Internet Banking Security Framework: The case of Ethiopian Banking Industry

Aychiluhim Desisa
HiLCoE, Computer Science Programme, Ethiopia
aychd@yahoo.com, chuchu.desisa@gmail.com

Tibebe Beshah
HiLCoE, Ethiopia
School of Information Science, Addis Ababa University, Ethiopia
tibebe.beshah@gmail.com

Abstract

Ever since the birth of the Internet, people have been using it more and more for accomplishing their daily tasks. One popular applications of the World Wide Web is Internet banking. Internet banking, however, is not without its risks: criminals have armed themselves with in-depth technical and even psychological knowledge in order to gain access to banking accounts of unsuspecting users.

One of the domains which uses this new communication channel for more and better interacts with its customers is the banking industry. Currently the use of Internet Banking is increasing rapidly in the Ethiopian banking industry. The significant growth in presenting and using of Internet Banking services such as responding to customers' requests on every time and every place and additive integration, leads to fast growth in fraud events and security problems world wide. Ethiopian banking is obviously not out of this security anxiety.

This paper finds that the critical way of Internet banking fraud is, in one way or another, social engineering attacks. This emanated from the client side security loop holes.

To implement enhanced security in Internet banking, the paper recommended holistic multi-layered security that stretches towards client's side security and national financial and security intelligence and team incorporated. The Internet Banking security framework and its major five security models have been developed and evaluated through expert evaluation method.

Keywords: Internet Banking; Internet Banking Security Framework; Holistic Multi-Layered Security; Authentication; CIA; Client's-side Security

1. Introduction

A major driving force behind the rapid spread of Internet Banking (IB) worldwide is its acceptance as an extremely cost effective delivery channel of banking services as compared to other existing channels. However, Internet is not an unmixed blessing to the banking sector. Along with reduction in cost of transactions, it has also brought about a new orientation to risks and even new forms of risks to which banks conducting Internet banking expose themselves. Regulators and supervisors worldwide are concerned that while banks should remain efficient and cost effective, they must be conscious of different types of risks this form of banking entails and have systems in place to manage the same. An important and distinctive feature is that technology plays a significant part both as source and tool for control of risks. Because of rapid changes in information technology, there is no finality either in the types of risks or their control measures.

Technology based banking is now bringing more choices than ever before in the financial sector. It is now becoming possible to access our bank account in multiple ways and take care of our financial affairs quickly and efficiently.

Banks have thrived with the explosive growth and availability of the Internet. A wide variety of services are offered to the customers. Paying a bill, checking the account balance, or applying for a loan can now be comfortably done from one's own home or office.

However, the new possibilities introduced with IB have also resulted in new security challenges.

Modern banking in Ethiopia, which was introduced in 1905, is finally making a leap to catch up with innovative banking services and products. One can easily observe that the home grown banks are introducing a new range of banking services based on ATM, Internet Banking, Mobile Banking, POS, SMS and Call Center banking as an extension of their traditional branch services. This truly heralds a new area of banking in Ethiopia.

In summary most of the study results indicated that the most vulnerable and most of the attacks directed at IB systems target the client/customer (the weakest link in the chain), focusing on obtaining authentication and identification information through the use of social engineering and compromising the user's IB access device in order to install malware which automatically perform banking transactions. It has been observed that any bank or organization normally concentrates on IT assets at the servers, tightly protecting the network perimeters, and implementing internal security layers around the servers. As a result, intruders are now paying closer attention to client-side vulnerabilities on users' workstations.

As we initially alleged to give an attention to the importance and challenges of client-side vulnerability, it generally takes the form of unpatched software on a desktop, laptop, or PDA. Use of dangerous applications is another client-side threat that should be given close consideration (e.g., file and desktop sharing). Intruders that exploit client-side vulnerabilities and gain unauthorized access to a user's workstation often also gain access to the company's sensitive information and can hijack the user's application sessions.

This fact indicates that secure Internet banking systems should provide security mechanisms that highly cover both client-side and server-side security in mitigating the risk of user related information leaks and security issues affecting the system and leading to fraud.

Therefore, given the multitude of ways in which threats could take advantage of vulnerabilities to harm the bank and its customers, Internet banking security risks are always present. Effective information security reduces these risks by protecting the bank and customers against threats and vulnerabilities, and then reduces impacts to its resources (financial and non-financial).

Internet banking security is achieved by implementing a suitable set of controls (like legal framework), including policies, processes, procedures, organizational structures and software and hardware functions. These holistic approach need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the bank are met.

Most research on Internet banking systems is focusing on security on the server's side and on network security (i.e., the creation of a secure channel between the clients' computers and the bank's servers) [2] and most of the attacks on Internet Banking used today are based on cheating the user to steal login data and valid TANs. Two well-known examples for those attacks are phishing and pharming that are generally categorized as social engineering.

