EDN NETWORK

Track hackers through cyberspace

Sherri Davidoff, Jonathan Ham - June 01, 2012

‘‘You are only coming through in waves . . . ’’---Pink Floyd[1]

Wireless networks are everywhere. They exist in enterprises, homes, subways, buses, cafes, anywhere people go. For an investigator, wireless networks can be a boon or a wretched headache. In the best scenarios, wireless networks provide easy access to client traffic, a convenient entry point into the network, and extensive access logs.

On the other hand, many wireless devices and access points do not retain access logs, especially when deployed with default configurations. Client systems tend to be connected transiently, and their physical locations are often unknown or difficult to pinpoint. Employees or attackers can set up rogue wireless networks, unbeknownst to central IT staff, for the purposes of convenience or covert data exfiltration. Wireless devices in the enterprise can pose a major challenge for forensic investigators--especially since these same devices are often accessible from the parking lot of a facility and can represent a major loophole in organizational security defenses.

Wireless devices have exploded in popularity during the past decade. It is impossible to enumerate all the wireless devices that exist in even a single person’s house, let alone a large corporate environment. Individuals often walk around carrying multiple wireless devices, such as cell phones, iPads, laptops, Bluetooth headsets, and GPS tracking devices.

Common types of wireless devices and networks include:

- AM/FM radios
- Cordless phones
- Cell phones
- Bluetooth headsets
- Infrared devices, such as TV remotes
- Zigbee devices, such as HVAC, thermostat, lighting, and electrical controls
- Wi-Fi (802.11)—LAN networking over RF
- WiMAX (802.16)—“last-mile” broadband[2]

Why investigate wireless networks? Here are some examples of cases involving wireless networks:

- Recover a stolen laptop by tracking it on the wireless network.

- Identify rogue wireless access points that have been installed by insiders for convenience or to bypass enterprise security.

- Investigate malicious or inappropriate activity that occurred via a wireless network.

- Investigate attacks on the wireless network itself, including denial-of-service, encryption cracking, and authentication bypass attacks.

In addition, you may find yourself capturing wireless packets, investigating wireless routers and switches, or conducting a forensic analysis relating to any other topic in this book where the physical layer happens to be air rather than a cable or fiber .

Wireless networks, particularly those based on IEEE 802.11 (“Wi-Fi”) standards, have proliferated in the last decade. These days almost no enterprise is without them. As a result, every network forensic investigator should be prepared to handle wireless evidence.

With computing devices getting smaller and more mobile, we are increasingly reliant upon wireless connectivity. The proliferation of mobile devices is putting pressure on government and enterprises alike to expand the availability of network access. In the United States, the Federal Communications Commission (FCC) has been instructed to facilitate ubiquitous broadband access.

If you calculate the expense of a network deployment versus the number of potential endpoints that can be supported, wireless networks are clearly the economical option. In general, it is cheaper to deploy a wireless network than run all the cables necessary for a wired infrastructure. This is especially important in sparsely populated areas where cables might have to be run long distances or over rough terrain, and also in high-density areas where older buildings were not designed with modern wiring needs in mind. As a result, wireless networks are being deployed in nearly every type of environment, often replacing or expanding existing network access.

In this chapter, we focus our attention on 802.11 “Wi-Fi” networks specifically. This is because Wi-Fi networks are extremely common both in the enterprise and at home, and we can leverage many of our previously discussed forensic techniques on 802.11 Wi-Fi networks. Many of the concepts we cover in this chapter are also applicable to other types of wireless devices and networks.

The IEEE Layer 2 Protocol Series

As previously discussed in Chapter 3, “Evidence Acquisition,” the IEEE has published a series of international standards (“802.11”) for Wireless Local Area Network (WLAN) communication. These standards specify protocols for WLAN traffic in the 2.4, 3.7, and 5 GHz frequency ranges. The term “Wi-Fi” is used to refer to certain types of RF traffic, which include the IEEE 802.11 standards. For more details about passive evidence acquisition of 802.11 traffic, please see Section 3.1.2, “Radio Frequency” in Chapter 3.

As analysts of network traffic, it is easy to get in the habit of assuming that all of the protocols that we care about are described in an IETF RFC. It is worth remembering that not all standards are sponsored by the IETF (see discussions in Chapter 4). Many of the core network protocols, especially at Layer 2, were instead proposed and published by IEEE standards groups--particularly the 802 series, which covers Ethernet (802.3), trunking (802.1q), LAN-based authentication (802.1X), and various aspects of Wi-Fi (802.11) including both WEP- and WPA-based encryption standards.

Track hackers through cyberspace - Cont'd.

Why So Many Layer 2 Protocols?

You may be wondering why we need so many different protocols for Layer 2 functionality. Often, network forensic students ask, “Why didn’t we just use existing Ethernet standards over RF just like we did over copper?” Radio frequency and copper simply don’t have the same physical characteristics, and so signals sent across them don’t behave the same way! In order to insulate Layer 3 protocols (chiefly IP) from those differences in physical properties, we need intermediary protocols to allow a uniform interface to the network layer, regardless of the physical media.

