A New Approach to Enhance Internet Banking Security

M. F. Mridha
Department of CSE,
University of Asia Pacific,
Dhaka, Bangladesh

Kamruddin Nur
Department of
CSE, Stamford University
Bangladesh

Aloke Kumar Saha
Department of CSE,
University of Asia Pacific,
Dhaka, Bangladesh

Md. Akhtaruzzaman Adnan
Department of CSE,
University of Asia Pacific,
Dhaka, Bangladesh

ABSTRACT
E-Banking in www is growing exponentially, but here consumer authentication, credential confidentiality, transaction information integrity are growing concerns. In this research work emphasize the protection of online banking. At first, E-banking is analyzed for all kinds of vulnerabilities and a practical investigation of all type of attacks is carried out. In this paper, a security-aware architecture is introduced to protect from several attacks. The proposed system has a secure protocol and certificate verification mechanism. The proposed system checks the authenticity of the sender first; then if appropriate, processes the incoming messages and stores them for further processing. This covers everything from phishing site detection to two-factor authentication. Having declared all current schemes for protecting online banking lacking in some way, the key aspects of the problem are identified. This is followed by a proposal for a more robust defense system which uses a small security device to create a trusted path to the customer, rather than depend upon trusting the customer's computer. This is followed by a description of a demonstration implementation of the system.

General Terms
Electronic Banking Security, E-Banking Security Protocol

Keywords
E-Banking Security Protocol, E-Banking Authentication

1. INTRODUCTION
The modern technology innovations are continuously improving and its impact changing social cultural and economic relationship vigorously. Multitude of e-services: e-commerce/e-payment, e-voting, e-governance, are revolutionary ideas that make life more easy, time saving, accessible and convenient. E-commerce service growth is exponential due to its speed, digitization, accessibility, user friendly, time saving in nature. E-payment is an integral part of e-commerce. There are three basic types of e-payment system: business to business (B2B), consumer to consumer (C2C) and business to consumer (B2C). Shehzad Ashraf et al. [1] B2C system got popularity as the universalization of www at 1990. A number of B2C systems requires debit/credit card for online payment. With the innovative ways of e-payment system, users are enjoying the facility to save time, money by using a number of online services, like e-transactions, payment of bills, purchase of goods etc.

At present the online banking system will connect to the core banking system operated by a bank and is in contrast to branch which was the traditional way customers accessed banking services. To access a financial institution's online banking facility, a user with internet access would need to register with the institution for the service, and set up a password and other credentials for customer verification. Financial institutions now routinely allocate customers numbers, whether or not customers have indicated an intention to access their online banking facility. Combined with online retailers there is a lot of money changing hands, directed only by communication over the Internet. This is very convenient and the ready access to the Internet in all first-world countries, coupled with the cost savings from closing bank branches, is driving the deployment and adoption of these services. Purely online transactions, how-ever, lead to increased risk. Now it is a simple task to target millions of people and a small percentage falling foul of the scam still represents a large return on investment. As few who use the Internet can have failed to notice this has led to the birth of the phishing scam and its huge growth. Phishing remains one of the highest profile online attacks against financial institutions. In reaction to the defensive schemes developed by the targets of attacks, many criminals have started to become more sophisticated. This is still lost in the noise of the remarkably successful but simple attacks, which explains why very few people are working on more robust systems. in this research work we focus on the attack and defense landscape surrounding online banking and how these high profile targets and their users can best be protected and shows that while the state of the art in attacks is very much more sophisticated than simple phishing attacks, they are still sufficiently low profile that few people are considering them. the followed by the application of the system to Internet shopping and to pro-viding better protection for consumers in the event of disputes with their bank. Much of this work was presented at the 12th Nordic Workshop on Secure IT-systems held at the University of Reykjavik in October 2007 [2].

The rest of the paper is organized as follows: Section II Motivation for the work. In section III literature review is discussed. In section IV used security model and their vulnerabilities are presented. The proposed security-aware architecture is introduced in Section V. Finally, this work is concluded in Section VI.

2. MOTIVATION
In this era the world is moving towards with an automated payment system that is compatible with international standards. But growing number security concerns are also hindering its popularity. It is evident that, safe and secure-transaction is the main concern of customer. Internet banking is a worthwhile research study so that the quality of services

in our banking sector can be enhanced for the future and internet banking has been widely studied in developed countries. Few studies have been done in developing countries, and it has not been investigated in our financial sector. Statistics shows that there is problem in using the Internet in our banking sector. The research aims at enriching the knowledge and understanding of factors affecting adoption of Internet Banking security in our banking sector. Specifically, the main objectives of this study are: Investigate the adoption of internet banking transactions security measure by individuals in our country and also our service provider.

