12-2017

Man in the Browser Attacks

Krishna Sai Anudeep Ayyagari
St. Cloud State University, kaayyagari@stcloudstate.edu

Man in the Browser Attacks

by

Krishna Sai Anudeep Ayyagari

A Starred Paper

Submitted to the Graduate Faculty of

St. Cloud State University

in Partial Fulfillment of the Requirements

for the Degree

Master of Science

In Information Assurance

December, 2017

Starred Paper Committee:
Jim Q. Chen, Chairperson
Susantha Herath
Sneh Kalia

Abstract

In the present world, everyone uses the Internet and to access the internet they would need to use a browser. Unfortunately, the benefits of the Web are also available to hackers to exploit its weaknesses. Man-in-the-Browser (MITB) attacks are utilized through Trojan malware that infects an Internet browser. This attack is dangerous because of its ability to hide from anti-virus software and steal information as a user from the browser. MITB is able to see information within the browser since no encryption occurs in a browser. This is a serious threat to financial institutions and many other secret institutions as well. No one is safe from a MITB once it is installed because it easily bypasses the security mechanisms we all rely on. This paper explains what MITB attacks are, and how dangerous are those, and how it can be identified and how can we prevent it by discussing various preventive techniques and its effectiveness. This paper will also help to create awareness to the people about this attack

Table of Contents

Chapter Page

List of Tables

List of Figures

Chapter I: Introduction

Introduction

A man-in-the-browser attack is designed to intercept data as it passes over a secure communication between a user and an online application. A Trojan embeds itself in a user's browser and can be programmed to activate when a user accesses specific online sites, such as online banking sites. Once activated, a man-in-the-browser Trojan can intercept and manipulate any information a user submits online in real-time (Safenet, 2015). A number of Trojan families are used to conduct MITB attacks including Zeus, Adrenaline, Sinowal, and Silent Banker. Some MITB Trojans are so advanced that they have streamlined the process for committing fraud, programmed with functionality to fully automate the process from infection to cash out (Safenet, 2015). MITB attacks are not contained to one region or geography; they are a global threat, affecting all regions of the world. However, they are especially prevalent in areas where two-factor authentication is densely deployed because even two-factor authentication can be deceived.

This mainly attacks the banking and financial sectors as well as national institutes. The attacks in Nasa Drone on February 2nd which had allegedly released 276 GB of sensitive data which includes 631 video feeds from the aircraft and weather radars (Thalen, 2016). In the UK, banks are suffering from an increasing number of MITB attacks. One financial institution alone reported a loss of £600,000 because of a single attack by the PSP2-BBB Trojan,(RSA White Paper, 2015). Five European countries such as Germany, the Netherlands, Spain, France, and Poland

have deployed two-factor authentication in the last few years, which have attracted a rise in the numbers of MITB attacks in these regions. Germany has been particularly hard hit by an abundance of MITB attacks as it is one of the few successful paths to commit online banking fraud in the country according to (Federal Office for Information Security, 2010; RSA White Paper, 2015). Lack of Awareness to the public of this attack is one of the main factors for many loses. If certain preventive techniques are taken care these many huge losses might not have occurred.

Problem Statement

Day-by-day technology is developing, unfortunately, even hackers are also using this developing technology and becoming more powerful. Lack of following safeguards and preventive methods are keeping the present financial world in serious threat and can cause huge losses. Many people are not aware of these kinds of attack and there is a need to find the awareness of this attack. There is no existing research access to the awareness levelResearch problem is to find awareness of Man-In-The-Browser attack and also investigate the safeguards and preventive techniques with related evaluations and their reasoning.

Nature and Significance of the Problem

What makes Man-in-the-Browser attacks popular is the ease to which it can be deployed to many systems at once via phishing links or through compromising legitimate sites. By clicking a link, Trojan malware can be installed with add-ons into a browser that has not been properly secured (Safenet, 2015). More attackers are moving away from the traditional Man-in-the-Middle (MITM) attack to the Man-in-the-

Browser (MITB) attack for these reasons. MITB attacks are difficult to detect as activity performed seems as if it is originating from the legitimate user's browser. Characteristics such as the HTTP headers and the IP address will appear the same as the user's real data. This creates a challenge in distinguishing between genuine and malicious transactions. This paper provides the seriousness of this attack to spread the awareness and their appropriate safeguards and preventive techniques.

Objectives of the Study

1. This study is to access the awareness of MITB attacks.
2. Comprehensive review of preventive and safeguard methods that minimize the MITB attacks.

Study Questions

Table 1

Study Questions

Project questions	
How can MITB be dangerous?	• Research the existing MITB Issues and highlight the financial and security losses and learning points.
How to spread awareness about MITB Attack?	• Create a short survey and make the people know about this attack
How can we identify MITB?	• Research on the following symptoms when a system is infected with MITB.
How can we protect from MITB?	• Research with various new viruses or Zeus.
	• Analyze the existing protection systems and check its effectiveness.

Definition of Terms

Man-in-the-browser (MITB): a form of Internet threat related to man-in-the-middle (MITM), is a proxy Trojan horse that infects a web browser by taking advantage of vulnerabilities in browser security to modify web pages, modify transaction content or insert additional transactions, all in a completely covert fashion invisible to both the user and host web application (Wikipedia.com).

Man-in-the-middle attack (MitM): is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. A man-in-the-middle attack is a similar strategy and can be used against many cryptographic protocols (Wikipedia.com).

Trojan is any malicious computer program which is used to hack into a computer by misleading users of its true intent (Wikipedia.com).

Summary

In the present world, the benefits of the Web are widely used and also available to hackers to exploit its weaknesses. Man-in-the-Browser (MITB) attacks are utilized through Trojan malware that infects an Internet browser. The main objective is to get aware and learn you to hide from malware and followed by some sub-objectives like differences between man in the middle and man in the browser attacks and also some recommendations on how we can avoid these attacks.

This attack is dangerous because of its ability to hide from anti-virus software and steal information from the browser as a user. So it’s important to learn the characteristics of this attack. This would also help to figure out if our system is

attacked or infected with MITB. Prevention is always better than curing so this paper would provide effectiveness to the Safeguards and Preventive techniques.

Chapter II: Background and Review of Literature

Introduction

Man-in-the-Browser plays a key role from the Modern Society. As you can see there is a lot of increase in the Crime rates for the Browser Attacks. The major antiviruses companies have analyzed the Browser attacks. IN 2015, there were 1,966,324 registered notifications about attempted malware infections that aimed to steal money via online access to bank accounts around 34.2% of user computers were subjected to at least one web attack over the year and To carry out their attacks, cybercriminals used 6,563,145 unique hosts according to the Kaspersky (2015).

Background Related to the Problem

According to a Symantec 2015 report, they detected 73% fewer financial Trojans in 2014, and a surge (powerful upward moment) in targeted malware incidents. The drop in financial Trojan infections in 2015 came amid a 232% increase since 2014 in malware families targeting some 93 organizations, according to Symantec's newly published Financial Threat 2015 report (Symantec, 2015). The Increase in cybercrimes and online frauds had motivated for research paper to create awareness on this attack and the possible solutions.

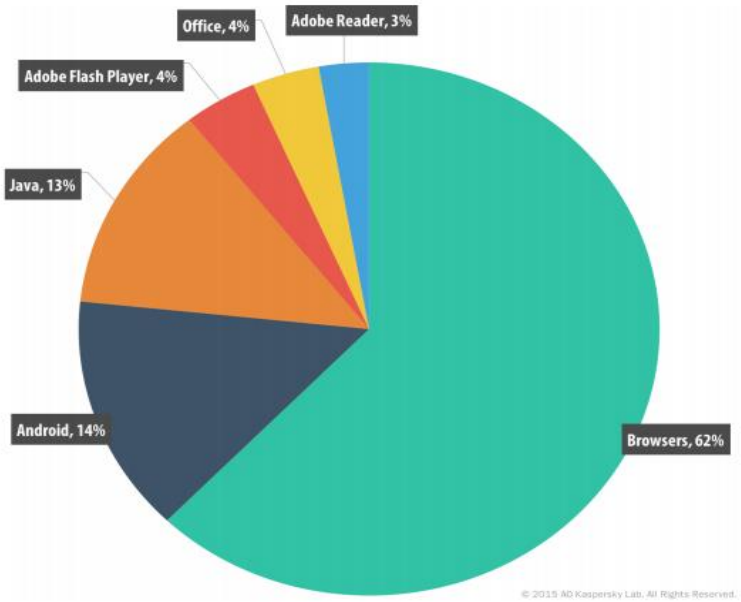

Figure 1. Antivirus report (Kaspersky, 2015).

Literature Related to the Problem

A comprehensive survey of solutions against client-side attacks can be found in the RSA White Paper (2015). The countermeasures against attacks on internet banking are categorized into two types. One type is known as two-channel authentication scheme, which uses two different channels between user and server. The other type is known as two-factor authentication scheme, which typically uses a password and a token. As a former example, mTAN (mobile transaction authentication number), Bhargavan, Delignat-Lavaud, Fournet, Pironti, and Strub (2014) has already been introduced in some European countries. When a bank server receives a transaction request from a user, it generates a one-time password and sends an SMS message which includes the one-time password with the details of the transaction. The user can verify the transaction details and approve it by

entering the password onto the website. If the user finds any forgery in the transaction details, he or she can cancel the transaction by not entering the password onto the website. This countermeasure assumes that it is impossible to forge the source address of SMS and that it is also impossible to eavesdrop and tamper with the transaction details. Moreover, it assumes that the mobile phone is free from malware.

