Mobile User Authentication System for e-Commerce Applications

Rania. A. Molla
Department of Computer Science
Collage of Computing and Information Technology
King Abdulaziz University
Jeddah, Kingdom of Saudi Arabia
rmolla@kau.edu.sa

Imed Romdhani, Bill Buchanan
School of Computing
Edinburgh Napier University
Edinburgh, UK
I.Romdhani@napier.ac.uk

Etimad. Y. Fadel
Department of Computer Science
Collage of Computing and Information Technology
King Abdulaziz University
Jeddah, Kingdom of Saudi Arabia
eafadel@kau.edu.sa

Abstract— **E-commerce applications provide on-line clients and merchants with a quick and convenient way to exchange goods and services. However, the deployment of these applications is still facing many problems such as security threats; and on-line attacks. These often cause users to be concerned about their own privacy and encourage them to stop using on-line methods. Thus, a number of on-line authentication technologies and methods have been developed in order to authenticate users and merchants, verify their identities, and therefore overcome e-commerce security threats. Although stand-alone authentication solutions have been successful in authenticating legitimate clients and in defeating on-line attacks, they are often weak in overcoming the Man-In-The-Browser (MITB) attack, which is a type of Internet threat that infects a web-browser in a concealed fashion, and is invisible to both client and host applications. This paper presents a Mobile User Authentication System (MUAS) that uses QR code technology to authenticate on-line users, through a challenge/response protocol. Based on this mechanism, the system integrates different authentication technologies and methods to provide an improved and secure on-line user and merchant authentication system that overcomes MITB attack, without compromising usability and ubiquity.**

Keywords— Authentication; Man-In-The-Browser attack (MITB); QR code; Out-Of-Band communication channel (OOB).

I. INTRODUCTION

With the rapid development of the Internet, e-commerce systems have grown to become more popular for on-line transactions, and this has led to increasing on-line fraud and security issues, which cannot be solved by a single technology. Thus, many researchers have proposed different on-line authentication solutions, by combining various technologies and methods such as: multi-factor authentication[1-3], biometrics [4-6], and smart card technologies [7, 8]. However, these solutions still suffer from some limitations, such as: cost; hardware dependency; lack of mobility, scalability and interoperability [9]. To overcome these limitations, other researchers have taken advantage of mobile phone technology features as a means for: on-line identity authentication [10-15]; secure virtual private networks login [16-18]; and for on-line financial transactions [15, 19-23]. Nevertheless, on-line banking continues to present challenges to the user's financial security and personal privacy. On-line attackers and fraudsters are often using advanced methods to target on-line clients. One of the latest and most dangerous methods is the Trojan to launch a Man-In-The-Browser (MITB) attack [24]. MITB is a Trojan that embeds in a user's browser application and can be programmed to trigger when a user accesses specific on-line sites, such as an on-line banking site. Once activated, it can intercept and manipulate any information a user submits on-line in real-time [25]. MITB is hard to detect and, in many cases, it succeeds in causing complete, concealed damage, where neither the client nor the bank is aware of any irregularity [26]. This type of attack highlights the need for a solution that securely authenticates users, and ensures the integrity of transactions in the face of an evolving threat environment context.

This paper introduces a new technique called Mobile User Authentication System (MUAS) that employees the widespread QR code technology, through a convenient challenge/response protocol. The proposed system minimizes the risk of MITB attack by using mobile devices, along with its cellular network as an Out-Of-Band (OOB) communication channel. OOB works by using the web-based application screen as the primary channel, while the cellular network is a second channel used to pass confidential information.

This paper makes the following contributions:

1) *Client/Server Mutual Authentication*
   The technique's first step is to secure the one and only web-based communication channel, through TLS/SSL protocol. It authenticates the client and the server in order to ensure message integrity and confidentiality.
2) *Minimal User Input.*
   This technique is a user-friendly challenge response authentication system, requiring the client to only submit his mobile number, and to capture the QR code.
3) *Overcome the risk of Man-In-The-Browser (MITB) attack.* This technique is designed in a way to overcome the risk of MITB attack, by restricting the use of PC browsers to client's mobile number submission only. And using an OOB communication channel for passing

confidential information, required for user authentication. Even if MITB exists within the client's browser, the type of submitted information cannot be useful for the attacker.

4) *Prevent Replay Attack***.**
The technique generates two similar random numbers on the merchant-side and the mobile phone-side, which will be compared against each other to ensure client and mobile phone legitimacy.

5) *Protect client's confidentiality.*
This technique requires no website registration nor memorizing any passwords, due to its vulnerability to server attacks. Therefore, no personal information is required to be submitted by the client, except for his/her mobile number.

This paper is divided into seven sections. Section 2 presents the threat addressed by this paper. Section 3 describes the core algorithm of the MUAS, along with its components and architecture. Section 4 presents the related work. Next, section 5 that presents the evaluation criteria and design. Section 6 discusses the security analysis. Finally, section 7 presents conclusion and future work.