3. LITERATURE REVIEW

The Secure Electronic Transaction (SET) is public key encryption based security mechanism developed to maintain to end security of debit/credit based transaction. SET architecture utilizes PKI to overcome limitation of SSL/TLS. Three things are mandatory to operate in SET are: digital signature certificate, dual signatures and digital wallet. SET maintains confidentiality and privacy of consumers credentials and purchase information by separate public key encryption, while in data transmission and data storage [2]. Schneier introduced the "attack tree" method of describing and analyzing the attacks on a system [3]. Attack trees are a form of root-cause analysis [4] which provides a graphical way of describing the security of systems. Goals will be something like 'steal money' and this is broken down into the steps required to achieve that goal, getting into more detail further down the tree. Attack strategies: There are four main types of attack on e-banking. All of the attacks seen at the moment fall into the first two categories: getting authentication credentials from the victim or modifying the victim's legitimate transactions. Credential harvesting, a very well-known online fraud in the UK is phishing, which is an attack de-signed to convince the victim to give away their online banking credentials to a third party. This and other similar scams or attacks which reveal credentials to the attacker fall into the class of credential harvesting. Phishing web sites deserve a separate section. They are the most commonly seen form of credential harvesting attack in the wild, usually combined with an email which tricks the user into accessing the web site. Someone closely connected to the thief must be physically close to the person while they are entering the PIN. The latter modifications allow for some scaling of the attack and in this form it has been seen on automated teller machines (ATMs) [6, 7] and in a number of petrol stations [8]. The latter being an insider attack and the former third-party tampering. It still, however, does not benefit from the economies of scale of the Internet and has quite a high level of risk.

E-payment security requirements: As e-transaction propagates, the financial information/consumers credentials are sent over insecure public wired/wireless network, so it requires a rigorous security mechanism that can ensure trust based mutual authentication, confidentiality and privacy, integrity, non-repudiation, prevention of double spending in a particular transaction. Following are the mandatory security factors to be considered in an e-payment system.

Authentication: The involved parties like the consumers, issuer/acquirer banks and e-service providers/merchants must be authenticated to each other in order to avoid false transaction and maintain consumer confidence.

Confidentiality: The e-transaction information, consumers credentials should be hidden from outsiders to refrain attacker. Further each of the participants should only know his preferred information.

Integrity: None should be allowed to modify, edition, alteration, deletion of transaction information.

Non-repudiation: The involved participants in a particular transaction will not be able to deny their activities during a particular transaction. Related information should have recorded. Privacy protection: Privacy protection is to safeguard the personally identifiable information (PII). Each of the involved participants should only know his desired information. Merchant should know only order of goods details, not the consumer's card number, hidden number, bank account. Bank should know only users purchase confirmation, bank account, and amount to be disbursed. Moreover, an outsider must not be able to trespass, espionage or release any information regarding the transactions.

4. USED SECURITY MODELS

At present the models used in online banking systems are based on several security layers, consisting on diverse parallel solutions and mechanisms which focus at protecting the banking application and the user's data, providing identification, authentication and authorization properly. Different types of security models are discussed below:

A. *Digital Certificates:* Digital certificates are used to authenticate both the users and the banking system itself. This type of authentication depends on the existence of a Public Key Infrastructure (PKI) and a Certificate Authority (CA) that reflects a trusted third-party who signs the certificates attesting their validity.

B. *One-Time Password Tokens:* One-Time Password devices are generally used as a common authentication factor that may be requested in target or random situations. This type of devices render captured authentication data useless for future attacks through the use of randomly changing passwords which can be used only once.

C. *One-Time Password Cards*: One-Time Password Cards constitute a less expensive method for generating dynamic passwords, also providing a common authentication factor. However, in some banking systems, passwords generated by OTP cards are reused a number of times before being discarded, rendering this system vulnerable to short term replay attacks.

D. Browser Protection: In this security model, the system is secured at the Internet browser level, which is used to access the banking system. The user and his browser are protected against known malware by observing the memory area allocated by the browser in order to detect such type of malware and hinder credential theft and capturing of monetary information.

E. Virtual Keyboards: Virtual keyboards were used to thwart the efficient use of key loggers. These devices are usually based on Java and software based cryptography, allowing portability between different devices. At present they are being replaced by other more efficient methods which require less processing power and slower transmission rates.

F. Device Registering: This model restricts access to the banking system to previously known and registered devices. Hardware fingerprinting techniques are

developed in conjunction with user identification through secret credentials.

