Journal of Humanities Insights 2(3): 146-148, 2018

Research Paper

Strategies of Safe Sign-in Online Banking for Safe Money Transaction

Gregory Timakhov, Luko Kasparov [1]

Department of Economics, Faculty of Humanities Sciences, University of Kiev, Ukraine

Received: 28 June 2018 Accepted: 08 August 2018 Published: 01 September 2018

Abstract

Nowadays, a fundamental requirement considered for a person, is known Internet Banking. However, this electronic system suffers from serious issues such as FOBIA attack. In fact, an attack in which the internet user are pushes into transport money to an account belonging to the hacker is known as FOBIA. Although, a widespread discussion is found on security imposed on FOBIA, no effective solution is suggested. In the present research a well-designed framework is provided to address the FOBIA. It means a mechanism called **Safe Mode Login Transaction (SMLT)** is presented through the study that its main purpose is to detect, prevent and recover the FOBIA.

Keywords: Internet Banking, FOBIA, SMLT

How to cite the article:

G. Timakhov, L. Kasparov, *Strategies of Safe Sign-in Online Banking for Safe Money Transaction, J. Hum. Ins. 2018; 2(3): 146-148, DOI: 10.22034/jhi.2018.70852*

1. Introduction

The Internet, due to its speed, flexibility and efficiency has been found a common tool to facilitate transactions conducted between suppliers and international corporations. Accordingly, the Internet has aided to the increased knowledge diffusion and emerging brand-new markets, so that the Internet markets and the online business are terms applied commonly. Indeed, the Internet and its productive tools play a significant role to the mentioned phenomenon [1]. The Electronic banking as a new industry takes advantage from the Internet, in order to interact through their banking accounts [2]. If there is common enthusiasm to benefit from the Internet banking, then users' confidence should be inspired that it is a reliable service. Correspondingly, it is required to warrant banks on its security [3].

An extremely large number of data on transactions are daily transferred online. It provides a unique opportunity for skilled criminal hackers to conduct cybercrimes by altering the online information system in a financial institution, transmitting a computer virus such as Trojan, manipulating the data and disrupting the performance of the information system. In fact, newborn crimes including cyber crooks, network hackers, cyber pirates, internet thieves emerged recently can threat the online information system [4].

It seems that there is a fundamental necessary for banks to take advantage of efficient security models in order to access to their banking system. Although, uncertain channels have been presented through the literature, several technologies and models are developed aiming at presenting a secure communication when numbers of transactions are increasing [5].

2. Life Cycle of Safe Mode Log- In Transaction

Four key processes are designed for SMLT mechanism. It means that SMLT comprises similarly detection, prevention and recovery steps mentioned previously in FOBIA; these key process can be expressed as follows:

2.1 Safe Mode Login (SML)

In fact, SML is a process that a user is able to log in personal banking system in safe mode. The process is found similar to the detection of FOBIA [6]. The detection is defined as a process through which the bank looks for the user who has a potential to become a FOBIA convict.

2.2 Safe Mode Alarm Reporting Technique (SMART)

The SMART process is one that performs equally as the mentioned prevention step of FOBIA. The step

[1] Corresponding author email: L.kasp.mikh@yahoo.com

through which a message is sent to authorities working in the bank as well as the nearest police station and emergency contacts, in order to prevent is known as SMART.

2.3 Safe Mode Transaction (SMT)

The situation in which a given volume of money might be transferred from the victim account of FOBIA to the attacker account of FOBIA is found safe mode transaction. All services presenting in banks can be performed in the safe mode, if they are through the SML.

2.4 Post Smart Transaction activity (POSTA)

The performance through POSTA is found equal to the recovery step of FOBIA. The recovery process is that one through which the safety of the victim can be guaranteed.

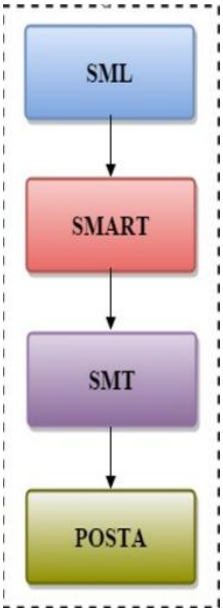

Figure 1. the life cycle of safe mode log-in transaction

3. The Framework of Safe Mode Login Transaction

Previously, it is mentioned that e-banking services can be applied by considering processes found necessary. Now, we are seeking to describe how internet banking services (for example, the fund transference) are used through the SMLT. The structure and operations can be presented through the framework of SMLT.

3.1 The performance of safe mode login transaction

The e-banking user is required to pass two process to login in mechanism known as SMLT.

3.1.1 General Login

The general log-in process is one through which the user logins generally and normally. In other words, there is a general log-in process for each e-banking user. It means that no evidence of using the SML to login is found in general log-in.

3.1.2 Safe Mode Login

A process through which the victim of FOBIA uses when he/she encounters an attack of FOBIA is found SML. Whenever we face an attack of FOBIA, the usage of the process is offered. It is required to benefit from SMLT separately, in banks. It is not operated unconsciously.

