ADITYA K SOOD

hacking 802.11 protocol insecurities

Aditya K Sood, a.k.a. oknock, is an independent security researcher and founder of SecNiche Security, a security research arena. He is a regular speaker at conferences such as XCON, OWASP, and CERT-IN. His other projects include Mlabs, CERA, and TrioSec.

adi.zerok@gmail.com

SECURITY AND PRIVACY ARE TWO CRIT- ical entities in any communication protocol. Security itself is a prerequisite for robust implementation of networks. In this article, I dissect the 802.11 [1] protocol attacks possible because of persistent problems in wireless networks. Before going into the attack patterns against the protocol, I will briefly describe how 802.11 works by splitting frames into functional objects.

The protocol is constructed to work between access points and stations. Every second (unless disabled), the access point transmits a signal in the form of wireless messages called beacons. The station listens for beacons on different frequencies called channels. Stations can also uses probe request messages to scan a certain network for finding an access point. This probing and beaconing initiates the association between a station and an access point. An association message is used for initial connection by using a request/response mechanism. Similarly, a dissociation method is applied for connection termination. The frames-based IEEE 802.11 Frame Format is used for sending data (Figure 1). Three types of addresses are used for sending data. The Service Set Identifier (SSID) [1] is defined for networks to uniquely identify various access points. The identification process is completed by sending a Preamble as a first element of the frame. The PLCP header holds information regarding receiver logic (data rate, etc.). The MAC header is used for address specification. The user data is checksummed (CRC) for transmission and reception errors.

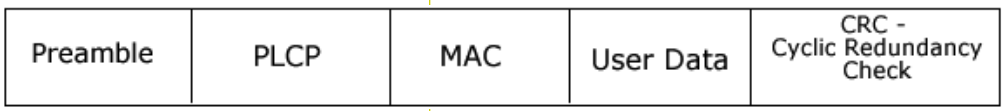

FIGURE 1: IEEE 802.11 STANDARD FRAME FORMAT

The access points can communicate wirelessly with other access points by using a process called wireless bridging. The Media Access Control uses four different types of addresses to complete the protocol communication. Transmitter Address (TA), Receiver Address (RA), Source Address (SA), and Destination Address (DA) comprise the 802.11 communication address pattern. The MAC frames are dissected into three main categories: control,

data, and management. The working functionality of the protocol revolves around this. Insecurities define the domain over which an attack occurs. The size of the attack surface increases with the number of insecurities in the 802.11 protocol. Attacks can be split into a logical hierarchy, shown in Figure 2.

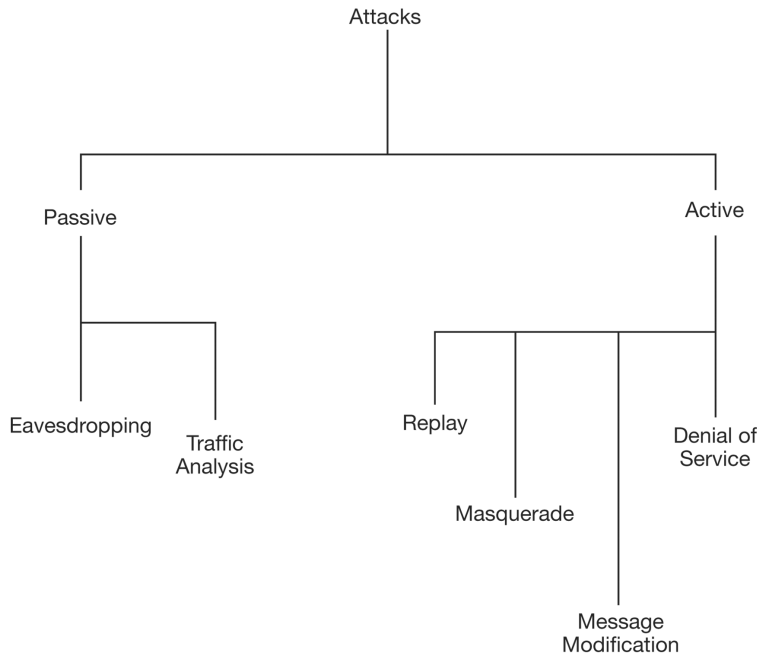

FIGURE 2: HIERARCHY OF ATTACK TYPES

Protocol Insecurities

MAC DISCLOSURE

One of the most insecure vectors in 802.11 is the public display of the MAC [2] address, which is a prime cause of spoofing attacks and traffic manipulation. 802.11 defines MAC operations in contention-free and contention-based modes. The term *contention* here means the procedure the station uses to communicate with an access point or media. Hijacking attacks take over a connection by masquerading the MAC address of a station. MAC relates to security context directly. ARP poisoning attacks are possible through man-in-the-middle techniques. These attacks are based on sniffing the network traffic. An attacker can easily change the MAC address of the devices under control. In this way an attacker performs the man-in-the-middle attack. On a shared network, it is possible to coexist with different hosts while having the same IP and MAC address, a state called piggybacking. The attacker must be very cautious in sending the packets in the network, because too many reset packets or ICMP unreachable messages can cause problems in the wireless network, resulting in network instability. A WIDS (Wireless Intrusion Detection System) catches the culprit host in the network when an attacker tries to kick the victim host out of the network. To overcome this