G. CAPTCHA: Completely Automated Public Turing test to tell Computers and Humans Apart, is a model presently used in some banking systems whose objective is to render automated attacks against authenticated sessions ineffective. This model requires the legitimate user to input information conveyed as scrambled images which are difficult for automated robots to process and recognize.

H. Short Message Service (SMS): This method has applied in some banking systems to notify users about transactions requiring their authorization. It provides a second authentication channel for transactions that fit certain characteristics by sending to the user a set of characters which have to inform in order to authorize and process the transaction through the online banking system.

I. Device Identification: Device identification is generally used together with device registering but it is also used as a stand-alone solution in online banking systems that aim at facilitating user access. This identification method is based on physical characteristics of the user's device through which it is possible to identify its origin and history information.

J. Positive Identification: Positive identification is a method in which the user is required to input some secret information only known to him in order to identify himself. It is adopted as a second authentication method.

K. Transaction Monitoring: In this model is not thoroughly analyzed in the present work, it is presently applied in all online banking systems, each of them using different techniques. Artificial intelligence, transaction history analysis and other methods that identify fraud patterns in previously processed transactions are among the various approaches to transaction monitoring.

4.1 Vulnerabilities of online Banking Systems

In Table 1 shows the vulnerabilities which affect each security model discussed in this research work. It does not represent all the vulnerabilities which may exist in such models but shows that those models are presently vulnerable to several attacks. The correct identification of the threats faced by current Internet banking systems is essential for designing more efficient models which provide a higher level of security.

Table 1: Vulnerabilities in Internet Banking Systems

Security Models Vulnerabilities	Security Models Vulnerabilities
Digital Certificates	Digital Certificate is possible to export A1 certificates and remotely utilize them and A3 certificates can be applied by more than one user at the same time, allowing adversaries to use stolen certificates.
OTP Token	OTP Token is the generated password may be captured and applied in real-time; The user may be lured into informing the password for unauthorized transactions through the use of social engineering.
OTP Card	Malware may collect passwords or lure the user into informing them.
Browser Protection	New malware remain active until they are detected by the model; Counterfeit online banking system web pages which prevent the protection from properly loading can be used to make the user input his sensitive data in an unsafe environment.
Virtual Keyboard	Known tools such as Screen loggers or mouse loggers may capture sensitive information; Decryption techniques and attacks focused on flawed encryption algorithms can also be applied.
Device Registering	Characteristics thought to be unique to the user's device may be reproduced; Information regarding the device's register can also be reproduced. An attacker can apply social engineering to persuade the user to authorize and register a malicious device.
CAPTCHA	The methods applied to scramble the information in the image are too simple, making it possible to extract the desired information using OCR software.
Short Message Service	The attacker may alter the cellular phone number to which the authorization messages are sent.
Device Identification	Device Identification is a characteristics thought to be unique to the user's device may be reproduced.
Positive Identification	In this model Information thought to be only known by the user may leak in the Internet and social engineering techniques may be used to discover such information
Transaction Monitoring	In this model malwares are creating behavior profiles which enable them to impersonate the user profile.

5. PROPOSED SECURITY-AWARE ARCHITECTURE

Security is the main concern and vital issue for the success of e-banking services. Multiple authentication mechanism can ensure consumers authenticity as well as remain anonymity. In this work, we introduce a secure protocol in E-Banking

architecture and a certificate to enhance the security of E-banking process. The proposed secure protocol in a receiver system processes certificate based messages before starting the transaction. In this section, we explain the proposed architecture with a "Secure Protocol" and Certificate.

5.1 Proposed E-banking architecture with Secure Protocol

A secure protocol is introduced in E-banking system to enhance the security. The newly introduced secure protocol is a data processing unit to provide an extra layer of security in E-banking systems. Whenever data comes through the secure channel, at first the secure protocol checks the data and decides whether the data should be started for further processing or discarded. Thus, if anything goes wrong during data processing or any malicious data is found, the secure protocol discards the data and terminates the entire transaction. The secure protocol has a processing stack, which is based on handshaking scheme, certificate verification, signature verification, and alert mechanism. A typical handshaking scheme is used in this work to maintain the sequence of the record's peer-to-peer and card emulation modes. The handshaking scheme notifies the sender about the acknowledgment of getting certificate and data. For reader-writer mode, it should be noted that data from tag comes at a time; therefore, the acknowledgement of handshaking scheme is not needed. The handshaking scheme initiates the process, as shown in Figure 1, by asking for a certificate. If the certificate and the signature match, request is stored for further processing. If there is any error at any point of time in the processing stack, data is discarded from the system and alert messages are generated. Newly introduced certificate verification process verifies the certificate of the tag. Certificate authority provides certificates to the authorized tag users. The certificate contains various information such as - Version, Certificate-Serial-No, Algorithm, Parameter, Issuer-Name, Expiry-Date, Issuer-Unique-Identifier, and Sub-Unique-Identifier. Certificate verification process compares every field of the received certificate with the stored certificate. If any mismatch occurs in this process, the alert mechanism sends alert messages to the user and terminates the process. The signature verification system verifies the signature. In the next step, the hash values of signature and message are computed. If two hash values are same (the signature of the message is verified), data is processed for transaction; otherwise transaction is discarded, and the alert mechanism sends alert messages and terminates the process.

