Multi-channel, Multi-level Authentication for More Secure eBanking

Mohamed Al-Fairuz
Department of Computing Science
University of Glasgow
Glasgow, UK
alfairuz@squ.edu.om

Karen Renaud
Department of Computing Science
University of Glasgow
Glasgow, UK
karen@dcs.gla.ac.uk

***Abstract*—For decades, traditional authentication methods have proved weak in protecting users and organizations from various different online attacks. These include brute force password cracking, phishing, sniffing, active man-in-the-middle attacks, and session hijacking.**

The introduction of the one-time-password (OTP) and multi-channel authentication (MCA) has proven ability to protect users' online accounts from being compromised. However, without careful thought being given to implementation details, these authentication methods can still have weaknesses that could allow real-time attacks to succeed. This paper presents guidelines on how multi-channel authentication should be implemented so that it adequately protects users' online accounts. The proposed structure can be used in personal banking or corporate banking applications and has the potential to withstand the most commonly deployed attacks.

In order to evaluate the proposed MCA and test user acceptance, a prototype web-application was implemented. Our evaluation of the MCA concept using this prototype with Omani participants showed that 61% of total 42 participants who evaluated the application are satisfied with the level of security offered by multi-channel authentication. 66% of them believed that it was easy to perform transactions. We found that most participants were not familiar with the vouching code (the fourth authentication factor proposed by RSA) implemented as part of the study. However, 69% stated that they found this feature convenient when the primary channel was unavailable. Finally, 79% of respondents agreed to recommend the multi-channel authentication mechanisms to others if implemented by their bank.

Keywords; authentication; multi-channel; multilevel; multi-process

I. INTRODUCTION

The Internet has become the most convenient and cost-effective environment for businesses around the globe [1]. It is a place where people with different cultural backgrounds and from different geographical places connect as if they are in one physical place sharing and communicating with each other in different electronic forms. For organizations, the web offers an open market with equal opportunities to compete with large businesses. Consumers are offered an online market place with a variety and wide range of products available at varying prices by different suppliers [2]. However, between organizations and consumers, there is communication cloud full of threats and ambiguous users who are connected along the way with subversive goals in mind. Anyone can start a business online and compete with other business players. It is crucial to know how to do business effectively in the online market [3] and to know the key factors that will help to maintain business presence in such an open and competitive market [1].

In section II, we review the user identification and the different authentication classes found the literature. Multi-channel authentication mechanism and its advantages over other type of authentication mechanisms is covered in section III. After that, in section IV, a general multi-channel authentication infrastructure is presented as well as guidelines for best implementation in e-banking application is discussed. We conclude the paper by presenting an e-banking prototype application designed to test user-acceptance of the proposed structure.

II. USER IDENTIFICATION

With the rapid progress of technologies related to networking facilities, more and more computers are now connected with each other than ever before. Unlike local limited networks, most computers are now connected to a larger global network to communicate and exchange resources electronically [4]. With this networking progress, there was a need to offer a security that would help protect connected users' resources and services from other users. Yang and Shieh (1999) described network security in terms of two basic requirements: secrecy and authentication. The former protects sensitive data against eavesdropping and modification, that is, ensuring privacy and integrity of the electronic data available or exchanged within the network. The latter prevents forgery and unauthorized accesses to the network's resources (i.e., ensuring that authenticity is taken care of).

Authentication is the process of confirming someone's identity. Hastings and Dodson (2004) described this process in terms of claimants, relying parties, and verifiers [5]. A claimant is the individual claiming to be a legitimate user to receive services and resources. A relying party is the provider of the services and resources the user needs. A verifier is another individual or an automated system that verifies the

claimant legitimacy in order to authorize delivery of services and resources provided by the relying party. The verification process is usually based on authentication factors such as facts, characteristics, behaviors, or knowledge known to both the claimant and the verifier. Based on these authentication factors, the researchers have classified authentication in information technology into three classes: knowledge based (KBA), token based (TBA), and biometrics based (BBA).

KBA is also called "something the user knows" and refers to the method of verifying a user's identity by matching one or more pieces of "secret" information supplied by an individual (claimant) against information sources associated with the claimant [6]. KBA is the most common authentication approach used in distributed systems today [7]. This is due to many factors including simple implementation requirements, low cost to implement and administer [8], and a high level of user acceptance.