First, an internet banking ID and SML password is requisite to take advantage of SML. Indeed, SMLT uses the General log-in ID. In other words, there is a common ID for General log- in and Safe Mode Login, while passwords will be found different. It is not likely to use similar passwords. Thus, it is consistently required that the user of SMLT keeps two passwords for General log-in and Safe Mode log-in. Certain recommendations will be suggested, if there is enthusiasm to implement SMLT, successfully:

- First, the user should visit the website belonging to the bank, if the user tends to enter to the e-banking or personal banking page.
- After the e-banking or personal banking button is clicked, the log-in window is displayed. The user requires to present two types of information on the log-in page: 1) login ID 2) SML password
- ID and password are required to enter on specified parts, then they are clicked. The forget password can be recovered, whenever it is forgotten.
- The password and ID will be verified, if they are matched to saved ones in the database. If they are verified, the user will be able to enter and if not, the user will be lead to the second step
- A link is established by the bank server, after he/she login successfully, so that any services are provided to the user. This is the moment that bank has been able to detect an attack of FOBIA.
- Now, the attacker makes the victim of FOBIA to transfer money in the Safe Mode Transfer Fund service. Hence, the victim takes the process as follows:
- To add beneficiary wait until the beneficiary is added
- To transfer money after adding the beneficiary etc.
- Services applied by the victim of FOBIA are presented in Safe Mode. Therefore, services are provided by the server as follows:
- Safe mode transfer fund
- Safe mode view account transaction
- Safe mode bills pay
- Safe mode utilities
- Safe mode other services
- At this time, the victim uses all services in the safe mode called Safe Mode Transaction (SMT). Then, the account logged off, after the money transferred

successfully to the account belonging to the attacker and SMT is applied.

- Currently, POSTA is adopted to perform recovery step of SMT.
- In the present step, it is kept to wait for the victim of FOBIA to get free from the attacker. When the victim is free, a security message would be sent to the bank by its FOBIA.
- First, POSTA sizes the attacker account of FOBIA, when the security message gets to the server. Then it is turn to recovery step of SMT in POSTA. The available process of the recovery is applied by POSTA.
- It is possible that the transferred money is withdrawn before the recovery is conducted, if so then the attack of FOBIA will be declared as the Bank Robbery and the loss of payment will be paid to the victim.
- Finally, the process is accomplished through the Session-end/logout.

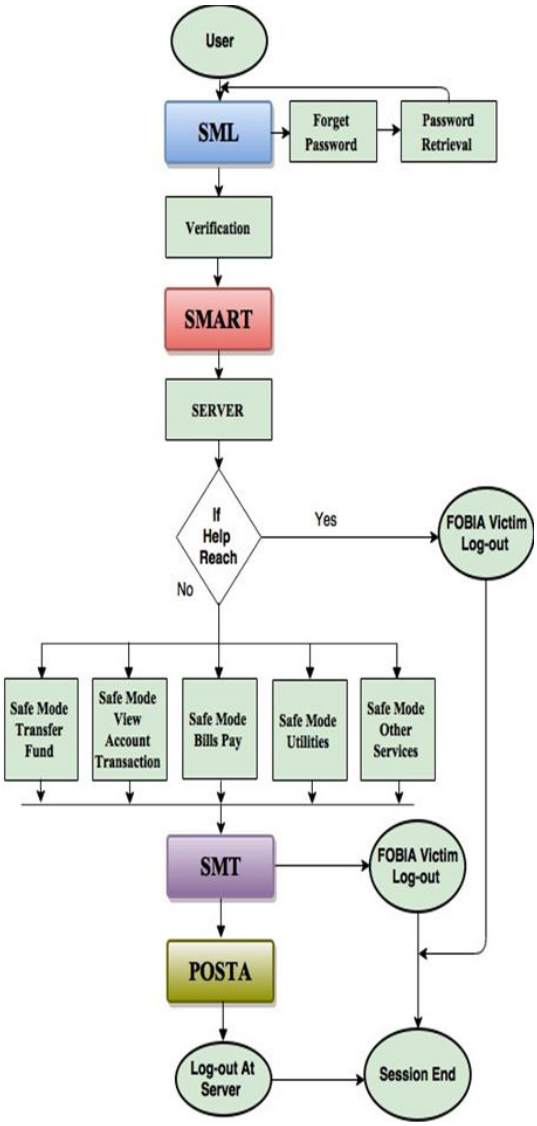

Figure 2. the framework of Safe Mode Login Transaction

4. Conclusion

Consequently, the prevention process can be established by SMLT, when FOBIA is detected. It is aided to avoid becoming a victim of FOBIA. If it so, then the recovery process of FOBIA is taken into adoption by SMLT. Hence, it is concluded that SMLT introduced as a security mechanism performs efficiently against FOBIA.

References

1. Alanazi, H. O., R. Alnaqeib, A. K. Hmood, M. A., Zaidan and Y. Al-Nabhani. 2010. On the Module of Internet Banking System. *Journal of Computing* 2(5): 133-143.
2. Omariba, Z. B., B. N. Masese and G. Wanyembi. 2012. Security and privacy of electronic banking. *IJCSI International Journal of Computer Science* 9(4), No. 3: 1694-0814.
3. Lasheng, Y. and M. Placide. 2009. Three-Tier Security Model for E-Business: Building Trust and Security for Internet Banking Services. *The 2009 International Symposium Computer Science and Computational Technology*, pp. 114-119.
4. https://sites.google.com/site/journalofcomputing/ www.journalofcomputing.org.
5. Peotta, L., M. D. Holtz, B. M. David, F.G. Deus and R.T. de Sousa. 2011. A formal classification of internet banking attack and vulnerabilities. *International Journal of Computer Science & Information Technology (IJCSIT)* 3(1): 186-197.
6. Jassal, R. K. and R. K. Sehgal. 2013. Study of Online Banking Security Mechanism in India: Take ICICI Bank as an Example. *IOSR Journal of Computer Engineering (IOSR-JCE)* 13(1): 114-121.