PREVENTING MAN IN THE MIDDLE (MITM) ATTACK FOR SECURING NETWORK

BY

MD. MANIRUL ISLAM

ID: 152-15-6135

MD. JANNATUL NAYEM

ID: 152-15-5621

MD. REZWAN MONDOL

ID: 152-15-5751

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Computer Science and Engineering

Supervised By

DR. FERNAZ NARIN NUR

Assistant Professor

Department of CSE

Daffodil International University

Co-Supervised By

MS. NAZMUN NESSA MOON

Assistant Professor

Department of CSE

Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY
DHAKA, BANGLADESH

APRIL 2019

APPROVAL

This Project titled **"Preventing Man in the Middle (MiTM) attack for securing IoT Network"**, submitted by **Md. Manirul Islam**, ID No: **152-15-6135**, **Md. Jannatul Nayem**, ID No: **152-15-5621** and **Md. Rezwan Mondol**, ID No: **152-15-5751** to the Department of Computer Science and Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on 2nd May, 2019.

BOARD OF EXAMINERS

Dr. Syed Akhter Hossain
Professor and Head — **Chairman**
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Md. Tarek Habib
Assistant Professor — **Internal Examiner**
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Moushumi Zaman Bonny
Senior Lecturer — **Internal Examiner**
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Dr. Swakkhar Shatabda
Associate Professor — **External Examiner**
Department of Computer Science and Engineering
United International University

DECLARATION

We hereby declare that, this project has been done by us under the supervision of **DR. FERNAZ NARIN NUR, Assistant Professor, Department of CSE** Daffodil International University. We also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

Supervised by:

Fernaz

DR FERNAZ NARIN NUR
Assistant Professor
Department of CSE
Daffodil International University

Co-Supervised by:

MS. NAZMUN NESSA MOON
Assistant Professor
Department of CSE
Daffodil International University

Submitted by:

MD. MANIRUL ISLAM
ID: 152-15-6135
Department of CSE

Nayem

MD. JANNATUL NAYEM
ID: 152-15-5621
Department of CSE

MD. REZWAN MONDOL
ID: 152-15-5751
Department of CSE

ACKNOWLEDGEMENTS

First we express our heartiest thanks and gratefulness to almighty God for His divine blessing makes us possible to complete the final year project/internship successfully.

We would like to special delivery my sincere gratitude to my advisors **DR. FERNAZ NARIN NUR, Assistant Professor**, Department of CSE Daffodil International University, Dhaka. Deep Knowledge & keen interest of our supervisor in the field of "*Internet of Things*" to carry out this project for her patience, motivation, and understanding. The guidance that have been provided to us helped us in all the time of research and writing of this thesis.

We would also like express our gratitude to the study board because they gave us the opportunity to finish our Thesis granting our extra time. After a very difficult period for us, their decision allowed us to complete our Thesis. Without their understanding we would not be able to complete it.

Last but not the least, we would like to thank our family for supporting and encouraging us throughout writing this thesis.

ABSTRACT

At present wireless network trends to be more and more popular among the population with the millions of users. The Man-In-The-Middle (MITM) attack is one of the most well-known attacks in computer security, representing one of the biggest concerns for security professionals. MITM targets the actual data that flows between endpoints, and the confidentiality and integrity of the data itself. MITM has been one kind of attack where a user gets between the sender and the receiver information. In this report we try to explain different types of MITM attacks. Man in the Middle (MITM) attack is one of the primary techniques in computer base hacking. In this types of attack where the attackers can collect many important data, inject false information, user lost their different types of online user ID and password. For this, we try to discover how this types of attack works, describe a method of man-in-the-middle attack based on ARP spoofing and try to create a method of preventing suck attack.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Man-In-The-Middle (MITM) attack occurs when communication between two user by an outside entity. It can happen in any kind of online communication sites, email, social media web browsing, transection of banking etc. The main target of the attacker to steal personal information, gain login information, account details, credit card number. MITM known as different types:

- Bucket-brigade attack
- Fire brigade attack
- Monkey-in-the-middle attack
- Session hijacking
- TCP hijacking

1.2 Motivation

Now-a-days the Man in the Middle Attack has been spread alarmingly. This attack creates miscommunication between people who wants to communicate with each other. Because in this attack, attacker can makes independent connection with the victims & whole conversation is controlled by the attacker. It is a great privacy issue for our society because we lost our personal information from this attack. So, we want to stop it as soon as possible. That's why we get motivated & choose this project

1.3 Objectives

- What are the causes of attack.
- Who are the victims of more attack.
- Find out the percentage of Victims in Bangladesh.
- What age's people are in the target of attack.
- Identify design and implement a suitable method of prevent data from MITM attack in Bangladesh perspective.
- How it effect of economic growth of Bangladesh.

1.4 Expected Outcome

i. 95% of HTTPS server are vulnerable & it creates a space for the attacker to attack.

ii. There are six ways a man can become a victim of man in the middle attack

a) Wi-Fi Eavesdropping

b) Man-in-the-Browser

c) Man-in-the-Mobile

d) Man-in-the-App

e) Man-in-the-Cloud

f) Man-in-the-IoT

iii. 64% of the selected web applications in Bangladesh are running with the vulnerabilities and specifically, government websites are in a critical state.

iv. In Bangladesh, 340 web applications out of 600 are vulnerable to various query splitting techniques of GET-based SQL injection and 60 web applications vulnerable to post based SQL injection attacks.

v. Young generation are the main target of MITM attack. On those attack we found 14% victim are at the age of under 20, 58% victim are at the age between 21-25, 20% victim are at the age between 26-40, 3% victim are at the age between 41-49, 5% victim are 50 years old or more.

vi. MITM attacks effects of economic growth in Bangladesh very badly. People are losing their important data by the MITM attack. It causes great economic hamper in our society.

vii. In Bangladesh's perspective ARP spoofing method is suitable to prevent data from MITM attack in Bangladesh.

1.5 Report Layout

This report consists of five chapters, and this section provides insight of all five chapters.

Chapter one provides introduction, motivation, objectives, expected outcome and report layout of the study. Chapter two provides background of research work and discussion. It also provides problem scopes and challenges of the research. In chapter three, we describe research subject and instrumentation discussion. Chapter four of this document describe our project experimental results and discussion. Lastly, chapter five is on conclusion, recommendation and implication for future study.

CHAPTER 2

BACKGROUND

2.1 Introduction

2.1.1 Wi-Fi and Ethernet

Nowadays Wi-Fi and Ethernet are the more used types of the networking. They are also share some common characteristics with one another. Ethernet became a standard known as IEEE 802.3 in 1985 and it provides services to the physical layer as well as the data link layer. The data transfer rates of the Ethernet standard is from 10 Mbps to 100 Gbps. The data transfer rates depends on the protocol that is being used [1].

2.1.2 The Hacker

Hacker is a person who find weakness of people by the using of computer systems. A hacker who has any skilled computer expert that uses computer, networking or other skill to overcome a technical problem. Their steal the information of people by the using different types of attacking tools [2].

2.1.3 The Victim

Victim are the persons who are facing many problem by the hacker. When their build their communication with others, hackers are trying steal their information for their revenges, blackmails and causes of personal business. In our figure 2.1 Alice and Bob build their communication and share their information and data. On the others side Eve is a hacker. He is trying to hack their sever and collect their information. But Alice and Bob are don't know about Eve. In this way hacker are steal their information but people are don't know about this [3].

Here Alice and Bob are make a conversation and Ave create man in the middle attack between Alice and Bob.

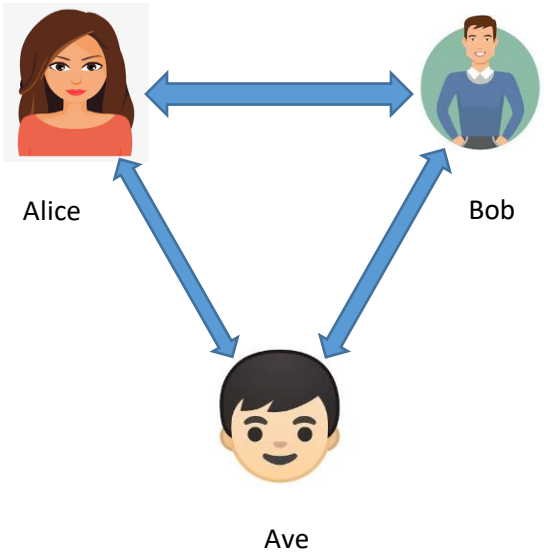

Figure 2.1: Sessions hijacking from victim

2.2 Related Works: Types of Man-In-The-Middle attacks:

2.2.1 Rogue Access Point

When the user use the devices, the device can be equipped with wireless cards & the user can try to auto connect the access point that is throw down the potential signal. At the same time the attacker can set up their own wireless access point and ruse the nearby devices to join their domain. For this all the victims network control by the attackers. This is dangerous, because the attacker can see the information of victims [4].

