ISSN:0975-9646

Security Issues on Banking Systems

Mohd Khairul Affendy Ahmad [#1] , Rayvieana Vera Rosalim[#2], Leau Yu Beng [#3], Tan Soo Fun[#4]
[#]*School of Informatics Science, Universiti Malaysia Sabah*
Jalan Sungai Pagar, 87000, Labuan F. T., Malaysia
[1]kei_ryisuke@yahoo.com.sg
[2]vieana_ray@yahoo.com
[3]leauyubeng@gmail.com
[*]*School of Engineering and Information Technology, Universiti Malaysia Sabah*
Jalan UMS, 88400, Kota Kinabalu, Sabah, Malaysia
[4]soofun4818@yahoo.com

***Abstract*- Bank is one of the example of institute that using Information Technology (IT) in its daily task to fulfill the organization's and customers' need. Business transaction, money transfer, ATM, credit card, and loan are some tasks that were done every day. Customers' personal information stored by the bank is also considered as private and should not be disclose to anybody with no authorization. Only legal staff and legal bank's customer can operate any of the tasks. Thus, bank has its own system to ensure their transaction works the way it is and prevent any activity that could cause lost to the organization and its clients or customers. Whether like it or not, some irresponsible people are always exist to challenge the robustness of a banking system. Even an amateur that claimed themselves as a hacker could transfer a sum of money from other account to his or her account without noticed. Bank account hacking has caused millions dollar losses around the globe. How this could happen? Was there any obvious weaknesses in the banking system that make it easily expose to treat? This article would discuss about the intrusion of banking system. It is important to realize how the security aspects in a banking system can influence such illegal activities which are then lead to a great lost to the financial institution. Some recommendations would be included in this article to help to reduce or prevent the intrusion in the future.**

***Keywords*— Banking Systems Intrusions, Authentication, Data Confidentiality, Integrity.**

I. INTRODUCTION

Technology nowadays gives an opportunity to satisfy the need of faster and efficient banking transaction. Information system that is used in a bank is not only between business to business (B2B) but also between business to customer (B2C). Intrusion is an action of accessing one place or system without the permission of the owner. If a system has been intruded, it means that it has compromise with the security aspects that is applied in the system. Intrusion might be done by anyone with security knowledge and could happen for any purpose – to gain and alter confidential data or to steal sum of money from the financial institution. Fault and failure caused by this intrusion not only decrease the system performance but also client and customer's trust towards this financial institution due to the risk of losing their money and assets in the bank. In U.S, the government requires banks to report all losses. According to Michael Higgins, a financial computer security consultant of Para-Protect in Alexandria, Virginia, banks usually want to avoid bad publicity by reporting losses as accounting efficiency errors [1].

II. POTENTIAL BANKING SYSTEMS INTRUSIONS

A. Distributed Denial-of-Service Attack

Denial of Service (DoS) is ranked as FBI's third highest threat after terrorism and espionage. Financial institutions that facing DoS attack could experience great lose of money due to losing clients and customer. It is also required high cost to repair the damage done by the attack [2].

Distributed Denial of Service (DDoS) is the most common attack that could happen in the banking system. DDoS involve hundreds or more 'zombie' computers to launch the attack to the targeted system. Before an attack is occur, attacker build an attack network by scanning for open port, poorly secure computer with no firewall or anti-virus software. A new program is installed in the 'zombie' computer. The program can self-propagates and automatically create a large attack network [3]. It might possibly contain both the code for sourcing a variety of attacks and some basic communications infrastructure that allow remote control [4]. These 'zombie' would send large number of packets to the system at the same time and force the real requested packets to drop due to time out. This type of intrusion can affect the availability and continuity of the banking system. The financial institution would fail to conduct transaction with its customer, business partner and vendors.

Another risk posed by the distributed denial of service attack is it can result a great number of loss of time, customers, money, and also compliance violations. Common risk that any financial institution or banking system would encounter is their operational, reputation and their regulatory. The operational risk may arise from fraud, error, or unavailability of products or services. Reputation risk is all about operational disruption cause by denial of service, which includes errors, delays, unavailability of information and the unauthorized access towards the system information or the banking systems. The regulatory risk covered about the lawsuit and enforcement actions towards the banks [5].

