An Analysis of the Online Banking Security Issues Reported by Hole, Moen, and Tjostheim

Fan Zhang, fzha012@aucklanduni.ac.nz

Department of Computer Science,
University of Auckland

Abstract. Online Banking has become increasingly popular globally, because it is so easy and convenient for Internet users to manage their bank accounts from anywhere of the world at any time. Banks have encouraged for this trend for years, since Online Banking also saves lots of resources for the banks regarding of staff training, investment for ATMs and branches, and other operations costs. The Internet enhanced the user experience of banking activities dramatically. However, since the Internet is not originally designed for Online Banking, Online Banking now is facing a wide range of security risks for both the banks and the Online Banking users such as brute-force attacks, distributed attacks, and social phishing. The banks have to increase their Online Banking security system constantly, which means the banks have to keep investing on the security systems all the time. Compared with the possibility of the lost from the potential risks, the banks may not want to update their current security systems, because the cost of upgrading security is too expensive and the risks of loss are low. Then this will leave the lots of security responsibilities to the Online Banking users. However, the customers' PCs actually are always the weakest link for the Online Banking security. The customers would rather to choose convenience and easy-to-use than complex login procedure for Online Banking. In other words they would choose great choose great user experience with foolproof security. This paper will discuss and analyze the Online Banking security issues reported by Hole et al. In this paper, both Lampson's work and Claessens' work will be used as a framework and a security analysis "language". The Online Banking security is a wide range of topic. This paper will discuss and analyze two important security issues related to the security policy, design and implementation which reported by Hole et al, focusing on client authentication and related attacks. This paper will use case study method to analyze both issues.

Acknowledgements

I would like to thank Prof. Clark Thomborson for the most valuable advices, great insights and support that made this paper possible.

1. Introduction

As technology evolves, many Internet applications become so popular. Online Banking (sometimes called the Internet banking or e-banking) is one of the Internet applications which have major impact on our modern life. The benefits of Online Banking (e.g. easy-to-use, convenience, fast, cost-saving) for both banks and Internet users make Online Banking so popular around world. Online Banking has changed the way how the traditional banking industry interacts with banking customers. There is no doubt Online Banking is one of the most sensitive tasks performed by the Internet users. Although banks have strongly encouraged their customers to do Online Banking and advertise the Online Banking is very safe and secure, apparent this is not true. Claessens discussed many security issues related to Online Banking [2]. Also in Lampson's "computer security in real world" [1], he pointed out that in general the most computers in real world are not secure because security is too expensive. Moreover, the communication via the Internet has made computer security very hard [1]. In fact the end users' PCs are weakest link of online applications. According to Lampson's "money talks" concepts for security, to make the banks/companies profitable, even sometimes the banks/companies learnt the inadequate security in their current systems, compared between the low risks of potential loss and high cost of security, the banks/companies may not want to upgrade their current security system [1]. In fact, in this case the banks leave the security responsibilities to the Internet users. In contrast, normally the Internet users would think it is the banks' responsibility to take care of the security. There is no mutual trustworthy environment/platform between the Online Banking systems and their clients [2]. Hole, Moen, and Tjostheim studied several Online Banking systems in Norway from 2003 to 2004. They reported several key security issues about the Online Banking security with descriptions of different possible attack scenarios. Hole's research indicated the design and implement of many online bank security is vulnerable for potential attacks in Norway during 2003 to 2004 [3].

The analysis and discussion of this term paper is based on the Lampson's work [1] and the Claessens' work. [2]. Butler Lampson's work is also applicable for Online Banking system. In Lampson's work, he identifies four goals of security: Secrecy, Integrity, Availability, and Accountability in terms of policy [1]. He also identifies three basic mechanisms for implementing security: Authentication, Authorization, and Auditing. These concepts will be a basic framework for this term paper for analysis of the Online Banking security [1]. This paper also uses Lampson's defensive strategies concept and "money talking" concepts [1]. Furthermore, the terminology and concept given by Claessens et al [2] will be used in this term paper as well. Below is a list of terminologies from Claessens' work used in this term paper.

