

**SECURITY CONTROL BY TICKET-BASED
ADDRESS RESOLUTION PROTOCOL**

CHIT HNIN WAI

M.C.Sc.

JUNE, 2022

**SECURITY CONTROL BY TICKET-BASED
ADDRESS RESOLUTION PROTOCOL**

By

Chit HninWai

(B.C.Sc.)

**A Dissertation Submitted in Partial Fulfillment of the
Requirements for the Degree of
Master of Computer Science**

(M.C.Sc.)

University of Computer Studies, Yangon

June 2022

ACKNOWLEDGEMENTS

First of all, I would like to express my inmost gratitude to **Dr. Mie Mie Khin**, Rector, the University of Computer Studies, Yangon, for allowing me to develop this research and giving me excellent guidance during the period of my dissertation.

Secondly, I would like to express my deepest gratitude to my supervisor **Dr. Si Si Mar Win**, Professor, Faculty of Computer Science, the University of Computer Studies, Yangon, for her caring and encouragement, and providing me with excellent ideas and guidance during the time of writing this dissertation.

Thirdly, I would like to express very special thanks to **Dr. Si Si Mar Win**, Professor, and **Dr. Tin Zar Taw**, Professor, Faculty of Computer Science, the University of Computer Studies, Yangon, as a Dean of Master's Course, for giving me the valuable guidance and suggestions during the development of this thesis.

In addition, I would like to acknowledge and special thanks to **Daw Mya Hnin Mon**, Associate Professor, the Department of English, the University of Computer Studies, Yangon. I would like to thank her for valuable supports and revising my dissertation from the language point of view.

Finally, I would like to extend my thanks to all my teachers who taught me throughout the master's degree course and my friends for their cooperation. The completion of my dissertation would not have been possible without the support and nurturing of my family.

STATEMENT OF ORIGINALITY

I hereby certify that the work embodied in this thesis is the result of original research and has not been submitted for a higher degree to any other University or Institution.

.....

Date

.....

Ma Chit Hnin Wai

ABSTRACT

Nowadays, communication is becoming more and more important to keep in touch with family and friends. Computer networks play a key role in this paper. To make this facilitating, Network engineers have used protocols for exchanging messages between computers. Many protocols are optimized to simplify the initializing these sites. However, it is still need to take security in some areas. This paper presents some of the vulnerability that exists in the Address Resolution Protocol (ARP) protocol and implements the Ticket based Address Resolution Protocol (TARP) by creating some spoofing attacks such as Man-in-the-Middle (MITM) attack and DoS attack to deceive a victim's machine and a router for exploiting the weaknesses of ARP protocol. In the experiments, TARP is implemented for ARP spoofing by distributing centrally secured mapping of MAC/IP address through existing ARP messages. This system explored some of operational vulnerability related with ARP security of deploying and administering. In this system, window operating system is chosen as to implement the attack as well as the defense creation.

CONTENTS

	Page
ACKNOWLEDGEMENTS	i
ABSTRACT	iii
CONTENTS	iv
LIST OF FIGURES	vi
LIST OF TABLES	viii
CHAPTER 1 INTRODUCTION	
1.1 Objectives of the Thesis	1
1.2 Related Work	2
1.3 Organization of the Thesis	2
CHAPTER 2 BACKGROUND THEORY AND RELATED WORKS	
2.1 Open Systems Interconnection(OSI) Model	4
2.2 Address Resolution Protocol(ARP)	5
2.2.1 ARP Request and ARP Reply	6
2.2.2 ARP Cache Poisoning Attacks	6
2.2.3 ARP Message	7
2.2.4 ARP Cache	9
2.3 ARP Cache Poisoning	9
2.4 ARP Cache Poisoning Methods	11
2.4.1 Unsolicited Response	11
2.4.2 ARP Request Attack	12
2.4.3 ARP Response Attack	12
2.5 Wireless Networks	12
2.5.1 Wireless LANs	12

2.5.2 Wireless Access Point	14
2.6 ARP Cache Poisoning in Wireless Networks	15
2.6.1 Attack Scenarios	16
CHAPTER 3 TICKET BASED ADDRESS RESOLUTION	20
PROTOCOL	
3.1 Ticket -Based Approach	21
3.2 The TARP Protocol	23
3.3 Ticket Format	24
3.4 Revocation	26
3.5 Attacks against TARP	28
3.6 Macro-benchmarks	28
3.7 Micro-benchmarks	29
3.8 Discussion	30
CHAPTER 4 SYSTEM DESIGN AND IMPLEMENTATION	
4.1 Sending ARP Request Frame from Sender to Receiver	33
4.2 Replying ARP Request by Receiver to Sender	37
4.3 Attackers	40
CHAPTER 5 CONCLUSION AND FURTHER	
EXTENSIONS	
5.1 Conclusion	40
5.2 Limitation and Further Extension	41
REFERENCES	42
AUTHOR'S PUBLICATIONS	

LIST OF FIGURES

Figure		Page
Figure 2.1	OSI Model Layers	5
Figure 2.2	The Reference Model TCP/IP	5
Figure 2.3	Host “A” broadcasts request for Host “D”	6
Figure 2.4	Host D Replies to Host A (unicast)	6
Figure 2.5	ARP Cache Poisoning Attack on Host “A” and Host “B” By Host “C”	7
Figure 2.6	An ARP Message Format	8
Figure 2.7	The ARP Poisoning	10
Figure 2.8	The ARP Poisoning Attack on Host A and Host B by Host C	10
Figure 2.9	Man-in-the-middle attack	11
Figure 2.10	Foundation Mode	13
Figure 2.11	Ad-hoc Mode	13
Figure 2.12	General set-up of wireless network with the wired network	15
Figure 2.13	Attacking Wired Clients by Wireless Client	16
Figure 2.14	Wireless client attacking a wired client and a wireless client	17
Figure 2.15	Attacking wireless clients	17
Figure 2.16	Attacking roaming wireless hosts	18
Figure 2.17	Attacking Two Wired Clients via a Wireless Client in a Home Deployment	19
Figure 2.18	Attacking a Wired Client and a Wireless Client in a Home Network	19
Figure 3.1	Static IP Address Assignment - Hosts Receive TARP Tickets during Initial setup, and include them with each ARP Reply	22
Figure 3.2	Dynamic IP Address Assignment – hosts receive TARP tickets during the Initial DHCP exchange, and include them with each ARP reply	23

Figure 3.3	TARP Reply Packet Format	25
Figure 4.1	Detail Process Flow	30
Figure 4.2	Sequence Diagram of System	31
Figure 4.3	Sender Login Page	32
Figure 4.4	Main Page of a Node	33
Figure 4.5	Checking receiver IP address and MAC address in sender's ARP cache	34
Figure 4.6	Sending ARP Request to All Members	35
Figure 4.7	Receiver Login Page	36
Figure 4.8	Check sender IP&MAC address in receiver ARP cache	36
Figure 4.9	Receiver Reply Ticket	37
Figure 4.10	Sender check ticket and send message to receiver	37
Figure 4.11	Receiver Receive Sender's Message	38
Figure 4.12	Detecting DoS Attacker	39
Figure 4.13	Detecting MIM Attacker	39

LIST OF TABLES

Table		Page
Table 3.1	Round-Trip Delay for ARP and TARP	28
Table 3.2	Execution Time for TARP operations	28

CHAPTER 1

INTRODUCTION

Every PC in Local Area Network (LAN) has a consistent Internet Protocol (IP) address and a physical Media access control (MAC) address. Communicating something specific from one machine to another in the equivalent or different network(s), MAC address of the objective machine is expected by the source machine. In this manner, getting the MAC address of objective on the off chance that missing in ARP reserve of source, a planning is required to have been laid out between IP address and MAC address. For this reason, ARP is utilized. From this it tends to be perceived that ARP is a vital piece of the organization layer and a stateless convention. ARP has some intrinsic security defects which make it defenseless against various ARP reserve harming assaults. Because of the significance of this issue, there has been a few arrangements proposed to settle it. Therefore, this proposed system implements effectiveness for ARP by utilizing T-ARP convention. T-ARP is a stateful convention, by putting away the data of the Request outline in the ARP store, to diminish the possibilities of different kinds of assaults in ARP. This system will be held every one of the valid statements of the first one for ARP, yet ARP will close off its security shortcomings prompting a more effective and gotten network.

1.1 Objectives of the Thesis

The major objectives of this thesis are as follows:

- To keep all of the benefits of the ARP but blocks its weaknesses in security by stateful protocol T-ARP.
- To defense the various cache poisoning attacks on ARP by using T-ARP.
- To investigate the efficiency of T-ARP.
- To implement network security by using T-ARP

1.2 Related Work

In recent years, several research works are tried to solve the attacks in the network layer. In this work, the Address Resolution Protocol (ARP) was utilized by PCs to plan legitimate addresses (IP) to actual addresses (MAC). Anyway ARP is an all confiding in convention and is stateless which makes it helpless against numerous ARP store harming assaults like Man-in-the-Middle (MITM) and Denial of administration (DoS) assaults. These imperfections bring about security penetrates consequently debilitating the allure of the PC for trade of touchy information. This framework presented a productive and secure form of ARP that can be adapted up to this multitude of kinds of assaults and is likewise a practical arrangement. It is a stateful convention, by putting away the data of the Request outline in the ARP store, to diminish the possibilities of different kinds of assaults in ARP. It is more productive and secure by communicating ARP Reply outline in the organization and putting away related sections in the ARP reserve each time when correspondence occur [1].

The defense system for DNS Hijacking and Cache Poisoning Attacks in the Domain Name System (DNS) was presented in 2005. DNS is the most part of the Internet and most IP networks so far as that is concerned. Regardless of the Domain Name System being significant, very few individuals have been known about DNS; not many understand what it is and how to keep its security. DNS deciphers the server names which people are bound to recollect into IP tends to which PCs use to explore through the Internet. In the majority of DNS exchanges, assurance of data is required. In view of its crucial job, DNS is engaged with complex Internet assaults both against the actual framework and other Internet. This framework forestalls its DNS and its weaknesses, different assaults to DNS system [20].

1.3 Organization of the Thesis

This thesis is organized as follows:

Chapter 1 introduces the proposed system and presents the objectives of the thesis, the related research works and thesis organization. The background theory of transaction processing is in the chapter 2. The Chapter 3 discusses the controlling for data recovery and the proposed system design and its implementation are expressed in

the Chapter 4. Finally, the conclusions, limitations and further extensions of this system are described in the Chapter 5.

CHAPTER 2

BACKGROUND THEORY

The network security protocols are mainly used to ensure secure internet connections and protecting sensitive data. These are a lot of predefined rules which control and manage the information exchange of by using a secure, reliable, and simple method. However, there are many vulnerabilities in these network protocols which lead to their threatening and pose serious challenges to network security. The well-known spoofing attacks may cause by the Address Resolution Protocol (ARP). This next section describes the important layers of OSI model in networking, the communication layer protocols and the attacks presented by the ARP protocols.

2.1 Open Systems Interconnection (OSI) Model

The OSI model is the standard model of organization engineering that contains seven layers [15]. Today, most true organizations utilize the TCP/IP model of organization design. Figure 2.1 spots the TCP/IP and the OSI models and one next to the other to show how the various levels of the TCP/IP model fall inside the layering shows of the OSI model. The figure additionally puts the various conventions in the TCP/IP model in light of the layer in which they work. Numbered the layers from 1 to 7 (from base to up).

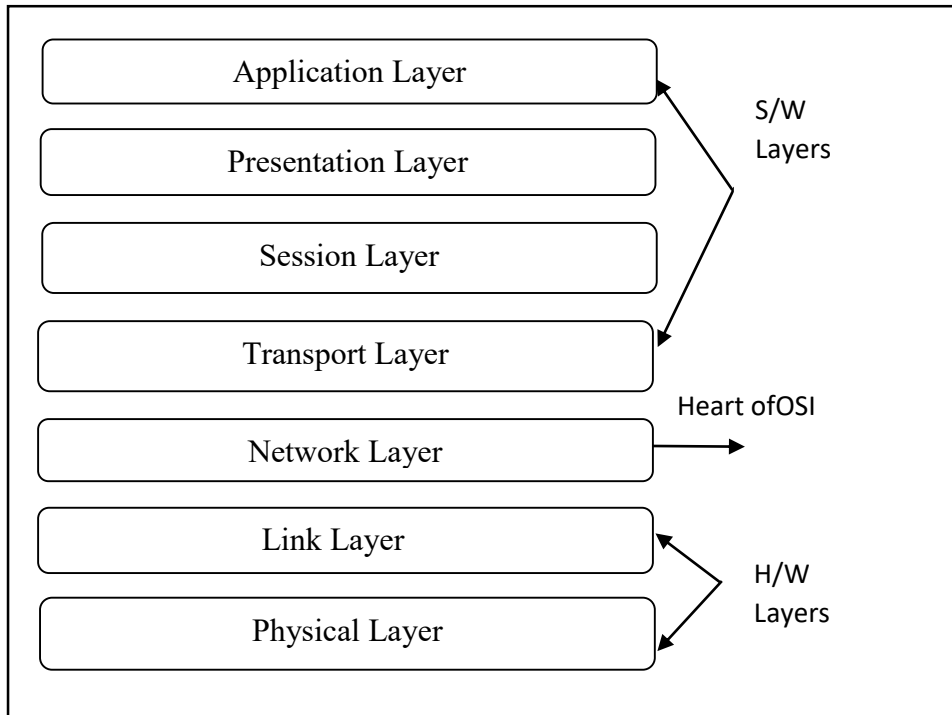


Figure 2.1: OSI Model Layers

The architecture of the TCP/IP reference model is shown in Figure 2.2.