B. Data Breach

Financial institutions have to aware about threats that would affect the system security in their organization. A data breach, one of the threat exists allows the information and data to go out from the system, making it viewable to others. A data breach is a very well known phenomenon where it involves highly sensitive and confidential data that might have been viewed, stolen, and also have been used by any

person or any organization without being authorized to do so. For example in security data breach, a case where involves five Connecticut banks are resulting from security data breach, affected from New Jersey company that processes credit card payments, according to the newspaper and internet reports. The effect of the data breach takes a great number of losses for the financial institution, where their credit card companies such as Visa and MasterCard contacted them about the breach, according to the internet site BankinfoSecurity.com. The banks that affected with the breach are Litchfield Bancorp, Apple Valley Bank of Cheshire, Dime bank of Norwich, Liberty Bank of Middletown, Chelsea Groton Bank and other 230 financial institutions [6].

Data breach happens when there are loopholes in the banking system, enables those unauthorized individual to get access to the system itself. It is due to the lack of security assessment, and also resulting from poor security system. Many banks have suffered loss when there exists data breach; losing information, losing capital, and in above example, losing card credit information and thus might influence the customer's trust towards the bank's service. Further analysis would result to several issues relating to the data breach, is a poor authorization management and lack of authentication mechanism which will take to the confidentiality and integrity issue of the system.

Loss of authentication or stolen identification, result from identity theft is the ticket for the criminal or unauthorized individual to simply get the authentication needed their own benefits. From the case example provided, the lost of credit card information for the financial institution is mostly due to the lack of authentication and poor authorization itself, that can lead to the data breaches. Without proper authentication and authorization, an individual can act by entering the system illegally, and thus taking any information they want. That is why the authentication and authorization being the utmost importance to protect any information system, especially when running a financial institutions.

Confidentiality and the integrity of the data in the system would likely been violated whenever there are security data breaches, done by unauthorized person. The data might loss its confidentiality when these unauthorized person view, alter or steal the personal information of the customer or the information security of the organization uses. The integrity of the system can also be affected, when these irresponsible people alter and changing the data information in the system, for example exchange a sum of money to their own account.

C. Malware

Malware is software program that design to alter and modify the computer's system without the authority of the user or owner, and this malware move from computer to computer and network to network. Malware can be including viruses, Trojan horses, worms, script attacks and also rogue internet code [7].

The malware attack can influence the confidentiality, integrity and availability of the banking system. In confidentiality, malware attacks are all including capturing keystroke, passwords and credit card numbers, uploading and downloading files, and also observing what is going on the server's screen. An attack against integrity however is also harming the banking system, where it modifies the system, such as the infected file and also data. Corruption of data files and also application files by unauthorized file writers, changing configurations of the banking system and also overwriting data are all influence the integrity of the banking system. Availability of the banking system can also be effected, where it includes the deletion of files and subdirectories, renaming of files, reboot or disabling the security systems and also denial of service attacks [8].

The damage resulting from malware attacks could be severe. An example for a malware attack is ATM breaches in Russia and Ukraine. Trustwave, a Chicago-based provider of information security and card industry have uncovered malware while investigate ATMs in Russia and Ukraine, for over few month. During the attack, about 20 ATMs were infected by the malware, allowing the attackers to steal data, PINs and also money. In the case, they were certain that the attackers was an inside work, because the attackers needs the physical access to the ATM in order to install the malware, and execute it. Ti would also seem that the attackers could be someone who gets a copy of the key to the ATM, opens the machine and loads the malware into the system [9].

Another example is The World Bank Group's computer network as one of the largest repositories of sensitive data about the economies of every nation has been raided repeatedly by outsiders for more than a year [10]. In this case, it is still not known how much information was stolen. Sources inside the bank confirm that servers in the institution's highly-restricted treasury unit were deeply compromised with spy software. The attackers also had full access to the rest of the bank's network for nearly a month in June and July 2009. In total, at least six major intrusions occur, two of them using the same group of IP addresses originating from China that have been detected at the World Bank since 2007, with the most recent breach occurring just a month before.