2.2.2 Sniffing Attack

By the Sniffing attack the attacker can intercepting of data by capturing the network traffic using a sniffer. When data is transmitted across networks if the data packets are not encrypted the attacker can easily read the data. By the application of sniffer an attacker can explore the network and gain information. That can eventually cause the network to crash or to become corrupted and also read the communication of the users. In figure 2.2 using the sniffer tools the sniffer can steal

the sensitive information from the network like E-mail traffic (SMTP, POP and IMAP traffic), FTP traffic (FTP Password, SMB, NFS), Web traffics (POP, IMAP and HTTP) etc [5].

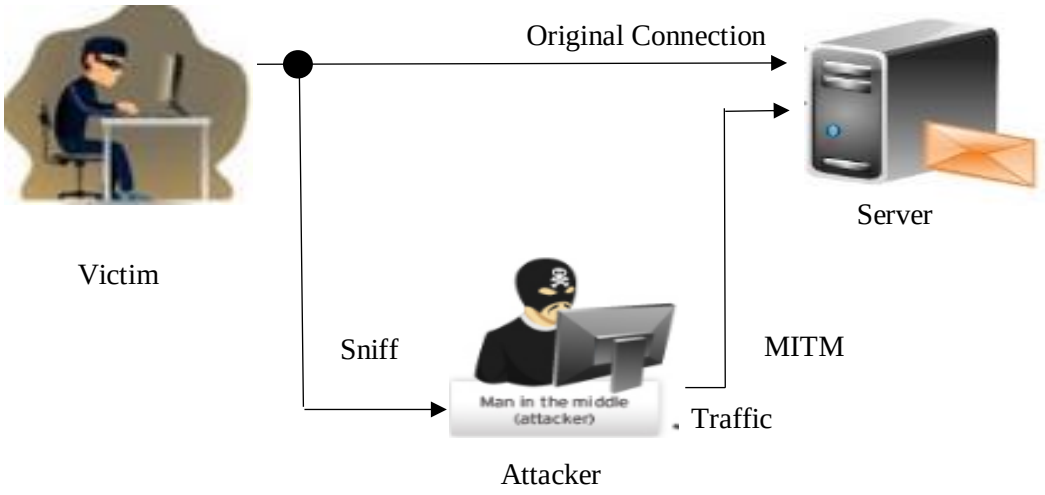

Figure 2.2: Sniffing data by MITM

2.2.3 Denial-of-Service (DOS Attack)

A denial of service attack is a one kind of cyber-attack in which can make a machine unavailable or down to work or processes anything by affected with DoS attack

The main target is high level profile for getting down and down any kind of website by this method [6].

2.2.4 Spoofing Attack

An attacker can spoof data from victim computer. When the user use their device to communication with others the attacker attack the same time to collect their data by the using of spoofing tools. There are some common types of attack usually known as ARP spoofing, IP address spoofing and DNS spoofing. With the help of packet sniffer we can able to watch, we can display it & we can log the traffic & this information can be accessed by the attacker [7].

2.3 Research Summary

For this research purpose we asked random internet user about some questions and getting results is given bellow:

Most of the user are student than job holder, no work and businessman [8]. The figure 2.3 show that 68.6% are students, 13.7% job holder, 9.8% have no work currently and 7.9% user are businessman.

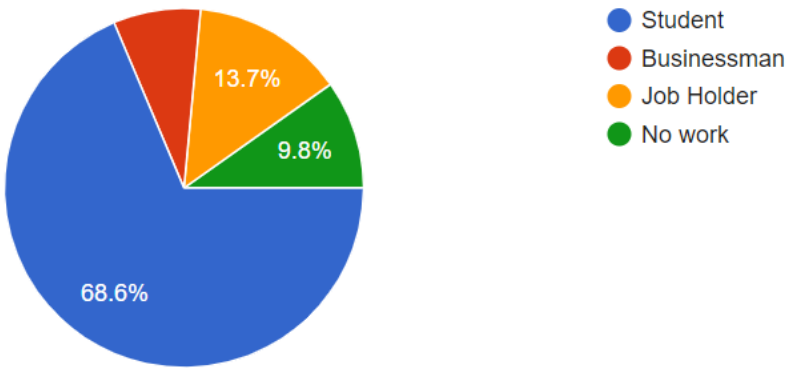

Figure 2.3: Percentage of internet user's categories

Where figure 2.4 represents 80% internet user's uses internet regular basis and only about 20% are non-regular.

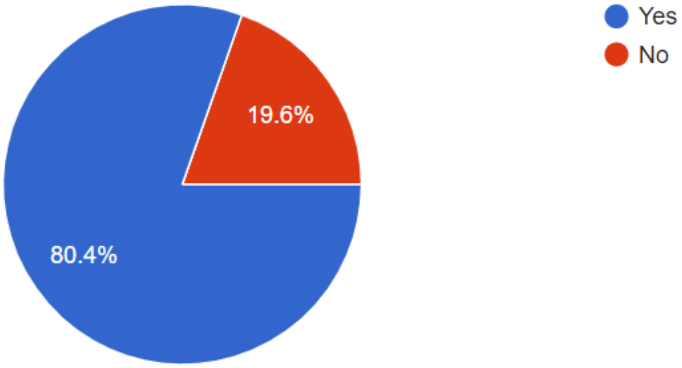

Figure 2.4: Percentage of regular internet users

The figure 2.5 are 53% users known about Internet of Things (IoT) and most of them are student only hear IoT.

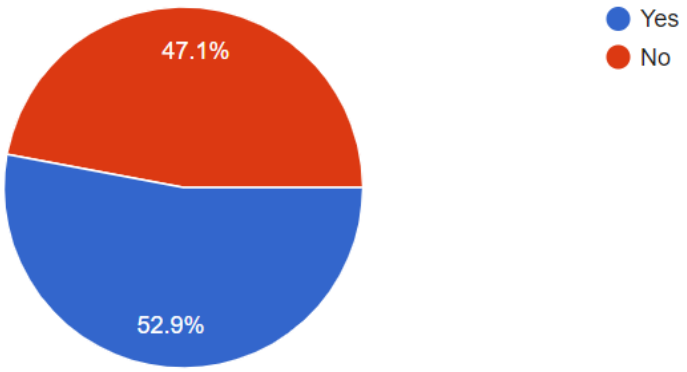

Figure 2.5: Know about IoT

In figure 2.6 37% users think internet is safe, 35% are not safe and 27% are thinking they are may be safe.

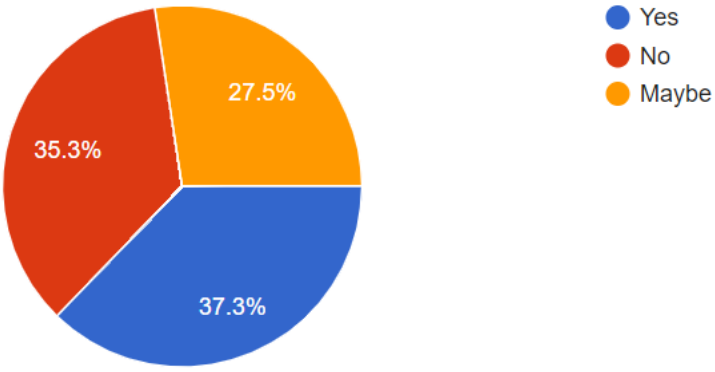

Figure 2.6: Percentage of internet safety

But in figure 2.7 about 60% users think they are not safe in internet browsing and 40% are think internet browsing is safe.

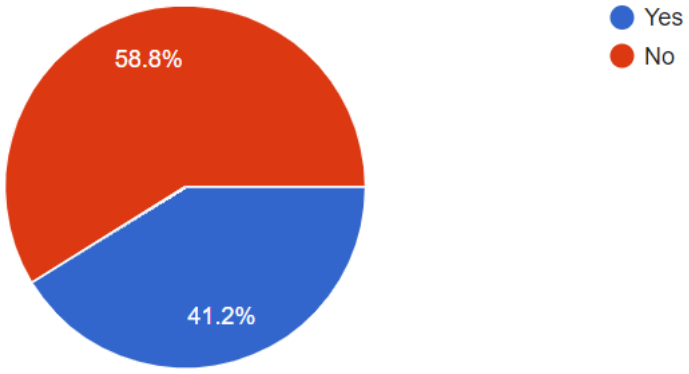

Figure 2.7: Users opinion about internet safety

After getting answer from all users of internet in figure 2.8 whose are answer our couple of questions, from them 60% users don't know about man in the middle attack and rest of 40% users are mix up from student, job holder, businessman and no work categories user.

