Securing Mobile Money Services in Tanzania: A Case of Vodacom M-Pesa

A. Basigie . Mtaho, L. Mselle

Department of Computer Engineering and Applications, The University of Dodoma
abasigie@yahoo.com

Department of Computer Science, The University of Dodoma
mselel@yahoo.com

Abstract

Recently Tanzania has experienced an increase in the use of mobile money (M-money) services. M-money services are currently used to facilitate a wide range of services such as electronic money transfer, financial transactions and utility bills payments. This paper examines security vulnerabilities in M-Pesa services in Tanzania. Security weaknesses in authentication, money transfer, withdrawal and deposit processes are identified and analyzed; and secure approaches for implementing these services are proposed.

Keywords: M-money, MNO, M-Pesa SMS, STK, USSD.

I. Introduction

The definition of “mobile money” varies across the industry as it covers a wide scope of overlapping applications. In general, mobile money is a term connoting the services that allow electronic money transactions over a mobile phone. It is also referred to as mobile financial services, mobile wallet and mobile payment (Ernst & Young, 2009). Mobile money includes three elements: an electronic stored value account linked to a user’s mobile phone, mobile phone software (application) that allows users to manage their accounts, and a network of agents through whom users can exchange between cash and electronic value (Heyer et al., 2010). M-money software provides a wide range of services such as money transfer, money deposit and withdrawal, access to banking services, bills payments and commodity purchases. Fig. 1 depicts an interaction between customer and agent via provider’s network in M-money system.

Figure 1. An interaction between customer and agent in M-money system
The use of M-money in Tanzania started in 2005 when Airtel introduced phone-to-phone airtime credit transfer. In 2008 Vodacom launched its M-money service called M-Pesa. Zantel Tanzania also introduced its M-money service in the same year, which was first called Z-Pesa (now called EasyPesa). In 2010, Tigo, the first mobile network operator (MNO) in the country launched its M-money service called Tigo Pesa. Currently there are four M-money services brands in Tanzania: M-Pesa, Tigo Pesa, Airtel Money and EasyPesa (Inter Media, 2013). Up to April 201, registered customer base of mobile payment services was 28.8 million in Tanzania, 8.5 million being active users (Bank of Tanzania, 2013).

When first introduced, M-money services were mainly used to provide services such as money transfer, money deposit and withdrawal and airtime purchase. Currently they are used to support a wide range of services such as banking services, utility bills payments, money payments, online purchases etc. Despite having a large number of customers M-money systems in Tanzania are faced with a number of challenges. M-money services in Tanzania are still at the infant stage. In the past MNOs were mainly dealing with voice and data services which are not as sensitive as financial transactions. M-money services were introduced by MNOs without having sufficient expertise and experience in providing banking services. M-money systems use Short Message Services (SMS) and Unstructured Supplementary Service Data (USSD) technologies to facilitate M-money services. However, these technologies are subject to numerous security threats (Mohsen et al.;2008).

The rest of this paper examines some security vulnerabilities existing in Tanzania M-money services, taking Vodacom M-Pesa as a case study. The paper is organized as follows:- part II gives an overview of Vodacom M-Pesa system, part III analyzes M-Pesa security problems in money withdrawal, deposit and authentication processes. Part IV proposes solutions for some of the security weaknesses existing in the current M-Pesa system.

II. Vodacom M-Pesa System

Vodacom M-Pesa is an M-money service introduced in 2008 by Vodacom, Tanzania Limited, the largest MNO in Tanzania. Currently M-Pesa is the leading M-money system in Tanzania. M-Pesa allows customers to carry out electronic transactions using mobile phones. The user interface technology of M-Pesa relies mostly on USSD to provide customer with menus, but also supports the use of STK interface for its agents. Since it was launched in 2008, M-Pesa has facilitated quick transfer of money among customers and quick access of banking services. As of May 2013, M-Pesa in Tanzania had five million subscribers (Telegeography, 2014).

