Novateur Publication's
International Journal of Innovation in Engineering, Research and Technology [IJIERT]
ICITDCEME'15 Conference Proceedings
ISSN No - 2394-3696

A MOBILE BASED ANTI-PHISHING AUTHENTICATION SCHEME USING CHALLENGE-RESPONSE AND QUICK RESPONSE CODE

Ganesh Kumar Mahato
Department of Computer engineering
Savitribhai Phule Pune University G.H.Raisoni College of Engineering and Management, Chas, Ahmednagar, India
gk6970@gmail.com

Sharma Kishan S.
Department of Computer engineering
Savitribhai Phule Pune University G.H.Raisoni College of Engineering and Management, Chas, Ahmednagar, India
shramak8976@gmail.com

Kurkure Shreyasi S.
Department of Computer engineering
Savitribhai Phule Pune University G.H.Raisoni College of Engineering and Management, Chas, Ahmednagar, India
shreyasi.kurkure@gmail.com

ABSTRACT
Quick Response (QR) code are 2D (two dimension) matrix code. Here it is use for secure authentication. Now days Internet is most commonlyused medium to access the information. People are using many website like online banking, insurance, shopping etc. these websites requires the strong authentication. Using a pair of username and password authentication scheme is not secure enough since attacker can collect information from web phishing and computer infection. Various malware or intended programs attempt to capture the confidential information from personal computer. Therefore, secure authentication scheme is required. Many authentication methods have been developed such as one time password, SMS base OTP system and some using bio-metric feature. Some of these authentications are fail due to network problem and increases the cost. People are increasingly used in all life fields, especially with the wide spread of Android smart phones which are used as QR-code scanners .In this paper, we propose a anti phishing single sign-on (SSO) authentication model using QR-code. This authentication scheme is secure against phishing attack and even on the distrusted computer environment. Quick Response (QR) Code can store large amount of encrypted data, and it also has error correction ability.QR-code which would be scanned by user mobile device and enter their password in mobile and again generate a QR-code in user mobile that QR-code would be scanners by webcam. For encryption and decryption we have used AES (Advanced Encryption Standard) algorithm and data unique at client side like IMEI number of the client android mobile device.

INTRODUCTION
An authentication method is proposed using two- factor authentication: mobile as one token and the challenge response method using quick response code. A Quick Response code is a two dimensional matrix code. It can store large amount of encrypted data, and it also has error correction ability.Inspite of massive use of current online banking system, it has many security loopholes as it's based on traditional password model, there is non-mutual authentication between user and bank server which leads to threats like phishing (stealing passwords and use of them for transactions), decoding communication lines, database hacking, etc.. To make transactions more secure but also keeping them easy for user, the proposed authentication system can be useful. Authentication is nothing but the process for identifying the person and providing the access to the system based on the identity of the person. The most commonly used method is static username and password. Remembering the password for many sites becomes difficult. There are different static and dynamic password systems, smart card based system, biometric, Kerberos, etc. used for authentication. The web attacks, malware attack, have increased. While accessing the information on the web, using an application on the network, public pc are insecure and for the physical access of the system the important issue is the security and authorization. The main aim of the authentication is to increase the identity, validity of the user and not to allow unauthorized access to the system. Challenge-response is used to protect phishing attacks and faster QR code generation.

BACKGROUND

DETAILS OF THE METHODS:-

REQUESTFROM UNTRUSTED COMPUTER

- User tries to access the finance website through untrusted local computer.
- User Types in the Client Id and clicks on submit button

WEB SERVER VERIFICATION PHASE 1

- Web server redirects user to extended authentication with Session ID, User Id and Server Info.
- The web server verifies the Server Info. If verification fails, then the request is assumed to be invalid and session aborts.

