

Online Banking and Modern Approaches Toward its Enhanced Security

A. Hisamatsu, D. Pishva, and G.G.D. Nishantha

Ritsumeikan Asia Pacific University, Beppu City, Japan

aimahi06@apu.ac.jp, dpishva@apu.ac.jp, gamagelk@apu.ac.jp

Abstract— Digital information has become a social infrastructure and with the expansion of the Internet, network infrastructure has become an indispensable part of social life and industrial activity for mankind. In recent years, the demand for online banking has increased and the number of people who rely on online transactions has tremendously increased. Thus, necessity for a reliable security for online transactions is ever than before. Furthermore, security concerns still exist among the general public when using online applications. The purpose of this paper is to explore why online banking is vulnerable to exploits and to introduce some of the modern approaches to secure online banking in an easy to follow manner. This paper, by pointing out pros and cons of existing countermeasure technologies, tries to serve as a tutorial to raise public awareness in information security developments and conceive a model for the future technology.

Keywords— MSW, MITM, Online Banking, mTAN, FINREAD, AXS-Card, ISC, ZTIC

I. INTRODUCTION

The concept of online banking started in the 1980's and it first became available for client use in 1995 [1]. Since then, the number of banks offering online banking services as well as demand for the service has increased. In the UK alone, the number of people using online banking has increased by 174% in just 5 years from 2001 to 2006 [2]. In the US, 53 million people, or one out of every 4 adults, used online banking in 2005. This corresponds to an increase of 47% when compared to 2002 [3]. Such an increase for online banking is happening in many other countries as well. As demands for online banking increase, the service has become more attractive to attackers and has provoked interests in exploration of spoofing mechanisms against systems providing such services. Consequently, the online banking has suffered from various malicious attacks such as Phishing scams [4], Man in the Middle Attacks (MITM) and Malicious Software attacks (MSW) and it is still vulnerable to such attacks [5]. In fact, the number of cyber crime is increasing every year as society becomes more dependent on network infrastructures [6]. In order to remedy the situation, there have been attempts to develop several counter measure systems using different methods. Such efforts have resulted in the invention of products and prototype systems such as mTAN, FINREAD, ISC, AXS-Card and IBM's ZTIC [7]. However, all

of these products and systems have their strengths as well as weaknesses and shortcoming in their functionalities. In this paper we demonstrate various modern approaches being used against MITM/MSW attacks. Furthermore, a deeper exploration of the IBM ZTIC will be shown to demonstrate the implications and technicalities involved in making online banking a more secured platform and to explain various desirable features a product needs to possess in order to become a feasible and marketable product. Finally we will try to identify a better approach towards making online banking more secured by analyzing and comparing advantages and disadvantages of each of the available approaches.

II. PROBLEM SCENARIO

Person X has an internet bank account and logs on to his/her online account to transfer money to another account to pay some bills. X enters the transfer amount and destination account number and receives a confirmation page and thinks that the transaction went well without any problems. At end of month, X receives the bank balance statement and finds out that large amount of money has been transferred to an unknown account.

Internet banking is vulnerable to MITM/MSW attacks because of the following two reasons [7]:

- 1 The potentially unsafe client PC, where communication between client and server ends.
- 2 All interaction with the user is done through the display and keyboard of the potentially unsafe client PC.

III. MODERN APPROACHES AGAINST MITM/MSW ATTACKS

To make today's banking system stronger against the MITM and MSW attacks, there are two objectives that must be met. Firstly, users must be presented with means to verify and approve transactions [7]. Consequently, users will be able to know the difference between the actual transaction he/she made and the resulting transaction that he/she receives. As such, the user can terminate the transaction right on the spot when the user finds out that something is wrong with the transaction. Secondly a secured communication should be built between the bank's server and the client system [7]. This security issue can be achieved by applying SSL/TLS (Secure

Sockets Layer/ Transport Layer Security) connection between sever and user's computer to avoid MITM attacks.