II. THE MAN-IN-THE-BROWSER ATTACK (MITB)

MUAS is an authentication system designed to provide a secure and easy-to-use system, while overcoming Man-In-The-Browser (MITB) attack. MITB has been defined by Almeida et al. [24] as "A Trojan that embeds in a user's browser application and can be programmed to trigger when a user access specific on-line sites, such as an on-line banking site".

MITB attack consists of two phases: The first phase is the infection of a target computer by means of phishing e-mails, requests to install updates, downloading interesting PDF documents, and so on, which causes malware-infected software to be downloaded into the user's browser. Whenever the user restarts the browser, the Trojan installs its extension into the browser's configuration, and start to load the extension. Finally, the extension registers a handler for every page load [24]. The second phase is the transaction takeover. Whenever a page is loaded, its URL is searched for by the extension. Next, all data submitted by the user is extracted from the browser and modified by the attacker, then the browser continues to submit the modified data to the server. The server performs the transaction on the modified data, generates a receipt, and send it back to the browser. Finally, the extension replaces the modified data in the receipt with the original data submitted by the user in the beginning. The browser displays the modified receipt with the original data, while the user thinks that the original transaction has been authorized correctly [24].

Numerous strong authentication techniques such as biometrics, grid card, OTP token, Out-of-Band OTP, EMV-CAP, smart cards and digital certificates are available, and effective against a wide range of threats [27]. However, most of these techniques require user interaction with the browser. Therefore, MITB can intercept them or wait until the user passes the challenge before taking over [24, 27]. Even Anti-Virus or Anti-Malware applications which are deployed to end-user computers in order to detect and disable malwares cannot be fully trusted. Malwares are rapidly changing and evolving making it difficult for client software to keep up [24, 27]. Therefore, a solution that uses an Out-of-Band (OOB) communication channel can be a powerful weapon against advanced threats, especially Man-In-the-Browser (MITB) attack, since it avoids using the communication channel often used by attackers. Moreover, this technique leverages devices such as mobile phones that are already in-use by most clients, and enables reviewing authentication details away from the influence of malware on the client's computer.

A. Problem Statement

In developing an e-commerce authentication system that overcomes Man-In-The-Browser (MITB) attack, the following questions arise:

- Who will conduct the authentication process?
- What kind of information must be provided by the client?
- How to verify the identity of the client and merchant through a QR code?
- What kind of technologies will be used to overcome the risks of Man-In-The-Browser (MITB) attack?
- Does the system satisfy the e-commerce security requirements?

III. MOBILE USER AUTHENTICATION SYSTEM (MUAS)

Our Mobile User Authentication System (MUAS) authenticates the user via a mobile phone. The system is based on a challenge/response protocol that generates and displays an encrypted QR code as a challenge, in which the client uses the mobile phone camera to capture, in order to generate a response that ensures user's authenticity.

In this section we present the core algorithm of the MUAS. We will explain the basic workflow, from Peuedo-Random Number Generation (PRNG), QR code cryptography, to user authentication process.

1) *Psuedo-Random Number Generation (PRNG)*
The system is based on generating two random-numbers. One on the merchant-side, and the other is on the mobile phone-side. Both numbers are generated using the same seed. The merchant generates its PRN (M-PRN) by using the mobile-number submitted by the client, while the mobile phone generates its PRN (MP-PRN) by using the mobile-number embedded in the International Mobile Subscriber Identity (IMSI), which is stored on the SIM card.

2) *QR code cryptography*
The MUAS QR code generation process is based on encoding the merchant's public-key, provider's name, merchant-generated PRN (M-PRN), and the response

end-point (URL) into a QR code, after encrypting it with the client's public key.

The reason behind including the provider's name and the response end-point into the QR code is to help the client ensures the QR code authenticity, and to specify where the mobile phone will respond to the challenge.

3) Authentication process

The authentication process is composed of two layers. The first layer is performed on behalf of the mobile phone-side, in which the client launches a PIN-protected application on the phone, called "DGCH". The second layer is performed on behalf of the merchant-side, in which verifies user's authenticity.

3.1) DGH application layer

Once the client launches the DGCH application (**D**ecrypt, **G**enerate, **C**ompare, and **H**ash) on the mobile phone, and selects the "start" button, the camera becomes activated to capture the QR code. The application extracts the encrypted contents by applying the client's private key to get the merchant's public-key, provider's name, merchant-generated PRN (M-PRN), and the response end-point.

Next, DGCH compares the recovered merchant-generated PRN (M-PRN) against the mobile phone-generated PRN (MP-PRN). If the comparison is a success, the application computes a response by comprising of the SHA256 hash of the mobile phone-generated PRN (MP-PRN), and sends the hashing result to the response end-point, along with the mobile phone-generated PRN (MP-PRN), after encrypting them with the merchant's public key. Otherwise, the DGCH gives an "Unsecure Transaction" message and exits the application.

