



# **Man-in-the-middle Attack**

*A thesis submitted to the Department of Electronics and Communication Engineering  
in Partial Fulfillment of the requirements for the degree*

**Of**

**BACHELOR OF SCIENCE IN ELECTRONICS AND TELECOMMUNICATION  
ENGINEERING**

**Presented by**

Sadiya Islam Luna

ID: 2015-2-55-020

**Supervised by**

Mohammad Rafsun Islam

Lecturer

Department of Electronics and Communications Engineering

East West University

**SPRING 2020**



EAST WEST UNIVERSITY

B. SC. ENGINEERING THESIS

---

*Man-in-the-middle Attack*

---

***Supervisor***

*Mohammad Rafsun Islam*

*Lecturer*

*Department of Electronics and*

*Communications Engineering*

***Author***

*Sadiya Islam Luna*

*ID:2015-2-55-020*

# Approval

This is to certify that the thesis entitled “Man-in-the-middle Attack”, submitted by Sadiya Islam Luna, ID: 2015-2-55-020 to the respected matter of the faculty of Engineering for partial fulfillment of the requirement for the degree of Bachelor of Electronics and Telecommunication Engineering (ETE) under complete supervision of the undersigned.

Supervisor:

.....

Mohammad Rafsun Islam

Department of

Electronics and Communications Engineering

East West University

Chairperson:

.....

Dr. Mohammed Moseeur Rahman

Department of

Electronics and Communications Engineering

East West University

## **Declaration of Authorship**

I, Sadiya Islam Luna, hereby declare that this thesis, “Man-the-Middle Attack”, consists entirely of my own work produced from research under the supervision of, Mohammad Rafsun Islam, Lecturer, Department of Electronics and Communications Engineering, East-West University. I also state that where any part of this thesis has previously not been submitted for a degree or any other qualification except for publication. , this has been clearly stated and duly acknowledged.

.....

Sadiya Islam Luna

ID: 2015-2-55-020

# Acknowledgement

First of all, I would like to thank the Almighty for giving me the strength, wisdom, and understanding of knowledge to complete my thesis. I would like to give my deepest gratitude to my advisor, Mohammad Rafsun Islam for the opportunity to research with him at the beginning of my research, his careful advice set out the right direction for me. He gave me a great deal of independence during the research process and was always willing to help in any way he could. Without his admirable enthusiasm for novel ideas on research, I cannot finish my thesis so well. Many thanks also go to all lecturers of the Faculty of Electronics and Telecommunication Engineering who have regarded me in one way or the other and have made a significant contribution to the successful completion of my degree. I am grateful and wish to thank my friends for the manifold support and encouragement.

Last but foremost, I would like to thank and express my deep appreciation to my family and, in particular, to my parents, who have given me the moral support and encouragement takes to achieve my degree. They've always been so patient, so understanding. All this would never have been possible without them.

*Dedicated To My Parents...*

# Abstract

The Man-In-The-Middle (MITM) attack is among the most well-known threats in the field of computer cyber security, one of the major issues for security analysts. MITM focuses on the specific data flowing between both the endpoints and the data security and integrity of information itself. These attacks had led to a terrifying loss of data. This project attempted to describe the specifics of MITM attacks, detection, and prevention mechanisms. In this paper, the literature on MITM is studied extensively to analyze and categorize the scope of MITM attacks. In general, classify MITM attacks based on several criteria, such as the position of its attacker on a network, and malicious strategies. Based on the list of impersonation methods, include effective solutions for the prevention of measures for every MITM classification. The implementation of how to mitigate and detect attacks against MITM has been performed with the help of virtualization tools. This study would help to provide a better understanding of the facts, and it will also propose the significance of the solution to important MITM attacks that have been described in the paper.

***Keywords— Man-in-the-middle (MITM) attack; ARP Spoofing; DNS Spoofing; MITM Prevention mechanism; Ettercap.***

# Table of Contents

<b>Chapter 1: Introduction.....</b>	<b>1</b>
1.1 Background.....	1
1.2 Definition of Man-in –the-middle Attack.....	2
1.3 How man-in-the-middle attacks work.....	2
1.4 Organization of thesis.....	4
<b>Chapter 2: Review of Literature.....</b>	<b>5</b>
2.1 Previous work.....	5
2.2. Progress of man in the middle attack.....	7
2.3 Present status of MITM attacks.....	8
<b>Chapter 3: Classification of Man-in-the-middle Attack.....</b>	<b>12</b>
3.1 Characterizations of MITM Attacks.....	12
3.2 Classification of MITM Attacks.....	12
3.2.1 Spoofing-based MITM Attack.....	13
3.2.1.1 ARP spoofing-based MITM attack.....	13
3.2.1.1.1 Attack Mechanism.....	15
3.2.1.1.2 ARP spoofing implications.....	16
3.2.1.2 DNS spoofing-based MITM attack.....	16
3.2.1.2.1 Attack Mechanism.....	18
3.2.1.3 DHCP spoofing-based MITM attack.....	18
3.2.1.3.1 DHCP Protocol.....	19
3.2.1.3.2 Classifications of DHCP spoofing.....	19



3.2.1.4 IP spoofing-based MITM attack.....	20
3.2.1.4.1 Attack Mechanism.....	21
3.2.1.4.2 Classification of IP Spoofing.....	21
3.2.2 SSL /TLS MITM Attack.....	22
3.2.2.1 MITM Attacks against SSL/TLS.....	23
3.2.2.2 SSL Protocol Architecture.....	24
3.2.3 BGP Based MITM Attack.....	25
3.2.3.1 Attack mechanism.....	25
3.2.3.2 S-BGP.....	26
3.2.3.3 Deployment of S-BGP in the Internet.....	27
3.2.4 FBS-based MITM Attack.....	27
3.2.4.1 GSM Based MITM Attack.....	28
3.2.4.1.1 MITM attack on GSM.....	29
3.2.4.2 UMTS Based MITM Attack.....	31
3.2.4.3 MITM attack on combined UMTS/GSM.....	31
<b>Chapter 4: Prevention Mechanism of MITM Attacks.....</b>	<b>34</b>
4.1 Spoofing based MITM defence Mechanisms.....	34
4.1.1 ARP spoofing defence mechanisms.....	34
4.1.2 DNS Spoofing defence mechanism.....	39
4.1.3 DHCP Spoofing Defence Mechanism.....	40
4.1.4 IP Spoofing Mechanisms.....	41
4.2 SSL/TLS defence mechanisms.....	42
4.3 BGP MITM defence Mechanism.....	43

4.4FBS Based MITM defence Mechanism.....	45
4.4.1 GSM MITM defence mechanisms.....	45
4.4.2 UMTS MITM defence mechanisms .....	47
<b>Chapter 5: Implementation &amp; Result.....</b>	<b>49</b>
5.1 DNS spoofing exploitation. ....	49
5.2 Description of tools.....	49
5.3 Performing attack.....	51
5.4 Result.....	58
<b>Chapter 6: Conclusion &amp; Future scope.....</b>	<b>59</b>
<b>Bibliography.....</b>	<b>60</b>

# List of Tables

## Chapter 2: Review of Literature

Table 1: MITM attacks on different communication channel service network .....	8
--	---

## List of Figures

Figure 1.1: Man –in –the-middle attack. ....	3
Figure 2.1: Graphical Representation of the different web browsers. ....	10
Figure 2.2: Top Network Attacks (McAfee Labs). ....	11
Figure 3.1: ARP spoofing Attack. ....	15
Figure 3.2: DNS spoofing Attack.....	17
Figure 3.3 : DHCP protocol. ....	19
Figure 3.4: DHCP spoofing classification. ....	20
Figure 3.5: Example of a MITM attack against SSL/TLS .....	23
Figure 3.6: SSL protocol structure .....	24
Figure 3.7: S-BGP attestation. ....	26
Figure 3.8: GSM architecture.....	29
Figure 3.9: MITM attack on GSM.....	30
Figure 3.10: Algorithm of the FBS-based MITM attack on GSM .....	30
Figure 3.11: MITM attack on combined GSM/UMTS networks: 1) IMSI catching, 2) obtaining valid AUTN, 3) GSM impersonation.....	33
Figure 5.1:Ettercap graphical. ....	50
Figure 5.2: IP forwarding enable.....	51
Figure 5.3 : Ettercap configuration command. ....	52
Figure 5.4: IP table command enable. ....	52
Figure 5.5: Uncommenting IPtables rules to redirect SSL traffics. ....	53
Figure 5.6: Unified sniffing being selected in Ettercap.....	53
Figure 5.7: Selecting interface in ettercap. ....	54
Figure 5.8:“Scan for hosts” being selected in the hosts section. ....	54
Figure 5.9: Target’s IP being selected in the Ettercap .....	55
Figure 5.10: DNS spoof plugin. ....	55
Figure 5.11: ARP poisoning being activated in MITM (attack) section. ....	56
Figure 5.12: Starting DNS Spoofing in ettercap. ....	56
Figure 5.13: Victim visiting the spoofed website. ....	57
Figure 5.14: Attacker capturing victim’s credentials in ettercap.....	58

# List of Abbreviations

MITM	Man-in-the-middle-attack
OSI	Open System Interconnection Model
ARP	Address Resolution Protocol
DNS	Domain Name System
DHCP	Dynamic Host Configuration Protocol
IP	Internet Protocol
SSL	Secure Sockets Layer
DOS	Denial-Of-Service
BGP	Border Gateway Protocol
FBS	False Base Station
GSM	Global System For Mobile Communications
UMTS	Universal Mobile Telecommunications System
HTTP	Hyper Text Transfer Protocol
TCP	Transmission Control Protocol
AA	Address Attestation
LAN	Local Area Network
LTA	Local Ticket Agent
ASA	Anti-ARP Spoofing Agent
SAKA	Secure Authentication And Key Agreement

# Chapter 1

## Introduction

### 1.1 Background

Man-in-the-middle (MITM) attacks build the assignment of maintaining knowledge vulnerable and private significantly difficult because attacks are regularly established from remote computers with fake addresses. While communications safety turned into in general that of the breaking of encoding transformations (as inside the case of the Enigma device during the Second World War, the matter of protection in computer networks additionally includes active interference by using attackers, and of these MITM attack is one of the most incredible. The MITM attack takes gain of the weaknesses in the validation protocols getting utilized by the communication events. As validation is in general supplied through third parties who problem certificate, the system of certificates technology becomes some other supply of capacity weakness.

These days cyber-attack is also a significant criminal offense and it's going to be a heatedly talked concerning issue additionally. A man-in-the-middle-attack is also a form of cyber-attack wherever an associate unapproved outsider enters into an internet correspondence by two users, continues to get aside from the two parties. The malware that's within the middle-attack frequently monitors and changes individual/classified knowledge that was simply completed by the two clients. A man-in-the-middle-attack as a convention is subjected to associate untouchable within the system, which may get to, study, and alter secret knowledge while not keeping any tress of management. This issue is serious, and most of the cryptographical frameworks while not having traditional confirmation security are debilitated to be hacked by the malware named 'man-in-the-middle attack. The MITM attack makes it possible for the hacker or the unwanted organization to snoop information through the backdoor. Nowadays, the use of the web or cellular networks can be applied to almost any aspect of our life. For example, we use domestic online keeping money, online shopping and entertainment, social systems, and so on. All of these online services store or share confidential data from users, which is a key target for programmers. Other than individuals, programmers target companies and organizations, resulting in enormous economic loss. In this modern world of "people and things constantly linked" by

internet consequences, it is extraordinarily common today, day after day, to be studied around effective attacks on related things and online services. It is regarded as one of the most effective attacks is known as Man-in-the-Middle (MITM), which contributes to the gaining of influence over the exchange of information between end-users [1]. Today, People live in the Digital Age ', where every user interacts directly or indirectly with the aid of the internet. The information shared must have a few levels of security and approval so that accurate contact is given to the client. In achieving a realistic level of security, cyber security plays one of the most vital parts. These days, for example, the individual and confidential information of users in online banking, entertainment, social organization, e-commerce, etc. are being dealt with through the networks, which converts an attractive target for hackers [2]. When communicating over the internet, these goals must ensure secure connections. Any web page is unprotected from attacks if it is not legally protected. The man-in-middle attack can be one of the most popular and effective attacks. In a man-in-the-middle attack, all devices (often a web browser and a web server) are positioned between attackers and captured or modified communication between the two. Then the attackers will collect data and copy either of the two operators. Such attacks can target e-mail communication, DNS lookups, and unsecured wifi networks in addition to websites. Typical targets of man-in-the-middle attacks include SaaS organizations, e-commerce firms, and financial app users. Man in the Middle Attack is one of the most dangerous considerations discussed in more detail in this paper.

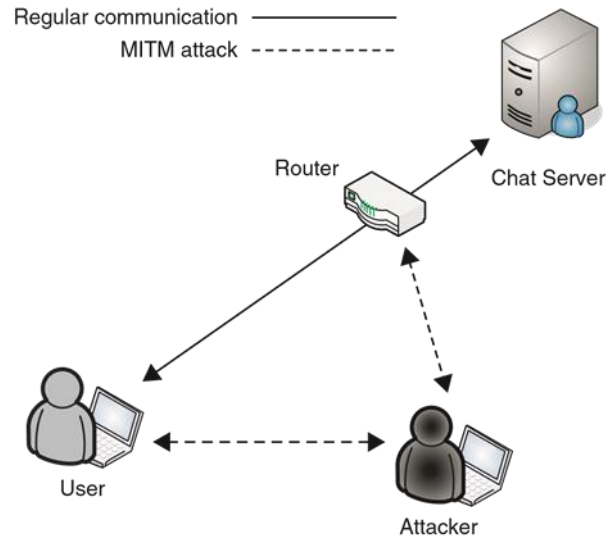
## **1.2 Definition of Man-in –the-middle Attack**

Man-in-the-Middle Attack (often abbreviated MITM) is a type of effective eavesdropping where the attacker generates independent communications with the victims and relays messages between them, making them feel that they are communicating directly to each other via a private link while the attacker manages the whole communication. A man-in-the-Middle Attack occurs only if the attacker can impersonate each endpoint to the satisfaction of the other endpoint. The standard data flow is seen in Figure 1.1 by the strong lines that go to and from the chat server, as well as the MITM attack, defined by broken lines.

## **1.3 How man-in-the-middle attacks work**

Based upon the specific connection of the attacker to the target network moreover Based upon the specific connection of the attacker to the target network moreover the kinds of protocols

adopted to enable the attack, a MITM attack can be analyzed using many techniques. Figure 1.1 provides an outline of the MITM attack structure. Although the figure is simple in explaining the concept, the purpose is to exhibit a snapshot of what could look like a classic MITM attack type.



**Figure 1.1: Man –in –the-middle attack.**

The attacker can use a number of methods to reroute the data between the recipient and the chat server. The attacker requires all messages to pass with his or her computer at the end of the day so that when in movement, he or she can sniff or fix this issue. Second, the attacker may target to fool the user's machine into believing that the attacker's device is the router. So the attacker can make another attack to fool the router into believing that the attacker's device is the user's machine. If the attacker has acted out such attacks on both the user's computer and the router, any data supposed to be transmitted between the router and the user's computer would be redirected via the attacker's device. The attacker also has the power to sniff and alter data meant to be accessed only by the user, the firewall, and the chat server. Although this form of attack sounds difficult, the use of many different methods allows it really simple for an even less advanced attacker to do so. He or she is powerful enough to carry out such a range of attacks until the attacker is being able to more efficiently introduce himself or herself into the connection



process. Network traffic sniffing, order injection, malicious code injection, and public key cryptosystem attacks would be used in these attacks. While many attacks have been listed, several others may be used by an attacker based on the motive of the attack.

## **1.4 Organization of thesis**

This chapter presents the Overall perspectives and the essential motivation behind the study. The rest of the thesis is structured such as follows:

**Chapter 2:** In this chapter, the previous work done in the area of Man-in-the-Middle attack has been analyzed. Then the progress and present scenario of Man- in –the-Middle Attack is also highlighted.