TBA is also referred to as "something you hold". This authentication class is based on tokens possessed by the user. The authentication principle does not rely on the user's memory but rather on the ability of the user to prove ownership of a token. In real life, these tokens are usually used to identify the user who carries them (e.g., ID card, hospital card, social security card) while in information technology these tokens are used and processed as part of the authentication protocol. Such tokens include an ATM card, smart card, and the one-time hash calculator.

Biometric authentication (BBA), in the other hand, refers to the use of physiological and behavioral biometrics to authenticate users [9]. No secrets are required to authenticate the user since authentication factors can be seen and captured by others. It relies on matching patterns of user characteristics or behaviors that are unique and distinguishable [10] and assumes that similarities of these characteristics or behaviors cannot be found in two or more users, beyond a reasonable threshold of doubt.

III. MULTI-CHANNEL AUTHENTICATION (MCA)

Most authentication studies carried out so far have proposed the use of single factor authentication such as passwords, passphrases, and PIN numbers to authenticate users. However, some businesses have extended the use of authentication process into *multilevel* authentication [11]. This was implemented by restricting some applications within the system by requiring an additional authentication step. For example, some banks allow users to login to their eBanking account using a single password. However, to pay utility bills, or transfer money, the user has to provide another password or passphrase to authorize the transaction.

These techniques have undoubtedly improved security but have not eliminated the possibility of some kinds of attacks (e.g., active man-in-the-middle/browser (MITM/B), real-time phishing/pharming (RTP/P), and malware [12]). Therefore, financial firms have come up with other schemes to overcome these drawbacks such as *multi-channel* authentication. This works just similarly to multilevel authentication but uses different and independent channels (i.e., web channel combined with mobile network channel). The channel, in this context, is the delivery medium that exchanges data between the end-user and the online service provider. Thus, for an attacker to gain full access to the user account, *all involved channels* must be compromised, clearly a far more challenging attack.

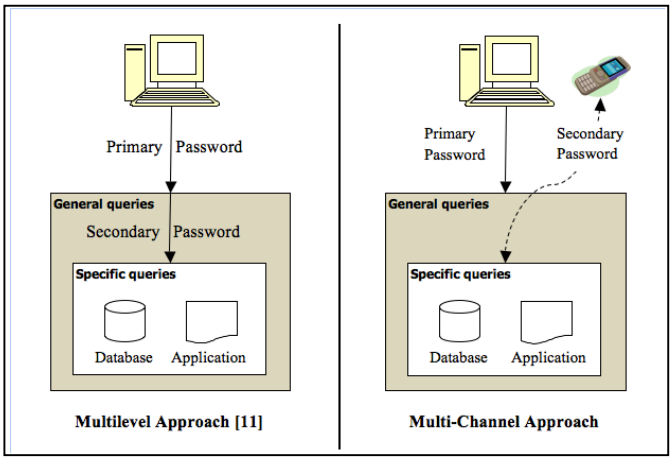

Figure 1. Multilevel vs. multi-channel authentication

Figure 1 demonstrates that in multilevel authentication, only one channel is used for different levels of authentication. This means that if the channel is compromised, all exchanged tokens can be compromised accordingly.

Unlike single channel authentication, MCA provides protection against most real-time attacks including MITM/B, RTP/P, and malware. Some of these mentioned attacks have the potential to capture and manipulate data exchanged between users (e.g., a bank customer) and the online service (e.g., eBanking web application) in real-time and are considered a global threat where attackers carry out attacks for financial gain [13]. Data integrity is not maintained and both sides (i.e., users and the online service providers) are often unaware of attacks at the time. This is the essence of the problem – the invisibility of the attack. The user will often only become aware of the illicit activity once he or she notices that the money is gone. With MCA, the attack is made visible especially if exchanged data has been altered by an attacker or malware. This is because the bank's system will not process transactions without user confirmation nor will the user verify transaction details he or she didn't request. The whole idea behind using two different independent channels is to ensure integrity and authenticity since the compromise of a single channel is insufficient to compromise the person's account.

