Man in the Middle: Attack and Protection

Enkli Ylli[a], Dr. Julian Fejzaj[b]

[a] *Faculty of Information Technology, Polytechnic University of Tirana, Sheshi Nënë Tereza ,Tiranë, Albania*
[b] *Faculty of Natural Sciences, University of Tirana, Bulevardi Zogu i Pare, Tiranë, Albania*

Abstract

The purpose of this paper is to take a closer look at Man-In-The-Middle (will be referred to as MITM) attack and defense. MITM also referred to in certain literature as a hijack attack, is one of the most well-known and widespread attacks in cybersecurity, targeting connection between two parties and directly putting into jeopardy the confidentiality and coherence of the data itself. This paper will delve into the current situation of cybersecurity and usage of Man-In-The-Middle attacks, what constitutes a proper MITM attack, why this approach is chosen among many other options, how such an attack is implemented in a real-life scenario and how we can achieve maximal protection for both individuals and systems.

Keywords 1

MITM, cyber security, wireless network

1. Introduction

As important as building an efficient system, network or application is, taking the correct measures in order to protect and offer a secure service is even more necessary. With the technological development comes increased risks and security threats and never has this been more true than in today's society.

Cybersecurity and cybercrime are two terms that go hand in hand with each other and are inversely correlated. While cyber security handles the protection of internet-related hardware, software and data from different threats, cybercrime encompasses the illegal activity that uses a computer as its primary means of commission and theft. [1] The inverse correlation between the two signifies their relationship; if cybersecurity measures are improved and increased, the possibility of cybercrime is reduced. But if cybersecurity is not on the correct level, the possibility of a cybercrime happening is increased heavily.

There is a multitude of methods that can be used in the execution of a cyber-attack. They vary from brute force attacks, which is a mostly outdated method to today's technological development, to Man-In-The-Middle (MITM) attacks, Denial Of Service (DOS or Distributed DOS), malicious attacks (includes worms, Trojans, viruses, spyware, etc.), phishing and so on. While they are all worthy of study and understanding, this paper will focus on MITM attacks.

Let us first introduce what a Man-In-The-Middle attack entails. As the name suggests, this is an interference where an attacker infiltrates the communication between two or more parties who are unaware of the existence of this attacker. The attacker may be either passively receiving information exchanged by the two participants or actively interfering and changing the data or information that is being communicated. The form of attack and further details will be discussed in the third section of this paper. This type of attack has been taking place since the 1980s and scientists have been actively studying and taking measures in the prevention of such activity among others.

Proccedings of RTA-CSIT 2021, May 2021, Tirana, Albania
EMAIL: eylli@yahoo.com (A. 1); julian.fejzaj@fshn.edu.al (A. 2)

Two main approaches are included in setting up a MITM attack[2]: creating fake networks that are controlled by the attacker or tampering with the connection between the victim and a legitimate network. The first method is widely used in attacking individuals using public Wi-Fi that nowadays is available in most cafés, institutions and businesses. The second method is a bit more sophisticated where there the infiltration entails a non-secured connection between the victim and the attacker and then a secured connection between the attacker and the genuine network. This can be very difficult to detect, especially if correct encryption and transference are then provided. However, the unsecured connection between the attacker and the victim can have devastating results especially depending on the type of information transferred, for example in online commerce or banking information.

Relating to MITM defense methods, there are some prevalent ways. From a user perspective, free public Wi-Fi connections are suggested to be steered clear of. They present an easy yet effective way of implementing MITM attacks and are much harder to detect especially from a user's perspective and the lack of proper precautions being taken. Warnings from certain browsers will flag illegitimate connections which is a simple way for a user to detect a not genuine connection. VPNs also prove to be efficient in offering a more secure connection. From a technological perspective, the two main ways of defense against MITM attacks rely on prevention primarily and detection secondarily.

In Section 2, this paper will be taking a closer look at MITM attacks, followed by in-depth information regarding MITM defense approaches in Section 3. In Section 4, this paper will be mentioning future works, followed by conclusions that will be provided in the final Section 5.