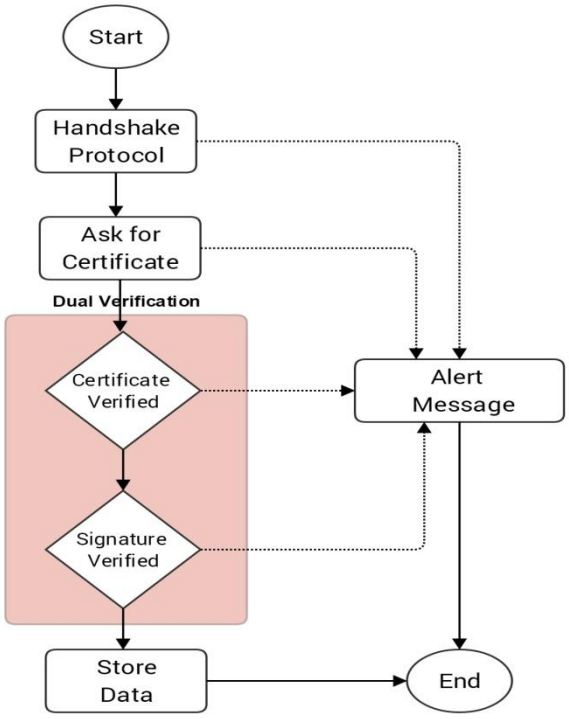

Figure 1: Proposed Secured Handshake Protocol with Certificate and Signature Verification

In the proposed method a modified alert mechanism is introduced to monitor the secure protocol and generate messages as needed. Alert messages include:

1. If no appropriate certificate is received or available then it will generate No Certificate.

2. If the received certificate is corrupted then it will generate Bad Certificate.

3. If the received certificate is not supported then it will generate Unsupported Certificate.

4. If the received certificate is expired then I will generate expired certificate.

5. If parts of the received certificate do not match then it will generate unknown certificate.

5.2 Certificate and Signature

Verification The receiver gets the certificate and decrypts it with the stored public key. If the certificate cannot be decrypt (most likely due to attacks) by the secure protocol, it terminates the whole process through the alert protocol. After passing the certificate verification, the rest of the task is processed (specifically, the hash values of the signature record is calculated and compared). If the calculated hash value matches with the stored hash value, the message is considered as original then E-transaction is executed. Otherwise, the message is discarded and the process is terminated through the alert mechanism.

6. CONCLUSION

This paper suggests a novel security protocol which is completely secure and user friendly and not burden to implement. Banking fraud cannot be eliminated without a dedicated, trusted security protocol. Stopping common forms of e-banking fraud is not sufficient to protect against the

criminals. The possible avenues of attack on Internet transactions and showed that the traditional phishing attack is only a small part of the attack landscape. However, general purpose computers are not themselves trustworthy agents of the user's intentions. In this work, a data processing secure protocol and a certificate per transaction are proposed to provide extra security.

7. REFERENCES

[1] Bowman, M., Debray, S. K., and Peterson, L. L. 1993. Reasoning about naming systems. .

[2] Ding, W. and Marchionini, G. 1997 A Study on Video Browsing Strategies. Technical Report. University of Maryland at College Park.

[3] Fröhlich, B. and Plate, J. 2000. The cubic mouse: a new device for three-dimensional input. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems

[4] Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[5] Sannella, M. J. 1994 Constraint Satisfaction and Debugging for Interactive User Interfaces. Doctoral Thesis. UMI Order Number: UMI Order No. GAX95-09398., University of Washington.

[6] Forman, G. 2003. An extensive empirical study of feature selection metrics for text classification. J. Mach. Learn. Res. 3 (Mar. 2003), 1289-1305.

[7] Brown, L. D., Hua, H., and Gao, C. 2003. A widget framework for augmented interaction in SCAPE.

[8] Y.T. Yu, M.F. Lau, "A comparison of MC/DC, MUMCUT and several other coverage criteria for logical decisions", Journal of Systems and Software, 2005, in press.

[9] Spector, A. Z. 1989. Achieving application requirements. In Distributed Systems, S. Mullender.