**University of Victoria**

**Department of Electrical and Computer Engineering**

**ELEC 591 Professional Practice**

**(Capstone Project)**

**Man-in-the-Browser (MITB) Attack Defense Strategies**

**Student name: Maninder Singh (V00879900)**

**Prabhjot Kaur (V00877155)**

**Barath Gosakan (V00874048)**

**Olumide Owoyomi (V00855280)**

**Mei Jia Liu (V00872728)**

**April 13, 2017**

**Abstract**

In recent decade, online banking provides more commercial opportunities and convenience for financial organizations and customers. With the popularity of online banking business, malware and attacks are surging aiming to financial institution. One of the most dangerous malicious attacks is Man-in-the-Browser (MITB) attacks, which is to deploy the malicious code to infect the browser when customers are employing online transactions. Man-in-the-Browser attack is that the users log onto infected bank browser to launch their transactions, thus, it is a quite difficult to detect and prevent the customers against this attack by the traditional security protection technique for bank system. This paper analyzes several common Trojan functionalities of MITB attacks, such as Zeus, Silent Banker, and URL Zone etc. MITB attacks contain some different categories which are browser helper objects, DOM module interface, Java script and AJAX, API hooking and cookie hijacking. Based on these functionalities, the article presents several proposed defense mechanisms that belong to active counter measures. OTP token with signature, Out-of-Band transaction details confirmation with OTP and cookie encryption are verified to be more effective against MITB in most situations, however, there are still some drawbacks for these solution models and it is necessary to improve these methods. Furthermore, the future work is suggested to combine active counter measures with passive counter measures to protect the customers and bank institution benefits.

**Contents**

Abstract......................................................................................................................2

Introduction...............................................................................................................4

Background…………………………………………................................................5

MITB Features and Functionality………………..…................................................6

MITB Attack Types………..……………………….................................................7

MITB Proposed Solutions..........................................................................................8

Conclusion and Future Work...................................................................................11

References...............................................................................................................12

**Introduction**

Internet banking is becoming increasingly popular because it is convenient and flexible in nature. Around 40% of the world population has an internet connection today. In 1995, it was less than 1%. The number of internet users has enlarged tenfold from 1999 to 2013. The first billion was reached in 2005, the second billion in 2010 and the third billion in 2014[1]. Now about eight years later, the people subscribing to online banking services have increased worldwide. With an increase in online banking, a considerable rise in some types of cyber crimes have been noticed. The financial services industry has become a primary target of cyber-attacks on a global scale. Although all types of cyber-crime have been on the rise, there has been a sharp increase in financial fraud resulting from computers infected with malware. One of the most dangerous types being Man-in-the-Browser (MITB) attacks.

An MITB attack is essentially a man-in-the-middle (MITM) attack, but unlike typical MITM attacks, which usually occur at the network layer, MITB attacks are introduced between the user and browser[2]. It is a proxy Trojan that contaminates a web browser and can modify web pages, modify transaction content or insert additional transactions, all in a completely covert fashion invisible to both the user and host application[3].

No one is safe from an MITB once it is installed, which easily bypasses the security mechanisms we all dependent on. MITB has ability to hide from anti-virus software and steal information from the browser as well also able to see information within the browser. Since no encryption occurs within the browser, security controls used by financial institutions are ineffectual. Two-factor authentication does not work because this malware can access to user account settings. Anti-fraud technologies used by banks to detect malicious activity are ineffective because the transactions seem to occur from the victim’s computer unit. Many banks have added additional layers of security for wire transfers using notifications such as SMS texts. Therefore, if an attacker can steal users’ credentials then he might have the ability to change notification settings in the bank account of the user. [4]

The losses recognized to financial fraud are frightening. The financial services industry has become a primary target of cyber-attacks on a global scale and, in 2009 alone, suffered losses totaling $54 billion an increase from $48 billion in 2008 and it is exponentially increasing continuously. Of equally important concern to financial services institutions is the damage cybercrime can cause to reputation, along with customer churn, both of which can have a significant impact, and possibly devastating, effect to revenue. Hence these terrifying security issues make man-in-the-middle (MITM) highly important to discuss. [5]

**Background**

Attackers are using newer and advanced methods to target online users or financial institutions. One of the fastest growing attacks is Man in the browser attack. The dissemination of man-in-the-browser attack is being helped by phishing attacks, social networking sites popularity and drive by downloads. There has been exponential growth in number of attacks over last years against financial institutions including Europe corporate banking and U.S. corporate banking markets. The major contributor towards spreading of man-in-browser attack is spear phishing. These days there is enough of data available on internet about individuals on social networking sites such as Facebook, LinkedIn which allows the adversary to collect enough credible data about them to send them emails in such a way that they will believe it to be true and will evoke a response. Forty five percent of employees indicate that they have received phishing emails at workplace [6].

