Practical man-in-the-middle attacks in computer networks

Abstract

Using public wireless networks pose a real threat to the privacy of users due to the possibility of man-in-the-middle-attack. This docu- ments the issue of wireless access points operated by an attacker. Meth- ods of creating an access point and executing attacks against its users are described in detail, including example usage of software tools and possible countermeasures against the attacks. In practical part the success and impact of attack tools is evaluated.

Contents

Table of Contents

Abstract 2

1 Introduction 1

2 Man-in-the-middleattacks 3

2.1 ARPcachepoisoning 3

2.2 DNSman-in-the-middleattack 4

2.3 Man-in-the-middleattackusingrogueDHCPserver 5

2.4 SSL/TLS man-in-the-middle attack 6

2.5 Fake access point 7

3 Fake access point 8

3.1 Setting up wireless access point 8

3.1.1 Requiredhardware 8

3.1.2 Requiredsoftware 9

3.2 Types of the access points 10

3.3 Creatingeviltwinaccesspoint 11

3.3.1 Cloningspecificaccesspoint 12

3.3.2 Karmaattack 12

3.4 Luring victims 13

3.4.1 Accesspointdenial 14

3.4.2 Clientluring 15

3.5 Countermeasures 15

4 SSL/TLSman-in-the-middleattacks 17

4.1 HTTPSstrippingattack 17

4.1.1 Sslstrip 17

4.1.2 Countermeasures 20
4.2 SSL/TLS certificate forgery 21
4.2.1 SSLsplit 23
4.2.2 Mitmproxy 25
4.2.3 Countermeasures 26
5 Practical tests 29
5.1 Creatingaccesspoint 29
5.2 Sslstrip 31
5.3 SSLsplit 33
5.4 Karmaattack 36
6 Conclusions 37
Bibliography 38

1 Introduction

Due to the recent increase in popularity of wireless networks, people became inured to using them for everyday communication. Users now expect availability of wireless networks in restaurants, hotels, schools, and other public places, and do not hesitate to use them for accessing sensitive information, for example, bank accounts or corporate databases. Such a behaviour pose a threat to the privacy of users, because if an access point (AP) is under control of someone with nefarious intentions, then this AP can be used for monitoring of and tampering with communicated data. This type of attack, when an attacker controls communication from the position between a client and a server, is called man-in-the-middle (MITM) attack. The aim of this document is to explore possibilities of MITM attacks in computer networks, with focus on attack techniques using fake AP. We describe principles of
practical MITM attacks, and also demonstrate practical usage of tools implementing these attacks. The tools are then used to evaluate security of selected applications against MITM attacks. Our goal is also to recommend best practices how to mitigate presented attacks.

The structure of this document is following. First, we describe the principle of MITM attack and give examples of this attack in computer networks. In Chapter 3, we summarize what hardware and software requirements have to be met for creating an AP capable of executing attacks against connected users. Then we describe how to clone an AP to create an evil twin AP, even automatically by using the Karma attack, and give recommendations how to avoid connecting to such evil AP. Chapter 4 deals with practical MITM attacks compromising encrypted communication. We describe how these attacks work and show usage of software
1. INTRODUCTION tools for executing them. For each of these

---

attacks we also describe

countermeasures how to mitigate the possibility of being a victim. In the Chapter 5 we present results of our practical testing of described attacks utilizing fake AP. In the last chapter we conclude how are the described attacks successful.

2 Man-in-the-middleattacks

In this chapter, we describe what an MITM attack is. We describe principles of this attack and give examples of MITM attacks that work on different layers of computer network. Basic idea of an MITM attack is that an attacker interposes himself in between two communicating parties and starts controlling their communication. Suppose Alice wants to communicate with Bob. If a malicious entity, called Mallot, manages to insert himself into the path of the communication between Alice and Bob, then he becomes the MITM and gains abilities of the attacker in the Needham-Schroeder attack model [1], meaning he is capable of reading and changing communicated messages. From this moment on there exist in fact two communication channels, one between Alice and Mallot and the other one between Mallot and Bob. Every message sent between Alice and Bob goes through Mallot and can be manipulated without any side noticing.

2.1 ARPcachepoisoning

ARP Cache Poisoning, or ARP Spoofing, is an attack working on the third layer of the ISO/OSI reference model [2]. The aim of this attack is to change routes of the traffic on a local network so the data goes through a malicious host. To achieve this behaviour a vulnerability in the Address Resolution Protocol (ARP) is exploited.