Literature Related to the Methodology

Day-by-day Trojan Viruses are increasing exponentially, so there has been extensive research on attacks to HTTPS/SSL connections and the browser cache, as well as corresponding defenses. Clicking through of SSL warnings. When an SSL warning is shown for a web page, the user is supposed to close the page to protect him/her from MITM attacks. However, 33.0% and 70.2% of users choose to click through SSL warnings on various websites in Mozilla Firefox (beta channel) and Google Chrome stable channel) respectively, according to the investigation by Akhawe and Felt (2013). Various other Man-in-the-Middle Attacks are explained in Saltzman and Sharabani (2009), Yaoqi et al. (2014), and these are related to Man-in-the-Middle. But now even hackers are updated with the new Man-in-the-Browser Attack which they started attacking from the Same internet Protocol addresses. Dhamija, Tygar, and Hearst (2006) observe a 68% click through rate, and Sunshine, Engelman, Almuhimedi, Atri, and Cranor (2009) even record 90-95% clickthrough rates depending on the type of page. Herzberg (2009) studies the basic and advanced indicators and their usability problems.

Attacks against HTTPS. Prior research has unraveled numerous attacks to compromise HTTPS (Bhargavan et al., 2014; Callegati, Cerroni, & Ramilli, 2009; Checkoway et al., 2014; Chen, Mao, Wang, & Zhang, 2009; Karapanos & Capkun, 2014; Marchesini et al., 2005; Marlinspike, 2009; Prandini, Ramilli, Cerroni, & Callegati, 2010). For example, Karapanos and Capkun (2014) present Man-In-The-Middle-Script-In-The-Browser (MITM-SITB) attacks to bypass enhanced Channel-ID-based defenses. Chen et al. (2009) focus on a malicious proxy named "Pretty-Bad-Proxy", which targets browsers' rendering modules above the HTTP/HTTPS layer to void the end-to-end security properties of HTTPS (Safenet, 2015). The theoretical analysis and experiments from Checkoway et al. (2014) show that it is practical to exploit the Dual Elliptic Curve Deterministic Random Bit Generator (DualEC) (National Institute of Standards, 2015) as used in deployed TLS implementations. Prandini et al. (2010) and Callegati et al. (2009) demonstrate practical examples to split the HTTPS stream to attack secure web connections and conduct MITM attacks on the HTTPS protocol.

Zeus, SilentBanker, and URLZone1, are infamous Trojans, which have been successfully used against on-line banking systems (OBS) to steal millions of dollars (Okinawa, 2013). They are primarily used to steal login credentials and card numbers with their security codes, but can also change transaction details on the fly (Okinawa, 2013). Two-factor authentication (excluding full transaction verification) is still inadequate to deal with browser rootkit attacks according to (Okinawa, 2013). So

the Man-in-the-Browser is more advanced that even Two-factor Authentication cannot support.

When browsing the web using HTTPS, if a user Alice ignores, or clicks through, the browser's SSL warning of an invalid SSL certificate, she exposes her browser sessions to a Man-In-The-Middle (MITM) attack, allowing attackers to intercept communication in the SSL channel. Recent work has measured the click through rates for SSL warnings, indicating that more than 50% users click through SSL warnings (Akhawe & Felt, 2013; Dhamija et al., 2006; Sunshine et al., 2009). A typical solution is to improve warnings of invalid SSL certificates (Felt et al., 2014; Sunshine et al., 2009). However, even with the knowledge of an invalid certificate, users often temporarily click through the warnings, e.g., to active Internet access in hotels or cafes through a portal with the self-signed certificate (Chen et al., 2009). Proxy cache poisoning attacks have been well studied (Huang, Xiang, Chonka, Zhou, & Deng, 2011; Klein, 2011). For example, Klein discusses how to use existing techniques, e.g., HTTP response splitting, to mount poisoning attacks on the reverse proxy and forward proxy (Klein, 2011). Huang et al. conduct experiments to poison the HTTP caches of transparent proxies via socket APIs, which cause malicious contents to be served by the proxy to all of its users (Huang et al., 2011).

Summary

There are many research papers on man in the middle attack and many people research on Trojans But day to day new Trojan are getting into the cyber world and each Trojan has its own characteristics and different from other Trojans.

This is making tough to cyber security experts. This paper would collaborate the preventive methods and their effectiveness.

Chapter III: Methodology

Introduction

This chapter describes the methodology how the Man-in-the-browser attacks research has been conducted. What are the main objectives of this research paper, along with sub-objects including the steps and process for the research.

Design of the Study

Man-in-the-browser is an advanced attack. People are unaware of this attack which is making hackers to hack easily. My research targets a sample set of 100 people belonging to various industries and students of different technologies. The aim of this survey is mainly to gather information about how much people are aware of this attack. This survey also creates awareness to the people. I have used Survey monkey website to post the survey

Table 2

Methodolgy for Research Questions

Research Question /Objective	**Approach / Design**
1.What is Man in the Browser and how it works?	Study the existing Research papers from IEEE and other databases
2.How dangerous can MITB be?	Antivirus Reports, financial reports , latest security breaches
3.Are People aware of this Attack ?	A Sample survey on various group of people
4.How can we identify MITB?	Research on the following symptoms when a system is infected with MITB
5.How can we protect from MITB?	Research with various new viruses like Zeus, Analyze the existing protection systems and check its effectiveness

List of questions.

1. Name of Participant(Optional)
2. What is your profession?
3. What is your major or field of expertise?
4. Have you ever heard of Man-in-the-Browser attack?
5. Have you ever heard of Man-in-the-Middle attack?
6. Have you ever heard of the concept of Trojan horse?
7. How likely would you research about Man-in-the-Browser attack?
8. How many news articles did you read about cyber security related attacks this year?
9. Have you ever been a victim of spam?
10. What did you do about the spam emails?
11. Do you update your browser(s) when an update is available?
12. Has your machine been infected by spyware/malware?
13. Have you ever clicked on a link/site that crashed your browser?
14. Did your computer ever been infected by a virus that damaged your computer components or data on your computer?
15. Can you describe any computer attack or virus you ever faced?

Data Collection

A short survey to be conducted among a few groups of people who are in different fields to know the level of awareness they have regarding security attacks that are happening through different sources. These people are picked randomly

from a group of students and it professionals from various countries. There are 107 survey responses received. The survey is sent to a random count of around 500 to 600 people.

Tools and Techniques

1) Website used for Surveys - AllCounted
2) Tool analyzed to understand how MITB works

   Browser Pivoting–Cobalt Stike

Summary

Based on the analyzing done on the different set of people it is obvious that people are not much aware of this attack. This lack of awareness is the advantage of the hacker to us this technique. Also, researching using various tools gave a clear picture of how the attack works from the implementation layer, Research on characteristics of various Trojans to check the characteristics of this attack

Chapter IV: Data Presentation and Analysis

Introduction

Man-in-the-browser would become dangerous if you do not know about the attack, many people are not aware of this attack which can lead to many dangerous outcomes. Especially in the present financial world, this would become disasters. Day-by-day technology is improving and even attacks are also improving. Prevention is always better so this chapter provides some recommendations

Data Presentation

A short survey has been conducted among a few groups of people who are in different fields to know the level of awareness they have regarding security attacks that are happening through different sources. There are a total of 105 responses. The results were quite interesting and are as follows.

1. Name of Participant(Optional)

   67 out of 105 answered to this question.

2. What is your profession?

   There is a 100% response for this question out of which 60% (63 out of 105) are students, 29.52% (31 out of 105) are software engineers, 2.86% (3 out of 105) are business and remaining 7.62% (8 out of 105) are from other professions.

3. What is your major or field of expertise?

   There are 104 responses and 1 skip for this question out of which 33.65% (35 out of 104) are in the field of computer science, 31.73% (33 out of 104)

are in the field of information assurance, 2.88% (3 out of 104) are in information systems, 8.65% (9 out of 104) are in other IT field whereas the remaining 23.08% (24 out of 104) are from non-IT background.

From this values, we can clearly see that 76.91% are from an IT background. Although the first three questions are related to the individual and not mainly to my research, it is important to know some general details about respondents as these details are mainly considered while drawing conclusions.

4. Have you ever heard of Man-in-the-Browser attack?

   Out of 105 people who responded, only 45 (42.86%) people know about the Man-in-the-Browser attack.