These two examples show the attacks done by malwares to the banking systems. In the attacks, the information in the banking systems was compromise, the information are either stolen or altered, and the security system in the banking system is violated. The result by the attacks may lead to a loss worth millions, and also it also influence customer's trust and customer's loyalty to the financial industry. Malware such as spyware are the most commonly used by attackers in order to maliciously steal the system's information, and violate the system's confidentiality and the system's integrity. The attackers as in the example are usually the worker or the insider of the organization, installed the software program in order to gain illegal information and to steal, modify, and also delete the information contained in the systems.

D. TCP/IP Spoofing

TCP/IP spoofing is one of the common forms of on-line camouflage. In IP spoofing, an attacker gains unauthorized access to a computer or a network by making it appear that a malicious message has come from a trusted machine by "spoof" the IP address of the machine [11].

IP address spoofing is the technique that can make the attacker to send packets on a network, without being intercepted and blocked by the firewall system. These firewall systems usually filter any external IP address who tried to communicate with it. However, using IP spoofing,

the attacker can mask its identity by making their IP address to appear to come from the internal network, thus making the firewall unable to intercept it, and so packets can easily transferred by the attackers. The objective and goal for this attack is that to enable the attacker to gain root access to the victim server, in this case the banking system, allowing the creation of a backdoor entry path into the targeted systems. Whenever the loophole for the past attack being covered, there is always a backdoor for the attackers to sneak in back to the server at any time. With the TCP/IP formats, it is very easy to mask a source address by manipulating an IP header. This technique used for obvious reason, to access unauthorized system and sends packet which may contains malwares, to gain information such as the customer's bank accounts, PINs, identification numbers, credit card numbers and so on [11].

IP address spoofing's favorite target is the financial institutions, or the banking system where they can gain profits. Recent survey shows that $2.4 billion in losses to banks is from the internet-based scammers, derived from spoofing and phishing. The major victims of spoofed emails include Bank of America, BankOne, First Union Bank, Barclays Bank and Lloyd's Bank [12].

Another possible threat for spoofing is it can lead into confidential data breach. One possible example is Rocky Mountain Bank, which have sent confidential and sensitive information to the wrong Gmail account [13]. The biggest loss in this example is the customer's trust towards the bank's service. The confidentiality and the integrity of the information have been violate, thus it also violates the customers trust to the bank.

The lost of confidentiality is a very serious matter, because it contain sensitive and important information about the client, and even about the institution and organization, and so confidentiality of a system needs to be taken care well by the organization itself. Loss of integrity however can result of loss of customer relationship, where the privilege given to the customer is being violated by any means, in this case by IP spoofing.

III. INTRUSIONS PREVENTION

Authentication mechanism is very important in ensuring the data in the system is protected from any unauthorized access that could interfere with the integrity of the banking system. Authentication also would make sure that the system is functioning well and trusted by any parties. To improve authentication, the banking system should increase their security performance by having two levels of authentication. First level is the password, and the second level is by providing with the user's personal information such as passport number or identification number. These can make the authentication security much safer and invulnerable.

An authentication that involving password usage should consider these things; the length and strength of the password, considering upper case sensitivity, character set and lifespan of the password. Password lifespan is the duration of time that the password can be use to access to the banking system. The shorter lifespan the password has, the lower risk of password compromising it takes. It a particular user does not access to the system for certain duration of time, the password should be terminated and the user needs to set a new password if he/she wishes to access to the system again [14].

But, for some cases, even with two levels authentication can't ensure the safeness of the information stored in a banking system. To eliminate these any other possible problem, three levels of authentication can be adapted. It is requires to use the biometrics authentication. Biometric is a way of identifying a person by its unique physical feature. The idea using biometrics authentication has already been developed, where the person's for example the eye and thumb being used as identification.

