Framework of Safe Mode Login Transaction for Forced Online Banking Intrusion Activity

Purnima Jaiswal, Prof. (Dr.) Vijay Singh Rathore

Abstract— Internet Banking has become the person’s basic requirement in today’s era. This basic requirement of internet banking is followed by some problems like FOBIA attack also. FOBIA is a new emerging attack of Internet Banking in which the Internet Banking user is pressurized to transfer money to an unknown account from his account. If we talk of any existing security measure against FOBIA attack then we find that till now we don’t have such type of mechanism which provides a complete solution against FOBIA. In our research paper we have proposed a well planned framework of a security mechanism for FOBIA. This security mechanism performs the detection, prevention and recovery of FOBIA. We have named this security mechanism as Safe Mode Login Transaction (SMLT).

Index Terms—Internet banking, FOBIA, SMLT.

I. INTRODUCTION
Because of the speed, flexibility, and efficiency that it offers, the Internet has become the means for conducting growing numbers of transactions between suppliers and large international corporations. In this way, the Internet has opened new markets to the world and has accelerated the diffusion of knowledge. The meaning of Internet markets or online business has been widely used in these days. The success of the business depends on its flexibility, availability and security. Since that the web-based systems should have a special way to design the system and implement it. [4] Electronic banking is a new industry which allows people to interact with their banking accounts via the Internet from virtually anywhere in the world. [1] For customers to use Internet banking services comfortably, they must have confidence that their online services are trustworthy and secure. Similarly, for banks to provide Internet banking services they need confidence in the security of online.[2]

Billions of financial data transactions occur online every day of the year 24 hours a day 7 days a week and bank cyber crimes take place every day when bank information is compromised by skilled criminal hackers by manipulating a financial institution’s online information system, spreading malicious bank Trojan viruses, corrupt data, and impede the quality of an information system’s performance. Cyber crooks, network hackers, cyber pirates, internet thieves is an emerging crime category of criminals and threat to online banking information security systems.[5]

Currently there is a clear need for efficient security models by banks which offer online access to their banking systems. In face of the growing number of transactions processed through online banking systems, several new security technologies and models which aim at providing authenticated secure communications through known insecure channels have been introduced in current literature.[3]

II. LIFE-CYCLE OF SAFE MODE LOG-IN TRANSACTION

The security mechanism named as SMLT has been created by involving four key processes. It is a complete detection, prevention and recovery solution of FOBIA. The key processes of SMLT are as follows.

A. Safe Mode Login (SML)
The login of a user in safe mode in personal banking is SML. This process works for the detection of FOBIA. Through SML the bank detects that the user is becoming the convict of FOBIA

B. Safe Mode Alarm Reporting Technique (SMART)
The alarming reporting process that works for the prevention of FOBIA is SMART. Through SMART a help message is sent to the bank authorities, nearest police station and emergency contacts to prevent the execution of FOBIA.

C. Safe Mode Transaction (SMT)
Transfer of money by using SML from the account of FOBIA victim to the account of FOBIA attacker is Safe Mode Transaction. All the bank services can be executed in the safe mode through SML.

D. Post Smart Transaction Activity (POSTA)
POSTA works for the recovery of FOBIA. If FOBIA can successfully be implemented then the recovery process can be executed with the safety of the victim.

Purnima Jaiswal, Research Scholar Career Point University, Kota, India.
Prof. (Dr.) Vijay Singh Rathore, Principal, Pinkcity Engineering College & Research Center.
III. FRAMEWORK OF SAFE MODE LOGIN TRANSACTION

In the above topic it is described that how the user uses e-banking services by following a certain process. In this section we have described how the user by using SMLT mechanism uses internet banking services especially in term of fund transfer. SMLT’s framework gives us a brief introduction of its structure and working.

