스마트폰을 이용한 Challenge-Response 인증

논 싸이라난[*], 요브네 탄 잉 후이[*], 김태용[**], 이훈재[○]
[*]말레이시아 멀티미디어 대학(MMU)
[○**]동서대학교 정보통신공학전공
e-mail: {thiranant.non@gmail.com;yvonne_lvl90@hotmail.com}[*], {tykimw2k, hjlee@dongseo.ac.kr}[○**]

Challenge-Response Authentication with a Smartphone

Non Thiranant[*], Yvonne Tan Ying Hui[*], TaeYong Kim[**], HoonJae Lee[○]
[*]Multimedia University, Malaysia(MMU)
[○**]Dongseo University, Dept. Information & Comm. Eng.

● Abstract ●

This paper proposes an one-time authentication system for web applications by making use of the quick-response code, which is widely used nowadays. The process is not time-consuming. It does not require any browser extensions or specific hardware to complete a task. The system uses QR code which is basically a two-dimensional black and white image encoding a piece of digital information. When a user logs into a site, the web server will generate a challenge encoded to form a QR code. The user captures a picture of QR code with a mobile camera which results in decoding the QR code. The challenge shall be sent back to the server; the web server then logs the PC browser in. The authentication using Challenge-Response is easy to understand and the process is fast. The system proposes the improvement of usability and security of online authentication.

키워드: authentication, chellenge-response, QR code

I. Introduction

Today, passwords are an important aspect of the computer security. They are widely known and used everywhere. However, single factor authentication is no longer secure nowadays; a poorly chosen password may result in being exploited. Nowadays even a strong password may not be enough to make sure that the users are safe from threats and the system is secure. Not that the password system is unsafe; on the contrary, there are many risks associated with the use of passwords. With many threats presently and the value placed on the information, systems that rely on passwords for security seem to be vulnerable; hence they can easily be exploited. The strong authentication is needed in order to ensure both the service providers and consumers are free from threats. The proposed system introduces a technique that provides a convenient challenge-response system for logging into websites. There are no other requirements, but a mobile with a camera. Users do not have to memorize passwords and the login process is fast.

II. Related Works

1. Web Authentication

As a number of people relying on internet to do business is increasing, the authentication system should also be improved. The internet has become a great environment for e-commerce, e-banking, e-services, etc. Security for these applications which that has highly secretive and confidential information is of great concern. This, an effective method is used to authenticate the identity of users. Accessing web-based services do require typing a username and password to authenticate. This is a significant vulnerability since it may anytime fall into wrong hands. The proposed online system requires a username with no password, but a capture of QR code. The web server verifies the existence of a username and generates a cryptographic challenge. No more passwords are required to log into the website. The web server will verify, once a user sends a capture of QR code. The registered mobile number shall be used as a keyword to retrieve the information from database.

2. Fast Authentication process

The authentication process applies the same concept as one-time password, that is something you know and something you have. A mobile is always switched on and is usually carried with us to everywhere. It can be considered to be a personal device that is not usually shared among other people, except in rare circumstances. Indeed, the personal and private information are stored, and they are to be kept secret. Since each mobile is unique, it is a very suitable device to be used as a factor for authentication. With internet browsers on PC, users can access the web server from anywhere and anytime. Browsers are not considered personal as mobiles. We always work on different PCs, different places. In addition, a user may share a PC with others.

With this challenge-response authentication that we are to propose, the system relies on the web server, a mobile device, and the mobile application that serves users as a connection between web server and a mobile. A mobile device with Wi-Fi can connect to the internet via wireless network access point, hence users can access the web server from anywhere. This technology has great impact on the system. It is said to be the main technology used for the fast authentication process, using a mobile device. Not only the Wi-Fi technology, but the 3G mobile system would work well. The use of both the mobile device and computer also provides a security benefit, as it protects against man-in-the middle attacks, and works as a secondary authentication that differs from the usual login system.

