2013

Security Perspectives for USSD versus SMS in conducting mobile transactions: A case study of Tanzania

Nyamtiga, Baraka

IJTEEE

ISSN 2347-4289

Security Perspectives For USSD Versus SMS In Conducting Mobile Transactions: A Case Study Of Tanzania

Baraka W. Nyamtiga, Anael Sam, Loserian S. Laizer

School of Computational and Communication Science and Engineering, The Nelson Mandela African Institution of Science and Technology (NM-AIST), Arusha, Tanzania.
Email: nyamtigab@nm-aist.ac.tz

ABSTRACT: Performing transactions using mobile devices is increasing rapidly in developing countries, Tanzania inclusive. USSD and SMS are among the technologies widely used in conducting mobile transactions. These two technologies have their strengths and weaknesses from perspectives of security of systems. They both utilize GSM Services and GSM Security is known to have inherent flaws in its encryption and authentication algorithms. A description for these platforms is given in this paper of what they are, their modes of operations, and an evaluation of their security as related to mobile banking systems. From the evaluations made; this paper suggests a method that is more secure for use in mobile banking systems. As a solution we propose some security features being added to the existing systems in order to improve data confidentiality, message integrity and user authenticity. The suggestions are based on the capabilities for the technology to accommodate these additional features to protect data that will supplement the protection offered by the GSM.

Keywords : Authentication ; Encryption ; GSM; Mobile Banking; Security; SMS; USSD

1 INTRODUCTION

According to GSMA industry group, the number of mobile subscribers in the world was estimated to reach 6 billion by the year 2013[1]. This increase in access to mobile services in the developing countries has resulted into a growing competition amongst telecom and banking industries. This in turn has led them to introduce a number of value added services (VAS) in order to acquire more of the market share and increase customer loyalties. A number of mobile transactions have been introduced in Tanzania that provide solutions for bill payments, mobile phone recharge, and money transfers. The schemes can be categorized into two main groups; *mobile money* systems that are offered by telecom companies and *mobile banking* systems that are offered by banking institutions. Example of mobile money systems in Tanzania include *M-Pesa* offered by Vodacom, *Tigo-Pesa* by Tigo, *Airtel Money* by Airtel, and *EzyPesa* of Zantel Tanzania. The mobile banking schemes include *SimBanking* offered by CRDB Bank, *NMB Mobile* of National Microfinance Bank, *ACB Mobile* of Akiba Commercial Bank, *TPB Popote* of Tanzania Postal Bank, and *B-Mobile* of BOA Bank among others. Mobile Banking describes a scheme that involves performing banking transactions using mobile devices. This scheme allows a customer to request information regarding the status of a personal account, and perform other related transactions as described above. The overall structure of the scheme for successfully performing a transaction begins with a consumer on one side and ends with a bank on the other. The other stakeholders involved include the Mobile Network Operator (MNO) and the Technology Vendor. This is illustrated in Fig. 1 below. There is a number of technologies with which customers can access the services. This includes WAP which is best described as mobile internet, Short Messaging Service (SMS), Unstructured Supplementary Services Data (USSD), and Interactive Voice Response (IVR). Two of these technologies are described in this paper; the SMS and the USSD technologies.