By applying these two security principle, numerous products have been developed to ensure safety of online banking transactions. These are IBM ZTIC, the most recently developed technology, mTAN, FINREAD, AXS-card, and Internet Smart Card (ISC). In the following sections, we explain their basic functions, their countermeasure approaches, and as well as their advantages and disadvantages.

A. mTAN

mTAN, which stands for mobile transaction number system, depends on the mobile phone technology. Basically, the way it works is that a server-generated one-time password is created and sent to the user's mobile phone via SMS (short message service) along with the details of a given bank transaction. The user can then verify the transaction details and approve it by copying the password to the web browser. The only weakness of this approach is that it considers the mobile phone (SMS) as a trusted platform, assuming that it is unlikely for an attacker to gain control to both the client PC and the mobile phone. But nowadays, because of the 3G technology, cell phones are exposed to the internet all the time which means that the SMS platform is no longer safe from MSW attacks. Furthermore, the increase of mobile phone users makes it more attractive for attackers to hack the system.

B. FINREAD

FINREAD (Financial Transactional IC Card Reader) project aims at establishing a standard for a trusted IC card reading device. The two major objectives addressed by FINREAD are interoperability and security. Interoperability is achieved by allowing applications developed to FINREAD standards to be downloaded and executed independent of the reader manufacturer. The FINREAD reader's security is ensured by having a dedicated secure display and a dedicated secure keypad which provide tamper resitant properties. The FINREAD reader runs its own secure authentication system to avoid counterfeiting and non-authorized copies of either the reader or the card [12]. Thus, FINREAD allows building highly secure Internet banking solutions but it has weaknesses as well –lack of mobility of the device and high costs associated with the production of the device– thus failed to get introduced to the market.

C. AXS-Card

As can be observed from Fig. 1, AXS-Card is a stand-alone device equipped with a display, keypad or fingerprint reader, and an optical interface device. This device provides the user a trusted platform where he/she can verify and approve transactions. The server firstly generates transaction information to be shown on the trusted client device. Then the information is encrypted and displayed on the screen of the client's PC as a flickering code. This code is then read by the optical interface of the AXS-Card, gets decrypted and passes the intact information to the user. In addition, the AXS-card checks the finger print of the user for authentication so that others cannot utilize one's card. Although by doing so, the

MSW attacks can be successfully stopped, a classical MITM can still eavesdrop the whole process of the transaction if the



Figure 1. AXS-Card [13]

attacker has means of decrypting the flickering code.

D. Internet Smart Card (ISC)

An actual Internet Smart Card (ISC) is shown in Fig. 2, which consists of a smart card with an integrated USB interface enabling the card to get attached directly to the PC. With this scheme, no smart-card reader or driver software is required and communication between the ISC and the remote server can be secured via a mutually authenticated SSL/TLS connection. The ISC works like a portable web server where it can generate dynamic HTML pages by itself which means that the card determines the layout of the data display. By doing so, the classic MITM attacks as well as phishing and pharming attacks can be prevented, but the weakness of this approach is that MSW attacks cannot be prevented because the ISC does not comprise a display which shows the user the true information about the transaction and let the user verify and approve the transaction. As aforementioned, the display connected to a PC cannot be trusted.



Figure 2. Internet Smart Card [14]

E. Zone Trusted Information Channel (ZTIC)

In response to the above mentioned attacks (MITM/ MSW) that are paramount in today's internet banking, IBM has developed ZTIC, a USB device similar to a flash memory stick, to provide security to the user in the face of these attacks [8] as shown in Fig. 3.