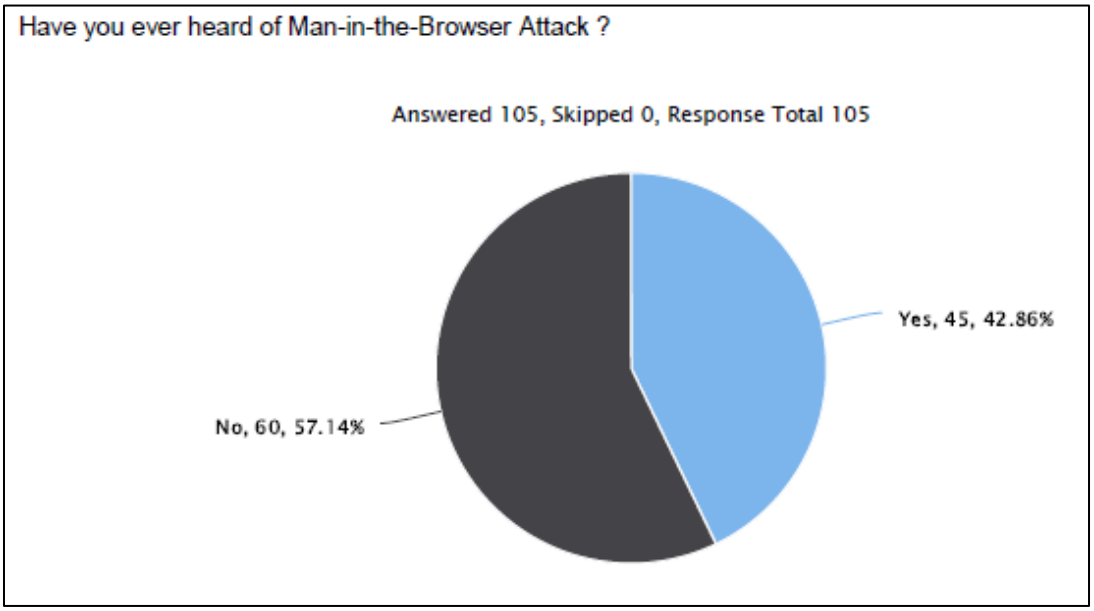

Figure 2. Survey report Q3.

5. Have you ever heard of Man-in-the-Middle attack?

   61.9% of this group are aware of this attack which makes is less vulnerable than Man-in-the-Browser attack.

6. Have you ever heard of the concept of Trojan horse?

   83.81% of this group are aware of the Trojan horse which means that most of them are aware of at least some of the cyber-attacks.

7. How likely would you research about Man-in-the-Browser attack?

   From the result, we know that out of 45 people who heard about the attack, only three were aware of this attack which makes others more vulnerable to this attack.

From the above four questions that are related to different types of attacks, we can say that clearly most of them have a little knowledge about Man-in-the-Browser attack and Man-in-the-Middle attack.

8. How many news articles did you read about cyber security related attacks this year?

   Out the results we can conclude that most of them are in 0-3 range and as the statistics clearly shows that there are 20.95% of people who haven't read any article on cyber security this year which makes them unaware of all the new kinds of attacks that are happening and most probably the victims to some of these attacks.

9. Have you ever been a victim of spam?

   The results are quite disturbing as there are 54.29% of people who are knowingly or unknowingly a victim of spam which means that out of a group of 77% IT background people and 23% of non-IT background there are most of the people who are unable to identify a spam.

10. What did you do about the spam emails?

    There are around 10% of people who opened a spam e-mail while most of the others either reported or deleted while some just ignored these emails. It is better to report and delete these kinds of emails than to just ignore them.

11. Do you update your browser(s) when an update is available?

    It is preferable to update your browsers as every update will have one or more bug fixes or some updated features which might be helpful in keeping your browser and system safe. Also, the response for this question is mostly positive which means that there is some sort of awareness among these people about the software updates.

12. Has your machine been infected by spyware/malware?

    There is 54.29% No and 45.71% yes to this question which means their browsers might not be the only cause for a spyware attack and there are many other means by which a machine can be infected by spyware/malware.

So, it is important to know what might be the different sources of malware and should be cautious about the data that is being transferred and the network and external devices to which the system is being connected.

13. Have you ever clicked on a link/site that crashed your browser?

    The answer to this question is mostly (59.05%) Yes which means that updating your browser only and not taking care of what you are searching

on the web or what you are clicking might also be the main reason for malware attack.

14. Did your computer ever been infected by a virus that damaged your computer components or data on your computer?

    There is a near ratio between Yes and No which means that there are most people who are not clearly taking care of what they do on the web or what kind of data network they are connected to or what kind of data are they transferring etc. to keep your data safe from attacks.

15. Can you describe any computer attack or virus you ever faced?

    There are few attacks that were described but there are many other attacks that are happening without our knowledge on our data.

Man-in-the-browser is one such attack of which most of the people are unaware as it is a mostly a passive attack. And a passive attack is highly difficult to be identified when compared to an active attack as it does not have any direct effect. But passive attacks might lead to many cyber-crimes which we can see in our day to day life and you might also be a victim to these kinds of attacks.

Data Analysis

The awareness clearly explained based on the survey that people are less aware.The anti-virus reports say day by day new Trojans are in the market. A thorough research is done on the Trojans from the latest Kaspersky Antivirus reports

Various types of Trojans.

Silent Banker.

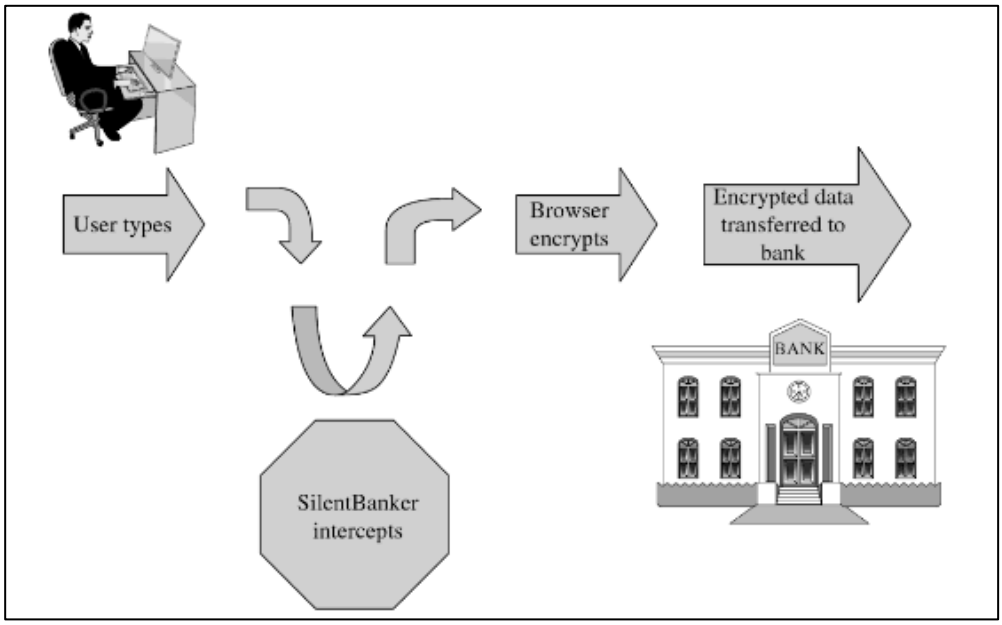

Figure 3. Silent banker (RSA White Paper, 2011)

SilentBanker the name itself says The SilentBanker Trojan offers several advanced MITB features which includes:

1) MITB scripts which have intercept data sent from the victim to the bank (RSA White Paper, 2011).
2) OTP grabber which can intercept and steal one-time password (OTP) codes used by banks to authenticate a user's money transfer according to (RSA White Paper, 2011).

How SilentBanker works. The silent banker uses Local HTML Injections and it creates a mimic of financial institutions' websites .As per RSA White Paper (2011) obtaining one-time passwords would be easier. SilentBanker typically waits until a victim successfully logs into the bank's website and will inject new HTML content.

The newly injected fields prompt victims to divulge sensitive data that is seldom requested by their service providers such as their debit card and PIN number. URLzone URLzone has the ability to inject code into a web page that is loaded into a user's browser to launch MITB attacks (RSA White Paper, 2011). The sample injection that creates a page with a fake error message looks like this which comes after the user has already provided a valid OTP (i.e., We are not able to complete your transaction at this time. Please try again later) according to Charles P. Pfleeger and Shari Lawrence Pfleeger (2012) and RSA White Paper (2011).

Gozi. The most common Trojan which can be handled now. A single attack by a single variant compromises more than 5200 hosts and 10,000 user accounts on hundreds of sites (Jackson, 2007) in a cyber security has listed the below statics:

- Steals SSL data using advanced Winsock2 functionality
- State-of-the-art, modularized Trojan code
- Spread through IE browser exploits
- Undetected for weeks, months by many AV vendors
- Customized server/database code to collect sensitive data
- Customer interface for on-line purchases of stolen data
- Accounts compromised by stealing data primarily from infected home PCs
- Accounts at top financial, retail, healthcare and government services affected
- Data's black market value at least $2 million

RSA White Paper (2011) research say adds the above two statistics:

1) Gozi has injections such as daily transfer limits and balances on checking, savings, and credit card accounts.
2) Gozi Trojan logs containing automated transaction procedures clearly show that Gozi is pre-programmed to determine what percentage of the account balance can be transferred at a time. To determine the amount of transfer, Gozi first retrieves the current account balance. Data Scraping is used by Trojans to access the page's source

Shylock. Shylock is a banking Trojan which utilizes man-in-the-browser attacks designed for banking login credentials from the PCs of clients and Banks. Kaspersky (2017) report has suggested couple of recommendations here are those:

- Don't open email attachments or hyperlinks you receive from an unknown sender. They could contain malware.
- Even if you receive a message with a link or attachment from a friend in a social network or messenger, try to verify the legitimacy of the message via alternative communication channels. Unfortunately, hacked social networks and messengers accounts are often used to spread malware (Kaspersky, 2017).
- When receiving an email or SMS from your bank, keep in mind that banks never ask to provide them with pin codes or passwords from accounts. It is also useful to remember that banks always use corporate mail domains for customer mailings and never use publicly available email services.

