National College of Ireland

Detecting and preventing Man in The Middle attack using Interlocking protocol and HMAC caused by perpetrator

MSc Internship

Cyber Security

Neha Patil

Student ID: x18200192

School of Computing

National College of Ireland

Supervisor: Mr. Vikas Sahni

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Neha Patil……

Student ID: 18200192……..……

Programme: Cyber Security…… **Year:** 2020……..

Module: MSc Internship……..……

Lecturer: Mr. Vikas Sahni……..……

Submission Due Date: 17/8/2020……..……

Project Title: Detecting and preventing Man in The Middle attack using Interlocking protocol and HMAC caused by perpetrator

Word Count: 7369…… **Page Count:** 20……..……..……

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.
I agree to an electronic copy of my thesis being made publicly available on NORMA the National College of Ireland's Institutional Repository for consultation.

Signature: ……

Date: ……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Detecting and preventing Man in The Middle attack using Interlocking protocol and HMAC caused by perpetrator

Neha Patil

X18200192

Abstract

Man in the Middle attack is one of the most threatening attacks to the data communication. Detecting this attack could be a crucial job for the cyber security professionals and there is no extensive technique for preventing this attack. In the process of the data communication the main motive of the cybercriminal is to interrupt and intercept on-going communication between legitimate users. Once this has been successfully achieved then by taking complete control over the communication channel, the attacker can further manipulate or discard the message for sake of gain. Thenceforth, the main objective of this project is to detect and mitigate Man in the Middle Attack using Interlocking protocol along with HMAC (Keyed-Hashing for Message Authentication) function instead of using one-way hash function for additional security. Where HMAC will provide further security against cryptoanalysis attacks and will be less affected by collisions. Nevertheless, HMAC's computing speed is faster than the rest of the existing algorithms and will provide ancillary security even if the hash function is broken. The proposed system is efficient enough to mitigate against Man in the Middle Attack.

1. Introduction

In today's digital world it has become effortless to communicate with each other using modern communication techniques. However, preventing this process from malicious entities and unauthorized access been proved to be strenuous and seems to be recurring challenge to cyber security expertise. In the process of data communication, securing the data while transmitting it over wired or wireless channel and preventing sensitive information from unauthorized access is a crucial task for a sender who is transmitting any kind of confidential information. Even though the data which will be transmitted is encrypted, there are chances of such data to be exposed by eavesdropper also, there are chances that attacker can interrupt the communication channel or particularly saying key exchange process which is used by sender and receiver. This type of method of tampering the communication by the human being is known as Man in The Middle Attack (MITM), Monkey in The Middle Attack or TCP Hijacking. OWASP specifies that MITM is not only attack but also a technique which can be implemented by penetration tester while performing the vulnerability assessment for organization or it can be utilized in the testing phase of web application development.

In 2015 according to the site called nakedsecurity.com about 49 hackers were caught all over the Europe for using Man in The Middle Attack and email phishing to trick users for ambush banking fraud. Man in the Middle Attack can invoke different types of attacks on your networks like Denial of service (DoS), DNS spoofing and Port stealing [2]. As mentioned above , the attacker interrupts the process of key exchange which take place between two legitimate users and proceed with creating two independent connections with sender and receiver by employing new keys. In the process of communication, the attacker will pretend as sender at receiver side and vice versa utilizing the fake key.

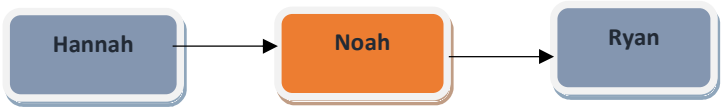

Figure 1: Man in the Middle Attack

- In the above case Hannah will initiate SSL handshake request for Ryan without knowing that the ongoing connection has been intercepted by Noah who is Man in the Middle.
- Post that Noah will initiate its different SSL session with Ryan.
- After establishing SSL session with Ryan, Noah generates and sends the certificate to Ryan which appears to him to be sent from Hannah.
- If Hannah accepts this certificate, then it means she has unknowingly established an SSL connection using Noah's fake key.
- This results in giving authority to Noah for intercepting the communication between Hannah and Ryan. Noah can alter or discard the messages sent by Hannah to Ryan via the SSL session he established with Hannah earlier without suspecting by both the sender and receiver.

The purpose of the project is to mitigate Man in the Middle attack which is causing by the eavesdropper by making the architecture more complicated and harder to understand by the middleman/Eavesdropper.

Motivation: Mainly the research conducted on preventing Man in The Middle attack uses RSA algorithm with conventional one-way hash function. The main objective of this project is to prevent and mitigate Man in The Middle Attack using HMAC function instead of using one-way hash function which will provide additional security against cryptoanalysis attacks and will be less affected by collisions. HMAC's computing speed is faster than the rest of the existing algorithms. However, HMAC will provide security even if the hash function is broken. Decryption in HMAC is much easier than the encryption process. The core mechanism of the proposed research is to encrypt and then split your message into two parts and transmitting it over a channel gradually so that the perpetrator cannot expose or alter the message even if he has sender's and receiver's public key. The first part will the

encrypted message itself and second part will contain result of the HMAC hash function. This will result into the Man in the Middle who is trying to eavesdrop will be unable to decrypt the first message by using its private key. However, it will result only in creating new message with some redundant information.

2. Related Work

Cyber criminals are continuously enhancing their skills for finding new tactics on daily basis for introducing vicious attacks. So, one of the new strategies is doing MIMT using Stealth MIMT. Attacker is manipulating and tricking users to carry out ARP poisoning by creating a dummy ARP response protocol configuration. For performing this malicious task this configuration is using WPA2 key management. Vikas Kumar had done some remarkable work for mitigating Stealth MITM attack, ARP poisoning and IP spoofing by introducing a Wireless Intrusion Detection System. NS-3 Network simulator has been used by researcher for the simulations.