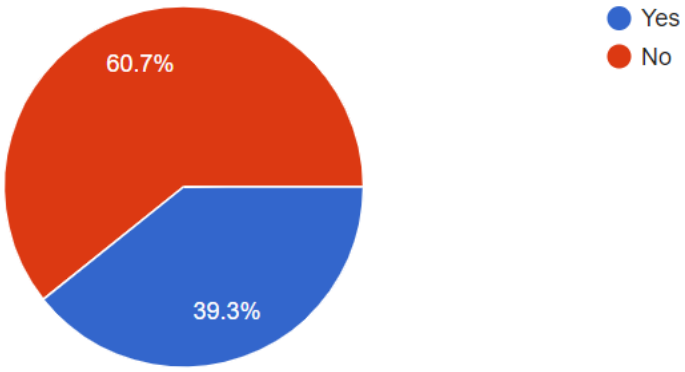

Figure 2.8: Internet users know about MITM

2.4 Scope of the Problem

In the era of business with e-commerce on its summit, we found that more sensitive information is being passed on computer network. We found that, financial & identity information are become very higher risk because user take advantage to modify it & doing business online with the help of web application. We also found that, sensitive user information is constantly transported between sessions after authentication & hackers are setting their best efforts to steal or modify them.

We face a variety of serious threats and risks in computer network. These threats are based on weakness co-operated with the ARP. When computer X tries to communicate with Y, ARP sends out a broadcast to the network devices asking 'who is Y? But there is no authentication built into ARP and thus ARP has no way of fixing whether the response is it really Y or not. By exploiting this lack of authentication, a malicious computer can ask ARP it is computer Y, after which ARP will begin controlling future requests for computer Y to the malicious computer.

The final result is the outpouring of data which can be an act of economic terrorism, exchange of data such as grade fixing and denial-of-service (DoS) attacks including Synchronization (SYN) floods & smurfing.

2.5 Challenges

Penetration testing in GNS3 simulator and Virtual machine is very difficult with low configuration computer because of we need at least two computer with different operating system. At a time running more than one virtual device made computer slow, facing lagging and sometimes computer in stuck.

After discuss with our supervisor, we decide to work with physical device and used two laptop computers and one Wi-Fi router.

CHAPTER 3
RESEARCH METHODOLOGY

3.1 Introduction

In our research we are try to detect MITM by the use of computer program use of Linux.. We collect articles & studying it & found an effect detection protocol which can detect MITM. Based on our study outcome, we found that software will be automatically designed to imitate the protocol. Finally a simulation will be directed to verify the effectiveness of the strategy. We will create a method which can prevent MITM.

3.2 Research Subject and Instrumentation

Research about spoofing Attack and instrumentation.

3.2.1 ARP Spoofing Attack

ARP means The Address Resolution Protocol. It's used to translate IP addressing Media Access Control (MAC) address in order to be properly transmitted. A physical machine address mean it has a protocol maps an IP address. In this types of attack, the malicious attackers links the hacker's MAC address with the IP address of a company's network. Attacker can see the data in the computer of the company. Main causes of ARP spoofing attack are compromised accounts, data steal and deletion and others. ARP also use for DoS, hijacking and different types of attack.

3.2.2 DNS Spoofing Attack

DNS poisoning is another types of MITM attack. DNS means The Domain Name System. It responsible for associating domain names to the correct IP address. When a user type the domain name for connect the server the DNS system corresponds that name to an IP address and allowing the visitor to the connect server. When a malicious attacker reroutes the DNS translation so that it points to a different server which is typically infected with malware and can be used to help spread viruses and worms, then then a DNS spoofing attack to be successful.

3.2.3 IP Spoofing Attack

The most generally-used spoofing attack is the IP spoofing attack. When a malicious attacker copies a legal IP address in order to send out IP packets using a trusted IP address then its successful. Repeating the IP address forces system to believe the source is reliable opening any exploited people up to various sorts of attacks using the "trusted" IP packets. The popular types of IP spoofing attack is a Denial of service attack, which over power and shut down the focused on server. The ability to perform DoS attacks the attackers can achieve the using of IP spoofing attack. In the event that such a large number of data packets reach the server, the server will be unable to handle all of the requests, causing the server to overload. If trust relationships are being used on a server, IP spoofing can be used to bypass authentication methods that depend on IP address confirmation.

The figure 3.1 shows that, victim browse a website and an attacker spoofing the victim ip address.

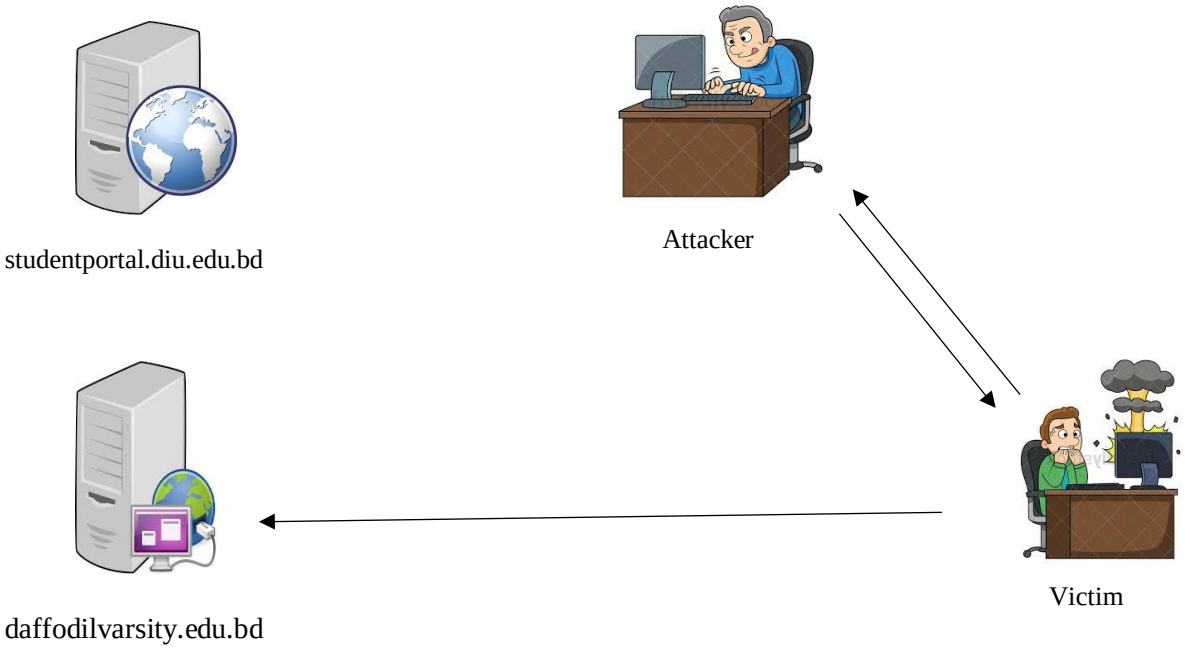

Figure 3.1: IP spoofing

3.2.4 Instrumentation

We need at least two computer and a wifi router with internet connection. One of two computers must have Linux based operating system for performing MITM. Another one is windows operating system. Also need some website for testing and we use here http://studentportal.diu.edu.bd/ and https://daffodilvarsity.edu.bd/

Our operation was operated by Linux terminal and Ettercap tools for getting host information and implementation MITM.

CHAPTER 4

EXPERIMENTAL RESULTS AND DISCUSSION

4.1 Introduction

Man in the middle attack is a one kind of silent attack, It's very difficult to detect that MITM occurring in your device. Basically it occurs in low security web portal which has only HTTP. Without web portal security, very easy to access data by MITM. Attacker can spoofing the packet from your computer and also can sniff URLs information with driftnet images.

4.2 Experimental Results

We experiment with physical devices in figure 4.1 which are connected by wifi network. Operation was done by Linux based computer and victims are using android device and other one is windows user. Attack in both operating system was successful. We sniff the data from them. In the mean time we get the image of their browsing sites as well as URLs.

We include here some of our experiment, how the attacker getting information by MITM.

Figure 4.1: Physical Devices

4.2.1 Experiment with a Windows / Android user

We are going to MITM an android user who is connected with our wifi network. Already we know the default gateway of victim mobile as he/she use our wifi network and we also know the local ip address of victim.

