Journal of Internet Banking and Commerce

An open access Internet journal (http://www.icommercecentral.com)

Journal of Internet Banking and Commerce, December 2015, vol. 20, no. 3

Highlighting the Vulnerabilities of Online Banking System

LAITH T KHRAIS

Ph.D Student, Poznan University of Economics, Poland, Tel: 00962962786873979

Email: **Laithkh82@hotmail.com**

Abstract

As a result of the growing use of the Internet and developing advanced technology systems globally, there has been an apparent increase in the usage of online banking system across the world, accompanied by widespread incidents of fraud and attack. This paper gives a simple description of the online banking mechanism and the nature of the attacks that involved in the process of conducting an online transaction through a computer, along with the security models and measures that can be used to block the threats.

Keywords: **Online banking; Attack techniques; Security**

INTRODUCTION

People use the Internet for various reasons such as shopping and online banking. The importance of the Internet has been contributed in the development of the banking system environment, which it played an important role in the globalization of the banking system. Hoehle [1] suggested that all research related to e-banking encompasses various disciplines of marketing, e-commerce, information system, business and management. Global Internet users are increasingly spending more time online. Because of this, the banks in most countries provide their services online to keep their online customers. This helps those users to perform most of their banking transactions only by visiting the bank’s website, and without being physically present in the bank. These factors facilitate business affairs, including the process of buy and sale, hence increasing the competition between banks and other financial institutes.

Online banking is an emerging form of digital banking aimed to provide banking services through electronic technology devices. It is considered to be a prerequisite for e-commerce, which grows as Internet banking becomes more widespread. It has also been defined as providing customers with banking operations and services directly through interactive Internet communication channels, or employing a new method of financial and banking services, thus it can achieve the desired satisfaction in terms of speed, accuracy, ease of use, and security, with the minimum need of physical presence in the bank. The online banking system provides benefits for banks as well as their customers. It enables to achieve results with the highest potential from sales transactions with the lowest possible cost and by reducing the physical facilities and resources required by the staff and reducing the waiting time in bank branches [2]. Regarding the customers, it enables them to perform electronic transactions at any time and place through the bank’s website. Therefore, it is not surprising that the banks globally are continuing to shift towards online services.

Banks can achieve a better performance, by having an accuracy in record keeping with secure transactions, keeping and maintaining the privacy of information and providing the services within the due time has a larger number of satisfied the online subscribers [3,4]. It also provides a protection against fraud and hack the personal account which prevents a third person to access the financial accounts and its misuse.

The number of attacks directed against the Internet users is continuously growing. Their computers are constantly targeted by viruses, worms, port scanning software, spyware, adware, malware, keyloggers. Some reports indicated that an unpatched Windows PC will be compromised within 12 minutes of connecting to the Internet. Therefore, financial providers need to guard against various types of online attacks and secure the online transaction become a major requirement and a new standard in the evaluation of the competitiveness for any banking online service provider.

Online banking system mechanism

Online banking is a series of processes that the client logs into the bank’s website through the web-browser installed on the PC and carries out various online transactions by using a private username and password. Online banking is carried out in four main phases illustrated in Figure 1.

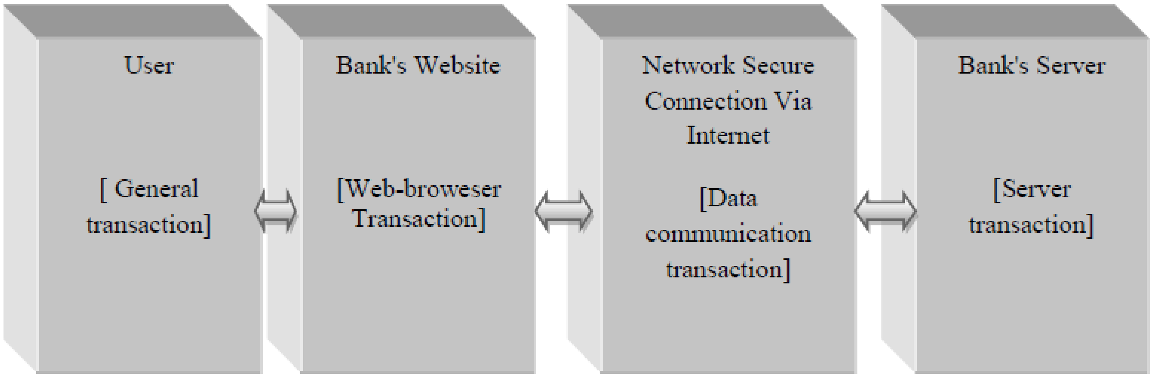
User
[General transaction]
Bank's Website
[Web-broweser Transaction]
Network Secure Connection Via Internet
[Data communication transaction]
Bank's Server
[Server transaction]

