IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A STUDY OF VULNERABILITIES IN ONLINE BANKING: BANKING THREATS AND SELF-PROTECTION TECHNIQUES

[1]Archana Srivastava, [2]Dr. Akhilesh Kumar

[1]Research Scholar, [2]Assistant Professor
[1]Computer Science,
[1]YBN University, Ranchi, India

Abstract: Online banking has become daily routine of customers using banking services. This service is very useful for all category of customers as it saves time. Every service has its drawbacks also, same in Online banking also, It is Vulnerable with theft and attacks. In this paper we have discussed about various banking attacks and different self-protection techniques**.**

Index Terms **- Online banking ; Attacks; Protection Techniques; vulnerability; threats ;theft ;data.**

I. INTRODUCTION

The cornerstone of any successful relationship is trust. These words can be proven with the example of relationship between a customer and a financial service provider. Without the self-confidence that their monetary data is safe, Consumers would be less expected to use online services.[1]. If customers will not use online banking services provided by different banaks then it will affect bank's reputation[2]. Security fissures can have a broad impact on not only the finances of a company, but also its reputation[3].

With the help of online banking only we can do lot of transactions such as banking, shopping, bill submission etc. [4] So the trust on online banking is very important. Online banking is also referred as Virtual Banking, electronic banking, Internet banking, Web banking, Cyber Banking, e-Banking. [https://en.wikipedia.org/wiki/Online_banking]

A faithful computer system is the system that we trust to deliver its services. Dependability includes availability, reliability, safety, and maintainability. This is not surprising considering the highly valuable information that all FSPs collect and maintain on a daily basis. According to a February 2010

report by Javelin Strategy & Research, total financial losses from identity fraud was $48 in 2008 and it increases to $54 in 2009

Expert criminal hackers can compromise bank information by manipulating the online information system of a financial institution, transmitting malicious viruses, corrupting data and degrading the consistency of the output of an information system [5]. There are now a wide range of cyber threats that can be very risky not only for large corporations, but also for regular users, who can be a possible target of cyber criminals while using an insecure sensitive data entry system, such as username, password, credit card numbers, etc.

There are different threats like Distributed Denial-of-Service attacks, Malware, botnets, phishing, IP-Communication threats etc. All of these risks aim to break one of the following criteria: anonymity, authenticity and accessibility.[6]

To continue its development, the security and privacy features relating to e-banking need to be improved quickly. Building a system 1 that can attest to the identity of both the sender and the recipient by a trustworthy third party who holds the identity certificates is therefore very necessary. To mitigate possible security vulnerabilities, many suppliers have built variants in order to moderate them.[7]We need to have some strong self-protection techniques to save our data.

In this paper I will discuss about various banking threats and different self-protection techniques to protect our data.

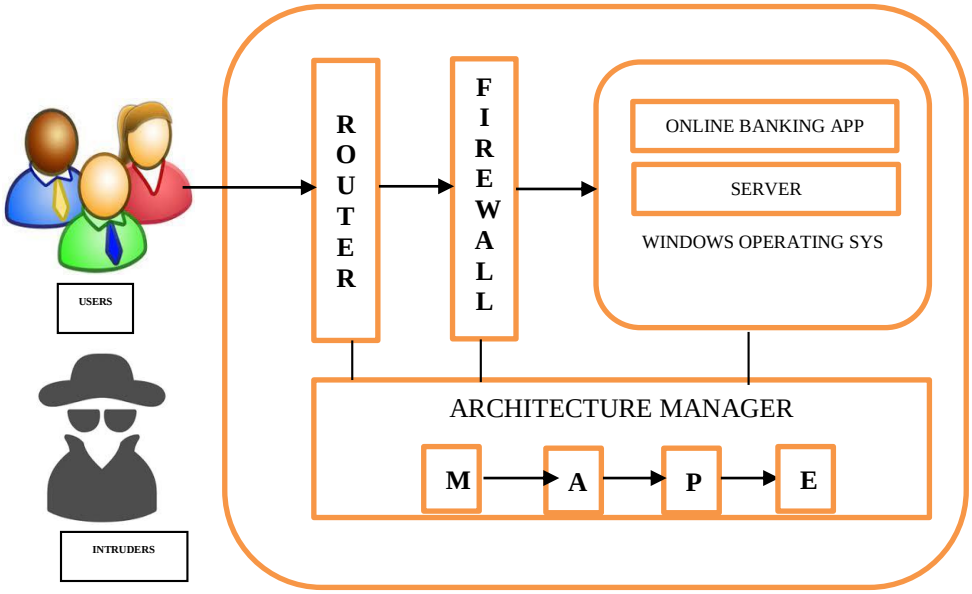

Figure: Online banking & Theft Process

SOFTWARE VULNERABILITY (DEFINITION)

