WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Secure Approach to Prevent Man in the Middle Attack in Communication Medium

Sayantan Chakrabarti [a], Moon Sarkar [a], Antara Jana [a]

[a] B P Poddar Institute of Management and Technology,Kolkata 700052, India

A B S T R A C T

Among different popular network attacks, MITM is one that is being used over a long period of time. In MITM, the attacker disrupts the communication between the actual user and the destination server gateway by redirecting the network traffic. ARP Spoofing is the most common type of attacking mechanism of the Wireless network. The attacker interrupts all traffic from victim's network towards the attacker's system by attacking over securely connected networks. In this paper, the practical attack has been demonstrated along with its detection and prevention technique which is the main goal of this paper. Here in this paper, an algorithm is made where lists are created at the time of connection towards the secured connection and after certain intervals more lists are created containing the addresses of the victim's machine such as IP address, mac and physical addresses. Both lists' addresses are then checked whether the addresses are same or not. If both the lists' addresses are matched, then secure communication will take place and if the addresses do not match an alert message is shown and simultaneously the user is logged off the hampered network connection immediately. Thus, preventing the victim's machine from further attack.

Keywords: Man in the middle Attack, Detection of MITM, Prevention of MITM, Network Security

1. Introduction

MITM or man-in-the-middle attacks are a type of common cybersecurity attack that enables the attacker to eavesdrop on the communication between two targets. This attack got its name from its attacking technique where it allows the attacker to situate itself between two legitimate communicating hosts, and enabling the attacker to listen to a conversation that they should not be able to listen to and hence the name "man in the middle". MITM techniques are usually established in early stages of cyber kill chain – during observation, obtrusion and exploitation. MITM is often used to garner credentials and to glean intelligence about targets. Some popular MITM techniques are-

ARP cache poisoning - ARP refers to low level process on network level that converts the MAC to the IP address. Here attackers trick your computer to think that the attacker's system is your default gateway by injecting false information into the system.

DNS cache poisoning- When an attacker gives you false DNS entry leading towards a different website is termed as DNS cache poisoning.

Wi-fi Eavesdropping- Attackers on public or unsecured Wi-fi networks listen to traffic, or create Wi-fi networks with common names to attract users to connect to these networks so they can steal credentials or various card information or anything that you communicate through that network.

MITM attacks have been around a long time and can be difficult to detect without taking proper steps. You have to actively keep a look at your communication to determine whether it have been intercepted because MITM can go unnoticed for a long period of time and till then its' too late to notice.

Proper checking of authenticate page and tamper detection implementation are the key methods to detect possible attack, but these courses of actions might require extra analysis after the act. Some preventive measures that can be taken are-

- Strong *WAP/WEP* encryption mechanism may prevent unwanted users from joining your network connection.
- Make sure to change default router credentials and keep on changing it on periodic basis.
- Public Key pair-based authentication like RSA should be used to ensure that your communications are being communicated with the right user.

The objective of this paper is to-

- To showcase how MITM is implemented using third party software.
- To detect the attacking network.

- To prevent victim's machine from MITM so as to stop identity theft.

2. Literature Review

MITM is a very popular type of attacks in network communication. Paper [1] describes about different types of possibilities of MITM in secure communication channel. Paper [2] discussed about various types of attacks that can be performed for MITM in communication medium. Paper [3] states that various MITM techniques are used for MITM in recent days for network attack. Various MITM attacks mechanism are also discusses in paper [4]. Paper [5] focuses on the various scenario of MITM with its effect. A key generation algorithm for MITM are discussed in paper [6].

3. Existing Work

There are few software already existing which detects MITM manually. They are mentioned below: -

Proxy.py

A lightweight open-source web sockets, HTTP, HTTPS andHTTP2 proxy server. It can handle a great number of connections likely ten thousand connections per second.

Burp

A tool with an automated and vulnerability scanning feature good for security professionals. Researchers can test web applications and identify bugs that can be exploited by the criminals.

Ettercap

An open-source network traffic analyzer and attacker. This tool allows to dissect and analyze wide range of network protocols and hosts.

These existing tools can be compared to the example of a flashlight where if you have to find something in the dark it can only cast light on the object but you yourself have to use your eyes to find the object because it does not tell you where the object is. Similarly, these softwares are the helping tools in detecting the attacking network but users have to actively search for the traffic by themselves, they do not tell you which is the attacking network.