The increased use of social networking sites and number of users using social networking websites has also played their part in spreading of malware and Trojans. Forty percent of users on social networking websites have encountered some form of malware attack [7].

Drive by downloads have also contributed in spreading of MITB attacks. A drive-in download attack initiates when a user clicks a link on email and he/she is redirected to a website which was made by attacker to infect users. About two of every thousand pages displayed to the users from search engine contains drive by download [8].

For example, Paul McCartney's fan page attack is one of the most prominent examples of this type of attack. In 2009, site was hacked by attackers for two days and persons who visited that site were silently infected by MITB Trojan. Also, UK banks have reported increasing number of MITB attacks. One financial Institution alone reported loss of £ 600,000 because of single MITB attack[9].

**MITB Features and Functionality**

There are many Trojan families used to conduct Man-in-the-browser attack. These Trojan families are Zeus, Bugat, Clod, Gozi (v2, 2010), Lamp, Mimicker, Patcher, Silent Banker, Silon, SpyEye, Syscron, and URLZone.Most common Trojan families are described as follows:

**1. ZEUS** - Zeus is the most effective crime ware kit ever observed by internet security community. This Trojan can seize various types of traffic. To conduct Zeus attack, attacker needs to have very less skills. All the attacker need to do is to steal cookies. As cookies have digital signature added to them to keep them secure. Also, a cookie cannot be created. So, attacker need to steal them and then present to the bank server to enter ongoing online banking session.

**2. SILENT BANKER** – Silent banker Trojan can intercept data from victim to the bank. It also works as OTP grabber. This Trojan has also ability to inject local HTML injection to copy the design of targeted bank website. In this Trojan attacker waits for victim to log in to bank's genuine website. When victim logs in successfully to bank's website, it injects new HTML content which has ability to steal sensitive data like debit card and PIN number.

**3. URL ZONE** – This Trojan continuously monitors the access on online banking websites. This Trojan depends upon social engineering schemes to conduct MITB attack. URL zone is capable of injecting code into web page that is currently loaded by user to launch Man-in-the-browser attack. In this Trojan, attacker waits for the victim to log in to bank's website and enter credentials. When attacker enters credentials and inputs OTP to complete the transaction, attacker injects another code which has capability to create a fake code error message.

**4. GOZI** – Gozi Trojan is preprogrammed in such a way that adversary can know what percentage of account balance can be transferred at one time. To determine what percentage of balance can be transferred, Gozi Trojan first retrieves the current balance in account, and daily transfer limits and then uses transaction authentication number to complete transfer.

**MITB Attack Types**

**1.Browser helper Objects**

These are the additional add-ons that are installed in the browser to provide added functionality. These were first introduced in the year 1993 in internet explorer and has been used ever since in all the browsers. The main issue is that this runs in the browser background using administrator privileges and are not detected by any antivirus software. So, when the malware is inserted as a browser helper object, it runs in the browser background using administrator privileges and is not detected by the antivirus software and this modifies fields and steals all personal information.

**2.DOM module interface**

DOM stands for Document object modelling interface. It is a unified interface for building web applications using various programming languages. It is responsible for event handling. So, when the MITB Trojan attacks it, it changes the registry events and in this way, it modifies the data.

**3. Java Script and AJAX**

Java script and AJAX are the two-popular means of web application programming nowadays. The thing is that they can override the default prototyped of the DOM module interface and have the capability to perform actions that are invisible to the end user. This vulnerability is used by Zeus to perform code injection into the browser to steal sensitive data.

**4. API Hooking**

This is like HTML rewriting. In this method, the malware acts as an intermediate between the victim’s computer and the sever and it is responsible for what the user sees in the browser.

**5.Session Hijacking**

session hijacking also called as cookie hijacking is the exploitation of a valid session by gaining access to the session key. The browser cookies contain very sensitive banking information. So once if the cookies are stolen, it is possible to establish remote desktop connection and gain unauthorized access to the system[10].

**MITB Proposed Solutions**

Many solutions are available for issues relating with Man-in-the-Browser attacks but the challenge with each of these solutions is that the demerits it poses to banks and individuals makes some of them unsuitable and usable. These methods are referred to as additional safeguards because apart from the conventional login with usernames and passwords these methods add an additional layer of security to bank and their customers.

In this chapter, we will look at some suggested solutions/ safeguard methods for Man in the browser attack and critically examine if it can be implemented with minimal cost and risk to both the bank and the customers. Some of the proposed solutions to be examined are listed below:

* Anti-Virus or Anti-malware applications.
* Separate Computer used for online Banking
* Tougher Browsing methods. e.g. disabling USB drives and auto-run on systems.
* OTP token with signatures
* Out of Band transaction detail confirmation plus OTP.