a) Client authentication of Online Banking: Entity authentication, Transaction authentication:

b) Authentication mechanisms for Online Banking: Fixed passwords, Dynamic passwords, Digital signatures hardware tokens

2. Overview of Security of Today's Online Banking

The trend of growth of Online Banking brings many security issues and increasing cost of implementing higher security system for both Online Banking users and the banks. Claessens said security is all about risks and associated cost in his paper [2]. The most critical issue of Online Banking security is to protect valuable information that is susceptible to unauthorized access by attackers. Hence, the banks must constantly increase security. At the same time, the banks must manage costs to make a profit. In contrast, increasing security is increasing the cost for attackers to break into the system, and increasing the punishment that the attackers may suffer. Hence the Internet criminals/attackers/crackers may lose motivation for hacking a high security Online Banking system.

In Claessens' work [2], he discussed many risks for today's Online Banking system, e.g. communication risks, client authentications, and human factors, etc. Based on Claessens' research h[2], it is shocking to see there are so many ways that the

attackers can choose to hack the current Online Banking systems, e.g. trojan horse, botnets, social phishing, new botnet coordination and so on. The profit driven attacks activity has risen dramatically at every possible level. Claessens believed it is about the new profit motive behind these cyber crimes [2]. Furthermore, many security experts discussed different security issues related to Internet crimes. The Internet related crimes and the security issues are not only applicable for Online Banking but also all server-client Internet applications. Jagtic el at discussed how attackers are using "social phishing" to get uneducated victims financial or personal information [4]. Jagtic described phishing is a form of deception in which an attacker attempts to fraudulently acquire sensitive information from a victim by impersonating a trustworthy entity. Typically, an attacker is misrepresenting himself as a large banking corporation or a popular website to send potential victim a "lure" email [4]. According to Lampson' a chain of trust model, the phishing attacks actually caused by lack of trustworthy environment between the banks and the Internet clients [1]. Moreover, the poor designed Internet browsers are providing hackers easy access to computer systems via browser-based attacks [5]. A new threat is emerging that attacks browsers by means of Trojan horses. These attacks are so called man-in-the-middle attacks between the user and the security mechanisms of the browser [6]. These new attacks cannot be detected by the user at all, as they are using real services. Furthermore there is no advanced authentication method can defend against these attacks, because the attacks are working on the transaction level, not on the authentication level. [6]

According to Claessens, there are so many ways to attack Online Banking customers, e.g. trojan-horse, virus, and man in the middle attacks. For more information please refer to Claessens' work [2]. The following section will focus on the security issues reported by Hole el at [3].

3. Case Studies

Hole el at reported several security issues related to Online Banking. This term paper will study two important security issues from the authors' findings. To analyze the authors' findings, both Lampson' security concepts [1] and Claessens' Online Banking concepts and terminologies [2] will be used as a security analysis framework and security analysis "language" for this term paper. In this term paper, I will use case study style to analyze the security issues, risks, and associated costs and/or usability issues. In each case study, an overview of the authors' findings will be given along with an evaluation. In the evaluation, the security issues reported by authors' findings will be explained in context of Lampson's concepts. Then followed by a security analysis, authors findings will be critically and appreciatively discussed.

Both security issues discussed in this term paper are very important for the design and implement of Online Banking security. However, since the two security issues focus on different aspect of Online Banking security, and they are not a series of security issues, hence the analyses are not equally weighted. Also, the security analysis is not trying to find the ultimate solutions for the reported Online Banking security issues. For simplicity's sake, in the authors' study, they considered the banks use only SSNs (Norwegian social security number) for Online Banking account login.

4.1. The security-by-obscurity policy for Online banking systems

4.1.1 Authors' findings

During the authors' study, the authors suggested the management of banks in Norway typically has little understating of real security and tends to assume a system is secure if all information about it is kept secure. They reported all banks employees have to sign nondisclosure agreements, which preventing them discussing any security problems with anyone outside their systems. The authors made this claim based on the banks' reaction when the authors tried to inform the selected banks about their findings. The authors believed that the banks' security-by-obscurity policy led to a false feeling of security instead of real security, making the systems vulnerable to

rather trivial attacks during 2003 and 2004. The authors claimed this policy is actually against real security.