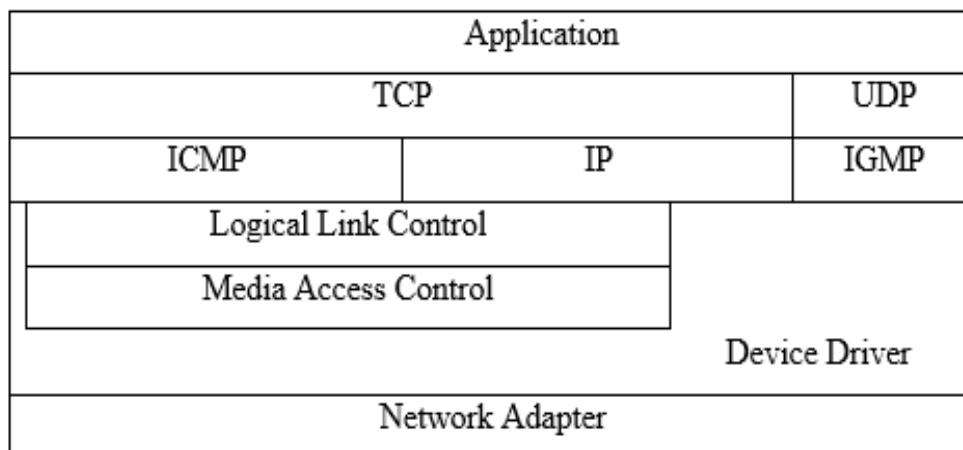


Figure 2.2: The Model of TCP/IP Reference

2.2 Address Resolution Protocol (ARP)

ARP is a communication layer protocol that performs the mapping process between the network layer and the data layer. It is used to identify the Media Access Control (MAC) address for the respective IP address. However, the host could not verify where the network packet came from on the peer to peer network. This vulnerability could lead to fake ARP. If the attacker is on the same LAN as the target

or is using a compromised machine on the same network. An attacker could use ARP spoofing. The attacker receives his MAC address to the target IP address. The attacker will receive any route intended for the target.

2.2.1 ARP Request and ARP Reply

When Machine A only knows IP address of Machine D and it wants to send a packet to D, Machine A need to broadcast ARP Request with IP address of D. The request operation of Machine A is as shown in following Figure 2.3.

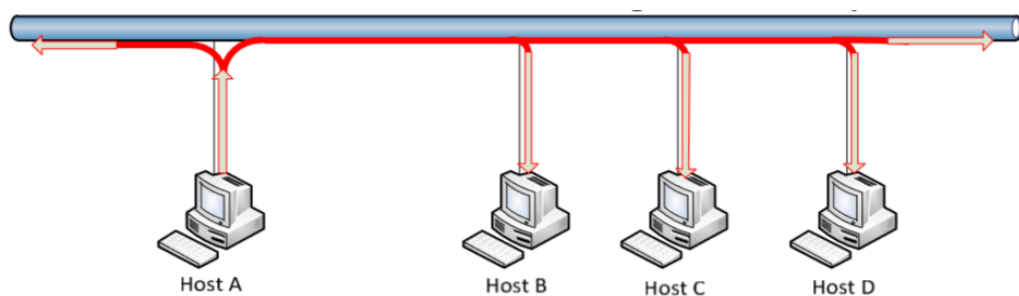


Figure 2.3: Host “A” broadcasts request for Host “D”

All machines on the neighborhood network get the ARP Request which is communicated. Machine D answers with its MAC address by unicast of ARP Reply as displayed in the following figure and update in D's ARP reserve with MAC of A. MAC address of Machine D is added by Machine A to its ARP reserve. Presently Machine A can conveys bundle straightforwardly to Machine D. The reply operation of Machine A is as shown in following Figure 2.4.

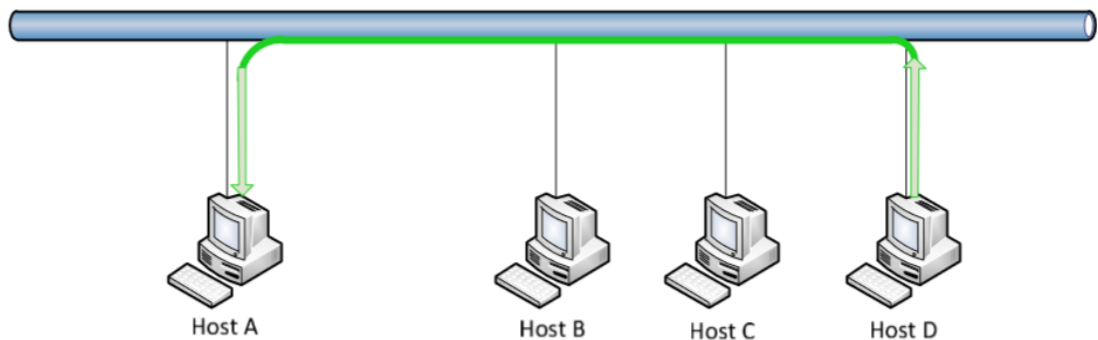


Figure 2.4: Host D Replies to Host A (unicast)

2.2.2 ARP Cache Poisoning Attacks

ARP store harming is the procedure by which an aggressor perniciously adjusts the planning of an IP address to its comparing MAC address in the ARP reserved of one more host by sending parodied ARP answer. So this method is additionally called ARP ridiculing. Host C is the assailant in the accompanying Figure 2.5.

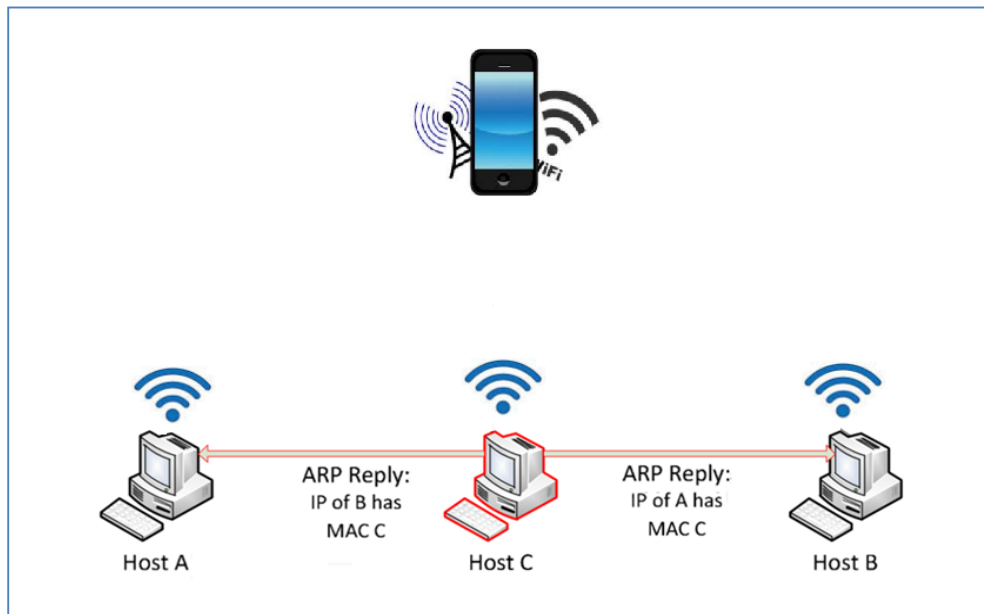


Figure 2.5: Cache Poisoning Attack of ARP on Host “A” and Host “B” By Host “C”

ARP cache poisoning is an attack that strongly effect all hosts connected to the same LANs network and this attack causes vulnerable to a malicious host.

2.2.3 ARP Messages

The ARP protocol send the four types of messages. In the operation field of ARP message, four values are identified for these four messages. These are the Request and Reply of ARP and Request and Reply of RARP.

0	8	15 16	31
Hardware Type		Protocol Type	
HLEN	PLEN	Operation	
Sender HA (octets 0-3)			
Sender HA (octets 4-5)		Sender IP (octets 0-1)	
Sender IP (octets 2-3)		Target HA (octets 0-1)	
Target HA (octets 2-5)			
Target IP (octets 0-3)			

Figure 2.6: An ARP Message Format

The format of ARP message is presented in Figure 2.6. The fields of an ARP message are described in the following:

- **Hardware Type** –Underlying hardware’s Type that is specified. e.g. Ethernet
- **Protocol type** –Protocol’s Type above this layer that is specified
- **HLEN** - Hardware address’s Length that is specified
- **PLEN** –Protocol’s Length(e.g. IP) address that is specified

Sender HA- MAC / Hardware Address of the machine that send the message

Sender IP – Sending machine’s IP address

Target IP – Destination machine’s IP address

Target HA - Destination machine’s MAC / Hardware Address

ARP Operation – Specifies the type of ARP message

- **Request of ARP:** When a machine sends an ARP demand it assign its MAC address, IP address, target IP address and message type of ARP. This ARP demand is communicated to every one of the machines in a similar LAN of the sending host. The objective HA is left clear for the machine with the objective IP address to assign.
- **Reply of ARP:** When a machine gets an ARP demand which contains its own IP address as the destination IP address, its MAC address is filled in the objective HA field. The machine makes an ARP answer with the upsides of the shipper and target fields in the ARP demand turned around and the Operation

field set to the op code of the ARP answer. This parcel is then sent exclusively to the mentioning machine.

- Request of RARP: Reverse Address Resolution Protocol (RARP) is the converse of ARP. A RARP demand is sent when a machine needs to get the IP address that relates to its MAC address. RARP demands are communicated in the LAN.
- Reply of RARP: RARP Reply is sent by RARP servers. On the off chance that the MAC address in the RARP demand has a place with one of the clients served by the RARP server, an answer is sent with its relating IP address.

RARP demands and RARP answers as these messages are shipped off by getting the IP address of the mentioning machine. The ARP reserve isn't impacted when RARP messages are sent or gotten. Thus the ARP Cache Poisoning is beyond the realm of possibilities with RARP messages. Likewise, most organizations utilize the Dynamic Host Control Protocol (DHCP) or a static design for IP address task; subsequently the use of RARP isn't normal. ARP messages are epitomized inside an Ethernet header before they are sent over the organization.

2.2.4 ARP Cache

In request to decrease network traffic, the ARP layer in each host keeps a store of the planning of IP address to MAC address for recently settled IP addresses. This store is kept up with for a brief timeframe and the passage is eliminated when its break lapses; the break is reestablished in the event that it is once more. A passage in the ARP store is made or refreshed in the accompanying cases:-

- Not long before a host sends an ARP answer to the machine which sent the ARP demand, it will make a section in its ARP store for the planning of the shipper's IP address to the source's MAC address.
- At the point when a host gets an ARP demand from another host, in the event that a passage relating to the IP address of the sending host exists in its ARP store, the section will be refreshed.

2.3 ARP Cache Poisoning

ARP Reserve Poisoning is the method by which an aggressor vindictively adjusts the planning of an IP address to its relating MAC address in the ARP store of

another host. It is carried out by sending ARP Reply packet with sender's IP address and MAC address to victim node as destination IP and MAC address. The ARP Poisoning is depicted in Figure 2.7. MITM is also an ARP Spoofing attack.

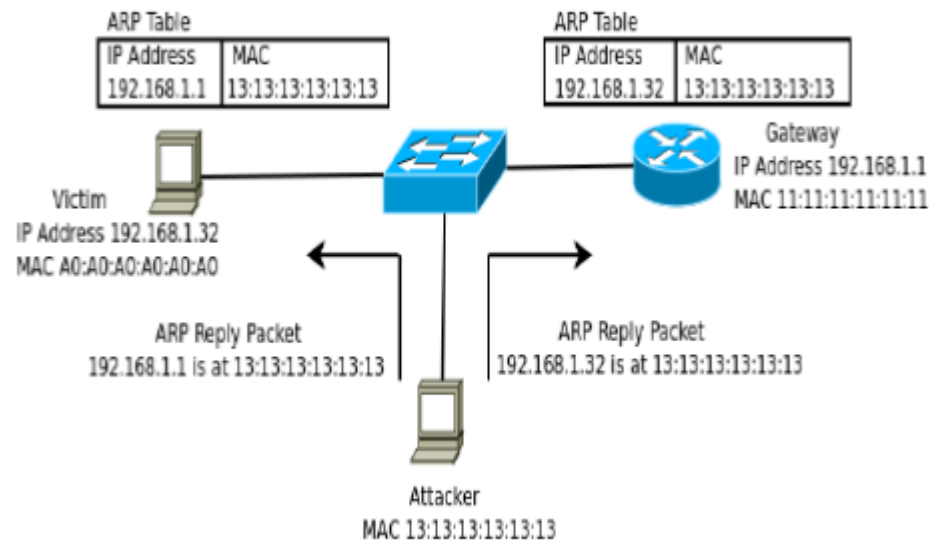


Figure 2.7: ARP Poisoning

For example, a man-in-the-center (MITM) assaulted by which the assailant can redirect the route passing between two hosts to pass through him.

