



Securing E-banking transactions by OTP (one time password) method (Look at SMS Technology)

Syed Masaid Zaman¹, Dr. Manoj Kumar², Dr. Qamar Parvez Rana³

¹(Ph.D Scholar (Department of IT) Shri Venkateshwar University Gajraula, U.P-INDIA

²(Department of IT) Shri Venkateshwar University Gajraula, U.P-INDIA

³(Department of Computer sciences) Jamia Hamdard, Hamdard University New Delhi-INDIA

Abstract: *There are a continuously rising number of customers who use electronic banking because of its expediency. But the security and privacy of Information may be one of the prime concerns to the Electronic banking users. The issue with Electronic banking applications is that they send information straightforwardly to customer in plain text form compromising with security. The solutions to the security issues require the use of software-based solutions that occupy the use of encryption algorithms. For this we suggest a challenge/response-based short-time password authentication methods using Symmetric cryptography in mixture with Software Security model. In this conceals bank hides clients transaction data is secure SMS using IDEA symmetric cryptographic algorithm and propel it to customer application supported handset. Customer application decodes information in secure manner the encryption and decryption are characterized by a secret key that the legal parties have to possess. So, in face of the present security issues and the developing number of attacks and consequent frauds, new internet banking systems ought to be planned as to given better authentication and identification.*

Keywords: Electronic Banking, security standards, short-time passwords.

I. INTRODUCTION

The security models for online banking systems currently in use are emphatically based on Internet banking user identification and authentication methods, which are also the mechanism where most Internet banking systems' vulnerabilities are found. The existing SMS system does not have any built-in procedure to authenticate the text and offer security for the text transmitted as data, because most of the applications for mobile devices are designed and developed without taking security into consideration.

1(a) Security:

Security of the transactions is the prime concern of the Internet-based industries. The lack of Security may result in serious damages the security issue that will be further discussed in the next section along with the possible attacks due to the inadequate protections. The examples of potential hazards of the electronic banking system are transferring funds, and minting electric currency, etc.

1(b) Authentication:

Encryption may help to make the transactions more secure. The Internet of today has turned into a fundamental piece of our Everyday life and the proportion of users expecting to be able to manage their bank accounts anywhere, anytime is constantly developing. As such, Internet banking has come to age as a crucial segment of any financial institution's multi-channel methodology, based on the assumption that only an authentic user is able to do so, successful authentication ultimately enables a certified user to access his private data.

1(c) Short-Time Password Solution:

Taking into consideration today's pervasiveness of malicious software and phishing attacks, any Internet banking solution must be defiant against stealing attacks. To overcome from this we suggest a challenge/response-based short-time password authentication method by means of symmetric cryptography in combination with a Software Security Model. The short-time password solution is in use at in software-based security systems, the coding and decoding of information is done using specialized security software.

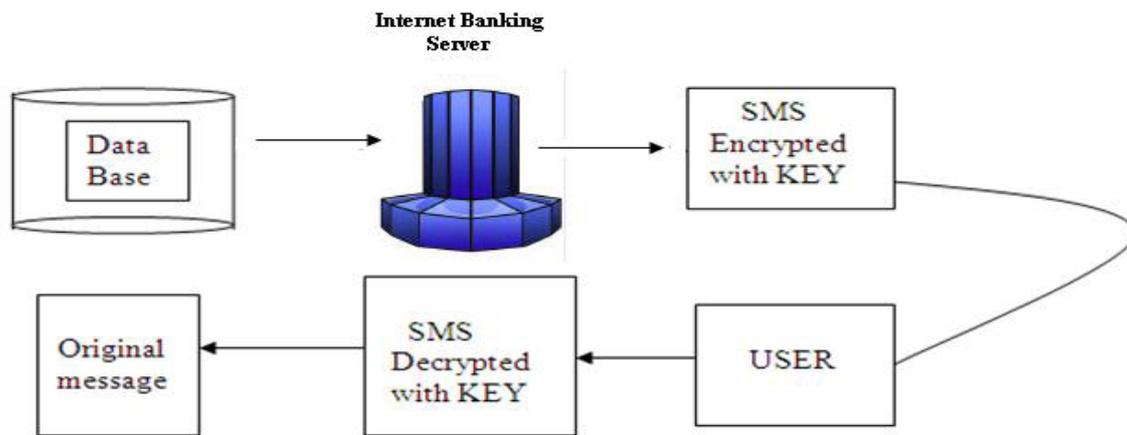


Fig 1: Architecture of Secure Transaction

The Figure (1) illustrate the Architecture of the Secure Transaction, where the Bank Server send the Encrypted message to the User and the User Decrypt's the message [8, 9], the encryption and decryption are characterized by a secret key that all legal parties have to posses. The application is build up using programming language Java and the J2ME environment. [10, 11]

