ISSN: 2321-7782 (Online)
Volume 3, Issue 2, February 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

A Mobile Based Authentication Scheme Using QR Code for Bank Security

Vaibhav Kale[1]
Computer Science
SCSCOE, Dhangwadi, Bhor,
Pune, India

Yogesh Nakat[2]
Computer Science
SCSCOE, Dhangwadi, Bhor,
Pune, India

Sameer Bhosale[3]
Computer Science
SCSCOE, Dhangwadi, Bhor,
Pune, India

Abhijeet Bandal[4]
Computer Science
SCSCOE, Dhangwadi, Bhor,
Pune, India

Ramesh G.Patole[5]
Asst. Professor
Computer Department
SCSCOE, Dhangwadi, Bhor,
Pune, India

Abstract: ***Now day's users use a single identity to access a multiple services.By using single sign on (SSO), most of users don't have to remember separate username and password for each service provider and attacker can easily collect the information from various ways like web phishing and computer infection, since using the pair of username and password authentication scheme is no more secure,since the development of information and technology protecting the personal information from infected computers has become difficult task to be achieved.Therefore, secure authentication scheme is required.since we propose a anti phishing single sign-on(SSO) authentication model using QR code.This model is secure against attack and even on the distrusted computer environment.Based on this we designed a secret hiding technique for QR code. Only the authorized users can encrypt and retrieve the secret data from marked QR code .The mechanism can be applied to the QR reader and mobile phone.***

Keywords: single sign-on; phishing; onetime password; QR code, Mobile authentication, Two factor authentication, data hiding error correction capability.

I. INTRODUCTION

Now days, users can access the Internet and get the data globally spread on the websites. Upon receiving a request for information, the server requests the user ID and password to prove whether the user is valid or not for authentication. However, there are several malicious links that could possibly make the authentication scheme possibility of being attacked or harmed. One of those is a web phishing, in which an attacker tries to acquire sensitive and important information such as usernames, passwords, and personal information such as credit card number or registration number so on. Specially, web phishing is worldwide used through the SocialNetworking Service (SNS), Such as Facebook, Gmail and twitter accounts. A user those who accessed the fake website could type in the ID/password or sensitive information on the fake website which may lead to identity theft. In our paper, we discuss web phishing problem on the single sign-on (SSO) authentication, propose an authentication scheme secure against the phishing attack and distrusted local computer environment. To avoid this malicious attack we use QR–code authentication scheme. QR code (quick response code) is a type of two dimensional barcode developed by Denso-Wave company in 1994. QR code can convey larger content, such as the text, web link, and phone number. Moreover, the error correction capability can restore the QR content if the QR code suffered from damaged. QR code becomes popular and provides widely business applications via the QR readers and mobile devices. The QR content, however, can be easily decoded by a QR

reader. To communicate a QR code with the secret content, the security of QR content raises an important issue. The sender *usually* stores the secret in a back-end database. Browsers can read the web link from the QR code and then connect to the website of the database. Only the authorized user with password can login and retrieve the secret. However, such manner requests that the QR reader needs to be online and exposes the risk of the database. Recently, many researchers have proposed barcode.

II. DEFINITIONS

QR (Quick Response) code is a two-dimensional matrix barcode introduced by the Japanese company Denso-Wave in 1994.QR code invented for tracing the products and storing the massive product data also used for storing username, password and some sensitive information of person like credit card no. This QR code now widely used in a variety of industries, including advertisement business cards, and sales wrapping. Figure 1 shows the QR code structure. Each QR code symbol consists of an encoding region and function patterns.

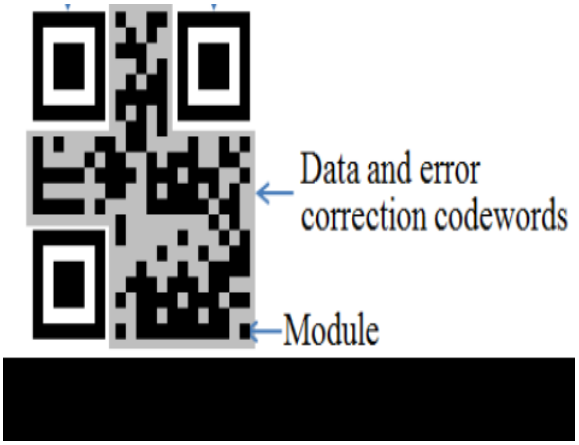

Figure 1: QR Code Structure

III. BACKGROUND AND RELATED WORK

A. *Communication channels:*

Different communication channels between mobile devices and computers.