problem attackers try to find a host that is active in the network but does not generate traffic. This results in virtual control of a host, because the attackers change their identity by transforming the identity addresses, thereby sending deassociate frames to the victim host. This process is considered to be silent control of the host. The network is flooded with deassociate frames that are continuously sent to the victim host by the attacker by spoofing the MAC address of the access point. In Linux the MAC address can be changed easily during boot time or with an efficient utility called sea [3]. It directly configures the adapter with the type of MAC address specified by the attacker. In a Windows environment the MAC address can be altered easily by changing the registry settings.

WEP INSECURE VECTORS

The Wired Equivalence Privacy (WEP) [4] is a security-driven mechanism used for wireless network security. The authentication is based on a challenge–response mechanism (Figure 3). The basic problem is that using the same keys for encryption and authentication breaks the rule of independent keys. Authentication covers the simple encryption and decryption check of a random number string. Another problem is preserving identity, as no tokens are used for transactions. The double XOR operation on a pseudo-random string with plain text enables an attacker to bypass the authentication mechanism easily without even knowing the secret key. This ambiguity marginalizes the security of networks substantially. Specifically, no standard method is defined for access control—it is entirely based on MAC list generation in which allowed targets are specified. Failure of identification by MAC or WEP key causes direct access failure and no connection. Another problem associated with WEP is that no particular method is provided to combat against replay attacks. The MAC address of the victim can be used to resend messages to an access point, which automatically decodes it since no subtle protection is provided to scrutinize replay requests.

Let's look at the mechanism of shared key message authentication flow for a better understanding.

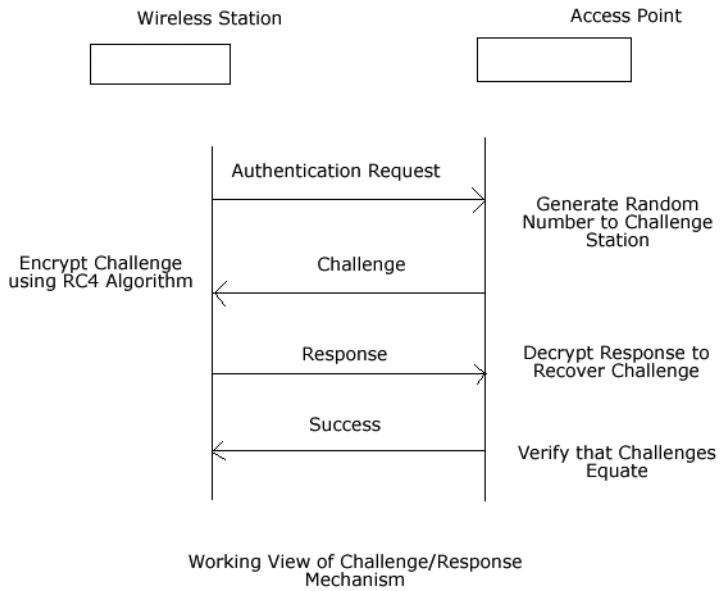

FIGURE 3: WEP CHALLENGE-RESPONSE AUTHENTICATION SEQUENCE

WEP uses a linear method to compute a cyclic redundancy check. An assumption has been made that if a message is computed with a CRC value and is encrypted, then data modification attacks can be circumvented. But this is totally false. Flipping a bit in the original message always shows the same flipping effect in the encrypted message. WEP is unable to prevent cipher text modification attacks. Message privacy can be bypassed easily through brute-forcing attacks on WEP keys or generating techniques to decode a message. As per standards it has been noticed that the 40-bit WEP key generation algorithm is vulnerable to a number of flaws, as a result of which brute-force attacks on 40-bit keys are easy to perform.

The attacks on WEP are classified as either passive or active. Passive attacks comprise attacks that are performed on the static log files, debug responses, etc. The FMS [5] technique is one of the finest key-recovery procedures. Attackers use this procedure effectively to crack keys in a static manner. Active attacks comprise injecting extra traffic in the network to crack keys within specific time limits. The injection of traffic accelerates the WEP-cracking process. Active attacks are possible despite less traffic. The injected traffic by the attacker not only enhances the cracking process but is also helpful in understanding protocol structure, which further results in host discovery and enumeration. It works on low-level protocol structure and analyzes the flags sent in TCP and ICMP protocols. So once an attacker understands the required pattern of traffic, the attacks become easy to perform.