Multi-channel authentication can meet different needs, depending on the business type and security levels required. Email applications, as an example, might require multi-channel authentication to be applied as the primary authentication level. Therefore, access to the user account can be denied until all authentication requirements have been met. However, the user is the one who should decide whether to enable these extra security measures or to disable them as the need for security varies from one user to another and even between different tasks by the same user.

Internet banking accounts might require a different setup. The most important tasks carried out are those which require modification of user's balance statement (transferring money or paying utility bills). Multi-channel authentication should be implemented only when there is a request issued by the user to commit such transactions. Otherwise, traditional authentication may be enough for read access to the user records (e.g., checking account statements and payments history). It is important that the applied security matches the risk levels. Excessive security is counter-productive.

Another example is in online community forums. Multi-channel authentication can be used only for moderators or site administrators as they have privileges to change the site's global settings and edit other users' posts and threads.

We can see that a multi-channel architecture can meet the needs of many applications on the Web. However, the implementation should focus on the security requirements of the target application (i.e., risk assessment), and, above all, should consider the cost and benefit of running such architecture from the user's perspective.

In theory, multi-channel authentication offers superior security over single channel authentication approaches. That is, for an attacker to compromise user account, different independent channels have to be compromised first before gaining full access to the user account. This makes it almost impossible for non-targeted attacks (i.e., attacks that are run randomly by scanning computers' IPs looking for possible open ports which could be targeted and attacked) to successfully compromise users' accounts. It also makes targeted attacks more difficult (i.e., attacks that are initiated with specific victim in mind, to successfully compromise the victim's online account) especially if the attacker is not geographically close enough to the user to gain access to designated devices used by some channels.

Nonetheless, improper implementation of multi-channel authentication could lead an attacker to manipulate details/factors exchanged by one channel to successfully take over the user's account or authorize transactions on behalf of the legitimate user.

In this paper, a general architecture of multi-channel authentication and implementation guidelines for eBanking applications are proposed. This proposal was tested by designing a web-application that simulates an eBanking application. The authentication mechanisms implemented by this application meets the guidelines presented by this paper. A discussion of the general architecture, the web-application designed, and best implementation practices & guidelines are presented in the following sections.

IV. EBANKING, MCA GENERAL ARCHITECTURE

Banking and telecommunication sectors are two major business players in today's market; their services have become necessities to many people all around the globe. The high level of user-acceptance of the Internet has led banking sector to introduce eBanking, or what is known as branchless or virtual bank. This refers to the use of the Internet as a remote delivery channel for banking services. Such services include traditional ones, such as opening a deposit account or transferring funds among different accounts, and new banking services, such as electronic bill presentment and payment (allowing customers to receive and pay bills on a bank's website).

Some banks, however, are still reluctant to move all these services online. The most obvious reasons are security and the unwillingness of these big financial firms to take the risk and connect their critical databases to an open world full of threats and ambiguous users. Although the advances of security solutions for such systems have shown very good progress in the past few years, there are still some security issues related to the customers themselves. Banks can protect their systems from external and internal attacks to some extent, but they have no control over their customers being deceived by attackers who can compromise their accounts once access tokens have been shared or stolen.

Figure 2 depicts a general view of how the proposed multi-channel authentication should be implemented (especially in eBanking). However, there will be some variations between one application and another, depending on the business needs and security level requirements as discussed in the previous section.

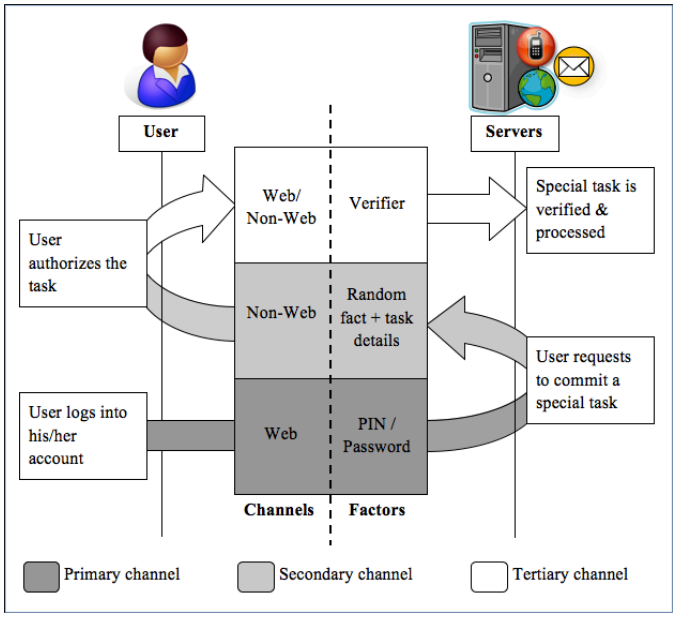

Figure 2. Multi-channel authentication archeticture (eBanking)