4.2.1.1 IP forward

By our Linux operating machine, in figure 4.2 we forward the ipv4 IP using command on figure that act our machine as a router.

sysctl –w net.ipv4.ip_forward=1

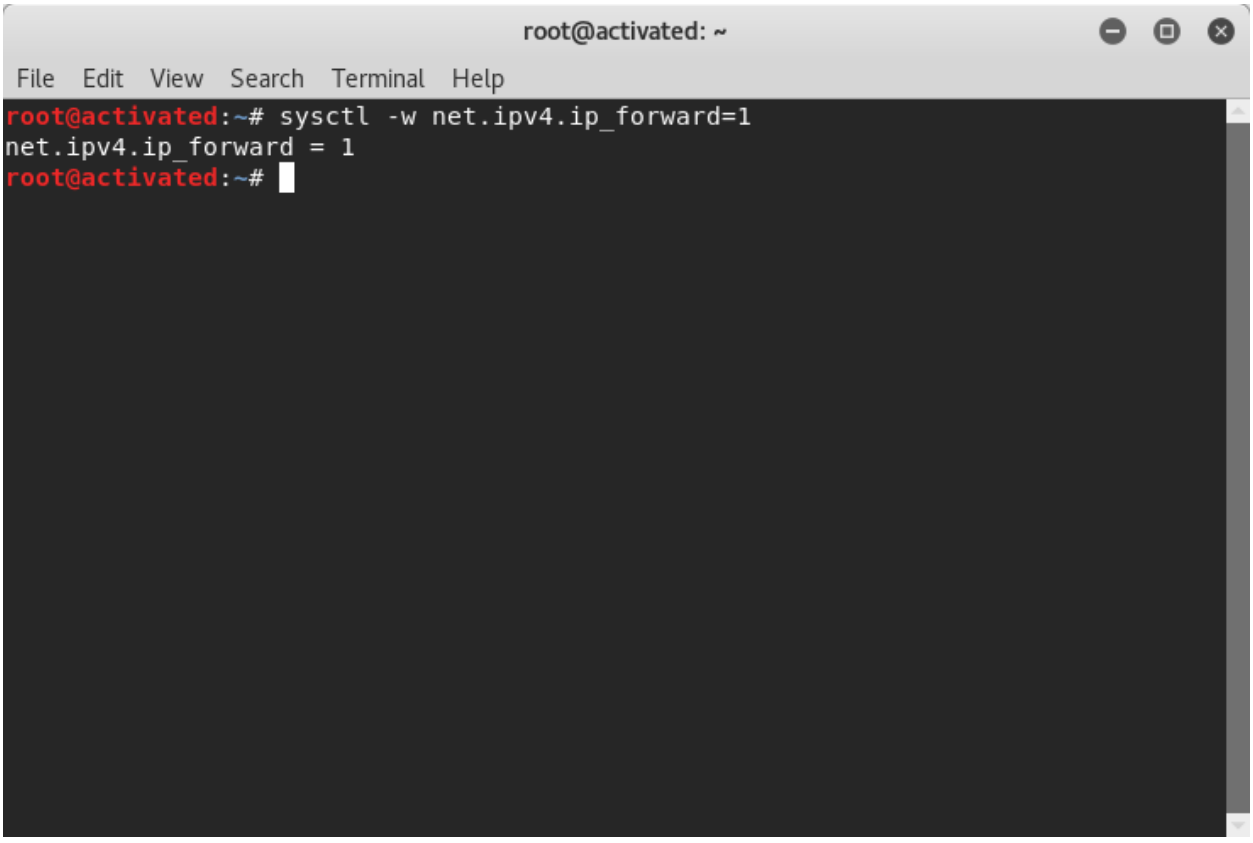

Figure 4.2: IP forwarding

4.2.1.2 Intercept packages from Victim with arpspoof

Intercepting packets from a target host on the network switched has possible by arpspoofing. ARPSPOOF is the effective way to sniffing traffic on a switch. Command like as;

arpspoof –i [network int name] –t [victim ip] [router ip]

Run this command in a new terminal like figure 4.3 and don't close before stop the man in the middle attack.

This process monitor the packet flow between Victim and Router.

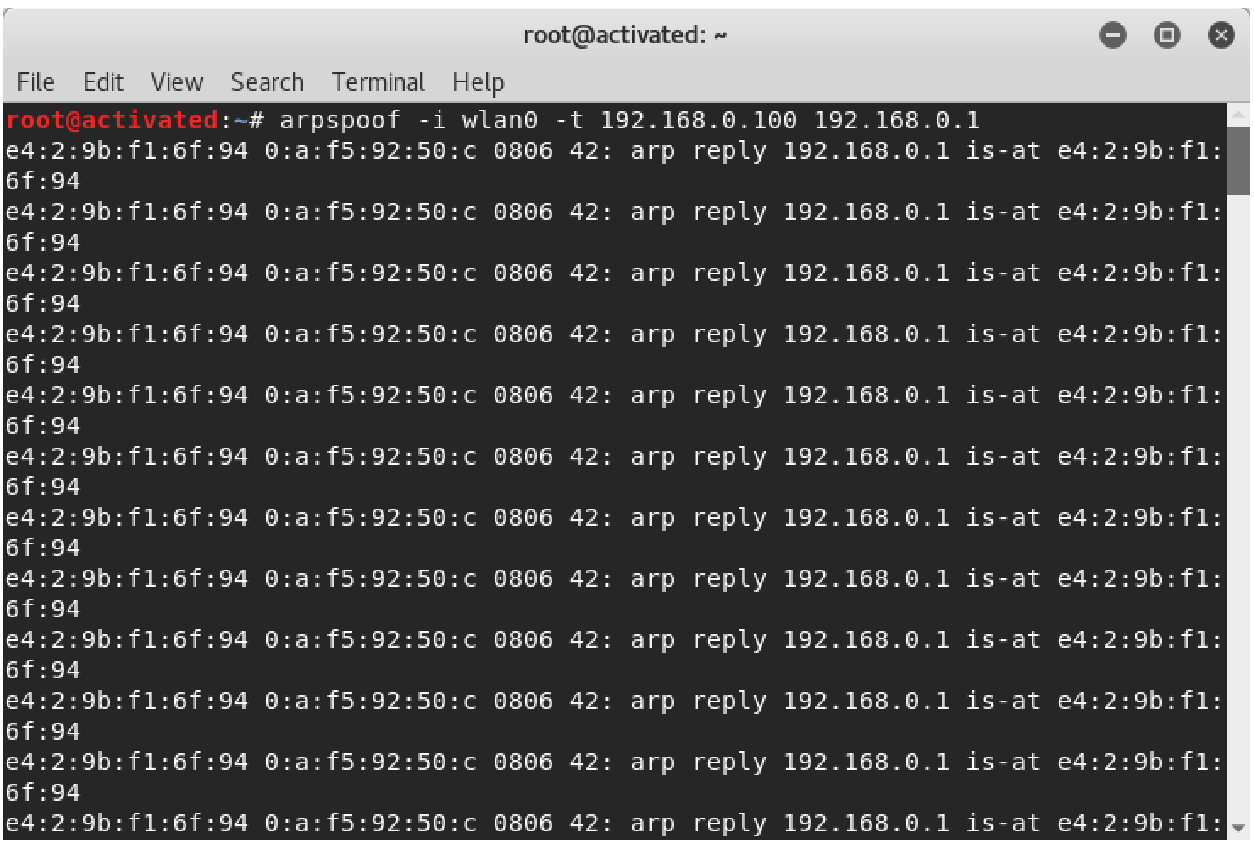

Figure 4.3: Intercept packages from victim with arpspoof

4.2.1.3 Intercept packets from router with arpspoof

Now intercepting packets from victim to router with new terminal looks figure 4.4 and command structure following:

arpspoof –i [Network Int Name] –t [Router IP] [Victim IP]

This command is same like 4.2.1.2 and it also don't close until the attack is stop.