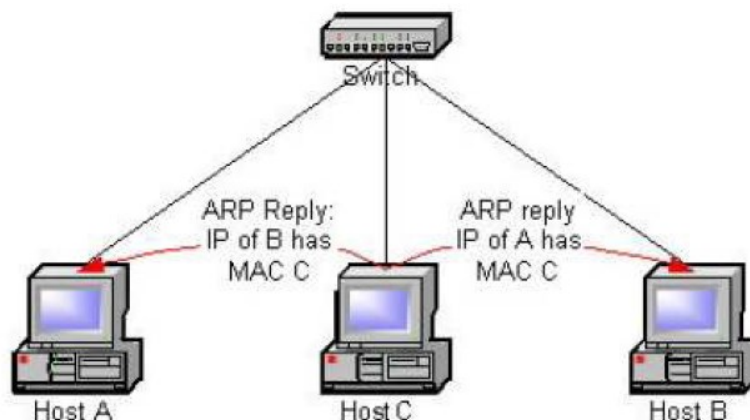


Figure 2.8: The ARP Poisoning Attack on Host A and Host B by Host C

In Figure 2.8, the aggressor is Host C. Host C executes the ARP Cache Poisoning assault by sending a ridiculed ARP answer to Host A expression that 'IP address of Host B guides to MAC address of Host C' and a mock ARP answer to Host B saying that 'IP address of Host A guides to the MAC address of Host C. ARP is a stateless convention and answers are not checked against forthcoming solicitations.

Subsequently Host A and Host B will refresh their ARP store with the planning got in the ARP answers.

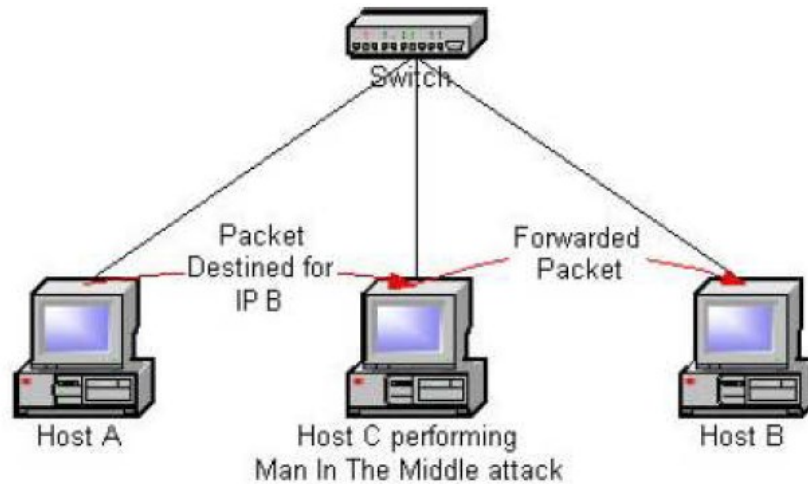


Figure 2.9: Man-in-the-middle attack

Once the ARP reserves of Host A and Host B are harmed, Host A will send all the traffic bound for Host B, to Host C. Likewise Host B will send all traffic bound for Host A, to Host C. Host C can now peruse all the traffic between Host A and Host B. On the off chance that Host C advances the parcels, subsequent to understanding them, to the genuine objective machine, then Host A and Host B will not identify that they are being attacked. MITM attack is one of the ARP Poisoning attack and attacking Host A and Host B by Host C with MITM is depicted in Figure 2.9.

2.4 ARP Cache Poisoning Methods

ARP Cache Poisoning, also known as ARP Cache Spoofing that allows attackers to deceive communication between network devices. There are three methods to poison the ARP cache.

2.4.1 Unsolicited Response

- A satirize ARP answer could be shipped off any host and the getting host will refresh its ARP store
- A satirize ARP answer could likewise be communicated to all hosts in the LAN, hence harming the ARP reserve of the relative multitude of hosts with only one Message

2.4.2 ARP Request Attack

When a host gets an ARP demand, the ARP layer in the host will refresh its ARP reserve with the planning expressed in the source IP and source MAC address fields of the ARP demand bundle [10], regardless of whether the solicitation was not so much for that host. Subsequently an assailant just has to send a parodied ARP demand (innately communicated) to harm the reserve of the multitude of hosts in a LAN.

2.4.3 ARP Response Attack

A malicious has in a LAN, on getting a genuine ARP demand, can send a satirize ARP answer. There could be a race condition between the caricature ARP answer and the genuine ARP answers in arriving at the mentioning host. The ARP store will be refreshed with the last gotten ARP reply.

2.5 Wireless Networks

Wireless network also called Wireless LANs (WLANs) are LANs that connects two or more network devices using wireless distribution techniques.

2.5.1 Wireless LANs

There are two different modes in the WLANs. They are foundation mode and Ad-hoc mode.

Foundation mode - In this kind of WLAN, every one of the remote clients imparts by means of a base station or a passageway (AP). The passageway goes about as an association with the wired organization, which is the spine for the WLAN. The operation of Foundation mode is depicted in Figure 2.10.

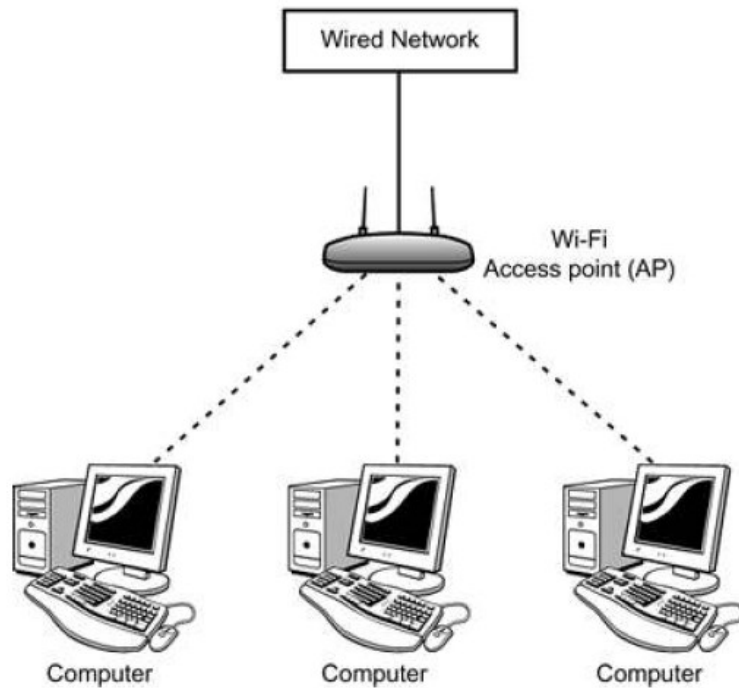


Figure 2.10: Foundation Mode

Ad-hoc mode -The wireless clients in this mode do not need any central server and they can communicate to each other on a peer to peer manner without the server.

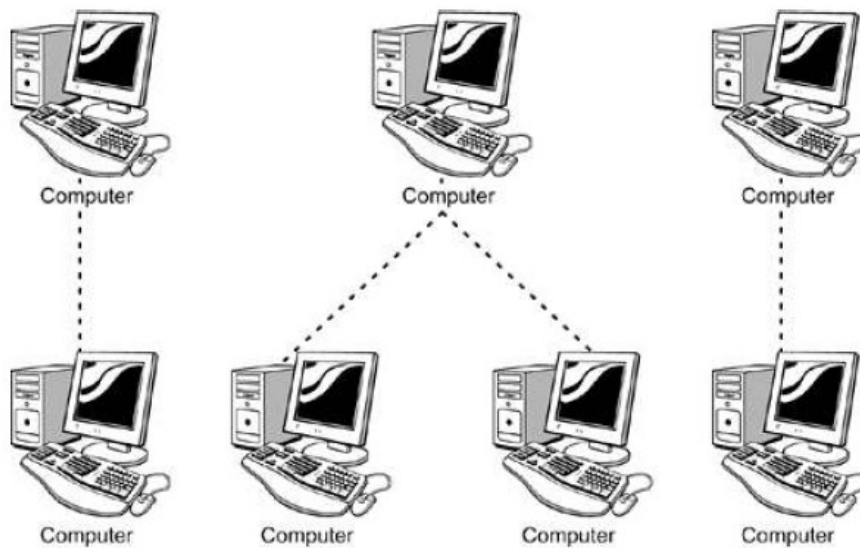


Figure 2.11: Ad-hoc Mode

For this task it might be thinking about the foundation method of WLANs. The ARP Cache Poisoning issue is to a greater degree. A danger when a remote client is attempting to go after the wired clients through a remote AP or a remote switch to which

they are completely associated. In specially appointed mode, there is no remote hardware to which the remote clients and wired clients are usually associated. Thus, the framework method of WLANs is where the issue exists.

2.5.2 Wireless Access Point

In the foundation mode, the remote clients can impart just through a passage. The passageway deciphers the radio waves got from the remote clients and sends it to the Internet utilizing an Ethernet association. Correspondingly the information got from the wired organization is encoded into radio waves and shipped off the remote clients.

A remote client needing to join a remote organization looks for accessible Access Points. Each Access Point consistently sends signals to illuminate remote stations regarding its presence. In the signal, Service Set Identification (SSID) is sent by the Access Point which recognizes one passageway from another. When the remote client has distinguished the passage it needs to go along with, it sends an affiliation solicitation to the Access Point. The AP and the remote client go through a handshake interaction, which incorporates trading data in regards to the organization and verification. The AP will verify intermediates network and the remote client correspondence with the remote client starting there ahead.

When the client is finished utilizing the remote organization, it needs to disassociate from the AP. By chance that the client doesn't disassociate and doesn't involve the organization for a particular timeframe, then the relationship of that client will break.

Elements of the Access Point:-

- Intermediates correspondence between two remote stations that are speaking with one another
- Goes about as a scaffold between the 802.11 organization and the wired organization like the 802.3 organization.

2.6 ARP Cache Poisoning in Wireless Networks

ARP store harming is an assault pervasive in LANs, i.e., all hosts associated with the very switch or centers as that of vindictive hosts are defenseless against this assault. Passageways go about as centers for remote organizations and go about as extensions between remote organizations and wired networks.

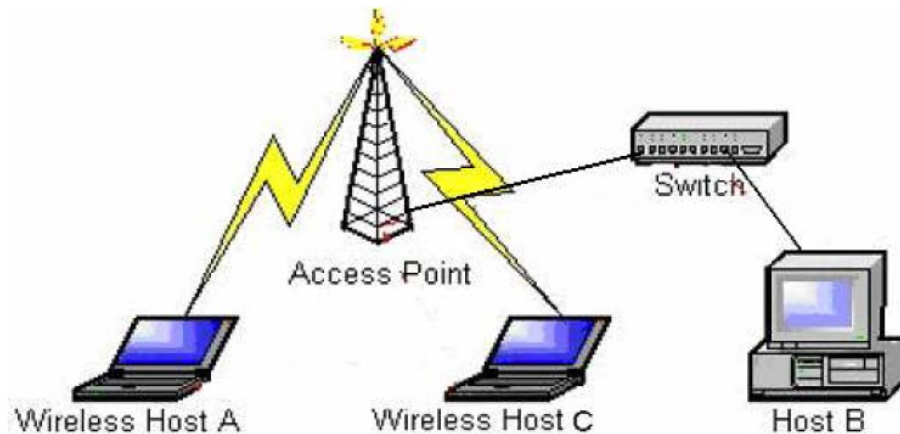


Figure 2.12: General set-up of wireless network with the wired network

As in the arrangement in Figure 2.12, the wired clients are associated with the very switch as that of the Access point. Any message broadcast from remote has A and C arrives at the wired Host B. The transmission space of an organization incorporates every one of the machines associated with a switch. Here the AP is associated with the switch, consequently every one of the remote hosts related with that AP has a place with the transmission space of that switch. The wired clients associated straightforwardly to the switch likewise fall in the transmission area of that switch. ARP demands are communicated in a LAN. Consequently every one of the hosts in the transmission area get the ARP demands. This thusly makes the wired hosts associated with the very switch as that of an AP helpless against an assault from remote clients.

By and large, in problem areas like bistros, vehicle sales centers and so forth, an Access Point will be given to clients who have a remote host to get associated with the remote organization. The overall arrangement is to such an extent that the AP will be associated with a change to which the bistro's wired hosts are likewise associated. The wired hosts could be sending private data among one another. This data can be

handily perused in the event that a malevolent remote client does a MITM assault utilizing ARP Cache Poisoning.

The ARP store harming assault can be performed regardless of whether the remote clients are in a remote organization empowered with security highlights like Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access (WPA). WEP and WPA scramble the Layer-2 parcels. ARP, being in a similar layer as IP, is a Layer-3 convention. Consequently the harmed ARP bundles sent in a remote organization are sent inside a WEP or WPA encoded outline. The remote clients that are doing the ARP stores harming assault have previously joined the organization and subsequently all parcels sent from these remote clients are scrambled. The Access Point will acknowledge and advance these bundles to the objective remote machine since they are WEP or WPA encoded at first appointed key. At the point when the bundle arrives at the objective machine the casing is unscrambled and the parodied planning is perused from the ARP outline. The ARP reserve is refreshed with the mock planning, in this manner harming the ARP cache.

2.6.1 Attack Scenarios

The five types of attack scenarios are described in the following;

- **Attacking Wired Clients**

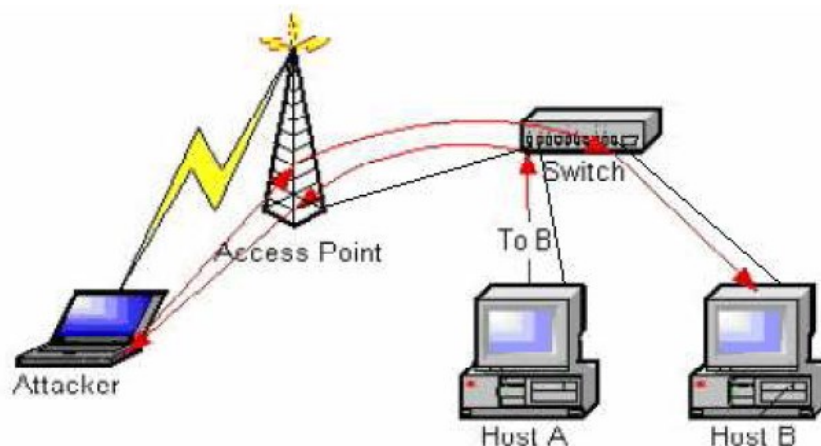


Figure 2.13: Attacking Wired Clients by Wireless Client

In Figure 2.13, a remote client, the Attacker, sends a mock ARP parcel to Host A expressing that Host B's IP address is planned to the Attacker's MAC address. Comparatively the Attacker sends a ridiculed ARP parcel to Host B expressing that

Host A's IP address has the Attacker's MAC address. In this way the Attacker harms the ARP stores of Hosts A and B, subsequently guiding the traffic between them to go through the Attacker.