4.1.2 Evaluation

Based on Lampson's three aspects of a secure system, the issue reported by the authors is about "*secrecy*", in terms of *"Specification/Policy"* [1]. In this case, the information of a certain Online Banking system is the *secrecy*, which is only available for the employees or the people who has assigned nondisclosure agreements. In other words, the authors are *excluded* from accessing the information kept by the banks as *secrecy*. This is also a part *protection/defense mechanism* of the banking industry, which is designed to distinguish the people's security level against a certain range of information.

Based on Lampson's model of *a chain of trust*, since the authors did not claim they signed any nondisclosure agreements with the selected banks, the authors' security statuses are still *untrustworthy*. No matter how high their academic credibility is, the authors are kept out of the *trustworthy* environment (inside of the banks).

Based on the Lampson's *access control model*, for the Online Banking security systems, the premier task of *access controls* (*guards*) is optimized to protect the online system behind it and information about themselves. For *simplicity of security design*, the banks would rather instantly deny any access request from any untrustworthy or potentially untrustworthy entities including (personals, computers). Also, *the access controls* will instantly deny any attempt to acquire the information about the access controls itself. The biggest challenge of *the access controls* for Online Banking system is the authentication process, which distinguishes the real trustworthy entities from the attackers, which will be discussed in the following cases.

Hence, it is a very general strategy for militaries, banks, or any organizations holding sensible information to protect their *secrecy* within the trustworthy environment. It is

a general practice of access controls to make sure that user clearance level must be greater than or equal to the classification level of accessed information.

4.1.3 Security Analysis

The authors claim the banks security policy "prohibits learning" and "cause the same mistakes to be repeated". This statement is only from the authors' point views. The authors did not realize that from the banks' point of views, if some attacker is *pretending to be a "good guy"* to obtain the information about the Online Banking systems. In fact, the attacker just wants to explore the vulnerabilities and weakness in the existing Online Banking system. Imagine if the banks just trust anyone who claims himself/herself is a "good guy", and then let them to acquire the design or the structure information of a certain Online Banking system. Then it will be much easier for the attacks to detect and find the vulnerabilities and the weakness effectively and efficiently. There is a very high possibility for the experienced and highly skillful attackers to launch their attacks targeting on the weakness of a certain system, without investing lots of time and money to study a certain Online Banking system. Therefore, without any trustworthy agreement/secure channel between the banks and the authors, there is no point for the banks to explode any Online Banking information to them at present.

4.2. Client Authentication VS a Combined Brute-Force/DDos Attack

4.2.1 Authors' Findings

The authors claimed the login procedure of some Norway Online Banking systems is vulnerable to the combined DDoS/brute-force attack during 2003 to 2004 period. Authors assumed an attack could control a large botnet and divides a set of SSNs across the networks' zombie PCs. Each PC could then try to log in an online account by assigned SSNs. And the attack combines brute-force and DDoS attacks. In authors' report, they assumed it would be difficult for the banks to distinguish between legitimate customers and zombie PCs trying to log on. Through experiments, the

authors assumed the attackers could have cracked approximately 66 accounts by using the above attack method. The authors claimed introducing the certificate didn't actually enhance security, since the attackers could also download the certificate if they knew the SSN and PIN. Depending on the actual PIN distributions, the crackers could expect to access significantly more accounts for a uniform PIN distribution. Furthermore, through experiments, the authors claimed the banks use a PIN calculator for client authentication which aims to provide two-factor authentication. However it is still vulnerable for the combined DDos/brute-force attacks, because the window size of PINs (windows size = 19) used by Norway banks is too small. The two-factor authentication with hardware token (PIN calculator in this case) could lower the possibility of success of hacking online accounts. However, two-factor authentication is not really secure, and effectiveness of using two-factor authentications is limited.

4.2.2 Evaluation

Based on Lampson's concepts [1], this issue of the Online Banking security is about "*Integrity*" in terms of *"Specification/Policy"*. One important goal of Online Banking system design is to meet *integrity,* and the attackers must to be *excluded* from accessing Online Banking system. In this case, the Online Banking security system needs to protect customers' money against the danger from the attackers. The Online Banking security system must have a strong "*lock*" to prevent the attackers and the Internet criminals to steal money from the legitimate customers' online bank accounts. Obviously, *integrity* is critical for Online Banking security: the attackers should not be able either to block the Online Banking service, or login the Online Banking accounts, or transferring any credits out of legitimate customers' accounts.