The structure above suggests that multi-channel authentication should be implemented on a multilevel structure. A user should be able to carry out basic functions throughout the web application by logging in using traditional authentication mechanism (e.g., knowledge-base authentication). At this stage, only read-access is granted. If the user would like write/modify access, then a one-time random "secret" with the task details should be trasmitted to him/her via a secondary channel (must be non-web). This is to ensure that the system delivers the secret factor through a channel other than the one used at time of user login. Task details are sent along with the secret factor to ensure that the user is aware of the transaction being verified. This is

important to avoid any possibility of MITM/B and RTP/P attacks.

Once the factor is received through the secondary channel, the user can verify the transaction using any available channel to submit the received secret. Only at this stage will the write/modify task be verified and authorised by the system.

It is important that we mention that the structure also suggests that the application should only allow a certain number of retries when verifying the one-time secret factors. This is important to avoid brute-force attacks which can succeed if no limitation rules are implemented by the system.

V. Web-application Prototype

In order to test the multi-channel authentication (MCA) mechanism proposed in this paper, a web-application that simulates an existing system has to be designed. This is important because people need to see MCA implemented into a system that they are familiar with.

A. Web-application Design

The application of MCA which best serves this purpose is the eBanking system. The application is widely used nowadays and authentication is a major factor that could affect the trust relationship between the bank online services and the bank clients.

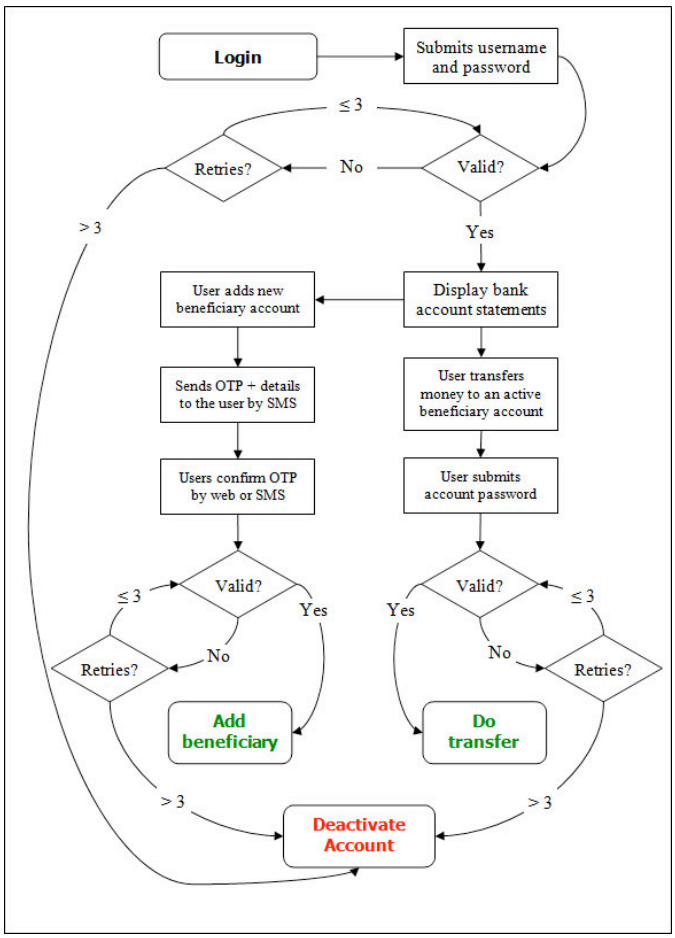

Figure 3. MCA in eBanking: prototype web-application flowchart

A fully-fledged eBanking web-application was designed that implements multi-channel authentication at transaction level. The web application requests users to authenticate themselves and their transactions several times along the way. This is done either traditionally (by memorized fixed passwords or pin numbers) or by MCA factors (variable one-time pin numbers or passwords). Figure 3 shows a flowchart of how the proposed multi-channel authentication was implemented in the eBanking web-application prototype.