INFORMATION EXCHANGE PHASE

- The web server generates a random nonce to avoid tracking by adversary.
- The web server concatenates OpenID, Server Info and random nonce, and encrypts it with shared secret key.
- The server generates a QRCode with the encrypted data and time stamp and sends to desktop computer.
- User Scans the QRCode using his/her Mobile device, and then decrypts the data using shared secret key. Thus mobile device acquires the information; OpenID and ServerInfo, and random nonce.
- User types in the password in Mobile device generates a random nonce and then user inputs the password on the mobile device.
- Mobile device encrypts OpenID, shared data, Password, and User Rand using shared key, and then creates a QR code with the encrypted data.
- Once the QRCode is generated on phone, it is transferred again to Untrusted PC.

LOGIN FROM UNTRUSTED PC - WEB SERVER VERIFICATION PHASE 2

- User enters the QRCode and clicks on login
- User gets the site home page
- If the same QRCode is used from different machine it is invalidated by the server

A Mobile based Anti-Phishing Authentication Scheme using QR code

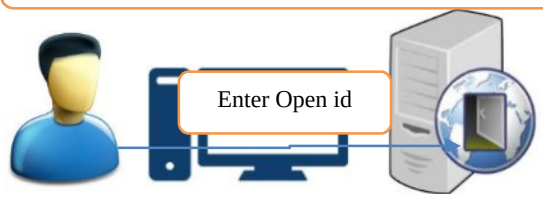

Figure 1 :-Flow of authnetication

TABLE 1:- SHOWS THE PARAMETERS IN OUR SCHEME.

Parameters	**Descriptions**
Open id	User fill URL in browser.
Client id	User identifier
Session id	A session Identifier
Random number	Random key[Generated by server]
Time Stamp	Generating time for QR code
IMEI	For identification purpose

LITERATURE SURVEY

1. Ms. Dhanashree Patil; Mrs. Shanti. K. Guru, "Secured Authentication using Challenge-Response and Quick-Response Code for Android Mobiles"

They presented that, Today Internet is the most widely used medium for accessing the information. On the internet, many websites are available for providing the information and also most of the services are getting Online such banking, insurance, shopping etc. These services providing websites requires the strong authentication. Multiple authentication methods have been developed such smart card based system, one time password, SMS based OTP system and some using biometric features .Some of these authentication systems require hardware devices, and this increases the cost. Users also have their accounts at many web sites, and they have to remember passwords of all these sites. To make the access easier, many websites support the concept of federated identity management, in which the user having a single account can log on to the other websites by authenticating themselves to a single identity provider. Android smart phones are getting more popular. In this paper, a system is proposed for secured authentication using Challenge Response, Quick Response Code, the identity provider and mobile phone, the most commonly used device. A Quick Response code is a two dimensional matrix code. It can store large amount of encrypted data, and it also has error correction ability.

2. Yung-Wei Kao, Guo-Heng Luo, Hsien-Tang Lin;Yu-Kai Huang, Shyan-Ming Yuan,"Physical Access Control Based on QR Code"

This paper is also an authentication system based One Time Password technique(OTP) and using QR code. The design consists of one server which stores the user information, mobile application that receives the mms and regenerates the QR code, and this QR code is shown to the client PC having camera for getting authenticated. The QR code contains the one time password that is send by the server.

3. Mukhopadhyay S., Argles, D.,"An Anti-Phishing mechanism for single sign-on based on QR-code"

This paper presented that, today internet users use a single identity to access multiple services. With single sign-on (SSO), users don't have to remember separate username password for each service provider, which helps the user to browse through the web seamlessly. SSO is however susceptible to phishing attacks. This paper describes a new anti-phishing SSO model based on mobile QR code. Apart from preventing phishing attacks this new model is also safe against man in the middle and reply attacks. Internet is becoming more and more user centric each day. With the advent of web 2.0 internet users are becoming more inclined to use services from multiple content and service providers (CSP or SP). Most SPs provide user registration service whereby a user can create his/her own account and maintain it. As such a user has to maintain separate user accounts (username and password) for each of the SPs he/she uses. A study shows that today a typical user needs to maintain about twenty five different accounts which require password and uses eight of them in a given day. Not only is this approach annoying to the user, it also raises some serious security questions, e.g. password fatigue.