Purpose of the Address Resolution Protocol is to translate IP address of desired host to the corresponding MAC address on the local network.

If one host wants to send data to a specific IP address, it broadcasts to the local network asking for MAC address associated with the given IP address.

The host with requested IP address sends a unicast reply

2. MAN-IN-THE-MIDDLE ATTACKS with its MAC address. Flaw in

this protocol is that there are no steps taken to verify whether the obtained pair of IP and MAC address is valid, giving the attacker a chance to forge responses claiming that somebody else's IP address belongs to his MAC address. Tricked host then stores this information to speed up future communications, which effectively redirects data to the attacker.

To obtain a position between the victim and the rest of the network an attacker must spoof MAC addresses of the victim and the gateway and accordingly forward the data between them.

Two variants of this attack exist depending of what type of control packet is manipulated. First option is to create forged ARP reply packet to poison cache of the victim with malicious translation of IP addresses to MAC addresses. However, most of the network devices ignore unsolicited replies. Second option is to forge ICMP packets. Internet Control Message Protocol (ICMP) offers various types of messages to obtain information about the network, such as *Echo Request*, *Echo Reply*, *Redirect* or *Time Exceeded*. The attacker sends the victim a specially crafted Echo Request message containing the attacker's MAC address and the IP address of, for example, the gateway as a source address, resulting in victim caching this malicious pair of addresses and sending data to the attacker instead of the gateway in the future.

2.2 DNSman-in-the-middleattack

Domain Name System (DNS) is a distributed system providing mapping between domain names and IP addresses. In the DNS protocol a client sends a request to the server with a domain name and the server responds with an IP address of the given domain. In the ISO/OSI model this protocol operates on the application layer, i.e. layer 7.

DNS MITM attack inserts an attacker between a victim and a DNS server, which enables him to provide incorrect information about mapping domain names to IP addresses [3]. The result is a victim wanting to visit regular websites but obtaining IP addresses of malicious sites

belonging to the attacker.

One way how to reach the MITM position is to intercept DNS request from the victim and reply on them faster than the authentic DNS server, resulting in replies from the DNS server being dropped by the victim host because they are no longer needed. The attacker has a good chance to respond faster than the genuine server because of possible recursive resolution of the IP address in the hierarchical system of domain names, but to be sure to respond first the attacker can slow down the server by flooding it with a large amount of DNS requests.

2.3 Man-in-the-middleattackusingrogueDHCPserver

Dynamic Host Configuration Protocol (DHCP) is an application layer protocol used for distributing network configuration parameters on a local network. Such parameters are, for example, assigned IP address, address of a local DNS server or address of a default gateway. If the attacker is capable of setting up his own DHCP server, then he can configure connected hosts in such a way that the address of a default gateway will be address of his machine, which will effectively re-route all the outgoing traffic to the attacker [4].

For the attack to be successful it is not sufficient to start broadcasting to the network that there is available a new DHCP server, because new hosts can still accept settings from the legitimate server. At first, services from all available DHCP servers must be denied, giving the attacker a space for controlling the local network. DHCP servers can be taken down

2. MAN-IN-THE-MIDDLE ATTACKS by either using the Denial of

Service (DoS) attack or the address starvation attack. Principle of DoS attack is to flood server with requests to slow it down, the address starvation attack consists of continual claiming IP addresses from the DHCP server until it runs out of them, making the server not able to serve new hosts.

When a victim host accepts configuration from the malicious DHCP server, it then sends all data to the attacker instead of the legitimate gateway. Attacker accepts this data, possibly manipulates them and forwards modified packets to the gateway to cover the existence of the MITM. Disadvantage of this attack is that incoming traffic goes from the gateway directly to hosts, so the attacker sees and controls only outgoing traffic.

2.4 SSL/TLS man-in-the-middle attack

Secure Sockets Layer/Transport Layer Security (SSL/TLS) are cryptographic protocols operating on the presentation network layer, i.e. layer 6. Their goal is to establish a secure connection between two sides communicating over an insecure network. These protocols provide confidentiality and optionally also authenticity of the exchanged messages, however, an attacker can under given conditions run an MITM attack to bypass the encryption and gain access to the plaintext [5]. The attacker can force the victim not to use a secure connection at all by manipulating the victim's HTTP traffic to prevent him from redirecting to a secure HTTPS site. Another way how to get access to the plaintext is to intercept certifi- cate provided by the server and pass to the victim a forged one with public key of the attacker, tricking the victim into encrypting messages directly for the attacker.