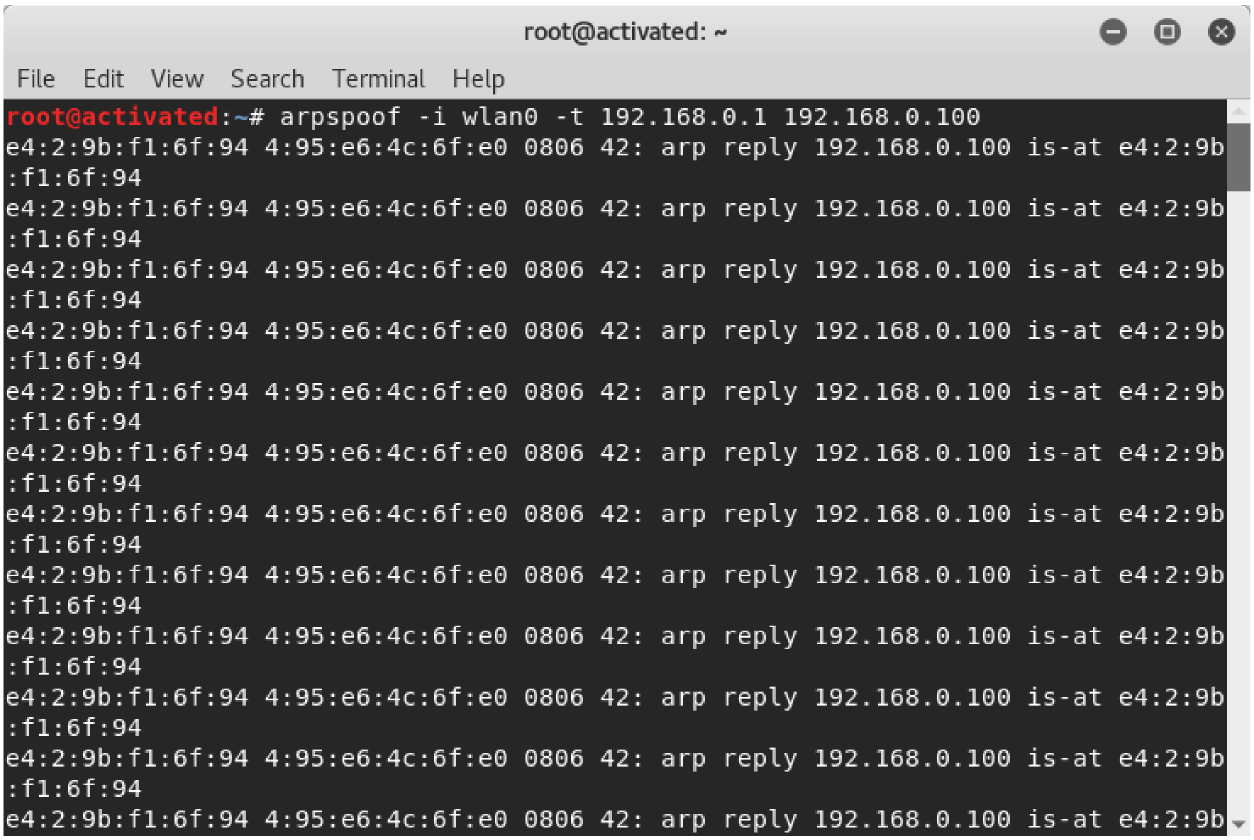

Figure 4.4: Intercept packages from router with arpspoof

4.2.1.4 Sniff images from victim navigation

Sniff image in figure 4.5 is the process for see the victim websites image. To see the image from victim browsing website we use driftnet program. This program can listen to network traffic and pics out images from TCP streams.

Structure of command line as bellow:

driftnet –i wlan0

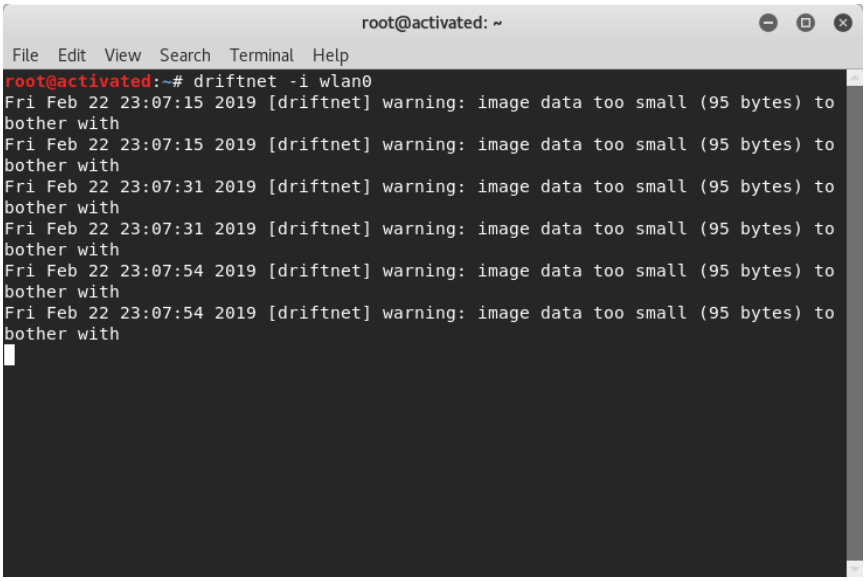

Figure 4.5: Driftnet command

Figure 4.6 shows snif image from victim browse site.

Figure 4.6: Driftnet output display terminal

4.2.1.5 Sniff URLs information from victim navigation

We use urlsnarf for getting the websites list that our victim visits. Urlsnarf sniffs all HTTP request in common log format as a output.

The structure of urlsnarf command like as;

urlsnarf –i [Network int Name]

After command in terminal we get the output with HTTP link. Once our victim visits the sites and we see like figure 4.7.

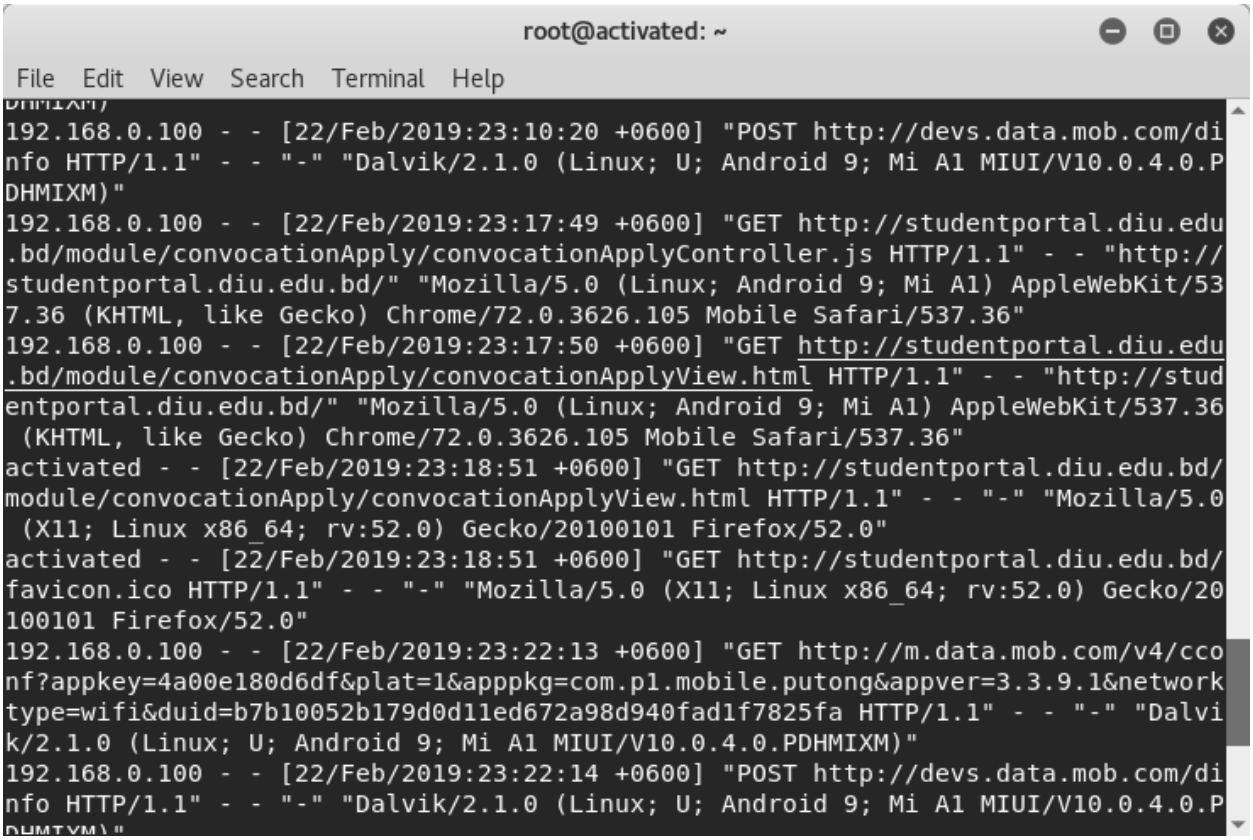

Figure 4.7: Sniffing ULRs from victim activity

While complete all process and getting information from our attacker close all terminal by press CTRL+C on every terminal.