- Try to avoid phishing websites: check whether a site uses a secure connection (https in the beginning of address bar).
- Avoid entering your sensitive data while using a public Wi-Fi network (Kaspersky 2017).

Browser pivoting. A visual Cobalt application by which can get a clear picture of Man-in-the-Browser generally. Man-in-the-browser malware uses two approaches to steal banking information.

1. They capture form data as it's sent to a server. For example, malware might hook PR_Write in Firefox to intercept HTTP POST data sent by Firefox (Cobalt, 2013).
2. They inject JavaScript onto certain web pages to make the user think the site is requesting information that the attacker needs (Cobalt, 2013).
3. Cobalt Strike offers a different approach for man-in-the-browser attacks. It lets the attacker hijack authenticated web sessions–all of them. Once a user logs onto a site, an attacker may ask the user's browser to make requests on their behalf. Since the user's browser is making the request, it will automatically re-authenticate to any site the user is already logged onto (Cobalt, 2013).

Malware like Zeus and its variants inject themselves into a user's browser to steal banking information. This is a man-in-the-browser attack. So-called, because the attacker is injecting malware into the target's browser.

Internet Explorer's architecture makes Browser Pivoting possible. Internet Explorer is an application that consumes several libraries. WinINet is the library Internet Explorer uses to communicate. The WinINet API is popular with malware developers because it allows them to request content from an URL with very little code. WinINet is more than a high-level HTTP library built on top of Windows sockets. WinINet manages a lot of state for the applications that use it (Cobalt, 2013).

Table 3

Man-in-the-Browser Trojan Examples (Wikipedia, 2017)

Name	Details	Browser
Agent.DBJP	Gone famous with uk bank attack	IE, Firefox
Bugat	Zeus based botnet	IE, Firefox
Carberp	targets Facebook users redeeming e-cash vouchers	IE, Firefox
ChromeInject	Websit impersonator	Firefox
Clampi	Botnet	IE
Gozi	Steels ssl	IE, Firefox
Nuklus	Targets using IE libraries	IE
OddJob	keeps bank session open	IE, Firefox
Silentbanker		IE, Firefox
Silon	Botnet based on specifc IE	IE
SpyEye	successor of Zeus, widespread, low detection	IE, Firefox
Sunspot	widespread, low detection	IE, Firefox
Tatanga	Multiple browsers	IE, Firefox, Chrome, Opera
Tiny Banker Trojan	Smallest banking Trojan detected in wild at 20KB	IE, Firefox
Torpig	Online banking	IE, Firefox
URLZone	Url link	IE, Firefox, Opera
Weyland-Yutani BOT	crimeware kit similar to Zeus, not widespread	Firefox
Yaludle	Internet explorer botnet	IE
Zeus	widespread, low detection	IE, Firefox

Summary

There are many viruses, Trojans the list and analysis provided are just a few of them. There are many unknown Trojans as well in the Market. But all these antiviruses in the market are trying to find these. It is a challenging task for today's Cybersecurity.

Chapter V: Results, Conclusion, and Recommendations

Introduction

Man-in-the-browser is one of the dangerous attacks. If neglected it is going to become worse. Every day new Trojan comes into the market each has their own features and characteristics. The research done in this paper is limited to certain Trojans. This chapter gives answers or recommendations to the research questions

Results

The results will be explained based on my research questions

What is Man-in-the-Browser? There are various definitions terminology for Man in the Browser.

A MitB Trojan works by utilizing common facilities provided to enhance browser capabilities such as Browser Helper Objects (a feature limited to Internet Explorer), browser extensions and user scripts (for example in JavaScript) etc. according to F-Secure (2007). Antivirus software can detect some of these methods (Gühring, 2007). The man-in-the-browser (MITB) attack leverages what is known as a Trojan Horse (or simply a Trojan). A Trojan is a malicious software that is somehow installed often initiated by various social engineering tactics and resides concealed on the user's computer, frequently undetectable by traditional virus scanning (Entrust Security, 2014).

A man-in-the-browser attack is designed to intercept data as it passes over a secure communication between a user and an online application. A Trojan embeds itself in a user's browser and can be programmed to activate when a user accesses

specific online sites, such as online banking sites. Once activated, a man-in-the-browser Trojan can intercept and manipulate any information a user submits online in real-time according to RSA White Paper (2011).

There are many other definitions for man-in-the-browser but these are the most frequent of all of them Whatever might be the definitions, explanation the attack is all same characteristics.

How dangerous can MITB be? The word Dangerous is not enough to explain the Man-in-the-browser attacks. Few of the terrible attacks are listed here. this contains some of the latest attacks

Eko and Smart browser are recent examples of MITB attacks that made the headlines. Eko discovered on Facebook Russia in early 2015, spread malware via Facebook direct messages and scam video postings. Victims were sent links to phishing websites replicating Facebook and YouTube and which prompted users to install video player extensions containing malicious code Andrey (Kovalev, 2017).

Once installed, the browser-based malware spreads and replicates the browser environment, a perfect combination for malicious web injection. In 2016 we have seen the emergence of advertisement injections and Facebook payload spam. Worryingly, the same technique is imminent for online banking attacks (Kovalev, 2017).

The smart browser is a wrapper-based malware which gains entry into vulnerable machines through user payment downloads and leaves a trail of unwanted or malicious extensions. Appearing on Google Chrome, Yandex Browser,

Opera and Firefox among others, Smart browser switches the browser to an auto-run mode and installs JavaScript-based extensions which spread malicious code even when the browser has been closed (Kovalev, 2017).

Recent items in the news “Swedish bank has informed the press that it has been stung for between seven and eight million Swedish krona–up to £580000” by a single Malware attack “Silent Banker Trojan Targets 400 Banks, Circumvents Two-Factor Authentication, just for starters” “Banking Spyware use stealth Techniques to hide and OWASP AppSecEU09 Poland some of them are very advanced, e.g., Mebroot” A security breach hit Card Systems Solutions resulting in the compromise of 40 million credit card account numbers. Custom Key loggers at Sumitomo provided IDs and passwords to intruders to wire $423 Million out of the bank (OWASP, 2014).

According to Thalen (2016),

> members of the AnonSec hacking group have released more than 276GB of data after allegedly spending months inside NASA’s internal network NASA wasn’t initially focused on drone’s data and upper atmosphere chemical samples. In fact, the original breach into NASA systems wasn't even planned, it was caught up in a gozi virus spread,

the hackers write, referring to an infamous Trojan that has infected more than 1 million computers.

This shows one of important institutions, Banks, companies could not even protect from these attacks. Think about the individuals about this attack Here are the some of MitB Capabilities according to Dougan and Curran (2012).

- Steal Data: MitB’s control on the browser gives it the ability to collect passively by keylogging, and actively by phishing. The Data entered the affected browser is with the hacker, with the ability for them to select

preferred data to steal It has the ability to modify the structure of pages displayed in the browser so you will not even have clue what is happening around.

- Modify Html: The name itself says the browser HTML will be manipulated there are used in two ways most commonly.
    1) Adding extra data entry fields which prompt the user to enter secret information than the required information which the bank etc. don't ask
    2) Modifying the server responses so that you will not be even known that you are attacked. Meanwhile, you realize your money will be lotted
- Modify Outgoing Data: This is similar to the modifying HTML It shows the level of access which can tamper the outgoing from the user might be submitting mostly in banks According to Dougan and Curran (2012). This makes the fraud very much harder to detect and therefore very much more likely to attack succeed but also to remain undiscovered for long enough for the attacker.
- Choose Targets: MITM mostly enables what data they want to access the information every version of MITB makes a list of items which they monitor the browsers. they won't be needing unnecessary data; they only need the text fields like passwords files they obviously don't want the YouTube history and additional data the user will be using. The domain-targeted attacks are chosen for their value, and this targeting allows the fraud to be tailored to the specifications of each chosen domain. For instance, is

clearly not of use to perform HTML injection attacks as discussed above without knowing what to inject and where to do so (Dougan & Curran, 2012).

