Enhanced Mechanism for Online Banking System through Cyber Crime Investigation

Mansi B. Joshi[#], Dr. Kuntal Patel[#]

[#]*School of Computer Studies, Ahmedabad University, Ahmedabad*

***Abstract*—Increase in the development of computer technologies has lead to an increase in the number of cyber crimes. Attacking low-security targets to access confidential data is the standard pattern of attackers. Most of the crimes take place when money is involved. The popularity of the *Online Banking System* and its increased use by customers worldwide has made this service a main target for cyber criminals.**

In this paper, we have proposed an architecture that acts as an interface between client and banking server, to investigate various kinds of attacks taking place while performing online transactions. It will perform various filtering operations to provide safe environment for transactions. It includes our newly developed concept of *Double Verification* to achieve our goal as a solution to improve security. Hence our proposed system will provide remedial measures and try to overcome some of the major issues related to cyber crimes occurring in the existing online banking facility.

***Keywords*—cyber crime, investigation, online banking, double verification, phishing, watering hole, pharming, man in the browser.**

I. INTRODUCTION

As the invention of new technologies is growing day by day, the cyber crime rate is also increasing rapidly. The use of "*Online Banking"* [1] has been preferred more, since the manual cheque payment process takes longer time. Large businesses that includes transactions of huge amount to be transferred from one account to another, primarily uses *"Online Banking".*

Online Banking System architecture differs depending on the configuration decided by the financial institutions. Thus, there is no specific architectural representation of this system. Basically, two options are available to the financial institutions for supporting their online banking services : *in-house services* and *third-party provider hosted services.* The financial institutions can choose their overall system configuration as per their need by combining these options.

A. *Third Party Provider Hosted Online Banking System*

The financial institution's network components such as online banking service website, banking server, firewall and intrusion detection system is hosted by its service provider. The institution does not have to daily supervise these components.

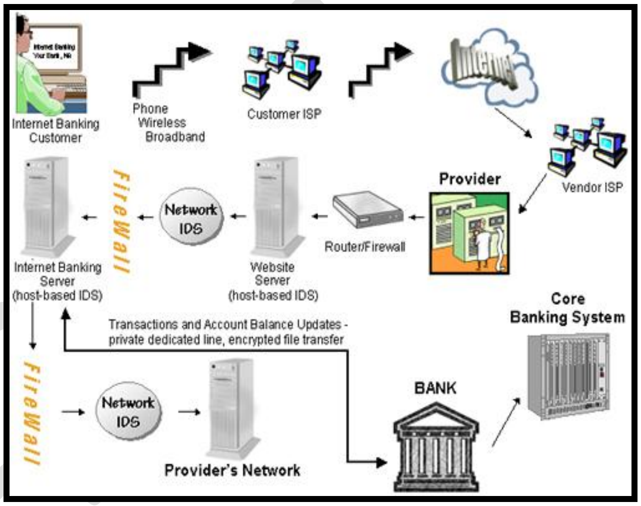

Internet Banking Your Bank, NA
Internet Banking Customer
Phone Wireless Broadband
Customer ISP
Internet
Vendor ISP
Provider
Router/Firewall
Website Server (host-based IDS)
Network IDS
FireWall
Internet Banking Server (host-based IDS)
Transactions and Account Balance Updates - private dedicated line, encrypted file transfer
Core Banking System
FireWall
Network IDS
Provider's Network
BANK

Figure-1 : Third Party Provider[2]

In this case, the customer sends a transaction request via phone or wireless broadband, through the Internet Service Provider (ISP). The request is then forwarded to the online banking service provider's ISP, through the means of Internet. The online banking service provider's ISP routes it to the provider.

The request enters the provider's network, which directs the request through the firewall to the application executing on the Internet banking server. The Internet banking server processes the request to carry out the transaction by verifying it through the core banking system containing databases.