**Chapter 3:** This chapter gives a detailed description of all the classifications of a man-in-the-middle attack.

**Chapter 4:** All necessary approaches for the prevention of man-in-the-middle attacks are provided in this chapter.

**Chapter 5:** This chapter describes the experimental configuration and how the program was used for the execution of the MITM attack.

**Chapter 7:** This sums up the conclusions and observations of the study. This also discusses future aspects of this thesis.

# Chapter 2

## Review of Literature

A review about man-in-the-middle attacks of communication networks in this chapter is provided. It highlights the previous work of MITM attack, progress of MITM and also the current scenario of MITM attack. The attack may be uncovered through the usage of time knowledge in real time contact in many cases.

### 2.1 Previous work

MITM attacks are among the oldest types of cyber-attack. Since the early 1980s, computer scientists have been looking into ways of trying to stop types of threats from exploiting or eavesdropping communication systems. To the best of our understanding, the term Man-In-The-Middle Attack was first stated by Bellare et al. in [3] with approval of [4]. In the security community, the word MITM has turned into a reference attack, with a growing number of citations per year. Ornaghi et al. were the first to propose a security-based tracking site for the suspect and survivor at a European conference in 2003. A. Ornaghi, M. Valleri, in the same year, suggests a concept on man-in-the-middle-attack [5]. They proposed a model of the MITM categorization and prevention mechanisms. In 2004, U. Meyer, S. Wetzel released a Document on the protection framework for the Universal Integrated Telecommunication Model (UITM) where they addressed cell communication 'man-in-the-middle-attack' [6].

In 2006, Kish published his thesis in a listed article, in which he presented MITM's system of encryption Use cipher Kirchhoff-loop-Johnson (-like)-noise [7]. In the security community, the term MITM has become a reference attack, counting a growing number of citations each year. It has been demonstrated that the first Kirchhoff-loop-Johnson (-like)-noise (KLJN) cipher is normally secured from man-in-the-middle (MITM) attack, whether the eavesdropping uses resistors and noise voltage generators much like the sender and the receiver. In all respects, a KLJN cipher is superior in terms of speed, robustness, maintenance, price, and the natural immunity of known quantum communication schemes against the man-in-the-medium attack.

Chomsiri, T. (2008) [8] three different topics presented and analyzed Procedures to avoid the analysis of confidential information E-commerce websites are accessible across the network utilizing MITM. Also, the author has experimented with several methods to capture/decrypt user

data and found that the Static ARP on the switch provides the best results. Hypponen and Haataja (2007) [9] performed work on efficient Bluetooth communication and demonstrated that their device was capable of stopping a MITM attack. Recently, several studies have been further published (Saif et al., 2018) in which specific styles of research on the revised edition of Bluetooth Security Networks has been performed in the implementation plan and different methods for preventing MITM in two-party contact have been addressed. Other published studies (Sounthiraraj et al., 2014) performed work on HTTP security and described MITM as a very important vulnerability and also addressed preventive strategies [10].

Gangan, S. (2015), mentioned MITM happenings DNS spoofing attacks: Password Response Protocol (ARP) server contamination, SSL and hijacking of sessions, and possible prevention measures. Conti, M. Conti. Et al. (2016), an extensive review of MITM attacks [11]. The authors defined and studied the range of MITM attacks and two commonly deployed network technologies, i.e., GSM and UMTS, in the Open Systems Interconnection (OSI) model. Also, implementation measures were given for each MITM class and the categorization of MITM mitigation strategies was ultimately introduced centered on the methods and sense of applicability. The author even provided a quick description of the MITM attacks on other Contact networks such as WLAN, LTE, NFC, etc. Kumar, M.M.S., Indrani, B. (2018) implemented site hijacking techniques and various forms of browser attacks. Authors have also addressed the latest HTTPS Apps useful for avoiding browser attacks [12].

The summary of above literature review, shows that such reports, together with previously established recognition and strongly indicate that the MITM attack has become extremely relevant and popular and, in general, can have an effect on any online activity. Some of them are extensively reviewed and widely analyzed. Researches have been published to detect issues within a particular system, such as MITM attacks on the Address Resolution Process (ARP) or within a specific technology such as Bluetooth. Some measures do not go through the specifics of each MITM attack properly but have partial coverage of the topology of the attack.

For example, A. Ornaghi and M. Vallerii formed the categorization of the MITM attack, which does not include all known attacks. Also, the researchers did not provide for the execution of the attacks but rather gave an abstract description of them. In comparison, the authors have sought solutions in preventive systems but with no clarification of the methods used. For every MITM

attack, they should have explained in the proper way. To give proper visualization about the MITM attack, they should add a large number of explanations of all the attack execution techniques. Also they would have given the prevention mechanisms with proper explanation.

## 2.2. Progress of man-in-the-middle attack

There are two distinct phases of efficient execution of MITM:

**a) Interception:** The initial phase intercepts the client's action via the attacker's device until it reaches its expected target. The most well-known (and easiest) way to achieve this is an idle attack in which the attacker renders free/open wifi hotspots available to general community. Commonly called in a way that is similar to their location, they are not protected by a watchword. Once a casualty gui has been rendered about such a hotspot, the attacker achieves complete penetrability to any online marketplace in details. Attackers attempting to pursue a more complex interception approach can conduct one of the following attacks:

- **IP spoofing** happens when an attacker trying to disguise himself as an application by modifying the packet headers in an IP address. Clients trying to get to the 'URL relating to the application are therefore conducted through the attacker's site.
- **ARP spoofing** is a way of linking the mac address of an attacker to a legitimate user's IP address on a local area network using fake ARP messages. Thereafter, information sent by the user to the delivery of the host IP is transferred to the attacker instead.
- **DNS spoofing**, otherwise known as DNS store poisoning, involves the infiltration of a DNS server and modification of the address record of a site. Additionally, clients trying to get across the site have been sent to the attacker's site via the modified DNS record.

**b) Decryption** when your web traffic has been intercepted, certain methods permit attackers to destroy website protection without your awareness and thus reveal your information. After avoiding the encrypted coding offered by the pages you visit, they can read your personal information in plain text. One includes staying within physical proximity to the actual victim, and a Man-in-the-Browser (MITB) Attack is specifically involving a browser infected with some form of malicious software proxy. The attacker wants exposure to an unsecured or ineffectively rooted Wi-Fi connection for a traditional MITM attack. Such kinds of connections are mostly found in the open regions of free Wi-Fi hotspots and also in the homes of a few people. An

attacker can use code to verify the switch that looks for specific defects, such as using default or poor secret keys, or security gaps due to the switch's poor arrangement. After the Attacker has found the impotence, they will then place their mechanisms in the middle of the client's PC and the client's visit sites.

According to its ease of execution, a fresher version of this attack was gaining popularity with cybercriminals. For a man-in-the-browser attack, one of the attacker's requirements is a solution to inserting malware into the PC, which would then insert itself into the device without the client's permission and then archive the info that is transmitted from the target and the site-specific, for example, financial entities that are embedded into the malware. After the malware has obtained the unique details it has been programmed to obtain, it sends the information back toward the attacker.

### 2.3 Present status of MITM attacks

Most of the MITM attacks nowadays are carried out using communication layers. Open System Intercommunication (OSI) and GSM networks are the communication channels that are most affected by MITM attacks. Table 1 displays MITM attack types on various OSI and Cellular Service networks.

**Table 1**

MITM attacks on various channels of communications

		MITM Types
<b>OSI Layers</b>	Data Links	ARP spoofing type
	Presentation Transport and Networking	SSL decryption, CA decryption IP spoofing
	Applications	DHCP spoofing, BGP type, DNS spoofing
<b>Cellular Networks</b>	GSM	
	UTMS	FBS type

In Table 1, we mention MITM attacks on cellular networks and OSI levels. Every layer applies various security strategies. However, neither is free of the attacks by the MITM. Orghani et al.

was the first to propose a security-based tracking site for the suspect and survivor at a European conference in 2003. The MITM attacks are categorized into three different categories: a) Monitoring LAN (Local Area Network).b) Tracking of virtual network LAN and c) Tracking of virtual networks. The author assumes STP mangle is a closed-loop MITM system because only un-managed traffic between two customers can be decoded by the attacker.

Since we all know, numerous people surf the internet and the numbers are rising every day. So protecting the data obtainable on the internet and ensuring internet protection is important because there remain various bad guys out within the world who want to get the advantage of this and have data breaches and different types of attacks without being recognized. Besides these known MITM attack scenarios, new changes occur and develop regularly in both MITM and other types of attack. Attackers also use malware, use modern social engineering techniques for spyware planting, keystroke loggers. Previous occurrences are being general and targeted at mass numbers of consumers. However, recent events have been aimed at attacks, most regularly directed at commercial firms

CNNIC, which is ministered by the Cyberspace Administration of China (CAC) was granted several untrusted digital records to the separate companies and the general public that were effective for two weeks and expired by April 2015, and that was released to the various companies and the public as a whole as check certificates.

The firewall will release certificates for various domains, and an SSL MIM attack could be conducted, loading this certificate into the firewall device. That's because about all operating system and web browser depends on this altered authorization and would cause a major issue in the ICA program. The web browser will cause problems by trusting the certificate because the holder of the certificate might translate quickly and monitor the contact inside the network with no previous warnings. Just as previously discussed, when users want to visit a specific website and without knowing the users are open to the MIM attack, the bad guys who are out there will show their fake website.

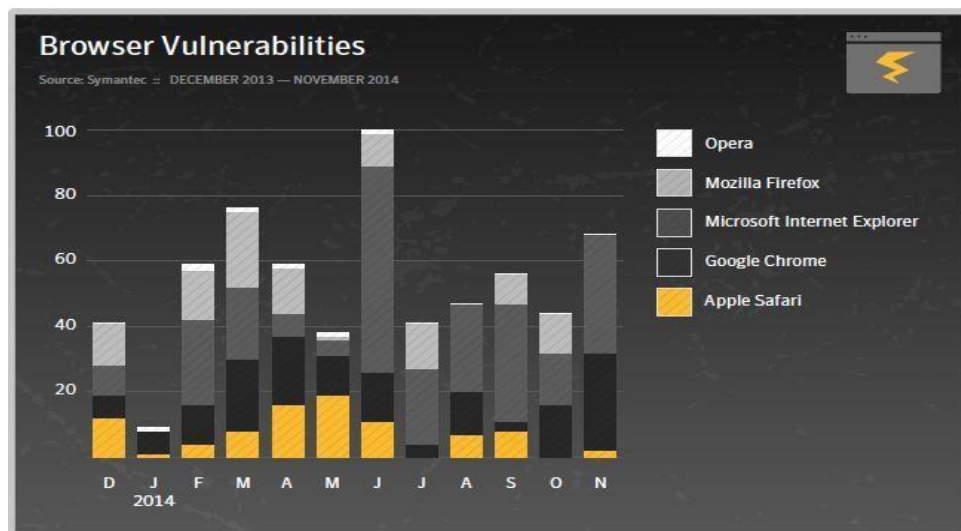
To take care of these differences and put them on the market, web browsers upgrade their current versions. Then the customer may also update and stay upgraded to the latest version. But we noticed that the internet of today often depends on sensitive data to be protected. As almost all

operating systems depend on most certificates, this scenario simply involves a fake certificate to take advantage of by undermining the protection of the complete system.

The threat by SSL on common websites such as google.com, Yahoo.com, live.com, and skype.com is another example of the MIM threat. Comodo, the trustworthy security body, released the fake SSL certificates. The attack, however, has been detected and false credentials have been removed. Such authorization allows various types of attacks, such as malware, will change web services.

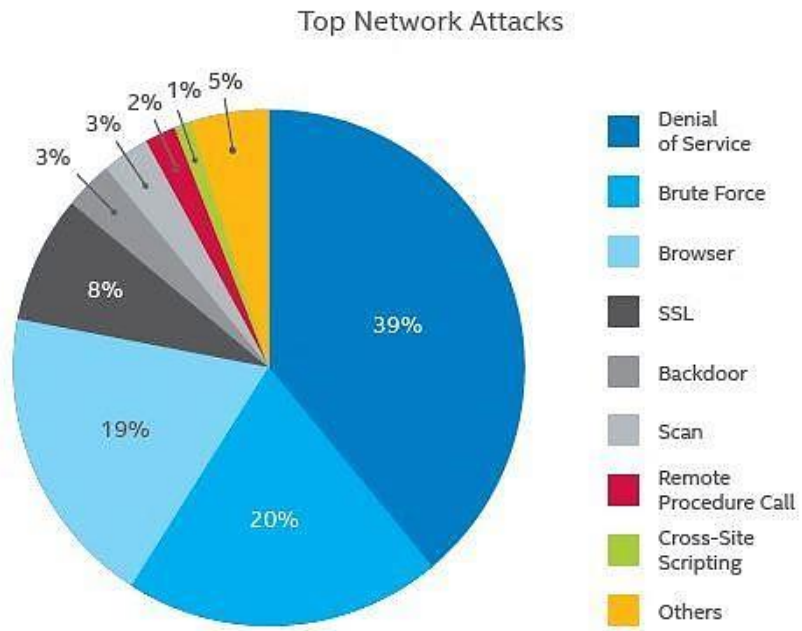
The browsers use sets of authorizations to validate the authenticity of TLS certificates. However, if the internet fails, these termination lists are not available. Consequently, untrusted certificates must permanently be coded into 7 browsers. It was suggested. The number of usable operating systems now has a revoked authorization digital updater enabled. The revoked authorization will be immediately updated without any app information by the automatic update.

The figure shows the statistical information used for the various browsers in our day-to-day life from December 2013 to November 2014 by Symantec Corporation. From the figure, we can underline the most vulnerable Internet Explorer in the diverse attacks.



**Figure 2.1: Graphical Representation of the different web browsers.**

From Figure we can see that, Cyber-attack, Brute Force, and Browser attacks are the largest of the network attacks. The Server Denial, browser, and SSL attack all form the MITM attack.



**Figure 2.2: Top Network Attacks (McAfee Labs).**



# Chapter 3

## Classification of Man-in-the-middle Attack

Throughout this chapter, an effort has been made to identify the MITM Attack category to improve database security. To measure the classification scheme by gathering MITM attacks scientific guides, electronic advisories, online user forums, web pages, and mailing lists. This repository can help users get a better understanding of MITM attacks. It compile weak and strong sides of algorithms through various communication networks. It can also be employed in the evaluation of threat prevention technologies and security software methods.

### 3.1 Characterizations of MITM Attacks

An electronic MITM in the public area can be visualized as a mall with free Wi-Fi and a malicious software-based wireless router. If a user visits the website of a bank from the phone or laptop at that moment, they may lose their bank details. It is possible to perform MITM attacks on various communication networks, such as GSM, UMTS, Long-Term Evolution (LTE), Bluetooth, Near Field Communication (NFC), and Wi-Fi. The goal of the attack is not only the actual data flowing between endpoints, as well as the confidentiality and privacy of the data of its own. At least three ways of characterizing MITM attacks are being defined, leading to three different categorizations.

- 1) Based on impersonation approaches, MITM.
- 2) MITM depending on the channel of communication in which the attack is conducted.
- 3) MITM on the pretext of a position of the attacker and the network target.

### 3.2 Classification of MITM Attacks

MITM Attacks may be classified into four basic types:

- **Spoofing-based MITM** is an attack in which, by means of a spoofing attack, the attacker intercepts a legitimate communication between two hosts and control data transmitted, whereas hosts are not aware of the presence of a middle man. In certain cases, the attacker spoofs devices between victims (e.g. DNS spoofing), in other cases (e.g. ARP spoofing), the attacker spoofs the devices of the victim directly. . Spoofing-based MITM attacks where an attacker intercepts the legitimate traffic by spoofing attacks and controls the transmitted data without the adverse presence of hosts.