Sending wrong email to a wrong person might look like a minor problem to a sender. But if the content of data which is highly confidential such as customers account information and the receiver has bad intention toward the email that he received, the organization could face major losses. According to Steve Jones; a Chief Technology Officer at Signal Financial Federal Credit Union in Washington, data leakage is a major treat thus such mistaken should be reduce and prevent with a technology hardware solution.

"When Jones decided on one data loss prevention solution, he saw it taking out this human element to a data breach. With three locations to cover, Jones needed three boxes: one at the credit union's primary location, a second one at the disaster recovery site and the third at the credit union's co-location site. These boxes scanned outgoing content on all types of TCP/IP traffic, http, FTP, even https traffic and stopped any traffic that had pre-defined information within them, including customer account numbers and other sensitive information. These features help scans data in email body and attachments. Thus it could reduce the accidental data breaches [15]."

When installing and updating systems equipment, the security parameters and setting should be review to make sure it is consistent with the intrusion risk assessment plan that the financial institution has. Firewall is placed between a network and the internet. It is operates from a specific computer and was separated from the network. Firewall function like a guard or a gatekeeper to a private network or computer system and determine incoming requests from reaching the network resources.

Firewall controls what kind of network traffic that can access through the network. Usually unauthorized communication or any possibility of attack from the internet to the network would be block. Well, of course the configuration setting of a firewall can be change to suit preference. Firewall is different from routers. Routers transport the data between networks while firewall screens the data that is going to be sent across a network. Firewall helps block uninvited guest or unauthorized personal from trying to connect or gain access to any file share that a bank organization has set up. At the same time, the organization own activities are not block and interrupted.

There are two types of firewall which is the hardware firewall and the software firewall. The difference between these two type is hardware firewall are built within devices such as routers where else software firewall are program that is installed on computers. Since hardware firewall is placed in a router, it functions to protect the whole network while the other kind protects individual computers.

In banking system, firewall can be used to control access to a certain system within the corporate network of the bank.

It can restrict or limit the access to highly sensitive banking system to particular employees. Traffic filtered is based on a set of security rules, depending on the need of security of the bank organization. For example a packet of data coming into the network is flagged by the firewall filters as having a breach on the defined rules, it will be denied entry to the network. Methods through which a firewall can regulate traffic in and out of a network include packet filtering, a proxy service or stateful inspection. A firewall can either be a hardware or software firewall. Ideally, a firewall should consist of both [16].

For an issue related to information integrity, there are lots of ways to prevent it from happen. Major threats for banking system is the employees as the insider, working in the bank itself, who have all the authority to manage and view related data and information, including customer's information. Especially those terminated employee, they would likely used their knowledge and authority to put the bank into catastrophe by deleting or violate important data. As administrator for the bank, it is strongly suggested to change or reset all passwords or any means, as the access to the database or data storage that the terminated employee can sneak into. Other than that, one time password can also be implemented, where the computers can only be accessed by password being prepared by the main server, monitored by manager responsible for the server. This method is an easy practice but yet it can protect millions of data, and thus protect the information integrity for the bank system.

For insiders that currently works at a bank, and have the intention violating banking system's information, monitoring privileged user activities is another strategy in protecting data integrity. All users and activities are recorded to analysis, recovery and develop additional security measure and development of legal action. Using this method, administrator can easily track down any irregular behavior. The method includes monitoring the employee's activity, on the basis who do the job, what task did they do, when they did the task and where the employee do the job. By using such information, administrator can compare their job time by time, and thus, if any irregular activity or behavior is being done, administrator can quickly prevent it. The employee's privacy might be violated, but the importance on securing the customer's information is more important and must be taken seriously.

Not only meant for the staff monitoring, this method could detect any outsider intruder. Information about system and file system, networks, and application is collected. The record must be keeping safely and located in a physical location separate from the devices generating the records.

