WiFi

Abstract
In this project part, we will look at the issue of intrusion detection in wireless networks. As you know, network security becomes more challenging in wireless networks as anyone within signal range may receive and interact with the network due to the lack of access control that a wired network would normally have through the physical access control of the building. In this assignment you will hence extend your monitoring beyond your own wireless network to record and correlate events that would indicate malicious attempts targeting your network's users. There are two types of defenses we will practice in this assignment: First, the 802.11w standard introduces a cryptographic message integrity check to the Wi-Fi protocol to validate the authenticity of wireless control frames, which will allow you to validate the frames from your infrastructure using an external cryptographic library and identify rogue device imposing your network. Second, your defense can also take a proactive approach and actively inject frames to prevent the rogue network from ensnaring your clients. While there are possibilities for actively defending your network and prevent a network attack from succeeding, not all strategies that are technically possible are legally allowed. In the last part, you will further investigate this tension and develop a mitigation plan compliant with the legislation in your area.

Security in wireless communication systems introduces the additional complication that effective access control for this unguided medium is difficult to establish in practice. While the area in which wireless signals are available can be somewhat limited, such mitigations are typically impractical to deploy or too costly compared to the level of risk an organization has attached to the threat. If a wireless link cannot be avoided, strong encryption and integrity checking can avoid the exposure of confidential data to an outside adversary, and limit the possibilities to modify and inject data into the communication systems.

A variety of risks are difficult to entirely control for in any wireless system. By launching a denial-of-service attack and flooding the wireless spectrum with random noise at a high power, it is trivial for an adversary to impair the availability of the communication system, but difficult for its owner to locate and counter this threat. Assaults on wireless availability can however be much more subtle and sophisticated, as we have seen in the discussion in chapter 4. Presenting an identical-appearing but malicious network to its users – the evil twin attack –, an adversary may obtain private data from unsuspecting users and implicitly also make the actual service they are trying to use unavailable. Specific systems such as wireless Ethernet face in addition to the easy possibility of spoofing link layer addresses also the challenge that an established connection may be broken down by a single control packet, which together forms a potent basis for an adversary to compromise the availability of a Wi-Fi network at a protocol level.

In this project part, you will extend your intrusion prevention system prototype by a module with capabilities to monitor attacks on the availability of a wireless Ethernet network, as well as detect attempts by a malicious party to obtain the pre-shared key for a WEP-secured 802.11 network. With the introduction of management frame protection in 802.11w, select control frames can be validated for authenticity by a message integrity code, based on the negotiated key between client and access point or a group key shared by all stations of a wireless network. To gain practical experience in applying cryptographic concepts, your IPS module for Wi-Fi will test management frames sent by the access point for authenticity.

Malicious Interference with a Wi-Fi Network

During its connection establishment with an access point, a client passes through three phases: starting from an unconnected status, it first completes an authentication stage, then an association stage to join a network. While the authentication step is used in WEP to test the client's knowledge of a pre-shared key in a challenge-response fashion, this exchange was functionally abandoned in WPA in favor of an EAPoL handshake after the establishment of a connection at the link layer. As described in chapter 4, WPA2 derives a pair-wise key between client and access point given the SSID, nonces and MAC addresses from both parties, and in case of WPA2-Personal also a pre-shared password. According to the Wi-Fi protocol description, the access point may reset an existing connection and ask the client to fall back to any of the prior stages, thus effectively requiring the station to redo the authentication and/or association handshake.

In absence of other means, devices derive the origin of a particular frame based on the included sender link layer address. As this address may be easily spoofed and is thus possible to inject frames on behalf of the access point with the request to break off and reestablish the connection, an adversary can easily deter select individual stations or any client from successfully joining an access point.

Task 1 *Create a module for 802.11 security in your intrusion detection system. The module registers with your IPS API and parses packets for evidence of a potential disassociation or deauthentication attack on the wireless network. Discuss whether you can conclude from the presence of disassociation and deauthentication frames for certain the presence of a malicious actor. How should you thus design your alert configuration rules for your IPS?* ■

In addition to interfering with the ability of clients to join and maintain a connection with the base station, the protocol design of the wired equivalent privacy (WEP) protocol also makes it possible for a third party to reveal the contents of encrypted packets, and to derive the pre-shared key used by the network. In hands-on 4.6, you see that using the injection of previously captured and specially modified frames, commonly available tools can recover the key in very little time.

Task 2 *Setup a wireless network with WEP encryption for testing, either using hardware or an access point emulated by a software package such as hostapd. Launch the ARP-request replay attack on your test network as described in the hands-on, and on a second network interface capture the packets exchanged in your network. Extend your module with the necessary functionality to detect* this particular *attack on your Wi-Fi network.* ■

Aside from generating a message to the administrator warning about an ongoing malicious interference with a network, it would also be possible to take an active approach to network defense, and for example use the disassociation frames described above to remove a maliciously acting client from a particular access point. Spoofed injected disassociation frames would also be an effective countermeasure if your IPS system would detect the presence of an unauthorized access point with your organization's SSID, that attempts to lure clients into connecting to the wrong base station and thus provide the ground for a follow-on attack. Most libpcap interfaces make it equally simply to inject arbitrary packets into the network as obtaining raw network packets, hence such a countermeasure is easy to add.