The way the application works is similar to many existing online banking systems. The users need to create and authorize beneficiary accounts before they are able to transfer money to them. This way the users will only need to authenticate using the MCA approach when creating beneficiary accounts. Subsequently memorized passwords can be used to authorize payments to these accounts. Two main authentication mechanisms were implemented: the use of memorized passwords defined by users, and multi-channel authentication. They serve different purposes and authenticate different requests but overall they complement one another. The study suggests that these authentication mechanisms should be kept flexible in terms of how often each should be implemented and during which phase of eBanking (login and transaction, or transaction only). However, MCA must present at some point along the way that leads the user to commit a critical transaction (i.e., creating beneficiary account or transfer money). Furthermore, it is essential that the user registers his/her independent channels, and that these are verified, at enrolment.

B. Implementation

Oman, a developing country, is located in Middle East where eBanking is less widely adopted and used by bank customers than in developed countries. Until May 2009, only four out of a total of 7 local banks in Oman offered eBanking services to their customers [14, 15]. Some of the current existing eBanking systems implemented by banks, including the major leading bank [16], offer only limited functionality such as account statements and payments history with payment transfers between customer accounts and bill payments.

According to Al-Sabbagh (2004), lack of confidence is one of two main factors hindering Omani customers from using eBanking [17]. Therefore, we felt that testing the overall user-acceptance of MCA in Oman will benefit both banks and customers. The results will indicate whether or not the users are willing to adapt eBanking with the MCA mechanism to build trust. It will also help bank decision makers to reassess eBanking risks after the adoption of MCA, which could result in pushing more banking services for customers online.

Several requirements for users to test this application were set up. At time of testing, each user was given or was asked to download a task guide that had a list of tasks the user should follow in order to test all features of the eBanking application with MCA. There were 7 tasks starting with registration and ending with completion of the questionnaire. These tasks are described as follows.

1) Registration

The registration process is the first requirement the user should fulfill. This works as an alternative step of the enrollment process to the bank system. However, in a real eBanking system, this task or step should not exist electronically and the only way for the user to enroll into the system is to approach the bank in person and apply for an eBanking account. This is important because there must be a way to check that the person applying for this service is who they claim they are. Furthermore, the bank can take steps to verify the ownership of the device being used as the independent channel.

In the web application designed, the registration process is divided into two stages: first the user is asked to open an account by choosing a username, password, and e-mail address. The application will check if there is no username matches the registered username and confirm the new account registration after that.

In the second stage, the user is asked to enter name, mobile number, and an alternative mobile number. The user mobile number will be used to interact with the user directly (passing to the user the one-time pin number (OTP) and task details as well as collecting from him or her the confirmation in case the user selects to verify the OTP by mobile network) and the alternative mobile number will be used solely for the case when the primary mobile device is lost or unavailable, hence, the use of a 4th authentication factor [18].

2) Mobile Number Activation

Along with the OTP, the SMS message includes a request code which acts as a unique code to differentiate between different messages that the user will receive (see figure 4). For example, if there is network lag and the user waited more than 60 seconds without receiving the SMS, he or she can request the application to send another message (with new OTP and different request code). If the user receives both SMSs at the same time, only the SMS message with a request code that matches the one displayed in the screen should be used to validate the mobile number. The same goes for all other SMS correspondences between the application and the user.

