Advanced Science and Technology Letters
Vol.109 (Security, Reliability and Safety 2015), pp.28-32
http://dx.doi.org/10.14257/astl.2015.109.07

Design of Micro-payment to Strengthen Security by 2 Factor Authentication with Mobile & Wearable Devices

Byung-Rae Cha[1], Sang-Hun Lee[2], Soo-Bong Park[3], Gun-Ki Lee[4] Yoo-Kang Ji[5]

[1]School of Information & Communications, GIST.
123, Cheomdan Gwagi-ro, Buk-Gu, Gwangju, 500-712, Republic of KOREA
brcha@nm.gist.ac.kr
[2]Dept. of Electrical & Electronics Eng. DongKang College,
50, Dongmundaero, Buk-Gu, Gwangju, 500-714, Republic of KOREA
Sang8147@naver.com
[3]Dept. Of Information & Communication Eng. DongShin Univ.
185, Geonjae-ro, Naju City, Joennam 520-714, Republic of KOREA,
sbpark@dsu.ac.kr
[4]Dept. of Electronic Eng. Gyeongsang National University
900 Gajwa-Dong Jinju Gyeongnam 660-701, Republic of KOREA,
gklee@gnu.ac.kr
[5]School of Information & Communications, GIST.
123, Cheomdan Gwagi-ro, Buk-Gu, Gwangju, 500-712, Republic of KOREA
Corresponding Author : gistjyk@gist.ac.kr

Abstract. As increasing services with mobile devices, authentication technology by mobile devices has diversified. Nowadays to cope with security threat of e-commerce high rick transactions need multi-factor authentication technology conjoined in one or more factors. This paper proposes 2-factor authentication technology for security enhancement in electrical micro-payment system.

Keywords: Micro-payment, NFC, Mobile, Wearable Device, 2 Factor Authentication.

1 Introduction

Development in smart phone and mobile communication brought new payment method. Recently newly rising are payment methods like mobile banking combined ICT technology, cash-coupon used in SNS, pin-tech and so on.

Behind this development various and intellectual hacking attacks for wrong purposes have occured.

The more complicated hacking tech becomes, the more difficult to react with simple authentication.

World widely e-banking attacks for monetary gain are on a rapid rising trend as follows; in third quater of 2013 malwares against e-commerce increased over a couple hundred thousand and grew by 38% over previous quater.

ISSN: 2287-1233 ASTL

In order to cope with complex security threat nowadays security card, OTP operator, mobile phone SMS authentication as well as ID/PW are used and China, Singapore, Europe adopted signiture deal technology actively using in high-risk transaction like large amount transfer.

Furthermore Singapore, Sweden, Norway, etc. are continuing to do research on integrated authentication service for managing complex user acceptance ways integrately and dealing with security threat efficiently.

Especially “Guidelines for e-banking authentication” of the Federal Financial Institutions Examination Council (FFIEC) and “Guidelines for risk management of e-commerce” of Monetary Authority of Singapore (MAS) recommend multi-factor authentication in high risk transactions.

Recently domestically many authentication ways are adopted like additional authentication sending authentication code to the mobile phone in large amount transfer and simple authentication only by fingerprint.

However in these various authentications the necessity of the standard for security and usability would be speculated by service providers and users.

This paper proposes 2-factor authentication technology by the user certification and smart watch on the purpose of security enhancement for electrical micropayments.

2 Related Researches

Authentication can be classified into three major base authentication technology which are possession, knowledge and property and other authentication factors.

Possession-based authentication is confirming transaction orders by text and numbers input using user devices like OTP, Smart card, Hardware security module(HSM) and so on.

Secondly knowledge-based is user memorizing ID/PW, PIN, etc, which is widely used as easy online authentication method.

Thirdly property-based is using bio-data like fingerprint, voice, iris, etc. Despite it’s high level of security, because of privacy problem it’s mainly used only as access control.

The other factors are electrical autograph, location information and so on.

The location information is the way offering services using GPS of smart phone only by the valid user location.

The following table1 shows the classification of authentication factors.

Table 1. Classification of authentication factors

	Combination	Example
Two Factor Authentication	Knowledge based + Property based	Password + OTP
	Knowledge based + Features based	Password + fingerprint
	Property based + Features based	OTP+ fingerprint
Three Factor Authentica-	Knowledge based + Property based + Features based	Password + OTP + fingerprint

tion		

Recently as mobile devices develop, high userbility authentication technologys using them are emerging.

Especially they include USIM, IC card, OTP, authentication certificates.

Also two channel authentication using additional authentication through registered cell phone in case of electrical fund transfer is the authentication by mobile devices.

As in the Fig.1 after the USER transfers knowledge-based or property-based authentication information to MOBILE DEVICE, each element autonomously or using security element creates new authentication information with additional possession based characteristic and authorizes user.

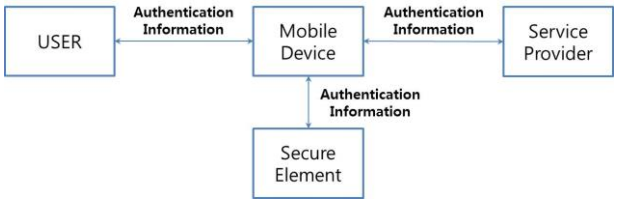

Fig. 1. Concept diagram of multi-factor authentication technique based on Mobile device

In order to do this multi factor authentication is required to meet the security requirements for object authentication framework in ITU-T X.1254.