A. M-Money Access Technologies

M-money systems use three access technologies: USSD, SMS and SIM Toolkit-STK (Inter Media, 2013). USSD technology is used to provide the mobile users with menu-driven, interactive services. Unlike SMS whose delivery is not guaranteed, the USSD enables a real-time “session” to be initiated between the mobile user and the USSD application platform. When the service is invoked, it permits data to be sent back and forth between the mobile user and the USSD application platform until the USSD service is completed (Janagoudar, 2013). Once the session terminates the USSD application platform may be configured to allow an SMS to be sent to the user via Short Message Service Center (SMSC) in GSM network.
B. **Customer Registration to M-Pesa Services**
A customer may register for M-Pesa services with any M-Pesa agent in Tanzania by filling a special registration form. During the registration a customer is required to provide the following information for inclusion in the registration form: the identification number, customer full name, physical address, date of birth, nationality and mobile phone number (Vodacom Tanzania, 2013). All information provided must be complete and accurate and signed by the customer. Upon registration with M-Pesa, a customer is provided with a secret word which must be kept secret at all times and which will be used to identify a customer. Upon activation of the account by the input of the start-key and choosing a secret PIN, a customer becomes entitled to access M-Pesa services (Vodacom Tanzania, 2013).

C. **The M-Pesa Agent**
To become an M-Pesa agent, one needs to be a registered company with at least 2-5 outlets to be ready to offer M-Pesa services. Agents are required to comply with Vodacom’s anti money laundering policy. An investment in cash float of about USD 1,480 is required for each active M-Pesa outlet. A company such as bank, hotel and major supermarkets can also become M-Pesa agent. These companies only need to operate one outlet to qualify for M-Pesa services. However, the agent must invest at least USD 3,700 as the cash float for each outlet applied for (Booz et al., 2010). The roles of agents include upgrading Subscriber Identity Module (SIM) card for customers who wish to register for M-Pesa, registering new M-Pesa customers, facilitating cash transactions; and educating customers. An agent is usually paid a commission by the MNO for each M-money transaction performed.

D. **Access to M-Pesa Services**
Any Vodacom user may access the M-Pesa services after fulfilling the following conditions:
1. Upon registering the SIM card (a chip that identifies subscriber’s phone numbers, and allows users to access various mobile network services).
2. Upon initial activation of the M-Pesa System by use of the start key (the one-time 4-digit PIN sent to the customer on registration for the purpose of activating M-Pesa account).
3. Upon having operational SIM “active” at all times. Upon the correct use of the PIN or password in accessing account information and doing services (Vodacom Tanzania, 2013).

To access M-Pesa service, the customer has to dial code *150*00#. Dialing this code provides a menu of M-Pesa with a wide range of services; which include mobile payments, mobile finance and mobile banking and general account management (Gencer, 2010). To select the service required, the customer has to follow a step-by-step procedure and provide the appropriate information depending on the service required. The agent usually accesses the M-Pesa services by invoking M-Pesa menu available in his/her SIM card.

E. **Security in M-Pesa System**
Customer Identification Document (ID) and PIN are two major security authentication mechanisms used in M-Pesa services. A single PIN number is linked to customer account at any time and only the account owner may use his/her mobile phone and PIN number. The customer must securely use his/her mobile phone and PIN for all transactions that take place on his/her
account. The customer should not disclose the PIN to any person including the staff at the customer care centre.

To enhance security, M-Pesa system confirms every transaction made by SMS and provides an updated balance of the M-Pesa account. Vodacom relies on the use of the PIN as conclusive evidence that a debit transaction was authorized by the customer, even if it were made without customer authority. Each transaction is issued with a unique receipt number that is included in the confirmation SMS. The receipt number is used for tracking and identifying all transactions carried out on customer’s account (Vodacom Tanzania, 2013).

