An effective Two Factor Authentication Method using QR code

Soonduck Yoo[1] *, Seung-jung Shin[1], Dae-hyun Ryu[1],

[1] Dept. of IT, University of Hansei, Korea, 604-5 Dangjung-dong Gunpo city Gyeonggi do Korea,
harry-66@hanmail.net, expersin@hansei.ac.kr, dhryu@hansei.ac.kr

Abstract. The most prevalent form of login has used an ID and password which is classified 1 factor authentication. However the lax of security, user required the more secure way to login so firms have implemented 2 factor authentication involving OTP(One time Password). Despite the increased security, users must endure the inconvenience of downloading a program on their device and inputting a 6 to 8 digit code. In this study we explore leading 2 factor authentication programs that combines both security and convenience using QRcode. By scanning QRcode with smart phone users can login to the website without to put a 6 to 8 digit code such as OTP. Users can enjoy the both security and convenience. We encourage further research into technological development within internet security systems because of the significant role security systems play in the growth of online markets

Keywords: Authentication, Account Control, Hacking, Telecommunication, Security.

1 Introduction

As information technologies develop, people put their information into online more and more therefore cyber-security is the most common concerning things nowadays. Our research is motivated from authentication to keep the security on website. Generally 1 factor authentication involving user's ID and password are used last 10 years. For security reason, 2 factor authentication with OTP(one time password) is commonly used with smartphone on recent technological advances in telecommunications. OTP way has an hassle to use by entering a 6 to 8 digit code for authentication. All of these concerning security threats provide the motivation for our research in advances to cyber-security. In this study, we explore the way allows users authenticate themselves by scanning a QR code on the website with their smart phone.

1.1 Two factor authentication

The issue with one factor authentication is the static nature of the security system. In the creation of an ID, there are 2 choices: the user may design his own or use an email address. However, the static one factor authentication exposes the personal information of users to sophisticated hackers. Today, dynamic security systems are necessary to counteract the memory hacking, key logging and network sniffing of hackers. To complement the 1 factor authentication, security systems developed 2 factor authentication. The original fixed ID and password form the 1 factor authentication remained, but a 2 factor authentication was layered on top. This additional layer requires a generated code from a peripheral device (ex. smart phones, tokens, etc.) for each log in.

1.2 Two factor authentication

There are three commonly classified levels of verification to explain 2 factor authentications. The first and most common is a ID and password. The second level requires additional verification, such as a personal item (mobile phone, token, security card and etc.). The final level demands the use of the user's biological information, such as a finger print, face recognition and etc. Two factor authentication systems combine two of the three levels of verification. One typical example of two factor authentication is a combination of the first level, ID and password, and the second, an OTP (One Time Password) [2]. We explored OTP(One Time Password) in details.

1.3 OTP service

Security systems developed 2 factor authentications to solve the problem of hacking, which the one factor authentication system was so susceptible to. The typical applied example of 2 factor authentication is the OTP system. According to the development IT, OTP is the one of most strong one to provide the security of websites and minimizes the potential of unauthorized access. To login user are required one time password which is normally provided on the smartphone involving put user ID and password. The OTP algorithm creates a 6~8 digits (1,000,000 ~ 100,000,000) number to authorize each login. Although the OTP provides strong security, the system is complicated and not easy to use. Even as a 2 factor authentication system, the OTP algorithm may be exposed to hacking, especially if users lose their OTP generating unit

2 New method to login using QRcode and smart phone

With the advent of smart phones, the accessibility of advanced authentication systems have increased and the need for such authentication has grown as well. In this study,

we will discuss QR(Quick Response) code about how this can be used to login instead of OTP in solving OTP problems, which can be easily exposed key logger hackings. The traditional barcode contains information in only one direction, but the QR(Quick Response) Code (Quick Response Code) contains the two-way information (horizontal and vertical), allowing for increased security. This is used many ways in the market involving smartphone scanning method.

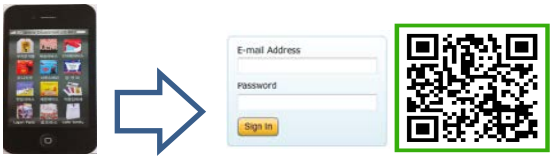

Fig 1 Login process

In our study, user put their ID and password and then scan the qrcode on the web site at the same time then the programs on the smartphone is activated and user click the approval button on their phone then the login is allowed automatically. In this case even if the hacker steals the login information by key logger program, they cannot login the website without approval from the user's smartphone. Instead of using user's ID and password with involving OTP, this system replace qrcode instead of OTP to login the website in a secure way. The purpose of this way is to solve the key logger hacking problems on the site. However we need more work to explore how to apply this way to the system in detail. We encourage further research into technological development within internet security systems because of the significant role security systems play in the growth of online markets

3 Conclusion

As information technologies such as smart phones develop, the threat of hacking grows in conjunction. To use the qrcode to login website were discussed and user put their ID and password on the site by scanning the qrcode with involving approval on their smartphone then the website allow to login automatically. This is able to solve the key logger problems and provide the strong security on line system. However we would to like to leave the way how to apply this system in detail for the future work. Our system provides easy of use as well as strong security. Even though this method requires a smart phone, the market applications for the system are immense.

References

1. Soodong Park, "Mobile Authentication System and It's Application based on 2-Dimensional Barcode and OTP". Hanyang University in Korea(2009)
2. Sang-ill Cho, "Stream Cipher-based OTP Authentication Protocols using Clock-Counter". Dongseo University in Korea(2010)

3. Kim, Yeon-soo, “Memory hacking Countermeasures Utilized OTP for Secure E-banking Transaction”. Soonsil University in Korea(2008)
4. Soonduck Yoo, Jung-Ihl Kim, “Open markets and FDS(Fraud Detection System)”. The Institute of webcasting internet and telecommunication, Vol.11 No 5 pp 113~130(2011)
5. Jang Jung ho, “A study on Security Management of Payment System in Internet commerce”. Konkuk University in Korea(2007)