4. Proposed Work

The proposed work should be progressed in following ways: -

- Make list of all the addresses such as Ip address, mac address and physical address as soon as it is connected to a network.
- At regular intervals of time keep creating another list of the addresses.
- Compare both the lists.
- If the addresses of both the lists are same, it should show All ok.
- When MITM is performed on the system, it should show an alert message.
- Log out of the network.

4.1 Flow of the proposed method

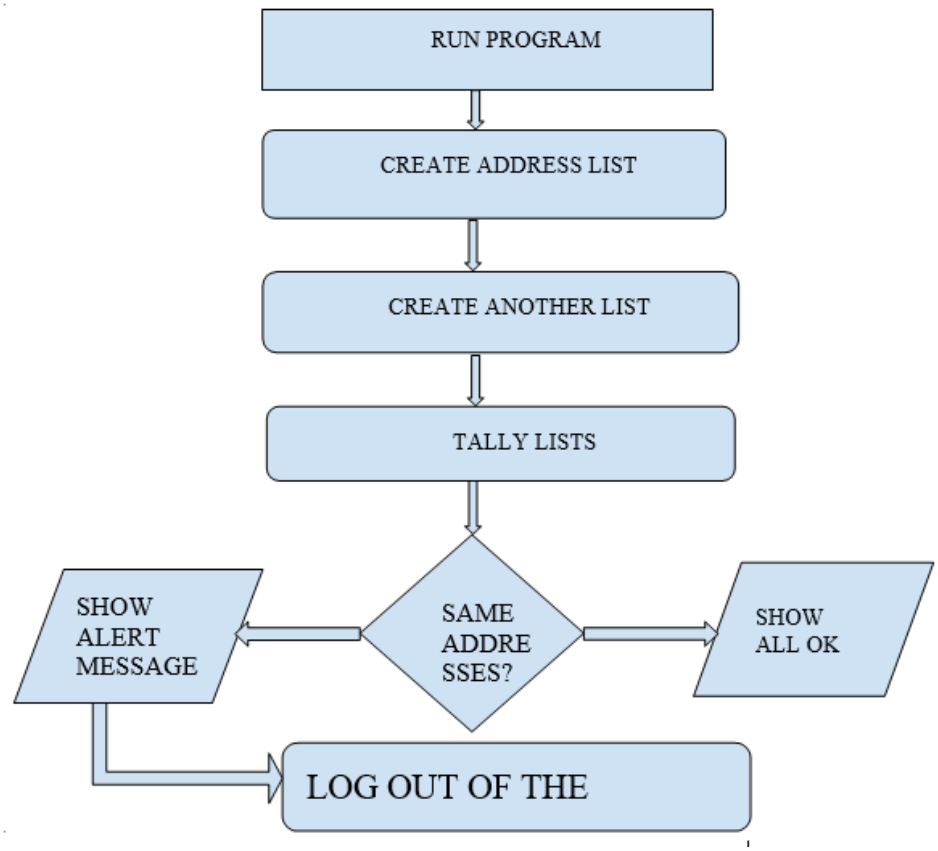

Fig 1. Proposed work flow of MITM prevention

- Implementing MITM
    - Should be connected to the same network as the victim's system.
    - Once connected in the network, in Ettercap graphical search for all local hosts.
    - Add the address of the victim's system in target1 and attacker's address in target 2.
    - Perform ARP spoofing.
    - In Wireshark, you can keep track of all the
    - traffic in the victim's system.
    - Therefore, MITM is implemented as discussed in Fig. 2.
- Detection of MITM
    - As soon as MITM is done on any system, the default gateway of the system changes.
    - You can keep track of this by manually running the command config -a in cmd.
    - In this project, the software automatically keeps on detecting MITM by keeping track of the addresses as shown in Fig.3.
- Prevention of MITM
    - Since the software keeps on checking the list of addresses, as soon as MITM is done it shows an alert message.
    - And as a precaution logs out of the victimized network for an indefinite time.