Before a customer deposits or withdraws money, a proof of ID is required. Types of identification that are allowed in M-Pesa include a voter’s card, driver’s license, valid passport and an introduction letter from the village or ward executive officer (which must bear a full name and photograph of the applicant). Other accepted customer IDs are employment ID, college or student ID, pension fund ID, tax ID and national ID (Inter Media, 2013).

F. Money Deposit Process

Fig. 2 illustrates the general model of M-Money deposit process. The process for the customer to deposit money in his/her M-Pesa account involves several stages. The agent first verifies the customer ID. After verifying the customer ID, the customer provides cash to the agent and the agent initiates the transaction (the agent accesses M-Pesa menu, selects money deposit option, enters the amount to be deposited, enters PIN and confirms the transaction). The process is achieved when the system sends a confirming credit and debit SMS to both customer and the agent respectively (Booz et al., 2010). Each SMS consists of a unique receipt number and an updated account balance and the agent’s name. Once the transaction is completed, it is recorded in M-Pesa agent log book by writing the amount deposited, account number and signature of the customer.

![Figure 2. M-money Deposit Process Model (Modified from Booz et al.; 2010)]
### G. Money Withdrawal Process

Before withdrawing money from the customer account the agent must verify the customer ID. Once verified, the customer initiates money withdrawal process (Accessing M-Pesa menu, selecting money withdrawal option, specifying the amount to be withdrawn, entering PIN and confirming the transaction). If the customer enters the correct PIN and specifies the correct amount, M-Pesa system will credit the agent’s account and debits the customer’s account. Successful completion of transaction together with the new balance in customer’s account is notified by SMS. Once the customer and the agent receive confirmation SMS from the M-Pesa system, the agent issues cash to the customer and the transaction is completed. In this model, the customer is paid money once the agent receives confirmation SMS from the M-Pesa system; otherwise the transaction is not affected. Fig. 3 illustrates the general model for M-money withdrawal process.

![M-money Withdrawal Process Model](modified_from_Booz_et_al._2010)

### III. Security Weaknesses in M-Pesa

The following are some of the security weaknesses inherent by the present M-Pesa system:

**A.1 The Use of More than one Type of Customer IDs**

One security weakness of M-Pesa is to allow the use of more than one type of customer ID. For example, a customer who used employer ID to register for M-Pesa account can later withdraw money by using another ID such as driving license, voter’s ID or any other ID. This situation makes it possible for a wrong or forged ID to be used.

**A.2 Weak Pin**

M-pesa PIN is a four digit number. Moreover, the PIN never expires and is written in plain text during the transaction. Such PIN therefore does not follow effective password management policies. Due to these weaknesses customer PIN can easily be guessed, smudged or snooped by unauthorized users.
A.3 Poor Verification of Customer ID
Another security challenge that M-Pesa agents are facing is on how to authenticate M-pesa customers. The agent usually inspects customer ID physically without having any other mechanism for proving or referencing the validity of that ID from the authorities which issued those IDs. This creates a loophole for a person to register for M-Pesa account with a forged ID.

A.4 Poor Transaction Confirmation Procedure
Before a sender completes a transaction the M-Pesa system requires the sender to confirm each transaction before it is fully executed. For example, when a person withdraws money, the last stage is to confirm the amount of the money to be withdrawn and to whom that money is transferred. Generally, the name of the recipient, amount to be transferred and the account number is displayed for verification. The aim is to avoid wrong or unintended transfer of money. Despite this procedure, several cases of transferring money to unintended recipient have been reported. Inaccurate data entry is the main cause of transferring money to unintended recipient. Some of the reasons that contribute to this problem include poor sender concentration when carrying out the transaction, user illiteracy and unfamiliarity with mobile phone.