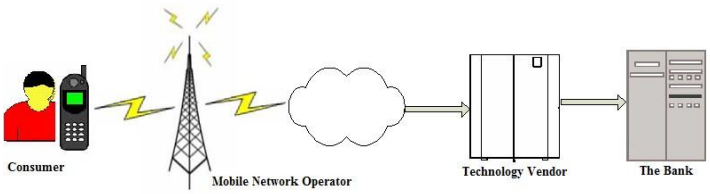

Fig. 1: Stakeholders in Mobile Banking System

GSM network is used widely in networking mobile connections. Its initial design was for use in voice communications but as the usage of mobile phone increases, additional means of data transmissions begin to be used; the most popular of which being SMS. SMS Services are highly utilized in delivering mobile banking services. The initial design of GSM was meant for subscribers to send non-sensitive messages. According to [2], Security considerations in terms of mutual authentication, data confidentiality, end-to-end security and non-repudiation were omitted with regard to the SMS service. Carrying sensitive customer financial details across GSM raises issues of security as personal details become vulnerable to security attacks. The security issues that exist in the GSM are mainly the cryptographic issues related to encryption and authentication algorithms. The A5 algorithm commonly used for encryption in GSM has been reverse engineered[3], [4], [5], [6] and the A3/A8 authentication algorithm have been spotted to contain several flaws that makes it possible to break it [2], [5]. These security vulnerabilities in the GSM make the technologies that utilize SMS services susceptible to attacks if they do not properly protect their data. Security issues in mobile transactions because of utilizing GSM services include SIM attacks and SMS attacks. Because USSD and SMS technologies both utilize SMS services; they are both susceptible to these attacks [7].

ISSN 2347-4289

2 SMS TECHNOLOGIES

2.1 SMS Overview

Short Messaging Service (SMS) refers to a wireless, radio-based service for transferring short alphanumeric messages among mobile phones on the GSM and UMTS cellular networks [8]. It was introduced in the wireless networks and was included in the GSM standards in 1991 [9]. It is a two way transmission service that makes use an SMS Center (SMSC) that acts as a store-and-forward unit for messages. The sender can receive a notification for a success or failure of the transmission thus providing a guaranteed delivery to the receiver. Moreover, a mobile handset is able to receive or send a message any time, even when an active call is in progress. If some failures occur, the message is kept in the network until the destination is available. It also has special features of out-of-band packet delivery and low-bandwidth transferring of message. An SMS is formatted as a byte array that contains a message header and body. The header section can be used to attach different details that need to be sent along with the message while the body contains the actual message. The Message length is up to 160 alphanumeric characters and can be converted to 70 ASCII characters using Base64 encoding. SMS service can be used to provide some additional services for mobile information services. This includes mobile electronic commerce, mobile transactions, news, sports, and entertainment services.

2.2 SMS Architecture and Operation

In its operation; the SMS architecture is as illustrated in Fig. 2 below. The necessary operations for supporting SMS are defined by the Mobile Application Part (MAP) layer using the services of the SS7.

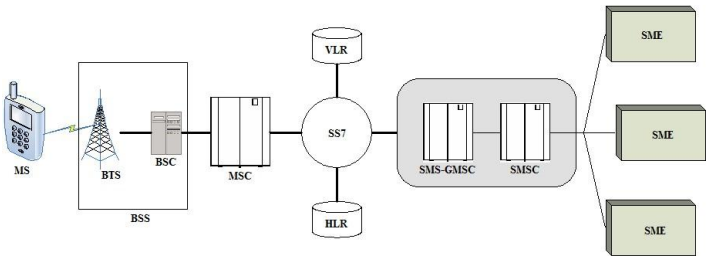

Fig. 2: SMS Architecture

A Short Message Entity (SME) is an element that can send or receive messages. Subscribers compose and send messages from a Mobile Station (MS) to the nearest Base Transceiver Station (BTS). The SMS is sent to the BTS using On-The-Air (OTA) interface; a standard used in wireless devices for transmission and reception of application-related data [10]. The BTS then forwards the SMS to the mobile's home SMSC through the Base Station Controller (BSC) and Mobile Switching Center (MSC) over Signaling System No.7 (SS7). SS7 is used by SMS service as a signaling channel to transmit data grouping [8].If the SMS is exchanged between subscribers in two different operators; the sender's SMSC repackages the message into a Short Message Peer to Peer (SMPP) Protocol format and forwards it using TCP/IP over private or public networks which are connected to the recipient's SMSC. After internal processing is completed, and interrogation for the destination location is done; the SMSC forwards the SMS over SS7 again to the nearest BTS around the identified destination. Again, using the OTA interface the BTS forwards the SMS to the destined Mobile Station (SME). The notification for delivery follows the same path in reverse order. SMPP is a standard telecom protocol for exchanging SMS messages between SMSCs. The SMS Gateway Mobile Switching Center (SMS-GSMC) receives an SMS from SMSC, interrogates a Home Location Register (HLR) for route information, and delivers the message to the visited MSC of the recipient's MS. Information regarding previously initiated delivery attempts to a specified destination that were unsuccessful is also kept in the HLR. The HLR informs the SMSC to retry delivering the undelivered SMSs when a mobile station that was previously unreachable is recognized by the network to be active [9].