Fig 2. Picture showing how to add targets in Ettercap

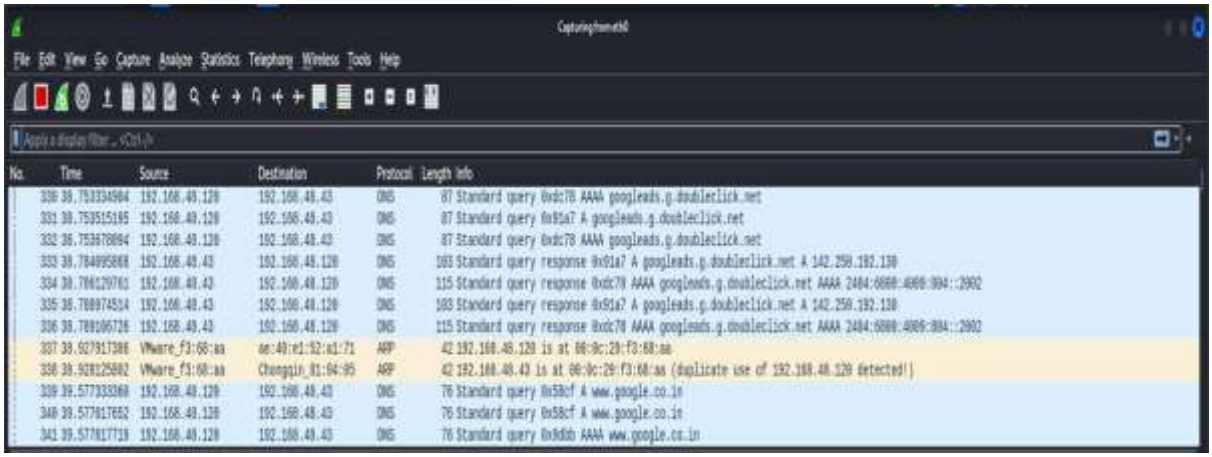

Fig 3. Picture showing network traffics in Wireshark

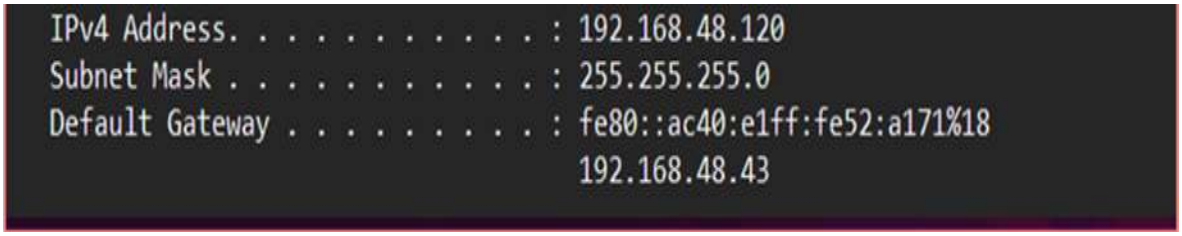

Fig 4. Picture showing IP addresses when connected to a network

5. Result Analysis

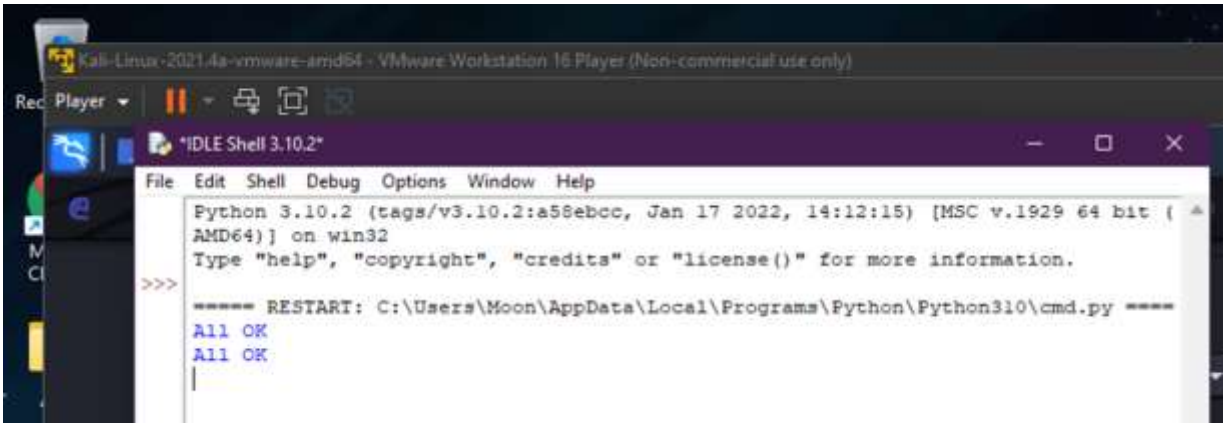

Fig 5. Picture showcasing the result shown when no MITM is done.