1. Input Device:- Various Input devices like keyboard ,mouse, keypad
2. Bluetooth:-Open wireless technology for short Distance communication requires a Bluetooth adapter connection.
3. Infrared Signals:- Short distance sending signals using Electromagnetic radiation wavelength.
4. Wireless Internet [Wi-Fi]:- Middle distance data is sending method. Requires AP device for communication.
5. Near Field Communication: - Very short range communication requiresan expensivereadable device. Used in smart card.
6. Sound: - Transferred by speak or through themicrophone. Weak discordance for external noise and low rate correction depending on the voice distinguish algorithm
7. Optical method:-Short distance message sending method. Transferred the data through the character or special format. QR code is one of them.

Here, we use the optical communication method for transfer a huge amount of data with high quality recognition. QR code has three merits compared to other communication methods. First, QR code does not require the network connection. Mobile device can read the data through the mobile camera irrespectively about network communication risk. Second, QR code can hold a considerably great volume of information: 7,089 characters for numeric, 4,296 characters for alphanumeric data, 2,953

bytes of binary (8bits) and 1,817 characters of Japanese Kanji/Kana symbols. In addition, QR code has error correction capability. Data can be restored even when substantial parts of the code are distorted or damaged. Third, users can read the QR code quickly with high recognition rate regardless of the direction or way.

B. Authentication Method:

Different Authentication Methods

1. Something You Know:-ID/Password, PIN, Combination of the characters or numbers. Check the users' identities through the remembered codes only.
2. Something You Have:-One time password [OTP], Smart Card, USB or hardware Tokens. Hardware or software tokens generate the password or secret information. This information is used for the authentication process during the limited time.
3. Two-Factor Authentication: - A combination of two types of authentication methods We use the mobile device for two-factor method" Something You Know" and "Something You Have" In our proposed scheme, we use mobile device for authentication, since mobile devices are the IT necessaries in the modem times.

C. Mobile Device Information:

1. Various types of mobile information: -This data is called "shared data" in the proposed scheme.
2. Embedded On Device:-These data is different from each device, and managed by product company or platform supporter. Managing the data or key is easy through the tracing the mobile device.
3. Communication Information: - This data is different depending on the registration information and managed by Telecommunication Company.
4. Authentication Information:-Secure Mobile Memory Card This data is different depending on the mobile memory card provided by trust company and, managed by authentication.

IV. ALGORITHM

ASE (acronym of advanced Encryption Standard) is a symmetric encryption algorithm.The algorithm was developed by two Belgian cryptographers Joan Daemon and Vincent Rijmen.AES was designed to be efficient in both hardware and software, and supports a block length of 128 bits and key lengths of 128,192, and 256 bits.

Steps in the AES Algorithm:-

The encryption process uses a set of specially derived keys called round keys. These are applied, along with other operations, on an array of data that holds exactly one block of data? The data to be encrypted. This array we call the state array.

You take the following steps to encrypt a 128-bit block:

1. Derive the set of round keys from the cipher key.
2. Initialize the state array with the block data (plaintext).
3. Add the initial round key to the starting state array.
4. Perform nine rounds of state manipulation.
5. Perform the tenth and final round of state manipulation.
6. Copy the final state array out as the encrypted data (cipher text).

V. PROPOSED WORK

To resolve the weaknesses of OpenID, we design an architecture providing SSO authentication with two factor mechanism.The proposed architecture solves the problems previously underlined with QR code.Our scheme consists of three phases: login request phase, QR code generation phase, and verification phase.The notations used in our scheme as:

1. SessionID :A session identifier
2. OpenID: User identifier
3. Serverinfo: Server information Server IP, name, identifier
4. Secret Key: Sharing secret key
5. random nonce:Random key [generated by server]
6. User Rand: Random key [generated by mobile]
7. Password: OpenID's password
8. Shared Data: Mobile information
9. TimeStamp: A sequence of characters