IMPLICIT DENIAL OF SERVICE

Wireless networks are prone to different types of denial-of-service attacks.

Clear to Send (CTS) and Request to Send (RTS) are control type frames. The RTS operation comes into play whenever a big packet is to be sent with continuous transmission. To avoid collision the station sends an RTS packet to an access point for reserving a channel for some time. If the access point agrees, a CTS packet is sent to the station in return. The client is unable to use the CTS packet because of the hidden-node problem. Attackers exploit CTS packets by continuously injecting them in the network to produce a denial-of-service attack. This reduces the robustness of the network, thereby resulting in service degradation.

The second factor involves communication failure between two hosts that are communicating on a connection-oriented basis; if a link fails in the connection-oriented protocol there should be retransmission of packets. This process is continuous until the whole datagram is passed to the destination. As a result of this the number of optimum packets is increased and so are the frames used to capture it. On the other side, if the frame size is decreased to reduce the incoming packet data to be sent, the problem persists because this enhances the fragmentation process in the network. Either way, a small mismatch in the network can cause large problems in the network.

The third factor that can lead to a denial-of-service attack is link disruption, which generates an excessive amount of traffic, which in turn generates routing updates. This type of problem persists in wireless networks when routers go down. If a router stops working, then a flood occurs that generates new data for the link state protocol. This means that the algorithm used in routing updates triggers with new data routes. As a result, load rises and network time is spent in overcoming this problem. If this process becomes periodic, then the routes are affected continuously, marking those specific routes as flapped. Distance vector protocols such as RIP/IGRP generate traffic regularly, but because of link failure produce a flood of regular updates.

An attacker can easily exploit any of these three factors to disrupt the functioning of a wireless network. None of the solutions to combat these factors is very reliable, because the root cause of these problems is protocol malfunctioning, which in itself entails technology manipulation.

The 802.11 insecurities are enumerated as follows:

- Tempering VPN tunnels: Virtual private networks are implemented with PPTP [6] and IPSEC. Attackers can easily attack PPTP to leverage a lot of information directly from the traffic flow. The technique is based on the concept of a falsified parameter. The attacker sniffs the traffic and tries to understand the packet layout used in communication. Basically, the attacker wants to control the authentication mechanism between the VPN server and the client. As we already know, PPTP implements MSCHAP [7] and MSCHAP-2 [6], the Microsoft Challenge Handshake Protocol for password authentication and password change protocol. Software has been designed by attackers to control the authentication credentials by a fake process. Attack software actively monitors the traffic and detects when a client tries to log onto a server using PPTP. The software activates a false dialog and tricks the user into providing credentials (a man-in-the-middle attack). An amateur user simply provides the credentials, which in turn are replayed by the attacker on the server.
- Once the MSCHAP hashes are sniffed, they can be cracked to produce a clear text password. Tools such as Ettercap with plug-ins can perform this task in an efficient manner.
- IPSEC attacks: Another possible attack target is IPsec. The attacker scans the whole wireless network against the IPsec implementation. With the help of denial-of-service attacks, the culprit can force the network administrator to shut down the IPsec implementation for some time. Actually, the IPsec concept is based on Internet Key Exchange (IKE), in which IKE scanners find the vulnerable host and compromise it by successfully running exploit code.
- Rogue access points: Rogue access points are used to attack wireless networks that use the EAP-MD5 authentication mechanism. For this an attacker requires a fake RADIUS [8]. RADIUS will provide fake authentication credentials to the client host. This is also considered a man-in-the-middle attack. A single machine can easily provide a base for both access point and RADIUS. Because of this stringent problem most administrators have started using the EAP-MD5 solution as a fallback only. The attack becomes more subtle when the attack starts jamming the real access point signals and injecting its own access point signals to a network a number of channels away. This gives the attacker hidden control over the network. Such jamming is possible by junk traffic being sent to the network with the help of tools that manipulate layer 1 functionality of the OSI model. Parameters used for the rogue access point should be similar to real ones, to avoid conflicts in the network. The layer 2 attacks are performed by sending deassociation and deauthentication packets to the victim to kick it out of the network. An attacker performs layer 1 and layer 2 attacks frequently and in a defined manner to exploit the functionality of rogue access points. This problem is inherited in wireless networks because of its open access point methodology.
- WPA insecurity context-cracking: Wi-Fi Protected Access (WPA) is a subset of the Robust Security Network (RSN) [9]. It defines the protected access mechanism in the form of the encryption protocol that is deployed in 802.11 wireless networks. Its running structure is differ-