3.1) Verification layer

The merchant decrypts the received hash and the mobile phone-generated PRN (MP-PRN) by applying its private key. The received hash is verified by applying SHA256 to the received mobile phone-generated PRN (MP-PRN). If both hashes are equal, the user is authenticated.

A. MUAS Assumptions

The MUAS assumes that TLS/SSL protocol is the standard communication channel in the proposed MUAS. The following table shows the notations used in the MUAS framework.

Notations	Meaning
MN	Mobile number
K_C	Client's public key
K^{-1}_C	Client's private key
K_M	Merchant's public key
K^{-1}_M	Merchant's private key
end-point	Merchant's URL address
PRN	Psuedo-Random Number
M-PRN	Merchant- Psuedo-Random Number
MP-PRN	Mobile Phone- Psuedo-Random Number

B. MUAS Architecture

The client in the MUAS initiates the process with the merchant through sending his mobile number. The authentication process performs a challenge/response protocol to authenticate the client. Figure 1 shows the proposed MUAS.

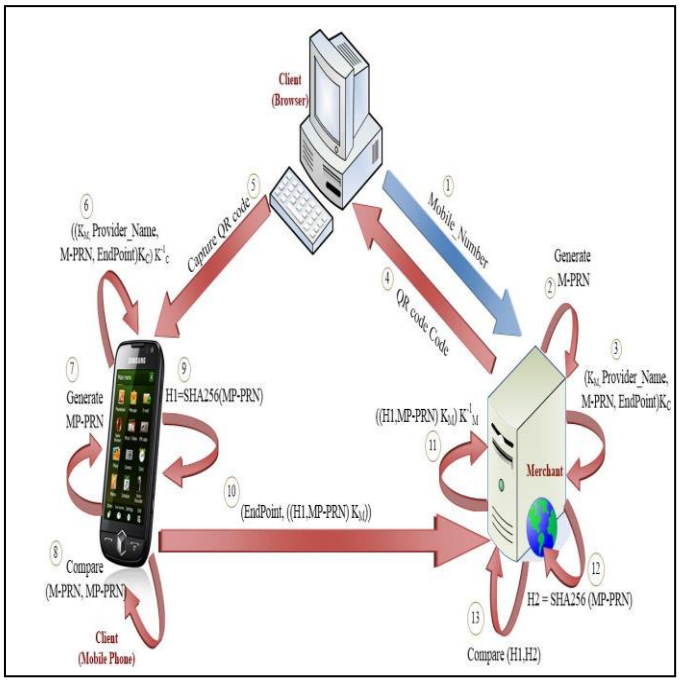

Fig 1. Mobile User Authentication System

The MUAS process works as follows (Figure 2):

1. The client initiates the process with the merchant, by sending his Mobile Number (MN).
2. The merchant generates a random number (M-PRN) from the original Mobile Number, provided by the user in the initialization process.
3. The merchant appends M-PRN with the merchant's public-key, Provider's Name (PN), and merchant's end-point (URL), in order to be encrypted with the client's public key (K_C) to represents the QR code contents.
4. The QR code is displayed on the client's PC.
5. The client captures the QR code with his mobile phone.
6. DGCH application decrypts the QR code contents by using the client's private key (K^{-1}_C) to get M-PRN.
7. A random number (MP-PRN) is generated from the mobile number embedded in the IMSI.
8. Next, DGCH compares the recovered M-PRN with MP-PRN. If the comparison is a success, then:

9. An SHA256 hashing algorithm will be performed on MP-PRN, and get Hash result (H1).
10. Hash result (H1) will be appended with the original MP-PRN, and encrypted with the merchant's public key (K_M) to be sent to the merchant.
11. The merchant decrypts the received Hash result (H1) and the original MP-PRN by using its private key (K^{-1}_M).
12. The merchant verifies the received H1 by applying the same hashing algorithm (as in step7) on the recovered MP-PRN, and gets a Hash result (H2).
13. The merchant compares H1 and H2. If both hashes are equal, then the merchant authenticates the user.

Otherwise, DGCH quits.