- **SSL /TLS MITM** is an attack where the attacker introduces himself into the contact channel between two victims (usually the victim's browser and the webserver) as a means of effective network interception. Then the attacker installs two separate SSL connections with each user so that the middleman is not exposed to both. The attacker transmits messages between them. This setup allows the attacker to capture and selectively change all messages on the wire.
- **BGP MITM** is an attacker who targets the hijacked traffic to the target. This allows traffic to be controlled through the Autonomous Station (AS) of the attacker and where traffic changes are managed.
- **False Base Station MITM (FBS-based)** is an attack that causes third parties to communicate with a BTS, and then, through the attacker tries to manipulate the exploitation of victims

### **3.2.1 Spoofing-based MITM Attack**

A spoofing attack is a malicious party's impersonation in the network of a device or user. Spoofing attacks are used as a platform for other threats, such as DoS, MITM, or hijacking session attacks. In all spoofing styles, perpetrators use the vulnerability of the same protocols-a lack of verification of the source and destination communications. There are several kinds of spoofing attacks that can be used by malicious parties:

1. ARP spoofing,
2. DNS spoofing,
3. DHCP spoofing,
4. IP spoofing.

Such MITM attacks focused on spoofing are discussed below:

#### **3.2.1.1 ARP spoofing-based MITM attack**

Network applications are using the ARP protocol to assign media access control (MAC) addresses to their network addresses. For LAN communications, ARP is crucial, as every frame leaving a host needs to include a MAC address for a destination. ARP is a trustworthy and most significant LAN communications protocol [13]. Adversaries change the local ARP cache table and link the MAC address of the host to the destination IP. ARP manages the two types of ARP request packets and ARP reply. The MITM attack provides access to privacy details for the consumer. Such ARP spoofing can be subdivided into two basic types namely host cheating and internal network gateway cheating. Whenever a server has to connect to a network of the same

client, it transmits the ARP message to the network. The cache entries are easy to manufacture as authentication mechanisms are absent.

By changing the local ARP cache table of victims (adding, upgrading database entries), the attacker can link the MAC address of a malicious host to a target host's IP. The attacker may therefore initiate a DoS target, attack MITM, and obtain entrance to confidential data.

If a host wishes to connect with another host based in the same network, the host must send an ARP response to all host positions on the network. It is expected that only the host with the declared IP can matter a response that includes its MAC address. Nevertheless, if the ARP cache is handled in a dynamic mode, fake ARP messages can easily make cache entries, as there is a lack of a proper authentication mechanism. The source machine also saves the IP to MAC entry in its local cache so that next time contact can be improved, the broadcasts are avoided.

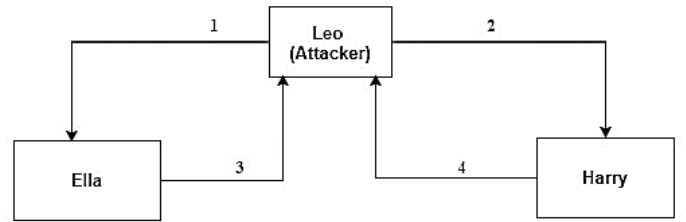
ARP is a stateless protocol, which lacks caching system security. Suppose we've got next network: the attacker Leo (IP= 10.0.0.5, MAC= FF: FF: FF: FF: FF: FF), the victim Ella (IP= 10.0.0.3, MAC= AA: AA: AA: AA: AA), and the victim Harry (IP= 10.0.0.4, MAC= BB: BB: BB: BB: BB: BB). The next steps to complete an ARP spoofing-based MITM attack are required (see Figure 3.3)

Leo gives Ella an ARP Response message saying IP: 10.0.0.4 has MAC address: FF: FF: FF: FF: FF: FF. This response upgrades the chart on Ella's ARP.

2) Leo also gives Harry an ARP Response message stating that IP: 10.0.0.3 has MAC address: FF: FF: FF: FF: FF: FF: FF: FF: FF: FF. This response changes the ARP table of Harry.

3) If Ella wants to send a message to Harry, it goes to Leo's MAC address FF: FF: FF: FF: FF: FF, instead of Harry's BB: BB: BB: BB: BB: BB.

4) If Harry wanted to send a message to Ella, it'll go to Leo as well.



Ella's ARP cache :	Harry's ARP cache :
IP <sub>Harry</sub> = 10.0.0.4 MAC <sub>Harry</sub> = BB:BB:BB:BB:BB:BB	IP <sub>Ella</sub> = 10.0.0.3 MAC <sub>Ella</sub> = AA:AA:AA:AA:AA:AA
IP <sub>Leo</sub> = 10.0.0.5 MAC <sub>Leo</sub> = FF:FF:FF:FF:FF:FF	IP <sub>Leo</sub> = 10.0.0.5 MAC <sub>Leo</sub> = FF:FF:FF:FF:FF:FF
Ella's ARP cache after ARP spoofing:	Harry's ARP cache after ARP spoofing:
IP <sub>Harry</sub> = 10.0.0.4 MAC <sub>Harry</sub> = BB:BB:BB:BB:BB:BB	IP <sub>Ella</sub> = 10.0.0.3 MAC <sub>Ella</sub> = AA:AA:AA:AA:AA:AA
IP <sub>Leo</sub> = 10.0.0.5 MAC <sub>Leo</sub> = FF:FF:FF:FF:FF:FF	IP <sub>Leo</sub> = 10.0.0.5 MAC <sub>Leo</sub> = FF:FF:FF:FF:FF:FF

**Figure 3.1: ARP spoofing Attack.**

### 3.2.1.1.1 Attack Mechanism

ARP does perform –

- If one device has to communicate with another, its ARP table will look up.
- If the MAC address is not contained in the list, otherwise the ARP request would be transmitted across the network.
- This IP address will be compared to the MAC address for all devices on the network.
- If this address is found by one of the machines in the network, it will react through its IP and MAC address to the ARP request.
- The requesting device must place the pair of addresses in its ARP stack, so there'll be correspondence.

### **3.2.1.1.2 ARP spoofing implications**

As mentioned above ARP spoofing where an attacker may transmit a fake ARP message in excess of a local area network to link the victim's IP address to the attacker's system mac address. As a result, all data meant for the victim can hit the attacker first. The attacker may then collect confidential information or plan for further attacks.

Several important implications will occur:

- When the attacker connects several IP addresses to the victim's Mac address, packets intended for several IP addresses may enter the victim on their own and may result in a denial of service attack.
- An attacker can steal the victim's session-id, then enters personal information
- The attacker can exploit and change the traffic targeted for the victim, which could lead to a man in the middle attack.

### **3.2.1.2 DNS spoofing-based MITM attack**

DNS spoofing is a form of attack in which a malicious attacker intercepts DNS queries and returns the address that instead of the actual address leads to its domain.

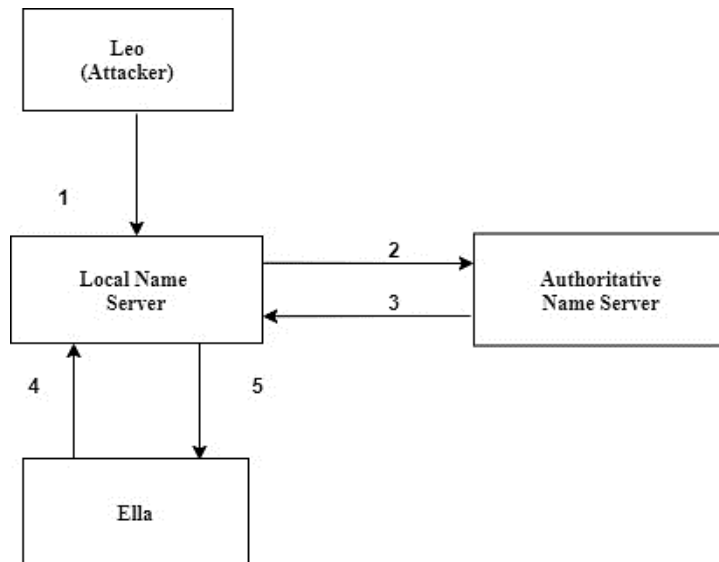
Hackers may use DNS spoofing to conduct a man-in-the-middle attack and guide the user to a false site that looks like the real one, or they can easily redirect traffic to a real site and steal details silently.

DNS spoofing, which is carried out through cache poisoning, is one of the most popular and dangerous DNS attacks (DNS spoofing is quite often named DNS poisoning). To increase performance, the DNS service uses a cache method, but it has several weak sides. DNS spoofing consists of inaccurate or destructive datatypes among symbol names and IP addresses being resolved by DNS storage.

Based on Kaminsky's [14] method: a network of two name servers, attacker Leo and victim Ella. Also, let's assume that the local DNS does not have the requested address query and that the Authoritative Name Server (ANS) is deployed by the attacker. Next steps should be performed to execute DNS spoofing Eve (see Figure 3.2):

- Leo makes a DNS server inquiry to retrieve the IP of a single website (dtu.dk).
- The local DNS server does not have the address, and the query is transferred to the ANS to mitigate it.
- ANS respond with incorrect details (dtu.dk IP address is 206.2.22.25) and potentially add a little more fields. Local DNS saves data to the TTL time cache.
- Ella enquires to locate the dtu.dk IP address.
- The DNS will respond with 206.2.22.25, and Ella will be directed to the server of the attacker.

At this point, Leo only has contact to single endpoint, which customs its rogue server. The attacker can introduce a rogue server phishing website or service that will connect with the original one to increase the attack to DNS spoofing based MITM. The example reveals the scheme of rogue DNS spoofing in the network, but claims Eve is not the owner of the ANS. Then she can send a spoofed message to local DNS immediately after it asks for ANS data. Local DNS would, therefore, overwrite caches and block responses from legitimate ANS, as a replay attack security.



**Figure 3.2: DNS spoofing attack.**

### **3.2.1.2 .1 Attack Mechanism**

As such, the ultimate goal of the attacker is typically the same regardless of the tool they use. Either they're trying to steal details, guide you to a website that helps them or steal personal information. The most talked-about strategy for spoofing DNS is utilizing cache poisoning. DNS spoofing is an overarching term and can be performed using different methods, like:

- DNS caching poisoning
- Committing a DNS server
- Implement a man-in-the-Middle Attack

To perform DNS spoofing, attackers need to overwrite local DNS routing entrances with scam data that will cause the user to utilize a rogue server. DNS renews the cache based on the TTL of the posts, and from time to time it searches for changes to certain DNSs. This can be used by the attacker to launch a DNS spoofing attack. There are two techniques of poisoning the cache:

- Inserting a rogue DNS server into the network that will generate fraud data (may lead to the spread of scam data no single to target DNS but to adjacent DNSs).
- Sending a fake DNS reaction right before the actual DNS sends a valid one (by default DNS accepts the first response, and discards the next automatic).

### **3.2.1.3 DHCP spoofing-based MITM attack**

DHCP is the protocol for the client-server. DHCP's architecture consists of a DHCP server that is responsible for allocating parameters to a DHCP client for network configuration. DHCP client is a host running the DHCP client program which requirements to connect to a network. The DHCP client requires network configuration parameters, including IP address, subnet mask, default gateway, DNS server, and leased time, to be able to communicate with other hosts in the network [15].

In the maintenance of networks, DHCP plays a significant role. DHCP, however, has a range of well-known safety issues, particularly:

- DHCP does not provide the root validation of DHCP messages. DHCP clients cannot, on the one hand, ensure that they are related to a reliable DHCP server. On the other side, the DHCP provider cannot guarantee that it connects with a legal device.

- Every DHCP response is sent in plain text.

### 3.2.1.3.1 DHCP Protocol:

- The host running the DHCP client program transmits DHCP DISCOVER messages to the network.
- The DHCP server that receives the DHCP DISCOVER message tests its usable network configuration parameters, in particular the IP address, and sends the DHCP OFFER response to the requesting device.
- When the client receives the proposal, the client sends the DHCP REQUEST message to the selected DHCP server to order the lease of the network outline factors listed above.
- The DHCP server which receives the request sends a DHCP ACK message as confirmation of the client's request. After this stage, the DHCP client can use these parameters for some time and requires a new set of parameters to request.

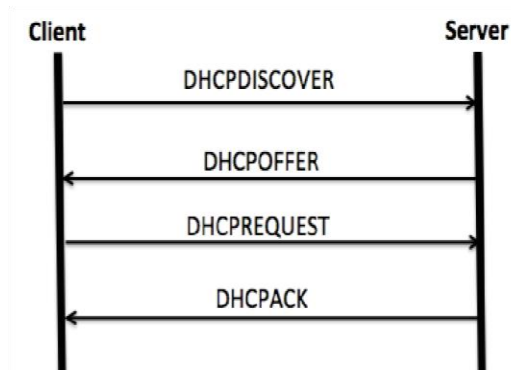


Figure 3.3: DHCP protocol.

### 3.2.1.3 .2 Classifications of DHCP spoofing

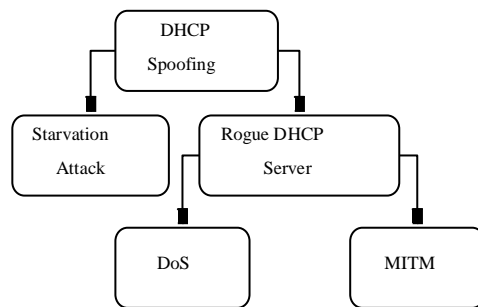
A number of DHCP attacks have been conducted based on vulnerabilities. Discuss the following possible attacks on the DHCP protocol below:

1. **DHCP starvation attack** occurs in which a user gives a set of DHCP DISCOVER messages to the DHCP server with spoofed MAC addresses. If the server receives this message, it assigns the appropriate IP addresses. However, the IP addresses available for each DHCP server are reduced such that the DHCP server will eventually run out of its



authorized clients' IP addresses. This is considered an attack of type Denial-of-Service (or DoS).

- The rogue DHCP server** is an unauthorized DHCP server installed on a network without the authorization of a network administrator. This can contribute to an issue when a new client tries to link to the network by transmitting a DHCP DISCOVER message. Such a message can be sent by a rogue DHCP server in front of a legitimate DHCP server. The rogue DHCP server will then send DHCP OFFER to the client before one from the legal server. Since DHCP OFFER includes network configuration parameters, such as the IP address of the default gateway, the client host can be designed with these parameters. The attacker can attach the IP address of the default gateway to his device. This allows the attacker to intercept and evaluate any packet transmitted from the client to the network.



**Figure 3.4: DHCP spoofing classification.**

### 3.2.1.4 IP spoofing-based MITM attack

IP is the main protocol on the Internet that runs on the network layer of the OSI architecture. IP spoofing is an attack in which a host (or rightful user) is impersonated on the IP layer by the attacker [16]. Mostly Cases aim to attack the relationship of trust between two hosts that relation depends on the IP source Key that authenticates a host correctly. The attack is nothing more than Possible where the goal host has a relationship of confidence with at Mind you one more host. The most common link of confidence is provided by the file with .rhosts found on unix operating Systems, though there are several more, for example, Unix files Servers. allow.equiv servers, etc. In itself, IP spoofing is quite simple, all the attacker has to do produces an IP datagram with deceptive source code. There is no way for the aim host to measure that an IP datagram has been spoofed, all it needs to rely on is the address of the IP source. IP spoofing is mostly on its own

restricted to provide privacy for the start of the intruder Attacks on the IP wall, e.g. ICMP redirects, ping flooding, etc.

#### **3.2.1.4.1 Attack Mechanism**

- The function is to send packets from the source host to the destination host exclusively based on the IP addresses in the packet headers.
- IP describes the packet architectures that encapsulate the data to be supplied.
- It also specifies the addressing methods used to mark the datagram with both the source and destination information.
- IP uses a connectionless design, which ensures that there is little knowledge regarding the communication state used to redirect packets to the network.
- In comparison, IP does not define a mechanism for validating the source validity of a packet. This means the attacker could manipulate the source address to be whatever it wants.