Moreover, based on Lampson's access control model [1], the assumption of the attack targeted on *authenticating principals'* procedures of Online Banking system in terms of authenticating principals/ authorizing access auditing the guard's decisions for implementing security.

Claessens et al made a distinction between entity authentication and transaction authentication for client authentication in his work [2]. The authors' assumption of the

attack actually targets on entity authentication. Although authors' assumptions are based on publicly available Internet information only, they illustrated the possible attacks clearly under a certain environment without attacking the banks system. Authors mentioned at end of their assumption, the one selected bank changed its login procedure in 2004. However, authors did not reveal what the changes are? How the changes improved online security system?

4.2.3 Security Analysis

4.2.3.1 Cost of attacks

According to Lampson's concepts [1], there is no absolute security. From attackers' point of views, security is actually about *cost* for attackers to break into a certain "*lock*"/environment/system/platform including time, money, and punishment. Compared with the benefit they could obtain once they hacked into it, if the cost for the attack is too high, the criminal or attackers would lose motivation to hack. The combined DDos/brute-force attack is not expensive for the attackers to launch. The techniques of brute-force and DDos attack are well known. The attack does not require high-level knowledge expertise to perform. In terms of *implementing security*, the potential punishment is also another cost for the attackers. In this attack scenario, the potential *punishment* that the attackers could face is actually rather low. Since the volume of victim PCs traffic of the large botnet at application lay is huge, it is very hard for banking detection system to stop the attack and to track the original attackers. In this case, the cost for the attackers is low. This attack is not only targeting on Online Banking system, but also applicable for any client-server systems. In terms of risk analysis, this threat is highly dangerous and the possibility of the potential attacks is also high.

4.2.3.2 Cost verse Profit for the banks

Security experts (e.g. Lampson and Claessens) differ on specifics but agree on cost for implementing security. Security costs lots of money not only for banks but also for many companies, organizations and government. In this case, the authors only looked at this threat from customers' point view. They overlooked banks' point of views. In

Lampson's work, Lampson believed although many companies have leant about inadequate security, they won't spend much money on security [1]. Lampson said "practical security balances the cost of protection and the risk of loss, which is the cost of recovering from a loss times its probability" [1]. There is no doubt this "money talks" concept is also applicable for Online Banking industry. Today, the most important issue associated with the growth of Online Banking is security – the protection of the valuable information is susceptible to unauthorized access by hackers. Banks must constantly increase security. At the same time, banks must manage costs to make a profit. Authors claimed the banks did not upgrading their security to against a certain potential risks. However, the authors did not realize the "Money talks" issue for Online Banking. The banks could reckon the possible loss for some risks is fairly low, compared with the investment of implementing higher security. Hence, banks would not invest on higher security to keep banks more profitable. As a junior security analyst, I reckon the cost should not be an excuse for the banks to implement higher security system to protect customers' assets.

4.2.3.3 User experiences

The authors also overlooked simplicity for designing a security system. Simplicity is another important element to design a security system.

Most of customers reckon it is the banks' responsibility to secure all customers banking information. Complex security procedure is against the convenience of Online Banking. The customers will not bank online without foolproof security. Today's customers are not yet ready for high technology devices to implement their digital signatures and verify their identities. Although Online Banking is growing, customers do not want to use hard tokens e.g. smartcards, or fingerprint identification devices. Customers are not ready to take on what they perceive to be unpleasant tasks in order to do bank online. As a junior security analyst, I reckon that banks and governments have responsibility to educate Internet users for higher security awareness, in order to protect them from a certain level of Internet crimes

