URSI GASS 2020, Rome, Italy, 29 August - 5 September 2020

Characterizing Wi-Fi Man-In-the-Middle Attacks

Andy Amoordon*(1), Christophe Gransart(1), and Virginie Deniau(1)
(1) Université Gustave Eiffel Campus Villeneuve D'Ascq

Abstract

Wi-Fi networks are widely deployed and used privately or professionally. However, many tools exist to implement Man-in-The-Middle attacks, on these networks, to intercept data. If certain Wi-Fi networks are protected, we all by negligence or compellingly use unprotected or poorly protected Wi-Fi networks, making it possible for attackers to collect sensitive information that can further be used for more virulent attacks. In this context, our research work aims to develop detection techniques, for Man-in-The-Middle attacks against Wi-Fi networks, by analyzing the Electromagnetic activity, i.e. the physical layer of the OSI model. We want to identify combinations or sequences of signals which can be indicative of the presence of such attacks. In this paper, we recall the Wi-Fi standards and their existing levels of protection. We describe in detail the steps involved in the implementation of Man-in-The-Middle attacks on public, private and enterprise Wi-Fi networks. Finally, from this detailed description, we identify the characteristics of the signals, sent by fake access points, which could allow us to devise a detection strategy.

1 Introduction

Wi-Fi networks are widely used and preferred to wired networks as they offer mobility, flexibility and rapid extension of the network. Wi-Fi networks, originally designed for convenience and home usage, are now a candidate for critical applications such as vehicular communication. In fact, the ITS-G5 technology, designed for vehicular communications, is based on the 802.11p standard [1]. However, Wi-Fi attacking tools have become prevalent and have made the protocol vulnerable to various types of attacks ranging from classical Denial of Service attacks (jamming, deauthentication attacks...) to more elaborated attacks such as Man-in-the-Middle (MITM) attacks [2, 3, 4]. MITM attacks (described in section 3) lead to a critical loss of data, privacy violations, and identity thefts. It is, therefore, important to detect and mitigate these attacks. Man-in-the-Middle attacks can be categorized into two classes: Man-in-the-Middle attacks on upper layers of the OSI model (layers 3-6) and Man-in-the-Middle attacks on lower layers of the OSI model (layers 1-2). Past research works have proposed detection mechanisms but only a few is based on the layer 1 (the physical layer) [5, 8, 9, 10]. This paper aims at characterizing and detailing MITM attacks on the Wi-Fi protocol and to brainstorm on an Intrusion Detection System (IDS) based on the physical layer.

Section 2 recalls important aspects of the IEEE 802.11 Wi-Fi standard needed to comprehend the MITM attack. Section 3 presents a characterization and description of Wi-Fi MITM attacks. Section 4 presents our idea for an IDS based on the physical layer. Finally, Section 5 explains our reasons for choosing to detect Wi-Fi MITM attacks on the physical layer.

2 The IEEE 802.11 Wi-Fi standard

Wi-Fi or Wireless-Fidelity[1] is a group of wireless network technologies based on the IEEE 802.11 standard. It is used as a medium of communication to wirelessly connect and give Internet access to devices in a Local Area Network (LAN). Wi-Fi uses the 2.4 GHz and 5.8 GHz radio bands which are divided into 20 MHz or 40 MHz channels. There are different generations of Wi-Fi; specified by distinct IEEE protocol standards. IEEE 802.11a, 802.11b, 802.11g, 802.11n and 802.11ac are some examples of Wi-Fi generations. Radio technologies determining radio bands, the maximum range, and speed differs from one Wi-Fi generation to another. A Wi-Fi network consists of Wi-Fi devices that can directly communicate with each other (ad-hoc mode) or communicate with each other via the intermediary of an access point (infrastructure mode). In this paper, we consider only Wi-Fi networks configured in the infrastructure mode. In the infrastructure mode, the Access Point (AP) needs to inform the devices of its presence and therefore periodically emits beacon frames. A beacon frame contains the name of the network (SSID) managed by the AP, the MAC address (BSSID) of the AP, the channel used by the AP, characteristics, and technologies supported by the AP. Wi-Fi networks can be encrypted or public/unencrypted. Encrypted Wi-Fi networks add an encryption phase after the authentication phase. When a client connects to a Wi-Fi network, it has to first authenticate to the access point. During the authentication phase, the access point accepts or denies the client's association request. Once the client has been authenticated, the access point eventually grants Internet access and encrypt the communication.