We’ve been talking about how a wireless access point is essentially just a Layer 2 hub, but it’s a little bit more complicated than that. A physical copper hub can be relied upon to deliver signals from each station to every other station.

For forensic investigators, it is important to realize that if you are capturing traffic from a wireless network, there may well be stations actively participating in the network that you cannot overhear from your vantage point, due to signal strength (unlike on wired media, where voltages propagate much more reliably through copper or fiber cables). This simple fact has far-reaching effects on both data link–layer protocols themselves and forensic analysis of the wireless evidence.

While Ethernet (802.3) is designed to use the “carrier sense multiple access with collision detection” (CSMA/CD) method, the 802.11 wireless protocols we discuss use “carrier sense multiple access with collision avoidance” (CSMA/CA). We briefly review these concepts in the next sections.

CSMA/CD

Ethernet, designed for wired networks, is a protocol based on CSMA/CD. What this means is that all stations on the network share the same medium--typically a star-shaped but essentially physically contiguous piece of copper. A single conductor can only transmit one single signal at a time, by raising the voltage on the line (a “one”) or reducing the voltage on the line (“a zero”). In other words, only one station can be using the “multiple access” medium at the same time. (There may be other more sophisticated and multiplexing ways to encode signals with electrons on copper, but that’s how Ethernet does it.) Meanwhile, it must be all stations’ responsibility to make sure that the wire is live and in use (the “carrier sense” part of CSMA) and to detect if any two stations are trying to use it at the same time (the “collision detection” part).

This isn’t always easy, as electrons don’t propagate down copper instantaneously, so two stations on the farthest ends of the circuit could commence sending at roughly the same time without realizing that someone else down the wire was trying to talk too. The specified result is that the first station that detects overlapping signals should send out a special “jamming” signal to all stations, essentially informing everyone that they need to stop talking and try again, but only after selecting at random a time increment to wait (so that they don’t all try at once again).

CSMA/CA

In wireless LANs, collisions cannot be reliably detected by the sender. On a wire, the high and low voltages will eventually propagate to every station, so long as they remain physically connected. In contrast, on a wireless network, it is entirely common to have multiple stations sharing the same frequency and channel, even if each station is not necessarily capable of detecting all signals from its peers. As long as a station can reliably send and receive signals to and from the access point, it can participate in the network. A station that can communicate with the access point but not other stations is referred to as a “hidden node.”

Since collisions cannot be reliably detected over radio frequency, 802.11 wireless networks are designed to use collision avoidance techniques by decreasing the likelihood that two stations will attempt to communicate at the same time. As described in the IEEE 802.11-2007 standard, before transmission, a station on the wireless network listens to determine if the transmission medium is idle. If it is busy, the station waits until the end of the current transmission, and then it waits an additional random amount of time before attempting to send traffic. This helps to reduce the likelihood that all stations will transmit at once. In addition, stations can also exchange control frames of message type “request-to-send” and “clear-to-send” to help avoid collisions, as described further in Section 6.1.2.1, “802.11 Frame Types.”[3]

The 802.11 Protocol Suite

The IEEE developed the 802.11 protocol suite as a standard for data link–layer transmission over wireless physical media, including the radio and infrared frequency spectra. 802.11 is designed to incorporate CSMA/CA, in keeping with the needs of the wireless physical medium.

802.11 Frame Types

The 802.11 protocol suite defines different types of frames. For forensic investigators, different types of frames contain different types of evidence, as we will see.

There are three types of 802.11 frames:

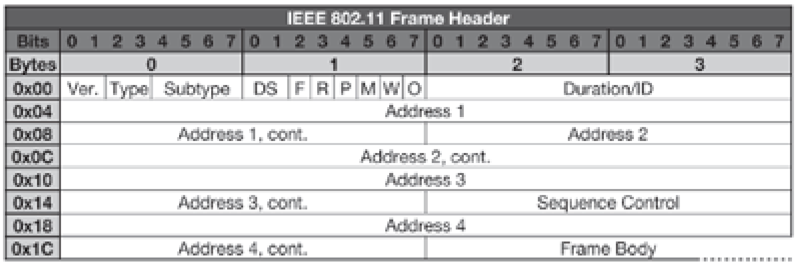
- Management Frames--Govern communications between stations, except flow control;

- Control Frames--Support flow control over a variably available medium (such as RF);

- Data Frames--Encapsulate the Layer 3+ data that moves between stations actively engaged in communication on a wireless network.

802.11 is a complicated Layer 2 protocol in many respects. Figure 6–1 is a chart that shows the 802.11 frame’s data structure. You’d be forgiven for looking at the chart in Figure 6–1 and wondering to yourself what the fields meant—especially since there are several 6-byte locations for frame addresses. The purpose of each “address” field is dependent upon the frame’s type and subtype.[4]

Management Frames Management frames (type 0) are designed to coordinate communication on any wireless LAN, from infrastructure networks to individual stations sending out probe requests. These frames are the glue that keeps the stations together through a single access point, or on an extended series of bridged access points. Management frame subtypes include Association Requests, Association Responses, Probes, Beacons, and others.