The proposed system works only in one case and that attacker should be static although for the dynamic hacker it is totally dependent on the capability of node to detect ARP poisoning properly [1]. The daily exponential increase in usage of internet leads to tremendous rise in volume of data processed by satellites. And this rise exposing the satellite communication to eavesdroppers and making them more active. The hackers are taking leverage of satellite channel for performing many malicious activities like manipulating the information, redundant packet sending, message reuse and forgery of data. Due to lack of encryption there is possibilities of replay attacks. Conventionally certificate-based protocols are being advised to use for preventing MITM attack. However, it does not work for satellite communication. The improved key exchange protocol has been introduced by In-A Song et al [2]. This protocol contrasts the existing protocols on different metrics like Timestamp, analysis of the performance, communication efficiency and resource management. Timestamp helps to detect MITM attack by executing two-way judgment. In addition to that it utilizes various ID parameters for preventing replay attacks. This protocol has been efficiently working for preventing MITM attack in operational satellite environment.[2]

2.1 Time Latency Analysis:

For calculating the time latency in any network timing analysis has been carried out. Timing analysis is nothing but the thorough analysis of digital circuit for verifying the timing constraint utilized by components and interfaces are meeting the suggested timestamp. Frequency analysis is been used by complex circuits for operating in intended way. Geoff Hamilton and Benjamin Aziz [3] have discovered the various vulnerabilities which can be further exploited using MITM attack present in current protocols like Wireless sensor network which are being used to analyze mobile systems based on timing analysis. For preventing these mobile systems, a static analysis has been conducted on them and as a result of that they found using precise timing model MITM can be prevented effectively. The outcome of the conducted analysis is defining the integrity property which leads toward MiM property of distance bounding protocol. The main objective of distance bounding

protocol is measuring the distance between two attributes with the help of precise timing. For an instance, this attribute could be status of authentication. However, this distance should be as minimum as possible and the packet arriving to target system should be in timely manner. For improving the security aspect and time constraints of the proposed system in real time scenario, some factors like Min/Max time getting engaged in completing the process of authentication should be taken into consideration as it is very simple for an attacker to exploit the steady protocol to carry out DoS attack on the networks well as slow protocol directly related to the cost so it could indirectly cause denial of resourses. Similarly, Visa Villivaara [4] et al introduced new methodologies for detecting MITM attack which uses the same fundamental elements.

The core of the proposed system is related to the time constraints utilized by the system without any authentication factor. In this system the MITM attack is being detected by analyzing the timestamp of the given TCP packet header. By taking the average of the time latency between data gathered from previous session and current connection the long delays can be detected which means the presence of the intruder in the network. The outcomes of this proposed system are providing high accuracy even in unusual circumstances. The authors proved that the time latency attribute can be set as a benchmark for detecting MITM with low probability of retaining the false positives. The scope of the proposed system is bounded to non-mobile systems only and the high-speed internet is highly recommended for the efficient functionality. However, the proposed system is used for monitoring some complex structured targets such as banking sites or a company networks which are not being targeted by the noobs and only interest the expert hackers.

Various efficient protocols are being used for detecting and preventing MITM attacks such as TLS protocol which authenticates the process of key exchange with the help of public keys infrastructure. On the other hand, Chuams protocol intended to detect suspicious activity within the network or MITM attack with the help of utilizing very low amount of resources and with the lesser assumptions. Chuams protocol presume that the eavesdropper may trick the users by pretending to be a legitimate user but cannot modify or interrupt the confidential communication. The working of this protocol is divided into three parts. In the first part, key exchange take place between participants. In part 2, generation of the random key. and in part 3, referring the predefined four scenarios participated check and verify that each has the similar two strings. If two participants are not having the same string, then it means the communication has been violated by the eavesdropper. Such reliable protocols, like TLS, are used by networks to reduce various cyber-attack threats, such as MITM. TLS uses a public key system to authenticate the exchange of shared keys. In a contradictory view, the Chaum protocol, which is another protocol used to detect MITM attacks, does so without implying the authenticity of the public keys exchanged. Has Three stages of execution are included in the Chaum[5] protocol. Two parties involved interchange public keys in the first step, while the production of random sting by both parties begins in the second step. The first party uses a

cryptographic way to connect itself to the formed string before transmitting the string to the second party after accepting the string. The third step involves all negotiating parties using 4 random "scenarios" to check the ownership by each party of the two right strings. In the event of an MITM attack, the above-mentioned protocol causes MITM to cause the two communicating parties to have separate pairs of strings in their hands.

The third scenario has been practically performed by Alan T. Sherman et 5 [6] for elaborating the efficiency with the help of timing analysis for detecting MITM attack in text messaging. They discovered that the distinguishable delays which were produced by an eavesdropper can be analyzed further to sense the presence of Man in the middle. With compare to other protocols like Zfone and Interlock, they have found out that Chuam's protocol works very efficiently against the more vicious attacks. However, the probability of receiving the false positive is greater as the external factors are not taken into consideration in the proposed system. Whereas we can increase the precision and accuracy of the results by conducting the research on the time constraints. By through study of the delay which we are getting into the result the rate of receiving false positive can be reduced and can make our more vigilant for sensing the presence of eavesdropper in the network.