entiated between home mode and enterprise mode. Home mode uses a Pre-Shared Key (PSK) and enterprise mode uses a RADIUS server for authenticating clients. A Pairwise Master Key (PMK) is computed from PSK and SSID. A hashing function is used for generating PMK. Precomputed hash attacks can easily be applied to crack the hashes. It works very effectively on WPA1 and WPA2 because both versions use four-way handshake mechanisms for association. The packets can be easily decrypted by hardware-based tools that accelerate the cracking process. The Extensible Authentication Protocol (EAP) [10] and Protected EAP (PEAP) [11] are very hard to exploit, because the working algorithm used is RSA. EAP is based on certificate exchange between server and client. The only method to compromise it is to steal the keys to control EAP on the network.

Overall Countermeasures

- Understand the organizational requirements. Normally, several layers of network protection are added (e.g., multiple authentication) to prevent attacks. How many layers depends a lot on the need of the organization and the physical structure of the network. If an organization plans on communicating financial transactions then it must be assured that a hacker will not be able to intercept the traffic and steal the credentials. If remote working is required then VPN solutions are advised. The network should be constructed in a simple manner, enabling the administrator to control and maintain the wireless network efficiently.
- Apply encryption in multiple layers. The main stress should be laid on the generation of WEP keys per user per session. This means users will encounter different WEP keys for every session they establish, thereby lowering the possible theft and reuse of the WEP keys because an attacker can benefit only when a user is active. Once the user closes the session the keys become useless. This technique is implemented with LEAP [4]. The number of packets encrypted with a LEAP-generated key is much lower than the number of packets required to break the algorithm. This type of encryption not only provides a secure mechanism but also an interoperable environment.
- Design VLANs as a backbone to wireless networks. In such a design, the access points are connected to the wired network physically or logically. This can be accomplished by setting a separate switched network, which is possible with VLANs. The administrator sets a VLAN device behind the firewalls. It enables the firewalls to filter the wireless traffic that is coming inside and leaving the network. Multiple layers of security can be added with extra features by enabling security devices.
- Alter the default setting of various network parameters and protocols to unique values. First, the default passwords should be changed. The SSID value must be changed to something different from the factory value. Second, change the cryptographic keys provided by the manufacturer for shared key authentication. Most wireless networks use SNMP agents. The default SNMP parameters should be changed. The default channels of access points should be set differentially to reduce conflict between two networks. The overall change in default parameters is advised to reflect specific organizational policies.
- Apply patches as soon as a vulnerability is released. This process should encompass every single item of hardware and software used in the network design.

- Apply security at the perimeter level. This includes the implementation of firewalls, WIDS, and other devices in switched networks. These devices provide physical layer security and work on defined policies. Actually, signatures and rules filter the traffic on the inherited benchmarks, thereby reducing the attack vector from the security point of view. These devices are considered as the default layer of security.
- Design and implement MAC access control lists to circumvent MAC attacks. These lists have predefined MAC addresses that are to be given access in the network by the administrators. The access lists use the grant and permit operation to perform in the wireless network. But the MAC address is distributed in a clear text so that it can be captured easily. For normal networks the MAC access control list can be implemented to reduce the intensity of attacks based on MAC.

These countermeasures can control wireless network attacks to some extent but cannot be considered as direct solutions for wireless security.

Conclusion

These issues with the IEEE 802.11 protocol lead to the hacking of networks. The various insecurities generate a large attack surface and defenses can be breached very easily. You can prevent attacks to some extent but you cannot eliminate them. The many countermeasures listed strengthen the security aspect up to a point but cannot make your network bulletproof. The basic problem resides in the presence of the complexity endemic to protocol requirements in wireless networks. Security is a process, not a one-shot activity. Implementing heavy security entails looking at the hidden artifacts in the network to dethrone concurrent attacks.

REFERENCES

[1] E. Danielyan, "802.11," *The Internet Protocol Journal*, 5, 1 (March 2002).

[2] "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY)Specifications," IEEE Standard 802.11, 1999 Edition.

[3] http://www.openbsd.org.

[4] N. Borisov, I. Goldberg, and D. Wagner, "Security of the WEP Algorithm," http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html.

[5] http://www.cs.umd.edu/~waa/class-pubs/rc4_ksaproc.ps.

[6] http://www.counterpane.com/pptpv2-paper.html.

[7] http://packetstormsecurity.org/groups/teso/chap.pdf.

[8] C. Rigney, S. Willens, A. Rubens, and W. Simpson, "Remote Authentication Dial-In User Service," IETF RFC 2865, June 2000.

[9] http://en.wikipedia.org/wiki/Robust_Security_Network.

[10] http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol.

[11] http://en.wikipedia.org/wiki/Protected_Extensible_Authentication_Protocol.