The user's experience using the challenges-response system is as follows. The user navigates a browser to the login page of the website, entering the username. The login page displays a QR code[1-2] to the user. The user captures the picture of the QR code with a mobile camera. The response after decoding is then re-encoded with extract user's device phone number and transmitted back to the site. The website will verify and redirect the user to the complete login process page. Two platforms can enhance the internet security and correctness. There are no specific hardware or browser extensions needed. Plus, capturing a QR code is fast, accurate and less error prone.

III. Challenge-Response Authentication with smartphone

1. Technologies involved in the system

Proposed system is simple, easy to implement in software, and is highly secured. The process basically make use of the existing QR Code technology, a website and a mobile communication device as a personal identifier. QR Code is a barcode technology that falls under the category of 2D barcodes. It was first invented by the company Denso wave and is now widely used commercially especially in Korea and Japan. The QR code is much more appealing compare to the traditional barcode is how it can stores information on both the vertical and horizontal directions, thus holding up to several hundred times more data than a traditional barcode [3-4].

The website can be done in a simple way, with not many complexities. Few necessary things are QR code generator and a database. Any web-based programming technology can be used to implement. A database is needed on the server side to store user's identification information such as the username, password and mobile number. The password field is used to store the temporary generated one-time password (OTP)[4].

Whereas more efforts should be put into a mobile application, that can deal with QR code, extract phone number from user's device, re-encode the data into challenge-response and be able to transmit to the web server. The correctness of the mobile application should be concerned. The mobile number should be encoded together with the original challenge to form a challenge-response and sent back to the website. For a database system, it is to be done with the website. The proposed system is computationally light, low processing power and possesses high efficiency. It does not always need to be updated, except for users’ information in the database.

2. Designing the system against threats

The authentication system is designed in the simple way, while it possesses strong security. The concept is basically deriving from one-time passwords, but the system can ensure users’ safety due to the uniqueness of their mobile devices. The system is designed in order to protect against these types of threats:

- Phishers cannot exploit a breach in the system since there is no use setting up a spoof of a website, since a QR code should be decoded and the mobile number is used as a key to authenticate users. Each mobile device is unique, it is almost impossible to find a device that can send a mobile number to the server, and acts in the same way as mobile devices. This thus eliminates man-in-the-middle or spoofer attacks.
- In case of the situation where the mobile device is theft,

quick revocation would be enabled. The particular mobile number will be deactivated and removed from database.

- Eliminates weak passwords who are vulnerable to dictionary attack (brute-force) and can be easily phished through a spoofed website. Thus, protect users who uses simple passwords or the same passwords at many different sites.

3. System work flow

Figure 1 shows the overall process flow of this QR Code Challenge-Response Authentication System. Before using the system, the user must first register themselves and create an account and key in the personal information such as, username, password and mobile number as identification factors in the database. When user is signing in, only username is required. The website will generate a piece of random challenge, that is unique per session, and encode it in a QR Code image to be used in the symmetric challenge-response authentication. The user then lunches the application and scan the QR code using the phone camera. The application then captures the challenge image and extract the challenge within. After that, phone number will be extracted and encoded together with the string of original challenge to form a challenge-response which will be sent back to the website via Wi-Fi connectivity. Verification process will be done on the website to check if the challenge matches the original one, and if the extracted phone number matches with the one in the database. If one of this fails the verification, user's access will be denied. If both passes the verification successfully, user's access to login will be granted.

Figure 2 shows QR code on login page, unique per session, encodes a random challenge to be used in the symmetric challenge-response authentication. And then Launches Authentication and Payment Web Application. Using phone camera, application captures challenge QR code and extracts challenge within. And then Application finds a shared secret key and response endpoint that match the provider name and desired user account. Figure 3 shows the evaluated results in android smartphone.