- Communicate with HQ: Once you receive the data needed it has to be retrieved to get the benefit. sometimes only data will not be useful. Designating a command server and giving that server control over individual infected machines is a particularly valuable secondary use of this ability as it allows for remote modification of the Trojan's parameters and for the software version of the infection to be updated. This, in turn, enables MitB domain and field targeting to be improved and provides a procedure by which new features and techniques can be added as they are devised (Dougan & Curran, 2012). There are many other ways to connect to the server, change the IP make others not know from which host the attack has been taken. there are moe elaborate phishing attacks for Trojan implementations that do not have sufficient control to suppress the warning. there are many efficient ways to do than to provide a Trojan with a library of instructions and scripts

Are people aware of this Attack? People are not actually completely aware. Even students in the security are not known for this attack. To analyze this I have created a Sample Survey with a size of 100. The survey was open for 1 week and is distributed in Social Media Students took a Major Role in Survey, Computer Science people participated more Below are the survey pie Diagrams.

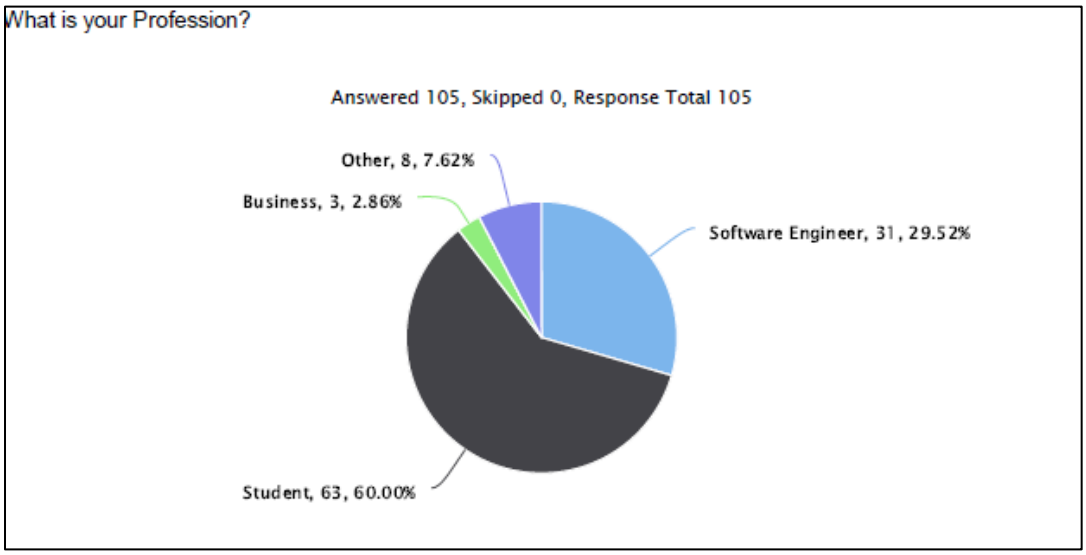

Figure 4. Survey report Q1.

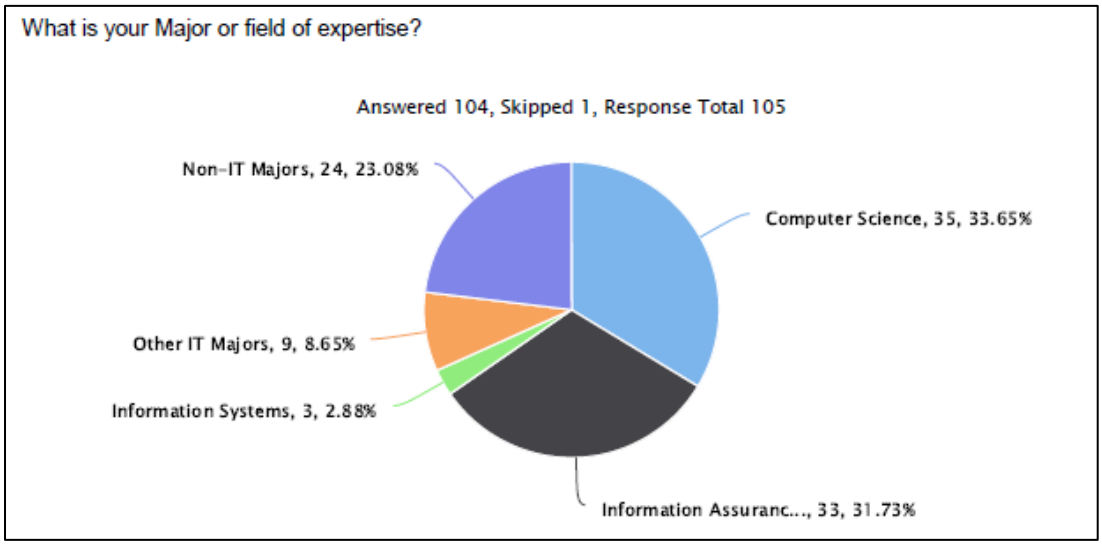

Figure 5. Survey report Q2.

There were many questions in the survey”

- 90% knows Trojan
- 70% knows Man in the Middle
- 57% not heard of Man in the Browser

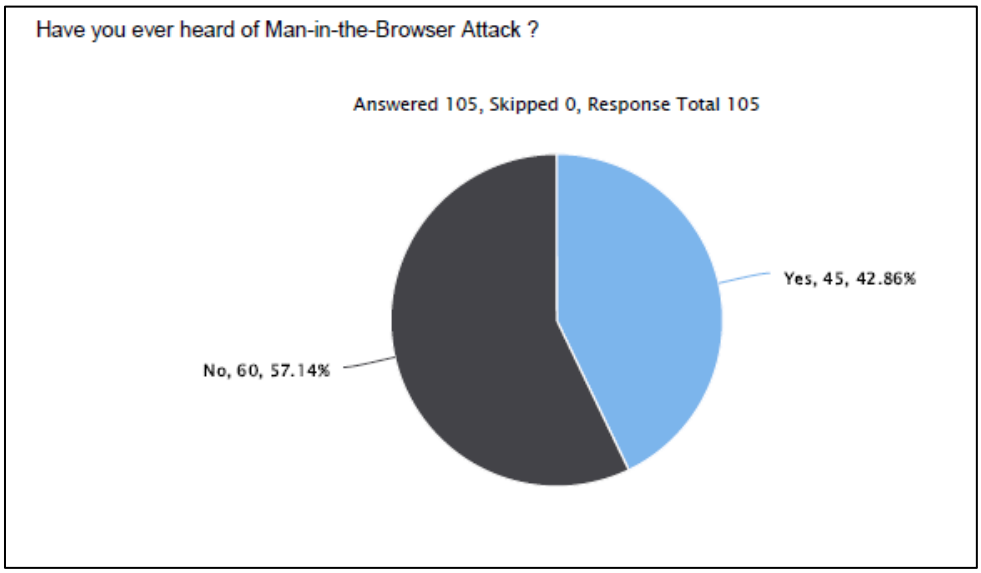

Figure 6. Survey report Q3.

People became so busy in the present modern world, most of the issues they don't read cyber security related issues, as you can see the survey done on educated people mostly with computer science background and software industries only 10% read more than 10 article in a year, and 12%, 5 to 10 articles. Rest all are not reading a cyber-related article, so, this will become the advantage to a hacker. The new Trojans characteristics, antivirus reports and many recent articles and the hacking related article will help us aware of the attack. The Man in the Browser, if we are not aware of this attack people, can never suspect if something is going wrong.

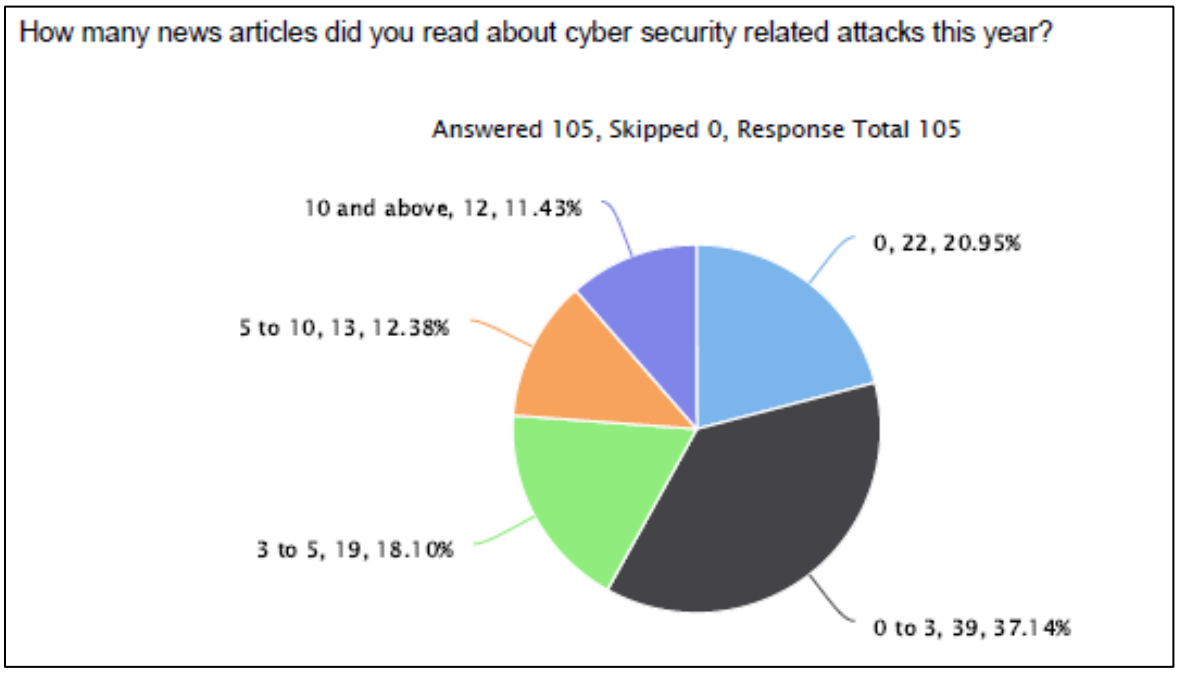

Figure 7. Survey report Q10.