Public access points usually accept any client by default and

[1] https://standards.ieee.org/standard/802_11-2016.html

do not encrypt the communication. Some public AP can be selective and redirect a client to a captive portal page (for the user to sign in or enter a password) before granting Internet access. But in any case, public Wi-Fi networks are not encrypted. In encrypted Wi-Fi networks, access points ask the client for shared secret during the authentication phase and normally use the shared secret (with other parameters) to encrypt the communication. There are two types of encrypted Wi-FI networks: private networks and enterprise/community networks. Private networks are networks meant for private use and connect a limited number of clients. A home network is an example of a private network. Enterprise/community networks are networks meant to connect a significant number of clients and potentially transmit sensible information. Two security protocols exist to encrypt Wi-Fi networks: Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA,WPA2,WPA3). There two types of WPA classes: WPA-Personal (WPA-P) security and WPA-Enterprise (WPA-E). WPA-P are meant for private networks while WPA-E are meant for enterprise/community networks. WPA-P uses a Pre-Shared Key (PSK) as an authentication protocol while WPA-E uses the 802.11x EAP protocol to authenticate clients. Detailing encryption and authentication protocols is out of the scope of this paper.

Wi-Fi devices communicate via two planes: the data plane and the management plane. User data frames are sent on the data plane and management frames on the management plane. In a public network, the data plane and management plane are not encrypted. In an encrypted network, only the data plane is encrypted unless the devices are using the 802.11w standard which has cryptographic and integrity mechanisms to secure the management plane. A third plane known as the control plane is used to route or roam clients.

3 Characterisation of the MITM attack

Wi-Fi devices do not know the exact position of their receivers and in most of the IEEE 802.11 generations, the devices use omnidirectional antennas to transmit data. Omnidirectional antennas emit data in every direction within a specific range. Every Wi-Fi device within this range receives the data. Wi-Fi adapters are normally set to "Managed mode" in which they, by default, discard data that are not addressed to them. Attackers can, however, set their Wi-Fi adapters to "Monitor mode" to capture all the traffic in a given Wi-Fi channel. If the traffic is not encrypted, the attacker can read off or modify frames. This technique of capturing and analyzing network traffic is called packet sniffing. Since Wi-Fi devices emit in every direction on a given channel, the attacker does not even need to authenticate to the network to sniff packets, he simply has to "tune" to the channel frequency and capture the data.

Packet sniffing can be circumvent using encryption. When the data is encrypted, an attacker sniffing a network cannot understand or modify the data unless he has the decryption key or cracks the encryption key. Data can be encrypted on different layers of the OSI model. It can be encrypted on the application layer using HTTPS/SSL, on the network layer using Virtual Private Network (VPN) and on the data link layer using layer 2 encryption such as WEP, WPA1, WPA2, WPA3 (as far as Wi-Fi is concerned). As mentioned earlier, public Wi-Fi networks do not use layer 2 encryption and are therefore vulnerable to the packet sniffing attack. That is why it is of paramount importance to use HTTPS websites or a VPN when using these networks. With upper layer encryptions, the attacker will not understand upper layers information but can still understand frames (layer 2 information).

The Man-in-the-middle attack is more elaborated and is based on the fact that clients need intermediaries to send their message. In an ideal world, all senders and receivers would be directly connected to each other and would not need intermediaries (such as routers or commuters...) to relay their message. However, since resources are limited, such direct configurations are unrealizable. Existing networks such as Local Area Networks (LAN), Wide Area Network (WAN) rely on intermediaries to transmit a message from an origin to a destination. On such networks, when a sender sends a message, the message is routed and commuted by different trusted intermediaries before reaching its destination. A Man-in-the-Middle attack, therefore, occurs when a trusted intermediary voluntarily packets sniff the relaying data or when a trusted intermediary is hijacked or usurped by an attacker to packet sniff the relaying data. MITM attacks can be targeted against different layers of the OSI model:

- Application layer: HTTPS spoofing, secure socket layer (SSL) hijacking or Domain Name Server (DNS) spoofing
- Network layer: Internet Protocol (IP) address spoofing via Adress Resolution Protocol poisoning (ARP)
- Data Link layer: Antenna identity spoofing, Simple and Advanced Stealth Man-in-The-Middle Attack [7]

In this paper, we consider only Man-in-the-Middle attack configurations for Wi-Fi networks. Man-in-the-Middle attacks on Wi-Fi networks consists in the identity usurpation of an existing access point. The attacker identifies a target Wi-Fi network and then creates an access point that emits the same beacon frames as the targeted access point. Consequently, there are two similar access points: one licit and one illicit. And, it is difficult for devices to differentiate between the two APs. Moreover, to save energy, devices are set to connect to access points having higher transmission power.