In line with this we have discussed the holistic security approach which will require a coordinated outlook of the banks, regulatory body, service provider, customer and other concerned stakeholders in order to implement a comprehensive suite of Internet banking security under this overall framework.

The framework mainly outlined with the concept of holistically multi-layered security approach comprising both technical and business requirements of all key stakeholders (banks, customer and regulators). The framework is built up on basic models of components that are designed on end-to-end security approach based on known frameworks, SABASA information system framework and SONA network architecture have been adopted.

2. Related Work

In this section some of the related research works done are discussed to elaborate their relationship to our work and to see its supportive climate and dissimilarity of those research works with that of ours.

The research work by Thorsten and Weigold on Secure Internet Banking Authentication [5] was one of the related works. The purpose of this study was to describe the current authentication threats and two proposed solutions as well as how these solutions can be extended in the face of more complex future attacks. The authentication schemes and attacks introduced in this work represent the standard of knowledge discussed in various publications dealing with user authentication. However, most of them provide an overview of schemes and corresponding attacks and don't attempt to draw a security landscape by relating them to each other in a sensible way. Moreover, this work presents mainly focusing on authentication solutions one based on short time password and one on certificates and then described how easily these solutions can be extended should sophisticated content manipulation attacks arise. Therefore, the focus of the research was on the two challenge response Internet banking authentication solutions rather than showing the basic security landscape like client-side vulnerabilities and its level of risk, so it doesn't satisfy the need of our study.

The other research work closely related to this research is the one done by Stawowski [1]. This study aimed at identifying and particularly focusing on the penetration testing guidelines for client-side threats that commonly used security technologies find difficult to mitigate by elaborating web browser attacks conducted in encrypted SSL tunnels, HTTP/HTTPS sessions hijacking and use of dangerous applications. In this research work Metasploit, Apache Tomcat, SSl-explorer and BurpSuite have been suggested as list of testing tools with specific required configuration settings.

Since one of our research objectives is to identify the level of client-side vulnerability and its risk level this research work is closer to our research work; however its basic focus was only on penetration testing guidelines for client-side threats.

The third research work reviewed dealt with "threat to online banking "done by Wüeest [4] in which the researcher mainly identified that the number of malicious applications targeting online banking transactions has increased dramatically in recent years. This represents a challenge not only to the customers who use such facilities, but also to the institutions who offer them, as evidenced by an ongoing trail in the US. The researcher described the idea that malicious applications employ two kinds of attack vector-local attacks which occur on the local computer, and remote attacks, which redirect the victim to a remote site. The possibility also exists that both approaches will be combined. The prevalence of malicious applications that steal financial account information has increased dramatically over the last year, often resulting in victims losing hard currency.

There are several factors that may have influenced the evolution of this type of malicious applications, but may be the dramatic increase in their prevalence is just because they have a higher chance to succeed than expected. The case of the businessman in Miami is just one example of many that have succeeded.

The log file on the server storing the data was accessible by anyone, most likely due to a misconfigured web server. A quick look at this log file showed a growing list of account numbers and corresponding passwords. Within an hour, the PHP script had added another 13 valid-looking account credentials. The site was online for another 24 hours before being shut down.

Interpolation of this data leads to the conclusion that the Trojan.Goldun.B attacker had received details for a large number of accounts, providing it with the opportunity to steal hard currency from the victims. The attack vectors used by this kind of malicious application can be categorized in two groups: local and remote attacks. Local attacks happen on the local computer during an online banking session. Remote attacks do not execute code on the local computer, but

redirect the victim to a remote site. Subsequently the reviewed research work mainly concentrated on categorizing attack vectors as local attacks or remote attacks. This may obviously strengthen our research work in identifying one of the basic threats in studying the holistic landscape of Internet banking security issues, client-side vulnerability, risk level, threats and attacks, etc. and its mitigation means. Hence it wouldn't directly satisfy the main objective on our research work.

The fourth research work related to this paper is the survey study made by Ayana Gemechu Bultum [3] in which the author examined adoption of E-banking in the Ethiopian banking industry with respect to the barriers which can influence firms from taking advantage of E-banking systems and expected benefits derived by adopting the system.

The study was conducted based on the data collected from four banks in Ethiopia; three private banks and one state bank. The result of the study indicated that the major barriers the Ethiopian banking industry faces in the adoption of Electronic banking are mainly Security risk, luck of trust which emanated from security risk, lack of legal and regulatory framework, lack of ICT infrastructure, etc.

This study suggested a series of measures which could be taken by the banking industry and by the government to address various challenges identified in the research work. Although the objective of the study was mainly to identify the major barriers that the Ethiopian banking industry is facing in line with adoption of E-banking in which security risk has got focused, this research work can be taken as a reason for the inception of our research ideas.