#### **3.2.1.4.2 Classification of IP Spoofing**

IP spoofing-based MITM is an attack when a malicious party intercepts a legal contract between two non-malicious parties. The malicious user manages the flow of contact and can erase or change the details received by one of the original participants without the awareness of any of the original endpoints. To achieve such results, attackers may use some IP spoofing techniques which may be classified as follows:

- **Blind and Non-Blind spoofing**

The distinction between these two forms is that the non-Blind spoofing of the attacker is from the same subnet as the target, which opens up the chance of sniffing on sequence and identification numbers. Blind spoofing requires an attacker to first send requests to a network and then analyze the transmission sequence. Both methods are usually used for DDOS attacks but are also executed as a data mining phase for an IP spoofing-based MITM attack.

- **ICMP Spoofing**

IP utilizes ICMP to deliver one-way messages to incorporate different error detection, input, and checking capabilities. ICMP has redirect messages that are usually used to alert routers of a better path. These messages can be misused to implement the MITM attack, as the ICMP does not have authentication mechanisms. The attacker spoofs ICMP Redirect messages to route victims' traffic via their router, where they can be eavesdropped and changed.

- **TCP Sequence-Number prediction**

TCP is a connection-oriented protocol, meaning a connection link should be established before communication begins. It is done with a three-way handshake: SYN, SYN-ACK, ACK. For data recognition, TCP uses sequence numbers. Such numbers enable the protocol to reduce data loss and classify out-of-order packets to ensure reliability in the same way. Numbers are generated in a manner known to both parties, pseudo-randomly. The concept of Sequence-Number Prediction is to find the algorithm of generation of sequence numbers, and then use that information to intercept an existing session (often referred to as an allowed session attack by Hijacking).

### **3.2.2 SSL /TLS MITM Attack**

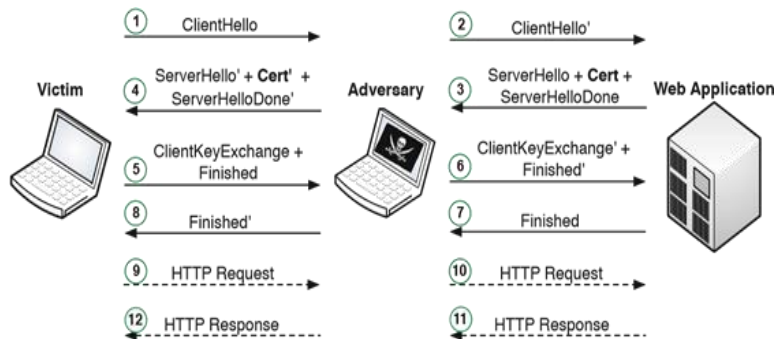
A brief introduction to this segment explains the SSL / TLS MITM attack. Then, describe the protocol of the SSL / TLS MITM attack.

Many e-commerce systems used currently use the Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocol to authenticate clients and files. Secure the contact path between the client and the server cryptographically [17]. While SSL / TLS offers support for user authentication based on public-key certificates, in reality, due to the slow implementation of such certificates, user validation typically occurs on the application layer. There are other choices here, include Personal Identification Numbers (PINs), Passwords, Passphrases, and strong security methods such as one-time password (OTP) or challenge-response (C / R) schemes. Although developers are contemplating SSL and TLS protocols, in the vast number of citizens to be healthy and safe in action SSL / TLS-based e-commerce systems that support e-commerce app authentication on the framework layer are weak Phishing, Internet spoofing, and most importantly Man-in-the-Middle (MITM) attacks. If the MITM is willing to place himself

between the customer and the application so that he can function as a proxy, authenticate to the computer on the device. The name of the customer. Even worse than that, if the MITM is working in real-time, most app authentication frameworks (decoupled) through the establishment of the SSL / TLS session) may be defeated Or it was misused. Generally, that is ignored as people speak the assumed reliability of SSL / TLS-based e-commerce systems, such as online banking or remote banking voting on the Net.

### 3.2.2.1 MITM Attacks against SSL/TLS

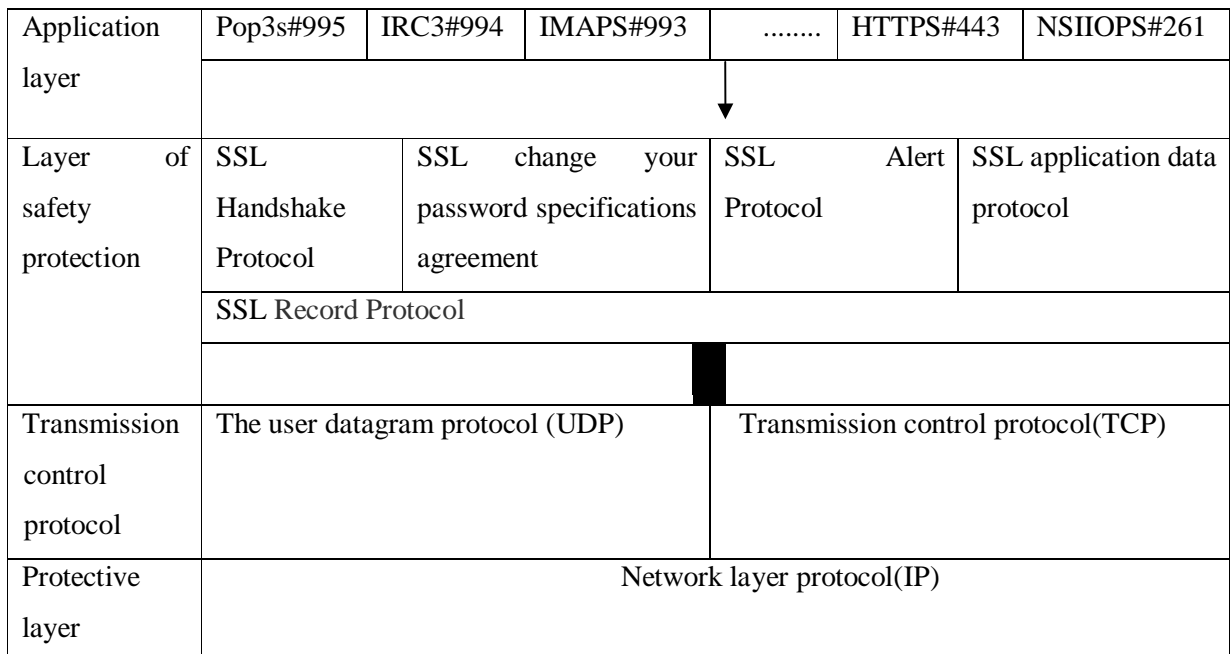
The security securities that SSL / TLS provides depend on the server's exact validation [18]. All these assurances are made useless if an adversary can convince users to approve a certificate illegitimately obtained as seen in Figure 3.5. Next, the attacker places himself among the victim's device and the server in the network direction. While the victim conducts a request to create a new SSL/TLS link through the server (message 1), the adversary uses a fake certificate (Cert') to intercept and respond to it (message 4). If the victim accepts this certificate, then the opponent (messages 5 and 8) completes the SSL / TLS setup, which has been successfully masked as a server. Around the same time, the adversary creates a new server SSL / TLS interface (messages 2, 3, 6, and 7). The opponent has two active SSL / TLS connections at this point: one with the victim, and the other with the server. But from the standpoint of the client and the server, there's only one safe connection in operation. The opponent can now decrypt, re-encrypt, and transmit all messages swap over among the victim and the server (messages 9 through 12). Consequently, the attacker can contact private information (e.g., passwords).



**Figure 3.5: Example of a MITM attack against SSL/TLS**

### 3.2.2.1 SSL Protocol Architecture

The SSL protocol is positioned in the TCP / IP network. Network System Architecture and Device System using TCP Providing a secure approach to the approach of intelligence forces Allows communication between the client and the server does not eavesdrop, and still search the file, and then select Customers to be audited. SSL protocol with encryption algorithm was completed, consultations on the secret key and computer correspondence Authentication until receipt of order, and after receipt what data is passed on via the program protocol Encoded. SSL consists basically of two protocols. Together with function, as seen in figure 3.6. From the Architecture, the SSL encryption specification can be used Consists of SSL communication form, SSL authentication update Protocol, SSL protocol, SSL alarm protocol, and SSL record protocol. The superstratum must, therefore, obtain the data creating it. Application line, utilizing a robust transport layer protocol e.g. TCP, UDP) to bring down to record data. The bottom of the SSL is the SSL record protocol, which loads encapsulation and transfers data that shape a superstratum. The encapsulation steps are as follows: First: High-rise data is separated into 214 bytes or smaller blocks; Second: Each block will be compacted and the message authentication code (MAC) will be handled, and then the MAC will be appended to the end of the related compressed data.



**Figure 3.6: SSL Protocol Structure.**

### 3.2.3 BGP Based MITM Attack

A brief overview of the BGP MITM attack is provided in this section. Then discuss the specifics of the S-BGP.

Internet routing is applied to utilize a multi-router distributed network organized into functional domains called Autonomous Systems (ASes) [19]. Using Border Gateway Protocol (BGP), updated messages, routing information are exchanged between ASes. BGP has a variety of bugs that can be abused to create issues such as consumer data misdelivery or non-delivery, network resource exploitation, network latency, and packet delays, and violations of local routing policies.

The Border Gateway Protocol (BGP), which is used to communicate routing details between autonomous systems, is an essential component of the internet routing network. Secure BGP (S-BGP) addresses essential BGP limitations by offering a modular way to check the validity and authorization of BGP control traffic. To order to encourage widespread acceptance, S-BGP must prevent unnecessary overheads (processing, bandwidth, storage) and must be increasingly deployable, i.e. interoperable with BGP.

#### 3.2.3.1 Attack mechanism:

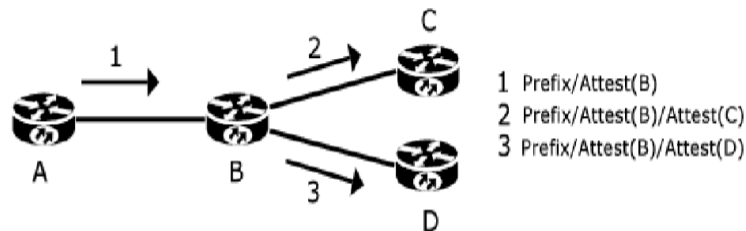
- This BGP-related MITM attack is based on IP hijacking and is also often referred to as BGP hijacking or prefix hijacking or hijacking of routes.
- When a compromised BGP speaker declares that it will take longer network prefixes to more common paths, this contributes to IP hijacking.
- If the BGP MITM attack is launched the traffic destined for any particular IP address will not reach the destination.
- To perform these attacks, the adversary must customize the advertisement routers for network usability. It then has to advertise specific routes inside the global routing table.
- Next, the attacker will deliver the network traffic to suitable destinations. These attacks by the BGP MITM cause the loss of some part of the internet.

### 3.2.3.2 S-BGP

BBN researchers developed Secure BGP (S-BGP) as an extension to BGP to shield BGP from mistaken or harmful UPDATES. S-BGP adds strong capabilities for authorization and authentication to BGP based on public-key cryptography. S-BGP generates three big BGP additions [20]. Firstly, it implements a Shared Key Infrastructure (PKI) for approving prefix possession and validating routes inside the inter-domain routing network. Second, BGP Updates are introduced with a new transitive attribute. The characteristic assures routing UPDATE permission and avoids path adjustments from intermediate S-BGP speakers.

Address Attestations and Route Attestations are two key features of S-BGP. The Address Attestation (AA) is generated by the owner of the prefix, and S-BGP routers are used to verify that the origin AS is authorized to advertise that address block. Route Attestations (RAs), on the other hand, are added by S-BGP routers in UPDATES, allowing the neighboring AS to propagate the route contained in that UPDATE. S-BGP is using PKI infrastructure to authorize AAs and RAs. Private keys are held in S-BGP speakers, while public keys are given by a hierarchical PKI network.

The RAs are daisy-chained as UPDATE flows through the S-BGP router sequence. Each S-BGP router along the path must validate the integrity of the UPDATE before signing and re-advertising the UPDATE to its neighbors. Figure 3.7 indicates an UPDATE flowing from the root AS speaker



**Figure 3.7: S-BGP attestations.**

A to router B and so on. The following 6 measures explain the procedure of the protocol.

1. A produces a RA for the P prefix that shows B as the next-hop for that path.

2. A sends the UPDATE to B, including the RA.
3. B validates the RA signature using the A public key.
4. B even searches the AA for P (retrieved offline) to verify if A is the real owner of the prefix.
5. B confirms whether B is the next hop in the RA.
6. B generates two new RAs for its peers C and D, contains each RA in a different UPDATE, and forwards both UPDATES to C and D.

### **3.2.3.3 Deployment of S-BGP in the Internet**

In addition to the basic issue of how to secure BGP, there is a problem with how to execute the solution on the internet. Deploying S-BGP would include the implementation of this technology by ISPs and router vendors, plus PKI help through registries that assign autonomous network numbers to ISPs and DSPs (downstream providers) and address prefixes to users. Due to the distributed management of the internet infrastructure, the expected increase in the size and connection of the internet, the high volume of BGP UPDATE traffic, and the limitations of resources in the routers and circuits of the internet, it is extremely important that S-BGP be scalable and progressively deployable.

- **Scalability** – The effect of S-BGP on the CPU and storage use of the router and the bandwidth of the network must be within reasonable limits.
- **Deployability** – To successfully deploy S-BGP, two main issues need to be addressed. First, the S-BGP counter-measure information must be transmitted among S-BGP routers in the same AS. Also, when S-BGP implements a new BGP path feature, it is important to have compatibility issues between S-BGP and BGP-4 so that these countermeasures can be deployed incrementally.

### **3.2.4 FBS-based MITM Attack**

A brief overview of the FBS attack as well as its relation to the MITM attack is given in this section.

False Base Station (FBS) attack is an attack when malicious third parties cover up their Base Transceiver Station (BTS) as a real BTS network. A fake BTS system is equipment that can act



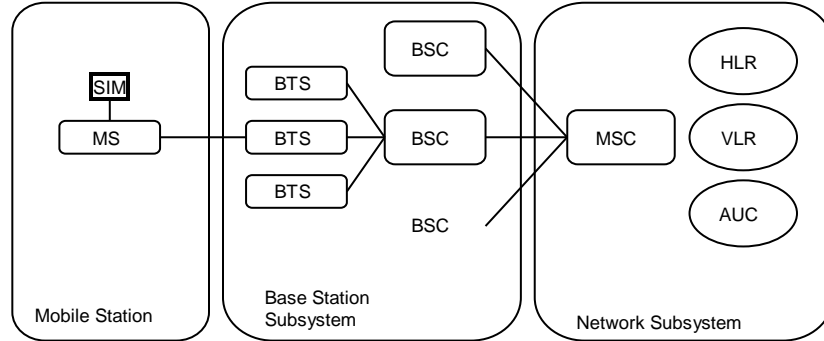
as a real BTS, it transmits BTS signal over the air and makes mobile phones connected to it in a covered area. FBS attack could include the real-time jamming system that blocks all active carriers in the area. Using the jamming method, attackers will drown legal BTSs and force victims to link to fake ones. One-way authentication systems, where connected nodes are unable to validate serving network authenticity, show weakness to the FBS attack. GSM and the combined networks GSM / UMTS, for example, are vulnerable to this attack. FBS-based MITM is an attack in which the victim is forced by third parties to connect to the fake BTS and then manipulate the victim's traffic using this station. An attacker may use a few fake BTSs with different protocols to execute such MITM.