IEEE 802.11 Frame Header				
Bits	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Bytes	0	1	2	3
0x00	Ver. Type Subtype	DS F R P M W O	Duration/ID	
0x04	Address 1			
0x08	Address 1, cont.		Address 2	
0x0C	Address 2, cont.			
0x10	Address 3			
0x14	Address 3, cont.		Sequence Control	
0x18	Address 4			
0x1C	Address 4, cont.		Frame Body	

Figure 6-1. The 802.11 frame's data structure, which includes four fields for 6-byte MAC addresses per frame. How each is used is dependent upon the frame's type and subtype.

Track hackers through cyberspace - Cont'd.

For forensic investigators, management frames are important for several reasons. First and foremost, they are not encrypted. As a result, these clear-text frames provide a wealth of information as to which stations are trying to communicate, in which ways, and with whom. At a minimum, type 0 frames are interesting because their subtypes indicate basic associative activities. In addition, with a bit of statistical analysis (as we'll soon see), they can provide a treasure trove of forensic data. From the information in a management frame, you can enumerate station MAC addresses, infer likely manufacturers, identify access point Basic Service Set Identification (BSSID) and Service Set Identifiers (SSIDs), investigate successful and failed authentication attempts, and more. Management frames are often the target of manipulation or the vector of attacks against an access point. As we will see, common attacks such as WEP cracking and Evil Twin attacks are often facilitated through manipulation of management frames, or simply careful attention to the details broadcast within them.[5]

Management frame subtypes include:

- 0x0 — Association Request
- 0x1 — Association Response – Status Code: 0x0000 — Successful
- 0x2 — Reassociation Request
- 0x3 — Reassociation Response
- 0x4 — Probe Request
- 0x5 — Probe Response
- 0x6 — Reserved
- 0x7 — Reserved
- 0x8 — Beacon frame
- 0x9 — Announcement Traffic Indication Map (ATIM)
- 0xA — Disassociation

- 0xB — Authentication
- 0xC — Deauthentication
- 0xD — Action
- 0xE — Reserved
- 0xF — Reserved

Control Frames

Control frames (type 1) are designed to manage the flow of traffic across a wireless network. One of the main challenges wireless protocol designers faced is the "hidden node" problem. Recall that while on a wired medium, it can be presumed that every station will eventually be able to see all nodes (as voltages propagate to all stations).

With RF, it is entirely possible that some stations cannot "see" each other, while still being networked using the same notional physical media (since they can each "see" the WAP). One way of addressing this problem is to have individual stations send "request to send" control frames, and for all stations to watch for corresponding "clear-to-send" and "acknowledgment" frames. That way availability of transmission and reception can be tested prior to the establishment of data circuits.

There are three control frame subtypes (as displayed by Wireshark, with the high-order nibble set to "1" for the "Control" type):

- 0x1B—Request-to-send (RTS)
- 0x1C—Clear-to-send (CTS)
- 0x1D—Acknowledgment

Control frames are relatively sparse, but can provide an investigator with information about timing and station MAC addresses.

Data Frames

Data frames (type 2) contain the actual data transmitted across the wireless network, including encapsulated higher-layer protocols. For instance, every IP packet that flows across the wireless 802.11 network is part of the payload of an 802.11 data frame.

There are many different data frame subtypes, including the Null function (subtype 4), indicating no data. However, the most interesting is likely to be those where the subtype is 0 (Data).[6]

As a forensic investigator, if the wireless network is not encrypted, or if you have access to the encryption key and can gain access to unencrypted data frames, then you can capture and analyze the wireless traffic at Layer 3 and above. Even encrypted data frames can still be analyzed using statistical flow analysis techniques to reveal volumes and directionality of traffic and stations involved.

Next: 802.11 Frame Analysis

See Part II: Click Here

References:

[1] R. Waters and D. Gilmour, “Comfortably Numb,” The Wall (EMI, 1979).

[2] Ian Mansfield, “WiMAX Companies Receive $504 Million in Funding for Last Mile Broadband Projects,” Cellular-News, October 20, 2010, http://www.cellular-news.com/story/45995.php.

[3] IEEE, “IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications” (June 12, 2007): 251, http://standards.ieee.org/getieee802/download/802.11-2007.pdf (accessed December 31, 2011).

[4] IEEE, “IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications” (June 12, 2007): 59–87.

[5] IEEE, “IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,” 79–87.

[6] IEEE, “IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,” 77–79.

Network Forensics: Tracking Hackers through Cyberspace, Rough Cuts by Sherri Davidoff, Jonathan Ham, Published Apr 2, 2012 by Prentice Hall. ISBN-13: 978-0-13-256514- with permission by Pearson Publishing. To purchase this book, click here.