2.2 Analysis on Behavioral Anomalies

Securing the data or stealing that data over the communication channel needed a thorough understanding of behavior of the network in normal as well as in unusual circumstances. Deviation of the outcome from the standard or expected result is known as anomaly. The comprehensive analysis has been performed by Jeffery L. Crume [7] on detecting Man in the Middle attack. The proposed system consists continuous recording system which track incoming IP address, time consumed by each session which is running on target server and User ID. In the given system each session has been allotted with the predefined time frame so if abrupt no. of sessions are caused by the one IP address then the actively analysis system will capture out this malicious activity and will record this suspicious IP address and will take the proper action against that IP. The research on Man in the idle attacks which are server-based shows that the presence of the intruder is there if server is receiving the noticeable amount of users requesting for the login into that server with the same IP address for no reason. The author has proposed a system which will detect suspicious ip which are crossing the threshold such as allowed number of User IDs within a predefined time frame or even the system will automatically prevent itself from such malicious activity. The explained system and the preventive method consist of some attributes which integrates the different level of risk tolerance accepted by different organizations. The stress on the server could be reduced by automatic detection of such malicious activity and the action taken post detection for preventing the system [8].

In order to successfully execute Man in the Middle Attack on LAN network one needs a methodology which consist of 3 steps. In step 1, Acquire access of the intended network, in step 2, capturing the ongoing traffic and in step 3, adjust, manipulate, or drop the network traffic. Yisroel Mirsky et al. [9] has described MITM attack as simple but very devasting class of attack where the confidentiality, integrity, and availability been compromised by

anonymous person who interrupted the network traffic. When a local area network (LAN) is involved, to successfully execute a MITM attack involves following a 3-step prototype; (i) procure network access (ii) catch the ongoing network traffic in motion (iii) controlling, adjusting, or dropping the traffic.

Yisroel Mirsky et al. explained the man-in-the-middle attack as a simple yet persistent attack where a malicious object ambushes network traffic and in the process risks the confidentiality, integrity, and availability of the system. The researcher has elaborated that some countermeasures on Man In The Middle Attack needs more detailed explanation, false positive rate is bit higher or they are not convenient enough. The proposed system is enables LAN which uses a process consisting of impulse outcome analysis used in area where acoustic signals are evolved with the fit in and play feature which helps in detecting Man In The Middle. This intended system works similarly to the mechanism of echoes inside the cave which capture the variations in earth surface moreover identical to the rapidity of ICMP echo request formation between two hosts. They further provided the analysis which includes the usage of neural network in the formation of echo from the pulses of structural standard pattern. Nevertheless, simulation outputs illustrate that Vesper can identify MITM attack, however the necessary analysis should be conducted on the various attributes like ping techniques, countermeasures, expanding the strategy for system using WiFi, VPN etc.

Virtual private network requires TLS for its formation and the most important aspect in TLS set up is authentication procedure which is being carried out by exchanging the key in the process of communication and implemented by importing the certificates on the system. If the proper authentication policy is not being used at the time of key exchange, then it will be susceptible to MITM attack. The standard process is to approve the various PKIs by verifying the certificate which uses public key infrastructure and trusted certificate authorities. However, by exploiting the security flaws, Man in the middle attack can be carry out if PKI which has been used is appears.

MIDAS framework used for distributed assessment proposed by Enrique de la Hoz [10] et al. he has stated that this framework can be further used for detecting the man in the middle attack. He has explained that this framework is dependent on past research carried out on system management and network monitoring and can be utilize for introducing new strategy which allows detailed analysis of the certificates from the host to verify the authentication in the process of TLS.

Enrique de la Hoz et al. presented a distributed certificate evaluation system called MIDAS and clarified that it could be used to detect man-in-the-medium attacks. The authors also explained that the methodology is focused on network traffic monitoring and management frameworks, with the goal of providing a new approach that enables the successful review of certificates by hosts to assess their validity during the TLS process. However, the functionality of this mechanism is impressive further analysis should be conducted to form practical Bayesian systems which has been utilizes to provide the defense mechanism against the various malicious activities taking place in the network as well as suspicious certificate import [11].

2.3 Interlocking Protocol:

In the process of communication, WiMAX communication has been used by the systems which uses Internet of Things to establish the reliable communication in the shady areas where signal strength decreases with the distance. Utilization of this strategy cause one shortcoming that attacker can disrupt the process of communication through Man-in the middle attack. For detecting such activities Tae-Ho Cho proposed a system which uses Interlocking protocol. The motive behind using this protocol is to utilize fixed time latency value instead of using distance between two cells and packet size [12]. The proposed system using a method dynamic time delay decision for minimizing time latency of the forced latency interlocking protocol in IOT based mobile communication. The outcomes are impressive and supporting the validation of method by decreasing improved latency by 88.19% and improved detection rate by 7.97%. in contrast to this research Robbi Rahim proposed a system which utilizes Interlocking protocol for detecting Man in the middle attack even though the attacker has manipulated the message by stealing and replacing the public key [13].

2.4 HMAC Protocol:

In the mobile environment with the evolution in RFID, sensors, and hand-held devices, it has become necessary to protect wireless channel from various malicious entities without compromising the resourses and storage space. For efficiently utilizing the resourses and calculation capacity Kavitha Boppudi has proposed a system which allows effective use of the reader's processing power and storage space and to reduce the demand for the device's computing and storage power by implementing lightweight protocol such as HMAC [14]. In contrast to this research K V V N L Sai Kiranand Harini N. has utilized HMAC protocol for enhancing the security in IoT environment. The proposed research implements the test bed for performing the experiments by combining various cryptographic schemes. And from the results it shows that HMAC is more efficient and secure that the rest of the algorithms [15].

As from the above work it is evident that much work and research has been conducted in the field of detecting and preventing strategies of MITM using timing analysis or behavior anomalies of the network. However, very less work has been done on the preventing methods using some complex and effective authentication protocol such as interlocking protocol. Nevertheless, interlocking protocol is using the conventional one-way hash function which might be exploited through Man In The Middle Attack. So, in the proposed system for enhancing the security aspect, combination of Interlocking protocol and by replacing the existing one-way hash function with HMAC hash function has been used. HMAC's computing speed is faster than the rest of the existing algorithms besides, it provides security even if the hash function is broken. Decryption process in HMAC is much easier than the encryption process which makes it very difficult to break.