**Anti-virus or Anti-Malware Applications**

Anti-virus and anti-malware software used by customers need to be installed and updated on all the machines used for online transaction so that it can help to detect any unwanted activity. The fact is that anti-virus deals with older and more established threats while anti-malware protects from latest and even more dangerous threats. Both of them can be run simultaneously on the machine without the risk of any collision or problem with the operation of the system. However, the draw back with this is that malwares are changing rapidly and it so difficult for software companies to keep up with the latest definitions available.

**Separate Computer Used for Online Banking**

The most secure way to secure financial transactions over the internet is to have a dedicated machine for interacting with online banking. This eliminates the threat of the source and so a system for this purpose cannot be used for surfing the web, or sending emails or to access any of the client’s social media accounts as this is a major entry point by man in the browser attackers today. Computers like this do not usually have an anti-virus or anti-malware installed in it and this method demands a very strict and disciplined level of compliance not to be tempted to do any other things. It is so inconvenient and even employees of the Bank don’t make use of this method in their daily dealings and business bankers with high tons of task to do will find this very rigorous to abide by.

**Tougher Browsing Methods**

This is a partial solution and not the best idea to avoid man in the Browser attacks. It can be done by directly buying changing registry information on the already existing machine which requires an expert to do and navigate, or buy buying a third- party software that enables disabling of USB drive and other components that might be connected on the machine. It is a standalone executable program and can is easy to run on your machine. However, the challenge with this method is that even though malwares find it difficult to attack this machine considering auto-run, and USB drives have been disabled, updates to anti-virus and anti-malware of system is difficult to run and exposes the system and user to other forms of attacks. This makes the computer secure from man in the Browser attacks but vulnerable to many other types of attack.

**OTP Token with Signature:**

One time password tokens are physical devices alternatively used to gain access to a restricted point, this is because it can function like a key to unlock a particular program or grant access to a particular application. It usually has a digital signature that is encrypted with a private key which is known only to the owner of the token. It serves as a proof of identity and can be used to confirm in banks where money should be transferred to. The challenge with using this method is that customers are made to input their details on the small token which in turn calculates a signature code for the customer from the information provided, this method is confusing to clients and because of the small size of the token makes the process hard for the customers.

**Out of Band Transaction Detail Confirmation plus OTP**

A method of improvement from the process described above is the OTP use in addition to an out of band confirmation. This method ensures that the customer not only receives a one-time pass code but is also sent a message through another band of communication like an SMS or a voice message indicating the summary of transaction he is about to carry out with complete details and the balance from his account. Also, a confirmation code is sent to him which will be used as a secondary means to finalize the transaction. The user can in turn review this information and continue in his browser with the financial transaction if only he is familiar with that transaction and its details. This method is a very effective method because even if an attacker gets into his browser to steal his information and passcode, he still requires the alternative method of contact used to connect with the customer which was his phone to confirm his transaction. Resetting of phone numbers being used by an account holder must be done with care and separation of duty method approvals in the bank to avoid the attacker leveraging on that to leverage on this to reset the phone number of the client before attacking him.

**Conclusion and Future Work**

MITB attacks are a global attack which are affecting all world banking security systems. Attacks became more complex, therefore, some new integrated defense strategies should be proposed for protecting bank security system effectively. OTP token with signature can take effect in online banking transactions, however, sometimes it is inconvenient. Out-of-Band transaction details confirmation with OTP can be effective in simple MITB attacks, only except combining with Man-in-the-Mobile attack, in which may be vulnerable. Therefore, the project will continue research passive counter measures, including IP-Geolocation, device-profiling and monitor user behavior. By integrated active counter measures and passive counter measures, we hope to find more effective defense strategies for protecting online banking security system with relative lower cost. In fact, the first line of defense strategies is to improve awareness to avoid clicking on unusual browser and request claiming. Comprehensive security strategies not only require the investment in technology, but also need to enact security policies against malicious code and provide security education to employees and customers.

**References**

[1] http://www.internetlivestats.com/internet-users/

[2] Chickowski, Ericka; “Man in the Mobile Attacks Highlight Weaknesses in Out -of-band Authentication,” 2010, www.darkreading.com/authentication/167901072/security/application-security/227700141/man-in-the-mobile-attacks-highlight-weaknesses-in-out-of-band-authentication.html

[3] https://www.owasp.org/index.php/Man-in-the-browser\_attack

[4] https://www.sans.org/reading-room/whitepapers/forensics/analyzing-man-in-the-browser-mitb-attacks-35687

[5]http://www.safenetinc.pt/uploadedFiles/About\_SafeNet/Resource\_Library/Reso urce\_Items/White\_Papers\_SFDC\_Protected\_EDP/Man%20in%20the%20Browser%20Security%20Guide.pdf

[6] RSA 2011 Workplace Security Report

[7] Sophos Security Threat Report 2011

[8] Microsoft Intelligence Report, Volume 9: 100

[9] RSA Anti-Fraud Command Center

[10] SANS institute “Analyzing Man in the Browser Attacks”