A. Working of Safe Mode Login transaction

In SMLT mechanism the e-banking user has two processes to login.

a. General Login

The log-in process which the user uses for general and normal use is known as General log-in. Each e-banking user has general log-in process. In another words a log-in process in which the user does not use SML for log-in also called General Log-in.

b. Safe Mode Login

The Log-in process used by the FOBIA victim at the time of FOBIA attack is called SML process. This process can only be used at the time of FOBIA attack. To avail the SMLT service the user has to apply in the bank separately. SMLT can’t be activated by default with internet banking.

In the first stage to use SMLT the user has an internet banking ID and SML password which is provided by the bank. Only the General Log-in ID is used for SMLT. It means the user will use common ID both for General Log-in and Safe Mode Login but the passwords for General Log-in and Safe Mode Login will be different. In no circumstance the passwords of both the ids will not be the same. The SMLT user has to keep two passwords always. One for General Log-in and, other for the Safe Mode Log-in.

Some steps are being used for the successful implementation of SMLT. They are as follows

- At first the bank’s website is visited by the user and then the e-banking or personal banking button is clicked on the home page.
- The login window is displayed after clicking on the e-banking or personal banking button. The user has to give two information on the login window
  - Login ID
  - SML Password
- ID in ID textbox and SML password in password textbox will be typed by the user and Submit button will be clicked. If the user forgets his/her SML password then by clicking on the forget password the user can retrieve or reset his/her password.
- The user’s ID and SML Password go to the verification after clicking on the submit button where the user ID and SML password are matched with the saved ID and password in the bank’s database server. If the matching get successfully then the user log-in, If not then in this case the user has to follow the second step again.
- The user’s link is established with the bank server after successful log-in and the user can use any services from the server and by this time the bank has detected that the user is becoming victim of FOBIA attack.
- Now the FOBIA victim uses the bank’s Safe Mode Transfer Fund service to transfer money in favor of the FOBIA attacker. The victim follows the existing process of the bank at that time. For ex.
  - To add beneficiary
  - Wait until the beneficiary is added
  - To transfer money after having added the beneficiary etc.
The services of the server used by the victim are executed in the Safe Mode. The server provides the following services to the victim –
- Safe Mode Transfer Fund
- Safe Mode View Account Transaction
- Safe Mode Bills Pay
- Safe Mode Utilities
- Safe Mode Other Services

The SMART Process gets executed at the backend of the server which works for the prevention of the FOBIA.

An alarm message is sent to the Police station, Bank authority and emergency contact by SMART until or unless responses not reached on a special number.

If the bank authority or police or emergency or any other help arrest the attacker by reaching the victim location or the attacker flees before the money transfer then the victim can log-out from the account by successfully prevention of FOBIA and at the same time on the server there is session end / log out.

If no help from nowhere reaches the victim then the FOBIA victim transfers the money in the account of FOBIA attacker.

All the services executed by the victim in the Safe Mode will be called Safe Mode Transaction (SMT). The victim log-out from the account by having successfully transferred the money safely in the attacker’s account and after having successfully execution of SMT.

Now on the server, a process Post Smart Transaction Activity (POSTA) executes which works for the recovery for SMT.

In this stage it is waited for the FOBIA Victim to be freed by the FOBIA Attacker. As soon as Victim is freed from the Attacker then a Safety Message is sent to the bank by the FOBIA Victim.

As soon as the Victim’s Safety Message reaches to the sever side, the FOBIA Attacker’s account is seized by POSTA first and then Recovery of SMT is made by POSTA. POSTA uses the bank’s existing process for the recovery of SMT.

If the FOBIA Attacker withdraws the money transferred from his account before recovery then in this case the bank declares this FOBIA Attack as Bank Robbery and pays the victim the loss of payment.

At the last stage the server ends the complete process through Session-end / Logout.

III. CONCLUSION

To sum-up we can say that SMLT starts the process of preventing as soon as it detects the FOBIA and helps the user to escape from becoming the Victim of FOBIA.

If the user becomes the victim of FOBIA then in this case SMLT execute the FOBIA recovery process. Thus we can conclude that SMLT is a complete security mechanism for FOBIA.
REFERENCES