### **3.2.4.1 GSM Based MITM Attack**

In the early 90s, the European Telecommunications Standards Institute introduced GSM as a telecommunications standard of the second generation (2 G). GSM covers more than 90 percent of the world population today, according to the mobility report, there are two basic types of services offered through GSM: telephony and data bearer. The GSM has undergone gradual improvements that have resulted in several versions such as GSM1800, HSCSD, EDGE, GPRS, and the third generation of cellular networks. The Global Mobile Communications System (GSM) several mechanisms have been adopted that provide authentication process [21] and confidentiality of user data.

The architecture of GSM (see Figure 3.8) consists of Mobile Stations (MSs) and BTS, which communicate with each other through radio connections. Every BTS connects to Controller Base Station (BSC). BSC connects to the Mobile Switching Centre (MSC), which is in charge of routing signals from and to fixed networks. The Home Location Register (HLR) and also the Visitor Location Register (VLR) are the two primary databases inside the GSM system for each mobile service provider. HLR is known for maintaining the details regarding the user and its present position.

VLR is liable for protecting visitor records. MSC links wireless and wired networks together. There is a hidden key for each GSM subscriber that is contained in the MS Subscriber Identity Module (SIM) card. There is another hidden key to the Authentication Centre (AUC) that is exchanged by both the subscriber and the AUC. For encryption and authorization deployment, AUC includes a collection of security specifications.

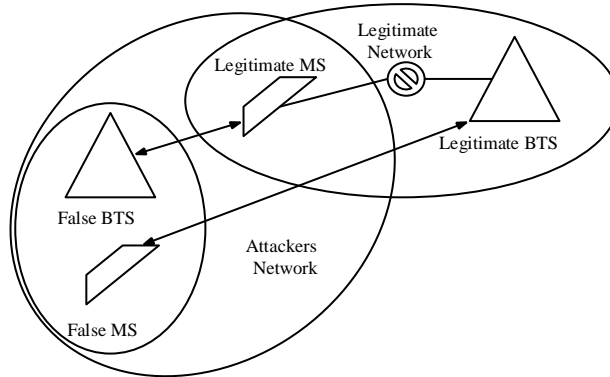


**Figure 3.8: GSM Architecture.**

### 3.2.4.1.1 MITM attack on GSM

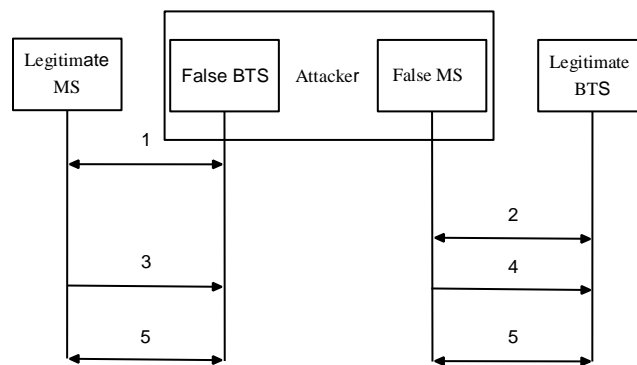
The vital concept behind the attack is to translate the same cell network code as the real GSM network to fake BTS and to assure the victim that such a station is correct. For example, the network consists of the Legitimate MS, the Legitimate BTS, 84 False BTS, and False MS. Attacker's network is a mixture of False BTS and False MS. Binds to the better transmitted BTS when in standby mode. False BTS would either be more effective than the original one, or similar to the mark. If the target is already linked, the attacker would have to create the specific stations. The algorithm for the FBS-based MITM attack on GSM is as follows:

- 1) The attacker creates a link between Fake BTS and Legitimate MS.
- 2) False MS imitates the victim's MS through the actual network by resending the identification details provided in step 1.
- 3) Victims MS shall send the False BTS their authentication information and cipher-suites.
- 4) Attacker forward communication from stage 3 to the Legitimate BTS with altered MS authentication capability not endorsing encryption (A5/0 algorithm) or a poor encryption algorithm (e.g. A5/2).
- 5) Legal MS and BTS share authentication request (RAND) and authentication response (SRES), which is forwarded by the attackers.



**Figure 3.9: MITM Attack on GSM.**

At last, the authentication is done. Both the following communications between the victim and the real network are transmitted via the attacker's entities, with an attacker's encryption defined, or no encryption at all. This influence is conceivable because GSM does not provide data integrity, as a result, the attacker can catch, modify, and forward messages. At the design phase of the GSM protocol, FBS appears to be unrealistic due to the costly equipment needed, but this method of attack is now completely available as costs have declined (Feher et al., 2018). Ho, Paik et. Al. (2010); in addition to explaining GSM protection issues, found out that the attackers are better prepared today.



**Figure 3.10: Algorithm of the FBS-based MITM attack on GSM network.**

### **3.2.4.2 UMTS Based MITM Attack**

In the early 2000s, the 3rd Generation Partnership Project (3GPP) developed UMTS, which is part of the third-generation (3G) telecommunications standards. According to Ericsson. Traffic and market report more than 45 percent of the world were protected by 3G in 2011 and would hit 85 percent in 2017. The cycle of rising UMTS results in the presence in certain places of one (GSM) or both (GSM and UMTS) base stations.

UMTS is the successor on GSM and contains several modifications to eliminate vulnerabilities. GSM facilitates the security and user verification of the network interface between BTS and MS. UMTS offers improvements and added functionality such as transmission information integrity safety and verification tokens. UMTS also provides better cryptographic primitives and 128-bit cipher keys. The communication speeds of UMTS networks are also higher.

From the beginning, the UMTS Authentication and Key Agreement (AKA) protocol were planned to overcome MITM attacks [22]. Mutual authentication utilizes an authentication quintet, which serves to guarantee that a bill is sent to the correct user. Support for GSM networks through UMTS contributes to vulnerabilities. The combination of two specifications helps us to interconnect, but that is roaming between two networks that are not similarly well secured from malicious attacks. As a consequence, certain compliance problems with GSM can be exploited with UMTS networks to perform MITM attacks.

### **3.2.4.3 MITM attack on combined UMTS/GSM**

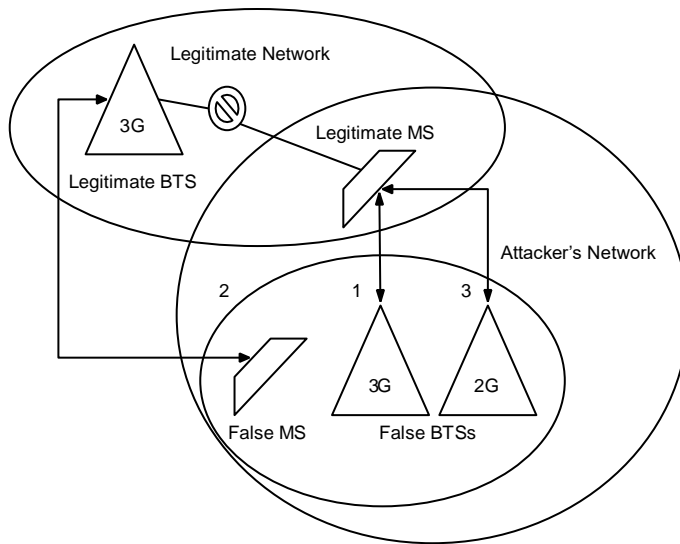
To set up a man-in-the-medium attack against a customer of a UMTS-only cell station, the attacker will have to impersonate a legal network to the device. However, in the case of UMTS-only hardware, the combination of two different protection protocols defends the mobile station from this attack: the AUTN authorization token and the validity of the protection mode command code.

UMTS assures the origins and freshness of authentication by way of AUTN. AUTN requires a Message Authentication Code (MAC) and Series Number (SQN). The right MAC means that the authentication token was created by the valid network, and SQN shows how old the AUTN is. Both values are verified on the MS side, but the AUTN process may be compromised if the user

is on the GSM network. Running MITM on a joint GSM / UMTS intruder has two difficulties: stealing AUTN and confirming that no coding is used during authentication.

The first problem can be solved by impersonating the victim's MS to false MS. The second problem can be solved by sending false information about the victim's MS encryption capabilities, leading to no encryption mode. For example, a network consists of the Valid 3 G BTS, Valid MS, False 3 G BTS, False 2 G BTS, and False MS. The network of Attackers is a combination of False 3 G BTS, False 2 G BTS, and False MS. including a MITM attack on GSM valid MS should not be linked to the local actual station. The MITM attack algorithm on a combined GSM / UMTS is as follows (see Figure 3.11).

- The attacker launches 3G Fake BTS and steals the International Mobile Subscriber Identification (IMSI) of the victim's MS.
- Attacker utilizes the victim's IMSI to impersonate the victim's MS to Fake MS. Then AUTN is disconnected from the actual network (from HLR utilizing the Legal 3G BTS link) and, after processing the data, the connection is broken. At this point, the attacker has an AUTN value that would prove to the Legitimate MS that False 2G BTS is a valid network.
- The attacker begins 2G Fake BTS and pressures the target to sign in. after the victim's MS has successfully verified the authentication token, the attacker sends a preferred encryption message or no encryption message.
- In the end, to stop MITM, the attacker must provide access to a real network through a connection between incorrect MS and a genuine network. The last step of the process has apparent drawback-it leaves a residue. Using False MS to redirect intercepted traffic will uncover the Universal Subscriber Identity Module (USIM).



**Figure 3.11: MITM attack on combined GSM/UMTS networks: 1) IMSI catching, 2) obtaining valid AUTN, 3) GSM impersonation.**

# Chapter 4

## Prevention Mechanism of MITM Attacks

Man-in-the-Middle (MITM) attacks become a strategy for hackers to steal information. Man-in-the-Middle attackers may use a variety of techniques to fool users or exploit vulnerabilities in the cryptographic protocol. It is important to take precautions to prevent MITM attacks before they occur, rather than try to detect them while they are active. Safe communication is not necessary to fully stop MITM attacks. The powerful and effective defense system required will successfully prevent an attacker from executing a MITM attack. This chapter discusses the significant mechanisms for preventing the man in the middle.

### 1.1 Spoofing based MITM defence Mechanisms

#### 4.1.1 ARP spoofing defence mechanisms

Abad et al. [23] Performed one of the most significant surveys of ARP defence. They evaluated the identification and prevention schemes for ARP spoofing attacks and defined ideal solution criteria. Oh.at.al presented a new technique to defence, and opposed the approaches previously proposed. The majority of systems can be categorized from two perspectives: the way they are configured (cryptographic, voting, hardware), and the way they are located (server-based and host-based). ARP spoofing protection strategies are described in the next pages, concentrating on systems that avoid MITM attacks from ARP. Recently numerous solutions have been proposed to address the issue of ARP spoofing. Some of them however have some critical disadvantages. The solutions can be categorized according to the following:

- **Detection of ARP spoofing**

Carnut and Al. [24] introduced an exchanged network design without the requirement for any advanced tools to identify such spoofing attacks. ARP defence system and ARP Guard were used by the sensor-based system to prevent internal network attacks such as ARP spoofing. Arp watch, open-source software for network control of Ethernet traffic operation, manages IP address matching databases.

A low-cost embedded intrusion detection device has also been suggested to effectively prevent and track ARP spoofing attacks but it involves the use of a host or switch.

Their analysis showed that the software properly identifies ARP attacks devoid of producing false positives (alarms that turn out not to be part of attacks). Nevertheless, attackers could hide behind the volume of traffic and stay undetected for a relatively long period. ARP-Guard and ARP Defender are popular devices that utilize a sensor-based system to track and identify numerous internal network threats, like ARP spoofing. Solutions analyse LAN and Simple Network Management Protocol (SNMP) sensor details and inform administrators when targeting the control network.

Arpwatch is open-source software that helps track network Ethernet traffic operation and maintains an Ethernet / IP address matching database. When a pairing shift happens suspiciously (IP, MAC) the network administrator gets a warning. This method is quite lightweight and readily accessible but it depended on the capacity of network administrators to identify non-malicious attacks and ARP spoofing attacks and to take effective action when the assault occurs. Hou et al. suggested a similar methodology in which they introduced the inspection module and built the attack Detection System (IDS) Snort.

- **Cryptographic solution**

S-ARP is a modified ARP extension, which uses public-key encryption to authenticate ARP responses. Both hosts establish private and public key pairs during the initial network communication and send them to the authoritative key distributor with signed certificates (AKD). Anybody may identify whether the transmitted request is from a valid user with public-key encryption. The spoofing attack of ARP is therefore avoidable. To security, P-ARP is an increased edition of this. For authentication of data, it uses the additional magic number and HMAC hash feature.

Gouda et al. [25] suggested another solution that would fix MAC and IP pair protection issues within the Ethernet. The design consisted of a stable network-connected device and two system-connected protocols: an invite-accept protocol and a request-reply protocol. Hosts sign their IP, MAC mappings with the host utilizing the invite-accept protocol. The request-reply protocols are used for hosts to get from the protected service database the MAC address of a host attached to



the LAN. This approach is not realistic, because this current address resolution mechanism involves modifying the specification of the ARP mechanism for each host. Another limitation is that the protected server serves a single point of network failure, which is an easy goal for DoS attacks.

Goyal et al. [26] suggested an update to S-ARP focused on the combination of digital signatures and one-time hash-chain passwords to authenticate ARP IP, MAC mappings. Their scheme is based on the same design as S-ARP but the smart use of cryptography allows it much quicker.

Lootah et al. [27] proposed another T-ARP approach to minimize S-ARP's computational expense by using the ticket principle (centrally created (IP, MAC) attestation for address mapping). This solution uses a Local Ticket Agent (LTA) and a Key Management System (KMS) to release a public key from the ticket to get the (IP, MAC) set. This approach is reverse compatible with the current ARP, but it can replay attacks and increase overhead efficiency.

The CLL protection extension, which gives LAN hosts authentication and anonymity via the safeguarding of all layer 2, including ARP and DHCP handholds, provides another remedy. In CLL both hosts are listed created on their (IP, MAC) address pairs by using public-key cryptography. Hosts authenticate swap cryptographic conditions, and compromise symmetrical session keys, by a message authentication code and an alternate cipher, for defending their corresponding unicast packets.

P-ARP is a new ARP authentication-based system, with few changes: In addition, P-ARP uses HMAC, which provides authentication data, the magic number, nonce, and hash function. The Hash function generates Nonce and HMAC values to hide the target IP address in the message for the APR request. The deficiency is the inefficiency against ARP DoS attacks and in reality, the solution slows the overall network output to unreasonable levels.

- **Voting-based solution**

Nam et al. [28] Suggested MRARP, the main voting-based ARP spoofing resistant protocol. If an ARP Request or Response request is received and announces a new MAC address for an IP address, MR-ARP queries the same machine (machine with an old MAC address) and tests whether that machine also uses a new IP address (this mechanism is based on the Antidote approach addressed later). In the case that the MR-ARP computer receives an ARP Request or a

Message Stating (Apple, MAC) Mapping for a new IP address, it asks neighboring machines to vote for a new IP address. For this method, voting can only be fair if the rate of the voting traffic of the machines in question is almost the same.

This condition can be fulfilled in the Ethernet, which may not be applicable in the 802.11 network due to the modification of the signal-to-noise ratio (SNR) traffic rate. To mitigate the drawback of the MRARP with the addition of EMR-ARP. The new protocol develops the voting process by incorporating computational puzzles, as well as achieving:

- Mitigation of ARP spoofing attacks in wired or wireless LANs;
- Backward compatibility with existing ARPs;
- Minimal infrastructure upgrade costs;
- Incremental deployment;
- Auto activation for newly joining nodes.

On the other hand, EMR-ARP requires too much computer time from devices. Improvements were suggested in 2013 through the GMR-ARP protocol, namely:

- an improvement in the fairness of voting relative to the MR-ARP, due to the decrease in too early Reaction packets and the empirical assessment of voting parameters;
- minimized voting traffic overhead, which is smaller than in previous voting protocols (MR-ARP, EMR-ARP);
- resolve computing capabilities by eliminating computing puzzles;
- In comparison to MR-ARP, GMR-ARP will secure improved computers as wired nodes and wireless nodes coexist throughout the same subnet.