4.2.1.6 Disable packet forward (while our attack has finished)

Completing all actions we need to disable packet forwarding again with this command on a new terminal.

```
sysctl –w net.ipv4.ip_forward=0
```

4.3 Descriptive Analysis

Generally a website build their communication using layer system. Most of the website has no extra secure layer like as Secure Socket Layer and Transport Layer Security. MITM attack can create a fake communication between user and server, finally attacker get the information from user.

Now a days all of user of internet is aware about losing their information. Because one of their information can hamper their life or more can be happen. Sometimes attacker can access information even there is SSL/TLS protocol on that system.

4.4 Summary

We analysis our own experience and other random users. All of them are don't know about MITM. But they are very close with internet day by day. Even their children are using internet now a days. So, its time to think about it and we tell them how to be protect from MITM.

CHAPTER 5

SUMMARY, CONCLUSIONS, RECOMMENDATIONS AND IMPLICATIONS FOR FUTURE RESEARCH

5.1 Summary of the Study

In this study we know that most of internet user don't know how their data sniff by hacker. We want to inform them to know about MITM and also ware how to be safe on internet. Internet is a vast aria, every day we engaged with one another by using internet. Visits lots of website and sharing our own information. We have to be very careful for sharing data in a website.

5.2 Conclusions

Currently we all are stay in modern era connected with internet. Anyone can steal our information any time. The attacker can use our information any kind of illegal purpose that is very dangerous for us.

So, we have to ensure secure internet browsing and also safe browsing for children.

5.3 Recommendations

For securing Internet of things for MITM, Users have to be very careful to share their information within a website. Must be ignore non-secure web portal.

They can use some tools for create security themselves, instructions are given bellow;

5.3.1 Virtual private network

VPN (Virtual private network) in figure 5.1 extend internet connection within public internet network with encrypted layered tunneling protocol for receive and send data.

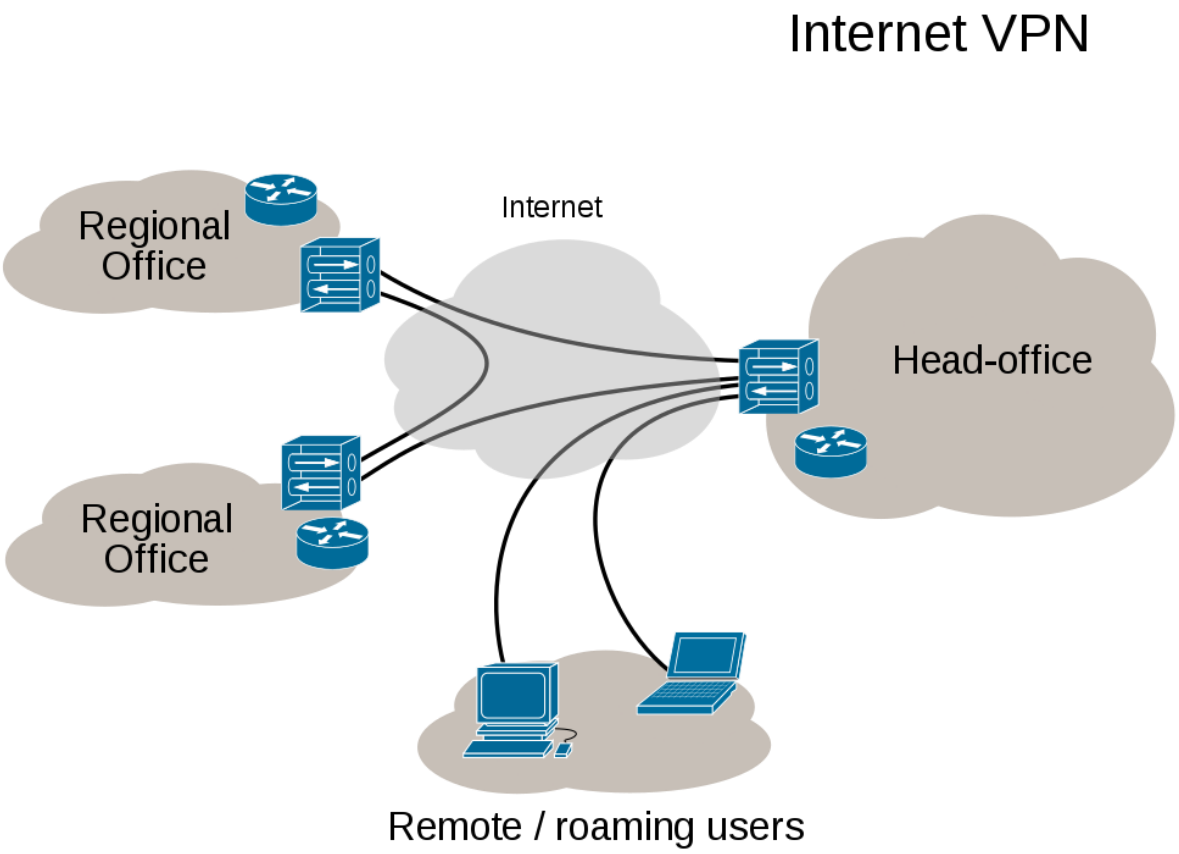

Figure 5.1: VPN (Virtual Private Network)

VPN setup

First install our exe file in your computer and run this software and you will see like bellow:

This window show the interface like figure 5.2 of our VPN software. Here we have to provide protocol type, user name, server address and password for connect VPN service.

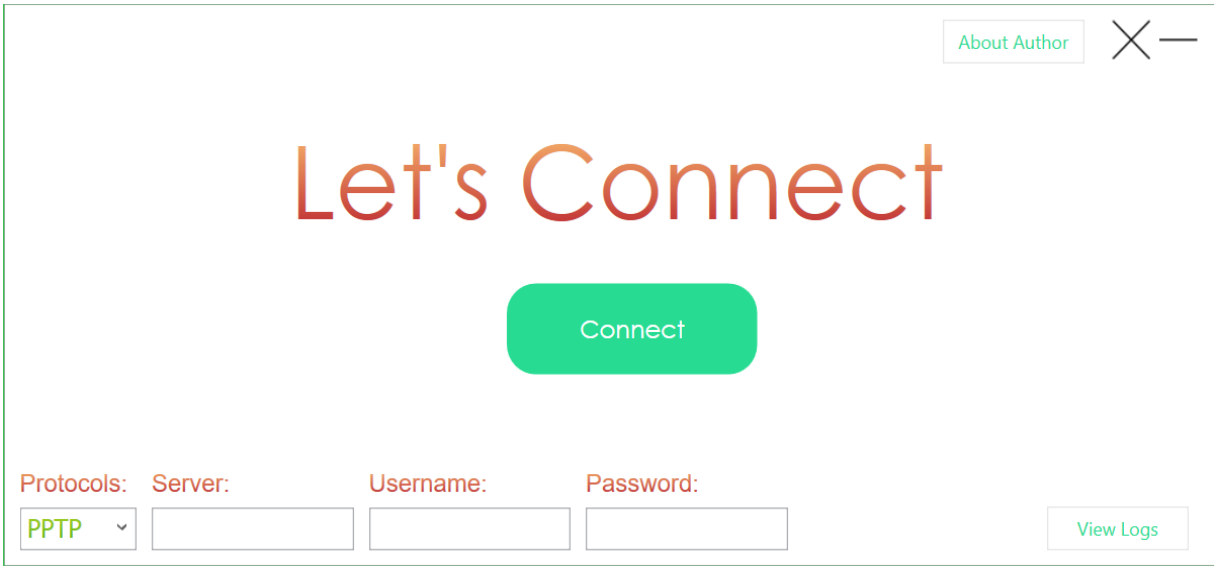

Figure 5.2: VPN software interface

5.3.2 Force HTTPS

Hypertext Transfer Protocol Secure is provide an extra layer of security on web based data transmissions. HTTPS encrypt data between user and server with this type protocol.

5.3.3 Public key pair based authentication

Public key pair is like as RSA based authentication that depend on different layers for communicating actually where we want to communicate and MITM trying to sniffing or somethings else.

5.4 Implication for Further Study

Preventing MITM and securing internet of things is now a days is very important. We have to be aware using internet. MITM is very easy and common method to exploit user data. Even user can't get any notification if they are under attack.

Reference

[1] Learn about Wireless Network, available at << https://en.wikipedia.org/wiki/Wireless_LAN >>, last accessed on 09-01-2019 at 11:00am

[2] Learn about Hacker, available at << https://en.wikipedia.org/wiki/The_Hacker >>, last accessed on 21-01-2019 at 7:00pm.