B. *In-House Online Banking System*

The financial institution can internally host the online banking system. The provider does not act as an intermediate between the Internet access and the institution's core processing system. The institution must supervise the network components every day.

In this case, the customer sends a transaction request via phone or wireless broadband, through the Internet Service Provider (ISP). The request is then forwarded to the online banking service bank's ISP, through the means of Internet. The online banking service bank's ISP routes it to the provider. The request enters the bank's network, which directs the request through the firewall to the application executing on the Internet banking server.

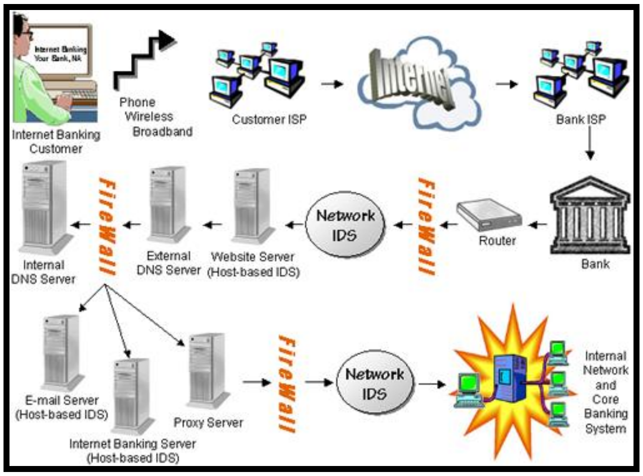

Internet Banking Your Bank, NA
Internet Banking Customer
Phone Wireless Broadband
Customer ISP
Internet
Bank ISP
Internal DNS Server
FireWall
External DNS Server
Website Server (Host-based IDS)
Network IDS
FireWall
Router
Bank
E-mail Server (Host-based IDS)
Internet Banking Server (Host-based IDS)
Proxy Server
FireWall
Network IDS
Internal Network and Core Banking System

Figure-2 : In-House Provider[2]

The bank has several application servers such as Internet banking application server, website server, e-mail server, proxy server, DNS. The router will send the transaction request around these application servers directly to the Internet banking server unless it is non-banking transaction. The Internet banking server processes the request to carry out the transaction by verifying it through the core banking system containing databases.

C. *Limitations of The Above Two Approaches*

Both the above architectures may include host-based Intrusion Detection System (IDS) in the website server or Internet banking server. Network IDS may reside within the network for checking any unauthorized activity taking place. The Internet banking server has basic filtering for managing network traffic.

There is no surety of having IDS in the online banking system architecture. Thus, there is a need of having some remedial measures for improving the safety in online transaction processing. The environment should be made more secure by eliminating some major threats in online banking.

D. *Our Approach*

In this paper, we have analyzed various threats that can exist while executing online transactions and could be a menace for the users. We are proposing an architecture which will overcome some major issues of the existing system such as *phishing, watering hole, pharming & man in the browser.* The concept of *"Double Verification"* will also be implemented for better security in our architecture.

II. PROBLEMS IN EXISTING SYSTEM

The existing system includes various problems while performing online transactions, which supports the hackers to perform unauthorized and disastrous activity. The following are four major issues which are required to be taken care of, they are :-

A. *Phishing*

Phishing [3] is a technique of sending emails posing as a reputable company in order to lure individuals to reveal personal information, such as passwords and credit card numbers, online. It leads to identity theft[4]. It is the most common technique used by hackers to fool the users. One of the common reasons found during the literature survey about phishing is the lack of proper knowledge of computer and mobile technology. Due to this reason people may click randomly anywhere on the screen and becomes the victim of phishing attack [5].

