An improved security model for identity authentication against cheque payment fraud in Tanzanian banks

Feno Heriniaina, R.[1] * Kitindi, Edvin[2]
1. College of Computer Science, Chongqing University, Chongqing- China 400044
2. Sokoine University of Agriculture, P.O. Box 3000 Chuo Kikuu, Morogoro, Tanzania.
* E-mail of the corresponding author: fenoheriniaina@cqu.edu.cn

Abstract
For most African countries including Tanzania, cheques are still the most commonly used method for non-cash payments. Financial institutions and businesses consider banks to be a safe place for their assets. During the last decade, Tanzania has noticed an increase of non-cash payment frauds that cause a huge economic loss, and decrease trust between clients and banks. In this paper, we propose an authentication mechanism to improve the banks` security model, and keep the clients` assets safe. The client will be fully in control of any withdrawal transactions that can affect his bank account. This proposed method is expected to reduce cheque frauds if adopted by Tanzanian Banks.
Keywords: Cheque fraud, Bank account, SMS authentication, One time pass generator, Authentication

1. Introduction

This work has been initiated based on the issues that banks are facing in developing countries. Much of the academic literature about banks in Tanzania focuses on two main topics; the use of information and communication technology, and the improvement of the banking system in terms of security. Banks in Tanzania offer different types of services that range from a savings account, corporate accounts, mobile money services (M-Money), and mobile banking (M-banking). Although all these available services are contributing a lot in the ease of payments and financial transactions, cash is still the most popular medium of exchange in Tanzania. Cheques remain the most frequently used non-cash payment instrument, especially when it comes to business payments. There are of two types, personal cheques and corporate cheques; and only the Central bank and some commercial banks are allowed to issue cheques in Tanzania. The major users of cheques are the government departments, corporate bodies, and individuals who deal with the government department and agencies [1-2]. Cheque use has been increasing significantly since the automation of the Dar es Salaam Electronic Clearing House in 2002[3].
In figure 1, we present the transaction flowchart for cash withdrawal using cheques, where a withdrawer in possession of a cheque would go to the bank and ask for the withdrawal of a given amount in exchange for the cheque note. Once at the bank, his credentials will be matched with the information provided in the cheque note and validated by the bank officer. Only if all the information matches, and the amount requested is available from the requested, account the cash value of the cheque note is provided to the withdrawer.