4. Pei-Yu Lin , Yi-Hui Chen , Eric Jui-Lin Lu and Ping-Jung Chen,"SecretHiding Mechanism Using QR Barcode"

We propose QR code is the commonly used two-dimensional (2D) barcode recently with the advantages of larger QR content and error correction capability.

Based on the error correction property of QR code, we designed a secret hiding technique for QR barcode. The proposed scheme can conceal the secret data into the cover QR code without distorting the readability of QR content. That is, general browsers can read the QR content from the marked QR code for the sake of reducing attention. Only the authorized receiver can encrypt and retrieve the secret from the marked QR code. The secret payload of the designed scheme is adjustable. The scheme can convey larger secret into a QR code according to the selection of the QR version and the error correction level. The simulations demonstrate that the designed scheme is efficient and low computational complexity. The mechanism can be applied to the QR reader and mobile phone.

5. H. C. Huang, F. C. Chang and W. C. Fang,"Reversible data hiding with histogram-based difference expansion for QR Code applications"

In this paper, we propose a new algorithm in reversible data hiding, with the application associated with the quick response (QR) codes. QR codes are random patterns, which can be commonly observed on the corner of posters or webpages. The goal of QR codes aims at convenience oriented Applications for mobile phone users. People can use the mobile phone cameras to capture QR code at the corner of web page, and then the hyperlink corresponding to the QR code can be accessed instantly. Since QR code looks like random noise and it occupies a corner of the original image, its existence can greatly reduce the value of the original content. Thus, how to retain the value of original image, while keeping the capability for the instant access for webpages, would be the major concern of this paper. With the aid of our reversible data hiding technique, the QR codes can be hidden into the original image, and

considerable increase in embedding capacity can be expected. Next, we propose a scheme such that when the image containing the QR code is browsed, the hyperlink corresponding to the QR code is accessed first. Then, the QR code could get vanished and the original image would be recovered to retain the information conveyed therein. Simulation results demonstrate the applicability of the proposed algorithm.

CONCLUSION

Security has become extremely important in the digital Market. Authentication methods should be seriously considered by services that store confidential information. Most of the users have android smart phones. These Smart phones have good processing power and memory size. As a mobile phone has become an indispensable accessory and carry-on device in real life, compared with the traditional key or access card, sending the authentication image by using mobile phones through MMS(Multimedia Messaging Service) allows the user to carry fewer objects and no extra specific hardware cost needed. So some security features can be deployed on them in order to identify a user to the service provider. Using QR Code successful authentication can be done. The use of QR code image for authentication makes it difficult to be accessed.

REFERENCES

[1] Ms. Dhanashree Patil; Mrs. Shanti. K. Guru "Secured Authentication using Challenge - Response and Quick-Response Code for Android Mobiles ISBNNo.978-1-4799-3834-6/14, ICICES2014

[2] Yung-Wei Kao, Guo-Heng Luo; Hsien-Tang Lin;Yu-Kai Huang, Shyan-Ming Yuan, "Physical Access Control Based on QR Code," Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), vol., no., pp.285,288,10- 12Oct. 2011

[3] Mukhopadhyay S., Argles, D., "An Anti-Phishing mechanism for single signon Based on QR-code," Information Society (i-Society), vol., no., pp.505,508, 27-29 June 2011 IEEE

[4] H. C. Huang, F. C. Chang and W. C. Fang, "Reversible data hiding withhistogram-based difference expansion for QR Code applications," IEEE Transactions on Consumer Electronics, vol.,57, no. 2, pp. 779-787, 2011

[5] Jaideep Murkute, Hemant Nagpure, Harshal Kute, Neha Mohadikar, Chaitali Devade "Online Banking Authentication System Using QR-code and Mobile OTP" Vol. 3, Issue 2, March -April 2013, pp.1810-1815 IJERA.