3. Research Methodology

As the primary objective of proposed system is to develop a protocol with higher accuracy, and which gives minimum false positive rate, Interlocking protocol along with HMAC hash function instead of using conventional one-way hash function has been used. Proposed system is intended to follow the CIA triad of data security that is Confidentiality, Integrity and Authentication besides that some other security attributes like nonrepudiation, access control and availability. From these 6 mentioned security attributes, 4 of them can be overcome by cryptography that is nonrepudiation, authentication, integrity, and confidentiality. Proposed system is try to cope up with 4 threat patterns and those are interruption which directly attacks on availability of the system, interception which will attack on nature of confidentiality, modification which will attack on Integrity and the last one that is fabrication which would attack against authenticity [26].

Core mechanism of the solution for preventing and detecting man in the middle attack is to first encrypt your message and then split it into two parts. First part will be encrypted message itself and on the second part HMAC function has been applied to make it more secure and transmitting it over a channel gradually so that the perpetrator cannot expose or alter the message even if he has sender's and receiver's public keys as the algorithm is completely hidden from him. [4]. Man in the Middle who is trying to eavesdrop will be unable to decrypt the first message by using its private key. However, it will result only in creating new message.

3.1 Overview of Interlocking Protocol:

Cryptography is a scientific technique which is been utilized for making the process of communication more secure. However, it targets to achieve prime security aspects like confidentiality, integrity, and authentication. RSA is an asymmetric encryption algorithm which utilizes public and private key for the process of encryption and decryption. However this algorithm is susceptible to the Man in the Middle attack. Interlocking protocol mentioned in the research is a protocol which is created by Ron Rivest and Adi Shamir to make the process of communication more secure by preventing it from interception caused by eavesdropper. The prime functionality of this protocol is to split your encrypted message into two parts and then send it over a channel. The first part could be encrypted message itself and the second part is one-way hash function. Which eventually results in eavesdropper to be unable to decrypt the message even if he is possessing private key. However, it will only create new message and will send it to the receiver. With the deployment of interlocking protocol it is possible to implement detection and prevention technique which provide outcomes with escalated accuracy. Below figure shows the implementation of interlocking protocol.

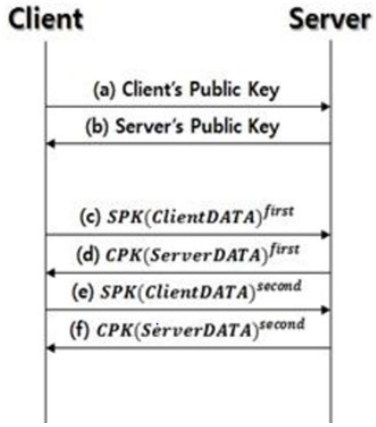

Figure 2: Interlocking Protocol

3.2 Overview of HMAC Algorithm:

In recent years, there has been a significant interest in creating a MAC based on a cryptographic hash code such as MD5, SHA-1 or RIPEMD-160. HMAC determines the function of the hash to be a black box. There are two main benefits of this. First, the latest edition of the hash function would be used as a basis for the implementation of the HMAC. The majority of the HMAC code is prepackaged and completely prepared for use without modification. Second, to replace the specified hash function in the HMAC deployment, simply remove the hash function module and transfer it to the new module. This could be done if you needed a quicker hash function. More precisely, if the reliability of the built-in hash function has been compromised, HMAC 's security could be kept simply by replacing the built-in hash function with a more secure one [25].

The main security attributes like authentication, nonrepudiation and integrity can be successfully achieved with the help of digital signature. In order to create the signature signing algorithm and the private key send by sender have been used. Verifying algorithm will be applied to the signature message pair by the receiver. The public key acts as a verification key on which verification algorithm has been applied on in order to verify the received message. If The status of this verification is true, then it means the message has been accepted; otherwise it is not accepted. For fulfilling this purpose of creation of digital signature hashing can be used. HMAC (hash message authentication code) is a particular message authentication code which consist of secret key and cryptographic has function. In this function unique hash value has been generated from the compressed image of the message. IF in case someone alters a message it will create different hash value as outcome even when the same hash has been used.

The HMAC-SHA256 [9] can be expressed as follows:

$$HMAC\ (K, M) = H((K \oplus opad) \parallel H((K \oplus ipad) \parallel M))$$

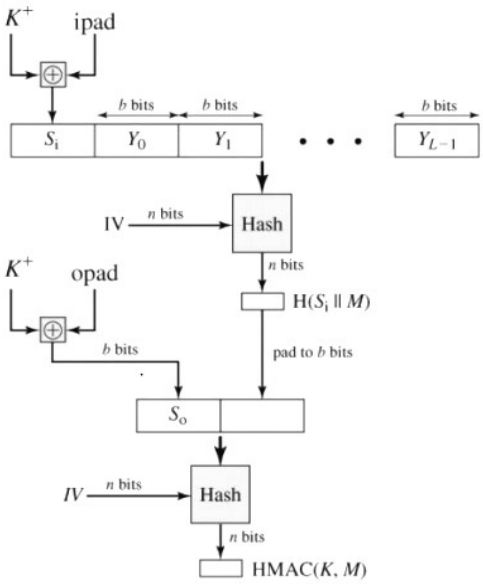

Figure 3: HMAC Function

4. Design Specification

To demonstrating interlocking protocol and HMAC hash function Python 3.8. has been used. Python is highly flexible and portable. However, it provides various cryptographic packages and functions and it is one of the best languages to implement cryptographic models. PyCharm 2019.2.2 which is an Integrated Development Environment (IDE) which was developed by JetBrains as cross-platform IDE has been used for the python programming. It is compatible with most of the operating systems like Windows, MacOS and Linux. It is very efficient and comes with various tools and functionality for building and writing applications. In this project following setup has been used to demonstrate Man in the middle attack's implementation.