Figure1: Online banking transaction

1. The computer's user runs on the installed operating system.
2. After the web-browser opened, users can access the bank's website and then enters the personal identifying number (PIN) and the password by using the keyboard.
3. The data input is encrypted by SSL (secure socket layer) and transmitted to the bank's server.
4. The bank's server decrypts the transmitted information and processes of the user's authentication.

The nature of attack techniques

Currently there is a clear need for efficient security procedures by banks which offer online access to their systems. In the face of the growing number of online transactions that are processed through banking systems, several new security technologies and procedures which aim at providing authenticated secure communication against the number of malware that exploit online banking system vulnerabilities. In order to propose the security models and solutions in general, it is first necessary to understand and determine the existing attack methods and vulnerabilities on which they are based. Hence, the attack strategies and techniques can be divided into three main vectors that can be used against online banking systems, such as:

- Firstly, a credential stealing attack (CSA), is where fraudsters try to gather users' credentials, either with the use of a malicious software or through phishing.
- Secondly, a channel breaking attack (CBA), involves intercepting the communication between the client side and the banking server, by masquerading

as the server to the client and vice versa.
• Thirdly, a content manipulation also called man-in-thebrowser (MiTB) attack, it takes place in the application layer between the user and the browser. The adversary is granted with privileges to read, write, change and delete browser's data whilst the user is unaware about it.

It is well-known that attacks against online banking systems are mostly cases dangerous. Alongside, financial firms are reluctant to report the hacker attacks to keep their reputation highly, retain the existing of online users and attract new users. Therefore, the online banking systems should be imposed an effective security procedures capable of identifying users and authorize a variety of transactions, thus mitigating fraud. Basically, banking systems need to verify user identity accurately to give an access permit to do banking transactions. The identification schemes are based on two main factors: unique secret information previously shared by the user and the bank "passwords" and unique characteristics of the device which is being used to access the service "device fingerprinting". However, if any of this information is compromised, including the user's device, the security system is compromised as a whole because it could allow the adversary to insert and capture information at a point of the system.

TYPES OF ONLINE ATTACKS

Most of the hacking tools are placed on the web, and they are downloaded into the user's PC when the user opens the web or e-mail. These tools can easily capture the password, account number, and personal data which the user entered. Moreover, they are even capable of replacing the input screen, and make the user see a counterfeit website of the bank which the hacker had installed in advance. For example, the hacking tool for online banking called, Zeus, contains a technology that detects and avoids the Anti-Malware software, and is constantly spreading new breeds or variants of Zeus mostly through famous websites, fake websites, phishing sites, emails, etc. Furthermore, the nature of attacks is more active and riskier than the past. Here are some types of attacks divided into two groups:

External attacks

Trojan attacks: The attacker installs a Trojan, such as a key logger program on a user's computer. This occurs when the users access to certain websites and downloaded programs. As they are doing this, the keylogger program is also installed on their computer without their knowledge. When the users log into their bank's website, the information in during that session will be captured and sent to the attacker. Here, the attacker uses the Trojan to make any illegal transactions at any time wants.

Man-in-the-middle attack: Here, a fake website is created to get the attention of users to this website. Normally, the attacker is capable to trick the users by disguising their identity to make it appear that the message was coming from a trusted source. Once successful, instead of going to the designated website, users don't realize that they actually entered into the fraudster's website. The information in during that session will be captured and sent to the attacker, then to do any illegal transactions at any time wants.