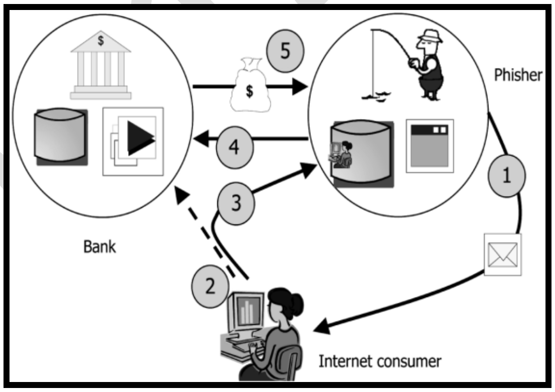


Figure-3 : Phishing Attack

In a phishing attack, a phisher sends fraud email to the internet consumer (user) pretending as a legitimate banking entity. The user gives his/her confidential details, considering the phisher as an official bank entity. Thus, the identity of the user is stolen and it is misused by the phisher to transfer money from the user's account which belongs to the official banking entity.

B. *Watering Hole*

Watering hole[6] is a technique evolved from phishing technique. Instead of luring users to visit website, this technique injects malicious code into specific web pages that are being frequently visited by users. Users get infected when they visit these web pages.

In a watering hole attack, the attacker collects the information about the sites on which he/she wants to insert the malicious code. Then, the malicious code is injected to the selected web pages. When the user visits these web pages, the injected malware gets transferred to the user's vulnerable system. With the help of this malware, attacker is now able to retrieve personal information and can perform unauthorized activities i.e. transferring balance from user's account to the attacker's account, without the knowledge of the user.

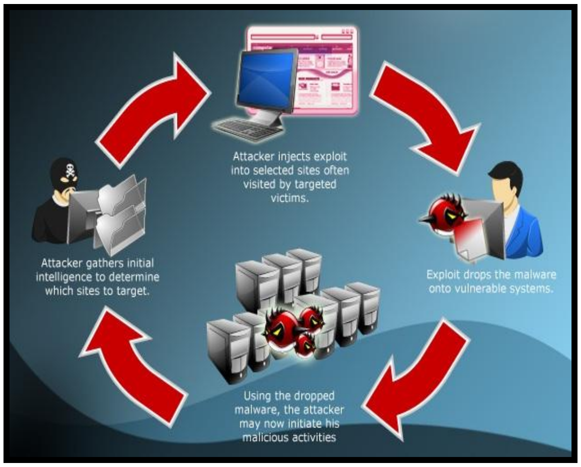

Attacker injects exploit into selected sites often visited by targeted victims.
Attacker gathers initial intelligence to determine which sites to target.
Exploit drops the malware onto vulnerable systems.
Using the dropped malware, the attacker may now initiate his malicious activities

Figure-4 : Watering Hole Attack

C. *Pharming*

Pharming is a technique in which the attacker takes control of a website so that when users try to access that website, they get redirected to the attacker's forged website. Pharming can be carried out by either changing the host files on victim's computer or by exploiting the DNS server.

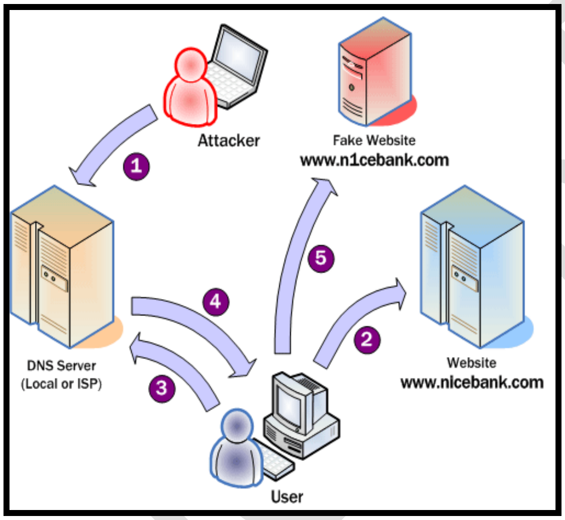
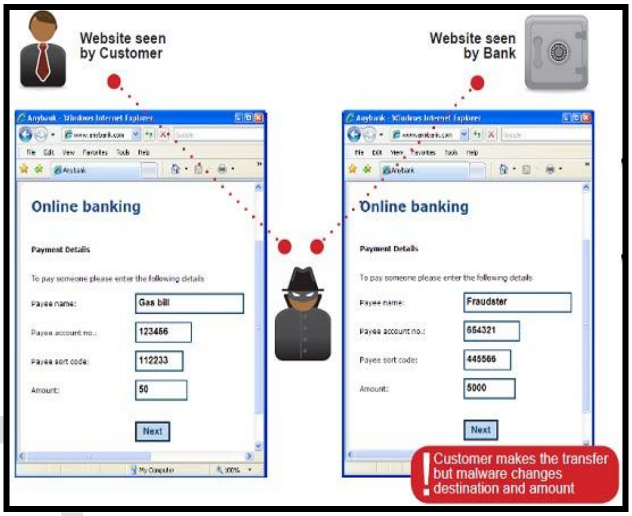