- **Attacking Wireless Client and Wired Client**

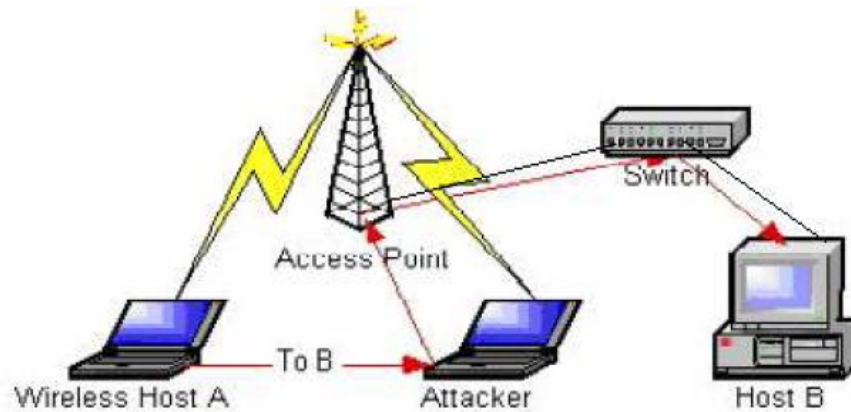


Figure 2.14: Wireless client attacking a wired client and a wireless client

In Figure 2.14, the Attacker sends caricature ARP parcels to wired Host B and Wireless Host A, in this manner harming their ARP stores. Both the casualties are in the much communicated space as that of the Attacker, subsequently parodied ARP bundles will arrive at the people in question.

- **Attacking Wireless Hosts**

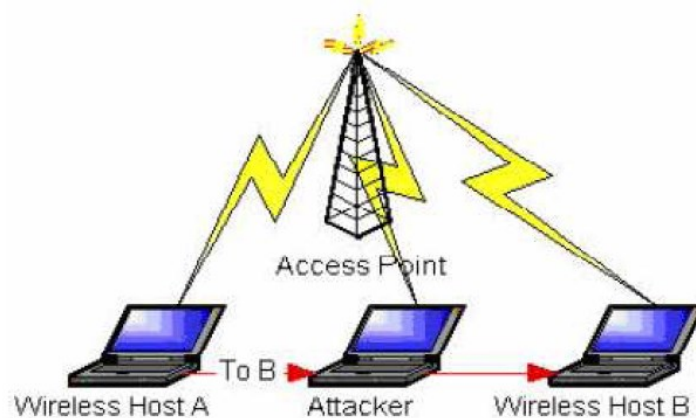


Figure 2.15: Attacking wireless clients

The two wireless hosts which are associated with the same AP as the Attacker are attacked by the attacker, while they are in the same broadcast domain.

- **Attacking Roaming Wireless Hosts**

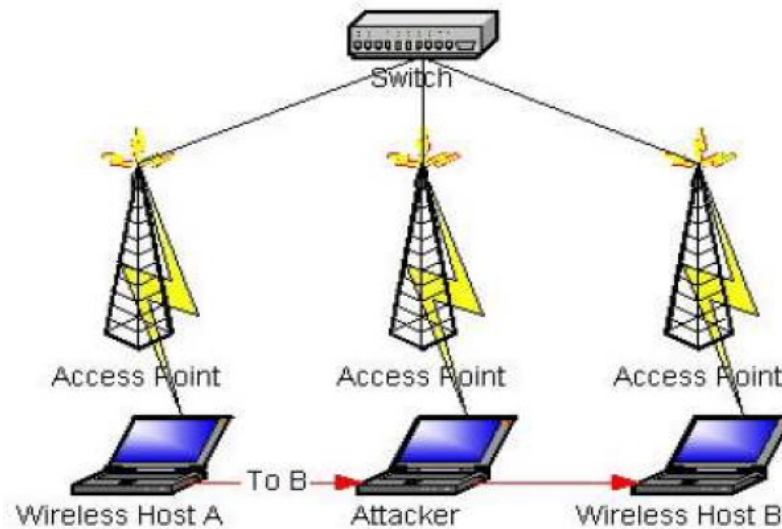


Figure 2.16: Attacking roaming wireless hosts

In Figure 2.16, there are different APs associated with a similar switch. In 802.11b organizations, to accomplish meandering, the APs should be associated with a similar switch. Because of this set up every one of the remote hosts related with these APs have a place in a similar transmission space. Consequently any manufactured ARP bundle sent from the Attacker can arrive at any remote host associated with any of these APs.

- **Attacking Home Networks**

Most merchants sell a joined switch, switch and passage in one gadget. In these gadgets, the switch is for wired clients in a similar LAN, the switch is for the clients to associate with their Internet Service Provider (ISP) and the AP is remote hosts in the LAN. Such a gadget fulfills the requirements of a home network.

In this blend gadget the AP is associated with similar switch as the wired clients. This outcomes in the wired clients are being helpless against an ARP Cache Poisoning assault from remote clients. With this consolidated home door gadget, the previously mentioned assault situations from 2.4.1.1 - 2.4.1.2 are conceivable on home organizations too, as displayed in Figure 2.17 and Figure 2.18.

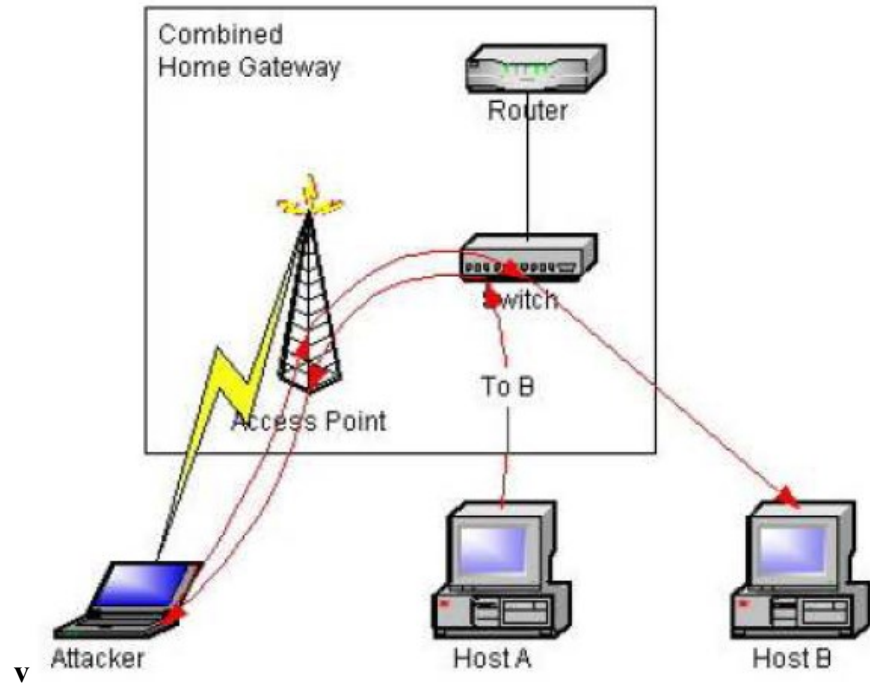


Figure 2.17: Attacking Two Wired Clients via a Wireless Client in a Home Deployment

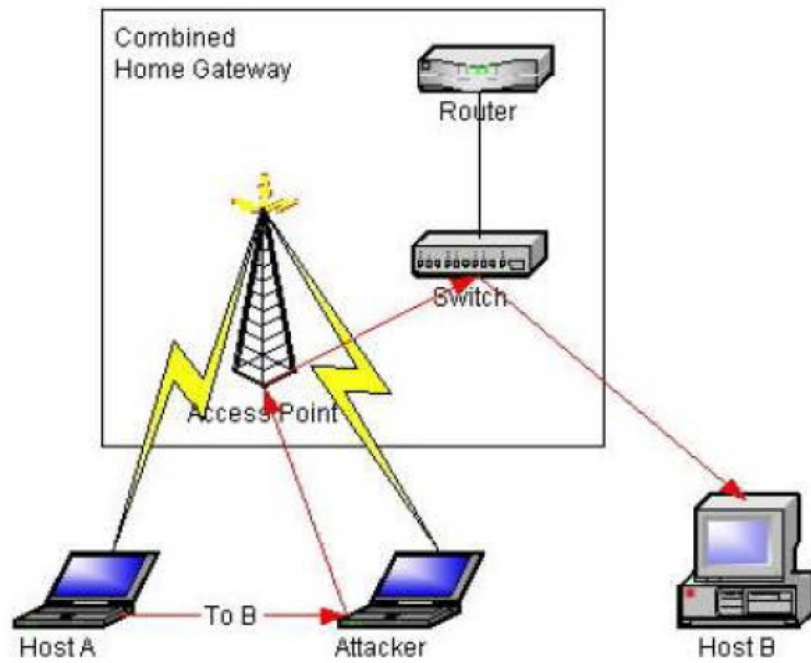


Figure 2.18: Attacking a Wired Client and a Wireless Client in a Home Network

CHAPTER 3

TICKET BASED ADDRESS RESOLUTION PROTOCOL

The Address Resolution Protocol (ARP) is the magic that binds the organization and connection layers of the IP convention stack. The essential capability of ARP is to plan IP addresses onto has equipment tends to inside a neighborhood. In that capacity, its accuracy is fundamental for legitimate working of the organization. Be that as it may, as different conventions inside IP, ARP is dependent upon a scope of serious and proceeding with security weaknesses [8, 9]. Foes can take advantage of ARP to mimic hosts, perform man-in-the-center assaults, or just DoS casualties. Besides, such goes after are unimportant to perform, and hardly any countermeasures have been generally sent.

Current organization conditions present two focal plan difficulties for ARP security. First and foremost, the arrangement should not need ARP be disposed of. The conveyed base of IP is enormous and various enough that supplanting any significant part of the IP convention stack is in fact and cost restrictive. Also, the expenses of carrying out ARP security should be negligible. Asset obliged gadgets and as of now computationally stacked has can't bear to financial plan a lot of assets for ARP security. Any arrangement that would certifiably change the presentation profile of ARP won't be taken on. The essential explanation that proposed arrangements [19, 10, 16, 21] have not been generally sent is that they presently can't seem to all the while address these two necessities.

This framework presents the Ticket-based Address Resolution Protocol (TARP) convention. Covering executes security by circulating midway produced MAC/IP address planning validations [3, 5]. These verifications, called tickets, are given to clients as they join the organization and are consequently circulated through existing ARP messages. Dissimilar to other well-known ARP-based arrangements, the expenses per goal are diminished to one public key approval for every solicitation/answer pair in the most pessimistic scenario. Thusly, TARP is a doable methodology for the different variety of existing organization competent gadgets. This framework will be given a nitty gritty depiction of the convention plan and its execution inside the Linux working framework. Our exploratory investigation shows that TARP holds similarity while diminishing the solicitation costs by as much as two significant degrees over existing

conventions. This framework will investigate a scope of vital functional issues including denial and steady organization and demonstrate the way that TARP can be sent with restricted managerial oversight.

Note that TARP typifies a focal plan compromise. Ticket age costs develop at the straight backwards of the ticket's lifetime. The ticket lifetime directs the weakness to replay attacks. Hence, directors can straightforwardly control cost and security through the choice of ticket lifetime. The capacity to adjust between these contending factors is a focal advantage to TARP's plan. There are investigated the administration of this tradeoff all through and think about the need of such splits the difference in the commonsense utilization of safety advances.

Security in goal administrations stays an open issue. Whether settling space or hostnames [15, 6, 7], cases of address proprietorship [3, 5], or other organization antiques, one necessities to validate the items and newness of gotten information. This work addresses another point in the plan space of these administrations. In that capacity, it tends to be utilized to educate regarding the particular expenses and benefits of goal administrations. Specifically, our commonsense examination shows that for particular sorts of goal, incredible execution gains can be accomplished by somewhat loosening up security prerequisites.

3.1 A Ticket-Based Approach

The significant defect in ARP is the absence of message verification. Until the end of this paper, it can be ordered ARP weaknesses as tending to be categorized as one of the two following classes:

- Answer parodying: fashioning an ARP answer to infuse another location relationship into the casualty's store
- Section harming: fashioning an ARP answer to supplant a location relationship in the casualty's store

The proposed framework tends to these weaknesses through the Ticket-based Address Resolution Protocol (TARP). Canvas carries out security by appropriating halfway created authentications [3, 5]. These verifications, called tickets, confirm the relationship among MAC and IP tends to through articulations endorsed by the nearby: Local Ticket Agent (LTA). Each ticket encodes a legitimacy period as a termination time. Obviously, the utilization of lapse times expects a few type of free clock

synchronization between the backer LTA and the approving clients. Such synchronization is a typical prerequisite for some conventions, and gadgets for its requirement are notable [7].