2.3 SMS Banking Solution

In SMS banking, a customer sends an SMS to request for information that contains a service command to a pre-specified number. The bank will then respond with a reply containing the specific information as requested. An SMS service is hosted on an SMS gateway that connects to a service provider's SMS Centre. An overview of SMS being used to provide banking solution is illustrated in Fig. 3 below.

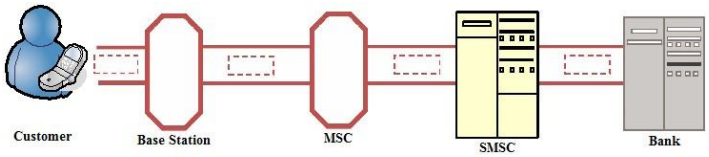

Fig. 3: SMS Banking

A registered customer initiates the transaction by sending a structured SMS (SSMS) message to the mobile banking service that instructs the SMS gateway to submit the message to the right SMS application [11]. The SSMS is sent to an SMS short code and passes from the client's phone through the GSM Network to the MNO SMSC. An SMSC stores this SSMS and forwards it to the SMS Gateway allocated to the address used by the Bank. The client's mobile number, forwarded by the SMSC with the SSMS will identify the customer and be used to return the response for the request accordingly.

2.4 Security of SMS

Despite being useful in conveying information to many recipients at minimal costs, the security afforded by SMS is not sufficient for financial transactions. This is because neither encryption nor integrity check mechanisms are enforced during its transmission across the GSM. Moreover, its nature of operation to store-and-forward makes things even worse because of the number of locations where the SMS data is available to others in clear format [12]. As a customer issues a request for transaction by sending an SMS, a copy of that SMS may be left on the handset and anyone with access to the customer's phone can see it. This creates a first point of vulnerability. When it reaches the SMSC, it is also stored in plain text making a second point of vulnerability. If a malicious attacker gets access to the SMSC he can misuse the messages by altering or adding some details for personal gain. The SMSC then forwards the message to the bank's mobile banking application (which can be administered by a technology vendor). At this point the message can be stored in encrypted or unencrypted forms adding a third possible point of vulnerability. The

ISSN 2347-4289

message is finally passed to the bank across a secured line, and assumed to be stored in a secured banking environment. Upon sending the transaction request to the bank, therefore, the SMS creates three susceptible points of vulnerability where SMS data is stored. This raises security concerns when this data is seen by some unauthorized individuals.

3 USSD TECHNOLOGIES

3.1 Overview of USSD

The Unstructured Supplementary Services Data (USSD) is a session-based, real-time communication technology for supplementary services. USSD is used in sending messages across a GSM network between a mobile client and an application server. It operates much like SMS but its session-based and interactive nature distinguishes the two. Unlike SMS, it does not operate by store-and-forward and its turnaround response time is much shorter for interactive applications than it is for SMS [12], [13], [14]. This makes USSD much faster and very cost effective as it involves simple operations that are also handset independent (old handsets to most recent smartphones can all access the service). USSD applications are characterized by menu-driven and interactive services and a request is invoked by dialing a number that is composed of asterisks (*) and hashes (#). Examples of these services include sports updates, movies, weather information, news, stock market, reservation applications (for planes/trains/ movies, etc.), voting/polling applications, mobile account balance checking and top up, and many others.

3.2 USSD Architecture and Operation

The USSD architecture is as illustrated in Fig. 4 below. When the service is invoked, a real-time, interactive session is established between a client and an application server on the network. This allows data to be exchanged between the customer and the service provider until the service is completed. A session needs to be allocated to every transaction request; the response for this request and the following series of requests and responses in that session all share the same session ID until the session is closed or times out [15]. The communication can be established even when a call is active because the two services use different communication channels [14]. USSD services use signaling channel while call services use traffic channels.