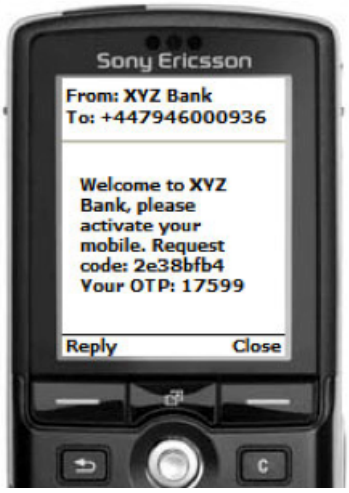

Figure 4: SMS message to authenticate users mobile

3) Select how to Verify the Onetime Pin (OTP) Number

After the user has successfully verified the registered mobile number, the application will ask the user to select how he or she would like to verify the OTP received from the application. There are two methods suggested:

a) Verifying OTP by web channel: this approach suggests that the user should receive the OTP by SMS, and then the user should input the OTP to the system by entering it in a text field displayed on the screen.

b) Verifying OTP by mobile network channel: the user will receive the OTP by SMS as suggested by the previous method, however, here the user should verify the OTP by sending it back to the system using mobile network (by SMS).

Once the user selects one of the available verification methods, the application will then creates a dummy bank account for the user and credits £10,000 to be used at later tasks.

4) Creation and Activation of a Beneficiary Account (Tasks 4 and 5)

The user in these tasks is required to create beneficiary accounts that can later be used to transfer money to them. There is no limit on the number of beneficiary accounts the user can create, however, the most important factor here is introducing the MCA mechanism for the user to test. For each beneficiary account the user creates, the application will send an OTP by SMS. The message contains the beneficiary account details as well as the OTP (see figure 5).

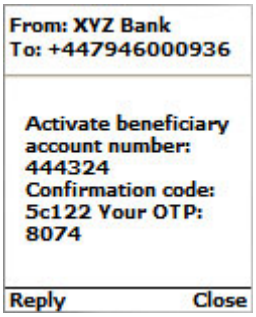

Figure 5: SMS message sample used to authorize a beneficiary account

Three important variables included in the SMS sent: *the beneficiary account number*, *the confirmation code*, and *the one-time pin number (OTP)*. The beneficiary account number helps the user to know if the beneficiary account created is the one the user is authenticating or another beneficiary account that has been created by an attacker. The confirmation code is an identification code for the message which the user should match with the confirmation code displayed on the screen; if matched, then the OTP sent in this message is the OTP to be entered on the screen (or to be replied back via SMS to the bank system if the user has selected to verify the OTP by SMS in task 3).

5) Transfer Money to a Beneficiary Account

After the user has successfully activated the new created beneficiary account, it is now time to transfer money to it. The user is instructed to choose the option "Transfer" opposite to the beneficiary account name and number by which another page will request the user to input the transaction details (i.e., transfer amount and description). Once submitted, another page will verify the transaction so the user can finally confirm it by submitting the registration password (the login password).

6) Activating the Alternative Channel Mode

In this task, the user is asked to test the 4th factor authentication approach introduced by RSA [18]. In real application, this should serve as an emergency authentication mechanism and only needed if the primary device (user mobile phone in this study) is not available. Therefore, an alternative medium can be used to process the user transactions until the primary device is available again. This can be done by creating a new beneficiary account just the way user did in task 4. However, this time the user should pretend that the mobile device is not available. The user will select the option "Switch to the Alternative Channel" from the activation window.

7) Questionnaire

After all tasks have been completed, the user is asked to fill a questionnaire concerning the usability and security of this study.

C. Questionnaire Results

1) Responses to Questionnaire

A total of 77 people have participated in the study. However, only 43 completed the questionnaire. Figure 6 shows major dropouts of participants in tasks 4 and 7. Task 4 is when users have completed mobile activation and have their bank account activated. After contacting some of these who dropped out at this point, they confirmed that they thought it is the end of the testing process and they didn't realize that they needed to complete further tasks which they didn't notice in the task guide.