2. MITM Attacks

Man-in-the-middle attacks are one of the most commonly used network attacks. This attack happens when the attacker manages to get in the middle between two parts of communication: the sender and the receiver. The attacker tricks the parts of the communication by making them believe that they are communicating with each other but in fact, the attacker controls the communication. Often the two parts of the communication are: the client and the server. As such, this paper will use this network topology to explain how MITM attacks are performed.

The client and the server communicate with each other using a legitimate communication channel. The client sends requests to the server and the server sends responses to the client based on the request that the client sent. The attacker using MITM attack destroys the legitimate communication channel and creates a new one, which is controlled by him. He tricks the client to believe that the attacker is the server and tricks the server to believe that the attacker is the client. So when a client sends a request to the server, the request is sent to the attacker and then the attacker forwards it to the server. The same thing happens with the response that the server sends to the client. This response first arrives to the attacker and then the attacker decides what to do with the response, forward it or not to the client. Being in the middle of the communication, between the client and the server, gives the attacker access to the information and the packets that are being transferred. The packets may contain sensitive information like passwords, username, login credentials etc. The attacker can drop the packets, sniff or manipulate them.

There are two types of MITM attacks: passive attacks and active attacks[4]. In the passive attack, the attacker receives the packets being transmitted and forwards them without making changes. In the active attacks, the attacker receives the packets and manipulates them. Then he forwards the manipulated packets. By the protocol used to perform MITM attacks there are three types of attacks:

- ARP Poisoning-IP spoofing
- DNS Spoofing
- DHCP Spoofing
- Wi-Fi Eavesdropping
- SSL Stripping
- HTTPS Spoofing

2.1. ARP Poisoning – IP spoofing

MITM attack using ARP Poisoning is the most commonly used technique to perform MITM attacks and this is because of the poor security of ARP protocol and also because it is the simplest way to perform the attack. Address Resolution Protocol (ARP) is a protocol that creates a mapping between MAC address and the IP address. These protocols work by using two types of messages: request and reply. The communication contains two parts: source host and destination host. ARP Request is broadcasted and is used to find which MAC address maps a certain IP. All the hosts get this request but only the host whose IP address matches the IP address in the header of the ARP Request responds to the request. To lower network traffic flow, every host has an ARP cache, which is a table that maps IP addresses with MAC addresses of every host connected to the network.

ARP Poisoning means the 'the poison 'of ARP cache using the main vulnerability of ARP protocol[10]. The vulnerability of ARP protocol is that is a non-state protocol and the hosts will accept ARP reply even if they haven't sent any ARP request. This means that they will update their ARP caches every time there is an ARP reply. Because the ARP requests are broadcasts, every host connected to the network can get the requests. The attacker sends a response using a copied MAC address, and he attacks the two parts of the communication. He attacks the source host and sends him an ARP Reply where he tricks the source to believe that the IP address of the destination host maps the MAC address of the attacker, and he sends an ARP Reply to the destination host where he tricks the destination to believe that IP address of source host maps the MAC address of the attacker. After this, the source thinks that the attacker is the destination and the destination thinks that the attacker is the source. So every information that source and destination hosts send to each other firstly passes to the attacker, and then he forwards the packets to them. This type of attack is performed on switches and access points but not on routers because the router will not pass ARP packets to other routers. ARP

2.2. DNS Spoofing

DNS is a protocol that translates domains into IP addresses [6]. It is an important internet protocol but has security problems and one of them is that the client can't verify the authenticity of the DNS Response that he gets. This means that the first response that the client gets, it's the one that is trusted and used. This flaw is used to perform DNS Spoofing.