II. SECURE SMS MESSAGES USING CRYPTOGRAPHY

The majority of the attacks directed at online banking systems target the user (the weakest link in the Chain), focusing on getting authentication and identification information through the use of Social engineering and compromising the user's Internet banking access device in order to install malware which repeatedly performs banking transactions distant from obtaining authentication data. This fact indicates that secure internet banking systems should afford security mechanisms as user independent as possible, mitigating the risk of user related information's leaks and security issues affecting the system and leading to fraud

2(a) SMS Security Algorithm: The International Data Encryption Algorithm (IDEA)

SMS messages are occasionally used for the exchange of confidential data such as social security number, bank account number, password etc. A typing mistake in selecting a number when sending such a message can have severe consequences if the message is understandable to any unauthorized receiver. In this application for sending encrypted SMS messages using cryptographic methods based on the IDEA Algorithm. The encryption algorithm is characterized by a secret key. The application is build up using programming language Java and the J2ME environment.

International Data Encryption Algorithm (IDEA) is very sheltered; IDEA operates on 64 bit blocks using a 128-bit key, and consists of a series of eight identical transformations (a *round*) and an output transformation (the *half-round*). The processes for encryption and decryption are similar IDEA derives much of its security by interleaving operations from different groups modular addition and multiplication, and bitwise eXclusive OR (XOR)

III. IMPLEMENTATION

In addition, communicating over wireless networks with a mobile device brings its own set of inherent risks. With familiarity and equipment, it is possible to intercept data most anywhere between your device and the end point of your intended communication. A J2ME system which is installed in all the mobiles users those who are registered with this system. The user who received the encrypted message has to enter into this application and present the corresponding key to decrypt and see the message. The encryption application associated data is in Java 2 Micro Edition (J2ME) application (MIDlet).

3(a) Bouncy Castle

Bouncy Castle is an open source encryption library; there is a lightweight edition suitable for use with J2ME. Bouncy Castle is an open source Java API for encrypting and decrypting data. Bouncy Castle is a Java Cryptography Extension (JCE) provider. JCE is an elective package that provides support for ciphers, keys, and message validation within the Java 2 Platform, Standard Edition (J2SE). Basically, a provider offers one or more algorithms for the encrypting and decrypting of data. To date, Bouncy Castle supports over 20 engines. **ProGuard** is an open source Java class files obfuscator. This is used to obfuscate the contents, which requires fewer memories to store.

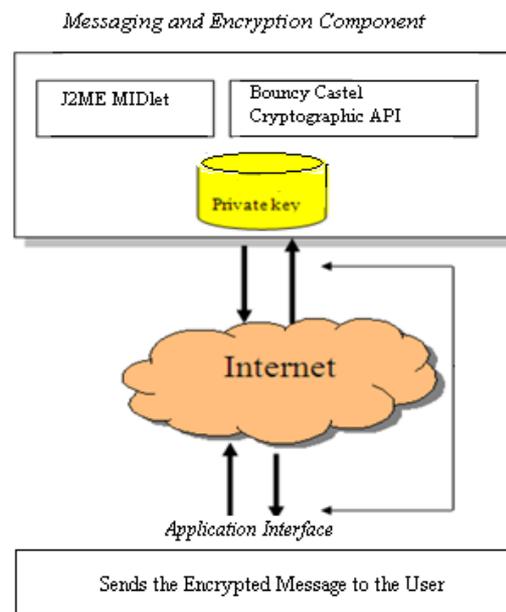


Fig 3: Shows the Messaging and Encryption Component

To execute the following process, the Sun Microsystems Wireless Toolkit formerly known as Java 2 Platform, Micro Edition (J2ME) Wireless Toolkit) is used. It is a state-of-the-art toolbox for developing wireless applications that are based on J2ME's Connected Limited Device Configuration (CLDC) and Mobile Information Device Profile (MIDP), and designed to run on cell phones, conventional personal digital assistants, and other small mobile devices. The toolkit includes the emulation environments, performance optimization and tuning features. Wireless Toolkit is an integrated development environment (IDE) creates J2ME MIDlet. The WTK contains an IDE, as well as the libraries required for creating MIDlets.

A MIDlet is created which accepts the text to be encrypted along with the key (Secret key) by using which the Encryption process is done by using IDEA algorithm. The Symmetric ciphers use the same key to encrypt and decrypt data, which is known as *secret key*. That is, the value of the key is kept secret between the two parties – those who encrypt the data and those who decrypt it.

The J2ME MIDlet which accepts the text and encrypts the text which is send to the user, when the user receives the Encrypted text can decrypts the text to find the original text. The Short time passwords or any Bank related confidential data can be secured by the using the Cryptographic techniques.

IV. CONCLUSION AND FUTURE WORK

Internet banking is offering its customers with an extensive range of services. Customers are able to interact with their banking accounts as well as make financial transactions from virtually anywhere without time limitations. In order for electronic banking to continue to grow, the security and the privacy aspects need to be enhanced. With the security and privacy issues resolved, the future of electronic banking can be very wealthy. The future of electronic banking will be a system where users are able to interact with their banks "worryless" and banks are operated under one common standard. The security models for online banking systems currently in use are strongly based on Internet banking user identification and authentication methods, which are also the components where most Internet banking systems' vulnerabilities are found.