Figure-5 : Pharming Attack [7]

In a pharming attack, the attacker hijacks the host files of victim's computer or DNS server. When user tries to access an official bank website, the malicious code on the DNS server redirects the user to the fake bank website which is created by the attacker. Thus, personal information is leaked to the attacker for using it in illegal activities i.e. Credit card redirection is a new technique that can be used to steal credit-debit card information of the user.

D. *Man In The Browser*

Man in the browser is a proxy Trojan horse that infects a web browser having low security. It is the greatest threat that exists in online banking. The malicious code resides in the browser as an Active-X control, browser extension, add-on plug-in or API-hooking; and it's able to modify the original content for attacker's benefit.


Website seen by Customer
Website seen by Bank
Anybank - Windows Internet Explorer
File Edit View Favorites Tools Help
Next
Customer makes the transfer but malware changes destination and amount

Online banking

Payment Details

To pay someone please enter the following details

Payee name: Gas bill

Payee account no.: 123456

Payee sort code: 112233

Amount: 50

Online banking

Payment Details

To pay someone please enter the following details

Payee name: Fraudster

Payee account no.: 654321

Payee sort code: 445566

Amount: 5000

Figure-6 : Man In The Browser Attack[8]

In Man in the browser, during online banking, user enters the transaction details in the given transaction form on the official bank website. The data which is entered by the user in the transaction form is changed by the attacker before the transaction is completed. The attacker modifies the destination and amount entered by the user and takes advantage during the transfer of funds.

III. PROPOSED ARCHITECTURE

Our proposed system architecture will try to overcome above specified major issues in *Online Banking System*, by integrating different components. It depicts a step by step process to eliminate such issues as follows :-

A. *Eliminating "Phishing"*

In phase-I, the proposed system will take the login details from the user and verifies it from the banking server. The system will receive response of the banking server and will send the same on user's registered mobile number. This helps the user to identify whether it is authorized or unauthorized access.