How can we identify MITB? Identifying that our PC is infected with any Trojan related to Man-in-the-browser are very complex. As the regular antivirus, we all rely is not going to be useful here all the times. We need to update the antivirus regularly. apart from this we should monitor the sites if they are asking for relevant information or not for example providing all personal details is not recommended

Detecting and preventing MITB attacks are complex for the following reasons:

- Location of malicious code, parts of malicious functionality are stored on remote servers and often an infected PC doesn't contain any malicious code at all. The harmful payload can change dramatically depending on websites and URLs visited. It's difficult to tell harmful scripts from legal ones (Kovalev, 2017).

- From the user's perspective, a malicious extension can look legal and be useful for users. It can work like a normal extension for some time, and only start to behave harmfully a month or two after installation (Kovalev, 2017).
- Malicious extensions live only in the browser and don't leave any traces in critical system areas, this makes them hard for anti-virus products to detect (Kovalev, 2017).
- A malicious extension can be harmful to the user and the web resource, by replacing ads and search responses with malicious content. For traditional anti-virus vendors, these ad injections are difficult to detect (Kovalev, 2017).

The general recommendations do not open pages you do not use regularly or less thrust worthy, it is advisable to always monitor your browsers add-on and checking Task managers and H keys.

Below are the reference screenshots.

Look for the Task Manager (ALT + CTRL+ Del) for Windows

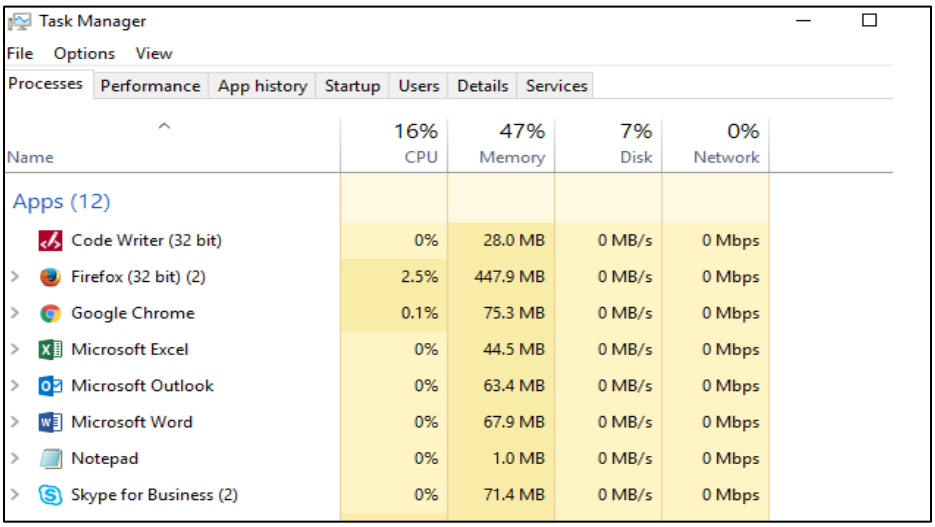

Figure 8. Screen shot of task manager.

Check the Background Process and look for any unknown background Process, use google to understand the background Process.

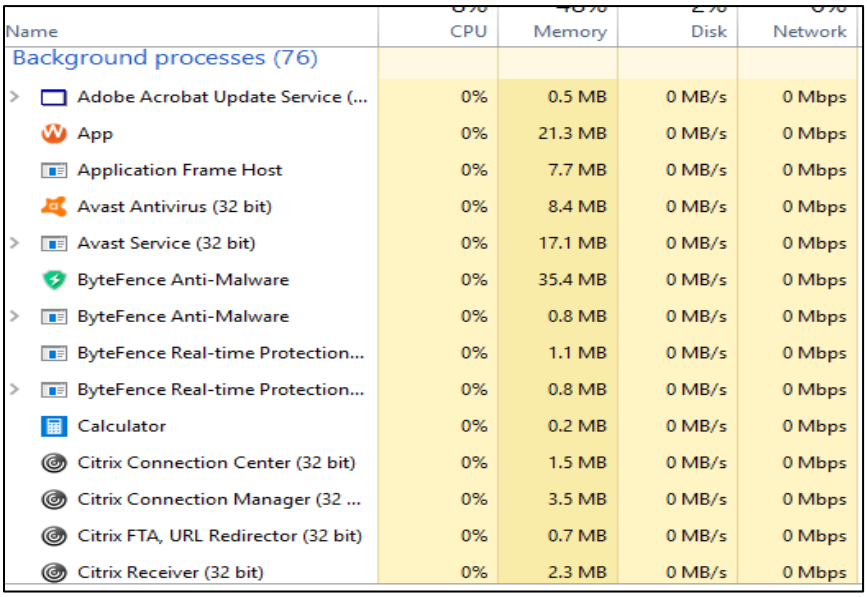

Figure 9. Screen shot of background process.

Go to command Prompt Click Reg Edit to check the Hkey process. Please refer the screenshot for sample “Registry Editor”.

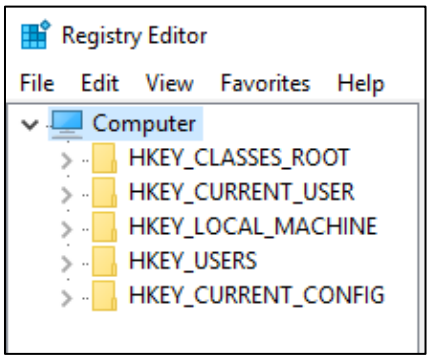

Figure 10. Screen shot of RegEdit.

Click on Local Machine, Software and see if there are any other files and use google search Engine to confirm if they are harmful.

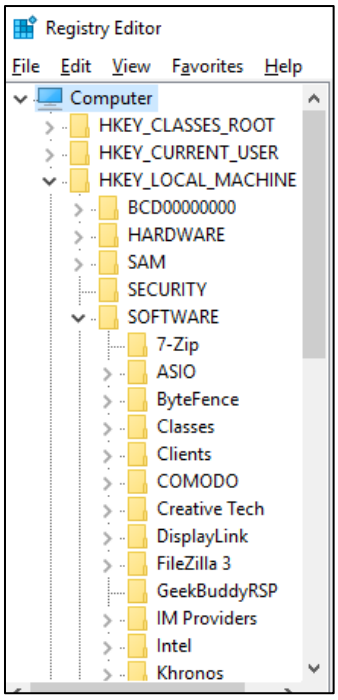

Figure 11. Screen shot of Reg Edit 2.

How can we protect from MITB? There is no clear method in which to prevent MITB attacks beyond in-depth monitoring and prevention on the endpoint. Endpoint management that involves monitoring and preventing the browser from

making changes to the system is one possibility to provide some defense against this attack according to (Cain, 2014).

The problem of protection arises since there is a lack of awareness of such attacks and to add the difficulty, authentication that uses today's standard are bypassed, such authentication includes:

1) Username with password
2) Client certificates
3) SecureID certificates
4) Biometry authentication
5) 2-factor authentication

If one Is relying on authentication with user and machine for authorization, the Trojan horse that works concurrently with the MiTB can bypass all that without affecting the login authorization.

Various solutions. Knowing the difficulty and complexity of such attacks protection can be tricky and come with pros and cons such solutions include:

Protection against man in the browser attacks.

Hardened browser. Hardening a browser or making the browser "More" secure is one way of minimizing the threat, steps include If one is running Adobe flash player, (a majority of today's browsers have it running) make sure to disable third party flash cookies. The next step is to uninstall Java unless it is being used actively by a user. Based on the browser the hardening steps are getting changed. Most of the MitB are getting attacked using Adobe and java. if we are not using these. we can

uninstall them for a safety process. Here are some of the instructions based on Browser.

Google chrome uses google search engine which captures our search history which will break the privacy.

According to Gizmo's (2015) install some ad blockers like.

Web of Trust (WOT): WOT covers a screen with warnings to decide whether the page is dangerous and you have the option to leave or stay. In terms of malicious sites, phishing sites, scam sites, and similar content this is a reliable plugin.

BitDefender TrafficLight: this if installed and you open upon a dangerous site, which is blacklisted by BitDefender, a page will not load. These include malicious pages, phishing sites, and fraudulent sites and many others.

Adblock Plus: This is a most common ad-blocker which blocks the virus which comes through ads. thus, restricting some dangerous websites.

