A Novel QR Code and mobile phone based Authentication protocol via Bluetooth

Sha Liu[*1], Shuhua Zhu[2]

[*1] School of Information Science and Technology, Jinan University, Guangzhou, China

[2] Network & Educational Technology Center, Jinan University, Guangzhou, China

shaliu@163.com

Keywords: List the keywords covered in your paper. These keywords will also be used by the publisher to produce a keyword index. Four-party; QR Code; OTP; Bluetooth; Authentication

Abstract. Password based authentication schemes are widely used in our daily life when we log into websites. However, there are varieties of problems with the simple methods, including susceptibility to unintentional exposure via phishing and cross-sites password reuse. We present a novel mobile phone based authentication scheme, which intends to provide security and usability greater than that of traditional two-factor authentication protocols. It contains four parties, i.e. the user, the mobile phone, the current computer and the remote server. At first, a user's personal device-mobile phone-stores the key token by scanning QR code, which is sent from the server after user completes the registration phase. Secondly, the current computer can use the Bluetooth device address registered in remote server to launch a connection request and then it can communicate with the mobile phone via Bluetooth. Thirdly, when user wants to log into a website, server would transmit an OTP(One time password)to user's mobile phone through the current computer in order to verify the user. Finally, our scheme has achieved the mutual authentication via Bluetooth. Our scheme only needs lower computation. In terms of users' requirements, our scheme provides request about changing bind-phone for legal users over the email address registered during registration phase. After usability and security analysis, we can demonstrate that the new scheme fits for the complicated network environment.

Introduction

The traditional user authentication factors can be divided into three categories: what you know, for example, user's name and password ; what you have, such as smart cards; what you are, such as fingerprint information. Password-based authentication, which is known as "one -factor authentication ", is one of the most widely used and accepted authentication type. It has some natural and practical advantages, however, its disadvantages are also obvious: users tend to use simple and easy-to-guess passwords, and often reuse passwords across different websites[1][2]. Therefore, some attackers have chances to steal user's password by launching off-line guessing attacks and phishing attacks. Meantime, server stores a lot of information as the form of plaintext , which can be easily stolen by attackers. As a result, user's personal information will be leaked which even would endanger the property security of users[3][4]. So some researchers made various efforts and attempts to improve password security, and the idea of one-time password -based authentication was proposed later. As the name suggests, a one-time password authentication is the password only be effective in a limited time, and the server does not need to store the user 's password table. It can resist against password guessing and dictionary attacks and achieves a big improvement in security[5]. However, one-time password is generated related to the specific complex algorithms, which is often used as an auxiliary role to help complete the authentication process[6] [7].

So many researchers tend to focus on the two-factor authentication, which not only inherits the advantages of password-based authentication, but also improves the security of this kind of authentication scheme. In recent years, two-factor authentication, especially the smart card -based authentication scheme, because of its low computation and high security, has been attracted more

and more attention from scholars[8][9][10][11][12][13], but it also has some inevitable problems, such as user usability. Even though smart cards are small and easy-to-carry, many users still not used to carry an additional device when they need to login into system; In addition, security of such schemes are questionable. It is based on the premise that information stored on the smart card is secure, but a growing number of researches have indicated that the secret information within the smart card can be extracted through some extraordinary measures, such as forced electricity cut-off, so security of these scheme designed on this assumption cannot be guaranteed.

With the development of smart phones, their features and applications become more perfect. To some extent , performance of some smart phones would be able to compete with small computers. Smart phones have become a necessity of people's daily life. So someone proposes a new form of two-factor authentication, password and phone, in accordance with this trend. It is a perfect solution to meeting the user practical considerations, while the amount of smart phones' computation and storage is much larger than smart card[14][15] .