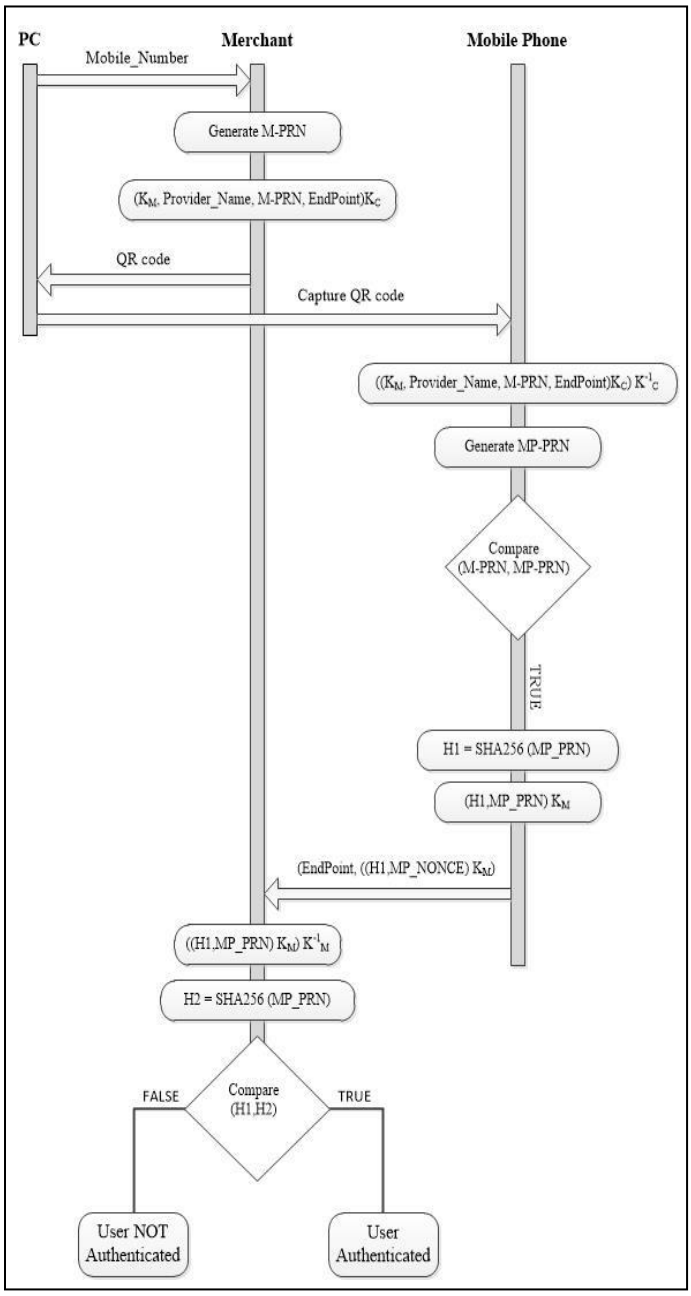

Fig 2. MUAS Authentication process diagram

Figure 3 shows the MUAS algorithm, which explains how to verify the identity of the client and merchant through a cryptographic QR code.

//Merchant-SIDE
IF (Mobile_Number)
1. Client_cert=Pass_ClientCert_to_merchant();
2. M_PRN=Generate_MPRN(Mobile_Number);
3. Merchant_PK=Extract_PublicKey_from_MerchantCert();
4. QRcode=Append(Merchant_PK,ProviderName,M_PRN, EndPoint);
5. Client_PK=Extract_PublicKey_from_ClientCert(Client_cert);
6. Encrypted_QR=Encrypt_QR(QRcode,Client_PK);
7. Pass_Encrypted_QR_to_PCbrowser(Encrypted_QR);

//Mobile Phone-SIDE
8. Captured_QR=Capture_QR_by_camera();
9. Client_PrivKey=Extract_PrivateKey_from_ClientCert (Client_cert);
10. **D**ecrypted_QR=Decrypt_QR(Encrypted_QR,Client_ Privkey);
11 .QR_Array=SplitString(Decrypted_QR);
12. MP_PRN=**G**enerate_MPPRN(IMSI_MobileNumber);
13. Compare_Result=**C**ompare(M-PRN, MP-PRN);
14. **IF** (Compare_Result==true)
    15. **H**ash1_MPprn=SHA256(MP_PRN);
    16. Hash_and_OrigMsg=Append(Hash1_MPprn,MP_PRN);
    17. Encrypted_Hash_OrigMsg=Encrypt_Hash(Hash_and_ OrigMsg,QR_Array[0]);
    18. Pass_EncryptedHash-to-Merchant(QR_Array[3] Encrypted_Hash_OrigMsg);

//Merchant-SIDE
    19. Merchant_PrivKey=Extract_PrivateKey-from Merchant (Merchant_cert);
    20. Decrypted_Hash_OrigMsg=Decrypt_RecievedHash (Encrypted_Hash_OrigMsg,Merchant_PrivKey);
    21. Hash_Array=SplitString(Decrypted_Hash_OrigMsg);
    22. Hash2_MPprn_by_Merchant=SHA256(Hash_Array[1]);
    23. Verify_Hash(Hash2_MPprn_by_Merchant,Hash_ Array[0]);
ELSE
Exit
END IF
END IF

Fig 3. MUAS Algorithm

IV. RELATD WORK

In e-commerce, all authentication evidence between the client and the merchant is exchanged through a single communication channel, usually the internet, making it prone to eavesdropping attacks. Given the large penetration of mobile phones, some recent studies considered extending the usage of SIM card authentication, along with its wireless mobile network, to web services for identity authentication. In addition, the mobile industry began to pay more attention to QR code applications in m-commerce, because of its simplicity and inexpensiveness in presenting diverse

commerce data. Moreover, it effectively improves mobile user experience through reducing mobile inputs [28]. Therefore, a lot of research work and technology studies have been done on mobile-based QR code applications to provide a secure and reliable e-commerce authentication system.