Vulnerabilities of Software In several different ways, the word 'vulnerability' is sometimes used in connection with computer security. Some breach of a security policy is connected with it. This may be due to lax rules on protection, or there may be an issue inside the program itself. In principle, vulnerabilities in present in all operating systems.
Shirey [1] defined software vulnerabilities as defects or weaknesses in system design, implement or operation management and can be used to break through security policies. [R. Shirey. Internet Security Glossary. RETF RFC2828, 2002]

A universal vulnerability is a state in a computing system (or set of systems) which either allows an attacker to execute commands as another user, or to access data that is contrary to the specified access restrictions, or to pose as another entity to conduct a denial of service. [8]

An exposure is a state in a computing system (or set of systems) which is not a universal vulnerability, but either allows an attacker to conduct information gathering activities or hide activities or includes a capability that behaves as expected, but can be easily compromised.[9]

II. DIFFERENT BANKING THREATS

2.1. PHISHING:

Phishing Banking Threat is related to sending fake email. Criminal sends fake email to various users and those mails are very lucrative, and if user clicks on those mail criminals can get their personal details. In the article “Banking Securely Online” which was in US, it was mentioned that if we setup a Online Banking account, we are likely to get this type of mail and if we will click on it , it will work as same as banking site and we may share our personal details and in very short time hacker can steal our money.

2.2 PHARMING:

Pharming is very similar to phishing but it is a advance technique to steal users data. It is an assault on an operating system's name resolution system that results in a fake IP address for a certain domain[10]. There's also a more advanced and hazardous attack that targets name servers rather than the operating system. The attack is known as DNS poisoning in this scenario, because it affects all customers that utilise the attacked name server.

2.3 MALWARE

It is designed with the intention to steal online banking credentials. Malware-infected end user devices, such as PCs and mobile phones, represent a threat to your bank's cyber security every time they connect to your network.[11] Sensitive data goes across this connection, and if the end user device has malware placed on it, that malware could attack your bank's networks if it is not secured properly.

Some infamous examples of banking malware include:

- **Zeus:** a trojan that recruits infected machines into an enormous botnet, and uses website monitoring and keylogging to steal banking credentials.
- **Qakbot:** created by hacker collective Mealybug, Qakbot incorporates worm characteristics to spread and is designed to collect banking credentials.
- **Ramnit:** a file infector that spreads mostly through removable drives. It collects a variety of login details, including those belonging to online banking.

2.4 THIRD PARTY SERVICES THAT AREN'T SECURE

In order to better serve their customers, many banks and financial institutions use third-party services from other providers. However, if those third-party providers don't have adequate cyber protection in place, your bank could be the one to bear the brunt of the damage[12]. Before deploying third-party solutions, it's critical to consider how you can defend yourself from security vulnerabilities posed by them.

2.5. DATA THAT HAS BEEN MANIPULATED

Hackers don't always go in to take data; sometimes they just want to tweak it. Unfortunately, this form of attack is difficult to identify immediately away and can cost financial organisations millions, if not billions, of dollars in losses. Because altered data doesn't always appear to be different from unaltered data on the surface, it might be difficult to tell what has and hasn't been changed if your bank has been hacked.

2.6 SPOOFING

Spoofing is a newer sort of cyber security problem, in which hackers imitate a banking website's URL with a website that appears and functions identically. When a user submits his or her login information, hackers steal it and store it for later use. Even more worrying is the fact that modern spoofing techniques do not rely on a slightly different but similar URL to target viewers who have already visited the right URL[13].
It is critical for you, as a bank or financial institution, to identify strategies to limit cyber security threats while still providing your consumers with easy, technologically sophisticated solutions. SQN has collaborated with Q6Cyber, a leader in the cyber security business, to help provide greater security against potential data breaches.

2.7. PASSWORD DATABASE THEFT –

User credentials are a valuable commodity, and many cybercrime rings exist only to get this data and sell it to the highest bidder or use it to gain access to user accounts. Hackers steal user information and passwords from one website's operator in order to gain access to other websites. Because many people use the same user ID and password for many sites, the attacker can access the victim's other accounts[14].

The Sinowal Trojan is a well-known cybercrime attack that has resulted in the theft of login credentials for over 300,000 online bank accounts and nearly as many credit card accounts. It was developed by a cybercrime group several years ago. In late 2009, phishing attempts targeted Microsoft Hotmail7, Google Gmail, Yahoo, and AOL, exposing thousands of email account user IDs and passwords.

2.8. IDENTITY THEFT:

According to the article "Online Banking—Advantages and Disadvantages" published on Financial Web, a financial institution may use cutting-edge security techniques to protect your information, but once you have your account available online, your information is vulnerable to hackers. Computer fraudsters are constantly attempting to circumvent existing security methods, and if your financial accounts are stored on a bank's server, they may be vulnerable to theft. All of your personal information associated with your account, including your Social Security Number, is also at danger.