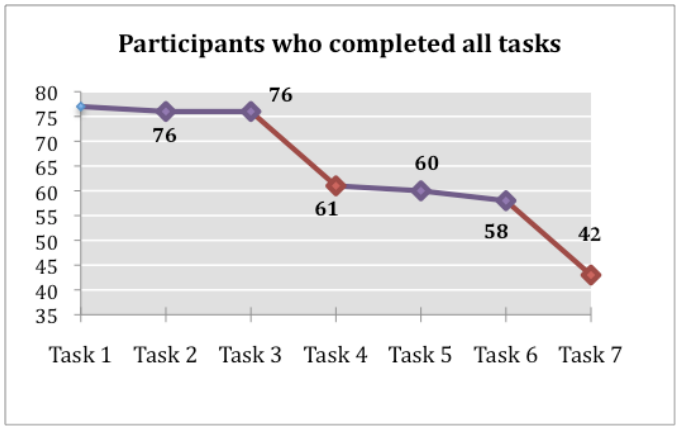

Figure 6: Participants who completed all tasks

Task 7, on the other hand, is where the users are asked to test the 4th authentication factor by pretending that their primary authentication device is not available. The fact that the users are testing this feature for the first time and that most of them have difficulties understanding the requirements (described in the comments bullet 4 of this section) could be the reason why there are so many dropouts at this stage.

2) Respondents

- Gender: The majority of responses (34 out of 43) were submitted by male respondents. The rest are from female respondents.
- Age: Most of the respondents (30) belong to the age group from 28 to 37 years. Only 9 respondents belong to the age group 18 to 27 years old and 3 respondents belong to the age group from 38 to 47.
- 69% of the respondents make use of Internet banking facility.

3) Important outcomes

Respondents were asked to rank how satisfied they were with quantity of communications, ease of use, and level of security.

- 57% of respondents are satisfied with the level of SMS communication between them and the application.
- 66% of them believed that it is easy to perform transactions, and
- 61% are satisfied with the level of security offered by multi-channel authentication.

4) Comments gathered from respondents have helped to explain the above figures.

- Most of the respondents found difficulties understanding task 7 which is asking them to utilize the forth authentication factor as an alternative channel if the primary channel is temporary unavailable. Nevertheless, 69% found that this mechanism convenient when primary channel is unavailable.
- Some respondents have suggested making the application user-friendlier.
- Most respondents agreed that authorizing transactions using multi-channel authentication mechanisms is better than traditional web authentication.
- 79% of respondents agreed to recommend the multi-channel authentication mechanisms to others if implemented by their banks.
- About 45% of respondents still worried of using public computers to carry out transactions whether multi-channel authentication mechanism is implemented or not.

VI. GUIDELINES FOR EFFECTIVE IMPLEMENTATION

For any online banking system to implement MCA, a "best implementation practice" set of guidelines have to be observed. These include:

- Users should not be allowed to enroll online. There must be a way to verify that the user registered to use the online services is legitimate and he or she is the real owner of the independent device being used to verify critical transactions.
- User correspondence details (e.g. mobile number, alternative mobile number) must not be displayed via the user online account and must be kept hidden from online access. The SMS protocol is not encrypted and the message headers can easily be altered by an attacker.
- Connection (web channel) between the user and the bank web-server must be encrypted and secured. This can be achieved by using the HTTPS protocol.
- Users should be allowed to choose whether to utilize MCA at beneficiary account creation level or at authorizing payment transactions level. Some users are more interested in authenticating each and every critical transaction while others prefer to minimize the number of times they use their mobiles to authenticate transactions. MCA also can be offered at login level if necessary but should never be eliminated from transaction level.
- Users should be allowed to request the bank server to resend the OTP by SMS in case of delays or mobile network lagging. However, each SMS message has to have a unique code that would differentiate it from other SMS messages. This is important to avoid confusion of which OTP to use if more than one message has arrived.
- Authentication of user and transactions must not share the same channel. If traditional authentication (e.g., password) is used to authenticate user at login page, then beneficiary accounts creation or payments must be authorized using a different secondary channel (e.g., mobile network).
- Users should be allowed limited retries to authorize critical transactions before the account gets deactivated.
- SMS notifications are vital when transactions are carried out. This should include transaction details as well as beneficiary account details. Also it is important to notify the account holder by SMS when the account has been deactivated for any reason.
- Users should be given the option to be able to lock their accounts at any time using the mobile network channel. If the user receives an SMS message, for example, requesting him/her to verify a given transaction without having initiated the request, alarm bells will ring. This request typically means that an attacker was able to compromise the primary authenticator and is trying to authorize a critical transaction. At this time, the user should be able to lock the account totally by sending an SMS command followed by the received OTP or by sending the OTP in reverse order to the bank server from the registered mobile device. This will deny the attacker any further actions in the account and will give the user time to report this incident to the bank. The SMS requesting locking of the account has to include the OTP sent to the user (whether in reverse order or following a command) to ensure that this message is being sent by the legitimate account holder and not some other person who is able to spoof an SMS to the bank server on the legitimate user's behalf.
- Users should only be allowed to unlock their accounts manually (by approaching the bank in person).
- The secondary channel (i.e. used for MCA mechanism) must be a two-way communication channel to allow different parties to agree to authorise one transaction. This is most suitable for corporate banking where a single transaction needs to be authorized by more than one person. For example, if there is an online transaction to be carried out by a corporate business, the employee will order the task online. The bank system will then send different OTPs to different people who are registered as people who should authorize such payments. Once all these OTPs are verified by these parties, only then the transaction will be fully authorized and carried out by the bank.