To safely perform address goal utilizing TARP, a host communicates an ARP demand. The host with the mentioned IP address sends an answer, joining recently got ticket. The mark on the ticket demonstrates that the LTA gave it, i.e., the MAC to IP address planning is legitimate (or possibly was at the hour of issuance — see denial beneath). The mentioning host gets the ticket, approving it with the LTA's public key. Assuming that the marks is substantial, the location affiliation is acknowledged; in any case, it is disregarded. With the presentation of TARP tickets, an enemy can't effectively produce a TARP answer and, in this manner, can't take advantage of ARP harming assaults.

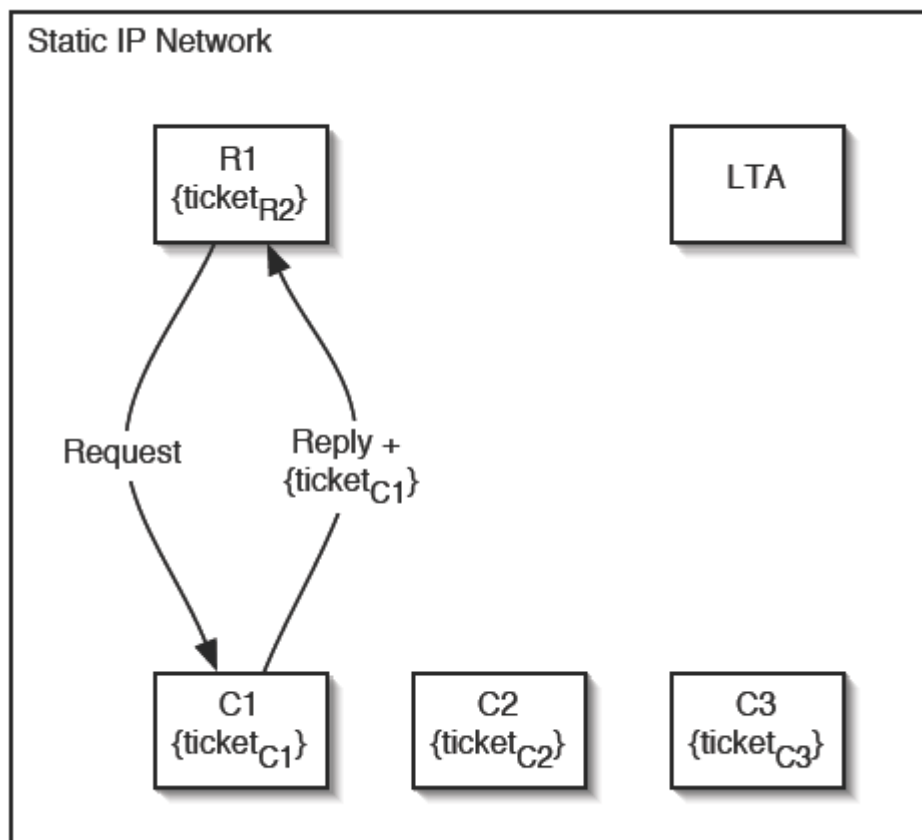


Figure 3.1: Static IP Address Assignment - Hosts Receive TARP Tickets

3.2 The TARP Protocol

The implication by which a ticket is made and disseminated is reliant upon whether the IP address tasks are static or dynamic. Outlined in Figure 3.1, at whatever point a host is added to a static task organization, it is designed with the organization public key, an IP address, and a ticket. Since the affiliations are probably not going to change oftentimes, setting long ticket lifetimes might be adequate. Notwithstanding, there are: security, execution, and authoritative contemplations connected with the determination of ticket lifetimes.

In unique IP organizations, has are relegated IP locations and setup boundaries by a design server utilizing the Dynamic Host Configuration Protocol (DHCP). Each host gets a rent on an IP address and sends a recharging demand upon lapse as displayed in Figure 3.2. Right now, the DHCP server might reassign the host a similar IP address.

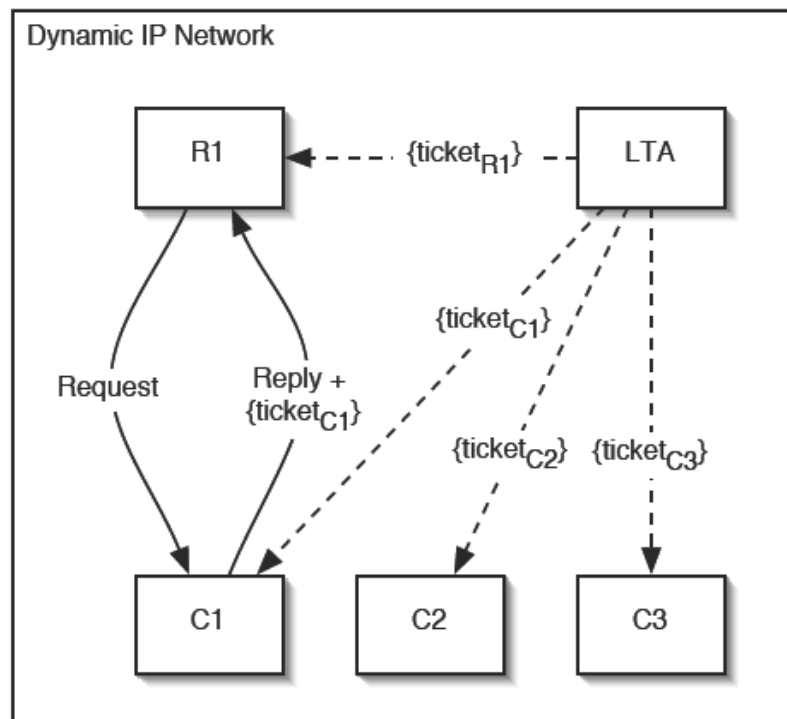


Figure 3.2: Dynamic IP Address Assignment - Hosts Receive TARP Tickets

In a TARP-enabled dynamic IP organization, the DHCP server additionally carries out the usefulness of a LTA. In light of a DHCP demand, the server bundles a ticket with the arrangement data. Likewise, the ticket lapses alongside the IP rent. Note

that tickets are by definition public, consequently a safe correspondence channel is superfluous. Having the DHCP server assume the part of LTA kills the requirement for extra ticket dissemination messages, consequently keeping up with straightforwardness of convention plan.

Also, utilizing this strategy for dispersion is coherent, as DHCP was intended to disseminate design boundaries. A host requires the LTA's public key to check tickets. Key conveyance is generally secure whenever performed out of band. While less secure, this circulation could likewise be performed through statement and client acknowledgment, like that in the Secure Shell (SSH) convention [39]. Tragically, this permits an enemy new strategies for assault. For this paper, we just think about manual dispersion of the LTA's public key.

The activity of ticket goal continues indistinguishable in both the static and dynamic cases whenever tickets have been appropriated to each host. Covering message stream is like the ARP, with the special case that the ticket is added to each answers as characterized in the previous section.

3.3 Ticket Format

Keeping up with in reverse similarity with ARP is significant for the reception of any improved location goal convention. Similarity is accomplished by incorporating the ticket into the ARP answer; no progressions need occur to the solicitation. As displayed in Figure 3.3, the ticket is annexed as a variable length payload, with the ticket header changed in like manner.

- The difference of the TARP reply form ARP is the ticket header. If it is a TARP reply *Magic* field in the ticket header is applied and it is assigned to 0x789a0102.
- *Type* field in TARP is designated the cryptographic algorithm while has only unique message type in TARP.
- In the ticket, *SigLen* is the length of signature. To ensure proper operation, he the information in the remaining fields are used.
- The address association are created by the *MAC Address* and *IPAddress*.
- How long the ticket valid is indicated by the *Expiration Time*.

- The time for generating and using ticket for ticket revocation is indicated by *Issue Timestamp*.

ARP Reply	
Magic	
Type	Sig-Len
MAC Address	
IP Address	
Issue Timestamp	
Expiration Time	
Signature	

Figure 3.3: TARP Reply Packet Format

3.4 Revocation

A truth of current organizations that IP/MAC address affiliations can alter; dynamic ties (e.g. DHCP) or changes in network design can happen before a ticket terminates. To be secure, one should give a repudiation system that safely informs clients about the tickets that they are presently not legitimate. Authentic investigations of repudiation have looked to restrict the expense of warning, e.g., CRLs and different information structures [18, 4, 20], limit notice dormancy, e.g., OCSP, or give systems to compromising security assurances and semantics [4, 17].

Denial addresses the focal tradeoff of TARP. Since denied ticket might be replayed out of the blue preceding its termination, executives might be enticed to keep the lifetimes short. Be that as it may, ticket issuance costs develop at the direct converse of the ticket lifetime. The capacity to adjust the harmony of these contending factors through the choice of ticket lifetimes is a focal advantage to its plan. The least complex strategy for taking care of denial is to give endorsements that are just legitimate for a brief time frame. This comparable to the brief declarations recommended in the SPKI/SDSI framework. When the tickets are just legitimate for a brief time frame, the weakness to replay is restricted and no notice is fundamental. It is note that a window of weakness to replay likewise found in S-ARP. The window that is equivalent to the reserve hold season of the ARP answer. Clients of TARP can give comparable window by setting the lifetime of the pass to the ARP store hold time. Be that as it may, the

weight of the making the tickets is on the LTA, as opposed to on the actual hosts. We tentatively investigate the expenses of the ticket creation and approval.

ARP affiliations are enduring in networks where IP addresses are allocated physically. Therefore it could be worthwhile to make tickets whose lifetimes are basically endless for these static affiliations. In those uncommon situations where mappings change, one can disavow through reissuance, every clients would just utilize the most recent expiry timestamp ticket. This "most recent ticket wins" method would be defenseless against dynamic assaults in which the foe can hinder conveyance of the new ticket. Such goes after address a strong foe inside the neighborhood, and may flag bigger and more difficult issues. Thus the gamble might be OK for some conditions.

The most reliable arrangement is to carry out a different denial administration. Such arrangements range from the conveyance of straightforward marked endorsement disavowal records to quick internet based confirmation of ticket legitimacy. The straightforward arrangements like CRLs are probable most suitable, as the expenses of the mind boggling ones would overshadow the expenses of getting ARP. Subsequently, the straightforward, minimal expense arrangements will be utilized in all organizations yet those with the most noteworthy security prerequisites.

A significant inquiry is the way to recuperate within the sight of give and take of the LTA. This problem is like CA recuperation in PKI frameworks. Dissimilar to numerous PKI organizations, all TARP clients overhauled by a LTA are probably going to be under a solitary regulatory space. Subsequently, it is sensible to expect that every client can be physically designed with another endorsement on a case by case basis. Bigger spaces might utilize procedures to diminish the effect of LTA split the difference, e.g., key parting, issue and deny LTA keys through nearby declaration the board benefits, and may utilize computerized administration apparatuses for the dissemination of LTA marking keys.

3.5 Attacks against TARP

Networks executing TARP are helpless against two kinds of assaults - dynamic host pantomime and DoS through ticket flooding. A functioning enemy that can be impeded all correspondence between two hosts can mimic its casualty by satirizing its MAC address and replaying a caught ticket. While this assault is available in the ARP, with TARP, the enemy can imitate the casualty as long as the ticket is substantial.

Besides, a variation of this assault is available in any arrangement that utilizes storages. Luckily, this assault can be moderated by utilizing a layer-2 switch with port security, subsequently forestalling MAC caricaturing.

A foe can likewise exploit the expense unevenness between producing a TARP answer and handling it. Taking advantage of this, a DoS assault can be sent off by flooding the casualty with counterfeit TARP answers. These counterfeit answers are unimportant to produce, subsequently permitting the foe to effortlessly send large number of TARP answers at an expense extends lower than the subsequent approval endeavor. By flooding a casualty with fake ICMP demands and comparing TARP answers, the enemy effectively dodges even a state-ful ARP execution and consumes the casualty's CPU assets. As this assault results from ICMP conduct, moderation requires transformation of that protocol.

3.6 Macro-Benchmark

The large scale benchmark notices the full circle season of the three tried conventions: ARP, S-ARP, and TARP. While direct estimation in the portion is potential, it picked an aberrant course, estimating delay at the application level. For this technique, ARP is utilized as a pattern. The above is determined by taking the distinction among ARP with both TARP and S-ARP. Since the above is the ideal outcome, the circuitous strategy creates similar outcomes as an immediate estimation. Furthermore, estimating delays from the application level not just reflects genuine expenses, it gives steady estimation among the tried conventions.

To see full circle delay from the application level, the framework utilized a custom ping program that flushed the framework's ARP reserve after all of the ICMP reverberation demand/answer pair. It is guaranteed that every estimation incorporated the above of address goal. The framework performed five analyses, each comprising of 1000 ICMP reverberation demands. These tests estimated the full circle delay for TARP and ARP with and without reserving. The results are shown in Table 3.1.

Table 3.1: Round-Trip Delay for TARP and ARP

Protocol	$\bar{x}(\mu\text{s})$	$\sigma(\mu\text{s})$	Median(μs)	\bar{x} Overhead(μs)
ARP	1178.59	259.98	1108	N/A
TARP	1364.21	253.93	1297	185.62

3.7 Micro-Benchmarks

Operationally separating TARP's above gives knowledge into how the convention will perform on various sorts of gadgets. Covering message stream starts by mentioning a location affiliation. Since the solicitation is indistinguishable from that of ARP, no above is presented. At the point when the remote host answers, a ticket is basically affixed to an answer. If this requires extra framework I/O and organization traffic, the above is unimportant. After getting a TARP answer, a host should confirm the ticket signature. This stage requires a lopsided cryptographic activity and ought to accordingly be researched. As TARP works in client space, reserve refreshes bring about extra setting switches, dialing back activity. Deciding this cost predicts the increase coming about because of a bit based execution. At last, TARP acquires critical execution upgrades by monitoring the ticket generation expense.

