacker eavesdropping on this process can collect both the plaintext (the random challenge) and the corresponding ciphertext (the encrypted response). This provides sufficient information to the attacker (the pseudorandom key stream produced by RC4) to respond to all random challenges sent (by XORing the pseudorandom with the challenge simulating RC4 encryption), and authenticating successfully.

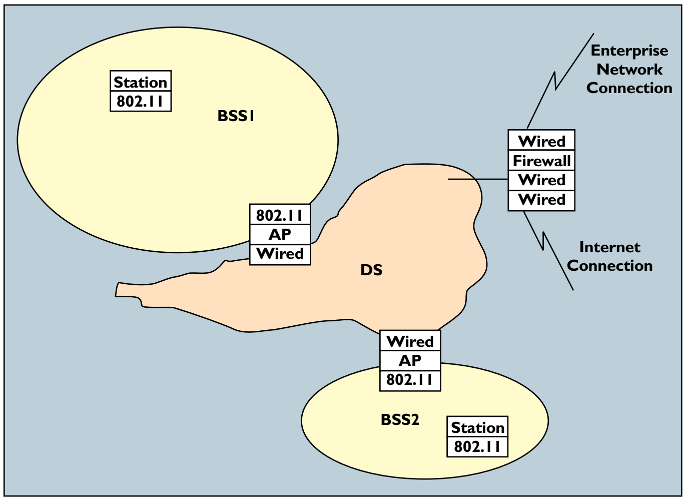

Figure 3. Place WLAN connections outside the enterprise firewall.

Existing Equipment. Given all of these problems with equipment built to current IEEE 802.11 standards, is there any way to safely use it? Yes, in many situations, but not all situations. Care must be taken to ensure the WLAN does not offer a way to bypass enterprise firewalls. If WLANs are treated the same as wired LANs, then stations are inside the firewall. Since today's equipment cannot keep outsiders from connecting to an enterprise WLAN, the WLAN itself should be placed outside the firewall. In this way, WLAN stations are treated like any other Internet host.

While WLAN stations cannot access enterprise resources, the WLAN can be used by outsiders to access the Internet. Adversaries may use the free bandwidth to launch attacks on other enterprises. This can be thwarted by employing a firewall with more than two ports. One port connects to the enterprise network, a second port connects to the Internet, and additional ports connect to WLANs. In this way, the firewall policy will determine which WLAN stations can access the Internet as well as the enterprise network. Figure 3 illustrates this architecture.

Virtual Private Networks (VPNs) offer a solid solution to many security issues, where an authenticated key provides confidentiality and integrity for IP datagrams. WLAN stations are treated similarly to dialup stations. First the user is authenticated, and the key is established. Then, the key is used to encrypt and integrity protect the IP datagrams. Software is readily available to implement VPNs on just about every platform. Deployment of VPNs is not always easy. While the software is getting better with each release, authentication depends on at least one of three factors: something you know (such as a password); something you have (such as a security token); something you are (such as your fingerprint). Using more than one factor is desirable, and using all three is the most secure. However, each factor comes with some administrative burden. This burden is excessive if the VPN software vendor has not already integrated the user authentication technique.

VPNs are not a ubiquitous solution. They only support the IP suite. If the protocol environment does not make use of IP datagrams, then a VPN will be difficult (or impossible) to deploy. In some cases, tunneling can be used to encapsulate non-IP traffic in IP datagrams prior to VPN processing.

Conclusion

The cryptographic security in the IEEE 802.11 standard is flawed. The standards is addressing these concerns, and while waiting for the standards committee to complete their work, many of these concerns can be addressed at the IP layer with a VPN [5]. However, a VPN is not a viable solution in networking environments that do not use IP. Furthermore, stations and access points are identified by MAC addresses. This is an appropriate name, but it must be coupled with an authenticator. The authenticator should be used in a robust authentication protocol to validate the claimed identity. Unlike the current protocol, the identities of both parties should be validated.

References

1. Arbaugh, W.A. *An Inductive Chosen Plaintext Attack Against WEP and WEP2.* IEEE 802.11 Working Group IEEE 802.11-01/230; www.cs.umd.edu/~waa/attack/frame.htm, 2001.
2. Arbaugh, W.A., Shankar, N. and Wan, Y.J. Your 802.11 wireless network has no clothes. In *Proceedings of the First International Conference on Wireless LANs and Home Networks* (Singapore, 2001), 131–144.
3. Borisov, N., Goldberg, I., and Wagner, D. Intercepting mobile communications: The insecurity of 802.11. In *Proceedings of the International Conference on Mobile Computing and Networking* (July 2001), 180–189.
4. Fluhrer, S., Mantin, I., and Shamir, A. Weaknesses in the key schedule algorithm of RC4. In *Proceedings of the 4th Annual Workshop on Selected Areas of Cryptography*, 2001.
5. Frankel, S. *Demystifying the IPsec Puzzle*. Artech House, Boston, MA, 2001.
6. Walker, J. *Unsafe at any key size: An analysis of the WEP encapsulation.* IEEE 802.11 Task Group E IEEE 802.11/00-362; grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip.

Russ Housley (housley@vigilsec.com) is the founder of Vigil Security in Herndon, VA.
William Arbaugh (waa@cs.umd.edu) is an assistant professor at the University of Maryland at College Park.