VII. CONCLUSION

Multi-channel authentication (MCA) is a relatively cost-effect way of protecting eBanking users from most known online attacks. If implemented correctly, no single attack could compromise user's account unless the attacker is able to take ownership of all the user's devices and their secrets. This will hardly happen without the user's knowledge and the user should have time to take action to prevent the attacker from defrauding him/her.

In this paper, we present a general structure and guidelines to implement MCA for eBanking. We also carried out an empirical study to test overall user satisfaction and acceptance of MCA in Oman. The designed prototype web application suffered from some usability issues which were identified by participants. These usability issues resulted in major dropouts at some points of the study where we ended up having feedback from only 42 participants out of total 77 people who participated in the study.

The web application has been modified and improved and all recorded usability issues have been corrected for an upcoming trail.

REFERENCES

[1] "The Impact of Strong Authentication on Usability," RSA Security Inc.2009 2009.

[2] D. Chaffey, *Internet marketing : strategy, implementation and practice*. London: Financial Times, Prentice Hall, 2000.

[3] M. E. Porter, "Strategy and the Internet," *Harv Bus Rev,* vol. 79, pp. 62-78, 164, Mar 2001.

[4] W.-H. Yang and S.-P. Shieh, "Password authentication schemes with smart cards," *Computers & Security,* vol. 18, pp. 727-733, 1999.

[5] N. E. Hastings and D. F. Dodson, "Quantifying assurance of knowledge based authentication," in *ECIW 2004: The 3rd European Conference on Information Warfare and Security*, 2004.

[6] Y. Chen and D. Liginlal, "A maximum entropy approach to feature selection in knowledge-based authentication," *Decis. Support Syst.,* vol. 46, pp. 388-398, 2008.

[7] I. Jørstad and D. V. Thanh, "The Mobile Phone as Authentication Token," *Telenor ASA,* 2007 2007.

[8] F. Piper*, et al.*, *Identities and authentication*. Cheltenham: Edward Elgar, 2005.

[9] K. Renaud, "Quantifying the quality of web authentication mechanisms: a usability perspective," *Journal of Web Engineering,* vol. 3, pp. 95-123, 2004.

[10] S. T. Kent and L. I. Millett, *Who Goes There?: Authentication Technologies Through the Lens of Privacy*: National Academies Press, 2003.

[11] "Password Managment," T. G. o. t. H. K. S. A. Region, Ed., ed, 2008.

[12] A. J. Menezes*, et al.*, *Handbook of Applied Cryptography*: CRC Press, Inc., 1996.

[13] "Making Sense Of Man-In-The-Browser," RSA, Whitepaper2009.

[14] (2009, 10 May). *Electronic banking in the Sultanate of Oman*. Available: http://ecommerce-journal.com/articles/15282_electronic_banking_in_the_sultanate_of_oman

[15] "Quarterly Statistical Bulletin December 2009," Dec 09 2009.

[16] (2010, 9 May). *Bank Muscat, About Us*. Available: http://www.bankmuscat.com/en-us/AboutUs/Pages/default.aspx

[17] I. Al-Sabbagh and A. Molla, "Adoption and Use of Internet Banking in the Sultanate of Oman: An Exloratory Study," *Journal of Internet Banking and Commerce,* vol. 9, 2004.

[18] J. Brainard*, et al.*, "Fourth-factor authentication: somebody you know," presented at the Proceedings of the 13th ACM conference on Computer and communications security, Alexandria, Virginia, USA, 2006.