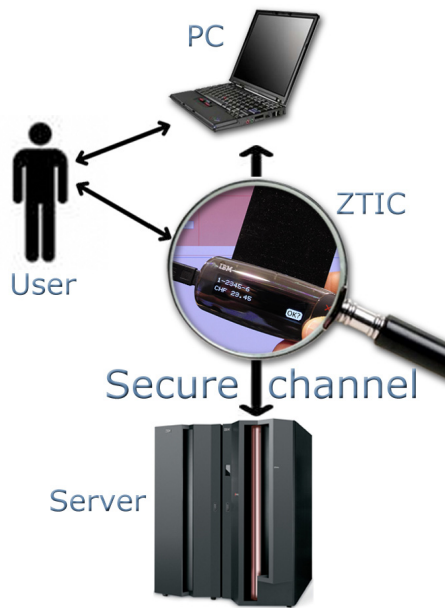


Figure 3. ZTIC Overview [10]

The Zone Trusted Information Channel (ZTIC), which is still at a prototype stage, adds a trusted and tamper resistant secure communication endpoint to the interaction between the clients PC and the Bank's Server [9]. The ZTIC is "hooked" into the communication path by a networking proxy running on the PC and it secures the system by constantly scanning through all the communication between the user's web browser and the server for sensitive information such as money transfer.

For every sensitive transaction, the ZTIC is designed to intercept the communication flow, extract vital information for display and it only executes the transaction after the user verifies that the operation is safe[7]. The verification is done by pushing the OK button after reading the contents on the display screen on the ZTIC and confirming the user's intended request. With regards to non sensitive information, ZTIC is designed to pass it on without the user's verification, so it doesn't result in user annoyance. It has, however, the disadvantage of slowing down transaction speed. Furthermore, because PCs come with USB ports at different locations and orientations, viewing of the ZTIC display screen may become difficult on some PCs.

IV. DEEPER EXPLORATION OF ZTIC

Considering that ZTIC is a recently developed technology and IBM claims to have addressed the shortcomings of earlier developed products, we decided to explore this product in some details.

A. ZTIC Operations

ZTIC includes a processing unit, volatile and persistent memory and it has a small display, two buttons which are ok and cancel) and (optional) smart card reader [7]. As can be seen from Fig. 4, ZTIC is supported by 2 network protocols, which are Transport Layer security and Socket Secure Layer.

TLS ensures that no third party may eavesdrop or tamper with any messages, when communicating between the server and client. TLS is a protocol that ensures privacy between communicating applications and their users on the internet. SSL has been universally accepted on the WWW for authenticated and encrypted communication between client and servers. SSL is a protocol that creates a secure connection between a client & a server, over which any amount of data can be sent securely.

ZTIC creates secure connection that's protected by TLS/SSL between user web browser and its own proxy; it also creates secure connection between back end server and its own secure display. It appears that eventually this can create a reliable secure connection between users and servers.

The operation begins when a user connects ZTIC to the computer. The user then interacts with a web browser to access the back end server. At that moment, TLS/ SSL connection will be created between the web browser and proxy, proxy and back end server as shown in figure 4. When the user makes a transaction, the transaction information will be shown on the secure display. Finally, after verification of correctness of the information, the user will then click ok button to complete transaction through SSL/TLS connection between secure display and back end server.

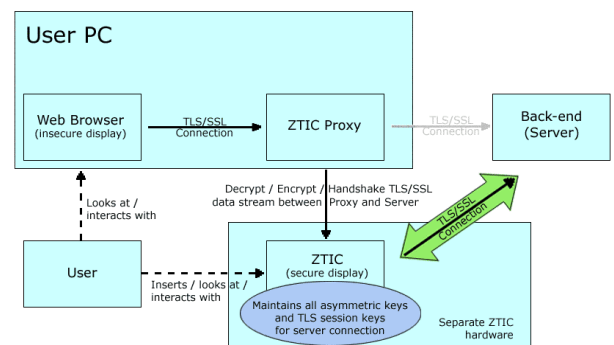


Figure 4. ZTIC Technical Operation [11]

B. Usability, Design and Evaluation

IBM still needs to test their product with users through survey or other means to see whether ZTIC can become an accepted product. For its ease of use at the client side, IBM will also need to explore ways to replace the proxy by VPN-like (Virtual Private Network) system to avoid the dynamic modification of web page. Moreover, ZTIC may need to come with a cable for attaching it to inaccessible USB ports and have a toggle option for the orientation of the display.