Malicious hackers: It refers to those who breaks into computers without a proper authorization. They can include both insiders and outsiders. Hacking as an activity has become more prevalent after the advancement in connectivity among computers. This allowed hackers to access the computer victim's remotely. Hackers can break into computer systems or supporting equipments like switches or routers, and that could entirely damage the reliability of the network.
Guessing passwords: Using software to test all possible combinations to gain entry into a network.

Phishing attacks: With the massive quantity of personal information being kept by various institutions (i.e. government and private), the protection of personal privacy became a big responsibility. Misuse personal details like social security numbers, driving license, bank accounts, etc. to conduct the fraudulent transactions. Phishing is one of the mechanisms that fraudsters use to obtain customers personal details leading to its use for fraudulent activities. For example, a phishing attack takes place when a user receives a fraudulent email (often referred to as a spoof email) representing a trusted source which leads to the fraudulent website used to collect a personal information. Most of the senior bankers felt that phishing is considered as a threat factor to the online banking services and they also felt that most of the customers have low knowledge levels about it.

Sniffers: It has also known as network monitors, this is software used to capture keystrokes from a particular PC. This software could capture login IDs and passwords.

Brute force: A technique to capture encrypted messages, then using a software to break the code and gain access to messages, user ID's, and passwords.

Worms: Destructive programs that replicate themselves without requiring another program to provide a safe environment for replication.

Logic Bombs: Designed to activate and perform a destructive action at a certain time.

Internal attack

Fraud or theft: Computer software could misuse to conduct the frauds, which is normally committed by insiders who could be employees or persons having access to computer networks internally. An insider attack is more serious in nature, because internal system users have knowledge of the system and access. So it's not easy of detecting them. Banks systems should contain preventive procedures to protect their online systems from exploitation both internally and externally.

Back doors or trap doors: Typically a password, known only to the attacker, that allows access to the system easily without a problem with the security procedures.

Errors and omissions: The integrity of information systems and data could be threatened due to errors and omissions, which is usually occurring during the capture of data. It could be either intentional or unintentional from the part of the user and detecting errors could be difficult occasionally. Computers lack the intelligence to detect and correct errors that are a part of the user inputs sometimes.

Employee sabotage: Disgruntled employee unhappy with his management maybe is trying to damage the information system resources available at his disposal as a display of revenge. Although this type of threat is less compared to other threats, it is still forming a threat to the company, which has to be observed, particularly when there is a strike call by workers or when an employee is fired as a part of downsizing exercise, such as:

- Destroying hardware or facilities
- Planting logic bombs
- Entering data incorrectly
- Deleting data
- Holding data hostage
- Changing data

In general, all commercial operating systems have vulnerabilities, also known as weaknesses in the computer system [5]. These vulnerabilities create an opportunity for possible threats to these systems. Security threats can be classified into several categories from internal to external, human or non-human, and intentional or non-intentional [6,7]. These threats could lead to the possibilities of disclosure, modification, destruction, or denial of use of that information.

THE SECURITY MODELS AND MEASURES

From the threats above, it became obvious that there is an urgent need for efficient security models by banks which offer online access to their banking systems. The online banking is carried out through a series of transactions in various environments between the end user and the system, and these transactions are always vulnerable to attacks from hackers. It must protect the end users of online banking with a multi-faceted security solutions that understands all the trends of hacking and gathering all the technologies that can ensure security for end user's data input, security for web browsing, and security for the connection network used.

Online information security is the protection of information systems used to transmit and store data during the series of transaction from unauthorized access and penetration. It is concerned with the protection of three characteristics of information: confidentiality, integrity and the availability through the use of technical solutions and managerial actions [8]. In sum, a solution that does not understand the specific attack techniques and the entire process of online banking transactions cannot provide countermeasures tools to block many attacks. The models adopted in online banking systems are based on several layers of security, consist of multi solutions and mechanisms which aim at protecting the online banking applications and the user's data in the whole process, such as:

Digital certificates

It is used to authenticate both the users and the banking system itself. This kind of authentication depends on the existence of a public key infrastructure (PKI) and a certificate authority (CA), which represents a trusted third-party who signs the certificates attesting to their validity.