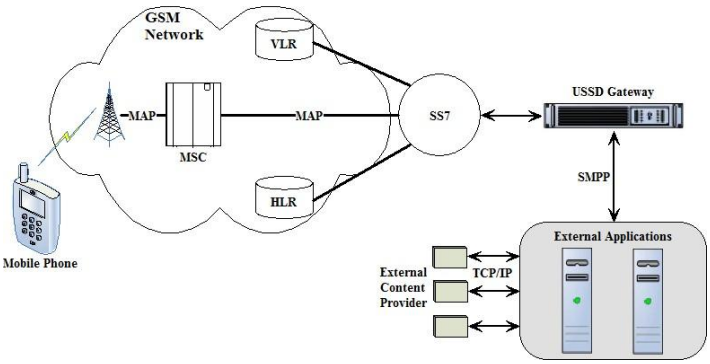

Fig. 4: USSD Architecture

The elements comprising the mobile network to carry data between the phone and the respective USSD application as well as the communication protocols they use are illustrated in Fig. 4 above. The MSC connects to the HLR via the SS7 in the home network. SS7 link also connects the GSM network with its components (VLR, HLR, and MSC) to the USSD Gateway. SMPP is used for communications between the external applications and the gateway. The USSD Gateway is open for integration with other telecom systems as well as the internet. USSD services are housed as applications in the network. They can reside in the MSC, VLR, HLR or an independent server that is connected using SMPP through a USSD Gateway [12]. Applications that are housed in the network are typically those which are under control of the mobile operator and the third-party applications are located in other telecom systems including the internet. When a message is not destined for an application in the VLR, MSC, or HLR; it is routed to the USSD Gateway by a USSD handler in these nodes using MAP protocol. The USSD code is interpreted by the gateway and routed to the corresponding USSD application server that contains the information requested by the customer. The relevant information is sent back by the application to the gateway which then formats the message into MAP and forwards it back to the user. USSD modes of operations can be categorized into two groups; the mobile-initiated operations and the network-initiated operations. A session is created between the mobile terminal and the network for all information transfers in a mobile-initiated operation. Also, an application in the network (as well as in the external application server) may at any time send a message to a mobile station in a network-initiated operation [14]. In both cases, the session must be released upon completion before another session starts.

3.3 Banking using USSD

The use of USSD in mobile banking is invoked by a registered customer and the request is received by the USSD Gateway through the MNO as shown in Fig. 5 below. The gateway forwards the request to the application server that communicates with the bank to service the requested transaction. The server response is returned through the MNO containing either the information requested or a text based MENU that requires a customer to choose the desired option by entering the corresponding number.

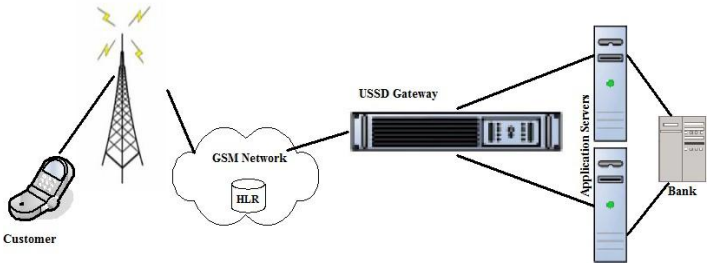

Fig. 5: USSD Banking

3.4 Security of USSD

Despite the convenience offered by USSD to customers in accessing banking services; the technology is not without its associated security risks. When compared to SMS, USSD is considered to be relatively more secure because no copy of the message is stored on customer's phone or at the SMSC. A single session is established between the mobile terminal and the application server, and at the USSD gateway the message is encrypted preventing data to be misused between the gateway and the server. The big risk lies on the fact that data car-

ISSN 2347-4289

ried within the communication channel is not itself encrypted [11]. If GSM encryption is broken, this data can be then be accessed [12]. As it has been mentioned earlier, the A5 encryption that is used in GSM has been reverse engineered and thus leaving USSD data vulnerable to attacks because messages are not encrypted on the GSM backbone [5]. Moreover, GSM encryption is only applied between the mobile terminal and the base station; across the rest of the operator's network, the message is in plaintext [16].