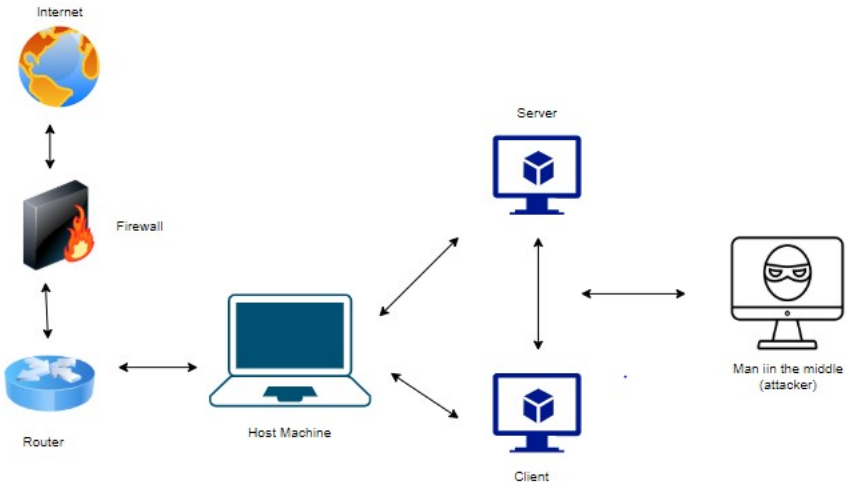

Figure 4: Proposed setup

Proposed Model:

In the proposed system we are showing conventional server-client communication. There are 3 classes client, server and middle_man. Their name represents their roles in the network. Localhost is our sever which is also known as a lookback address. We are pointing out to the localhost for sending the message [24]. And simple python code has been written for creating a socket client. However, socket module function present in python has been used. The socket. connect(hostname, port) opens a TCP connection to hostname on the port. Nevertheless for intercepting the ongoing communication between server and client another piece of python code has been written which has been provided with both public and private keys of server and client.

Following are the steps involved in the implementation part.

1. The client and server class represent the 2 parts involved in communication.
2. Here we simulate the situation where the attacker diverts the client to different server and that server acts as a proxy. In this manner the attacker intercepts the packets from both sides.
   -> this situation occurs when the attacker can inject some javaScript
   -> this is also caused due to xss
   -> this scenario will apply even when we tap into the network hardware.
3. The client sends the packets to port 11112 which is the proxy server.
4. The proxy saves the packets and forwards the packets as it is to the server at port 11111. This form of passive attack is difficult to detect as the attacker does not manipulate the data transfer.
5. The client connects to the server using tcp/ip protocol.
6. The server generates a key pair and sends the public key to the client.
7. The client also generates a key pair and sends its public key to the server.
8. The attacker incepts the public keys on both the sides.
9. The server encrypts the message and divides the hash into 2 part. It encrypts the second part of the hash again using same key and algorithm.
10. The server sends and first part to the client.
11. The client receives the first parts.
12. The client also encrypts the message and divides the hash into 2 part. It encrypts the second part of the hash again using same key and algorithm.
13. The client sends first part of the hash to the server.
14. The server receives the first part.
15. The server sends the second part of hash to the client.
16. The client too sends the second part of the hash to the server
17. The client decrypts the second part and joins it with the first part using a pre-defined algorithm.
    Again, decrypts the complete message.
18. The server does the same.

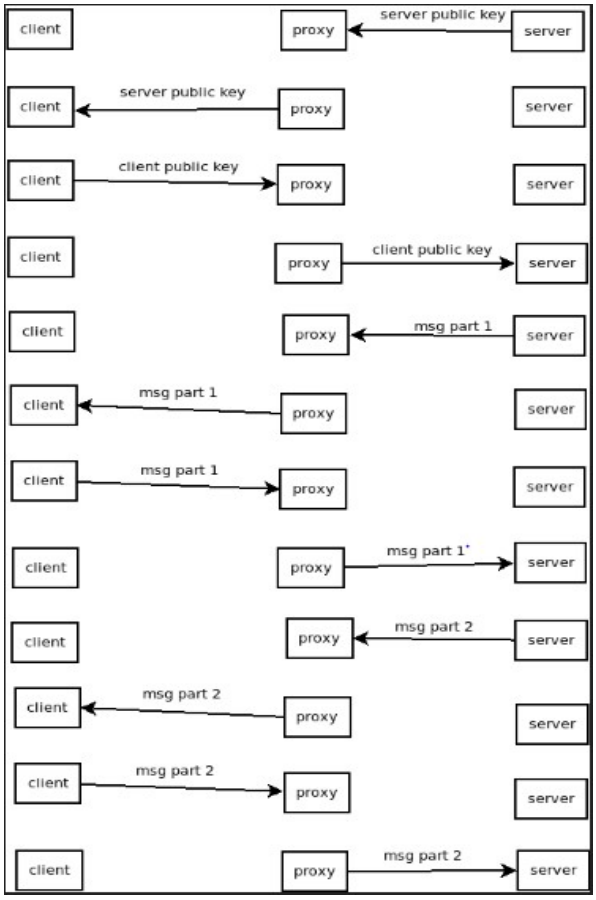

Figure 5: Server-client communication.

5. Implementation

The implementation part of the project demonstrates the techniques and procedures utilized for providing the solution. A program that starts a Secure Socket Layer (SSL) handshake which is a three-way handshake was written. The software will terminate the connection as soon as the certificate has been obtained from the local party. A further software for comparative analysis has been developed.