In term of certification, because ZTIC is still at a prototype stage, it has not yet been exposed to appropriate security evaluations and tests for vulnerabilities in the system. One of the potential vulnerability areas that needs to be tested is the buffer overflow error, which happens when data is written in part of the memory not allocated for storing data, thus erasing other important data and causing malfunctions.

C. Performance and Functionality Improvement

As it is at a prototype stage, there are no wide means for performance measurement, other than a handful of trial measurements that have been performed by a few banks. The results of performance seems to be good except for the slight slowdown in the speed of the transaction[7].

According to IBM, the most time-consuming part is the cryptographic operations within the ZTIC, which uses symmetric algorithms such as the AES for encrypting/decrypting the data stream and asymmetric algorithms during SSL/TLS session establishment [7]. To solve this speed problem, IBM plans to change the symmetric encryption routine into assembly code, a low level computer language, which can speed up the performance by up to 4 times.

Another method to increase the speed of decrypting transaction data received from the servers is to possibly perform symmetric operations within the proxy.

IBM is also considering to come up with a version of ZTIC that allows the insertion of ID1 (credit card size) smart card to make its usage more flexible. Furthermore, for maintenance purposes, ZTIC may be made to be updatable by a server with new HTTP profiles as well as renewed user credentials and certificate. A detailed listing of ZTIC functionalities in terms of how it addresses various design goals are shown in Table 1.

Table 1. A List of ZTIC Design Goals & Implemented Solutions [7]

Design Goals	ZTIC Solutions
CIA	Operation of SSL/TLS
Protection from Malware	Display Critical Data On Trusted Device; No Caching of Data on the PC
Protection from MITM Attacks	Mutually Authenticated End-to-End Session Establishment
Protection From Phishing Attacks	Automatic Session Establishment with Securely Stored Credentials
Non – Repudiation	Use of Smart Card Slot and PIN Entry
User Acceptance / Convenience	Small, well-known form factor; No Software Installation, Works on All OS; Fast User Interaction
Service Provider Acceptance	Almost None Server Side Changes Required; Ease-of-Installation
Cost – Efficiency	Low-Footprint software on Cheap Chip; Option to Retain Smart Card Investments

V. SUMMARY OF MODERN APPROCHES

As can be observed, all the modern approaches and systems have their advantages and disadvantages. The mTAN allows a user to obtain critical information through the cell phone but it does not account for the vulnerabilities that cell phones have and the possibility for its exploitation. The FINREAD

provides a highly secured internet banking solution by providing a separate tamper resistant device but it uses expensive hardware and is not very mobile. The AXS-card can provide protection from malware by using its optical device to read the flicker code and display on its screen but it does protect the user from MITM attacks. The ISC protects users from phishing and MITM attacks by automatically establishing a mutually authenticated session with the bank server but it does not protect the user from malware. The ZTIC, on the other hand, provides a secured internet banking solution by exposing the attacks to the users when completing an online transaction, but has the disadvantage of slowing down the transaction speed and having inflexible display screen.

Table 2. Pros and Cons of Each Approach

Products	Pros	Cons
mTAN	Information Is Transmitted Through Another Platform	Does Not Account For Vulnerabilities Of Cell Phones
FINREAD	Highly Secured Internet Banking Solution	Lack Of Mobility And High Cost Of Production
AXS-Card	Protection From Malware	No Protection From MITM Attacks
ISC	Protection From Phishing And MITM Attacks	No Protection From Malware
ZTIC	Highly Secured Internet Banking Solution	Time Consuming Operations: Slower Transaction Speed

VI. CONCLUSION

The usage of online banking is increasing worldwide and a secured means of transacting is in high demand. Thus there have been attempts to develop counter measures using different methods and such efforts have resulted in the development of various systems and products such as the mTAN, FINREAD, AXS-Card, ISC and ZTIC.