Insecure transaction confirmation can create a loophole for a dishonest agent to commit fraud. For example, in the present M-pesa system a dishonest agent may direct the customer to transfer money to another agent’s account and pretend that it is his/her own account. Once such transaction gets completed, the agent can deny that the transaction was successfully done because the confirmation SMS will be missing. This fraud can succeed for two main reasons: first, the recipient’s physical location is not provided to the sender during confirmation process. Including recipient location would enable the sender to be aware from the beginning at what location the transaction is directed. Secondly in the current M-pesa system, once the recipient receives money in his/her account, he/she can directly withdrawals it without even knowing the sender. This is possible because in M-pesa system once you receive the money no any security word is needed to authenticate you as the right recipient of that money. These weaknesses affect security of money transfer service in M-Pesa system.

Another weakness observed is that the confirmation process is done at the end and a customer is supposed to confirm that transaction in few seconds, otherwise the transaction automatically terminates. If the customer is not careful enough or familiar in using the service he/she can just confirm an erroneous transaction. The best approach would be to allow the confirmation of the recipient to start first so as to enable the sender to know exactly from the beginning to whom the money is transferred. Also apart from verifying recipient’s name, amount and account number the geographical location of the sender can also be added. Introducing recipient location in the list of attributes to be confirmed and allowing the confirmation of the recipient to be done prior to the execution of the entire transaction will facilitate avoidance of transferring the money to unintended accounts.

A.5 Lack of End-to-End Verification
Unlike in banking systems where the bank teller has to verify customer signature and photograph physically and then compare them with electronic copies stored in the system, the
agent relies on one side authentication by just examining customer ID. If the customer has forged the ID and places his photo, the agent will not detect it. This loophole allows for a fake customer to use a forged ID to access M-Pesa Services.

A.6 Lack of Printed Receipts
Another weakness in M-pesa services is that the agent does not issue a printed receipt to the customer once the money withdrawal or deposit transaction is completed. As already explained, each transaction is issued with a unique receipt number that is included in the confirmation SMS. However if the SMS is compromised, there will be no evidence to indicate that the transaction was carried out between an M-Pesa agent and a customer.

B. Common Examples of Security Problems in M-Pesa

a) The agent or customer may transfer money to unintended recipient. When such event is reported to M-Pesa customer care center, the first step is to examine if that transaction took place. If the M-Pesa system shows that the transaction took place, it rolls back the money to the sender. In case that money has been withdrawn, the loss is bone by the customer or the agent.

b) A dishonest agent can use his power to deposit money to the customer’s account. Immediately when the customer leaves the agent’s location, the agent reports to M-Pesa customer care center requesting for transaction to be reversed. The money is then returned to the agent by M-pesa system. The customer will have to bear the loss. This is example of a repudiation attack.

c) There is a case when the agent deposits money to the customer’s account. The money gets deducted from agent’s account. However, the customer does not receive the confirmation SMS and his account is not credited. In this situation the agent refuses to return the cash to the customer.

d) A customer withdraws money from his/her account via agent’s account, the money gets deducted from the customer’s account but the agent does not receive a confirmation SMS, nor his account is credited. The agent requests the customer to wait until she/he receives the confirmation SMS. If the SMS is not received by the agent, the agent may refuse to refund the customer.

e) After depositing the money to his account via M-Pesa agent, the customer receives the confirmation SMS from the M-Pesa system. In some cases such transaction does not change the customer’s original balance. When the customer contacts customer care, the M-Pesa system records show that transaction did not take place. Such a situation leaves success and failure of the transaction in the hands of M-Pesa system which is invisible.
III: Proposal for Improving Security in M-Pesa Transactions

A.1 Improving Authentication
To enhance security and minimize the use of forged IDs, M-Pesa system could limit each customer to use only one unique ID for money transactions. This will minimize the impersonation attacks.

A.2 The Use of Effective Pin
M-Pesa system can enforce the use of strong PIN among customers and agents. Such PIN must be renewable, and should not be restricted to 4 digit number. To enhance security, M-Pesa System can allow the use of PIN which combines alphanumeric letters and special symbols, and must be more than 4 characters in length.