A. SIM-based Identity Authentication

The use of mobile phones and their SIM cards for identity authentication has been the focus of many studies, in order to provide secure, reliable, and easy-to-use on-line authentication solutions. Van Thanh et al.[11, 14] proposed some solutions tailored for Single-Sign-On (SSO) authentication, in which users can access services from their PC/laptop. The user's browser is redirected to the identity provider (IdP) for logging in, using some extra hardware devices, such as SIM-card readers, USB dongle, or cables to connect the mobile to the PC. In some cases, Bluetooth connection is required. SSO Authentication can also be used for users accessing servers from their mobile phones, where, in this case, verification is done through SMS messages.

Al-Qayedi et al. [10] and Me et al. [12] proposed other authentication approaches that combines traditional web-based username/password approach, with mobile-based challenge/response authentication, and an OTP, in order to provide privacy and eavesdropping security.

Abe et al. [13] proposed a similar, yet better solution requiring an (IdP) software running on the mobile phone. Whenever a user requests a service, the service provider redirects the user to the IdP on his mobile phone. The IdP software generates a digital signature, and sends it to the service provider for verification.

In summary, most SIM-based identity authentication approaches meet the requirements of mobility, usability, availability, and security. On the other hand, it increases the risk of MITB attack, due to the use of PC browsers as the main communication channel. While MUAS decreases the risk of MITB attack by employing QR code in an OOB communication channel.

B. SIM-based QR Code Authentication

The simplicity and cost effectiveness of QR code technology have caused a number of new approaches to use it in on-line authentication solutions. QR code works quickly by establishing a secure connection between the server, desktop, and the mobile phone [29]. Dodson et al. [29] proposed Snap2Pass, a technique in which a client creates an account, and logs into a website from a PC browser. The technique works by the client capturing the displayed QR code, which encodes a cryptographic challenge, and sending the cryptographic response to the server for verification. Vapen et al. [30] proposed a similar approach called 2-clickAuth which is based on implementing an Identity Provider in the OpenID federated identity management system, making the authentication solution available to all users of sites that support OpenID. Both approaches provide high levels of security, availability, and usability. Compared to MUAS, our approach does not require an account creation with any website, nor requires an Identity Provider, since it can be applied to any e-commerce website. Moreover, both approaches do not overcome the risk of MITB attack. Where Snap2Pass account creation phase lacks QR code cryptography, and 2-clickAuth uses an untrusted PC to capture the response generated by the mobile phone.

Choi et al. [31] proposed a similar approach to 2-clickAuth, yet it employed an extended authentication server, to prevent phishing server attacks in Single-Sign-On (SSO). The extended server generate a QR code to be captured by the mobile, which in turn generates another QR code to be captured by a webcam. This two-way QR code generation can be effective against MITB. But on the other hand, it is less practical.

Kim and Jun [32] proposed an authentication technique by using a registered mobile phone. Whenever a registered user requests a service from the service provider, the service provider extracts the user information and generates a QR code. The mobile phone analyse the QR code contents, and send them to the service provider for validation. In comparison to MUAS, our approach requires the client to only submit his mobile number. While the proposed approach requires no user input, which in turn helps minimize the risk of MITB attack. But on the other hand, the client's mobile phone needs to be registered with the service provider.

C. SIM-based Encrypter QR Code Authentication

Ease of QR code capturing and contents viewing are considered as the technique's main shortcomings, especially in authentication systems, where security is essential. Therefore, a trend toward combining QR code technology with cryptography can help ensure recipient's authorization, and increase QR code contents security and confidentiality, required for authenticating users. As a result, a number of techniques have been proposed to use the QR code in the field of cryptography. Dey [33] proposed SD-EQR, an algorithm to store messages in an encrypted format with a password and sends it to the destination hidden in QR code. The algorithm works by generating a secret code from a chosen password, which will be added to each letter of the message, in order to generate the first phase of encryption. Followed, is reversing the encrypted message. Finally, an exclusive-OR is performed. Compared to MUAS, our QR code cryptography requires less computations than SD-EQR, since MUAS algorithm only performs one level of encryption.

V. SYSTEM DESIGN AND EVALUATION CRITERIA

In this section, we present the system design and initial evaluation criteria of the proposed MUAS.