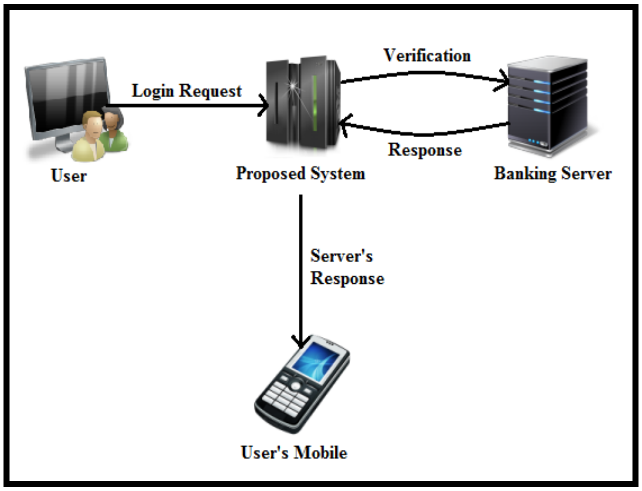


Figure-7.a : Phase-I, Login Details

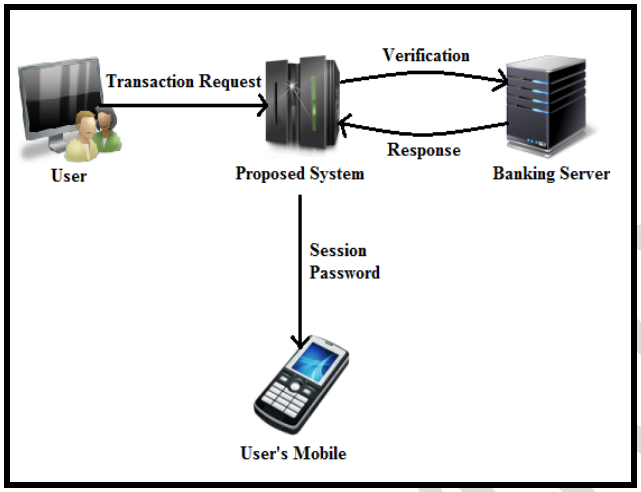


Figure-7.b : Phase-II, Transaction Details

In Phase-II, the user will be able to perform transactions. When the user request's a transaction to be processed, banking server verifies the balance and gives response to our intermediate system. Our system will randomly generate the session password and sends it to the user's registered mobile phone. For successful completion of transaction, user must utilize the session password.

B. *Eliminating "Watering Hole & Pharming"*

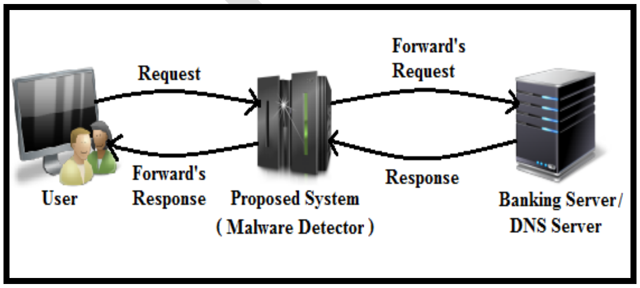


Figure-8 : Malware Detection Phase

In order to eliminate the problem of watering hole and pharming, our system will act as a malware detector to identify that the request is free of any kind of malware that may be injected to banking system. The system may use various techniques to detect malware i.e. anti-virus software, hardware address verification mechanism. Thus, our intermediate system will contain malware detection softwares to act as a filter to user's requests.

C. *Eliminating "Man In The Browser" & Foundation Of Our Proposed System Architecture*

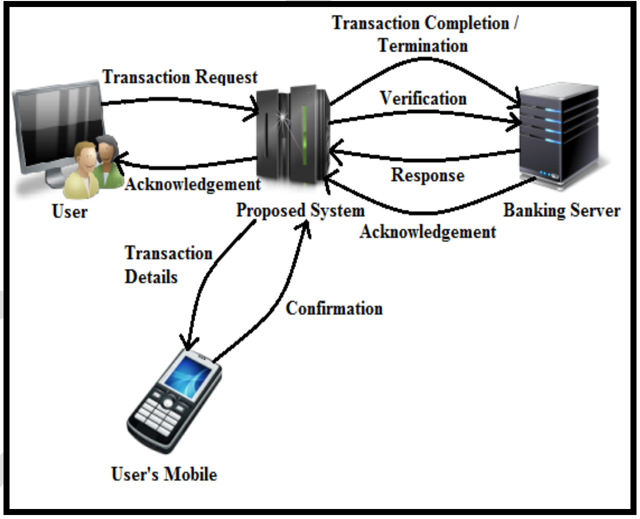


Figure-9 : Transaction Processing In Online Banking

(Model Flow of Our Proposed System)

When the user will request a transaction, the proposed system will forward the request to the banking server for verification. Banking server will send a response to the intermediate system. If the response is positive, our system will send the transaction details to the user's registered mobile number. The transaction details will include the account to which amount is to be transferred and the amount.