[3] Learn more about Session Hijacking, available at << https://www.sciencedirect.com/topics/computer-science/session-hijacking >>, last accessed on 01-02-2019 at 9:00pm.

[4] Details about Rouge access point, available at << https://en.wikipedia.org/wiki/Rogue_access_point >>, last accessed on 19-02-2019 at 5:00pm.

[5] Learn about more Sniffing attack, available at << https://en.wikipedia.org/wiki/Sniffing_attack >>, Last accessed on 03-03-2019 at 9:00pm.

[6] About the attack of Denial-of-service attack, available at << https://en.wikipedia.org/wiki/Denial-Of-service attack >>, last accessed on 03-03-2019 at 10:30pm.

[7] Learn about spoofing attack, available at << https://www.forcepoint.com/cyber-edu/spoofing >>, Last accessed on 13-03-2019 at 8:00pm.

[8] Survey form of IoT, available at << https://moniruldipu.blogspot.com/2019/03/survey-form-for-iot.html >>, last accessed on 28-03-2019 at 1:00pm.

Appendix

Package Configuration

```
<?xml version="1.0" encoding="utf-8"?>
<packages>
  <package id="Infragistics.Themes.MetroLight.Wpf" version="1.0.0" targetFramework="net45" />
  <package id="MahApps.Metro" version="1.2.4.0" targetFramework="net45" />
  <package id="WpfAnimatedGif" version="1.4.14" targetFramework="net45" />
</packages>
```

App Configuration

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
    <configSections>
        <sectionGroup name="userSettings" type="System.Configuration.UserSettingsGroup, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" >
            <section name="SurfOpenly.MySettings" type="System.Configuration.ClientSettingsSection, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowExeDefinition="MachineToLocalUser" requirePermission="false" />
        </sectionGroup>
    </configSections>
    <startup>
        <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5" />
```

```
    </startup>
    <userSettings>
        <SurfOpenly.MySettings>
            <setting name="index" serializeAs="String">
                <value>0</value>
            </setting>
            <setting name="serveradd" serializeAs="String">
                <value />
            </setting>
            <setting name="serveruser" serializeAs="String">
                <value />
            </setting>
            <setting name="serverpass" serializeAs="String">
                <value />
            </setting>
            <setting name="serverpskey" serializeAs="String">
                <value />
            </setting>
        </SurfOpenly.MySettings>
    </userSettings>
</configuration>
```

Application

```
<Application x:Class="Application"
    xmlns="http://schemas.microsoft.com/winfx/2006/xaml/presentation"
    xmlns:x="http://schemas.microsoft.com/winfx/2006/xaml"
    StartupUri="MainWindow.xaml">
    <Application.Resources>
    </Application.Resources>
</Application>
```

Main window

```
<Window x:Class="MainWindow"
    xmlns="http://schemas.microsoft.com/winfx/2006/xaml/presentation"
    xmlns:x="http://schemas.microsoft.com/winfx/2006/xaml"
        xmlns:gif="http://wpfanimatedgif.codeplex.com"
    Title="SurfOpenly" Height="359.91" Width="799.137" WindowStyle="None"
Visibility="Visible" BorderThickness="1" ResizeMode="NoResize"
BorderBrush="#FF3BBF53" Icon="./Resources/web-icon.png"
WindowStartupLocation="CenterScreen">
    <Grid>


        <Label x:Name="lb1" Content="Let's Connect" Margin="183,68,146,0"
FontFamily="Century Gothic" FontSize="65" Background="{x:Null}" Height="104"
VerticalAlignment="Top">
```

```
        <Label.Foreground>
            <LinearGradientBrush EndPoint="0.5,1" StartPoint="0.5,0">
                <GradientStop Color="#FFF1A565" Offset="0"/>
                <GradientStop Color="#FFC33737" Offset="1"/>
            </LinearGradientBrush>
        </Label.Foreground>
    </Label>

    <TextBox x:Name="tb_pskey" HorizontalAlignment="Left" Height="27" Margin="526,321,0,0" TextWrapping="Wrap" Text="" VerticalAlignment="Top" Width="133" FontFamily="Tahoma" FontSize="16" SelectionOpacity="0.4">
        <TextBox.Foreground>
            <LinearGradientBrush EndPoint="0.5,1" StartPoint="0.5,0">
                <GradientStop Color="#FF9FCD24" Offset="0"/>
                <GradientStop Color="#FF5EB814" Offset="1"/>
            </LinearGradientBrush>
        </TextBox.Foreground>
    </TextBox>
    <Label x:Name="lb6" Content="Pre-Shared Key:" Margin="521,291,146,0" FontFamily="Arial" FontSize="16" Background="{x:Null}" Height="30" VerticalAlignment="Top">
        <Label.Foreground>
            <LinearGradientBrush EndPoint="0.5,1" StartPoint="0.5,0">
                <GradientStop Color="#FFF1A565" Offset="0"/>
```

```
                <GradientStop Color="#FFC33737" Offset="1"/>
            </LinearGradientBrush>
        </Label.Foreground>
    </Label>
    <ComboBox x:Name="com_protocols" Width="77" HorizontalAlignment="Left" Height="27" BorderBrush="{x:Null}" Background="{x:Null}" IsEditable="True" IsReadOnly="True" SelectedIndex="0" IsSynchronizedWithCurrentItem="True" Margin="10,321,0,10" FontFamily="Tahoma" FontSize="16">
        <ComboBox.Foreground>
            <LinearGradientBrush EndPoint="0.5,1" StartPoint="0.5,0">
                <GradientStop Color="#FF9FCD24" Offset="0"/>
                <GradientStop Color="#FF5EB814" Offset="1"/>
            </LinearGradientBrush>
        </ComboBox.Foreground>
        <ComboBoxItem Cursor="Hand" Content="PPTP"/>
        <ComboBoxItem Cursor="Hand" Content="SSTP"/>
        <ComboBoxItem Cursor="Hand" Content="L2TP"/>
    </ComboBox>
    <Label x:Name="lb2" Content="Protocols:" Margin="5,291,710,0" FontFamily="Arial" FontSize="16" Background="{x:Null}" Height="30" VerticalAlignment="Top">
        <Label.Foreground>
            <LinearGradientBrush EndPoint="0.5,1" StartPoint="0.5,0">
                <GradientStop Color="#FFF1A565" Offset="0"/>
                <GradientStop Color="#FFC33737" Offset="1"/>
```

```
            </LinearGradientBrush>
        </Label.Foreground>
    </Label>
    <TextBox x:Name="tb_server" HorizontalAlignment="Left" Height="27" Margin="97,321,0,0" TextWrapping="Wrap" Text="" VerticalAlignment="Top" Width="133" FontFamily="Tahoma" FontSize="16" SelectionOpacity="0.4" HorizontalScrollBarVisibility="Disabled" UseLayoutRounding="False" VerticalScrollBarVisibility="Auto" RenderTransformOrigin="0.5,0.5">
        <TextBox.Foreground>
            <LinearGradientBrush EndPoint="0.5,1" StartPoint="0.5,0">
                <GradientStop Color="#FF9FCD24" Offset="0"/>
                <GradientStop Color="#FF5EB814" Offset="1"/>
            </LinearGradientBrush>
        </TextBox.Foreground>
    </TextBox>
    <Label x:Name="lb3" Content="Server:" Margin="92,291,644,0" FontFamily="Arial" FontSize="16" Background="{x:Null}" Height="30" VerticalAlignment="Top">
        <Label.Foreground>
            <LinearGradientBrush EndPoint="0.5,1" StartPoint="0.5,0">
                <GradientStop Color="#FFF1A565" Offset="0"/>
                <GradientStop Color="#FFC33737" Offset="1"/>
            </LinearGradientBrush>
        </Label.Foreground>
    </Label>
```

```
<TextBox x:Name="tb_username" HorizontalAlignment="Left" Height="27" Margin="240,321,0,0" TextWrapping="Wrap" Text="" VerticalAlignment="Top" Width="133" FontFamily="Tahoma" FontSize="16" SelectionOpacity="0.4">
    <TextBox.Foreground>
        <LinearGradientBrush EndPoint="0.5,1" StartPoint="0.5,0">
            <GradientStop Color="#FF9FCD24" Offset="0"/>
            <GradientStop Color="#FF5EB814" Offset="1"/>
        </LinearGradientBrush>
    </TextBox.Foreground>
</TextBox>
<Label x:Name="lb4" Content="Username:" Margin="235,291,473,0" FontFamily="Arial" FontSize="16" Background="{x:Null}" Height="30" VerticalAlignment="Top">
    <Label.Foreground>
        <LinearGradientBrush EndPoint="0.5,1" StartPoint="0.5,0">
            <GradientStop Color="#FFF1A565" Offset="0"/>
            <GradientStop Color="#FFC33737" Offset="1"/>
        </LinearGradientBrush>
    </Label.Foreground>
</Label>
<TextBox x:Name="tb_psdd" HorizontalAlignment="Left" Height="27" Margin="383,321,0,0" TextWrapping="Wrap" Text="" VerticalAlignment="Top" Width="133" FontFamily="Tahoma" FontSize="16" SelectionOpacity="0.4">
    <TextBox.Foreground>
        <LinearGradientBrush EndPoint="0.5,1" StartPoint="0.5,0">
```