In this paper, we adopt a variety of current mainstream techniques and proposes an innovative QR-Code based four-party authentication protocol. There are four parties involved in the authentication process: user, remote server, the current computer, and smart phone. New protocol uses two-factor authentication type: password& phone. The user firstly needs to register with remote server by name, phone's Bluetooth device address and e-mail address. Then phone would scan QR-Code that contains the token information generated by server, and store the token in the phone. In the authentication process, the current computer based on the Bluetooth address sent by server to initiate a Bluetooth connection with the user's smart phone, the current computer would send one-time passwords and other information to the user 's smart phone via Bluetooth.

Our Contribution

Our protocol is novel and the state of art. The major innovations as the following:Our protocol is a new two-factor based authentication involved four parties, based on our understanding of the field, we should be the first one scheme to take the current user 's computer into consideration among the authentication phase, and regard the current computer as a trusted device and credible channel in our protocol. This can increase the safety and operability. Registration information in our protocol, including user's name and the phone's Bluetooth device address and e-mail address, as far as we know, we should be the first one to adopt the Bluetooth device address as part of registration information , previous studies did not take into account the use of users' Bluetooth device address. The device authentication schemes even did not intend to consider a Bluetooth connection. It can easily and quickly implement Bluetooth connection between the current computer and user's smart phone in order to realize the communication. Compared with the schemes based on SMS messages, It can avoid the security problems of information transmission and the fees paid to the operators.

Our protocol also uses a currently very popular and commercial two-dimensional code, QR Code technology, as a visual OOB, transmitting the authentication tokens distributed by registration server and some secret information . It can avoid leakage and theft problems when the server sending messages to the phone, and it can also save the overhead and reduce the latency.

Our protocol draws on a self-verified timestamp technique[16] from the one who generates the original timestamp to verify the validity of the counterpart timestamp, which effectively solves the clock synchronization problems in most timestamp based authentication schemes, the timestamps can be also used as nonce, which can save the overhead of generating random numbers .

Our protocol selects one-time password generation algorithm, users can get the current password via Bluetooth, which can improve the security of scheme.

Paper Organization

The rest of the paper is organized as follows. Section 4 covers background about several technologies involved in our scheme. Then, we describes our new authentication in details in section 5.In section 6, we discuss the usability and security of our scheme. Finally, in section 7, we make our conclusions.

Related Work

QR Code. QR Code (Quick Response Code) is a two-dimensional code standards, which was first by a Japanese company Denso proposed by the invention in 1994[17].In 2000, it successfully became an ISO International Standard . Initially , QR Code is designed to be applied in the control of automated production processes and design, but later it is widely used in many other areas .

QR Code is a matrix symbol , with high data capacity, high-speed data acquisition, high-density data printing and other features. Compared to a linear one-dimensional codes , two-dimensional code can store more data and requires a relatively longer time to read and process the data.

OR Code Based Authentication. More and more people start to concern about such a small two-dimensional code , because it's really convenient , people can add friends, log into a website and even complete payment by scanning it. In terms of social networking and commercial purposes, it is already everywhere, and there are some people doing some researches about authentication by adopting it.

In 2006, McCune[18] proposed a two-dimensional code based device pairing authentication framework. This is the first instance of a detailed application of the two-dimensional code in the authentication scheme. In 2009, Guenther et al [19]proposed a QR Code and mobile phone based two-factor " challenge - response" mechanism as authentication scheme ,which contains "data + nonce" content called "QR-TAN". It was the first time that QR Code considered as the main technology to be used in authentication scheme. But the scheme was based on public and private key system, and there were not good methods to solve the problem of generation and distribution of keys, making it difficult to promote this method in practical life-use. In 2010 , Liao et al [20]proposed an innovative QR Code -based and one-time password authentication protocol. It uses timestamp technique replaced conventional random numbers to achieve lower computation and small storage features. However, the protocol didn't take into account that the need to address the timestamp network clock synchronization issues, and it demonstrated that the protocol still has security flaws.