The transaction will only takes place when user sends the confirmation message to our system after verifying the transaction details. This will eliminate the *Man in the browser* issue; even if the attacker has changed the account details or amount, the user will identify the modification and will be able to terminate the transaction by sending negative response to our system.

Thus, this model architecture eliminates the four major issues of *Online Banking* namely *Phishing, Watering Hole, Pharming & Man In The Browser*.

IV. ADVANTAGES AND DISADVANTAGES

The proposed intermediate system has the following advantages and disadvantages :-

A. ADVANTAGES

The proposed system will increase the safety for processing online transactions as all the information will be parsed through this system. It will perform various filtering functions and security procedures to provide secure setup for online transactions.

Double Verification technique will check that the information has not been modified by external entity. Thus, it will ensure the users that the transactions are maintaining integrity. The system will try to eliminate the major issues that can lead to cyber crime by following various procedures to check information flowing from user to the banking server.

B. DISADVANTAGES

As a new intermediate system is introduced, the cost is going to rise for the complete setup. Since the information will pass through the proposed system, the online banking transactions will proceed slowly, thus reducing the speed of processing.

The major disadvantage of this system is its crash. If this system will stop working unknowingly or any kind of anonymous attack takes place on it, no transaction will be processed as the bridge between users and banking server has broken. Thus, delay in the procedure of online transactions will take place until the problem in system is solved, which may be crucial to the businesses that deals with urgent money transfer.

V. CONCLUSION

The invention of new technologies is growing day by day which has led in the increase of cyber crime rate. *Online Banking* is the prime target for cyber criminals. This paper describes a way to reduce the cyber crimes on online banking transactions. The Model architecture has been proposed to eliminate the main issues such as phishing, watering hole, pharming, and man in the browser. The model architecture describes an intermediate system between the user and the banking server. The intermediate system will act as a bridge between the user and the banking server to process the online transaction. This system has its brighter side as well as darker side. It may not be the cure for the crimes taking place in online transactions, but the system can definitely help to reduce the occurrence of it.

REFERENCES

[1] Wikipedia, the free encyclopedia. Online banking. *Wikipedia.* [Online] [Cited: March 15, 2014.] http://en.wikipedia.org/wiki/Online_banking.

[2] Federal Financial Institution Examination Council (FFIEC). E-Banking Components. [Online] [Cited: March 11, 2014.] http://ithandbook.ffiec.gov/it-booklets/e-banking/introduction/e-banking-components.aspx.

[3] Credit Counselors Corporation. Phishing Scams Lead to Identity Theft. [Online] [Cited: February 23, 2014.] http://www.cccindy.com/credit-counseling-blog/phishing-scams-lead-to-identity-theft/.

[4] Justice K.N. Basha, Judge, Madras High Court, Chennai. *Seminar And Workshop On Detection Of Cyber Crime And Investigation.* Hyderabad : s.n., 2010.

[5] Dr. Kuntal Patel, Parimal Patel, Phishing in Mobile Devices: Survey and Prevention Mechanism, IJSR - International Journal of Scientific Research, Volume:2, Issue:3, March 2013

[6] ll, Oscar Celestino Angelo Abendan. Watering Hole 101. [Online] [Cited: February 23, 2014.] http://about-threats.trendmicro.com/RelatedThreats.aspx?language=au&name=Watering+Hole+101.

[7] [7] http://www.bustathief.com/what-is-pharming-dns-poisoning/ [Cited: October 10, 2014]

[8] [8] Paganini, Pierluigi. Man In The Browser attacks scare banking world. [Online] [Cited: February 23, 2014.] http://securityaffairs.co/wordpress/17538/cybercrime/man-browser-attacks-scare-banking.html.