Script Safe: This add-on will block all scripts and other dangerous content. Even you land up on a dangerous page this add-on will not let the page run the script. Thus, you are protected from harmful scripts and many privacy threats. But there are few flaws that many useful pages or good pages also run some scripts, those will get failed so we need to manually add those scripts.

The objective of our protocol is to provide trust communication between a client and a server as well as preserving the secrecy of the user's sensitive information. In order to achieve this objective, we have incorporated the TPM based remote attestation in order to provide the platform integrity verification. In addition, we

have adopted the Secure Remote Password (SRP) (Wu, 1998) as the secure key exchange protocol in order to provide zero knowledge proof that allows one party to prove themselves to another without revealing any authentication information such as password (Mat Nor, Abd Jalil, & Ab Manan, 2012).

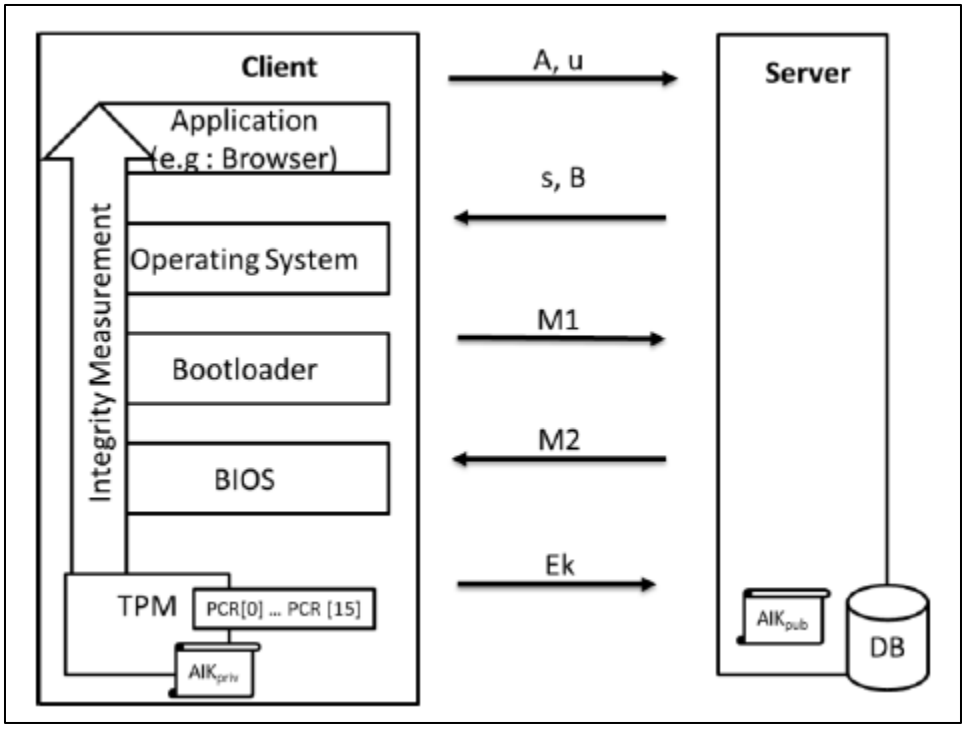

Figure 12. Key exchange and attestation phase (Mat Nor et al., 2012).

Key Exchange and Attestation Phase (Mat Nor et al., 2012). The benefits of hardening a browser are that it is easily available to users as needed, it may reduce functionality and ease of use that adding add-ons to browser help. The problem of doing this step is that it is not full proof to the MiTB attack.

Virtual machine. Another way of prevention is to have a secure virtual operating system installed in the user's PC, one may use VMWare with a secure OS such as Open BSD for important secure transactions. The benefits of using a virtual

machine is that it fairly cheap and it is not hard to use from the user's perspective. It also adds to the complexity of successfully executing MiTB attack. The cons of having a virtual machine are not that easy and user-friendly as a secure browser, and lastly, it can be tedious for the user to constantly logging in the virtual machine to do important transactions.

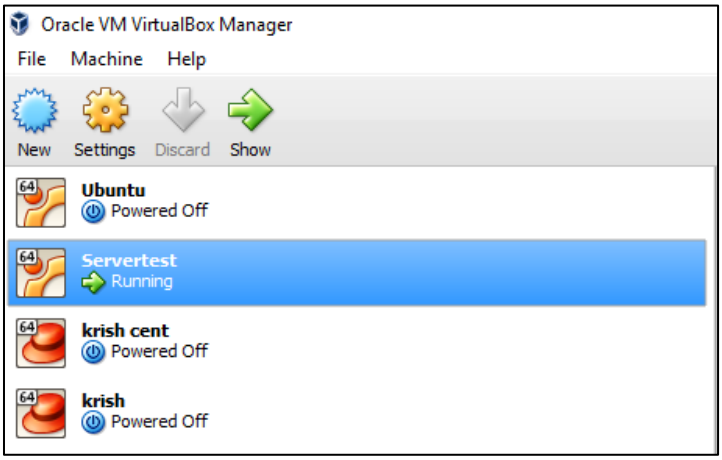

Figure 13. Virtual box sample.

Creating a Virtual Machine using any tools like Oracle VM and use only for Banking.

Runtime application self-protection. It is one of the new security technology which can detect and prevent real-time application attacks. It prevents the attacks without human intervention by using self-protection and reconfiguring automatically.

According to VeraCode (2016), the technology could either be in diagnostic mode and simply sound an alarm regarding an attack, or it could be in self-protection mode and stop a potentially malicious execution.

RASP's protection measures include the following (Veracode, 2016):

1) User session termination

2) Application termination

3) Alert to security personnel

4) Warning to user

Out of band solution. Out-of-band communication system is a robust method for security. Many research papers proved this is the most efficient way to protect from man-in-the-browser. When a Trojan is installed into user's browser these out-of-band communications include something like SMS, Postal mails, or Emails, etc.

The RSA Adaptive Authentication Out-of-band Phone module provides users with a one-time passcode that appears in the Web browser. The system will then ask the user to select one of the phone numbers previously recorded during enrollment at which to receive a phone call and an automated phone call is generated. The call reviews the transaction details and prompts the user to enter the one-time passcode that is displayed on the Web browser into the keypad on their phone. Once the number is entered into the phone and confirmed to be correct number, the transaction will continue without disruption, (RSA White Paper, 2014).

Other recommendations. Users should not click through SSL warnings on any site in normal browsing mode (Chen et al., 2009). As a precaution, they should also clear browser cache, i.e., the web cache and HTML5 AppCache, before visiting a site processing sensitive information, especially after an SSL warning is clicked (Chen et al., 2009).

The settings of 21 browsers like Javelin, Web Explorer and Web Browser are observed, these are not provide the option for users to clear cache. Safari, IE,

Android Default Browser, and Maxthon have the Clear cache button but the setting does not specify web cache and AppCache. Chrome and Firefox, support various options for users to clear browsing data. However, clearing cache takes several steps. For example, on Chrome users would need to click Setting → Privacy and then Clear browsing data. Most of the browser don't allow cache to clear the data. This can also become a loophole to hacker.

Whilst MITB and web extension attacks are difficult to detect and therefore defend against, users and worse. providers can work together in the fight against cybercrime as it continues to (Kovalev, 2017). Detection and protection policies from both the server-side (web services) and client-side (browser and AV vendors) can provide a belt and braces style protection against MITB attacks (Kovalev, 2017).

Server-side techniques which incorporate content security policies (CSP) and reporting capabilities can be implemented in all modern browsers and operate in two modes: reporting-only mode and blocking mode (Kovalev, 2017). In reporting mode, violations are reported but without blocking the browser. In blocking mode, all violations are blocked by the browser and reported back to the URL (Kovalev, 2017).

Table 4

Effectiveness of Various MITB Preventive Processes

Methods	**Effectiveness against MITB**	**Reasoning**
Use strong password, Biometric, Grid Card, Mutual Authentication, OTP Token, Smart Card & Digital Certificate	Not effective	Malware can intercept or wait until user has past this challenge before taking over
Basic Security Awareness, keep OS, Browser updated, Anti-virus/Anti-malware	Maybe	Chances of getting infected by Malware is lower though still high if using vulnerable OS/Browser
Using separate system for and only for Online banking	Yes but inconvenient	Chances of getting infected by Malware is lower but it is inconvenient and requires strict discipline which is rare
Out-of-Band Transaction Detail Confirmation plus OTP	Yes	User has opportunity to view transaction details in a separate communication channel financial institution must take care to protect against easy reset of the out-of-band contact details

Table 5

Effectiveness of Various MITB Passive Processes

Methods	Effectiveness against MITB	Reasoning
IP Location tracking	Not effective	This is effective only when credentials are stolen and used from elsewhere. In the case of MITB attack, the request comes from the genuine user's browser so a server cannot distinguish based on IP location of the device profile.
Device profiling	Not effective	
Fraud Detection based on Transaction type and amount	Sometimes	Some banks have fraud detection based on transaction details. However, such detection is typically done as a batch process and not in real time and therefore any detection is normally much after the attack.
Fraud Detection based on user behavior	Good	User profiling to create a baseline normal behavior so that abnormal behavior can be detected and a user can be alerted before an actual transaction takes place.