2.9. ACCESS

You can access your account 24 hours a day, seven days a week, and 365 days a year with online banking. You can use your online checking account to pay bills online. You have the ability to transfer funds, update your personal account preferences, and check current account statements at any time.

Figure: Various Banking Threats

2.10. MAN-IN-THE-MIDDLE ATTACKS

The term "man-in-the-middle" (also known as MITM) refers to when communication between two parties is intercepted. This allows cybercriminals to not only spy on your conversations but also alter them for their own evil goals if they can successfully impersonate each endpoint (in this case, you and your bank). For example, you may believe you're speaking with your bank over a secure connection, but the communications are being delivered and received by the attacker[15]. The attack is carried out directly in your browser in the event of "man in the browser" attacks. SSL encryption, which is supposed to protect you from traditional "man in the middle" assaults, is rendered useless in this situation.

III. SELF PROTECTION TECHNIQUES

3.1 USING GENUINE ANTI-VIRUS SOFTWARE:

Always use real anti-virus software to safeguard your computer from phishing, malware, and other security risks. Antivirus software assists in the detection and removal of spyware that can steal your personal information.

3.2 AVOID USING PUBLIC WI-FI OR USE VPN SOFTWARE

The most serious danger of an unsecured Wi-Fi network is that a hacker may easily sit between the end user and the hotspot and track all of the data. Hackers perceive an unsecured connection as an opportunity to infect your device with malware. As a result, you should avoid using public Wi-Fi hotspots for online or mobile banking, as well as making payments on ecommerce sites.

If you use public Wi-Fi frequently, though, you should install VPN software on your computer. It offers a safe environment.

3.3 CHECK YOUR ACCOUNT REGULARLY

On their websites, most banks have a 'last logged in' or 'login history' tab. So, if you find any inconsistencies, reset your password right away and contact your bank.

3.4 REGULAR CHANGES AND STRONG PASSWORD IS REQUIRED:

This may looks old method, but it is critical to protect your account and retain anonymity. And, of course, don't give out your personal information to anyone. Your bank will never ask for sensitive information over the phone or via email[16]. Make sure your banking passwords are kept private if you've written them down in a notepad or a diary. Also, make sure your passwords are strong and long.

Figure: Various Self Protection Techniques

3.5 AVOID SIGNING-IN TO YOUR NET-BANKING ACCOUNT VIA MAILERS

It is always safer to type the bank URL directly into your browser rather than being led to it via a promotional email or any third-party website[17]. A bank will never ask you for your account login details, as previously stated. So, if you receive a bogus email offering to redirect you to your bank's website, and you enter your personal information on the landing page after clicking it, your login is at danger.

3.6 AVOID PUBLIC SYSTEMS TO LOGIN FOR NET BANKING

If you're using a public computer, you're more likely to have your login information stolen. If you must log in from these locations, make careful to clear the cache and browsing history, as well as erase all temporary files from the computer. Allowing the browser to remember your ID and password is also a bad idea. Alternatively, you we may use incognito mode.

3.7 SUBSCRIPTION FOR MOBILE NOTIFICATIONS

Any questionable transaction will be instantly alerted to the user via these notifications. Whether the transaction exceeds or falls below the specified limit, you'll receive an alert with the remaining account amount. Not only will the bank notify you of transactions, but it will also notify you of failed login attempts to your net-banking account.

3.8 ALWAYS LOG OFF:

After you've finished your online banking, always remember to log off and close your browser. This will clear the workstation's memory of all evidence of your stopover.

3.9 PASSWORD-PROTECT YOUR COMPUTER:

Always protect your system by a Password and never share it with others. This can help to keep safe your system from other customers who may use it , if it is stolen or left unattended.

3.10 AVOID USING ADMINISTRATOR MODE:

Use administrative mode carefully, since anyone who gains access to it will have practically unrestricted access to downloaded software and stored data. For everyday use, it's significantly better to create a user account and log in with it. [18].

3.11 BE AWARE TO POTENTIAL FRAUD:

Be aware that certain phoney websites exist with the intent of impersonating you and collecting your personal information. Links to such websites are occasionally included in e-mail communications purporting to be from financial institutions or other reputable organisations[19]. Even if it appears to originate from your bank, never click on a link embedded in an e-mail.

Phishing attacks employ spam e-mails to entice you to click on links that can download malware straight to your computer or redirect you to a bogus website[20]. As a result, every e-mail received from an unknown source should be deleted as quickly as possible for security reasons. There is a spam filter that may isolate spam e-mail into a distinct spam folder, allowing you to readily recognise it. Protecting your system from phishing attacks is as simple as removing unwanted spam without reading it.