5.1 Hardware and Software Specifications

For the implementation of this project, an 8th Gen i5 Processor Laptop with 8 GB Ram was used. Our hardware is good enough to support the python coding which has been used for implementing server, client, and Man in the Middle.

The localhost which we are using as server has Windows 10 64-Bit OS. Following is the list of tools and software utilized for conducting experiment.

- **Python 3.8.4** – Python is a best suited for the execution of cryptography for analysis purpose. This language is supported by several IDEs for its implementation Python, itself a flexible and creative computer language, has widely available ezPyCrypto plus Stepic

libraries. ezPyCrypto is a basic API for armed cryptography in Python. It encrypts and decrypts random statistic bits, such as strings or data, using uneven key cryptography.

- **Wireshark** – for the purpose of this project we are using Wireshark software for capturing the packets. Wireshark is a commonly used cyber security application to intercept different packets on the host machine network, such as HTTPS, SSH, Telnet, and FTP. In the initial stage of our demo we are turning on the Wireshark to capture all network traffic and we will further analyse it for determining the Man in the Middle attack.
- **Python Packages** – various python packages and libraries were used for implementation of our cryptographic model such as RSA, sympy and numpy. The packages and libraries installed for this project has been listed in the configuration manual in detailed.

5.3 Code Tuning and Setup

In the initial setup it is mandatory to turn on the Wireshark in loopback mode for capturing all network traffic.

- **Server.py**: This file contains the code to setup our localhost as a server for the purpose of communication with the client.
- **Client.py**: This script consists of the code for setting up our client which will act as receiver. We have used Python socket programming for implementing the client.
- **Crypto.py**: This piece of code contains the core functionality of our project which includes implementation of interlocking protocol and HMAC hash function.
- **Middle_man**: This is the file which contains the python code for our Man in The Middle which is been used for intercepting the ongoing communication between server and client. We have provided public and private keys which has been generated from RSA.py file.
- **Output**: Outcomes of the project can be observed using different software. The captured packet by Middle_man can be seen using Wireshark software. We can see message transferred inside the terminals client.py, server.py by running these files on your command prompt. Nevertheless, we can observe junk caused as middle_man.py is not able to properly decrypt the message.

6. Evaluation

The experimental results obtained by simulation are discussed in the following sections. The analysis has been carried out using Wireshark. These simulations are conducted on an 8 GB RAM, 2.60 GHz Intel Core i5 processor and Microsoft windows 10 OS.

The Man in the Middle Attack Detection script is implemented in python. Wireshark was used to illustrate the communication initiation process between the client and the server. Here TCP handshake occurs and, once the connectivity is formed, the actual data frames begin to flow. Which gives us a good understanding of the flow of packets in the tcp / ip.

6.1 Server client Communication Analysis:

After running the python script named server.py for initiating the key exchange mechanism of this project for further communication between client and server. Where sever is local host and for client another python script using python sockets has been written.

Below screenshot will demonstrate Key exchange and message transmission from the server side to the client

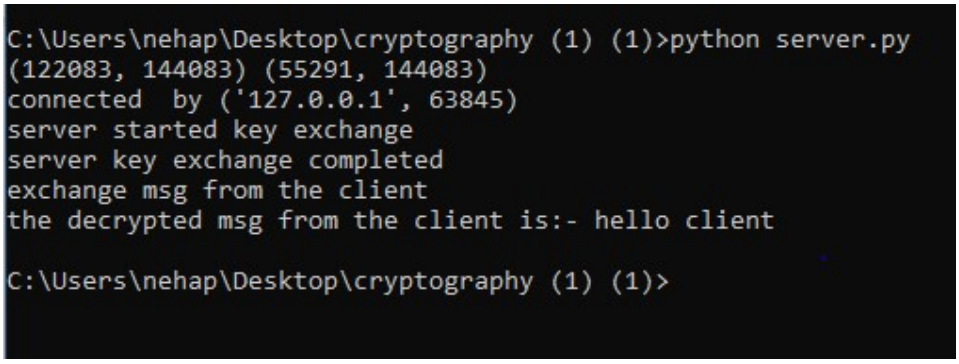

Figure 6: Server Key exchange

Post TCP handshake key exchange will initiate and after authorisation actual message transmission will take place.

Below screenshot demonstrates key exchange and message transmission at client side.

Client

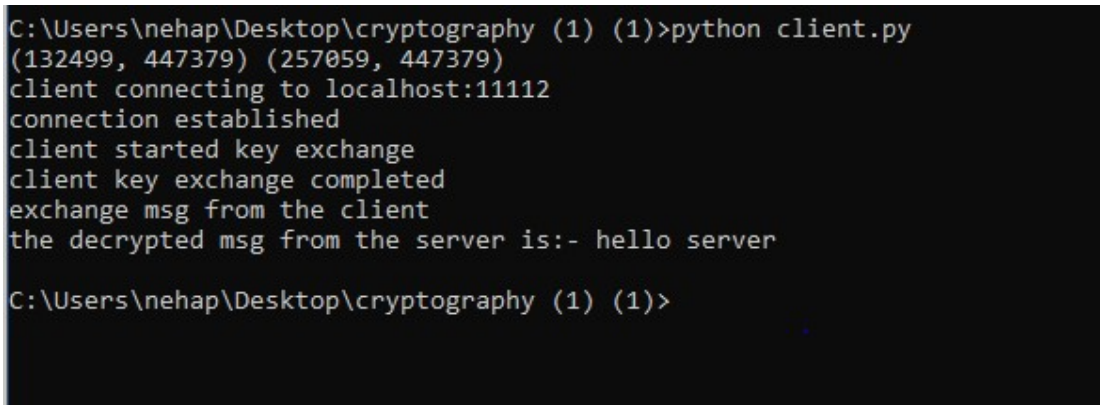

Figure 7: Client Key Exchange

6.2 Man in the Middle Attack Analysis:

Once the exchange initiates between server and client man in the middle will intercept it and will send his key to sever and client for intercepting the communication. However, due to the lack knowledge of the algorithm which has been used in the communication he will not be able to decrypt it. And he will only get the redundant information.