In 2013, Harini [21]proposed a two-factor authentication scheme called "2CAu" that was based on public-private key system. It adopted multiple technologies, such as QR Code, one-time password , smart card, to achieve mutual authentication. However, the scheme faces the same problem with Liao's. Besides, there was an issue that users need to carry on smart card, so the usability will be greatly reduced . In the same year, Soonduck et al[22] proposed a simple authentication scheme based on QR Code. This scheme used user name and password , and then verified the mobile phone to scan two-dimensional code to complete the two-way authentication process.

Proposed Scheme

There are four parties involved in our scheme ,including a remote server(S), the current computer(C), user(U) and mobile phone(M). Authentication process is divided into four phases as follows: the preliminary phase, the registration phase , the login phase , the authentication phase and change bind-phone phase. Notations of the symbols used in scheme are as followings :

Smart phones defined in our scheme should have some features: it is relatively moderate volume, with a high resolution touch screen, and also has a high pixel camera, meaning that it has a

relatively strong computing power and can handle a relatively sophisticated authentication information.

ID_u : User identification ;

B_Adds : Bluetooth device address ;

E_Adds : E-mail address

K : Long-term key remote server ;

$Token_u$: The remote server to users of tokens ;

$E_{QR}(.)$: QR Code encryption algorithms

$D_{QR}(.)$: QR Code decryption algorithms;

OPW : Remote server -generated OTP password ;

$h(.)$: Single-secure hash function ;

T : Current timestamp ;

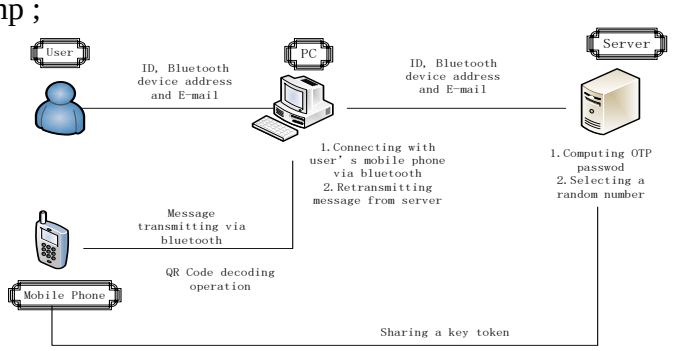

Fig 1 Four-party authentication scheme

Preliminary phase. During the authentication process between U and M , U should confirm the identity of M and M need also to check the identity of U by password and gesture.

Fig 2 authentication between user and mobile phone

Registration phase:

Step 1. U submits ID_u , B_Adds and E_Adds to S .

Step 2. S check ID_u , ID_u and E_Adds , if any information has been registered , S requires U to reselect the new information. Otherwise, S computes $Token_u = h(ID_u \| K \| T_r)$, $E_{QR}(Token_u)$.

Step 3. U computes $D_{QR}(E_{QR}(Token_u)) = Token_u$, store it securely on the phone.