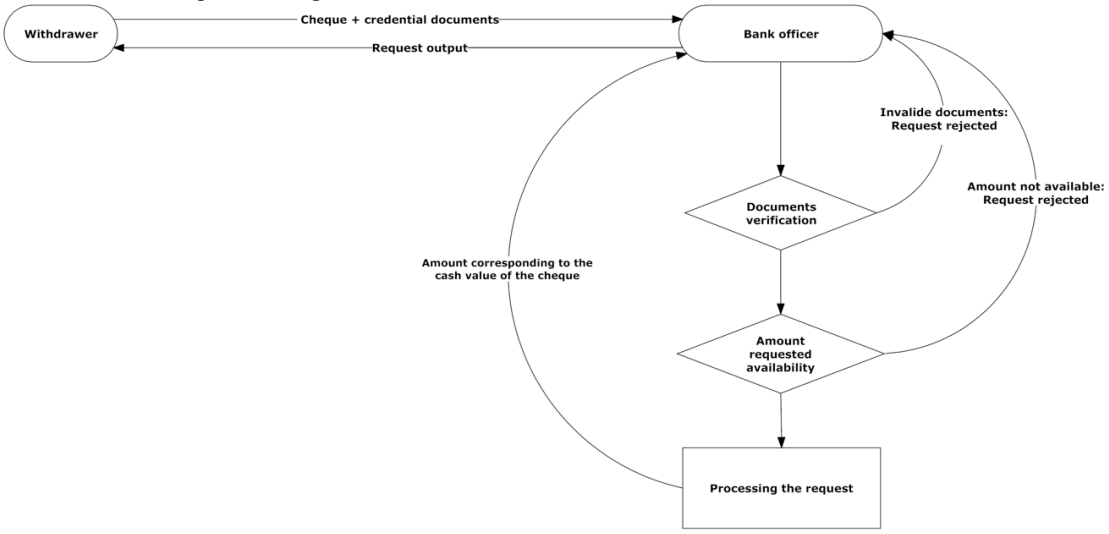

Figure 1: Transaction flowchart for cash withdrawal using a cheque

There are some cases, which we did not illustrate in the flowchart, when the processing of the transaction might also be rejected or interrupted; for example if the account has been frozen, the cheque has been reported as lost, etc.
Based on this empirical flow diagram for processing cash withdrawals using cheque notes at the bank, the account owner has less to no interaction in the process. In other words, if the person in possession of a presumably valid cheque note arrives at the bank, manages to perfectly fake all the requested documents (document forgery), and pass the verification phases at the bank; the account owner will be left with less assets at the bank, without even being made aware of the fact at the time. Many cases like this have happened in Tanzania as reported in [4].
In the following section, we introduce a model that will re-enforce the security of the customers' accounts in Tanzanian banks.

2. Improved security model for identity authentication against cheque fraud (IAACF):

The prevalence of the threats in cheque processing are based on the empirical flow chart discussed above; the customers' bank accounts need further protection of their assets. A safe cheque processing model should allow only the owner of the assets to control and utilize his funds that were placed at the bank. The bank should only process the payment of cheque notes that were genuinely from the account signatory and are endorsed with his consent. Yet, both the banks and the customer are responsible for safeguarding the assets, however, the bank has more responsibilities in ensuring that all the customers registered for its services have their assets safe and out of reach from an unsolicited third-party. To address and ensure that both the bank and the customer play their respective roles, toward this common goal of insuring the safety of the deposited assets at the bank, we propose a model for identity authentication against cheque fraud. Before we get into the details of the systems model, we need to introduce the following terminology, which is used throughout our discussion in this paper. These include SMS-info, Threshold, One time pass generator, SMS-request, registered mobile phone, and static personal password as being defined hereunder.

2.1 Terminology

SMS-info: it is a short text message that is designed to inform the user about the completion of a given transaction. It includes the following information; Transaction ID, Amount withdrawn, Time, and date of the transaction.
Threshold: it is a user-defined amount, with a minimum set by the bank, which defines the point at which a confirmation for a given transaction is needed. Below this threshold, withdrawal and transfer will not require any further action from the account owner (signatory), however, the SMS information will be sent as acknowledgement of the transaction that affected the account.
One time pass generator: it is a hardware device that the bank will provide to the account holder (signatory) when opening an account or later when he requests one. The device will be used to generate a random number, referred as a "one time pass" to be used each time when an SMS-request for transaction confirmation is received. Having the one time pass, a dynamic password will require the customer's confirmation for the authentication processes.
SMS-request: when a given transaction (request for withdrawal) has an amount higher than the user-defined threshold, the bank will send a short text message that informs its client about the specific transaction request, and prompts the client to grant the bank the approval for processing the request. The client (signatory) should then call the bank`s toll-free telephone number, using his registered mobile phone, and he should confirm account ownership and allow the transaction by providing: his personal password and the one time password just generated by the device.
Registered mobile phone: it is the signatory`s personal mobile phone number registered during the opening of the bank account, or when requesting for the service at his Bank. This can be changed if necessary.
Static personal password: it is a user-defined password composed of 6 digits. It is a password that will provide read only access to the user`s data for account ownership verification.
As most banks in Tanzania already have a web system that allows their customers to check their balance online (a read only access query to the bank`s database), the same password that grants access to such information could be used for the implementation of this proposed model. Doing so reduces the number of passwords that the costumer will have to remember.

2.2 Identity authentication against cheque frauds (IAACF)

In a normal transaction, a cheque note is provided to an individual (or an organization) in exchange for goods or a service. Later, this cheque note has to be exchanged for money in cash at the bank. We will use the term "withdrawer" to be the person in possession of the cheque, who requests its cash value in exchange at the bank. The bank officer will start processing a request by receiving the withdrawer`s documents, credentials, and cheque note. Once past this verification phase, the bank officer will initiate the submission of the SMS-request asking the account signatory whether the given transaction should be processed. If the account owner chooses to grant permission to the bank

officer to process the withdraw request, he has to call the toll free dedicated number of the bank using his registered mobile phone number, and go through the automated verification system starting as presented in figure 2.