A.3 Improving Agent and Customer Authentication
To enhance security during transaction, a new mode of authenticating the customer and agent is proposed. Both customer and agent must verify each other’s physically and online via the provider network before transaction. Fig. 4 illustrate the proposed M-Pesa money withdrawal model. As shown in Fig. 4, to verify agent authentication, the customer must inspect the legitimacy of the following particulars before he/she initiates the transaction: agent number, full name, ID, TIN, business license, location and agent transaction log book. In order to confirm the validity of these particulars, the customer must validate agent number via provider network. The provider network will return the agent name, tax identification number and agent location. The customer will then determine if information from the network matches with agent’s particulars. Only when there is one-to-one match, shall the customer trust the agent.

To verify customer authentication, the agent must first inspect the customer credentials and

![Figure 4. Proposed M-Pesa withdraw model](image-url)

examine whether the photo in the ID is that of the customer. The customer ID must have the following particulars: customer’s full name, ID number and date of issue, photograph, phone
number, occupation, sex and age. Then the agent will have to verify customer’s particulars online via the provider network. The agent will use the customer account number as an input to request other customer’s particulars from the network. The system must reveal the customer’s name, ID number, gender and location of the customer. The agent will compare these credentials with those supplied by the customer to determine the authentication. If there are credentials which do not match with those retrieved by the network, the customer authentication shall be deemed to have failed.

A.4. Modifications in Money Transfer and Receiving Processes

As shown in Fig. 4 and 5, in order to prevent unintended customer from accessing the money transferred to his/her account by another customer, a new model of accessing M- money credited in recipient account is proposed. A customer and agent must use a combination of PINs and a receiving key. A PIN will allow user to access money transfer service while a receiving key is five character user’s defined secret key that will enable a recipient to receive the money. After performing the transaction, the sender must inform the recipient the receiving key used. Once the confirming credit SMS is sent by M-Pesa system to the recipient, to access the money, the account holder must input the PIN together with a receiving key to enable the receiver account to be updated after receiving a credit SMS. Failure to input a correct receiving key will cancel the transaction and rolls back the money to the sender. A customer transferring money to another customer or agent transferring money to a customer must both use PIN and receiving key to eliminate the problems of sending money to unattended recipient account. The alerting SMS is the message sent to notify the recipient on a certain financial transaction affecting his/her account. This message must include information about the current amount to be received, sender’s name and location (agent or customer). It must also prompt the recipient to send the receiving key to the M-Pesa system. The recipient must get a chance to respond to this message by entering the correct receiving key. After inputting the correct receiving key, the recipient will get the confirming SMS together with the new updated balance. The recipient must then check the balance from the provider network to verify the confirmation SMS. Finally, at the end of the transaction the agent must also issue the printed receipt to the customer for further references. Fig. 5 illustrates the proposed M-Pesa deposit model.

This model works in similar way to the proposed M-Pesa withdrawal model except that in this model the agent is the one who initiates the transaction. Similar to M-Pesa money withdrawal, this model requires the customer to provide his/her ID whenever he/she wants to deposit money to his/her account via. In case the customer wants to send money to another customer via the agent account, the customer must supply at least full name of the customer, location and account number of the customer.
IV. **Conclusions**

M-money services are useful for facilitating quick financial transactions, electronic money transfer, online purchases and utility bills payments. There are some inherent security weaknesses in M-Pesa authentication procedures, password management and money transactions. The paper has proposed some security solutions to mitigate some of the problems in two main aspects: securing customer and agent authentication procedures and money transactions. MNO must ensure that they provide services which not only are simple to use but also sufficiently secure. Improvement in money deposit and withdraw processes and in the authentication mechanisms are urgently needed. Therefore the proposed models are recommended to be used by MNOs in order to improve security of M-money services in Tanzania.

**REFERENCES**