DNS Spoofing is a type of attack where the attacker prevents the client from accessing the legitimate server and directs him to a fake one that is controlled by the attacker [7]. This is done by manipulating DNS entries in the DNS table. When a client wants to access a website, he sends a DNS Request to the DNS server to get the IP address of the site and the DNS server sends back this IP to the client using DNS Response. The request and the response transmitted between the client and server, is protected by an identification number. If the attacker manages to identify this number then he can attack the client by sending him a fake DNS Response before the client Request arrives at the legitimate DNS server. To identify this identification number, the attacker performs MITM using ARP spoof and gets the packets the client is sending. Because the DNS traffic is not encrypted or authenticated he can read the identification number and then send a fake DNS response to the client and directs the client to a fake website controlled by the attacker. In this way, the attacker can read all the data that the client is filling in the fake website. This type of attack can be executed not only in LAN networks but also on other networks. This can be achieved by using a static IP for the fake DNS server and then attacking DNS cache using viruses and not ARP Spoofing.

2.3. SSL Stripping

Removing SSL encryption in a segment between source and destination is a serious threat to the confidentiality claimed and offered by the service offering.

Usage of weak algorithms on SSL creates the opportunity to break. Firstly the user creates a HTTP connection and then redirected to HTTPS. By detecting the first connection request attacker will change data and then continue to establish an HTTPS connection between himself and the server, and an

unsecured HTTP connection with the user, acting as a "bridge" between them.
The most usable scenario that user experiences when browsing the internet is redirection through HTTP 302. This scenario can be used also undetected in Wi-Fi Eavesdropping

2.4. Wi-Fi Eavesdropping

This type of attack has to do with creating a fake AP and let other users connect to IT. The most classic scenario is when the AP doesn't have a password. Being in complete control of the AP one can sniff all traffic and also implement in a successful manner SSL Stripping and HTTPS Spoofing. This can also be implemented with ARP spoofing of a legitimate SSID in a hotel or nearby a bank so that the probability of accessing any important information is higher.

2.5. HTTPS spoofing

Representing for example a fake website with a fake certificate a malicious can receive data and then after decryption can do a copy of them, modifying and then pass the info to the legitimate server. Data can be financial, usernames or passwords etc. In internal LAN there can be different scenarios of using SSL Stripping for example by using ARP spoofing. In an internet scenario, DNS Spoofing can be utilized to SSL Stripping. With DNS spoofing changing manually DNS record for some domain or web site with the reference IP of a fake host with a fake or legitimate stolen certificate. This type of attack has a very vast usage during Covid-19 with fake sites represented as legitimate to steal juicy information or money.

2.6. DHCP Spoofing

Another way to perform MITM attacks is by using DHCP Spoofing and can be executed in LAN networks. DHCP is a protocol based on a DHCP server that dynamically assigns every host connected to the network an IP address and other configurations like subnet mask, DNS, default gateway etc. The attack used to perform DNS Spoofing is Rouge DHCP Server. In this type of attack, the attacker creates and adds to the network a rouge DHCP server which he controls. When a client is connected to the network he sends the request message to communicate with DHCP Servers. The request is caught by the two DHCP Servers, the legitimate one and the fake one, but the client will accept the server that responds first. Usually, it is the server that is closer to the client who responds first so to be sure that the rogue server responds first, the attacker can use DHCP Starvation. By using DHCP Starvation the attacker sends many requests to the legitimate server but doesn't respond to the responses he gets by DHCP Server. This makes the legitimate server have no free addresses to offer. The legitimate server can't respond because it is being DOS-ed, so the rogue server responds and sends to the client the configurations. These configurations contain as default gateway the attacker's IP address so all the communication is headed to the attacker and controlled by him.

3. MITM Defense: Prevention and Detection

While MITM attacks may not be as common as viruses, worms and phishing, commonly referred to as ransom ware, they do present an increasing threat by roughly thirty-five per cent of all attacks. The reason for this is due to the work that goes into setting up a MITM attack that can be simplified by just using ransom ware attacks. However, they still present a threat to organizations in general.