However, this method will generate additional overheads in wireless mesh networks, especially in large-scale networks, because the requests for votes are made in broadcasts.

- **Hardware solution**

To provide extra security, some switches implemented a feature called Dynamic ARP Inspection (DAI). DAI safeguards the network against many commonly known MITM-based ARP spoofing attacks. It ensures that only valid ARP requests are forwarded and responses are sent. The Ethernet shift monitors the legality of the received ARP packet using the trusted database (IP,

MAC) mapping database. This database is however handled either manually or dynamically by DHCP snooping.

- **Host-based Solution**

Tripunitara et al. [29] Also suggested a host-based middleware approach to asynchronous identification and protection of ARP spoofing attacks. To detect the attacks the solution depends on duplicates. Thus, whether the host is spoofed or under DoS attack, it will not be protected by the system. However, the approach is not realistic because it involves stream-based protocol stacking and modifications on all network hosts. Anticap is a kernel patch that avoids ARP spoofing attacks on different UNIX-dependent operating systems. The solution excludes ARP updates providing a MAC address that varies for that IP address from the current table entry. Anticap does not operate in complex DHCP-enabled networks and is accessible is for a limited quantity of effective structures.

- **Server-based solution**

An antidote is a non-cryptographic approach that aims to avoid ARP spoofing by contacting the previous owner of a given IP address and giving it higher priority in the event of MAC conflicts. The antidote cannot, however, avoid spoofing a new IP address if a malicious ARP response first arrives. Certain network IP addresses are limited in their use with fixed devices. One typical example is the address of a gateway. Genian NAC can provide the functionality required to restrict the use of IP on this fixed device. When the device's MAC address which can use IP is set in Genian NAC, the device with the other MAC will block node communication when using the IP. ARP cache detox (broadcast ARP packets with the right network MAC address) stops network devices from configuring the ARP cache to the incorrect MAC address.

- **ASA (anti-ARP spoofing agent) software**

Address resolution protocol (ARP) is commonly used to manage the mapping of layer addresses between data connections (e.g. MAC) and networks (e.g. IP). Also though most hosts rely on automatic and complex control of ARP cache entries, it is well known that current implementation is vulnerable to spoofing or denial of service (DoS) attacks. Several methods exploit ARP protocol bugs, and previous attempts to fix the shortcomings of the 'original' ARP architecture were unsatisfactory. Suggestions to modify the definition of the ARP protocol would

cause serious and unacceptable compatibility issues. Other proposals require the addition of custom hardware to monitor malicious ARP traffic and many organizations cannot afford this cost. This research shows that most risks can be effectively removed. ARP vulnerabilities are caused by the installation of an anti-ARP spoofing agent (ASA) that intercepts unauthorized exchange of ARP packets and blocks potentially unsafe communications. The proposed approach requires neither the use of kernel ARP software nor the installation of traffic monitors. The agent uses the User Datagram Protocol (UDP) packets to enable networking between hosts transparently and securely. The authors have implemented Windows XP agent software and experimented. The outcomes indicated that ARP hacking tools could not penetrate ARP-protected hosts.

#### **4.1.2 DNS Spoofing defence mechanism**

Heartberg et. [30] Al. provided defense mechanisms against DNS spoofing as well as suggested their taxonomy. Different DNS defense spoofing schemes are described below:

Anax is a realistic solution that uses techniques for machine learning. The findings of tests revealed a relatively low false-positive rate (0.6% of all new resource records) and a good identification rate (91.9 percent) .Detection of DNS spoofing Another real-time scheme, Cache Poisoning Detection System (CPDS). It has a lower dependency, higher reliability, and more applicability than Anax. Many methods use the peer-to-peer (P2P) sharing networks. The fundamental principles behind such procedures are similar to voting protocols based on ARP ( Approaches verify the validity of a DNS query, transmit DNS requests to hosts on the network, or communicate with a variety of trustworthy peers, and then send the majority response.

- **Entropy increasing mechanism**

Entropy-enhancing mechanisms are strategies that introduce more randomness to DNS packets to mess with invalid DNS response injections. Several proposals have been released in recent years, most notably: Source Port Randomisation (SPR), Randomisation (IPR) source/destination IP address, DNS 0x20 encoding[, WSEC-DNS, DNScookies Nevertheless, the creation of substantial additional entropy to DNS requests would not defend against DNS spoofing, and the attacker can still be able to poison domain names of high value. Therefore, the need for alternate or additional defensive strategies remains. TSIG has been introduced based on mutual secret

keys and one-way hash techniques. SIG (0) was proposed that was based on the technique of public-key authentication. The public keys are kept in DNS as signer property records and passwords. SIG (0) is more expensive asymmetric operations than TSIG since TSIG uses keyed hash codes that involve the injection of invalid DNS responses by inexpensive computations. Several proposals in the past few years. S-DNS is a proposal based on the key management scheme Identity-Based Encryption (IBE). S-DNS is a simple security solution with low overheads for computation and communication. It targets the various types of DNS database engagement from iterative, recursive, and caching schemes. It is an easy solution and needs fewer overheads in communication and computation.

- **Artificial neural network solution**

Bai et al. [31] recently described a defense against DNS spoofing attacks by artificial neural networks (ANN). Researchers have managed to build a 3-layer ANN: input, hide, and output. The input consists of three parameters: ANSWER, AUTH, ADD, which presents: number of RRs of authority, RRs of response, and other information. The network output layer corresponds to 10 possible groups that estimate the latency of packets from the least reliable (0) to the most reliable (10). Packets below Level 5 are considered manipulated and will be rejected, while others are considered accurate and accepted. The neural network generates weights for these DNS Response packet fields after training. After testing configurations, the performance tests showed excellent results. The average identification ratio is 98 percent for both accurate and forged packets.

#### **4.1.3 DHCP Spoofing Defence Mechanism**

Most recently, Dinu et al. [32] analyzed solutions aimed at making more stable and presenting their concept to DHCP. The solutions for avoiding DHCP spoofing attacks are provided below.

- **Enable DHCP Snooping**

DHCP snooping is a security mechanism that filters and maintains untrusted DHCP messages, and retains a binding table for DHCP snooping. With this method, switch ports are optimized in two different states, trustworthy and untrusted. When the port is designed to be trusted, the DHCP response may be received. Otherwise, if the port is untrusted, it will not be enabled to accept DHCP responses, so if the invalid attacker DHCP response tries to access an untrusted

port, the port will be disabled. It would be a long time to configure all ports for various trustworthy and untrusted states and not every switch port has to be designed to allow DHCP snooping. If a port is not designed to be a trustworthy port, it is treated as an untrusted port by default. DHCP snooping also works with DAI.

- **Port security**

Port security is another way to avoid these attacks, as Port Security only considers the frame's MAC source to establish filters and then set the MAC addresses that are permitted on a specific port (useful against MAC flooding attacks). The concern here is that these devices do not modify this MAC, but instead randomize the DHCP payload area Client Hardware Address (CHADDR). This area, along with the client identifier, is of great significance because the server can use it to differentiate between specific client requests. Without that, it would be hard to distinguish between the different users when using a DHCP Relay Agent.

#### **4.1.4 IP Spoofing Mechanisms**

Ingress filtering and IPsec are the primary security mechanisms for IP spoofing. Several IP spoofing solutions are listed below:

- **Router-based solution**

A mechanism is known as Distributed Packet Filtering, which filters packets based on interface and flow. This checks whether the packet has passed from source to destination along an unknown path. Packet passport program on which hash algorithm and symmetric cryptography were based are introduced.

- **Host-based solution**

A responsive structure known as stack path identification has been introduced in which each router uses its IP marking area. It guarantees equal labeling for all packets going in the same direction. This allows for the correctness of the address. Hop Count Filtering (HCF) tests source prefix validity based on the binding value between the prefix and the hop list. The approach generates a large number of false negatives, as it is easy to find the fake network and the attacker has the same length e. Besides, the attackers which modify the initial TTL value can bypass HCF.

## 4.2 SSL/TLS defence mechanisms

A variety of proposed approaches aimed at protecting SSL / TLS from MITM attack using third-party organizations that provide different advantages: first contact security to a new domain, flexible certificate validation for all public domains, and minimum web application specifications. On the other hand, they face challenges: implementation and operating costs, a more complicated confidence model, and processes for revoking certificates, new privacy threats. The proposed approaches are described below:

- **Detection of forged certificates**

Solutions in this segment are identical to the identification schemes previously addressed in other protocols. Certificate Transparency (CT) produces a centralized audit log of HTTPS certs, which is verifiably appended and monitored by independent monitors. ICSI Certificate Notaries Program automatically receives certificates on various individual websites and eventually aggregates them into a single database nearly in real-time. EFF SSL Observatory, or Crossbar proposals, actively scan the internet either by querying TLS-enabled servers or by asking users to submit the certificates they see. Both of these approaches have more details on all of these methods have extra details on certificates and support to verify their sources, but use third parties.

- **Certificate pinning solution**

This approach addresses the MITM attack by combining hosts through their anticipated X.509 certificates or public keys. In such a system, servers must publish certificates and public keys (which will be used for potential handshakes of SSL / TLS), so users will be able to detect whether there have been any modifications.

- **Multi-path probing solution**

The SSL/TLS MITM attack is usually executed as a targeted attack rather than a global one. This means that the attacker has to persuade only one or a few victims of the authenticity of the certificate, although not all users are reliable. The distributed voting strategy is therefore successful against the SSL/TLS MITM attack. Such approaches are similar to ARP voting-based algorithms. Wendlant et al introduced a program named perspectives, which is spread over the web and functions like a notary. Each notary shall establish a local archive with recognized certificates. Based on the voting process, credentials of notaries are denied or approved.

The solution has been provided as a plugin for Firefox. Convergence is a related approach, even with more general design.

and crowd processing capabilities. Some systems include the Double Check and Detector Project. The Detector Project has each customer working as their notary. Due to the capability to connect from different network locations, it uses the Tor network to check the authenticity of server certificates. Multipath analysis can detect replacement attacks from local certificates but not attacks in which all the traffic to the host is modified. Notary approaches could also give rise to false positives when servers switch between alternative certificates. Besides, customers can experience slower SSL / TLS contact times as several notaries are consulted during certificate validation.

- **Force SSL/TLS connection solution**

This category of solutions forces communicating parties to use the SSL/TLS connection. ISAN-HTTPS enforcer makes use of the Javascript API to enforce HTTPS redirection. When the webserver responds to a request from the browser of the user, it also responds to HTTPS redirection with messages and scripts.

- **TLS extensions**

First, Dietz et al. proposed the approach to Origin-Bound Certificates, and then Balfanz and Hamilton changed it to the extension of Channel IDs. It is a TLS extension that improves client security but as Karapanos et al. have demonstrated, it could not prevent MITM attacks. In short, browser stores private/public key pairs created with a TLS-enabled webserver during the TLS handshake. Public keys are termed channel IDs and are used across multiple TLS connections to identify the browser. The method blocks most of the current MITM attacks, as attackers can't impersonate the client (without stealing the legitimate browser's self-signed private key. It does not, however, stop an impersonated server from providing the client with a cacheable malicious JavaScript file, which is later executed in the sense of the victim's website and potentially exfiltrates data by trying to connect to the accurate server.

### **4.3 BGP MITM defence Mechanism**

Huston et al. [33] and Subramaniam et al. [34] surveyed BGP security and focused on vulnerabilities to create the protocol safe. However many methods have been proposed to take security to BGP. The significant security strategy for BGP MITM attack is stated below:



- **BGP MITM detection**

Numerous BGP MITM attack mitigation methods are victim-centric (responsible for identifying their IP hijacking), infrastructure-based (centralized database-based), and peer-centric (communication-based peer IP hijacking). Hu and. Al. proposed a real-time strategy involving data-planning strategies and control-plans. In the sense of potential routing, some should stop rogue Butt. It did not use the appropriate method for detecting fingerprints and also did not describe the problem-solving firewalls. Hong et. Al. The IP hijacking detection technique was presented based on network accessibility and fingerprinting methods.

- **IP prefix filtering**

Most networks can hardly make IP prefix announcements when necessary, and may only declare their IP prefixes to certain other networks, not to the Internet as a whole. Each AS in BGP implicitly trusts the peer ASes with which it shares routing details. Doing so helps avoid unwanted hijacking of routes and may discourage the AS from adopting fake IP prefix claims.

- **Proactive prevention scheme**

This scheme would block the spread of attacks. Non-cryptographic strategy very great BGP Will eliminate a lot of weakness due to BGP.IT take on new path details for routers and thus avoids spreading the threat.

- **Resource Public Key Infrastructure (RPKI) system**

The network operators have started to embrace and introduce a BGP hijack protection mechanism widely known as the RPKI method. The RPKI used in this scheme consists of a four-level certificate database: (i) a type A named Route Origin Authorization (ROA) links an IP address block to its registered BGP origin AS (es), (ii) a type B binding a router to the AS number to which it belongs, and (iii-iv) certificates C and D binding respectively IP addresses and AS numbers to their respective owner's public key. The chain of certification resembles the sequence of AS number and IP address delegation, with the IANA serving as the root certificate authority for RIR certificates, the RIR serving as the ISP certificate authority, etc. Each certificate must be signed with its holder's private key and must also include its public key. The framework provides for two distinct techniques Securing BGP:

(i) secure route origination use ROAs (Type A Certificates) to verify that the IP address block in question is the origin of the authorized AS(es). The router would then be able to check the validity of the obtained BGP update for the specified IP address block and BGP origin AS by (a) querying the RPKI for the ROA relevant to the IP address block and checking its cryptographic validity, and (a) if the ROA is correct, check that the origin AS and the length of the IP prefix found in the BGP update match to the permitted origin AS (es) and the length of the prefix in it. This stops an attacker from releasing a block because he does not own.

(ii) Secured route propagation helps to avoid the forgery of the AS path by ensuring that each AS in the AS path is not impersonated. This is achieved by making each router sign an update to the BGP that is being propagated so that subsequent routers may check, using the RPKI type B certificate, that all routers which have signed the update belong to both the ASes contained in the route.

#### **4.4 FBS Based MITM defence Mechanism**

The prevention mechanisms for FBS spoofing-based MITM are arranged out in this section. The significant proposed solutions are discussed below:

##### **4.4.1 GSM MITM defense mechanisms**

The GSM specifications have been revolutionized over time. Researchers have experimented in two key ways to avoid MITM on GSM: improved security protocols and stronger cipher algorithms. The mechanisms are listed as follows:

- **End-to-end Security**

The simplest, fastest, and supreme cost-effective approach is to apply for end-to-end security or protection on the application layer. Most vulnerabilities in GSM security (except SIM cloning and DoS attacks) do not threaten ordinary people, and their targets are typically restricted to specific groups, so it is fair and cost-effective for these groups to protect their communications through end-to-end protection. Because the encryption and security establishment is carried out at the end-entities, no improvements to the GSM hardware would be needed. In this case, they cannot decode the encrypted data without having the true ciphering key, particularly through the communication is eavesdropped on by the police or legal authorities, unless a safe enough

cryptographic algorithm is implemented. It should, therefore, be transparent to both the GSM operator and the service provider to prevent illegal activity.

- **Using secure ciphering algorithms**

Operators that use newer and more reliable algorithms, such as A5/3, providing that these updates are made possible by the GSM consortium. The cryptographic algorithms used should be applied to both BTS and mobile phones. Any modification to cryptographic algorithms needs the consent and support of software and hardware suppliers because they will make necessary improvements to their goods. The cryptographic algorithms should be applied to cell phones, and agreement with the manufacturers of mobile phones is also required. A lone improvement of the cryptographic algorithms deployed, however, cannot be so useful. Since the ciphering algorithms are modified with the best, the attacker will easily impersonate the real network and compel MS to deactivate the ciphering function, such that authentication protocols need to be changed as well.