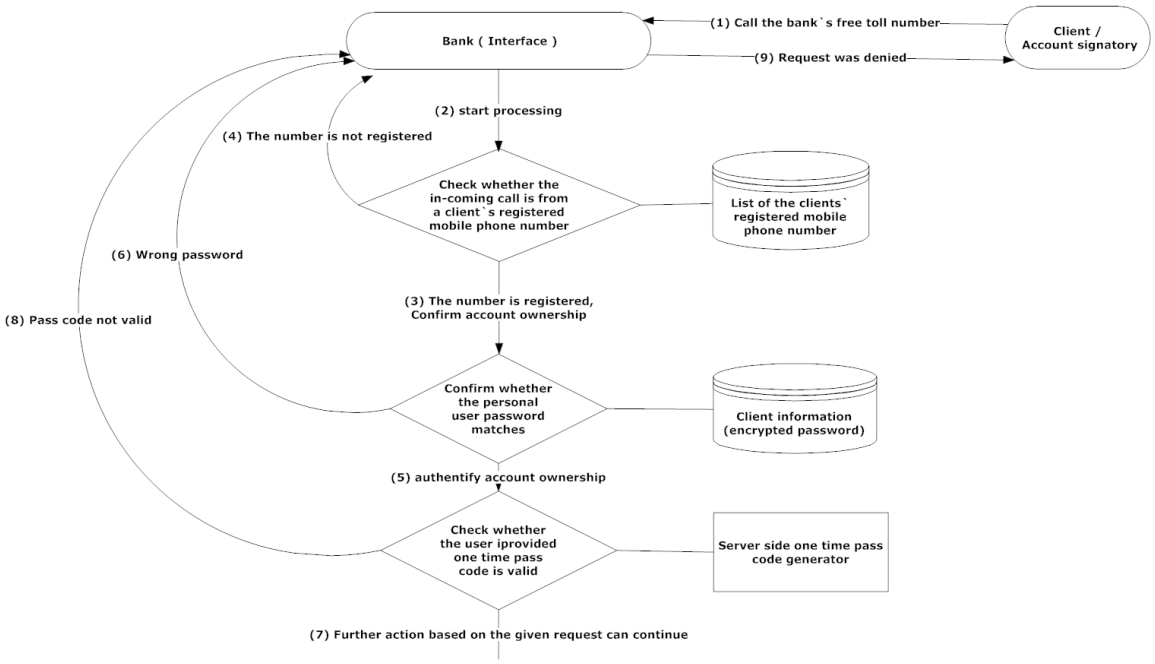

Figure 2: Diagram of the verification system steps necessary to complete transaction processing.

From the time the customer (also referred to as client or signatory in the figure) calls the toll free dedicated number of the bank, and the system checks whether the calling number belongs to registered customer. Only a call originating from a registered mobile phone number can be used to grant a transaction for withdrawal request. When the incoming number is mapped within the bank`s database, the customer has to confirm account ownership by providing the correct password for the given account. Last, a second authentication has to be passed which is providing the one time pass by typing it on the phone`s keypad when prompted to do so.

Still referring to the diagram in figure 2, a successful withdraw request will start from 1 and go through 2, 3, 5, and 7 which is for the bank officer to provide the requested cash in exchange for the bank note. The complete flowchart for this improved security model for identity authentication against cheque fraud is presented in figure 3. A valid and permitted withdraw request will start from 1, go through the empirical system which consists of the verification of the withdrawer`s documents, and availability of the requested amount. Next the process continues through 2, checking whether a need for transaction approval is needed in order to complete the payment transaction. If the requested amount for withdrawal is below the account owner`s defined threshold, the bank officer will proceed to the payment in cash for the withdrawer in exchange for the provided cheque note (step 7), then an SMS-info will be sent to the account owner.