MITM attacks on SSL/TLS encryption are described in more detail in the Chapter 4.

2.5 Fake access point

In order to obtain control over the traffic in the wireless network an attacker can set up his own malicious AP. Such AP would appear as a regular point for connecting to the network, but all the traffic going through will be observed and possibly manipulated by the attacker. The attacker can either passively wait for connected hosts or actively lure them to his network by cloning existing APs or APs requested by the wireless devices.

This topic is covered in more detail in the Chapter 3.

3 Fake access point

Creation of a malicious AP is an effective, yet easy to deploy method of running an MITM attack. In the simplest form, the attacker creates a publicly accessible wireless network, waits for some users to con- nect, and monitors all their data traffic. The attacker can then under given conditions collect their personal information and credentials, for example, passwords, credit card numbers, etc. This type of attack can be potentially highly effective due to the popularity of Wi-Fi capable devices such as laptops, smartphones or tables and ubiquitous presence of wireless networks in restaurants, hotels, university campuses, office buildings and so on. Advanced methods of luring potential victims does also exist, capable of connecting users to the attackers network without their explicit permission. In this chapter, we first describe what kind of hardware and software equipment is necessary for establishing a malicious AP. Next, we discuss how the AP can operate in situations when the connection is limited. At the end, we describe how to clone existing APs and how to disconnect users from the networks they are currently using.

3.1 Setting up wireless access point

3.1.1 Requiredhardware

Wireless AP can be created by using a wireless router or a mobile wireless device. Specialised network auditing tools in a form of wireless routers can be purchased, for example, WiFi Pineapple [6]. However, using a mobile wireless device as an AP, for example, laptop or smartphone, brings higher mobility and better performance. Modern mobile devices

3. FAKE ACCESS POINT are usually already equipped with tool for

sharing wireless connection, this functionality is called tethering [7]. For better results an external antenna should be used to enhance the signal strength. Stronger signal makes the malicious AP visible to the devices in a wider range and increases a chance of the attack to be successful, because mobile devices try to connect to the known network with the best signal strength to maintain a stable connection. The most popular wireless adapters with external antennas that may serve as APs are Alfa AWUS036H, Alfa AWUS036NHR and TP- LINK TL-WN722N [8].

If we want to perform an analysis of traffic in a wireless network, the used wireless adapter should support switching to a monitor mode. In monitor mode we can see service messages broadcast in the network we listen to, for example, *Probe Request* messages important for the Karma attack described in the Section 3.3.2.

If connection to the internet is needed but there isn't available a connection to a standard computer network, a GSM module can be used to connect to the Internet through a mobile network.

3.1.2 Requiredsoftware

Standard operating systems, such as Windows, Mac OS X, or Android, are equipped with a tethering functionality, but to be able to read or manipulate the data going through the fake AP, a special software is needed. In this section, we describe what tools are available for creating an AP and processing the data going through.

Access point creation Although an option to create an AP is usually already available in standard operating systems, a more customizable way of doing so is often required. There are many tools for creating APs, providing options to, for example, 3. FAKE ACCESS POINT set Service Set Identifier (SSID, name of

the network), MAC address, or operating channel. These tools can also integrate advanced attacks such as Karma or HTTPS stripping attack, which will be discussed later. The examples of such tools are *hostapd* [9], *airbase-ng* [10], *WebSploit Framework* [11], *Ghost Phisher* [12], *MANA Toolkit* [13], *Subterfuge* [14] or *easy-creds* [15].

Data manipulation Attackers can choose from a variety of instruments to manipulate the communicated data in real time. The goal of such manipulation can be to, for example, infect victims with a malware or hack inside an encrypted communication to extend the MITM attack. The examples of such programs are *mitmproxy* [16], *sslstrip* [17], *SSLsplit* [18], *Etter- cap* [19], *Mallory* [20] or *Metasploit* [21].

3.2 Types of the access points

Attacks using a fake AP can be divided by the type of the network they are connected to into three classes.

- *Offline AP* – malicious AP can be able to collect credentials even if it is not connected to the Internet. This attack uses methods based on a social engineering to trick the victims to think that they are really online. One method is to clone most popular web sites and provide these clones to the victims, who will enter their passwords and reveal them to the attacker. Another method is to set up a captive portal, a page where users will be redirected, and ask there for entering personal information or passwords. An example of this attack is to ask for a password to an existing wireless network.