Operation	Average(μs)	σ
Ticket Signature Verification	119.12	2.00
Update of ARP Cache	74.07	7.15
Ticket Generation	4535.36	68.33

Table 3.2: Execution Time for TARP Operations

Table 3.2 sums up the miniature benchmarks. The exploratory climate was more controlled than that of the full scale benchmarks, subsequently, even with one hundred runs, a little standard deviation was accomplished. The ticket signature confirmation comprises principally of a 1024-cycle RSA signature check. There is no such thing as ticket in the reserve. The typical season of 119 μs compares straightforwardly to the distinction between the two TARP varieties estimated in the large scale benchmark. The store update likewise mirrors the qualities estimated in the large scale benchmark.

Assuming TARP was carried out in kernel space, 74 μ s would be practically disposed of, eliminating basically all above when tickets are reserved. At last, ticket age requires 4.5 ms. this is where the genuine force of TARP is presented.

3.8 Discussion

As recently demonstrated, TARP does exclude key and ticket dissemination messages. Rather than making another dissemination convention, DHCP is utilized. Clients getting tickets close by DHCP answers can promptly validate the DHCP answer by confirming the mark on the ticket. Notwithstanding, this just gives one-way confirmation. At times, confirming clients prior to circulating DHCP rents and tickets might be expected to limit network access or stay away from assaults, for example, IP address pool weariness.

While TARP effectively and productively forestalls store harming, it is pointless without an arrangement for steady organization.

The main obstruction holding the blended organization back from working is the check of an ARP answer. A TARP empowered have can't just acknowledge all ARP answers; this negates any security acquired from the new convention.

Despite the fact that TARP is intended to interoperate with ARP to work with gradual organization, has running ARP are not at all safeguarded by TARP. Additionally, TARP hosts' reserve sections referring to white listed has are likewise likely to harming. To accomplish the most from TARP all hosts on the neighborhood ought to be moved to TARP.

CHAPTER 4

SYSTEM DESIGN AND IMPLEMENTATION

The Address Resolution Protocol (ARP) is important for IP networks to ensure proper operation. However, some vulnerability in the ARP protocol enables a raft of IP-based impersonation such as man-in-the-middle, or DoS attacks. The proposed system is implemented to detect and defend these vulnerabilities by using TARP protocol.

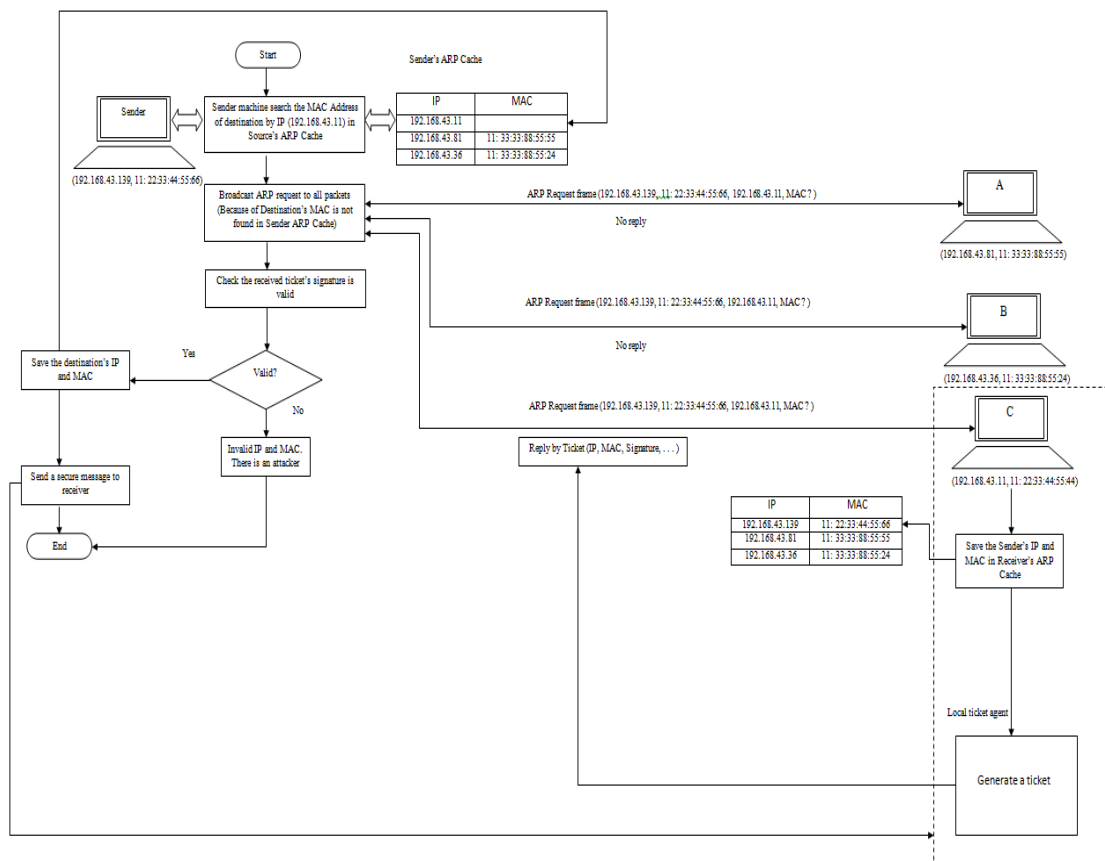


Figure 4.1: Detail Process Flow

In this system, TARP is implemented to provide security by centrally distributed secure MAC / IP address mapping with existing ARP messages. This implementation shows the detail process of the TARP protocol within the window operating system (Window 10) and developed by C#.Net Programming Language on Microsoft Visual Studio 2015. The detail process flow of the system is shown in Figure 4.1.

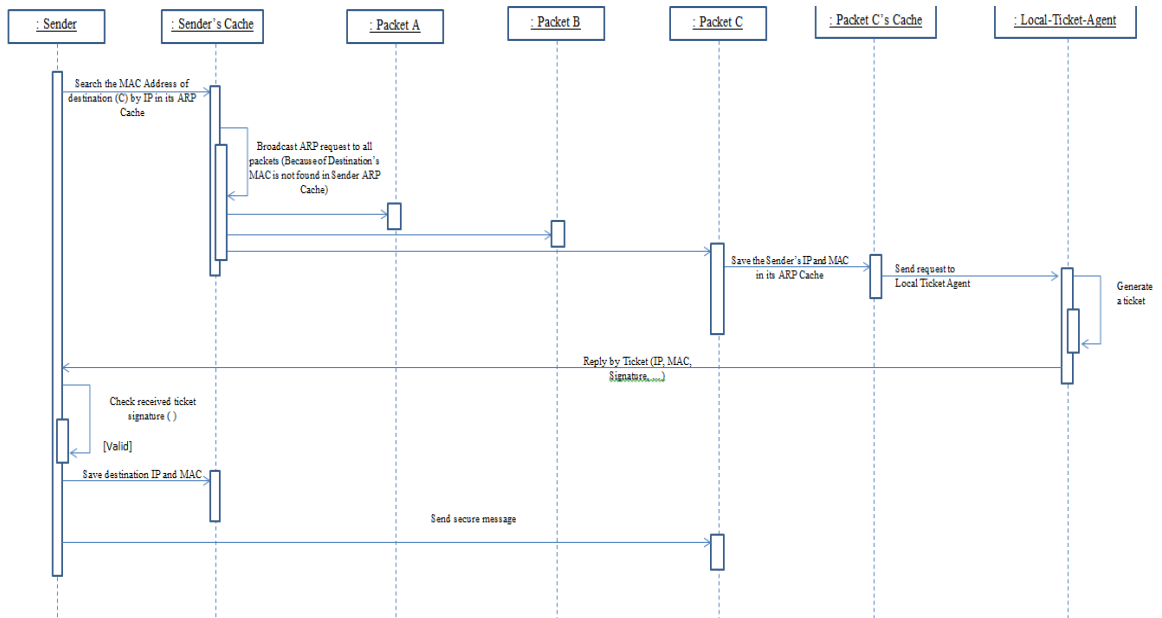


Figure 4.2: Sequence Diagram of System

When a sender packet want to send message to the receiver packet, the sender must check the receiver packet's MAC address in its ARP cache (Sender's ARP cache). If the receiver packet's MAC is existed in the sender's ARP cache, the sender can directly send the message to the receiver packet. If not, the sender must send the ARP request to the receiver packet. This request will contain sender's (IP, MAC) and receiver's (IP). The request will send to all members in this system. Only the real receiver with respect to the requested IP address will reply the request by sending security Ticket. The sender will check the reply message via ticket information to maintain the security. If the reply message is not compact, the system marks the reply as attacker reply (such as DoS attack or Man_In_The_Middle attack). For sequential explanation point of view, the sequence diagram is shown in above Figure 4.2.

4.1. Sending ARP Request Frame from Sender to Receiver (Receiver's MAC not exist in Sender's ARP Cache)

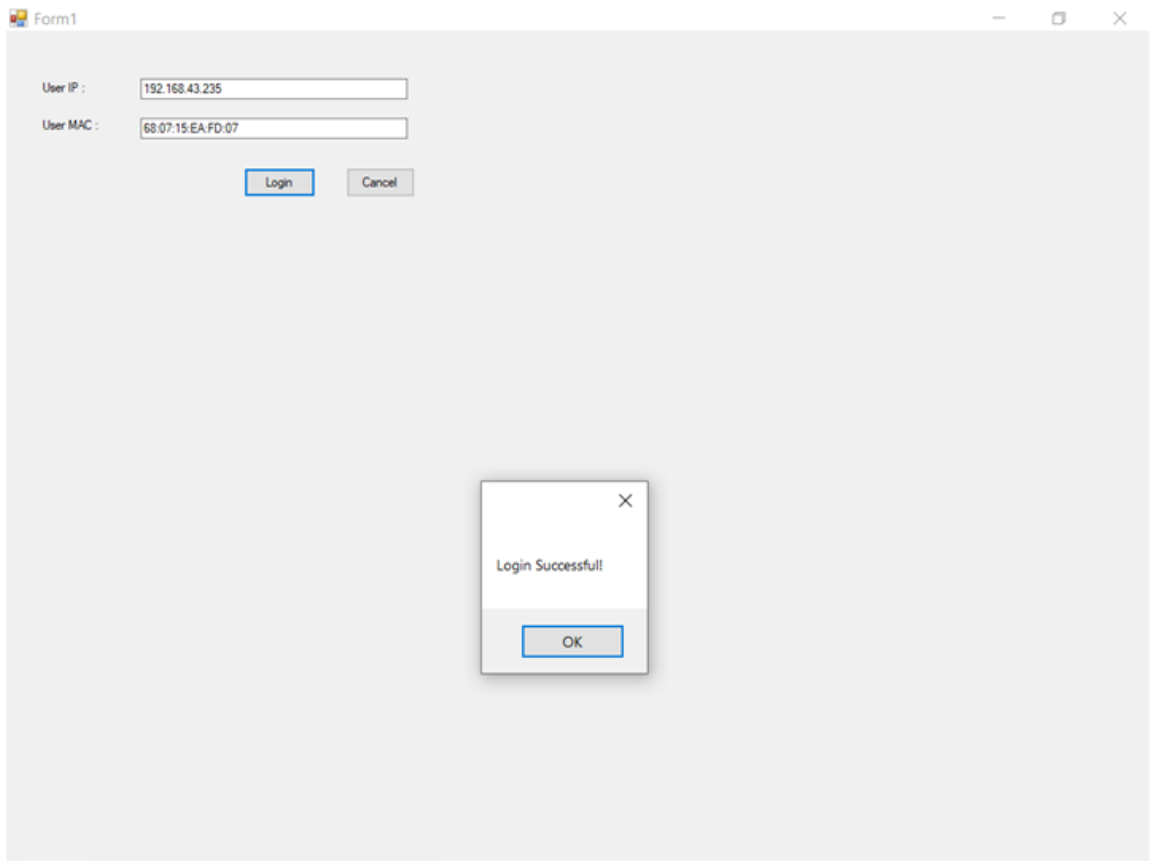


Figure 4.3: Sender Login Page

When a node wants to send a packet via the proposed system, the user must be login by User IP and User MAC address for authentication purpose. After the proceeding of authentication process is finished, the user will reach to the main page of authenticated login user. The main page of each node will consists of five main menus. They are: “Member List” menu, “Send Message” menu, “ARP Cache” menu, “Check Attacker” menu and “Received Ticket” menu.

Main			
Member List	Send Message	ARP Cache	ReceivedTicket

Figure 4.4: Main Page of a Node

“Member List” menu in figure is used to view the members which is exist in the same network. Member List show the IP address of each member for communication purpose. “Send Message” menu is to send message to the desire node in the network. Figure 4.5 shows the detail process of message sending request. Before sending ARP Request Frame to the receiver, the system will check the receiver’s MAC in sender’s ARP cache. So, the system supported a button “Check in ARP” to check the destination IP and MAC is exist or not. If not, the request frame must be send to all members as shown in Figure 4.6.