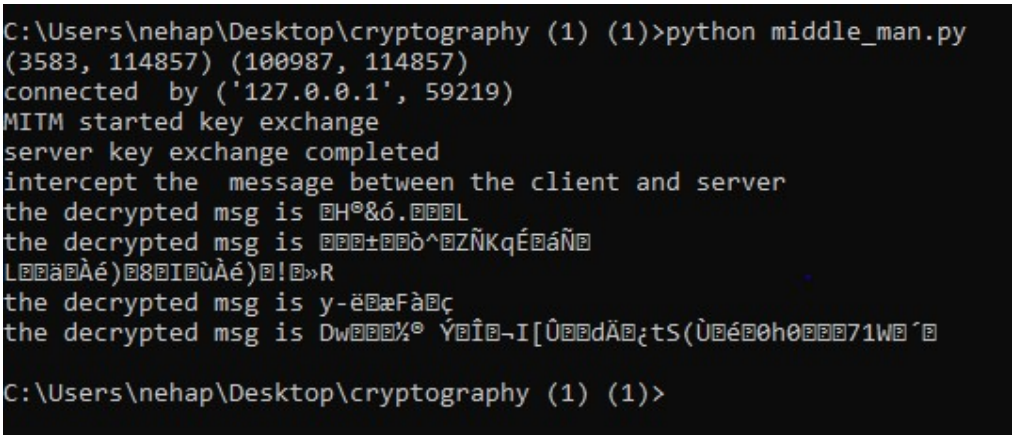

Figure 8: Man in the middle interception

6.3 Discussion

The main objective of this research was to check if the inclusion of HMAC hash function in the interlocking protocol can enhance the security of the communication systems and provide additional shield against the cyber threats. For the scope of this research, experiment has been conducted to effectively mitigate Man-in-the-middle attack on the ongoing communication between two users. It was achieved by splitting the message into two parts using interlocking protocol where HMAC was applied on the second part of the message. In order to do so, two separate python scripts were developed - one was related to applying HMAC hash function on the second part of the message while the other one combines it with the interlocking protocol.

In the first scenario, Public key of the server and client was provided to the attacker through the developed python scripts. After initialization of the communication between client and server, attacker successfully intercepted the communication and established connection with server and client using the provided public keys. This process of interception can be observed in Wireshark which illustrates the three way handshake between client-server, client-attacker, and server-attacker. Once the communication started, attacker eavesdropped the process and intercepted the messages sent between server and client. However, the attacker was unable to decrypt those messages and ended up getting dump on the screen.

In the second scenario, attacker had the knowledge of encryption algorithm used for initial encryption of the message as well as the interlocking protocol which was used to split the message into two parts. Although the attacker was able to successfully intercept the communication, yet he was unable to decrypt the message. The reason being the additional security measures introduced by HMAC. The attacker was totally unaware of the double encryption applied on the second part of the message which was the primary objective of this research. The research showed that implementing crypto system using interlocking protocol and HMAC hash function provided more robustness and security to the network against the 'Man In The Middle Attack' and can be adopted as an additional security measure in the field of TCP/IP communication.

7. Conclusion and Future Work

The goal (Interlocking protocol for detecting and preventing Man in the middle attack using HMAC) has been accomplished by developing a python script to detect presence of preparator between the network who is eavesdropping the ongoing communication process. The solution is able to efficiently detect the presence of Man in the Middle. The developed python script is platform independent so it could be used across various OS. The script can further be customized according to the industrial requirements. The mechanism can be deployed on the perimeter of the company network (firewall) and could obstruct any unauthorized attempt to reach or hamper with sensitive information. Project's outcomes prove that the implementation is successfully able to detect Man in the Middle Attack. This work is done on localhost to secure the communication using tcp/ip, however, the similar approach of project could be further expanded to other communication and network protocols such as DNS, HTTP, and HTTPs and so on. The script has to update constantly the functionality it uses to detect malicious traffic, as the hackers are developing too. The script can be configured as a different entity for any network that interacts with or without a firewall. Nevertheless we can extend the protocol by adding new rules such as random splitting in which message will be split in multiple parts rather than splitting it into 2 parts.

Acknowledgement:

I would like to take this opportunity to thank my supervisor Mr. Vikas Sahni for his throughout support and valuable guidance during this research project. I have benefited from his assistance at several stages in the course of this research project, particularly while implementing new ideas. His optimistic outlook and faith in my work encouraged me and gave me the ability to do so. His diligent editing contributed greatly to the development of this study. However, meetings and discussions were crucial to inspire me to think outside the box, from differing viewpoints, in order to form a comprehensive and accurate critique.

References:

[1] Vikas Kumar et al. *Detection of Stealth Man-In-The-Middle Attack in Wireless LAN* 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing

[2] In-A Song and Young-Seok Lee, "Improvement of Key Exchange protocol to prevent Man-in-the-middle attack in the satellite environment," *2016 Eighth International Conference on Ubiquitous and Future Networks (ICUFN)*, Vienna, 2016, pp. 408-413.

[3] Benjamin Aziz and Geoff Hamilton. Detecting man-in-the-middle attacks by precise timing The Third International Conference on Emerging Security Information, Systems and Technologies, SECURWARE 2009, 18-23 June 2009, Athens/Glyfada, Greece.