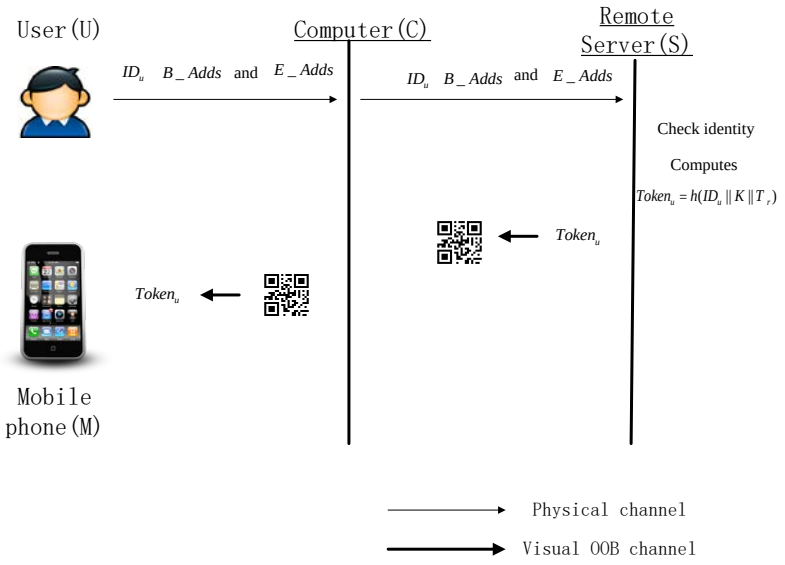

Fig 3 Registration phase

Login phase. Step 1. U sends a login request, and inputs ID_u. S sends B_Adds to C, then C initiates a Bluetooth connection with M through B_Adds.

Step 2. S generates password OPW and transmits it to C, and C forwards it to the user 's mobile phone M via Bluetooth, then the user obtains OPW.

Step 3. U submits $\{ID_u, h(OPW \| T_1), T_1\}$ to S.

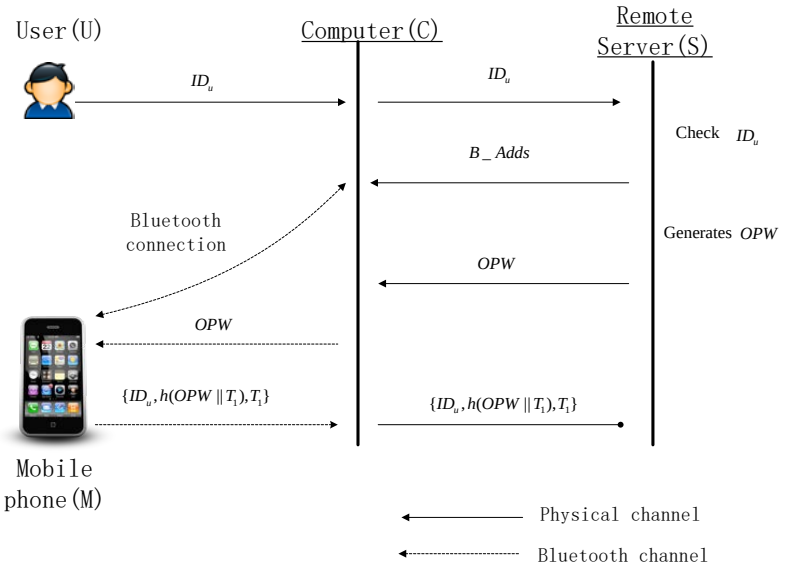

Fig 4 Login phase

Authentication phase :

Step 1. S authenticates $\{ID_u, h(OPW \| T_1), T_1\}$, and generates a random number R.

S computes $Token_u = h(ID_u \| K \| T_r)$,

$A_u = E_{Token_u}(T_1 \| T_2 \| R)$, $B_u = h(T_1 \| \mathrm{R} \| T_2)$, T_2 is the current timestamp of S

Step 2. S transmits $E_{QR}(A_u)$, B_u to U ..

Step 3. After receiving the information from S, U calculates

$D_{QR}(E_{QR}(A_u)) = A_u$, $D_{Token_u}(\mathrm{A}_u) = D_{Token_u}(E_{Token_u}(T_1 \| T_2 \| R)) = T_1 \| T_2 \| R$,

U checks $T_1^{'} - T_1 \le 2\Delta T$, $T_1^{'}$ is the current timestamp of U. If the inequality holds, U verifies $B_u^{*} = h(T_1 \| R \| T_2) = B_u$. If the equality holds, U successfully authenticates S.

Step 4. U calculates $C_u = E_{Token_u}(T_3 \| T_2 \| R)$ and $D_u = h(T_3 \| \mathrm{R} \| T_2)$,then sends the message $\{C_u, D_u\}$ via Bluetooth, finally transfer to S.