3.5 USSD versus SMS Technologies

As much as USSD resembles SMS in its operations; the two technologies have some unique distinctive features that differentiate them. Table 1 below summarizes the comparison between USSD and SMS technologies.

TABLE 1: Comparison between SMS and USSD

Features	***SMS***	***USSD***
Communication Protocol	SS7	SS7
Payload Length	160 alphanumeric characters	182 alphanumeric characters
Analogy	E-mail Application	Chat Application
Communicating Entities	From phone to SMSC then to recipient	Between phone and application server on the network directly
Communication Characteristics	Uses store-and-forward operations	Real-time, menu-based continuous sessions
Use of signaling channels	YES SMSC involved	YES No SMSC is involved
Involved Operating Costs	More costly because of SMS involvement	Less costly (direct from mobile to server)
Security	Less secure	Relatively more secure

4 SURVEY RESULTS AND DISCUSSIONS

4.1 Survey Analysis and System Modeling

A research survey that was done in telecom companies and banking institutions in Tanzania revealed that many banks adopt the USSD technology in their mobile banking services provision. Situation analysis revealed a number of areas that are most vulnerable for security attacks. These include at the *client end*, in the *communication channels*, and on the *server end*. These vulnerabilities are illustrated in Fig. 6 below and can be summarized as *lack of end-to-end security* for the data being transmitted, *vulnerabilities in the authentication mechanisms,* and *vulnerabilities in the application server security policies*.

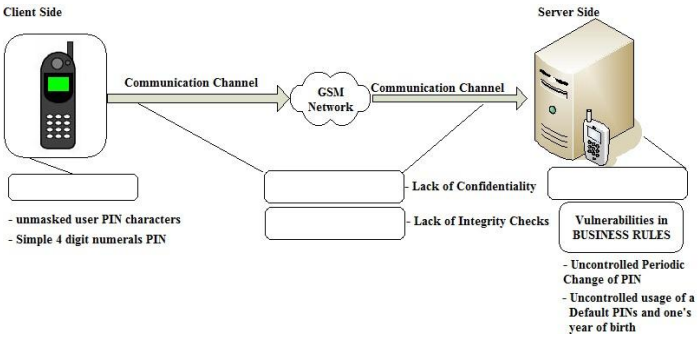

Fig. 6: Security Vulnerabilities in existing systems

The PIN characters entered by a customer on one's phone are not masked, thus being visible to someone who may be watching. Also, the PIN used is only 4 digit numerals which can be easy to guess. Moreover, there is a lack of data confidentiality as data is not encrypted between the customer and the server and there are no mechanisms for integrity checks. Additionally, the security policies in the application servers leave some vulnerabilities which can be exploited to perform attacks on the system. Periodic changes of PIN are not enforced, and the use of a system's default PIN is allowed in some systems. To address these vulnerabilities; a model was designed to cater for enhanced security controls. The features to be included in the model included *encrypting* data across the communication channel to ensure end-to-end security, calculating *message digests* for message integrity checks, increasing the domain of characters to be used in a PIN (mixture of *letters*, *symbols*, and *numbers*) and *masking* the PIN characters as they are being typed in. Along with these; the improvements to be made on server security policies include enforcing *periodic change* of PIN, prohibiting the usage of someone's year of birth as a PIN, and restricting the use of a system's default value as a PIN. These features along with other processing involved in sending a secure SMS are illustrated in Fig. 7 below.