```
                <GradientStop Color="#FF9FCD24" Offset="0"/>
                <GradientStop Color="#FF5EB814" Offset="1"/>
            </LinearGradientBrush>
        </TextBox.Foreground>
    </TextBox>
    <Label x:Name="lb5" Content="Password:" Margin="378,291,334,0" FontFamily="Arial" FontSize="16" Background="{x:Null}" Height="30" VerticalAlignment="Top">
        <Label.Foreground>
            <LinearGradientBrush EndPoint="0.5,1" StartPoint="0.5,0">
                <GradientStop Color="#FFF1A565" Offset="0"/>
                <GradientStop Color="#FFC33737" Offset="1"/>
            </LinearGradientBrush>
        </Label.Foreground>

    </Label>

    <Rectangle x:Name="rec2" HorizontalAlignment="Left" Height="60" Margin="330,177,0,0" Stroke="White" VerticalAlignment="Top" Width="167" RadiusX="19.5" RadiusY="19.5" Fill="#FF27DC92" Cursor="Hand">

    </Rectangle>
```

```
<Image x:Name="connecting" gif:ImageBehavior.AnimatedSource="Resources/477.gif" Margin="502,184,221,129" Visibility="Hidden" />

<Label x:Name="lb_con" Cursor="Hand" Content="Connect" HorizontalAlignment="Left" Margin="374,192,0,0" VerticalAlignment="Top" FontFamily="Century Gothic" FontSize="16" Foreground="White"/>

<Image x:Name="minimizeapp" HorizontalAlignment="Left" Height="25" Margin="761,10,0,0" VerticalAlignment="Top" Width="26" Source="Resources/substract.png" Cursor="Hand"/>

<Image x:Name="closeapp" HorizontalAlignment="Left" Height="25" Margin="730,10,0,0" VerticalAlignment="Top" Width="26" Source="Resources/cross-out.png" Cursor="Hand"/>

<!-- <Image x:Name="contype" HorizontalAlignment="Left" Height="52" Margin="736,296,0,0" VerticalAlignment="Top" Width="56" Source="Resources/connect-icon.png" ToolTip="Choose Connection Type" MouseDown="Image_MouseDown_1" Cursor="Hand"/>

<Rectangle x:Name="rec1" HorizontalAlignment="Left" Height="358" Stroke="White" VerticalAlignment="Top" Width="870" Opacity="1" Visibility="Visible">

    <Rectangle.Fill>

        <LinearGradientBrush EndPoint="0.5,1" StartPoint="0.5,0">

            <GradientStop Color="#FFB1E0F5" Offset="0"/>

            <GradientStop Color="#FFF6FBFB" Offset="1"/>

        </LinearGradientBrush>

    </Rectangle.Fill>

</Rectangle> -->
```

```
<Image x:Name="icobultin" HorizontalAlignment="Left" Height="134" Margin="575,53,0,0" VerticalAlignment="Top" Width="153" Source="Resources/1438642616_icon_mission-am1.png" ToolTip="Predefined Connections" Cursor="Hand" Opacity="0.01" Visibility="Hidden"/>

<Image x:Name="icocustom" HorizontalAlignment="Left" Height="134" Margin="171,187,0,0" VerticalAlignment="Top" Width="153" Source="Resources/rsz_vpn-icon.png" ToolTip="User Defined Connections" Cursor="Hand" Opacity="0.01" Visibility="Hidden"/>


<Label x:Name="lb7" Content="Choose Connection Type" Margin="10,26,281,0" FontFamily="Century Gothic" FontSize="40" Background="{x:Null}" Height="78" VerticalAlignment="Top" Opacity="0.01" Visibility="Hidden">
    <Label.Foreground>
        <LinearGradientBrush EndPoint="0.5,1" StartPoint="0.5,0">
            <GradientStop Color="#FFF1A565" Offset="0"/>
            <GradientStop Color="#FFC33737" Offset="1"/>
        </LinearGradientBrush>
    </Label.Foreground>
</Label>
<Label x:Name="lb8" Content="A list of predefined free VPN servers." Margin="496,192,17,0" FontFamily="Corbel" FontSize="16" Background="{x:Null}" Height="45" VerticalAlignment="Top" Opacity="0.01" Visibility="Hidden">
    <Label.Foreground>
        <LinearGradientBrush EndPoint="0.5,1" StartPoint="0.5,0">
            <GradientStop Color="#FF1AB0DC" Offset="0"/>
```

```
            <GradientStop Color="#FF2128BF" Offset="1"/>
          </LinearGradientBrush>
        </Label.Foreground>
      </Label>
      <Label x:Name="lb9" Content="Configure your own VPN connection." Margin="292,303,221,0" FontFamily="Corbel" FontSize="16" Background="{x:Null}" Height="45" VerticalAlignment="Top" Opacity="0.01" Visibility="Hidden">
        <Label.Foreground>
          <LinearGradientBrush EndPoint="0.5,1" StartPoint="0.5,0">
            <GradientStop Color="#FF1AB0DC" Offset="0"/>
            <GradientStop Color="#FF2128BF" Offset="1"/>
          </LinearGradientBrush>
        </Label.Foreground>
      </Label>
      <ComboBox x:Name="com_servers" Width="77" HorizontalAlignment="Left" Height="27" BorderBrush="{x:Null}" Background="{x:Null}" IsEditable="True" IsReadOnly="True" SelectedIndex="0" IsSynchronizedWithCurrentItem="True" Margin="10,321,0,10" FontFamily="Tahoma" FontSize="16" Visibility="Hidden">
        <ComboBox.Foreground>
          <LinearGradientBrush EndPoint="0.5,1" StartPoint="0.5,0">
            <GradientStop Color="#FF9FCD24" Offset="0"/>
            <GradientStop Color="#FF5EB814" Offset="1"/>
          </LinearGradientBrush>
        </ComboBox.Foreground>
```

```
        <ComboBoxItem Cursor="Hand" Content="US Server 1"/>
        <ComboBoxItem Cursor="Hand" Content="US Servver 2"/>
        <ComboBoxItem Cursor="Hand" Content="L2TP"/>
    </ComboBox>
    <Button x:Name="infoapp" Content="About Author" HorizontalAlignment="Left" Margin="618,10,0,0" VerticalAlignment="Top" Width="93" Height="28" BorderThickness="1" Background="White" BorderBrush="#FFE6E6E6" Foreground="#FF27DC92"/>
    <Button x:Name="viewlogs" Content="View Logs" HorizontalAlignment="Left" Margin="687,320,0,0" VerticalAlignment="Top" Width="93" Height="28" BorderThickness="1" Background="White" BorderBrush="#FFE6E6E6" Foreground="#FF27DC92"/>
  </Grid>
</Window>
```

mitm17april

ORIGINALITY REPORT

28%	27%	2%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	ijiet.com Internet Source	8%
2	ir.knust.edu.gh Internet Source	6%
3	www.rapid7.com Internet Source	4%
4	ourcodeworld.com Internet Source	2%
5	www.checkmarx.com Internet Source	2%
6	projekter.aau.dk Internet Source	2%
7	studyregular.in Internet Source	1%
8	en.wikipedia.org Internet Source	1%
9	"Security in Computing and Communications", Springer Nature, 2013	<1%

	Publication	
10	Alam, Delwar, Md. Alamgir Kabir, Touhid Bhuiyan, and Tanjila Farah. "A Case Study of SQL Injection Vulnerabilities Assessment of .bd Domain Web Applications", 2015 Fourth International Conference on Cyber Security Cyber Warfare and Digital Forensic (CyberSec), 2015. Publication	<1%
11	prithak.blogspot.com Internet Source	<1%
12	dalspace.library.dal.ca Internet Source	<1%
13	www.terrajp.co.jp Internet Source	<1%
14	parlinfo.aph.gov.au Internet Source	<1%
15	repository.up.ac.za Internet Source	<1%
16	trg.fke.utm.my Internet Source	<1%
17	drvijayy2k2.blogspot.com Internet Source	<1%