The ZTIC is still at the prototype stage and further improvement in its functionality and performance is expected. Its present attributes, however, seems to surpass any of the competitors in terms of effectiveness and ease of use at both client side and server side.

We showed that IBM ZTIC maintains data confidentiality and integrity through the use of SSL/TLS protocols. It provides protection against MITM/MSW attacks by means of intercepting communication flow from client to server and displaying critical information on the 3rd party device (ZTIC). Its compact size, plug-and-play characteristics, minimal server setup requirements can also make it a more attractive product. Finally the ZTIC is also cost efficient since does not use expensive electronic components. We can therefore conclude that ZTIC is an innovative device with the aim of making online banking more secured. If it successfully passes through wide usability test and performance measurement criteria, it

has a good potential to become a choice product for online banking application in the near future.

ACKNOWLEDGMENT

The authors would like to thank Mr. Jin, Mr. Bilesanmi, Mr. Fofana and Mr. Sukhbaatar for their useful help and valuable comments during the initial phase of this work when it was done as a class project.

REFERENCES

- [1] A. Shandilya. (2007) Online Banking: Security Issues for Online Payment Services. [Online]. Available: <http://www.buzzle.com/articles/online-banking-security-issues-for-online-payment-services.html/>
- [2] APACS. (2009) Online banking usage amongst over 55s up fourfold in five years. [Online]. Available: http://www.apacs.org.uk/media_centre/press/08_24_07.html/
- [3] PewInternet. (2009) Online Banking 2005. [Online]. Available: <http://www.pewinternet.org/Reports/2005/Online-Banking-2005.aspx/>
- [4] Easier Inc. (2008) Cyber crime soars with rise of online banking. [Online]. Available: http://www.easier.com/view/Finance/Banking/Online_Banking/article-201056.html
- [5] University of Michigan. (2008) Security flaws in online banking sites found to be widespread. [Online]. Available: [http://www.ns.umich.edu/htdocs/releases/story.php?id=6652 /](http://www.ns.umich.edu/htdocs/releases/story.php?id=6652/)
- [6] Consumer Fraud Reporting. (2009) Internet Fraud, Scam and Crime Statistics. [Online]. Available: http://www.consumerfraudreporting.org/internet_scam_statistics.htm/
- [7] Thomas Weigold, Thorsten Kramp, Reto Hermann, Frank Höring, Peter Buhler, Michael Baentsch, "The Zurich Trusted Information Channel – An Efficient Defence against Man-in-the-Middle and Malicious Software Attacks", In P. Lipp, A.-R. Sadeghi, and K.-M. Koch (Eds.): TRUST 2008, LNCS 4968, pp. 75–91, 2008.
- [8] IBM Zurich. (2009). IBM Zone Trusted Information Channe. [Online]. Available: <http://www.zurich.ibm.com/ztic/>
- [9] Michael Baentsch, Peter Buhler, Reto Hermann, Frank Höring, Thorsten Kramp and Thomas Weigold, "A Banking Server's Display on your Key Chain", ERCIM News 73, online edition, April 2008.
- [10] IBM Zurich. (2009) IBM Zone Trusted Information Channel. [Online]. Available: http://www.zurich.ibm.com/ztic/images_fig1.html/
- [11] IBM Zurich. (2009) Technical Operation of ZTIC. [Online]. Available: <http://www.zurich.ibm.com/ztic/operation.html/>
- [12] FINREAD. (2009) Press Pack. [Online]. Available: <http://mediakomm.difu.de/aktuell/FINREAD-PRESS-PACK-v5.pdf/>
- [13] Red Dot Award. (2009) AXS-Card Pro - The Internet Passport Biometric Secured Token. [Online]. Available: <http://en.red-dot.org/2784+M5c30bbe5994.html/>
- [14] Giesecke And Devrient. (2009) Internet Smart Card Technology. [Online]. Available: http://www.gi-de.com/portal/page?_pageid=42,54860&_dad=portal&_schema=PORTAL/