ISSN 2347-4289

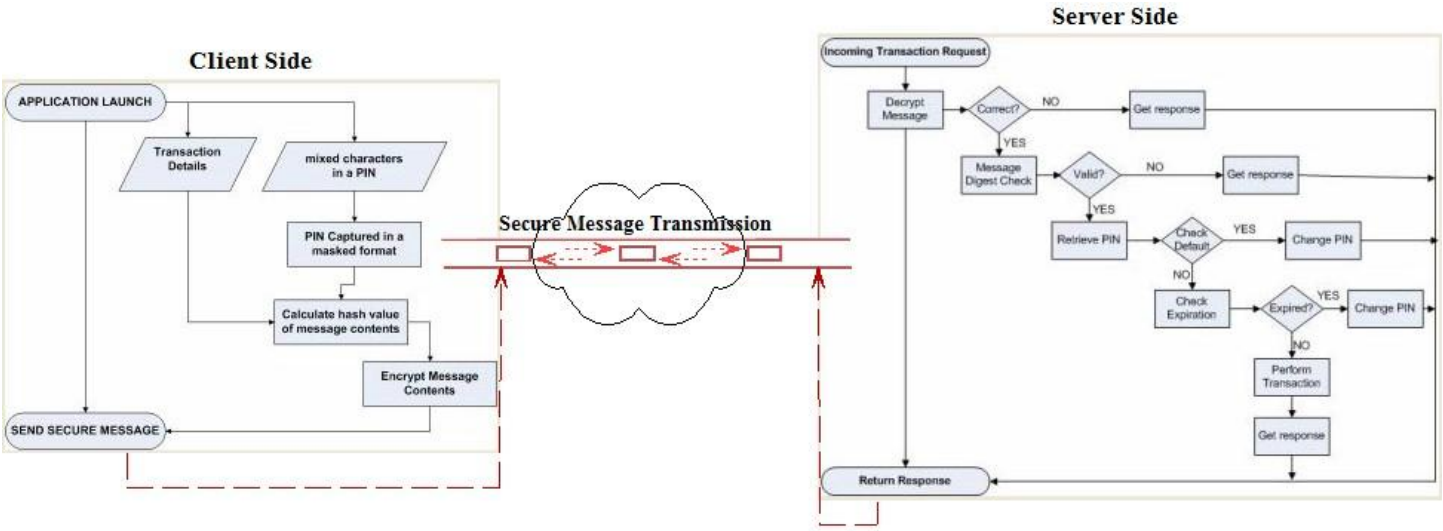

Fig. 7: Client and Server Side Security Processing Mechanisms

4.2 Discussions

In this section we discuss the capabilities for the SMS and USSD technologies to accommodate the proposed enhancements in the model. With USSD; the server application programmers are given flexibility to give the USSD gateway the contents to forward along with instructions whether the session still continues or it has ended. User inputs on the mobile phone largely depend on the USSD implementation for a particular phone as different phones have different USSD implementations. In order to incorporate these features in USSD it depends on the USSD gateways and mobile phones manufacturers. In order to mask PIN characters, it depends on the type of input field given to the phone by the gateway; whether a simple *text field* or a *password field*. This comes down to the manufacturer incorporating a feature in the USSD gateway to command for different input fields as it forwards the contents to the phone. Again, encryption and decryption on the phone is not supported with the current USSD implementations. The client is given a MENU of options from which one makes a choice; there is no room for cryptography application unless the USSD implementation on that particular phone requires encrypting the responses prior to sending them. Still, this relies on the phone manufacturer to be affected. We see therefore that; to incorporate the enhanced security features in the existing USSD technology, it would rely on the interventions of mobile phones and gateways manufacturers. This seems to be a long shot because different manufacturers have different standards in their products. The case is different for SMS because of its asynchronous nature. A java application installed in customer's phone can be used to provide the added features. The application will be used to capture the security details, generate a secure message and send the SMS via GSM. The client application will have a corresponding server application to receive and process the customer's requests. The minimum requirement for the customer to use the application is a mobile phone that supports JAVA. Many people in Tanzanian communities have access to these phones that are equipped with standard built-in *Java Virtual Machine* (JVM) to support java applications among other things. The java application shall handle the cryptographic operations (encrypt/decrypt and calculating message digests), and conceal user's inputs. With SMS, therefore, we need only a mobile application installed and no intervention from manufacturers is needed. Despite being relatively less capable to support these additional features, USSD however, remains to be a more convenient technology for applications in which quick responses are of essence. Also USSD provide handset independent solutions and it is highly cost effective. For those applications not involving very sensitive information (like financial and military information), USSD provides a best solution. Furthermore, the security flaws of the GSM have been addressed in higher generations above the 2G systems; i.e. UMTS, EDGE, 3G and above. 3GPP have replaced the weak crypto proprietary algorithms (COMP128, A5/1, A5/2) with a stronger encryption algorithm, KASUMI. This algorithm has been rigorously peer reviewed making it more agreeable, and encryption has been extended from the mobile to the base station controller instead of ending at the BTS. Service providers can therefore choose to utilize the higher GSM generations to handle the mobile transactions instead of 2G. This option will render them to incur more expenses and will reach a small number of customers, only those in townships where the coverage of these systems (3G, etc.) is prevalent. Those users in remote areas having access to 2G only will be denied of such services.