4.2.3.4 Trustworthy Environment

The Authors also overlooked the trustworthy environment aspect when they were reporting the security issues. Security experts like Lampson and Claessens use different species but they both agree the trustworthy environment /platform is important for a security system [1] [2]. Authors claimed the PKIs can solve the security issue. However, based on Lampson's trust of chain model, without a trustworthy environment and secure communication channel, any link between the legitimate clients and the banks are still vulnerable. Increasing security in a single factor/link of a security system would not make the whole system more secure. Both Lampson and Claessens indicated the typical client PCs are very vulnerable [1] [2]. However, when most banks designed their Online Banking system, they have made assumptions the users' PCs, operating systems and softwares form a secure end-point in this process [2]. Claessens indicated Virus, Trojan horses, and other malicious program can temper with the installed root certificates [2]. They can steal a user's private keys. They can spoof the user interface or mislead users [2]. Based on both Lampson and Claessens' security concepts, a secure environment should be build between banks and clients, not just increasing security for a single link or factor for an online system. The trustworthy environment should be resistant to the phishing and pharming attacks, and also social engineering or man-in-the-middle attacks. Implementing PKIs for Online Banking security is not sufficient without a trusty worthy environment.

5 Conclusion

Lampson said most computers today are insecure because security is costly in terms of user inconvenience and foregone features. People are unwilling to pay the price [1]. I believe this concept is very true and it is very useful for Online Banking security analysis. Today, more people who are less technically savvy are using Online Banking. Most major banks currently support Online Banking, as it enables them to serve far more customers than by traditional banking. Online access also reduces physical visits to the bank, which saves customers' time and money, and saves banks'

cost as well. However, the popularity of Online Banking has attracted the Internet criminals to attack Online Banking customers. Attacks have been launched against Online Banking customers worldwide. Hole et al illustrated several attack scenarios for Online Banking system, which is related to the security policy, design and implementation of security. As long as the profit is much bigger than the cost and punishment, the attack against online banks will not stop. Authors also illustrated two factor authentications with pin calculator by itself might not offer the level of protection some banks keep claiming about. Any system has its own deficiency. According to Lampson's a chain of trust and Claessens' trust platform, the better online security system requires more than one technology or a multi-factor mutual authentication platform. In other words, it requires a trustworthy environment/channel between online banks and the clients. Any advanced security technology or security method by itself will be useless when it is facing more complex attacks targeting on any other weakest link of security system, e.g. customers' PCs. Advanced the technology is not the only solution against the security issues with Online Banking authentication. The banks and governments should invest to educate the Online Banking clients and the general public about the proper way to safeguard their online transactions. The financial institutes should also start to investigate more ways for the legitimate clients and the banks to easily identify each other. Both the banks and the clients have responsibility for the Online Banking security. They could not simply make assumption that the opposite end is perfectly secure. As a junior security analyst, I reckon to further protect the banks, the clients and all Internet activity. It is important to look into improving the real time Internet crime detection system on the backbone of the Internet around world. So any malicious transactions can be detected before they even happen. Then Internet will become much cleaner and purer. This paper is presented as only the beginning of the necessarily long and active research in Online Banking Security. Further research is definitely required for these issues related to Online Banking. We will need many risk experiments to find better, usable and workable solutions.

References

[1] B. Lampson, "Computer Security in the Real World", *IEEE Computer 37:6,* 37-46, June 2004.

[2] J. Claessens, V. Dem, D. Cock, B. Preneel, J. Vandewalle, "On the Security of Today's On-line Electronic Banking Systems**", Computers & Security 21(3), pp. 253-26 5, 2002**

[3] Hole, K.J.; Moen, V. Tjostheim, T., Case study: Online Banking security, **Security & Privacy, IEEE Volume 4, Issue 2, March-April 2006 Page(s):14 - 20**

[4] T. Jagatic, N. Johnson, M. Jakobsson, F. Menczer, "Social Phishing"**, *Commun. ACM 50(10),* pp. 94-100, October 2007.**

[5] C. Grier, S. Tang, S. King, "Secure Web Browsing with the OP Web Browser**", in *IEEE Symp. on Security and Privacy (SP 2008),* pp. 402-416, 2008.**

[6] P. Gühring, "Concepts against Man-in-the-Browser Attacks", 15 pp., web manuscript, published circa January 2007. Available: http://www2.futureware.at/svn/sourcerer/CAcert/SecureClient.pdf, 23 July 2008