[4] Visa Villivaara et al. Detecting Man-in-the-Middle Attacks on Non-Mobile Systems ACM Conference on Data and Application Security and Privacy, 2014 At San Antonio, Texas, Volume: 4th

[5] Cyber Defense Lab Animation of Chaum's protocol for detecting a man-in-the-middle

[6] Jeffery L. Crume Detecting and defending against man in the middle attacks United States patent. Patent no. 8, 533, 821, B2. International business machines Corporation, Armonk NY(US)

[7] Y. Mirsky, N. Kalbo, Y. Elovici, and A. Shabtai, “Vesper: Using Echo-Analysis to Detect Man-in-the-Middle Attacks in LANs,” arXiv:1803.02560 [cs], Mar. 2018 [Online]. Available: http://arxiv.org/abs/1803.02560. [Accessed: 06-Apr-2020]

[8] E. de la Hoz, G. Cochrane, J. M. Moreira-Lemus, R. Paez-Reyes, I. Marsa-Maestre and B. Alarcos, "Detecting and defeating advanced man-in-the-middle attacks against TLS," 2014 6th International Conference On Cyber Conflict (CyCon 2014), Tallinn, 2014, pp. 209-221.

[9] Folarin Samuel, 2019 Improved SSL/TLS man-in-the-middle attack detection technique using timing analysis and behavioral anomalies Research in Computing, National College of Ireland

[10] Jeffery L. Crume Detecting and defending against man in the middle attacks United States patent. Patent no. 8, 533, 821, B2. International business machines Corporation, Armonk NY(US)

[11] John R.; Bennett, Forrest H.; Andre, David; Keane, Martin A. Automated Design of Both the Topology and Sizing of Analog Electrical Circuits Using Genetic Programming. Artificial Intelligence in Design '96. Springer, Dordrecht. pp. 151–170. doi:10.1007/978-94-009-0279-4_9

[12] Rahim, Robbi. (2017). Man-in-the-middle-attack prevention using interlock protocol method. Journal of Engineering and Applied Sciences. 12. 6483-6487.

[13] “A method for detecting man-in-the-middle attacks using time synchronization one-time password in interlock protocol based internet of things,” Journal of Applied and Physical Sciences, vol. 2, no. 2 [Online]. Available: https://www.academia.edu/34914658/A_method_for_detecting_man-in-the-middle_attacks_using_time_synchronization_one_time_password_in_interlock_protocol_based_

[14] Efficient HMAC Based Message Authentication System for Mobile Environment, Kavitha Boppudi,Sathish Vuyyala, International Journal Of Advanced Engineering Sciences And Technologies Vol No. 11, Issue No. 1, 208 – 212.

[15] Kiran, S.K.V.V.N.L.; Harini, N. Evaluating Efficiency of HMAC and Digital Signatures to Enhance Security in IoT. Int. J. Pure Pllied Math. 2018, 119, 13991–13997.

[16] Bishop, C.M Pattern Recognition and Machine Learning, Springer, ISBN 978-0-387-31073

[17] Brian Hernacki and William E. Sobel Detecting man in the middle attacks via security transitions United States patent. Patent no. 8,561,181, B1. Symantec Corporation, Cupertino CA(US)

[18] Alan Johnston, Avaya, Inc., Washington University in St. Louis- January 20, 2014 "Detecting Man in the Middle Attacks on Ephemeral Diffie-Hellman without Relying on a Public Key Infrastructure in Real-Time Communications"

[19] Najjar, Mohannad. (2015). d-HMAC — An improved HMAC algorithm. IJCSIS international journal of computer science and information Security. 13.

[20] V. R. Kulkarni, S. Kalmani, and S. Vernekar, "Secured Hash2 based Message Authentication Code using GUI Controls," 2013, doi: 10.5120/13269-0772.

[21] J. Kim, A. Biryukov, B. Preneel, and S. Hong, "On the Security of HMAC and NMAC Based on HAVAL, MD4, MD5, SHA-0 and SHA-1 (Extended Abstract)," in Security and Cryptography for Networks, Berlin, Heidelberg, 2006, pp. 242–256, doi: 10.1007/11832072_17.

[22] E. Khan, M. W. El-Kharashi, F. Gebali and M. Abd-El-Barr, "Design and Performance Analysis of a Unified, Reconfigurable HMAC-Hash Unit," in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 54, no. 12, pp. 2683-2695, Dec. 2007, doi: 10.1109/TCSI.2007.910539.

[23] H. A. Al Hamid, S. M. M. Rahman, M. S. Hossain, A. Almogren, and A. Alamri, "A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility With Pairing-Based Cryptography," IEEE Access, vol. 5, pp. 22313–22328, 2017, doi: 10.1109/ACCESS.2017.2757844.

[24] G. Nath Nayak and S. Ghosh Samaddar, "Different flavours of Man-In-The-Middle attack, consequences and feasible solutions," 2010 3rd International Conference on Computer Science and Information Technology, Chengdu, 2010, pp. 491-495, doi: 10.1109/ICCSIT.2010.5563900.

[25] H. E. Michail, A. P. Kakarountas, A. Milidonis and C. E. Goutis, "Efficient implementation of the keyed-hash message authentication code (HMAC) using the SHA-1 hash function," Proceedings of the 2004 11th IEEE International Conference on Electronics, Circuits and Systems, 2004. ICECS 2004., Tel Aviv, Israel, 2004, pp. 567-570, doi: 10.1109/ICECS.2004.1399744.

[26] E. S. I. Harba, "Secure Data Encryption Through a Combination of AES, RSA and HMAC," Engineering, Technology & Applied Science Research, vol. 7, no. 4, pp. 1781–1785, Aug. 2017.