5 Conclusion And Future Work

A description for SMS and USSD technologies has been given along with their security strengths and weaknesses. USSD's security is relatively stronger when compared to that of SMS because of its session-based nature. However, the security flaws in GSM network that is utilized by both of these technologies call for additional security mechanisms being incorporated to supplement GSM security. This study has revealed that SMS is more capable to accommodate these additional security features than USSD. For USSD to accommodate them, intervention by mobile phones and gateways manufacturers is needed while SMS only needs a JAVA enabled mobile phone. Therefore, SMS is deemed to provide a better security solution for mobile transactions over GSM as compared to USSD. SMS can utilize a java mobile application to provide the required confidentiality and integrity of SMS messages while improving user authenticity as well. A detailed model and

ISSN 2347-4289

its implementation for enhanced security controls in mobile banking systems in Tanzania are yet to be done. The choice of appropriate cryptosystems, key management schemes, testing and validation of the model are the directions for our future works.

REFERENCES

[1] Marvels, M. Mobile Marvels: The Economist. 2009 [cited 2013 11 August]; Available from: http://www.economist.com/node/14483896.

[2] Emmanuel, A. and B. Jacobs, Mobile Banking in Developing Countries: Secure Framework for Delivery of SMS-banking Services. 2007, Citeseer.

[3] Biryukov, A. and A. Shamir, Real time cryptanalysis of the alleged A5/1 on a PC. 1999.

[4] Barkan, E., E. Biham, and N. Keller, Instant ciphertext-only cryptanalysis of GSM encrypted communication, in Advances in Cryptology-CRYPTO 2003. 2003, Springer. p. 600-616.

[5] Toorani, M. and A. Beheshti. Solutions to the GSM security weaknesses. in The Second International Conference on Next Generation Mobile Applications, Services and Technologies, 2008. NGMAST'08. 2008: IEEE.

[6] Kaur, G., P. Kaur, and K.K. Saluja, A Review of Security issues and mitigation Measures in GSM. International Journal of Research in Engineering & Applied Sciences, 2012. Volume 2(Issue 2 (February 2012)): p. 16.

[7] Brown, J. and E. Cecchetti, Attacking the Phone. 2012.

[8] Zhang, F., H.-W. Yang, and C. Song. A security scheme of SMS system. in Asia-Pacific Optical Communications. 2005: International Society for Optics and Photonics.

[9] Van der Merwe, P.B., Mobile Commerce over GSM: A Banking Perspective on Security. 2003, University of Pretoria.

[10] Medani, A., et al., Review of mobile short message service security issues and techniques towards the solution. Scientific Research and Essays, 2011. 6(6): p. 1147-1165.

[11] Krugel, G.T., Mobile Banking Technology Options. FinMark Trust, 2007.

[12] Sanganagouda, J., USSD: A communication Technology to Potentially ouster SMS Dependency. 2011, ARICENT.

[13] Desai, S., Mitigating Security Risks in USSD-Based Mobile Payment Applications. 2011, AUJAS: Bangalore.

[14] Taskin, E., GSM MSC/VLR Unstructured Supplementary Service Data (USSD) Service. 2012, Uppsala University.

[15] Gupta, P., End to End USSD System. 2010, Tata Teleservices Ltd: India.

[16] Chong, M.K., Security of mobile banking: Secure SMS banking. Data Network Architectures Group. University of Cape Town, South Africa, 2006.