Considering the foundation of the indication of the result in the research that mainly identified the security risk of E-banking is the major reason for less adoption while this erode the trust of clients our research work mainly focuses of narrowing the gap that are identified in [3]. Nevertheless our research work and the above study basically have dissimilarity in the objective of the research. Hence, it will not satisfy our main and specific objectives.

The fifth related work is the one contributed by Balcha Reba [6], in the research work on state of cyber security in Ethiopia, in which the researcher identified currently cyber security policy and standards are inexistent in Ethiopia. Information security law, ethics and relevant legislation and regulation concerning the management of information in an organization is not yet developed. He elaborated more that, with absence of these conditions, it will be impossible to think of reliable cyber security issues. Therefore, formulation of cyber security policy and standards shall be given due attention. Furthermore, to develop more secure computing environments in the future, staffing of information security function has to count on the next generation of professionals to have the correct mix of skills and experience necessary to anticipate and manage the complex information security issues.

Accordingly, he suggested trainings on information security principles are needed to prepare and create professionals of technology to recognize the threats and vulnerabilities present in existing systems and to learn to design and develop the security systems needed in the near future.

The author tried to put concisely that, information security issue is not only a problem that technology can address alone but also a problem of management to solve. Therefore, legal frameworks in the form of policy and standards are the most prerequisites to establish efficient and reliable cyber security systems.

3. The Proposed Solution

The study in this paper indicated that, for developing countries like Ethiopia, to achieve the most secured Internet banking channel of service, banks should follow the holistic and integrated security approach that include but not limited to participation of all key stakeholders like the bank, customers, regulatory bodies and service providers to fulfill the recommended security implementation framework.

Concepts learned from literature review and survey result, particularly from interview, leads to

propose a framework that realizes holistic approach of IB security for Ethiopian banking industry.

In this research the identified major stakeholders embraces the banks (government and private banks), regulatory bodies (NBE, INSA, FIC, and ECER^{2}T).

The approach for designing the new IB security framework was in such a way that starting by general framework and then going down to detailed components modeling.

The proposed framework is made up of two layers; Inner and Outer layers. The inner layer contains five major models and fifteen (five by three) interrelated sub components identified during the study that equally contribute for holistic multi-layered security approach. The outer layer comprises national regulatory bodies.

The major models in inner-layer that are components of IB security framework proposed in this paper are: IB Customer Site Security Model, IB-AAA Model, IB Risk Management Model, IB Security Defensive & Offensive Model and IB Security Checklist.

The newly designed and proposed Internet Banking Security Framework depicted in the succeeding general framework model (Figure 1) is designed based on Cisco SONA framework principles and we adopted and linked the IB security framework with egg anatomy and its security structure. This is a good example of a bigger issue in IB security. The eggshell security has hard outer shell but a soft runny middle that is represented in IBSF as Outer-layer and Inner-Layer respectively. Once the shell is breached the game is effectively over.

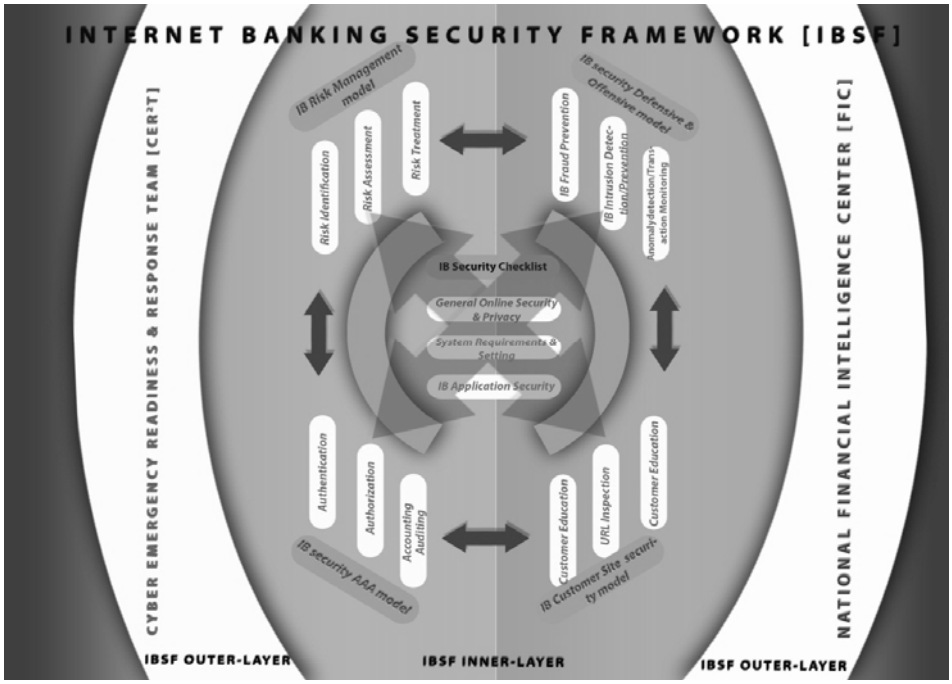

Figure 1: Graphical Representation of the Proposed IB Security Framework

4. Discussion

According to the survey analysis we made, all banks in Ethiopia implementing Internet Banking service motivated to facilitate some security landscapes focusing only on bank site security and believed that customer site security is up to the customer to secure or not. However, it has been identified that the major security threat is social engineering and its loophole is customer site security.