After creating a fake access point operating at higher power than the licit one, the attacker can either wait passively for devices to connect to his fake access point—which can

be long unless the users are continuously moving— or actively disconnect the clients from the licit AP by emulating a Denial of Service of the licit AP. To emulate the Denial of Service of the licit access point, the attacker can either jam the channel of the licit access point or send de-authentication frames to the clients of the licit access point. De-authentication frames are management frames that are sent by the AP to terminate a connection with a client. As mentioned earlier, management frames are encrypted only in the 802.11w standard. When Wi-Fi devices are not IEEE 802.11w compatible, they sent management frames in clear which means that it can be easily spoofed. In the MITM attacks, the attacker spoofs the MAC address of the licit access to send the de-authentication frames. When the device receives the frame, it believes that it comes from the licit AP and terminate the connection. De-authentication frames are normally sent in case of handover from one signal weakening AP adapter to another AP adapter with a stronger signal. So, when a client is disconnected, it will automatically try to connect to another AP with the same BSSID.

Attacker undertakes the following steps to make a Man-in-the-Middle attack:

1. The attacker sniffs the Wi-Fi bandwidth and identifies potential public Wi-Fi network targets.

2. The attacker creates a fake Wi-Fi access point that spoofs the beacon frame of a targeted public Wi-Fi.

3. There are now two access points. If the attacker chooses to passively wait for the client to connect to his fake access point, he would normally configure his access point to transmit at higher power that the licit access point. In such cases, new clients would normally connect to his fake access point. Clients that are already connected to licit access might end up connecting to the fake access point if they are mobile and become out of range of the licit access point. Else, the attacker will have to actively jam the licit access point or de-authenticate the connected clients.

4. The attacker can now sniff the connection.

The predominant advantage of undertaking a Man-in-the-Middle attack for an attacker is that it allows him to bypass the layer encryption in which the attack is performed. When a communication between A and B is encrypted, only A and B can understand/modify data. Any external entities (packet sniffing the communication) would not be able to understand/modify data unless A or B communicates their decryption key. When a device connects to a fake AP without knowing that the AP is controlled by an attacker, it will perform layer 2 encryption with the fake AP. This encryption is ineffective as it is performed with the fake AP itself. The fake AP, and by extension, the attacker has the decryption key and can understand/modify data. For this reason, it is highly recommended to use several layers of encryptions (HTTPS, VPN...).

Depending on whether the network is public or private, the attacker may have to undertake some extra steps:

- Public Wi-Fi networks

  Public Wi-Fi networks are easy targets as they are not encrypted. The attacker simply has to create a fake access point, emitting the same beacon frames as the licit AP, and force (or wait passively for) devices to connect to his AP. Devices will seamlessly connect to the fake AP as they would do on handover or roaming - the user will not be notified.

- Private Wi-Fi networks

  Private networks use PSK to authenticate the devices and this adds a level of difficulty for the attacker. PSK or Pre-Shared Key is most commonly known as the Wi-Fi password. If the attacker sets up a fake access point usurping the identity of a licit AP without the correct PSK, devices, upon disconnection, would not seamlessly connect to the fake access point. They will be able to detect that the fake access point, although emitting the same beacon, is not the correct one. And if the user manually tries to connect to this network, the device would normally warn him. To be able to seamlessly fool a device to connect to his AP, the attacker needs to have the Wi-Fi password and configure its access point to work with the same Wi-Fi password as the licit access point.

  The password can be, depending on the scenario, easily obtained or cumbersome to obtain. During public events or conferences, Wi-Fi passwords are usually publicly displayed. In such cases, the attacks have no extra effort to do. Else, the attacker has to obtain the password by using other hacking techniques such as social engineering. For instance, the attacker can ask imprudent users the Wi-Fi password by email or invite them to click on a poisoned email or social media link to install a payload on their device and read the saved Wi-Fi passwords file. The attacker can also wait for users to manually connect to his access point even if they are being warned by devices. Users would tend to ignore the warning as they might not have been sensitized against this attack or simply because they are disconnected from the Internet and want to regain access. The attacker can then redirect the imprudent user to a fake network configuration page asking him to confirm the Wi-Fi password of the network. Ultimately, the attacker can use dictionary or brute-force attacks to crack the Wi-Fi password.

  Since a private Wi-Fi network is protected by a static and unique password, once the password is obtained, the attacker can de-authenticate all devices in the private network and force (or wait for) them to seamlessly connect to his access point.

- Enterprise/community Wi-Fi networks

  Enterprise/community Wi-Fi networks or WPA-E encrypted networks do not use static passwords. Each user has a unique username and password to authenticate to the access point. The AP is connected to a RADIUS server which verifies the credentials. Certificates can also be installed on devices and used to authenticate access points - this procedure is called double authentication and it is a powerful counter measurement against Man-in-the-Middle attacks [6].