As you will see repeatedly throughout the book, network security can however not only concern itself with technology, but what is possible, desired and in the end implemented is also determined by economics, law and policy. Case study 4.1 showed that jamming of a wireless channel or denying access by means of a protocol attack is actually violating the U.S. Communication Act, but similar laws exist also in other jurisdictions around the world.

Task 3 *Investigate the legal situation in your jurisdiction. Are you allowed to willfully interfere with a third party? Does the situation change if the interference is done for defensive purposes to protect your own network from intrusion? What are the implications for network security measures you may or may not take?* ■

Authenticity Verification of Protected Management Frames

The amendment through 802.11w brought new means for cryptographic verification of management frames into the Wi-Fi standard. Access points can now include a message integrity code with important messages, which clients can check for authenticity and only follow with a reaction if the frame has indeed been sent by the base station. Message integrity checks require a secret key between all participating parties, while a cryptographic signature requires the distribution of a public key via a reliable channel to every receiver.

A closer look at the handshake and key derivation of WPA2 shows that there are two possible groups of key material that could be used for a message integrity check. Each client negotiates a pairwise transient key with the access point, and the first 128 bits of the PTK are for example already used to create MICs on EAPoL messages. The last 128 bits are as the temporal key designated for data encryption and authentication, and can be used for MICs on Wi-Fi frames. After the successful handshake, the base station forwards the group temporal key (GTK) to the newly joining client which is shared by all devices associated with the access point.

The different scope of the available key material naturally guides how message integrity codes for management frames are generated. Frames broadcast to the entire group are protected given the group key[1], unicast frames contain a MIC derived from the pairwise key, which is generated based on AES-128 in CBC-MAC mode. Since in order to include a MIC clients need to know the GTK or PTK, it is also immediately clear that only a small subset of management frames can be verified by this design. As on the one hand disassociat, deauthentication or channel switch announcements are typically sent after a client has joined the network and completed the WPA handshake, these management frames can in principle contain a verification tag. Beacons, probes, authentication and association management frames on the other hand are usually sent before the completion of the WPA phase, and clients would hence not be able to determine the authenticity of the frame even if a MIC was included.

Task 4 *Study the WPA(2) handshake and description of the format of the Managed MIC information element (MMIC) in chapter 4. Suppose a client receives a broadcast and a unicast management frame from the access point containing a valid MIC. Can the receiver be certain that either frame was sent by the base station?* ■

[1] To be more precise, these messages are protected by the integrity GTK (IGTK) which is generated by the access point and delivered encrypted by the KEK to the clients during the handshake.

Extra-Credit

In the following, you will include your Wi-Fi IPS module to check the integrity of protected management frames, to practice the application of cryptographic building blocks in a network security concept and include an external cryptographic library into your code. As protected unicast frames (for example disassociation packets) are easier to generate in an environment that you share with other students than protected broadcast frames (general channel switch announcements), we will focus only on unicast frames in this example. For security reasons you should never implement elementary cryptographic algorithms such as AES yourself, instead investigate *vetted* libraries that provide AES encryption and decryption with an interface to the language you have implemented your IPS in.

> **Task 5** *See the attached documentation for a description of the AES-CBC-MAC calculation in WPA. Extract the relevant fields from the disassociation frames and validate the integrity of the MIC.* ∎

Together with this project description you are provided with a packet trace in pcap format of a client performing an WPA2 handshake with an access point that enforces management frame protection. You can derive the temporal key from the EAPoL handshake between both devices, knowing that the password for this wireless network is “PASSWORD”. Alternatively, you can avoid this implementation step and read in the TK from an external source into your IPS module. In this pcap trace, the PTK for the four iterations are

```
PTK 1:
02 83 2e e8 2b cc 97 1a 98 44 1d b9 b0 90 5a 75 51 86 ac ab ed 3e e2 30
db a1 38 30 e8 73 ee 2a 22 34 11 2c c5 34 f3 a0 d4 53 aa 15 f7 df b8 b9

PTK 2:
c1 1d bc 18 da 24 28 fa df 37 12 7f e7 75 35 b3 1c d3 0e 60 cd 1c 09 5d
2d 87 3c e7 33 13 8f 72 d5 ee b8 10 0b c3 de de b3 2e a9 df 19 94 f5 a0

PTK 3:
91 5e 5e 95 cf 30 1b f0 d8 a2 bb c1 31 05 6e 5b c4 a5 2a 08 37 50 f0 27
3b 98 48 98 66 ec 61 ae df 94 28 1f 95 73 d6 85 4e 65 e3 3d cf f1 96 67

PTK 4:
af e9 7f cb 9e 1f f2 64 9f a7 c0 27 6f b5 cf 25 cc 4f ac fc 77 f5 06 09
65 8e b7 ec ad 48 4a d6 59 1a b5 1f c0 83 a1 dc 50 e4 85 1e f0 f8 3b 9c
```

In addition to the example packets, you can also test your implementation with the reference test vectors provided in the appendix of the 802.11w standard.