A. System Design

Figure 4 shows the MUAS architectural design. The components of the proposed system are described as follows:

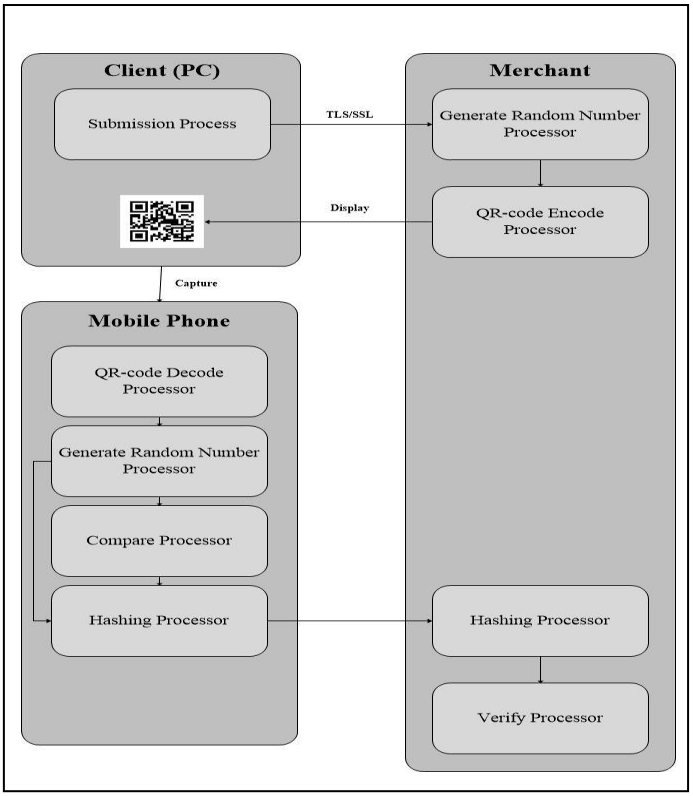

Fig 4. MUAS architecture

1) Client (PC)

Submission Process: it initiates the MUAS through submitting the client's mobile number.

2) Merchant

Generate Random Number Process: it uses the mobile number as a seed to generate the merchant-random number.

QR-code Encode Process: it appends the merchant-random number with the merchant's public-key, provider's name, and merchant's URL address, encrypt them with the client's public key, and generate the QR-code.

Hashing Process: it performs an (SHA256) hashing algorithm on the received mobile phone-random number, generated by the mobile phone.

Verify Process: it compares both hashes to verify user's authenticity.

3) Mobile Phone

*QR-code **D**ecode Process:* it decodes the captured QR image, and decrypt it using the client's private key.

***G**enerate Random number Process:* it generates a random number, from the mobile number embedded in the IMSI.

***C**ompare random Numbers:* it splits the appended QR code contents to get the merchant-random number, and compares it against the mobile phone-random number

***H**ashing Process:* it perform an (SHA256) hashing algorithm on the mobile phone-random number.

B. Evaluation Criteria

The trend towards designing an on-line authentication system have extended beyond solving security issues to systems which are available and user-friendly.

The MUAS employment of a secure personal device, such as a mobile phone is considered an ideal solution for on-line authentication systems, since the phone is always with us and always switched on, which makes it available at all times. Moreover, using mobile phones eliminates the need to carry around extra hardware for authentication, which in turn help satisfy the mobility and usability features.

MUAS can be considered as a user-friendly system, due to the requirement to submit the minimum amount of information, which is the mobile number.

The proposed system satisfy the following e-commerce security requirements:

1) Integrity

The generation of random number processor at the merchant-side and mobile phone-side ensures integrity, in which both processors generate the same random number, due to using the same seed. Even if an intruder manipulated the mobile number submitted by the client, which is unlikely to happen, due to the use of TLS/SSL, the mobile phone-side will notice the manipulation and will stop the authentication process immediately.

2) Confidentiality

The QR code encoding/decoding processors at the merchant-side and mobile phone-side ensures confidentiality through encapsulating and encrypting significant information into a QR code. These information can only be revealed to the legitimate mobile phone holder, who must use his PIN-protected private key to decrypt the information, which will be used in the authentication process. Therefore, even if the mobile phone was stolen, the private key cannot be obtained, due to the use of a PIN.

3) Non-repudiation

The hashing processor at the mobile phone-side satisfies the non-repudiation security requirement through hashing the random number generated from the embedded IMSI. The hash result is sent to the merchant to be compared against another hash generated from the submitted mobile number. This can be considered a legal proof that the client has placed an order.

C. Implementation

The basic prototype of MUAS framework has been implemented using C++ Builder XE3. The next step will be to simulate the framework's protocol using NS2 to test its speed, reliability, and scalability.

VI. SECURITY ANALYSIS

Assume a secure SSL/TLS communication channel between the client (PC), and the merchant. TLS/SSL protocol has been developed by the Internet Engineering Task Force (IETF) as the standard protocol for providing security services in the context of e-commerce over the internet [34]. The primary goal of employing SSL/TLS in the MUAS is the client/server mutual authentication, and their encryption algorithm and cryptographic keys negotiation which ensures authenticity, privacy and integrity for data being sent between the communicating parties. Moreover, the MUAS employs an Out-Of-Band (OOB) communication channel (cellular network) for QR code capturing, to reduce the use of PC browsers, which in turn helps overcome the risk of Man-In-The-Browser (MITB) attack.