  If double authentication is not enabled, attackers can perform MITM attack using a fake AP connected to a fake RADIUS server. However, as the password is not shared, even if he succeeds in obtaining the credential of a user, only one user will be affected. If double authentication is enabled, the attacker will have to use social engineering techniques to install a fake certificate validating his access point in the client's device before creating a fake access point.

4 An IDS based on lower OSI layers

We aim at developing an Intrusion Detection System based on the physical layer. Existing IDS are for upper layers [5]. The benefit of working on the physical layer is that detection mechanisms can be transposed on similar wireless protocols. Moreover, attacks are detected more rapidly because the signal does not have to be transcoded and the whole bandwidth can be monitored at the same time. By analyzing the EM activity, the IDS would be able to detect and notify users or network administrators of the presence of fake access points.

Detailing steps of MITM attacks helps to identify indicators to detect the attacks. For example, when there is a Man-in-the-Middle attack, there is forcibly the appearance of a fake access point, and high probably an excessive amount of de-authentication frames in the Wi-Fi channel. An excessive amount of de-authentication frame can be easily detected on power spectra. For the appearance of a fake access point fully forging all characteristics of a licit AP, we can use indicators from the data link layer to identify the fake access point. For instance, knowing that a fake access point will forcibly emit identical beacon frames at different time intervals, we can detect the appearance of a fake access through active signal surveillance on different time scales. Moreover, fulling forging AP would work on the same channel as the licit AP and since the channel cannot be used concomitantly, we would observe fluctuations in power at different time intervals.

5 Conclusion

In this paper, we have characterized Man-in-the-Middle attacks and detailed steps to undertake MITM attacks on Wi-Fi networks. We also explained that depending on the security level of the target network, attackers may have to perform extra steps. Finally, we brainstorm about how detailing the steps of the attack can help us to design an IDS based on the physical layer.

References

[1] Mirjami Jutila ; Johan Scholliers ; Mikko Valta ; Kaisa Kujanpää , "ITS-G5 performance improvement and evaluation for vulnerable road user safety services," *IET Intelligent Transport Systems*, **11**, 4, May 2017,pp.126–133, doi: 10.1049/iet-its.2016.0025 .

[2] Vanhoef; Mathy; Piessens; Frank, "Advanced Wi-Fi attacks using commodity hardware," *Proceedings of the 30th Annual Computer Security Applications Conference*, pp. 256–265, 2014.

[3] M.Cunche, "I know your MAC address: targeted tracking of individual using Wi-Fi," *J Comput Virol Hack Tech 10*, pp. 219–227, 2014, https://doi.org/10.1007/s11416-013-0196-1

[4] Y. Zou; J. Zhu; X. Wang; L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," *in Proceedings of the IEEE, vol. 104, no. 9*, pp. 1727–1765, September 2016.

[5] S. C. Sethuraman; S. Dhamodaran; V. Vijayakumar, "Intrusion detection system for detecting wireless attacks in IEEE 802.11 networks," *in IET Networks,vol. 8, no. 4*, pp. 219-232, 7 2019.

[6] H. Hwang; G. Jung; K. Sohn; S. Park, "A Study on MITM (Man in the Middle) Vulnerability in Wireless Network Using 802.1X and EAP," *2008 International Conference on Information Science and Security (ICISS 2008)*, Seoul, 2008, pp. 164-170.

[7] M. Agarwal; S. Biswas; S. Nandi, "Advanced Stealth Man-in-The-Middle Attack in WPA2 Encrypted Wi-Fi Networks," *in IEEE Communications Letters*, vol. 19, no. 4, pp. 581–584, April 2015.

[8] M. Y. Bambang Setiadji; R. Ibrahim and A. Amiruddin, "Lightweight Method for Detecting Fake Authentication Attack on Wi-Fi," *2019 6th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, Bandung, Indonesia, 2019, pp. 280-285.

[9] K. Vieira; F. L. Koch; J. B. M. Sobral; C. B. Westphall; J. L. d. S. Leão, "Autonomic Intrusion Detection and Response Using Big Data," *in IEEE Systems Journal*, pp. 1–8, 25 October 2019.

[10] K. F. Kao; W. C. Chen; J. C. Chang; H. T. Chu, "An Accurate Fake Access Point Detection Method Based on Deviation of Beacon Time Interval," *2014 IEEE Eighth International Conference on Software Security and Reliability-Companion*, San Francisco, CA, 2014, pp. 1-2.