A good Intrusion Prevention System (IPS) is not only able to detect harmful intrusion but also essential to ensure protection of confidential data and assets in a banking system. The IPS must able to identify any potential dangerous intrusions accurately and minimize false positives alarm. With this feature, it actually could decrease the cost of damage and potential impact from an attack or intrusion such as the Denial of Service (DoS), buffer overflows, and malware. On example of IPS that has these outstanding features is the McAfee Network Security Platform. It's not only protect the banking system network, servers and desktops but also offering other advantages. A centralized, consolidated dashboard and robust reporting has saves IT administration time and money from monitoring the network. The highly stable solution has also improved network performance and, by preventing attacks, reduces network downtime and the risk of interruptions to online banking services. This IPS also is only IPS that could prevent encryption attacks [17].

IV. CONCLUSION

System intrusion is not somewhat new that occur around the world, but it have been occur a long time ago since the existence of computers. In the previous years , times when the early development of computers shows that the computer system intrusion is lesser than today, it is probably because the technology back then was still poor, and the consciousness about intruding computer's system is yet to be developed.

Banking system intrusion shows the vulnerabilities that exists in financial institution, that have been used by those illegal and unauthorized individuals or groups to intrude an area with secure environment. The violation of system security is all about the money, challenges to intercept data, challenges with acquaintance, data breach, and poor authentication and authorization. With all of the weaknesses occur, well, it is a treat for anybody with high experience and knowledge in information systems to get into the system, using, stealing, modifying and even deleting information in the system.

Financial industry such as banks plays major role in prepare the people a good service, good system, and the best security systems that can meet customer's expectation and also to attract prospective customers to use trust and using their system to keep their personal data, information and most importantly their money safe. Although there is always vulnerabilities occur around the time, banking system should have a backup plan or other shields in order to handle any malicious behavior, that intend to violate the customer's information. Ways of prevention should be taken care like the one that has being stated in this paperwork. As the conclusion, with the developing of high technology and information systems around the world, banking system should not be left behind in term of security system, and should keep a sharp eye when there any vulnerabilities in authentication and authorization that may lead to confidentiality, availability and integrity issues.

REFERENCES

[1] David H. Freedman. "How To Hack A Bank." ,Forbes ASAP, 2000.
[2] Susan Orr. "DDoS Threatens Financial Institutions-Get Prepared!", Reyman Group, Inc, 2005.
[3] Larry Rogers, "What is a Distributed Denial of Service (DDoS) Attack and What Can I Do About It?", CERT Carnegie Mellon University, 2004.
[4] David Moore, Geoffrey M. Voelker and Stefan Savage, "Inferring Internet Denial-of-Service Activity", Proc. USENIX Security Symposium, Washington D.C, 2001.
[5] Susan O., "DDoS Threatens Financial Institutions", Reymann Group Inc., 2005.
[6] Mark S., David K., "Credit card breach affect Conn. banks and credit unions", Waterbury Republican-American (Connecticut), 2009.
[7] Grimes, R.A., "Malicious Mobile Code – Virus Protection for Windows", O'Reilly Media Inc., Sebastopol, CA, 2001.
[8] Harley, D., Slade, R., Gattiker, U., "Viruses Revealed", McGraw-Hill, 2001.
[9] Marsia, S., Information Security magazine, 2009.
[10] Richard B., "World Bank under Cyber Siege in 'Unprecedented Crisis'", Fox News, 2008.

[11] Matthew T., “IP Spoofing:An Introduction”, 2003.
[12] Kruck, Gregory P., “Spoofing – a Look at an Evolving Threat”, The Journal of Computer Information Systems, 2006.
[13] Mike M., “Banks Sends Confidential Email to Wrong Address”, Grab-Some-Popcorn Dept, 2009.
[14] Clifford A. Wilke, “Infrastructure Threats -- Intrusion Risks”, 2000.
[15] Linda McG., “Data Loss Case Study: How to Tackle the Email Threat”, Bank Information Security Articles, 2008.
[16] Kivumbi, “Difference Between Hardware Firewall and Software Firewall”, DifferenceBetween.net, 2009.
[17] “McAfee Network Security Platform Protects Bank Customers’ Financial Assets and Personal Data”, McAfee, Inc, 2009.