Step 5. When receiving the message from U, S computes $D_{QR}(E_{QR}(C_u)) = C_u$

$D_{Token_u}(C_u) = D_{Token_u}(E_{Token_u}(T_3 \| T_2 \| R)) = T_3 \| T_2 \| R$,

S should verify if R is equal to the initial value. Then S checks $T_2^{'} - T_2 \le 2\Delta T$, $T_2^{'}$ is the current timestamp of U. If the inequality holds, S should verify $D_u^{*} = h(T_3 \| R \| T_2) = D_u$. If the equality holds, S successfully authenticates U. So far, U and S completes the two-way authentication.

Step 6. S calculates $Token_{u1} = h(ID_u \| K \| T_r \| T_{a1})$, $E_{QR}(Token_{u1})$. T_{a1} is timestamp of S.

Step 7. U computes $D_{QR}(E_{QR}(Token_{u1})) = Token_{u1}$ and stores it on the phone instead of the old one.

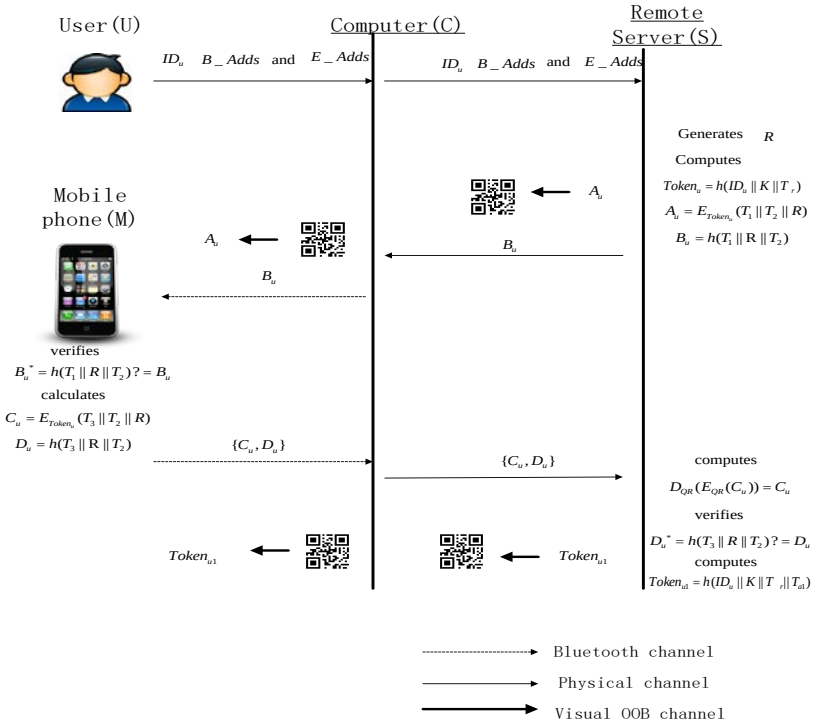

Fig 5 Authentication phase

Change bind-phone phase

If the previous user 's bind-phone has been lost or stolen by someone, users can propose the request to the remote server for changing bind-phone.

Step 1. U enters ID_u and sends the change request to S. A piece of the audio document contains some random characters generated by S. And all of these are sent to the associated Email address registered by user in registration phase, U should download the audio document and read it, then input the random characters AD.

Step 2. U submits $\{h(AD \| T_1), T_1, NewB\_Add\}$ to the S, T_1 is the current timestamp of U.

Step 3. S checks $T_1^{'} - T_1 \le \Delta T$, $T_1^{'}$ is current timestamp of S, and verifies the validity of ID_u, $NewB\_Add$.

Step 4. S checks $A = h(M \| T_1) = A^*$. If the equation holds, S accepts the requirements of changing bind-phone by U.

Step 5. S recalculates $Token_c = h(ID_u \| K \| T_r \| T_c)$, $E_{QR}(Token_c)$.

U uses a new mobile phone to read and compute $D_{QR}(E_{QR}(Token_u)) = Token_c$, stores it on the new phone.