As general observation from literature reviews and interview made, most of the time layered security control is recommended for such channel of services which necessarily use the public network like the Internet. But the current situation observed in the Ethiopian Banking industry is that even the layered

security control that mainly focuses on bank's site security (authentication and network security setting) is not adequate.

The result of this research will help banks to revisit their focus of attention in constructing and implementing IB security to reduce threats and attack logically tied to this channel of banking service. More specifically the research indicated that in addition to bank's side server's security, security enforcement and measures should also equally focus to address well customer site security.

In the proposed framework, customer site security is given due attention to be equally addressed as bank side security do.

5. Conclusion and Future Work

This paper articulates current Internet banking problems and discusses the need for strong security implementation on both server and clients sides for the Ethiopian banking industry

The general objective of this paper was to propose a generic Internet Banking Security framework for the Ethiopian banking industry. To achieve the objective, we selected the Ethiopian banking industry to understand the current IB security by investigating the implementation of this banking service and identify factors that affect the implementation of security in line with this channel of banking service. After gaining knowledge from the survey study, then put it in to the existing knowledge on the subject matter, which are identified from literature reviews. Finally, we come up with a new framework that helps the banking industry for exercising IB security implementation in a secured way.

Therefore we recognized a holistic multi-layered security to overcome the gap currently observed and this has been attested by security experts through interview and discussion conducted. The proposed IB security framework therefore deliberated the inclusion of inner-layer (which includes bank site and customer site security) and outer-layer security (which includes national fraud protection institutes) consideration holistically in a collaborative way of coordination.

The inner-layer of IBSF is built up from five major models: IB Customer Site security model, Risk Management Model, IB Authentication, Authorization and Auditing (AAA) model, IB Defensive model and IB security checklist while the outer-layer consists of Ethiopian Financial Intelligence Center (FIC) and Cyber Emergency Readiness and Response Team (CER^2T).

The framework enables banks to have a standardized approach of addressing IB security by realizing the holistic approach of security requirements

On bank's side, on top of well known security approaches, we proposed out-of-the band authentication approach in which the banks should perform transaction based monitoring and authentication for high value transaction through telephone and SMS and anomaly detection should also be carried out. This should be done in collaboration with national FIC and $ECER^2T$.

It is also worth mentioning that a holistic approach of securing IB environment will reduce the danger of economic & reputation loss.

We recommend that customer side URL inspection tool should further be developed for its performance and compatibility and thorough testing should be done and also in the future the research should consider the usability issues. This depends on what constitutes an acceptable security level and on the trade-off between usability and security.

Developing a program that redirects the message sent from intruders to clients as means of impersonation or phishing to the bank dedicated server to be automatically investigated through some tools or manually by authentication team and/or a program that compares the fake URL or domain name against bank's genuine web address before displaying to customer, i.e., comparing and if got differed either notifying the client or totally blocking before the customer clicks the address would be an ideal to significantly reduce social engineering attack and consequently minimize massive economic loss.

References

[1] Mariusz Stawowski, "Client side Vulnerability Assessment", retrieved from http://www.clico.pl/services/Clientside_Vulnerability_Assessment.pdf, Last accessed on 15/05/2013.

[2] Laerte Peotta and Marcelo D. Holtz, "A formal Classification of Internet Banking Attacks and Vulnerabilities", International Journal of Computer Science and Information Technology (IJCSIT), Vol. 3, No 1, Feb 2011.

[3] Bultum, Ayana Gemechu, "Adoption of Electronic Banking System in Ethiopia Banking Industry: Barriers and Driver", May 2012, retrieved from http://ssrn.com, Last accessed on 01/03/ 2013.

[4] Candid Wüeest, Threats to Online Banking, Symantec Security Response, Dublin, July 2005, retrieved from, http://virusbtn.com/, Last accessed on 01/05/ 2013.

[5] Thorsten K. & T. Weigold, Secure Internet Banking Authentication, retrieved from http://www.zurich.ibm.com, last accessed on 07/04/2013

[6] Balcha Reba, "State of Cyber Security in Ethiopia", Ethiopian Telecommunications Agency, Standards and Inspection Department, Standards Division, June 2005, retrieved from http://www.itu.int/osg/spu/cybersecurity/contributions/Ethiopia_Reba_paper.pdf, Last accessed on May 20/2013.