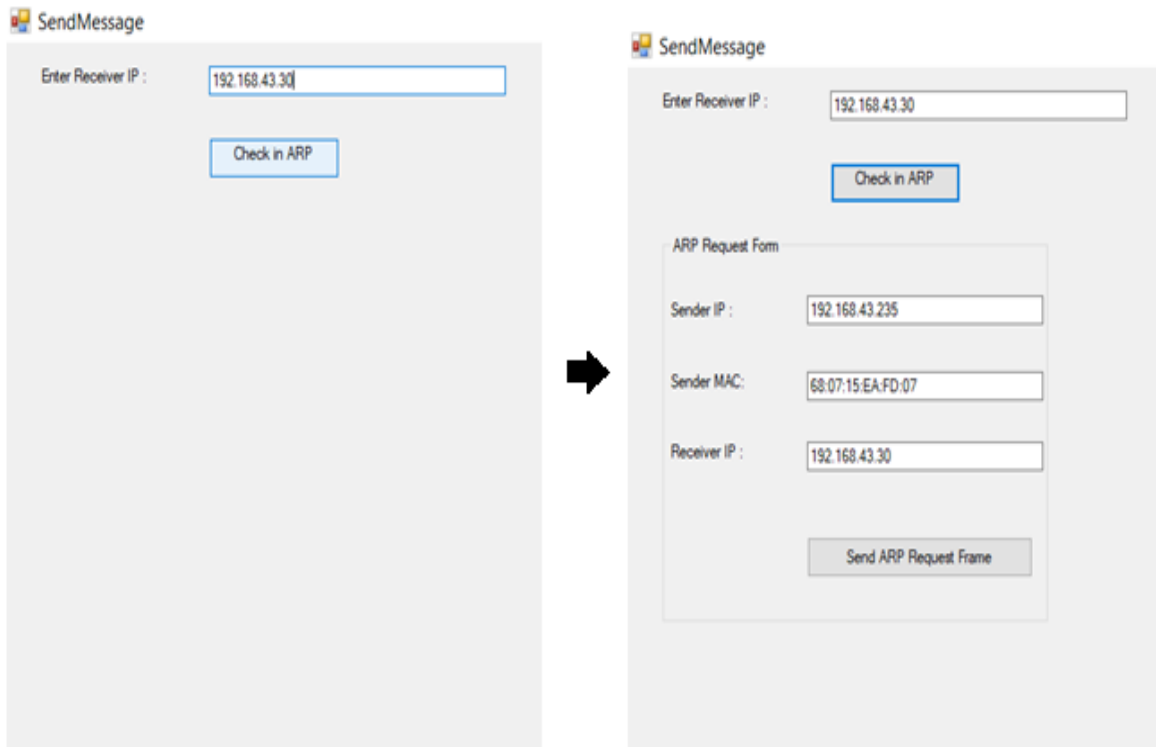


Figure 4.5: Checking Receiver IP Address and MAC Address in Sender's ARP Cache

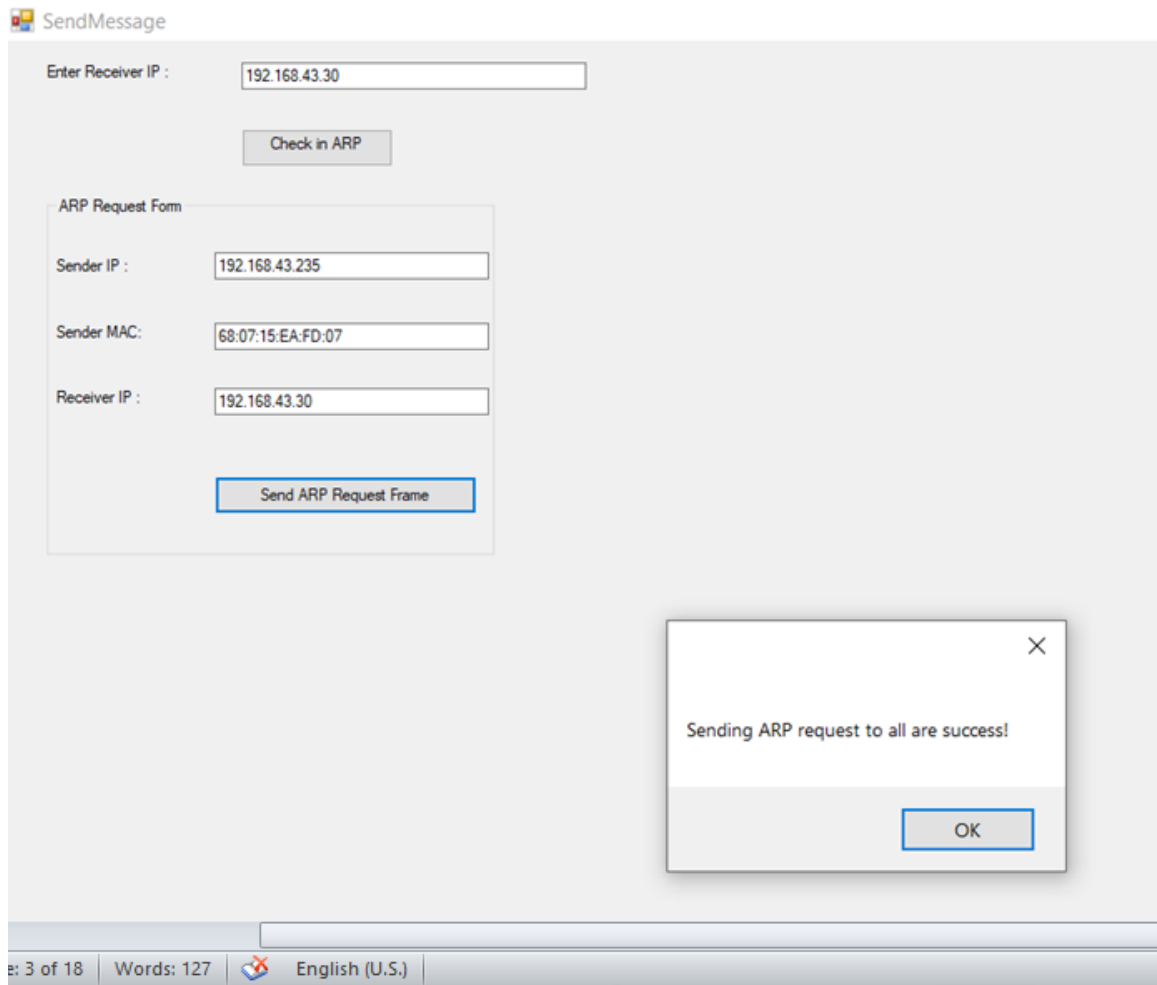


Figure 4.6: Sending ARP Request to All Members

4.2 Replying ARP Request by Receiver to Sender

After the receiver login processing is authenticate, the receiver can check the APR Request message in its APR cache. In the receiver's ARP cache, sender's (IP, MAC) address will be found as shown in figure 4.8.

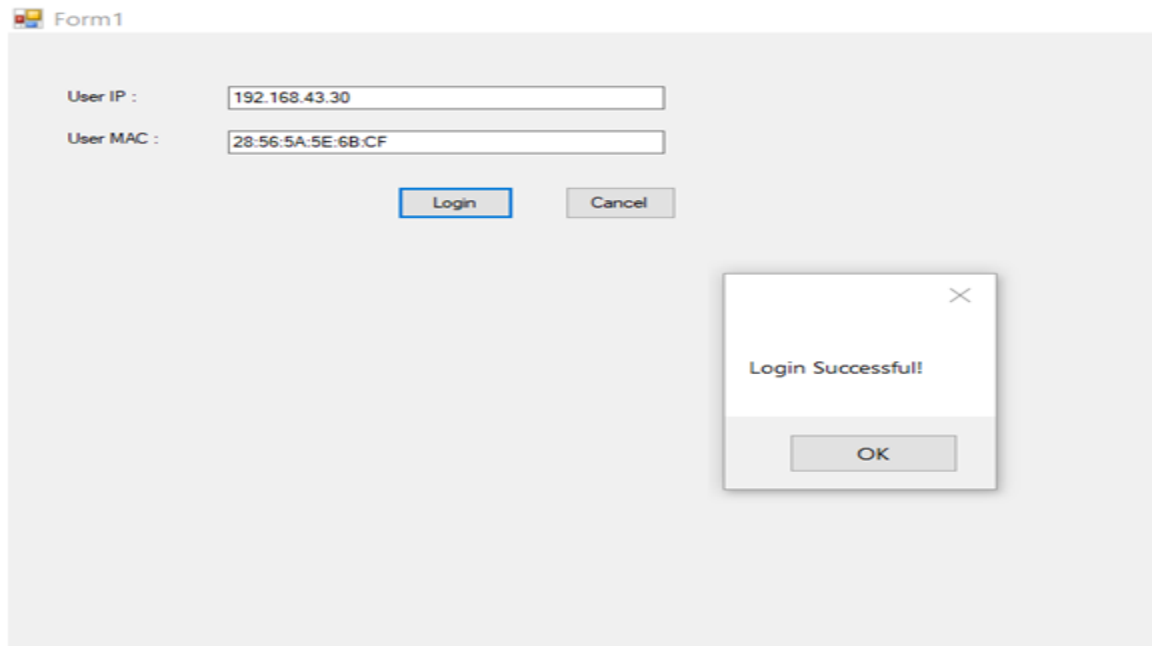


Figure 4.7: Receiver Login Page

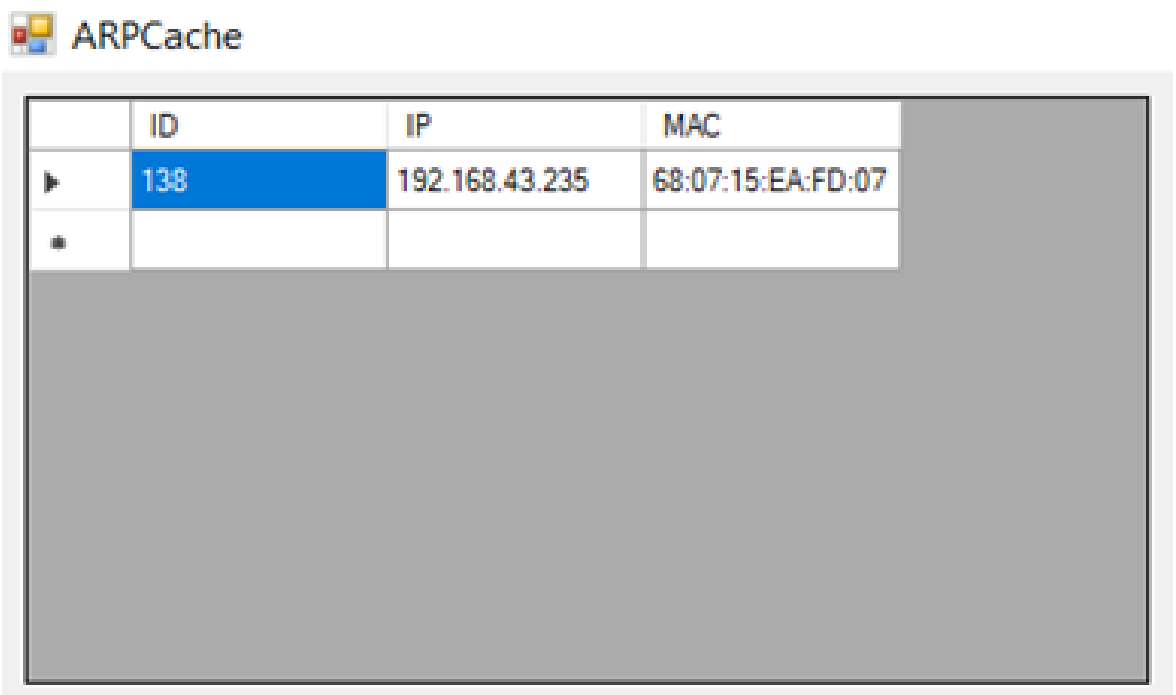


Figure 4.8: Check sender IP&MAC address in receiver ARP cache

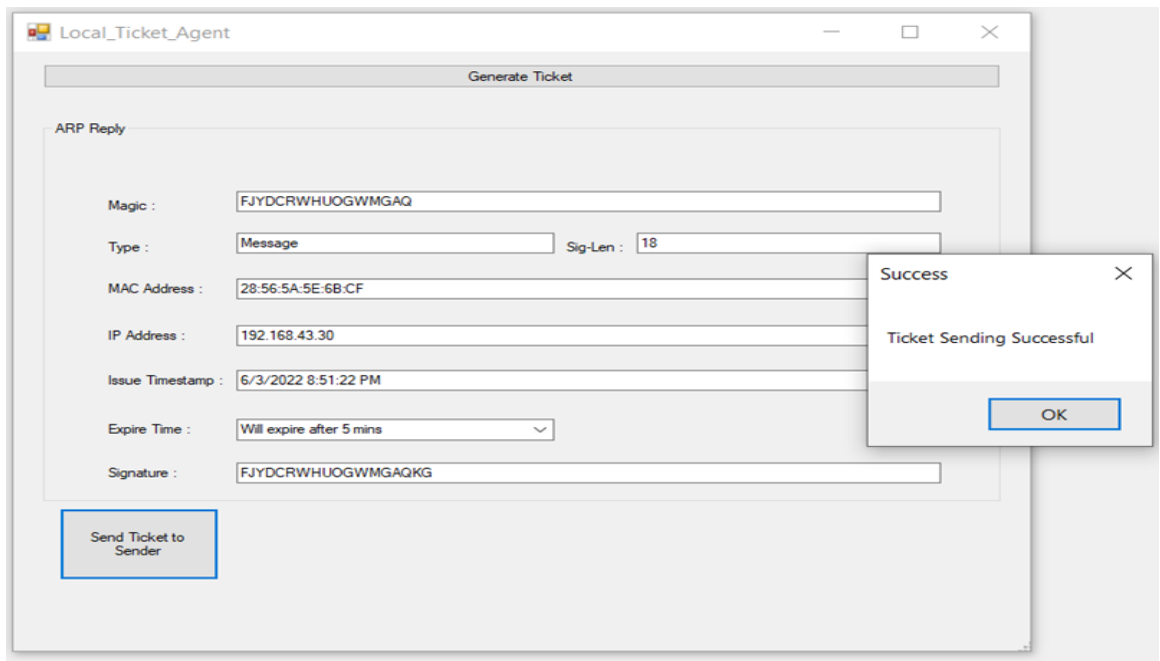


Figure 4.9: Receiver Reply Ticket

When the receiver reply the sender’s ARP request, the receiver generate a ticket to control and eliminate the ARP spoofing. The ticket includes Magic, Type, Sig_Len (signature length), MAC Address, IP Address, Issue Timestamp, Expire Time (Ticket Expire Time) and Signature as shown in Figure 4.9. Then, the receiver sends back the generated ticket to the sender.