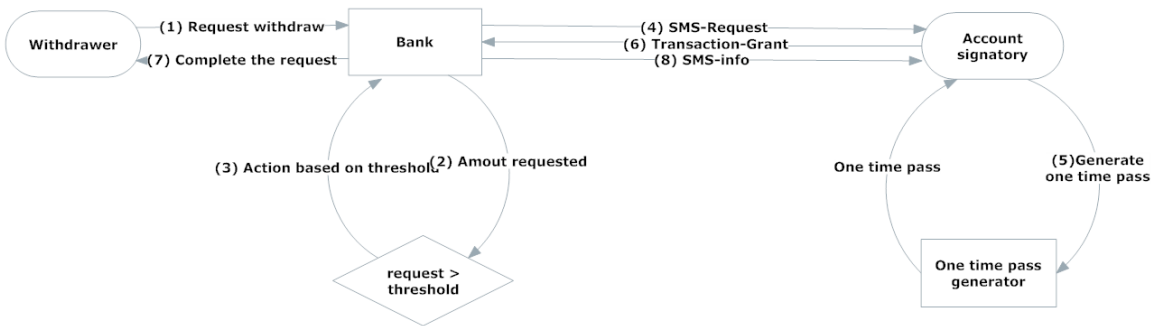

Figure 3: The proposed flowchart diagram for the improved security model

Otherwise, the bank officer will initiate the submission of an SMS-request, which is step 4. The account signatory will have to grant permission (step 5 and 6) for the bank officer to complete the transaction (step 7). Like the previous case, the complete process ends with an SMS-info being sent to the account owner.

To reduce the human intervention during the confirmation process, and to speed up time sensitive transactions, figure 4 below presents the option that allows the account signatory to give a green light to the bank to directly proceed with any withdrawal requested by a list of white listed entities up to a certain amount, without any need for further request for transaction authentication confirmation. White listed entities are the individuals or organizations trusted by the account holder, so that the payment made to them will only require the minimum verification steps to be processed.
To strengthen the user authentication system, especially for services provided on the Internet, a two-factor authentication technique, requiring something the user knows, has proven to be efficient for many services that need strong authentication.
Although in this paper, we are mainly focusing on how to reduce the financial loss due to cheque fraud, we borrow the well-established technique for authenticating users during online transactions in our proposed authentication model. When receiving the SMS-request, the account signatory will have to validate the transaction for the bank officer to further proceed with the transaction. He has to call the free toll number of the bank using his registered mobile number (something the user has), in order to start the authentication phase. If the used mobile phone number is registered to a given client account at the bank, the signatory will be required to input his personal password (something the user knows).