Conclusion

Man-in-the-Browser is the future nightmare to fininacial institutes as well as IT industries. Lack of awareness of this attack will make it worse. The world is in an "arms race" and should expect that criminal ingenuity will continue to be applied; attacks will get more and more difficult to thwart. Countermeasures will continue to evolve and be replaced by more effective approaches (Entrust Security, 2014). A combination of anti-virus software, server, and client-side prevention methods are needed to fight against man in the browser. There is no specific clear method which

can prevent MITB attacks apart from beyond in-depth monitoring and prevention on the endpoint or client side encryption. This endpoint management which involves depth monitoring and preventing the browser from making changes to the system is one of the possibility to provide some defense against this attack. Many banks have even offered software that detects MITB type malware. User education is mentioned as a method to prevent these attacks.The present survey says even students, people with IT background are not aware of this attack. Even trained security experts are getting fooled easily with Man-in-the-Browser attacks. Transaction verification is the safest process. Out of Band is one of the Method all the research papers, security experts are saying to be safe.

Day by day new Viruses are coming into the System so Security Awareness and best practices are required to protect oneself against getting infected with malware with regular software updates. Hackers are getting updated with the technology. It is our responsibility to get updated with technology, latest software updates and browser updates especially while dealing with the Online transaction one must monitor and report immediately if you find something unusual.

There are famous quotes by Robert Kiyosaki and Bruce Schneier:

"The Only person who is going to give security and the life you want is YOU"

"Security is not a product, but a process"

Future Work

The present cyber world is still not safe with Man-in-the-Browser Attack. There are still a big need of Strong antiviruses in the cyber world to counter this attack.

Also, many people are using the Mobile devices nowadays So the hackers are coming with a new attack called Man-in-the-Mobile. There should be strong protection systems need to build for both the attacks.

References

Akhawe, D., & Felt, A. P. (2013). Alice in warningland: A large-scale field study of browser security warning effectiveness. In *USENIX Security Symposium*, pp. 257–272.

Bhargavan, K., Delignat-Lavaud, A., Fournet, C., Pironti, A., & Strub, P.-Y. (2014). Triple handshakes and cookie cutters: Breaking and fixing authentication over TLS. In *2014 IEEE Symposium on Security and Privacy (SP)*, pp. 98-113.

Cain, C. (2014). *Analyzing Man-in-the-Browser (MITB) attacks*. SANS Institute. Retrieved from https://www.rsa.com/content/dam/rsa/PDF/Making_Sense_of_Man_in_the_browser_attacks.pdf.

Callegati, F., Cerroni, W., & Ramilli, M. (2009). Man-in-the-middle attack to the HTTPS protocol. *IEEE Security & Privacy, 7*(1), 78-81.

Checkoway, S., Fredrikson, M., Niederhagen, R., Green, M., Lange, T., Ristenpart, T, et al. (2014). On the practical exploitability of dual EC in TLS institutions. In *USENIX Security Symposium*, pp. 319-335.

Chen, S., Mao, Z., Wang, Y.-M., & Zhang, M. (2009). Pretty-bad-proxy: An overlooked adversary in browsers' HTTPS deployments. In *2009 IEEE Symposium on Security and Privacy*, pp. 347-359.

Cobalt strike. (2013). Retrieved from https://blog.cobaltstrike.com/2013/09/26/browser-pivoting-get-past-two-factor-auth/.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. In *Proceedings of the 24th ACM Conference on Human Factors in Computing Systems,* pp. 581-590.

Dougan, T., & Curran, K. (2012, March). Man in the browser attacks. *International Journal of Ambient Computing and Intelligence, 4*(1), 29-39. Retrieved from https://www.sans.org/reading-room/whitepapers/forensics/analyzing-man-in-the-browser-mitb-attacks-35687.

Entrust Security. (2014). *Defeating man-in-the-browser malware*. Retrieved from https://www.entrust.com/wp-content/uploads/2014/03/WP_Entrust-MITB_March2014.pdf.

F-Secure. (2007, February 11). *Threat Description: Trojan-Spy: W32/Nuklus.A.*

Federal Office for Information Security. (2010). *The IT security situation in Germany 2007*. Retrieved August 12, 2010, from https://www.bsi.bund.de/cae/servlet/contentblob/471384/publicationFile/28209/Lagebericht\2007_englisch_pdf.pdf.

Felt, A. P., Ainslie, A., Reeder, R. W., Consolvo, S., Thyagaraja, S., Bettes, A., Harris, H., & Grimes, J. (2014). Improving SSL warnings: Comprehension and adherence. *CHI*. Retrieved from https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/43265.pdf.

Gizmo's. (2015). *How to harden your browser against malware and privacy concderns*. Retrieved from http://www.techsupportalert.com/content/how-harden-your-browser-against-malware-and-privacy-concerns.htm.

Gühring, P. (2007, January 27). Concepts against Man-in-the-Browser Attacks.

Herzberg, A. (2009). Why Johnny can't surf (safely)? Attacks and defenses for web users. *Computer Security, 28*(1), 63-71.

Huang, X., Xiang, Y., Chonka, A., Zhou, J., & Deng, R. H. (2011). A generic framework for three-factor authentication: Preserving security and privacy in distributed systems. *IEEE Transactions on Parallel and Distributed Systems, 22*(8), 1390-1397.

Jackson, D. (2007). Threat analysis-Gozi virus. Retrieved from https://www.secureworks.com/research/gozi.

Karapanos, N., & Capkun, S. (2014). On the effective prevention of TLS man-in-the-middle attacks in web applications. In *USENIX security symposium* (pp. 671-686.

Kaspersky (2017). *Kaspersky financial report*. Retrieved from https://usa.kaspersky.com/internet-security-center/threats/shylock-banking-trojan-definition#.WMoXzTvyvIU.

Klein, A. (2011). Web cache poisioning attacks. In *Encyclopedia of crytpgrophy and security* (p. 1373). Springer.

Kovalev, A. (2017). *Protecting against man in the browser attacks*. Retrieved from https://betanews.com/2016/12/22/man-in-the-browser-attack-protection/.

Marchesini, J., Smith, S. W., & Zhao, M. (2005). Keyjacking: The surprising insecurity of client-side SSL. *Comput Secur, 24*(2), 109-123.

Marlinespike, M. (2009). *New tricks for defeating SSL in practice*. BlackHati.

Mat Nor, F. B., Abd Jalil, K., & Ab Manan, J. (2012). Mitigating man-in-the-browser attacks with hardward-based authentication scheme. *International Journal of Cyber-Security and Digital Forensics (IJCSDF), 1*(3), 204-210.

National Institute of Standards and Technology. (2015). *Guidelines for the selection and use of Transport Layer Security (TLS) implementation*. Washington, DC: U.S. Department of Commerce.

Okinawa. (2013). Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). In *17th International Conference on Financial Cryptography and Data Security*, April 1-5, 2013.

OWASP. (2014). *Testing software*. Retrieved from https://www.owasp.org/images/e/e4/AppsecEU09_The_Bank_in_The_Browser_Presentation_v1.1.pdf.

Pfleeger, C. P., & Pfleeger, S. L. (2012). *Analyzing computer security: A threat/vulnerability/countermeasure approach*. Pearson Educations.

Prandini, M., Ramilli, M., Cerroni, W., & Callegati, F. (2010). Splitting the HTTPS stream to attack secure web connections. *IEEE Security and Privacy, 8*(6), 80-84.

RSA White Paper. (2011). *Making sense of man-in-the-browser attacks: Threat analysis and mitigation for financial institutions* (pp 3-7). Retrieved from http://viewer.media.bitpipe.com/103918378634/129527718816/MITBWP0510-RSA.pdf.

Safenet Security Guide. (2015). Man in the browser. Retrieved from http://www.safenetinc.pt/uploadedFiles/About_SafeNet/Resource_Library/Resource_Items/White_Papers__SFDC_Protected_EDP/Man%20in%20the%20Browser%20Security%20Guide.pdf.

Saltzman, R., & Sharabani, A. (2009, February). *Active man in the middle attacks: A security advisory*. A white paper. IBM Rational Application Security Group.

Sunshine, J., Engelman, S., Almuhimedi, H., Atri, N., & Cranor, L. F. (2009). Crying wolf: An empirical study of SSL warning effectiveness. In *Proceedings of the USENIX Security Symposium*.

Symantec Corporation. (2015). *Financial threat report gives consumers security tips.* Author.

Thalen, M. (2016). *Hackers allegedly hijack drone after massive breach at NASA*. Retrieved from http://www.infowars.com/hackers-allegedly-hijack-drone-after-massive-breach-at-nasa/.

Veracode. (2016). *Runtime application self-protection (RASP)*. Retrieved from https://www.veracode.com/security/runtime-application-self-protection-rasp.

Wikipedia. (2017). Man-in-the-middle attack. Retrieved from https://en.wikipedia.org/wiki/Man-in-the-middle_attack.

Wu, T. (1998). The secure remote password protocol. In Internet Society Network and Distributed Systems Security Symposium (NDSS), San Diego, pp. 97-111.