This paper describes current online banking problems and discusses the need for security testing for online banking. The system allows user to carry out all banking transaction securely from anywhere, anytime. We have implemented system using symmetric key IDEA algorithm.

In future better power consumption algorithm like blowfish can be tried out. Steganography can also be applied for secure Internet banking and mobile banking transactions. We can use concept of STK, SIM application toolkit where bank can stored the application and encryption keys on SIM.

REFERENCES:

- [1] Sandeep Singh Ghot ra, Baldev Kumar Mandhan, Sam Shang Chun Wei, Yi Song, Chris St etket ee, Secure Display and Secure Transactions Using a Handsetl, Sixth International Conference on the Management of Mobile Business.



- [2] Dilla Salama Abdul Minaam. Hatem M. Abdul Kadir, Mohily Mohamed Hadhoud," Evaluating the effects of Symmetric Cryptographic algorithms on Power Consumption for different data types, International Journal of Network Security, Volume 11, September 2010.
- [3] Managing the Risk of Mobile Banking Technologies, Bankable Frontier Associates.
- [4] Richard E. Smith. Authentication: From Passwords to Public Keys. Addison Wesley, 2001.
- [5] Encryption Issues. <http://www.muc.edu:80/cwis/person/student/lockett/encryption.html>
- [6] Internet Security. <http://cfn.cs.dal.ca/Education/CGA/netsec.html>
- [7] MICROSOFT, An in-depth perspective on software vulnerabilities and exploits, malicious code threats, and potentially unwanted software, focusing on the first half of 2008 [Report]. Security Intelligence Report, January through June 2008.
- [8] M. JOHNSON, A new approach to Internet banking. University Cambridge. (PhD) 2008, p. 113.
- [9] Carneiro, B. and Sousa, R. T., Identifying Bank Frauds Using Crisp-DM and Decision Trees, International Journal of Computer Science & Information Technology. October, vol. 2, 2010, pp. 162 - 169.
- [10] Development, Why is J2ME MIDP superior to WAP, <http://www.developnet.co.uk/wap.htm>.
- [11] Laitinen, H., 2001, Sun's 2001 Worldwide Java Developer Conference, Development Tools for the J2ME, http://www.forum.nokia.com/main/1,35452,1_0_75,00.html.
- [12] Java 2 Platform, Micro Edition – J2ME, Official Site, <http://java.sun.com/javame/index.jsp>.
- [13] CEM, — Common Criteria for Information Technology Security Evaluation, version 3.1, 2006. [Online]. Available: <http://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R2.pdf>
- [14] A. Hiltgen.; T. Kramp; T. Weigold; "Secure Internet -banking Authentication," IEEE Security and Privacy, vol. 4, no. 2, 2006, p.21-29.
- [15] F. Puente; J.D. Sandoval; P. Hernandez; C.J. Molina; — Improving online banking security with hardware devices, 39th Annual International Carnahan Conference on Security Technology (CCST'05), 2005. 11-14 Oct. 2005 pp.174 – 177.
- [16] Testing Verification and Validation Workshop, 2008. ICSTW'08. IEEE International Conference, 9-11 April 2008 pp. 294 – 302.
- [17] K.Chikomo, M. K. Chong, A. Arnab, A. Hutchison (2006), —Security of mobile banking, University of Cape Town, South Africa, Tech. Rep. [Online]. Available: <http://pubs.cs.uct.ac.za/archive/00000341/01/SecurityofMobileBankingpaper.pdf>.
- [18] A. Shamir, — Identity-based cryptosystems and signature schemes, in CRYPTO: Proceedings of Crypto, 1994.
- [19] N. Croft, M. Olivier, — Using an approximated One-Time Pad to Secure Short Messaging Service (SMS), in Proceedings of the Southern African Telecommunication Networks and Applications Conference (SATNAC), 2005, pp. 71–76.
- [20] Sun Microsystems Wireless Toolkit <http://java.sun.com/products/j2mewtoolkit>
- [21] Bouncy Castle <http://www.bouncycastle.org/>
- [22] ProGuard <http://proguard.sourceforge.net/>
- [23] Computer security <http://searchsecurity.techtarget.com>

AUTHOR



Syed Masaid Zaman is pursuing Ph.D programme in Information Technology at Shri Venkateshwar University Gajraula, U.P India. He received the B.Sc and M.Sc. degrees in Information Technology from SMU University in 2005 and 2008, respectively. His research interest includes E-Banking, E-banking securities, New technologies in Internet banking, cyber risks, cyber securities, implementation of Biometric technologies in E-banking etc. He published 5 research papers in international journals and also participated and published abstracts in International and National Conferences, seminars and Workshops in his research field.