Security and Performance Analysis

Usability Analysis. 1. Calculation. Throughout the certification process, it involves only a one-way hash function arithmetic and QR Code for encryption and decryption operations. Therefore, it is clear that the entire load calculation of whole scheme is relatively lower , and the new scheme can be applied to many lightweight computation based applications, while it is also very easy to implement it on devices to achieve promotion. 2. Technology. Our scheme draws on the self-verified timestamp technology. It not only solves the problem of clock synchronization , but also avoids the resource consumption from generation of random number. Compared to similar schemes, our scheme is more efficient and simple. The scheme also uses a one-time password , which combined with the time stamp technology has enhanced authentication security. For servers, our scheme has reduced the overhead of storing password table and avoided the risk of being leaked passwords. To a certain extent, it has improved the efficiency of authentication. 3. Equipment. Authentication scheme just needs the user's mobile phone, which has regarded as a daily-life auxiliary equipment, without any additional hardware. It is no doubt that our scheme could eliminate extra burden to users and improve the usability of t scheme.

Security Analysis. 1 Attack Model. Assuming that certified environmental is relatively closed, not including the more broader common areas, such as train stations and the airports. In these places, there are many factors interfere with the authentication process that we cannot control.

We assume that information transmitted over visual OOB channel, the program cannot be eavesdropped, blocked and modified, the message transmitted via Bluetooth may be eavesdropped by attackers, in other words, an attacker could reply and modify these information, which affects the certified process. 2 Security Features. 1) Mobile Information Security. In our authentication scheme , the mobile phone as a token of long-term storage media plays a crucial role in the authentication, and user should store it safely . However, once mobile phone is lost or stolen by someone, user can change the server bind-phone, and user can rebind a new phone. So, even people who have get phone can't log in through the mobile phone directly and can't get the server's long-term key K from $Token_u$, because of the security of one-way hash function , therefore our scheme could ensure the information security . 2) Remote server security. From the previous section , attacker finds it difficult to forge a legal user by $Token_u$.Both server and user know long-term key K, as the one-way hash function is not reversible. Meanwhile attacker can't impersonate the server, because the attacker can't get one-time passwords and user 's phone $Token_u$. 3) The current computer security. The current computer has been regarded as a secure channel to transmit information between mobile phone and the server via Bluetooth, it is suggested that user should do the login operation on own computer. When computer has connected with the user's phone over Bluetooth connection, user need to confirm that whether it is your current computer . In the authentication process, messages are appended with a time stamp which are carried out cryptographic operations before they are transmitted through current computer. This allows the server and user to authenticate message whether it is original, which is largely avoiding man-in-the-middle attacks and replay attacks, so the current computer can be trusted. 4) User Security. If users have always carefully keep their mobile phones, the attackers will not have chance to obtain users' phone. In the authentication process, the user needs to use the mobile phone for Bluetooth connection to transfer message, attacker can't get the user's mobile phone. The

communication information all contain a timestamp and hash operations, thus ensuring that information can't be eavesdropped by attacker.

Conclusion

In paper, a novel QR-Code based authentication scheme is presented. There are four parties participate in the scheme: a remote server(S), the current computer(C), user(U) and mobile phone(M). The new scheme draws on a self-verified timestamp technology and QR Code technology to resist reply attacks and man-in-the-middle attacks. In addition, it adopts a onetime password to improve security of authentication. And it uses a mobile phone to connect with current computer via Bluetooth, which reduced the consumption and improved the efficiency. In our scheme, we select a one-way hash function and encryption and decryption operations for two-dimension code, which contains a lower computing. After usability analysis and security analysis, we can find that our scheme is more simple, secure and friendly compared with other similar type of schemes, and it extremely suits for practical applications.