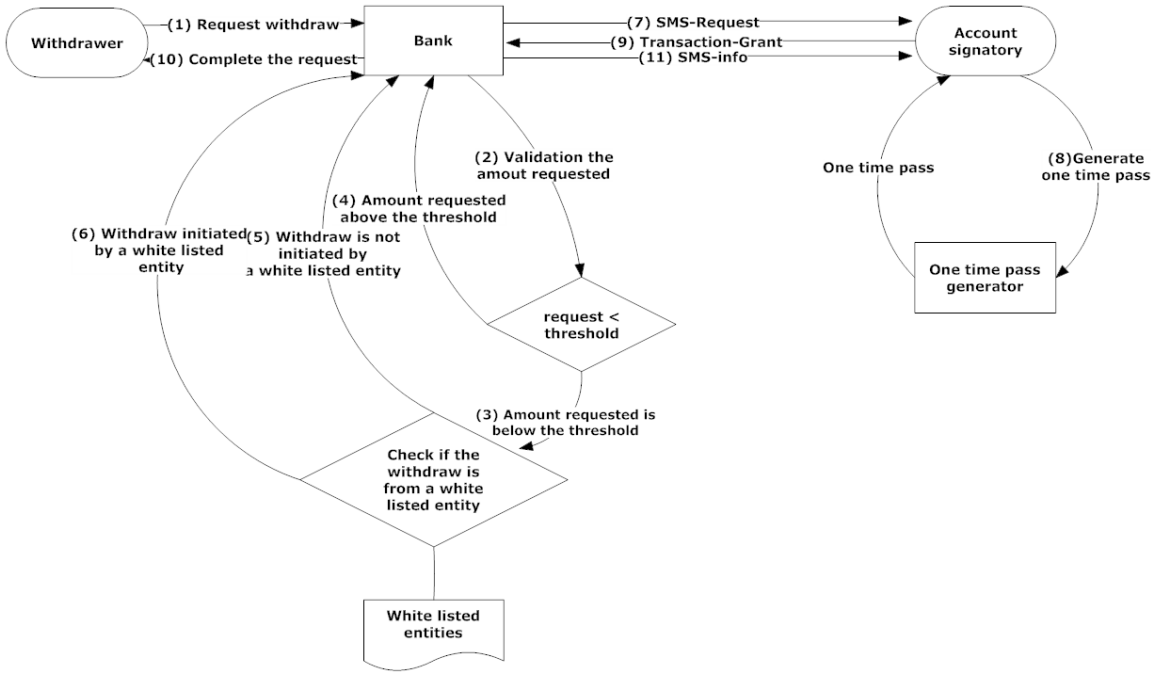

Figure 4: Transaction flowchart diagram for the white listed entities

Although requiring the user to call from a registered mobile number, and confirm account ownership by entering a private and personal password should be enough to validate the authentication, the risk is still high. Considering that the phone could be easily stolen, and that most of the time people use short or easy to remember passwords, this authentication method faces the same vulnerabilities as the common online authentication model that requires the user to enter a login and text-based password [5]. In this proposed authentication model against fraud towards bank in Tanzania, we add an extra layer of authentication that again requires something the user has: the one time password. This is a great solution for the fear of a password being stolen, since a new one-time password is required each time the user needs to validate a transaction.

2.3 The one time pass generator

Since the 1990's, a message authentication code (MAC) has been used to verify the integrity and the authenticity of information sent between two communication parties in computer systems and networks. Making use of cryptographic

hash functions, M. Bellare & al. [6] present a hashed message authentication code (HMAC) system. M'Raihi, et al. [7] describes an algorithm for generating a one-time password based on HMAC. A time based one-time password (TOTP) is presented, [8] and instead of operating with a counter like a HMAC-based one time password, it uses a time based moving factor.

The one time password generator and the validation server should have the same value of internal clock, so that the generated one time password within the same time-step will be the same during the validation phase. In our model, validation is performed after the phone number and static password has been confirmed, when the user is calling the free-toll number of the bank, and then enters the valid one time pass as shown in the one time pass generator.

Further details about the generation of the one time password, the recommended time-step, and resynchronization between the one time password generator and the validation server are available [8], but are out of scope of this paper.

3. Conclusion

In this paper we present a model that could be implemented by Tanzanian banks to strengthen the security of their clients` assets from fraudulent activities, by adding extra layers of verification systems in order to complete withdrawal transaction processing.

The SMS-info system used within the service offered by the banks in Tanzania will advise their clients promptly of any activities that affect their accounts.

The proposed system will require both the bank and the client to cooperate in efforts to protect the assets. Once the account owner writes a cheque, they will have to validate that withdraw if it exceed the threshold amount, or if the withdrawer is not white-listed. Setting up the proposed system that uses the SMS-request would highly reduce check fraud in the process of money withdrawal from banks.

We recognize that the implementation of the proposed security model comes with a cost, but we judge it to be worth the investment in order to safeguard the banks` reputation and clients` assets.

The presented model is not as perfect as one might think, as we did not consider the management of the existence of multiple account signatories that should be able to grant any legitimate transaction for withdrawal requests. This paper could stand as a backbone for any further works in regards to the issue.

If put into effect, this is a great improvement in terms of capital loss, as it will speed up any pursuits and complaints if the client notices suspect transactions on his account.

References

[1] Bank of Tanzania, Tanzania Automated Clearing House: Cheque Standards and Specifications (September 2013). Available at: http://bot.go.tz/PaymentSystem/Cheque%20Standards%20and%20Specifications%202013.pdf. Accessed on January 13, 2015.

[2] Bank of Tazania - Frequetly Asked Questions. Available at http://bot.go.tz/PaymentSystem/FAQ.asp. Accessed on January 13, 2015.

[3] Bank of Tanzania, Payment Systems in the Southern African Development Community - Tanzania chapter, available at: http://www.bot-tz.org/PaymentSystem/Tanzania_NPS_Greenbook.pdf, accessed on January 13, 2015

[4] Confirmation: A Key Control To Minimize Finacial Sector Fraud.
Available at http://iiatanzania.org/articles/confirmation-key-control-minimize-finacial-sector-fraud, accessed on January 13, 2015

[5] A. Adams and M. A. Sasse. Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures. Communications of the ACM, 42:41–46, 1999

[6] M. Bellare, R. Canetti and H. Krawczyk, "Keyed Hash Functions and Message Authentication", Proceedings of Crypto'96, LNCS Vol. 1109, pp. 1-15.

[7] M'Raihi, et al. HOTP: An HMAC-Based One-Time Password Algorithm (December 2005). Available at https://tools.ietf.org/html/rfc4226, accessed on January 13, 2015

[8] M'Raihi, et al. TOTP: Time-Based One-Time Password Algorithm (May 2011). Available at https://tools.ietf.org/html/rfc6238, accessed on January 13, 2015