IV. FUTURE SCOPE

In future we can develop a strong self protection technique to add something like biometrics. As we all know two major category of biometrics are used i.e Thumb Impression and Face Recognition system. By adding this we can protect our data in more secured way.

V. CONCLUSION

In this paper I have discussed about Online Banking, what is it how it works. Then I have discussed various banking Threats for various category of users. Then I have discussed Various Self Protection Techniques by using which a user can protect their data. I have also discussed what else could be added to protect users data because Banking Services are most important part of our life

REFERENCES

[1] Top Online Banking Threats to Financial Service Providers in 2010.

[2] "Impact Of Online Banking Services: A Study", Dr. G. Nedumaran, Baladevi Kaleeswaran, Department of Commerce, Alagappa University,Karaikudi December 2017, ISBN: 978-81-935783-1-5

[3] "E-Banking concept", Mohd. Abdul Taufeeq, Excel Journal of Engineering Technology and Management Science (An International Multidisciplinary Journal) Vol. I No. 10 June – July 2016 – 17, ISSN 2277-3339

[4] "Security in Online Banking Services – A Comparative Study", Samir Pakojwar, Dr. N. J. Uke, International Journal of Innovative Research in Science, Engineering and Technology, Vol. 3, Issue 10, October 2014

[5] "Software Vulnerabilities, Banking Threats, Botnets and Malware Self-Protection Technologies", Wajeb Gharibi, Abdulrahman Mirza, International Journal of Computer Science Issues, Vol. 8, Issue 1, January 2011 ISSN :1694-0814.

[6] "A Survey on Online Banking System Attacks and its Countermeasures",Navjeet Kaur, International Journal of Computer Science and Network Security, VOL.15 No.3, March 2015 ,pp: 57

[7] "Enhancing Protection Techniques of E-Banking Security Services Using Open Source Cryptographic Algorithms", Adel Khelifi, Maher Aburrous, Manar Abu Talib, 14th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing-2013

[8] "E-BANKING FRAUDS AND FRAUD RISK MANAGEMENT",Rupesh. D. Dubey,Dr. Anita Manna, Tactful Management Research Journal,ISSN-2319-7943

[9] A Systematic Survey of Self-Protecting Software Systems ERIC YUAN, NAEEM ESFAHANI, and SAM MALEK, "ACM Transactions on Autonomous and Adaptive Systems, Vol. 8, No. 4, Article 17-January 2014

[10] "Comparitive Study of Online Banking Security System of various Banks in India", Rajpreet Kaur Jassal, Dr. Ravinder Kumar Sehgal, International Journal of Engineering, Business and Enterprise Applications (IJEBEA)-2013, Page 90 ISSN (Print): 2279-0020

[11] "Software Vulnerabilities, Banking Threats, Botnets and Malware Self-Protection Technologies", Wajeb Gharibi, Abdulrahman Mirza, International Journal of Computer Science Issues, Vol. 8, Issue 1, January 2011 ,pp 236

[12] "Enhanced Authentication In Online Banking ", Gregory D. Williamson, Journal of Economic Crime Management Fall 2006, Volume 4, Issue 2

[13] "Online Banking and Cyber Attacks: The Current Scenario", Dr. Manisha M. More Meenakshi P. Jadhav Dr. K. M. Nalawade, International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 12, December 2015

[14] "Considerations Regarding the Security and Protection of E-Banking Services Consumers' Interests", Vrincianu, Marinela , LianaAnica-Popa, The AMFITEATRU ECONOMIC journal-2010, pp 388-403.

[15] "E-Banking: Security risks, previsions and recommendations", Meriem Tabiaa , Abdellah madani , Najib El kamoun , International Journal of Computer Science and Network Security November 2017, VOL.17 No.11, 189

[16] "Analysis of new threats to online banking authentication schemes", Oscar Delgado , A. Fuster-Sabater , J.M. Sierra , ACTAS DE LA X RECSI, SALAMANCA, 2008

[17] " Customers' perception of information security in internet banking", Nikola Milosavljević, Sara Njagojević, "Advances in Economics, Business and Management Research, volume 108-SENET 2019

[18] [18] "Cyber Security Analysis of Internet Banking In Emerging Countries: User and Bank perspectives ", Zafar Kazmi , Jaafar M. Alghazo , Ghazanfar Latif , "2017 4th IEEE International Conference on Engineering Technologies and Applied Sciences (ICETAS)

[19] Electronic Banking: Impact, Risk and Security Issues Teju Kujur , Mushtaq Ahmad Shah , International Journal of Engineering and Management Research Volume-5,October-2015, Page : 207-212

[20] "What obstruct customer acceptance of internet banking security and privacy, risk, trust and website usability and the role of moderators,", I. Aboobucker, and Y. Bao, Journal of High Technology Management Research, vol. 29, pp.109-123, April 2018.