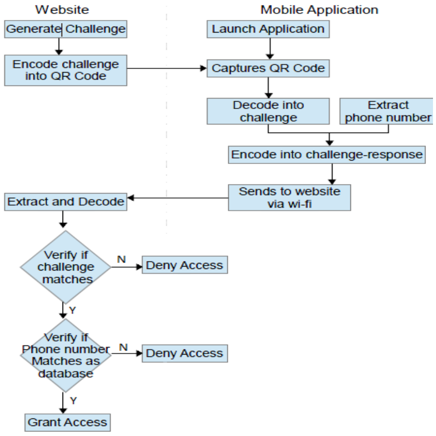

Fig. 1. System Flow Chart

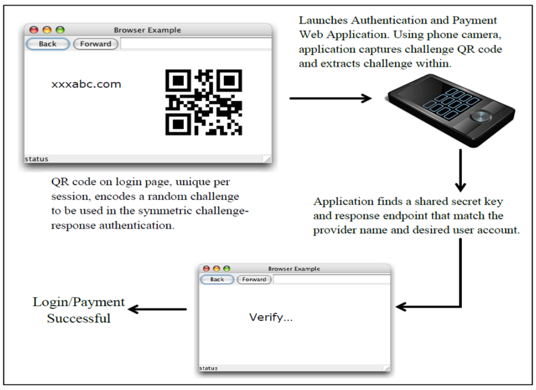
Browser Example
Back
Forward
xxxabc.com
status
Launches Authentication and Payment Web Application. Using phone camera, application captures challenge QR code and extracts challenge within.
QR code on login page, unique per session, encodes a random challenge to be used in the symmetric challenge-response authentication.
Application finds a shared secret key and response endpoint that match the provider name and desired user account.
Login/Payment Successful
Verify...

Fig. 2. System operation

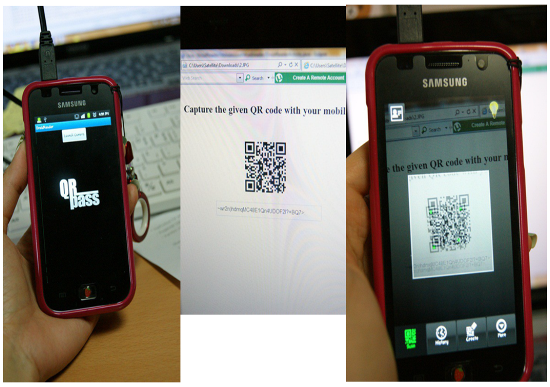
SAMSUNG
QRpass
Capture the given QR code with your mobil
the given QR code with your

Fig. 3. Test Result

IV. Conclusion

In this paper, we proposed an implementation of a simple two-factor authentication system which utilize the popularity usage of QR Codes nowadays and a smartphone device for a secure login or payment transaction. With the system proposed, the vulnerability of the traditional single factor authentication, for example: password, can be easily overcome. Users no longer need to memorize their passwords, typical, weak passwords that can be easily spoofed or exploited can be also avoided. The idea of this system is that, by leveraging the mobile device as a personal identifier, compared to PC, brings many advantages in improving the security of log in process in terms of the mobility, efficiency and flexibility of the proposed system.

References

[1] P. Kieseberg, M. Leithner, M. Mulazzani, L.Munroe, S. Schrittwieser, M. Sinha, E. Wieppl, "QR Code Security", In TwUC'10, 8-10 November, 2010, Paris,France.

[2] W. Liang, W. Wang, "On Performance Analysis of Challenge/Response based Authentication in Wireless Network," In Center for Advanced Computing and Communication (CACC) 03-06 and 04-08.

[3] F. Aloul, S. Zahidi, W. El-Hajj, "Two Factor Authentication Using Mobile Phones," Available at http://www.aloul.net/Papers/faloul_aiccsa09.pdf

[4] Y.S.Lee, "Online banking authentication system using mobile-OTP with QR-Code," Available in Proceeding of ICCIT'2010, 5th Internation Conference, pp. 644-648, 2010.