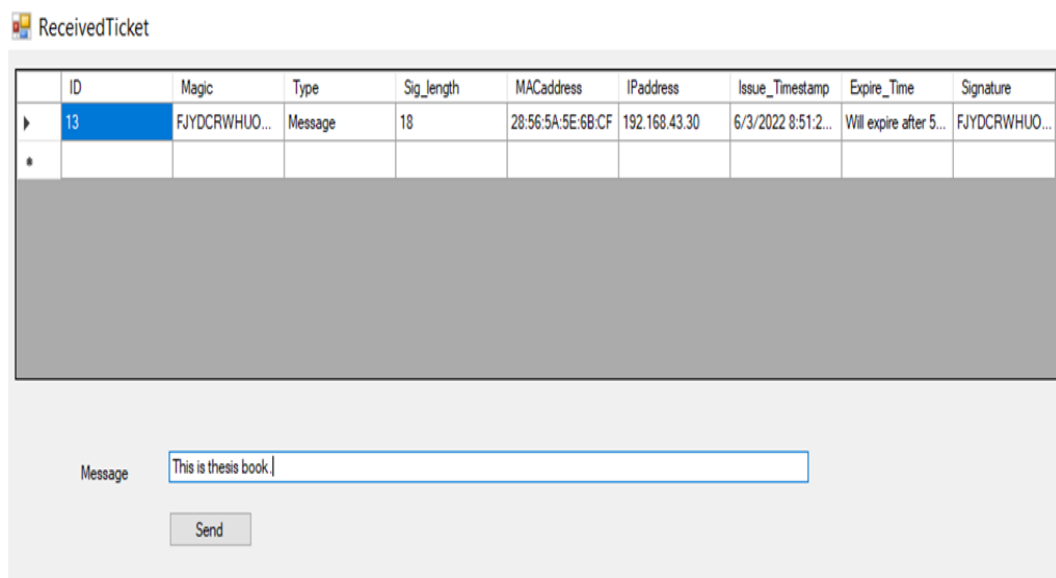



Figure 4.10: Sender Check Ticket and Send Message to Receiver

After receiving receiver's ticket, the sender check and ready to send message as shown in figure 4.10. The message from the sender will be seen by the receiver is as following Figure 4.11. The sender message will be attached with the sender's IP to the receiver.



The screenshot shows a window titled "Messages" with a table of received messages. The table has four columns: a selection column with a right-pointing triangle, an "ID" column, a "Message" column, and a "Sender" column. The first row is highlighted in blue and contains the ID "32", the message "This is thesis book.", and the sender IP "192.168.43.235". A second row is partially visible below it, containing a small black dot in the selection column and empty cells in the others.

	ID	Message	Sender
▶	32	This is thesis book.	192.168.43.235
•			

Figure 4.11: Receiver Receive Sender's Message

4.3 Attackers

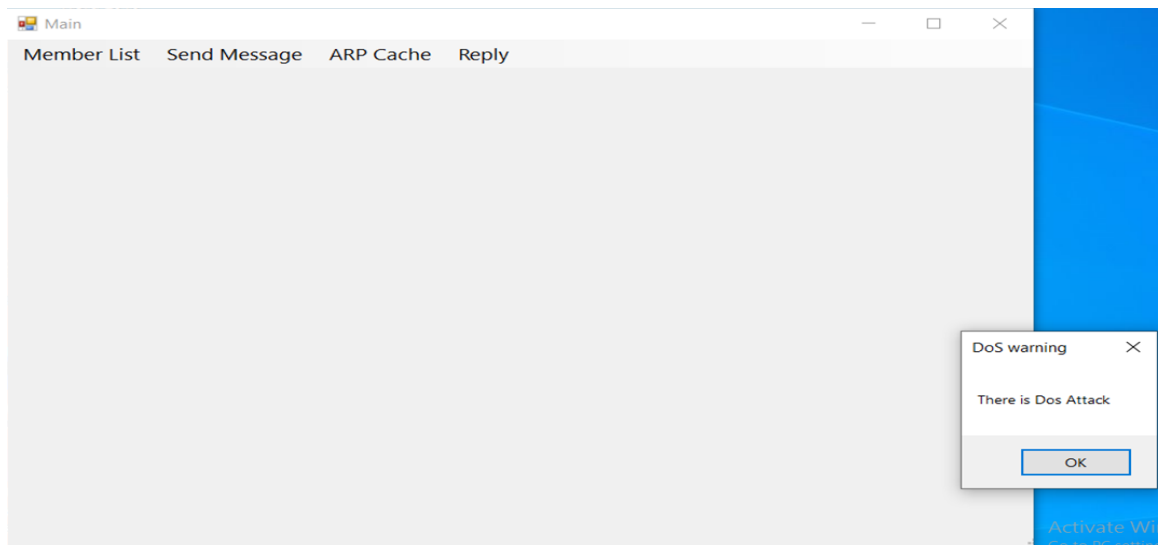


Figure 4.12: Detecting DoS Attacker

The system detects two types of attackers such as: DoS attacker and MITM attacker by checking the reply message whether the reply ticket is included or not and valid or not. This system will show the detected attacker as shown in Figure 4.12 and Figure 4.13.

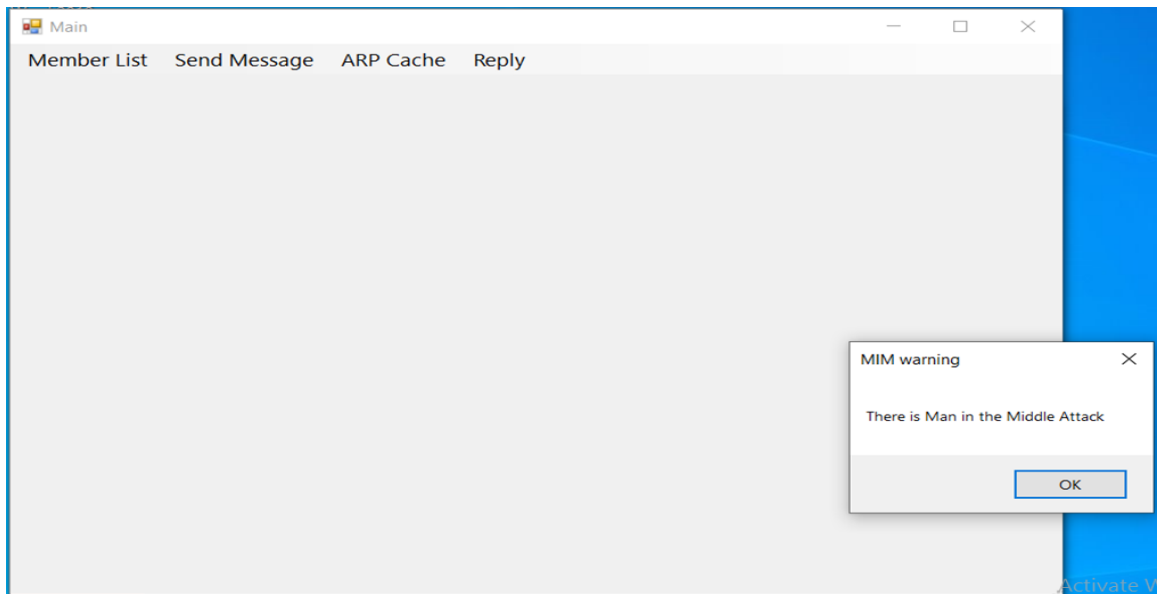


Figure 4.13: Detecting MITM Attacker

CHAPTER 5

CONCLUSION AND FURTHER EXTENSIONS

ARP spoofing has become a major problem in the current situation. It can cause many other attacks like MITM attack on a secure socket layer. Therefore, steps must be taken to prevent such an attack. This system implements TARP for network security as an extension to ARP and preventing to ARP spoofing attacks. TARP achieves resilience to cache poisoning. TARP reduces cost by as much as two orders of magnitude over existing protocols.

5.1 Conclusion

Remote organizations have turned into a basic piece of the present organizations. The simplicity of arrangement, minimal expense, portability and high information rates have contributed altogether to their prominence. The mode of information transmission in remote organizations makes them intrinsically less secure than wired networks. For remote organizations to get to the Internet they should be associated with a wired organization by means of an Access Point or a remote switch. This has driven remote organization hardware makers to execute remote Access Points and remote switches with an implicit switch for wired clients and a WiFi passage for remote clients. The setup inside the gear is with the end goal that the wired and remote

organizations are inside connected together to such an extent that they are in a solitary Local Area Network (LAN). This blend of wired and remote organizations represents another class of assaults on wired networks by means of uncertain remote LANs. One such class of assault is the Address Resolution Protocol (ARP) Cache Poisoning assault. Contingent upon the remote LAN set-up, beforehand secure wired organizations might become defenseless against assaults from remote clients in a similar LAN as the wired client. Worked as an enhancement to ARP, TARP provides completeness and flexible to reserve harming. It decreases cost by as much as two significant degrees over existing conventions (e.g. SARP, ESARP).

5.2 Limitation and Further Extension

ARP weaknesses will stay a serious organization security issue until a good option is acknowledged. This system is demonstrated TARP to be more reliable, yet much work stays before our execution can be comprehensively utilized. Expansions including support for dynamic conditions are imperative. At long last, we look for additional functional experience; a more profound comprehension of the expenses and impediments of the methodology must be gathered from field testing.

REFERENCES

- [1] Anatomy of an ARP harming assault. <http://www.watchguard.com/infocenter/article/135324.asp>, got to June 2015.
- [2] B. Bit and J. Dimov. Remote passages and arp harming: Wireless weaknesses that uncover the wired organization. <http://downloads.securityfocus.com/library/arppoison.pdf>.
- [3] C. Adams and R. Zuccherato. A General, Flexible Approach to Certificate Revocation, June 1998. <http://www.entrust.com/securityzone/whitepapers.htm>.
- [4] C. A. Gunter and T. Jim. Summed up authentication denial. In POPL '00: Proceedings of the 27th ACM SIGPLAN SIGACT discussion on Principles of programming dialects, pages 316-329, New York, NY, USA, 2010. ACM Press.
- [5] Cisco Systems. Impetus 4500 Series Switch Cisco IOS Software Configuration Guide, 12.1(19)EW.
- [6] D. Bruschi, A. Orgnaghi, and E. Rosti. S-arp: a protected location goal convention. 2013.
- [7] Infoblox was founded the defense system for DNS Hijacking and Cache Poisoning Attacks in the Domain Name System (DNS) in 1999 in [Chicago, Illinois](#), by Stuart Bailey who was at the [University of Illinois](#)
- [8] J. Galvin. Public Key Distribution with Secure DNS. In Proceedings of the sixth USENIX Security Symposium, pages 161-170, July 2016.
- [9] K. Seo, C. Lynn, and S. Kent. Public-Key Infrastructure for the Secure Border Gateway Protocol (S-BGP). In Proceedings of DARPA Information Survivability Conference and Exposition II. IEEE, June 2001.
- [10] M. Gouda. furthermore, C. Huang. A solid location goal convention. PC Networks, 41:860-921, January 2013.
- [11] M. Noar and K. Nassim. Certificate Revocation and Certificate Update. In Proceedings of the 7th USENIX Security Symposium, pages 217-228, January 1998.

- [12] M. Myers. Revocation: Options and Challenges. In R. Hirschfeld, editor, Financial Cryptography FC '98, volume 1465, pages 165-171, Anguilla, British West Indies, February 1998. Springer
- [13] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. RFC 4035, Protocol Modifications for the DNS Security Extensions. Web Engineering Task Force, March 2005.
- [14] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. RFC 4034, Resource Records for the DNS Security Extensions. Web Engineering Task Force, March 2005.
- [15] R. Droms. Dynamic host setup convention. RFC 2131, March 2017.
- [16] R. Droms and W. Arbaugh. Validation for dhcp messages. RFC 3118, June 2011. <http://www.ietf.org/rfc/rfc3118.txt?number=3118>.
- [17] R. Housley, W. Portage, W. Polk, and D. Solo. RFC 2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile. Web Engineering Task Force, January 2019.
- [18] S. M. Bellovin. Security issues in the tcp/ip convention suite. PC Communications Review, 2(19):32-48, April 2009.
- [19] S. M. Bellovin. A glance back at "security issues in the tcp/ip convention suite". In twentieth Annual Computer Security Application Conference (ACSAC), pages 229-249, December 2014.
- [20] W. Aiello, J. Ioannidis, and P. McDaniel. Beginning Authentication in Inter domain Routing. In Proceedings of tenth ACM Conference on Computer and Communications Security, pages 165-178. ACM, October 2013. Washington, DC.

AUTHOR'S PUBLICATION

- [1] Chit Hnin Wai, Si Si Mar Win, “Security Control by Ticket Based Address Resolution Protocol”, the Proceedings of the 9th Conference on Parallel and Soft Computing (PSC 2022), University of Computer Studies, Yangon, Myanmar, 2022.