Acknowledgements

This work is supported by the National Natural Science Foundation of China (Grant No. 61272415, 61272413, 61133014). It is also supported by the Science Program of Guangdong Province, China(Grant No.2012A080102007,2011B090400324, 2011B090400469, 2012B040305008, 2012B091000136, 2012B091000038) ,the Engineering Research Center Program of Guangdong University, China (Grant No. GCZX-A1103) and Technology Plan Program of Guangzhou City, China (Grant No.2013Y2-00071)

Reference

[1] Yan, J. J., Blackwell, A. F., Anderson, R. J., & Grant, A.. Password Memorability and Security: Empirical Results. IEEE Security & privacy, 2004, 2, (5), pp 25-31.

[2] Bonneau J. Measuring password re-use empirically. Light Blue Touchpaper, 2011.

[3] Bonneau J, Herley C, Van Oorschot P C, et al. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In Proceedings of the 2012 IEEE Symposium on Security and Privacy, IEEE, May 2012, pp 553-567.

[4] National Cybersecurity Awareness Month Updates,. https: //www. facebook. com/ notes/ facebook-security/ national-cybersecurity-awareness-month-updates/ 10150335022240766 accessed 2011

[5] Haller N, Metz C, Nesser P, et al. A one-time password system. RFC 1938, May, 1996.

[6] Haller N. The S/KEY one-time password system. 1995.

[7] Liao I E, Lee C C, Hwang M S. A password authentication scheme over insecure networks[J]. Journal of Computer and System Sciences, 2006, 72,(4), pp 727-740.

[8] Lamport L. Password authentication with insecure communication. Communications of the ACM, 1981, 24, (11), pp 770-772.

[9] Hang M S, Li L H. A new remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics, 2000 , 46, (1) pp 28-30.

[10] Das M L, Saxena A, Gulati V P. A dynamic ID-based remote user authentication scheme. IEEE Transactions on Consumer Electronics, 2004, 50, (2) pp 629–631.

[11] Xu J, Zhu W T, Feng D G. An improved smart card based password authentication scheme with provable security. Computer Standards and Interface, 2009,31, (4), pp 723-728.

[12] Song R. Advanced smart card based password authentication protocol. Computer Standards and Interfaces , 2010, 32, (5), pp 321-325.

[13] Li X, Niu J W, Khan M K, et al. An enhanced smart card based remote user password authentication scheme. Journal of Network and Computer Applications, 2013, 36, (5), pp 1365-1371.

[14] D. van Thanh, T. Jonvik, B. Feng and I. Jorstad. Simple Strong Authentication for Internet Applications using Mobile Phone, in Global Telecommunication Conference(IEEE GLOBECOM), New Orleans, 2008.

[15] Aloul F, Zahidi S, El-Hajj W. Two factor authentication using mobile phones. 2009 ACS International Conference on Computer Systems and Applications, AICCSA 2009. IEEE, 2009, pp 641-644.

[16] Tsaur W J, Li J H, Lee W B. An efficient and secure multi-server authentication scheme with key agreement. Journal of Systems and Software, 2012, 85, (4), pp 876-882.

[17] QR Code. com. http: // www. denso-wave.com/ qrcode/ index-e.html accessed: Sept 16, 2009.

[18] McCune J M, Perrig A, Reiter M K. Seeing-is-believing: Using camera phones for human-verifiable authentication. Security and privacy. Proceedings of the 2005 IEEE Symposium on Security and Privacy. IEEE, 2005, pp 110-124.

[19] Starnberger G, Froihofer L, Göschka K M. QR-TAN: Secure mobile transaction authentication. 2009 International Conference on Reliability and Security, ARES'09.. IEEE, 2009, pp 578-583.

[20] Liao K C, Lee W H. A novel user authentication scheme based on QR-code. Journal of Networks, 2010, 5, (8) pp 937-941.

[21] Harini N, Padmanabhan T R. 2CAuth: A New Two Factor Authentication Scheme Using QR-Code. International Journal of Engineering & Technology, 2013, 5,(2) pp 1087-1094.

[22] Yoo S, Shin S, Ryu D. An effective Two Factor Authentication Method using QR code. 2013.