Multi factor mechanism should offer two or more different shaped authentication factor for user authentication.

Multi factor authentication mechanism using mobile device (TTAK.KO-12.0221)' the standard made in 2013 categorizes into four and describes requred service model and protocol for the security of multi factor authentication technology by mobile device.

As the international standard ITU-T X.1158 in 2014 is set and includes various multi factor authentication mechanism used in not only domestic but also foreign e-commerce.

This standard presents detailed security requirements to a minimum necessary for the case of multi-channel and safe mobile device. Thus it can be used as the guideline by the service provider who want to introduce real services.

3 Design of Micro-payment to Strengthen Security by 2 Factor Authentication with Mobile & Wearable Devices

NFC-based electrical micro-payment system for revitalizating traditional markets corrects the shortcomings of POS in traditional markets and expands business area for retailers from cash to mobile transaction.

The figure 2 shows NFC based micro-payment process. Previously developed systems have problems like missing mobile devices. To solve them 2-factor authentication is proposed as shown in the fig.4.

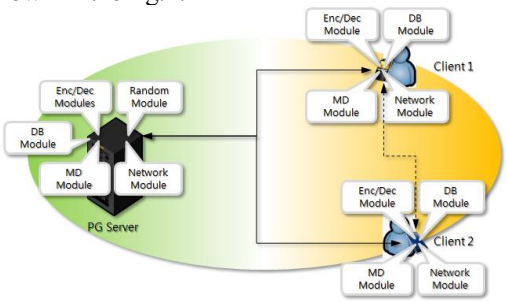

Fig. 2. NFC-based Micro-payment process by knowledge-based authentication

For the 2-factor authentication using the smart watch as wearable device which has secure elements the electrical micro-payment is made through the authentication of user and smart phone together. As shown in the fig.4 NFC-based micro-payment system can strengthen the security by double factor authentication.

Fig. 3. Mobile & wearable device-based 2 factor authentication technique

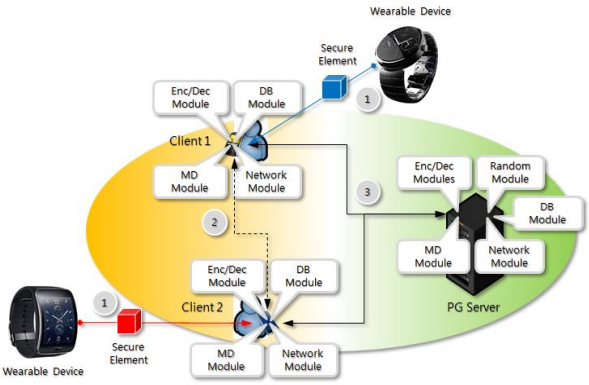

Fig. 4. NFC-based Micro-payment process by 2 factor authentication

The new business model establishment of existing NFC-based electrical micro-payment system by 2-factor authentication in the fig.4 and the designs of various payment types according to the absent of multi factor elements are needed.

4 Conclusions

As increasing the services using mobile devices, various authentication technologys are introduced (developed) and nowadays for coping with security threat of high risk transactions multi factor authentication technology combined one or more factors is recommended.

This paper for the purpose of security enhancement of micro-payment systems proposes 2-factor authentication technology with knowledge-based authentication by user and possession-based authentication by smart watch.

References

1. Smith, T.F., Waterman, M.S.: “Identification of Common Molecular Subsequences.” J. Mol. Biol. Vol.147, pp.195-197 (1981)
2. Christoforos Ntantogian, Stefanos Malliaros, Christos Xenakis.: “Gaithashing: A two-factor authentication scheme based on gait features.,” Journal of Computer & Security, vol.52, pp17-32 (2015)
3. Apple touch ID, http://support.apple.com/kb/HT5883
4. Argyropoulos S, Tzovaras D, Ioannidis D, Strintzis M. A.: “Channel coding approach for human authentication from gait sequences,” IEEE Trans Information Forensics Security Sept. (2009)
5. Yoo-Kang Ji, Byung-Rae Cha,: “Prototype design of NFC-based electronic coupon ecosystem with object memory model,” Contemporary Engineering Sciences, vol. 7, No. 22, 1105-1112, (2014)
6. Chun-Ta Li, Chi-Yao Weng and Chun-I Fan.: “Two-Factor user Authentication in Multi-Server Networks” International Journal of Security and Its Applications, Vol.6, No.2, pp.261-268, (2012)
7. Sultan Ullah, Zheng Xuefeng and Zhou Feng.: “TCLOUD:A Multi-Factor Access Control Framework for Cloud Computing”, International Journal of Security and Its Applications, Vol.7, No.2, pp.15-26, (2013)
8. Soonduck Yoo, Seung-jung Shin and dae-hyun Ryu.: “An Innovative Two Factor Authentication Method : The QRLogin System” International Journal of Security and Its Applications, Vol. 7, No.3 pp.293-302, (2013)