In the proposed system, the merchant generates a random number from the received mobile number, appends it with the merchant's public-key, provider's name, and merchant's end-point. Next, it performs RSA cryptography, and form the QR code. RSA is an asymmetric algorithm, which ideally suited the real-world use, as the secret key does not have to be shared, the risk of being known is much smaller than symmetric algorithms. In terms of security, RSA is considered the most secure algorithm. Finally, the mobile phone performs a hashing algorithm (SHA256) on the random numbers, and sends the hash result along with the original message to the merchant for verification. SHA256 was chosen due to its high speed and its reasonable digest size.

VII. CONCLUSION AND FUTURE WORK

Initially, on-line fraudsters used to steal customer's personal information by sending phishing e-mails, in order to steal money from their internet banking account. Nowadays, fraudsters are using newer and more advanced methods to defraud on-line clients. One of the most dangerous methods is Man-In-The-Browser (MITB) attack. Therefore, this paper proposes a Mobile User Authentication System (MUAS) that integrates a number of technologies to help achieve a stronger authentication solution, such as mobile phones, cryptography, hashing, and QR code. The MUAS mutually authenticates the client and the merchant, while overcoming the MITB by reducing the use of PC browsers, and using mobile phones along with their cellular network instead. Moreover, the MUAS satisfies e-commerce security requirements: authenticity, integrity, confidentiality, and non-repudiation.

This research is part of a larger scope, in which the future work will extend the MUAS client and merchant authentication to on-line transaction authentication, and verifying legitimate mobile phone holders through GSM Mobile Network (GMN). In other words, a mobile electronic transaction layer will be integrated to MUAS. Where the mobile phone will verify the integrity of the client-generated confidential information by passing it to the merchant, bank, and GSM authentication server, all the way back to the mobile phone. The future framework will authenticate all parties involved in the transaction, while ensuring data confidentiality, non-repudiation, and defeating MITB attack.

REFERENCES

[1] S. Hallsteinsen, I. Jorstad, and T. Do Van, "Using the mobile phone as a security token for unified authentication," in *Systems and Networks Communications, 2007. ICSNC 2007. Second International Conference on*, 2007, pp. 68-68.

[2] X. Yin, J. Zou, C. Fan, and P. Zhou, "An Improved Dynamic Identity Authentication Scheme Based on PKI-SIM Card," in *Wireless Communications, Networking and Mobile Computing, 2009. WiCom '09. 5th International Conference on*, 2009, pp. 1-4.

[3] T. Fan Yu and P. Su Gui, "Design of Two-Way One-Time-Password Authentication Scheme Based on True Random Numbers," in *Computer Science and Engineering, 2009. WCSE '09. Second International Workshop on*, 2009, pp. 11-14.

[4] C. Li, Y.-x. Yang, and X.-x. Niu, "Biometric-based personal identity-authentication system and security analysis," *The Journal of China Universities of Posts and Telecommunications*, vol. 13, pp. 43-47, 2006.

[5] M. Xiaoming, "Study on the Model of E-Commerce Identity Authentication Based on Multi-biometric Features Identification," in *Computing, Communication, Control, and Management, 2008. CCCM '08. ISECS International Colloquium on*, 2008, pp. 196-200.

[6] M. Yildiz and M. Gokturk, "Combining Biometric ID Cards and Online Credit Card Transactions," in *Digital Society, 2010. ICDS '10. Fourth International Conference on*, 2010, pp. 20-24.

[7] N. Li Huang and D. T. Tan, "A novel JavaCard-based authentication system for secured transactions on the Internet," in *Networks, 2000. (ICON 2000). Proceedings. IEEE International Conference on*, 2000, pp. 262-266.

[8] T. Qian, Z. Junwei, F. Chunxiao, and Z. Xiaoying, "A mobile identity authentication scheme of e-commerce based on Java-SIM card," in *Information Networking and Automation (ICINA), 2010 International Conference on*, pp. V2-114-V2-118.

[9] T. Do van, A. Nachef, J. D. Aussel, I. Jørstad, R. Perlman, J. Vigilante, *et al*. (2006). *Offering SIM Strong Authentication to Internet Services*. Available: http://projectliberty.org/liberty/content/download/397/2750/file/SIM_Strong_Authentcation_Whitepaper.pdf

[10] A. Al-Qayedi, W. Adi, A. Zahro, and A. Mabrouk, "Combined Web/mobile authentication for secure Web access control," in *Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE*, 2004, pp. 677-681 Vol.2.

[11] T. Do van, T. Jonvik, T. Do van, and I. Jorstad, "NETp1-09: Enhancing Internet Service Security Using GSM SIM Authentication," in *Global Telecommunications Conference, 2006. GLOBECOM '06. IEEE*, 2006, pp. 1-5.

[12] G. Me, D. Pirro, and R. Sarrecchia, "A mobile based approach to strong authentication on Web," in *Computing in the Global Information Technology, 2006. ICCGI '06. International Multi-Conference on*, 2006, pp. 67-67.

[13] A. Tsuyoshi, I. Hiroki, and T. Kenji, "Implementing identity provider on mobile phone," presented at the Proceedings of the 2007 ACM workshop on Digital identity management, Fairfax, Virginia, USA, 2007.