Proposed System Architecture:-

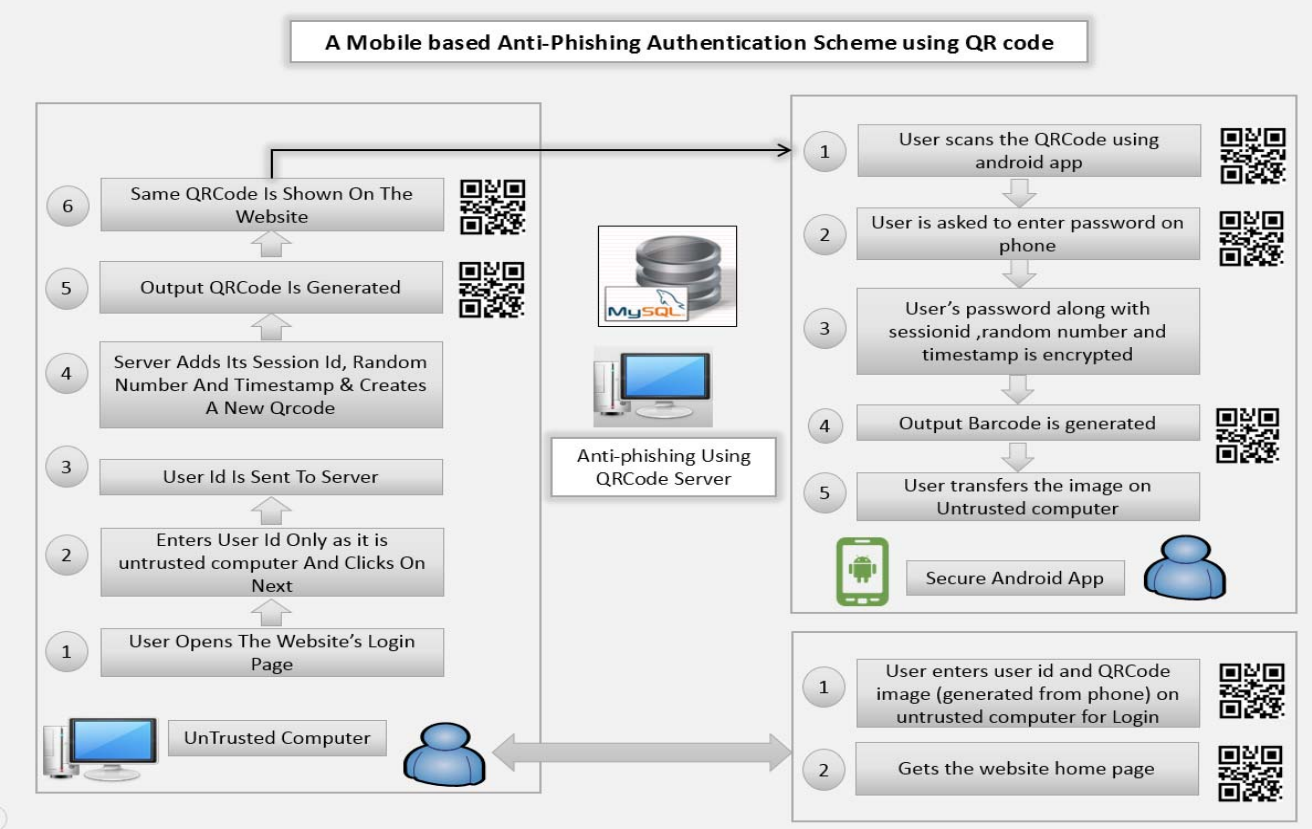

Figure 2:System Architecture

A. Request From Untrusted Computer

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

B. Web server Verification Phase1

3. Web server redirects user to extended authentication with SessionID, User Id and ServerInfo.

4. The web server verifies the Server Info. If verification fails, then the request is assumed to be invalid and session aborts.

C. *Information Exchange Phase*

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

D. Loginfrom Untrusted PC- Web server Verification Phase2

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

VI. ADVANTAGES

1. Most secure app for data communication.
2. Provides anti phishing feature to all users.

References

1. Shoji Sakurai, Shinobu Ushirozawa, "Input Method against Trojan Horse and Replay Attack "Information Theory and Information Security(ICmS), pp.3S4-3S9, Jan 2010.
2. Ken Birman. "In Computers We Trust" Distributed Systems Online, Dec200S.
3. MicroSoft Security Intelligence Report http://www.microsoft.comlsecurity/sir/keyfindings/default.aspx
4. J.Hursti, "Single Sign-On", in Proceeding of Helsinke Univ of Technology, Seminar on Netwokr Security, 1997.
5. Aloul.F, Zahidi.S, EI-Hajj.W "Two factor authentication using mobile phones" Computer Systems and Applications(AICCSA 2009), pp. 641-644, May 2010
6. A. Vapen, D. Byers, and N. Shahmehri, "2-C1ick Auth – optical challenge-response authentication," in Proc. Conference on Availability, Reliability and Security (ARES), 2010.
7. Yue Liu, Ju Yang, Mingjun Liu "Recognition of QR Code with mobile phones" Control and Decision Conference, pp.203-206, May 200S
8. Denso Wave Inc, "QR Code. Com" http://www.denso-wave.comlqrcodelindex-e.htrnl
9. OpenlD, "OpenlD Authentication 2.0," December 5, 2007.
10. A. Nanda and M. B. Jones, "Identity Selector Interoperability Profile,"July 2008.