There are a number of implementations that have proved to be helpful in preventing a MITM attack. A simple approach is the implementation of Hypertext Transfer Protocol Secure (HTTPS) which is used to offer a secure communication environment in a network context [8]. Well-known sites and browsers will notify users if the connection they are using is not secure, which in general has greatly impacted the decline of MITM attacks in public WIFI spots. Upon notification, rapid closure of the WIFI connection must be insured in order to prevent further risks.

Relating to ARP Poisoning, some methods for the prevention of such an attack includes using S-ARP instead of ARP, which solves security-related issues for ARP but has

problems with scalability. The second mode of prevention lies in the implementation of static MAC addresses in which a single IP is connected to a single MAC. This is effective because an attacker cannot send a false MAC address. However, this is not very sustainable because it requires the involvement of the administrator to configure the static relationship between the IP and MAC address. Dynamic ARP Inspection (DAI) is a method that validates ARP packages in a given network. DHCP snooping needs to be firstly implemented, saving records based on exchanged messages, deterring ARP packages that do not follow the previous records, offering proper protection against MITM attacks.

A well-known saying explains that prevention is better than a cure and nowhere is it more applicable than in the world of cyber security. The meaning lies on the fact that preventing an issue is much easier than detecting or even fighting the malware itself. A common way to help with prevention is the application of encryption. Using cryptographic protocols among which TLS (Transport Layer Security) and previously SSL which is now deprecated that offer proper data encryption is a great way to prevent these attacks. Rightly there have been flaws previously in SSL which have led to the deprecation of the protocol and now TLS has taken over proving to be much more efficient in the task of encryption and authentication. It should be mentioned that continuous updates have been made in both protocols in order to repair flaws or increase their capabilities and mechanisms to adapt to the continuing technological advancements.

In using TLS, the communication process is built on a key-based infrastructure, meaning the identity of both or more parties can be authenticated via public key cryptography. Thus, the connection is private as the data transmitted is encrypted using keys that are generated uniquely for each connection channel. This mutual authentication is generally what prevents the possibility of a MITM attack, considering both the end-user and server are mutually validated, eradicating the possibility to access and decryption of the data that is being transmitted, without knowledge of the specific keys.

Another method of prevention is the implementation of the DNS (Domain Name System) extension named DNSSEC (Domain Name System Security Extensions). This extension adds security to the lack of mechanisms in DNS to authenticate data and originators, thus helping with MITM DNS Spoofing attempts and DNS cache poisoning. The way DNSSEC does this is by adding authentication on the origin of the data. However, it should be mentioned that in order for DNSSEC to be a valid detection method on MITM attacks and to maintain data origin authenticity and integrity, both servers and resolvers must use the DNSSEC protocol. [3]

A quite effective way of preventing a MITM attack is by using Virtual Private Networks (VPN) [9]. As the name suggests, a VPN is practically the extension of a private network over a public network (usually the Internet) in order to enable users to communicate on top of the public network as if they were connected to a private network. This is associated usually with increased security and proper encryption to prevent possible attempts to read or manipulate transferred data and overall communication. In the MITM context, a VPN hides the user's communication route and encrypts their network traffic as well as hides the IP address[9]. This concealment makes it very difficult for an attacker to trace the IP address and in turn initiate a proper attack.

Another issue worth mentioning is the usage of viruses in MITM attacks. As we mentioned previously, attackers will use whatever method is easier for them and brings the best results. A method that helps with that is a somewhat hybrid between a ransom ware and a MITM attack. There is a way that can be used to initiate a MITM attack, by which viruses are used to start off such an attack. Thus, it is important for a user to have proper antivirus software installed in their device prior in order to protect against malware infections that conceal bigger threats.

Regarding prevention methods relating to Rogue DHCP Server MITM attack, a good prevention method is using DHCP Snooping[11] . The main job is to improve the security of the DHCP server, by effectively preventing malevolent or unacceptable traffic. DHCP Snooping is configured on switches so that it can control the responses towards discovering packages that the switch receives.