[14] D. van Thanh, T. Jonvik, F. Boning, D. van Thuan, and I. Jorstad, "Simple Strong Authentication for Internet Applications Using Mobile Phones," in *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*, 2008, pp. 1-5.

[15] M. Ashraff, M. L. Kabir, S. M. Aziz, and B. k. Dey, "A Conceptual Framework for a SIM-based Electronic Transaction Authentication System," in *Network and Parallel Computing Workshops, 2007. NPC Workshops. IFIP International Conference on*, 2007, pp. 65-71.

[16] D. van Thanh, I. Jorstad, T. A. Johansen, E. Bakken, and D. van Thuan, "Pervasive service access with SIM-based VPN," in *Mobile Adhoc and Sensor Systems, 2009. MASS '09. IEEE 6th International Conference on*, 2009, pp. 836-841.

[17] W. Audun, L. Lars, J. Ivar, and D. Than van, "Secured enterprise access with strong SIM authentication," in *Enterprise Distributed*

Object Computing Conference, 2006. EDOC '06. 10th IEEE International, 2006, pp. 463-466.

[18] T. Do Van, T. Jnvik, I. Jrstad, B. Feng, and T. Do Van, "Strong authentication using dual SIM," in *Intelligence in Next Generation Networks, 2009. ICIN 2009. 13th International Conference on*, 2009, pp. 1-4.

[19] C. Le-Pong and C. Jyh-Yen, "SIM card based e-cash applications in the mobile communication system using OTA and STK technology," in *Wireless, Mobile and Multimedia Networks, 2006 IET International Conference on*, 2006, pp. 1-3.

[20] R.-J. Hwang, S.-H. Shiau, and D.-F. Jan, "A new mobile payment scheme for roaming services," *Electronic Commerce Research and Applications*, vol. 6, pp. 184-191, 2007.

[21] J. T. Issac and J. S. Camara, "An anonymous Account Based Mobile Payment Protocol for a Restricted Connectivity Scenario," presented at the Database and Expert System Applications, 2007. DEXA, 07. 18th international workshop on, 2007.

[22] A. A. Tabandehjooy and N. Nazhand, "A Lighweight and Secure Protocol for Mobile Payments Via Wireless Internet in M-commerce," in *e-Education, e-Business, e-Management, and e-Learning, 2010. IC4E '10. International Conference on*, 2010, pp. 495-498.

[23] A. Bottoni and G. Dini, "Improving authentication of remote card transactions with mobile personal trusted devices," *Computer Communications*, vol. 30, pp. 1697-1712, 2007.

[24] M. Almeida, E. Dimogerontakis, U. Buyuksahin, and A. Tarhan, "Man-In-The-Browser Attacks," 2011.

[25] (2011). *MAKING SENSE OF MAN-IN-THE-BROWSER ATTACKS - Threat analysis and Mitigation for Financial Institutions*. Available: http://twimgs.com/darkreading/authentication/Making_Sense_of_Man-in-the-Browser_Attacks.pdf

[26] M. Almeida, E. Dimogerontakis, U. Buyuksahin, and A. Tarhan, "Man-In-The-Browser Attacks," Decemebr 20, 2011.

[27] (2010). *Defeating Man-in-the-Browser: How to prevent the Latest Malware Attacks against Consumer and Corporate Banking*.

[28] J. Z. Gao, L. Prakash, and R. Jagatesan, "Understanding 2D-BarCode Technology and Applications in M-Commerce - Design and Implementation of A 2D Barcode Processing Solution," in *Computer Software and Applications Conference, 2007. COMPSAC 2007. 31st Annual International*, 2007, pp. 49-56.

[29] B. Dodson, D. Sengupta, D. Boneh, and M. S. Lam. (2009, Snap2Pass: Consumer-Friendly Challenge-Response Authentication with a Phone. Available: senguptas.org/Documents/secure2pass_www2009.pdf

[30] A. Vapen, D. Byers, and N. Shahmehri, "2-clickAuth Optical Challenge-Response Authentication," in *Availability, Reliability, and Security, 2010. ARES '10 International Conference on*, pp. 79-86.

[31] C. Kyeongwon, L. Changbin, J. Woongryul, L. Kwangwoo, and W. Dongho, "A mobile based anti-phishing authentication scheme using QR code," in *Mobile IT Convergence (ICMIC), 2011 International Conference on*, pp. 109-113.

[32] K. Young-Gon and J. Moon-Seog, "A design of user authentication system using QR code identifying method," in *Computer Sciences and Convergence Information Technology (ICCIT), 2011 6th International Conference on*, 2011, pp. 31-35.

[33] S. Dey, "SD-EQR: A New Technique To use QR Codes in Cryptography," *International Journal of Information Technology & Computer Science (IJITCS)*, vol. 3, pp. 11-21, May/June 2012.

[34] "The Secure Sockets Layer (SSL) Protocol Version 3.0 ", ed: Internet Engineering Task Force (IETF), RFC: 6101, August 2011.