- **SAKA( secure authentication and key agreement )Protocol**

A new safe GSM protocol named "SAKA" to keep GSM networks from having numerous security issues and attacks [35]. This proposed protocol improves the limitations of the original GSM authentication process, including not allowing shared authentication; heavy bandwidth usage between VLR and HLR; overhead storage capacity in VLR; and excessive HLR with cellular authentication. This protocol often reduces the need for coordination between the MS mobile station and the HLR home network. The SAKA protocol produces minimum overhead interaction when compared with all other current and planned GSM protocols. Authors say that the SAKA protocol has lowered bandwidth usage by an average of 56 percent during the authentication process, which is the highest bandwidth decrease for any GSM system.

- **Securing the backbone traffic**

Encrypting the backbone traffic between the components of the network can prevent the attacker from eavesdropping or modifying the transmitted data. While this approach can be introduced without the GSM consortium's support, it still needs the hardware manufacturers' cooperation.

#### 4.4.2 UMTS MITM defense mechanisms

The solution of UMTS MITM attack is given below:

- **Aka(authentication and key agreement) Protocol**

There are limitations in GSM to boost security UMTS authentication and key agreement AKA are suggested at the network stage for authentication Various AKA protocols have been introduced to include security for contact parties in mobile communications at various stages. Many AKA-based symmetric key protocols have been proposed for the UMTS network to improve UMTS AKA security and the effective use of bandwidth during authentication.

- **Cocktail-AKA**

The Cocktail-AKA protocol is implemented on vector validation (AVs). Compared to UMTS-AKA AKA, It reduces computational and communicational overheads The Cocktail-AKA protocol utilizes two types of Avs: Medicated AV (MAV) and Prescription AV (PAV). MAV was analyzed and determined by the service network (SN), PAV measured by the home environment (HE). When the authentication stage is started, the SN distributes MAV, HE distributes PAV and generates an AV for shared authentication with the MS. Cocktail AKA protocol to Avoid MITM attacks, but it is vulnerable to impersonation attacks that contribute to MITM attacks.

- **S-AKA**

S-AKA is a modern authentication and key agreement system safe from redirect, MITM, and DoS threats [36]. In the procedure, SN must constantly produce random numbers to ask MS to respond to the corresponding responses for increasing authentication. S-AKA decreases network usage by up to 38 percent but raises the number of messages needed to authenticate mobile subscribers.

- **NS-AKA**

NS-AKA prohibits MITM from utilizing an external EK key between MS and VLR. The suggested approach is therefore free from redirection and impersonation threats. It reduces the exchange rate of 60 percent of messages compared to the UMTS AKA protocol.

- **Secure-AKA**

- An Enhanced and effective Extra protocol, namely "Secure-AKA" Network of UMTS.
- The Secure-AKA protocol offers common validation among MS and HLR, as well as between MS and VLR, equivalent to other Yeah protocols.
- The Secure-AKA protocol prohibits UMTS from redirecting attacks (such as AP-AKA, S-AKA, COCKTAIL-AKA), man-in-the-medium attacks (such as S-AKA), COCKTAIL-AKA), replay attack (as with all AKA), active attacks in the compromised network (as with all AKA) and denial of service attack (by Secure-AKA only though S-AKA offers selective prevention).
- The Secure-AKA is capable of reducing the bandwidth usage between the VLR and the HLR and reducing the VLR storage space.
- This fully overcomes the issue of counter synchronization that occurs in UMTS-AKA because the smartphone customer and the roaming network node do not retain a clock. This is possible with the message authentication code (MAC3) and the DK key of the proposed protocol.
- This protocol covers the true identity of will MS, i.e. the International Mobile Subscriber Identification (IMSI), and determines a provisional identity, i.e. the Temporary Mobile Subscriber Identity (TMSI) as during the authentication process. The other existing protocols do not have the security of identification across the network.
- Secure-AKA provides negligible communications and computation overheads relative to all current and new Yeah protocols in the literature.
- On average, the Secure-AKA protocol requires fewer bandwidth and has a fixed exchange rate of messages during authentication relative to all current AKA protocols for the UMTS network.
- Secure-AKA protocol minimizes 65 percent of the bandwidth usage during the authentication phase relative to UMTS-AKA, which is the highest reduction of the bandwidth of any AKA protocol.

# Chapter 5

## Implementation & Result

Various attacks are mentioned, as seen in the previous chapters. Therefore, its implementation alongside the related threats and their countermeasures is important to understand. This chapter discusses the implementation of MITM attacks through DNS spoofing and also provides a brief description of its tools. Then present the implementation process result.

### 5.1 DNS spoofing exploitation

In this segment, the genuine attack has been executed in the virtual environment to demonstrate how the ARP cache poisoning occurs in the network. DNS spoofing is a form of attack where the DNS server allows and utilizes inaccurate information from an unauthorized host. The host is executing a man in the middle of the attack. For example, a host is connecting to the [www.facebook.com](http://www.facebook.com) website. The attacker spoofs the host's DNS who are attempting to communicate. Then the host traffic will be redirected to the attacker, and the attacker will have sent the traffic to the host victim. But instead of having a reply from Facebook, the host would get an attacker's response. So, the victim will be redirected to the attacker's website.

To perform DNS spoofing the tools are needed will be as follows:

- Attacker Machine- Kali Linux
- Victim Machine- Windows 7
- Ettercap

### 5.2 Description of tools

**Attacker Machine- Kali Linux** Kali Linux is a Software platform, originating from Debian, developed for automated forensics and penetration testing. It is among an ethical hacker's strongest defense packages. Kali Linux is maintained and funded by Offensive Security Limited. It was created by Devon Kearns and Mati Aharoni. More than 300 penetration testing devices are accessible at Kali Linux. Kali Linux supports multiple languages, as well.

## Ettercap

The tool Ettercap was developed by Alberto Ornaghi and Marco Valleri (a.k.a Alor and NaGa). It's an open-source, free resource. It runs on various UNIX operating systems such as Linux, Mac OSX Solaris, and others. Ettercap is a LAN's switched on multipurpose sniffer/interceptor/logger. It has developed into a powerful network exploitation device as apart from the man-in-the-middle attack it can do character injection, packet filtering, killing every link, etc. Once Ettercap places itself in the middle of a switched connection, all communication between the two victim hosts can be acquired and analyzed, and then if the attacker can benefit from the situation.



**Figure 5.1: Ettercap graphical.**

There are two key sniffing options:

- **Unified sniffing**

This method sniffs out all the packets that pass through the cable. You can choose whether or not to place the interface in promise mode (-p option). The packet that is not directed to the host running Ettercap will be progressed automatically by routing layer 3.

- **Bridged sniffing**

It utilizes two network interfaces and moves data from one to the other when doing sniffing and information filtering. This sniffing method is stealthy because there's no way to find someone in the middle of the wire.

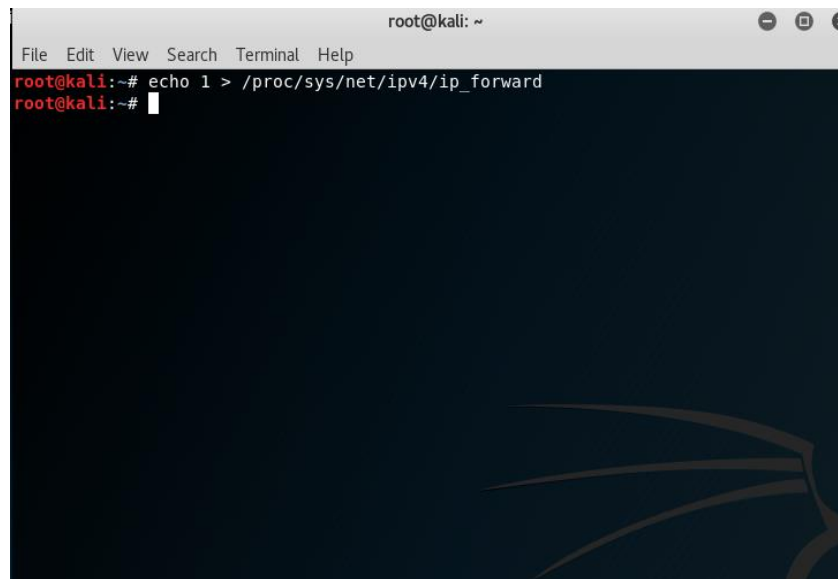
### 5.3 Performing attack

- **Virtual box setup**

On the Oracle VM Virtual Box, the Man-in-the-Middle (MITM) attack was implemented. An open-source software platform facilitates virtual computer development and management. The Virtual box app can be downloaded from the oracle virtual box website. Build a virtual environment with two VMs. The attacker computer running the Linux operating system kali, and 2. The victim's machine running the Windows Operating system.

- **Procedure**

At first, Packet forwarding enabled on kali Linux system.

A terminal window titled 'root@kali: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the command 'echo 1 > /proc/sys/net/ipv4/ip\_forward' being executed, followed by a prompt 'root@kali:~#'.

```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~#
```

**Figure 5.2: IP forwarding enable.**



```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward  
root@kali:~# locate etter.conf  
/etc/ettercap/etter.conf  
/usr/share/ettercap/doc/etter.conf.5.pdf  
/usr/share/man/man5/etter.conf.5.gz  
root@kali:~#
```

**Figure 5.3: Ettercap configuration command.**

```
root@kali:~# vi /etc/ettercap/etter.conf
```

**Figure 5.4: IP table command enable.**

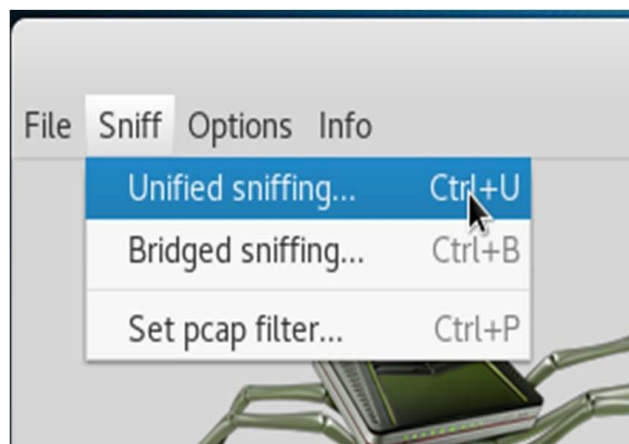
Next, the etter.conf file has been modified to uncomment on the two IP table's rules under SSL. Ettercap can now analyze SSL.

```
# if you use iptables:
  redir_command_on = "iptables -t nat -A PREROUTING -i %iface -p tcp --dport %port -j
REDIRECT --to-port %rport"
  redir_command_off = "iptables -t nat -D PREROUTING -i %iface -p tcp --dport %port -j
REDIRECT --to-port %rport"
```

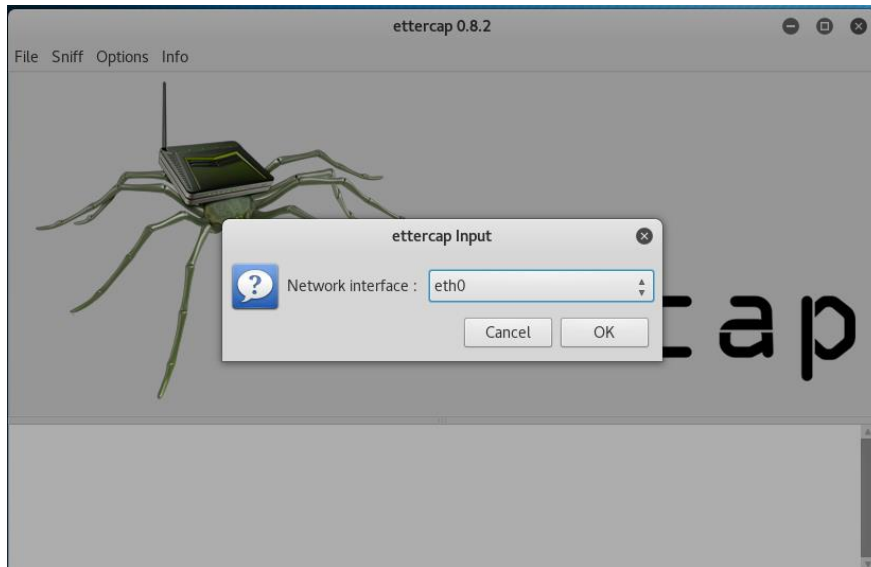
**Figure 5.5: Uncommenting IPTables rules to redirect SSL traffics.**

## Using Ettercap

The Ettercap graphical is now accessible for use in Kali Linux applications. Unified sniffing begins in the graphical application Ettercap and eth0 being selected for the interface.



**Figure 5.6: Unified sniffing being selected in Ettercap.**



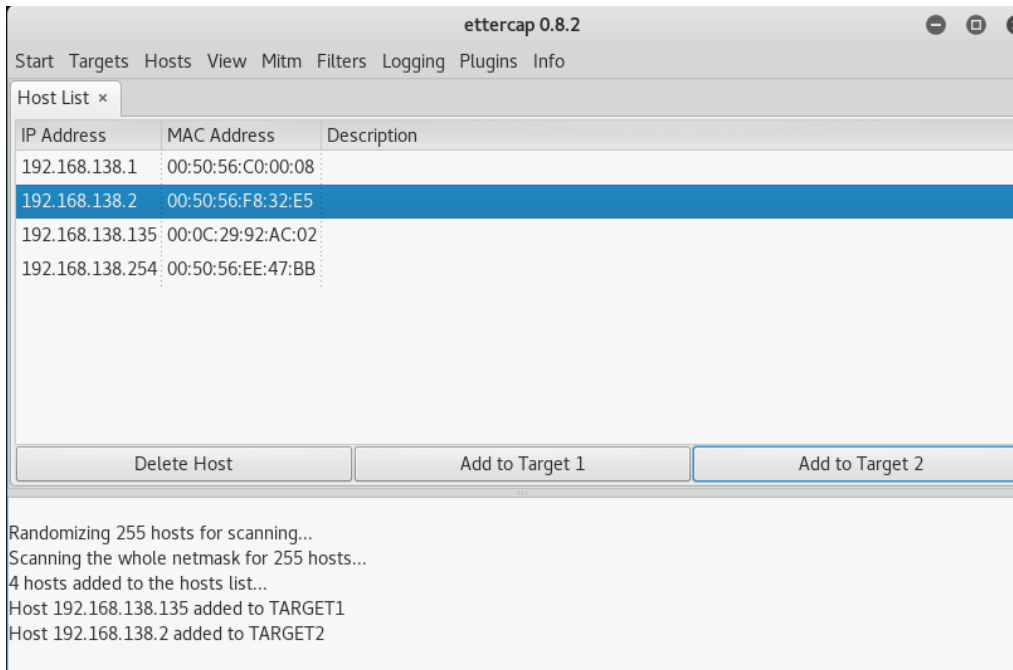
**Figure 5.7: Selecting interface in Ettercap.**

Once Ettercap starts the unified sniff; then I have to scan for hosts to select the targets. So I go to the hosts and select the hosts to scan for. When the host search is chosen, the app will begin searching for the hosts in the network.