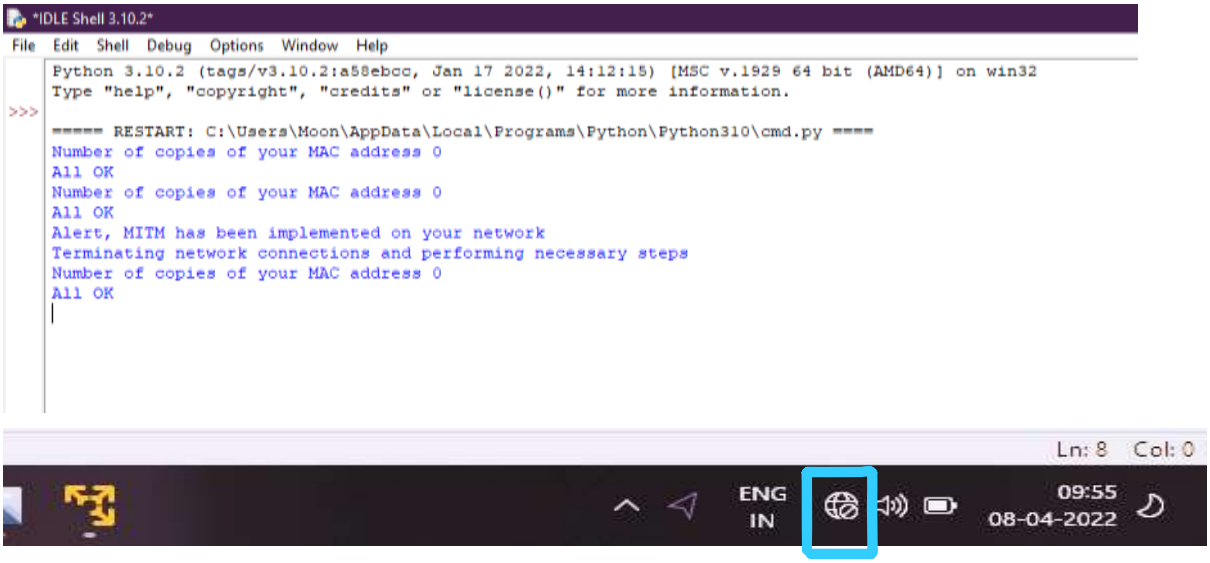

Fig 6. Picture showcasing the result shown when MITM is performed in a victim's software.

6. Conclusion

Therefore, we can conclude from this report that MITM is the one of the most popular attacks in today's world where cyber-crimes are increasing at alarming rate. This attack cannot be detected easily. Once it is implemented in any device there is a high risk of identity theft. To detect MITM one has to keep track of the addresses i.e., IP, physical and mac addresses. It is nearly impossible to prevent MITM. This algorithm that has been mentioned in this paper is very helpful in terms of preventing MITM because here a user does not have to manually keep track of all the addresses and check if the default gateway is changed or not. Our software automatically keeps track of the addresses and alerts you once MITM is performed and logs you out of the hampered network eventually preventing the victim from identity threat.

7. References

[1] Eskil Christensson; Man in the Middle Attacks On Software Defined Network; Mälardalens Universitet Akademin För Innovation, Design Och Teknik Västerås, Sverige,2023.

[2] Enkli Ylli, Dr. Julian Fejzaj; Man in the Middle: Attack and Protection; Proccedings of RTA-CSIT 2021; 2021.

[3] Danish Javeed, Umar Mohammed Badamasi, Cosmas Obiora Ndubuisi, Faiza Soomro, Muhammad Asif; Man in the Middle Attacks: Analysis, Motivation and Prevention; International Journal of Computer Networks and Communications Security VOL. 8, NO. 7, 52–58, 2020.

[4] Avijit Mallik, Man-In-The-Middle-Attack: Understanding In Simple Words, Cyberspace: Jurnal Pendidikan Teknologi Informasi Volume 2, Nomor 2, 109 – 134, 2018.

[5] Mauro Conti; Nicola Dragoni; Viktor Lesyk; A Survey of Man In The Middle Attacks; IEEE Communications Surveys & Tutorials; 2016.

[6] Simon Eberz, Martin Strohmeier, Matthias Wilhelm, and Ivan Martinovic; A Practical Man-In-The-Middle Attack on Signal-Based Key Generation Protocols; ESORICS 2012, LNCS 7459, pp. 235–252, 2012. © Springer-Verlag Berlin Heidelberg 2012.