Regarding the prevention of DHCP Starvation, it can be handled via port security implementation. What port-security does is that prevents DHCP starvation by limiting the number of MAC addresses on a switch port.

A very big reason why prevention is so incredibly important when considering MITM attacks is that the detection of a MITM attack is incredibly difficult. If one is not actively searching for a Man-In-The-Middle attack, it can go unnoticed for quite some time which in effect will allow enough time for the attacker to do what it requires before proper measures are taken. What can be done in these cases is tamper detection, which practically checks the time and latency in an occurring communication. Increased latency may reveal possible occurring attack if records show that such a communication should not occur for the measured time.

4. Future Works

MITM attacks have many implementation forms and this paper present and analyze them theoretically. A good work for the future may be the practical implementation of these attacks in real-world scenarios and combine them with other types of attacks like DOS, sniffing and phishing. A very interesting aspect is the protection from MITM attacks. Day by day the number of internet devices is increasing so protection is very important. We can analyze and test how successful are the defensive approaches explained in the paper and what can be done to improve them. But the protection also includes prevention and detection of these attack before they happen and this is done by creating algorithms, frameworks and implementing them practically. Also, a good work for the future may be analyzing if new technologies like 5G are protected by MITM attacks.

5. Conclusions

Network and data security are and will continue to be an interesting topic in computer science. The increase in the number of users who use the internet and also the increase of the services that are offered online makes this topic really important. Many of these services use user's personal data, and they do not always offer security and protection. Security problems can be caused by user carelessness but in many times they are caused by the network protocols. There are many network security threats but this paper was focused on Man-in-the-Middle (MITM) attacks. Firstly, this paper analyzed what MITM attacks are, and then it explained the different types on how these attacks can be implemented. The most commonly used attack is ARP Spoofing, but this paper also examined DNS Spoofing and DHCP Spoofing. For every type of attack, this paper also analyzed the best practices that offer protection. It is important to note that online security cannot be achieved only by securing the network but it should be combined with the cautiousness and carefulness of the network user.

6. References

[1] Gade, Nikhita Reddy & Reddy, Ugander. (2014). A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies.

[2] Conti, Mauro & Dragoni, Nicola & Lesyk, Viktor. (2016). A Survey of Man in the Middle Attacks. IEEE Communications Surveys & Tutorials. 18. 1-1. 10.1109/COMST.2016.2548426.

[3] S. Ariyapperuma and C. J. Mitchell, "Security vulnerabilities in DNS and DNSSEC," The Second International Conference on Availability, Reliability and Security (ARES'07), Vienna, 2007, pp. 335-342, doi: 10.1109/ARES.2007.139.

[4] James Forshaw , ATTACKING NETWORK PROTOCOLS A Hacker's Guide to Capture, Analysis, and Exploitation , William Pollock , 2018 , pg. 95-103

[5] PROWELL, Stacy, Rob Kraus, Mike Borkin. Seven Deadliest Network Attacks (Seven Deadliest Attacks), Syngress, 2010.

[6] GREGG, Michael. Certified Ethical Hacker (CEH) cert guide. Indianapolis, Pearson, 2014.

[7] Ian Green. DNS Spoofing by The Man In The Middle. SANS Institute, 2005

[8] Bruce Hartpence, "Packet Guide to Core Network Protocols", O'Reilly Media, 2011, pg. 30-70

[9] AMINE, Abdelmalek, Otmane AIT MOHAMED a Boualem BENATALLAH. Network security technologies: design and applications. IGI Global, 2013, s. 156-157.

[10] Bavithra Raju, MITM Attacks through ARP poisoning, 2016, [Online] URL: https://www.researchgate.net/publication/3135

68165_MITM_Attacks_through_ARP_poisoning

[11] Mukhtar, Husameldin & Salah, Khaled & Iraqi, Youssef. (2012). Mitigation of DHCP starvation attack. Computers & Electrical Engineering. 38. 1115-1128. 10.1016/j.compeleceng.2012.06.005