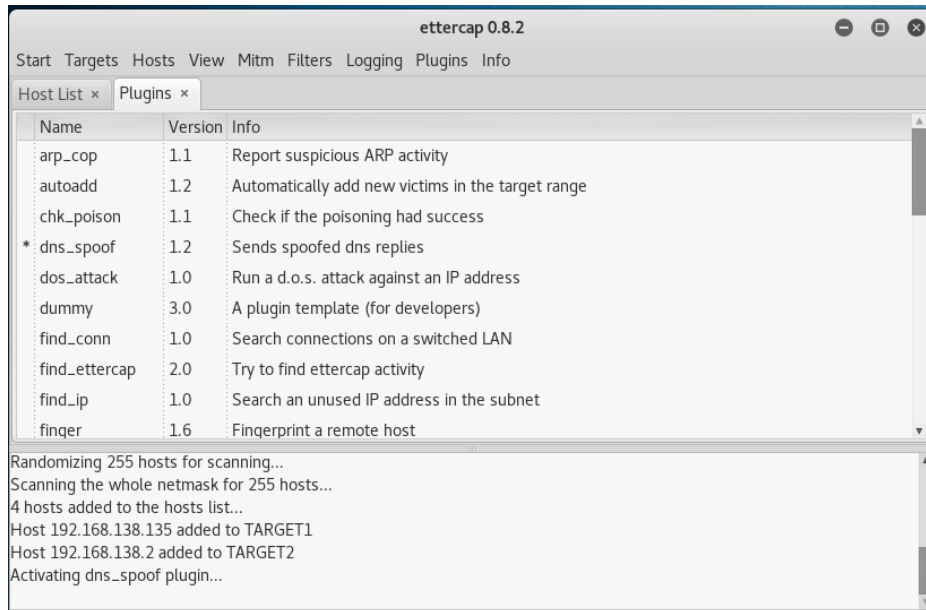
**Figure 5.8: “Scan for hosts” being selected in the hosts section.**

Then the victim’s machine added as target 1 and gateway as target 2. Here target 1’s IP address was 192.168.138.135 and gateway’s IP address was 192.168.138.2.



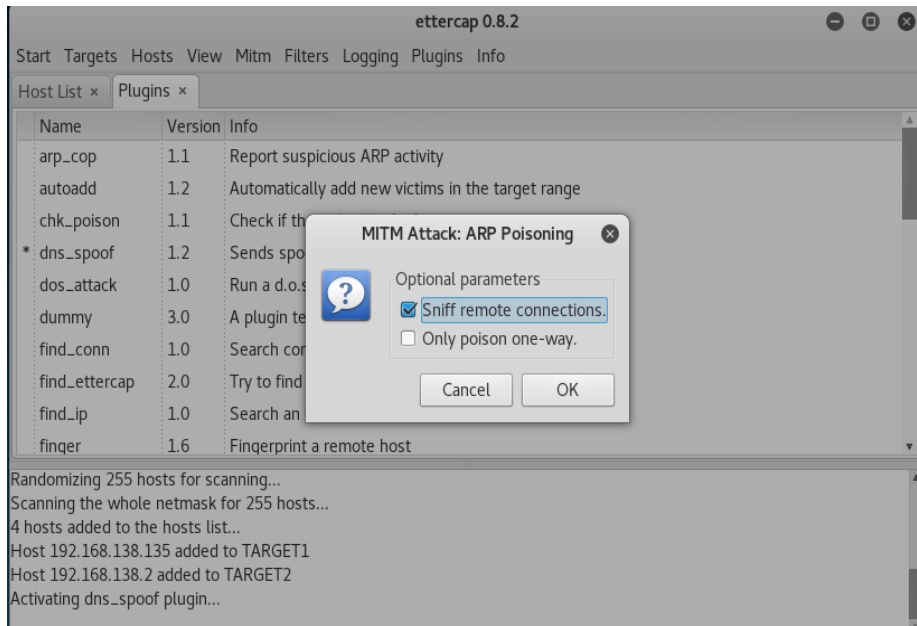
**Figure 5.9: Target's IP being selected in the Ettercap.**

Next, the DNS spoofing plugin started,



**Figure 5.10: DNS spoof plugin.**

Then ARP spoofing activated to sniff the remote connection.



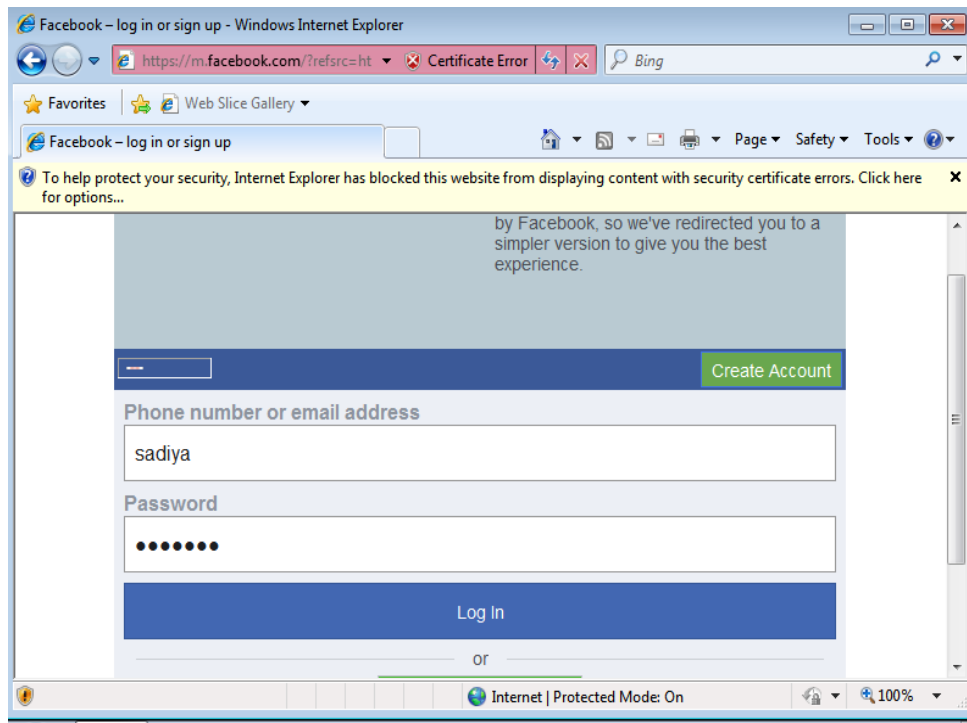
**Figure 5.11: ARP poisoning being activated in MITM (attack) section.**

Finally, DNS spoofing started with Ettercap.



**Figure 5.12: Starting DNS Spoofing in Ettercap.**

Victim machine, Windows 7 was attempting to connect to Facebook via Internet Explorer 8 by supplying the username and password. SSL was allowed, so he thought that he was browsing safely.



**Figure 5.13: Victim visiting the spoofed website.**

Then switched to attacking the kali Linux machine where Ettercap was still running. To observe that Ettercap was able to capture the victim's username and password successfully. So, it was able to successfully bypass SSL and execute a man-in-the-middle attack.

## 5.4 Results

As seen in the figure, Ettercap was successfully bypass SSL and execute a man-in-the-middle attack. So, when victim visited the SSL-enabled website from internet explorer 8, man-in-the-middle attack succeeds.



**Figure 5.14: Attacker capturing victim's credentials in Ettercap.**

# Chapter 6

## Conclusion & Future scope

This paper provided a detailed study of MITM attacks and reviewed MITM attack possibilities in communications systems. This document aims to raise user awareness about the effects and countermeasures of MITM attacks. It is a necessity for each self to be aware of attacks follow reliable security and measures when on the internet. First described what a MITM attack principle is and what types of attacks occur in networks. All the MITM classifications are discussed, with the user being able to identify the specification of the attacks. Data security and confidentiality have become the needs of the hour. Based on that, along with their description, different MITM defense mechanisms have been provided. The final chapter is devoted to how effortlessly an attacker can execute a Man-In-The-Middle (MITM) attack using quick and easy and open source tools such as Ettercap and SSL Strip. Testing the attack showed that the man-in-the-middle attack remains a real threat to network security. This study could help the user to observe some safety precautions that may prevent stolen of his data. There is still a lot to explore in this area. Many approaches have been suggested from time to time to avoid the execution of MITM Attacks, but several of them remain an issue. This paper explained the many consequences of MITM attacks that security researchers have recently noticed. This analysis could efficiently prevent and detect attempts to MITM attacks in the local network. This will include a thorough study of possible information infrastructure directions, as well as a technological analysis of emerging developments.



## Bibliography

- [1] Bharat Bhushan ; G. Sahoo ; Amit Kumar Rai, "Man-in-the-middle attack in wireless and computer networking — A review," in 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA) (Fall), IEEE. 2018.
- [2] Ankita R Chordiya; Subhrajit Majumder ; Ahmad Y Javaid, "Man-in-the-Middle (MITM) Attack Based Hijacking of HTTP Traffic Using Open Source Tools," IEEE International Conference on Electro/Information Technology (EIT), IEEE.2018.
- [3] S. M. Bellovin and M. Merritt, "Encrypted key exchange: Passwordbased protocols secure against dictionary attacks," in IEEE Computer Society Symposium on Research in Security and Privacy, p. 72–84, IEEE. 1992.
- [4] R. Demillo and M. Merritt, "Protocols for data security," computer, vol. 2, no. 16, pp. 39-51, 1983.
- [5] Alberto Ornaghi and Marco Valleri, "Man in the middle attacks," in Blackhat Conference, 2003.
- [6] U. Meyer; S. Wetze, "On the impact of GSM encryption and man-in-the-middle attacks on the security of interoperating GSM/UMTS network," in 15th International Symposium on Personal, Indoor and Mobile Radio Communications, IEEE. 2004.
- [7] L. B. Kish, "Protection against the man-in-the-middle-attack for the Kirchhoff-loop-Johnson (-like)-noise cipher and expansion by voltage-based security," Fluctuation and Noise Letters, vol. 06, no. 01, pp. L57-L63, 2006.
- [8] T. Chomsiri, "Sniffing Packets on LAN without ARP Spoofing," in Third International Conference on Convergence and Hybrid Information Technology, IEEE. 2008.
- [9] Konstantin Hypponen, Keijo M.J. Haataja, "Nino" man-in-the-middle attack on bluetooth secure simple pairing," in 3rd IEEE/IFIP International Conference in Central Asia on Internet, IEEE. 2007.
- [10] David Sounthiraraj , Justin Sahs , Garret Greenwood , Zhiqiang Lin , Latifur Khan, "Smvhunter: Large scale, automated detection of ssl/tls man-in-the-middle vulnerabilities in android app," In Proceedings of the 21st Annual Network and Distributed System Security Symposium (NDSS'14), 2014.
- [11] Mauro Conti, Nicola Dragoni, and Viktor Lesyk, "A Survey of Man In The Middle Attacks," IEEE Communications Surveys & Tutorials, vol. 18, no. 3, IEEE.2016.

- [12] Ankita R Chordiya ; Subhrajit Majumder ; Ahmad Y Javaid, "Man-in-the-Middle (MITM) Attack Based Hijacking of HTTP Traffic Using Open Source Tools," in IEEE International Conference on Electro/Information Technology (EIT), IEEE.2018.
- [13] Perna Arote ; Karam Veer Arya, "Detection and Prevention against ARP Poisoning Attack Using Modified ICMP and Voting," International Conference on Computational Intelligence and Networks, IEEE.2015.
- [14] Gopi Nath Nayak and Shefalika Ghosh Samadda, "Different Flavours of Man-In-TheMiddle Attack, Consequences and Feasible," in 3rd International Conference on Computer Science and Information Technology,IEEE. 2010.
- [15] Surakarn Duangphasuk ; Supakorn Kungpisdan ; Sumeena Hankla, "Design and implementation of improved security protocols for DHCP using digital certificates," in 17th IEEE International Conference on Networks,IEEE. 2011.
- [16] Voravud Santiraveewan ; Y. Permpoontanalarp, "A graph-based methodology for analyzing IP spoofing attack," 18th International Conference on Advanced Information Networking and Applications,IEEE. 2004.
- [17] Muhammad Murad Khan ; Majid Bakhtiari ; Saeid Bakhtiari, "An HTTPS approach to resist man in the middle attack in secure SMS using ECC and RSA," in 13th International Conference on Intelligent Systems Design and Applications,IEEE. 2014.
- [18] Italo Dacosta, Mustaque Ahamad, and Patrick Traynor, "Trust No One Else: Detecting MITM Attacks," Computer Security – ESORICS, pp. 199-216, Springer. 2012.
- [19] S. Kent ; C. Lynn ; K. Seo, "Secure Border Gateway Protocol (S-BGP)," in IEEE Journal on Selected Areas in Communication, vol. 18, no. 4, pp. 582 - 592,IEEE. 2000.
- [20] Stephen Kent , Charles Lynn, Karen Seo, "Design and Analysis of the Secure Border Gateway Protocol (S-BGP)," Proceedings DARPA Information Survivability Conference and Exposition. DISCEX'00,IEEE. 2002.
- [21] Zhe Chen ; Shize Guo ; Kangfeng Zheng ; Yixian Yang, "Modeling of Man-in-the-Middle Attack in the Wireless Networks," in International Conference on Wireless Communications, Networking and Mobile Computing,IEEE. 2007.
- [22] G. Rose ; G.M. Koien, "Access security in CDMA2000, including a comparison with UMTS access security," IEEE Wireless Communications, vol. 11, no. 1, pp. 19 - 25,IEEE. 2004.
- [23] C. L. Abad and R. I. Bonilla,, "An analysis on the schemes for detecting and preventing arp cache poisoning attacks," in 27th International Conference on Distributed Computing Systems Workshops (ICDCSW'07), p. 60,IEEE. 2007.

- [24] M. Carnut and J. Gondim,, "Arp spoofing detection on switched ethernet networks: A feasibility study," in 5th Simposio Seguranca em Informatica,IEEE. 2003.
- [25] M. G. Gouda and C.-T. Huang, "A secure address resolution protocol," Computer Networks," in Information Security and Privacy, vol. 41, no. 1, pp. 57-71, Springer. 2003.
- [26] V. Goyal and R. Tripathy, "An efficient solution to the arp cache poisoning problem," in Information Security and Privacy, pp. 40-51, 2005.
- [27] W. Lootah, W. Enck, and P. McDaniel, "Tarp: Ticket-based address resolution protocol," Computer Networks, vol. 51, no. 15, p. 4322– 4337, 2007.
- [28] S. Y. Nam, D. Kim, and J. Kim, "Enhanced arp: preventing arp poisoning-based man-in-the-middle attacks," IEEE on Communications Letters, vol. 14, pp. 187-189,IEEE. 2010.
- [29] M. V. Tripunitara and P. Dutta, "A middleware approach to asynchronous and backward compatible detection and prevention of arp cache poisoning," in 15th Annual Conference on Computer Security Applications Conference (ACSAC'99), p. 303–309,IEEE. 1999.
- [30] A. Herzberg and H. Shulma, "Antidotes for dns poisoning by offpath adversaries," in Seventh International Conference on Availability, Reliability and Security (ARES), pp. 262-267, IEEE.2012.
- [31] X. Bai, L. Hu, Z. Song, F. Chen, and K. Zhao, "Defense against dns man-in-the-middle spoofing," in Web Information Systems and Mining, pp. 312-319, Springer. 2011.
- [32] D. D. Dinu and M. Togan, "Dhcp server authentication using digital certificates," in 10th International Conference on Communications (COMM), p. 1–6,IEEE. 2014.
- [33] G. Huston, M. Rossi, and G. Armitag, "Securing bgpa literature survey," Communications Surveys & Tutorials, vol. 13, no. 2, pp. 199-222, IEEE. 2011.
- [34] L. Subramanian, V. Roth, I. Stoica, S. Shenker, and R. Katz, "Listen and whisper: Security mechanisms for bgp," in 1st Symposium on Networked Systems Design and Implementation (NSDI), p. 11, 2004.
- [35] Neetesh Saxena , Narendra S. Chaudhari, "SAKA: a secure authentication and key agreement protocol," CSI Transactions on ICT, p. 331–341,IEEE. 2013.
- [36] C. L. Abad and R. I. Bonilla, "An analysis on the schemes for detecting and preventing arp cache poisoning attacks," in 27th International Conference on Distributed Computing Systems Workshops (ICDCSW'07), p. 60,IEEE. 2007.