One-time password (OTP) tokens

It is commonly used as a second authentication factor, this kind of devices renders the captured of authentication data useless for future attacks through the use of changing passwords dynamically which can be used only once.

One-time password (OTP) cards

It is a less expensive method for generating dynamic passwords, also providing a second authentication factor. However, in some banking systems, passwords generated by the (OTP) cards are reused a number of times before being discarded.

Browser protection

In this model, the system is secured at the Internet browser level, which is used to access the banking system. The user and browser are protected against known malware by monitoring the memory area allocated by the browser in order to detect such malware.

Device register

This method restricts access to the banking system by known and pre-registered devices only. Hardware fingerprinting techniques are used in conjunction with user identification through secret credentials.

Completely automated public turing test to tell computers and humans apart (CAPTCHA)

The CAPTCHA has been implemented to prevent automated scripts (Bots) from jamming registration or login page. It is a method recently adopted in some banking systems whose objective to make electronic attacks against authenticated sessions ineffective. This method requires the user legitimacy to input information turned into scrambled images which are difficult for automated robots to process it.

Short message service (SMS)

This method has been applied in some banking systems to notify users about transactions requiring their authorization. It provides a second authentication channel for transactions that fit certain characteristics by sending a set of characters to the user in order to have authorize and process the transaction through the online banking system.

Device identification

This identification model is based on physical characteristics of the user’s device through which it is possible to identify the information about its origin and history.

Pass-phrase

It is a security model based on information held by the user. It is usually used as a second authentication method in a transaction that involves money movement.

Positive identification

It is a model where the user is required to input some secret information only known to the same user in order to identify himself.

Biometric authentication technology

Biometric has been identified as one of the potential technologies to improve the security. It is an automated method to distinguish the customers through their biological characteristics and traits such as fingerprints, finger vein patterns, retina, and voice recognition. Biometric characteristics are unique for each person and difficult to forge, which is why biometric verification and authentication is commonplace in immigration control, law enforcement, and forensic studies. Consequently, banks are also moving towards the use of biometric identification technology because of its ability to offer more advanced security.

CONCLUSION

With the explosive spread of the Internet and electronic financial transactions such as online banking have become a universally accepted common practice. The online security service has become an essential requirement and a new directive critical in the evaluation of the competitiveness of an online banking service and other financial institutions. Therefore, the providers of online banking services should be more responsive to security requirements, and makes the online transaction have a layered protection against security threats. The necessity for a strong authentication solution became inevitable in banking services because of the growing pace of the transition technology adoption along with the unfortunate rise in fraud and security breaches. The strong authentication such as two factor authentication, usage of biometrics and quantum cryptology along with a proper way of customer sensitization are important to increase security and reduce the stealing of customer data. Banks should take the security considerations as part of their service offerings. Accordingly, it is obligated to provide a safe banking online environments based on the advanced security procedures.

REFERENCES

1. Hoehle H, Scornavacca E, Huff S (2012) Three decades of research on consumer adoption and utilization of electronic banking channels: A literature analysis. Decision Support Systems 54: 122-132.

2. Sarel D,Marmorstein H (2003) Marketing Online Banking Services: The Voice of the Customer. Journal of Financial Services Marketing 8: 106-118.

3. Zeithaml VA, Parasuraman A, Malhotra A (2002) Service Quality Delivery through Web Sites: A Critical Review of Extant Knowledge. Journal of the Academy of Marketing Science30: 362-375.

4. McKitineyV, Yoon K, Zahedi FM (2002) The Measurement of web customer satisfaction: An expectation and disconfirmation approach. Information System Research 13: 296-313.

5. Landwehr C (2001) Computer security. International Journal of Information Security 1:3-13.

6. Loch K, Carr H, Warkentin M (1992) Threats to Information Systems: Today's Reality. Yesterday's Understanding.MIS Quarterly 17: 173-186.

7. Whitman M (2003) Enemy at the Gate: Threats to Information Security. Communications of the ACM 46: 91-95.

8. Gordon L, Loeb M (2002)The Economics of Information Security Investment. ACM Transactions on Information and System Security 5: 438-457.