International Journal of Security and Its Applications
Vol.9, No.8 (2015), pp.253-260
http://dx.doi.org/10.14257/ijsia.2015.9.8.22

Prototype Design of Mobile Micro-payment to Enhance Security by 2 Factor Authentication

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

[1,5] School of Information & Communications, GIST, KOREA
[2]Dept. of Electrical & Electronics Eng. DongKang College, KOREA
[3]Dept. of Information & Communication Eng. DongShin Univ. KOREA
[4]Dept. of Electronic Eng. Gyeongsang National University, KOREA
brcha@nm.gist.ac.kr, Sang8147@naver.com, sbpark@dsu.ac.kr, gklee@gnu.ac.kr, gistjyk@gist.ac.kr

Abstract

As there's increase in 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 [1, 5]. Behind this development various and intellectual hacking attacks for wrong purposes have occurred. The more complicated hacking tech becomes, the more difficult to react with simple authentication [2, 9].

World widely e-banking attacks for monetary gain are on a rapid rising trend as follows; in third quarter of 2013 malwares against e-commerce increased over a couple hundred thousand and grew by 38% over previous quarter [4, 9]. In order to cope with complex security threat nowadays security card, OTP opera-tor, mobile phone SMS authentication as well as ID/PW are used and China, Singapore, Europe adopted signature deal technology actively using in high-risk transactions like large amount transfer. Furthermore Singapore, Sweden, Norway, etc. are continuing to do research on integrated authentication service for managing complex user acceptance ways integrity 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 [6, 9].

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 [7-9].

This paper proposes 2-factor authentication technology by the user certification and smart watch on the purpose of security enhancement for electrical micro-payments [9].

ISSN: 1738-9976 IJSIA

2. Related Work

2.1. FinTech and FinTech Ecosystem

Financial technology, also known as FinTech, is a line of business based on using software to provide financial services. Financial technology companies are generally startups founded with the purpose of disrupting incumbent financial systems and corporations that rely less on software. Fintech companies, as they've come to be called, are easing payment processes, reducing fraud, saving user's money, promoting financial planning, and ultimately moving a giant industry forward. Here are 15 Fintech companies that made a mark over the past year and will be interesting to watch in 2015: BillGuard, Planwise, OnDeck, Wealthfront, Currency Cloud, Stripe, Epiphyte, AstroPay, Banking Up, Square, Tipalti, Flint, Check, Zipmark, and WePay [10-12].

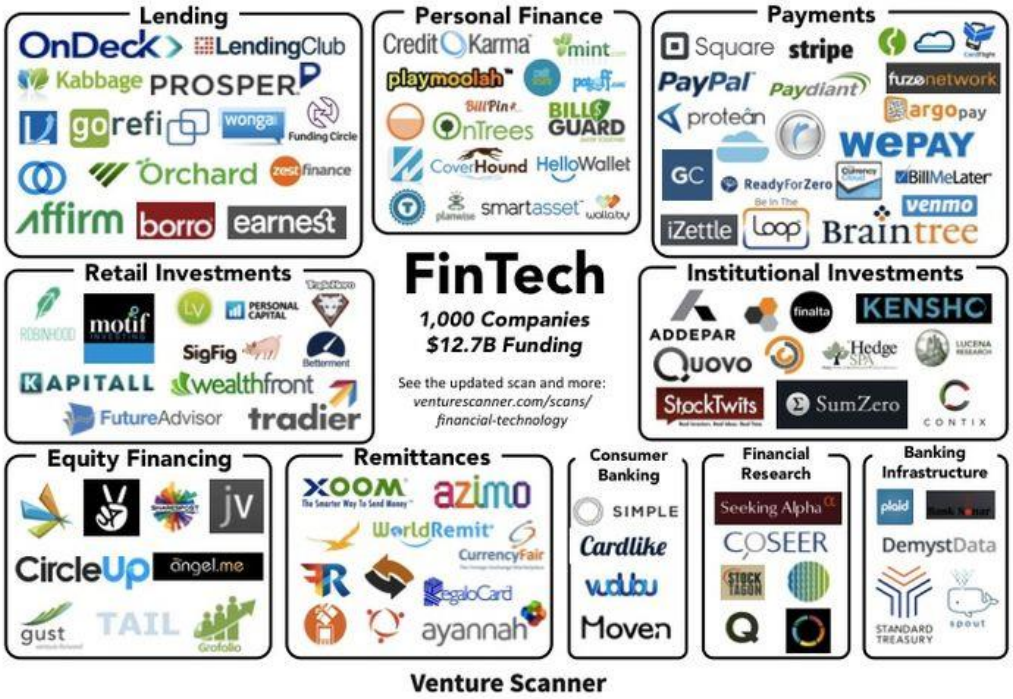

Figure 1. FinTech Landscape Overview (Venture Scanner, Oct. 2014)

Figure 1 focuses on the impact that FinTech is having on product innovation, traditional corporate development and brand loyalty. It covers a quick overview of the FinTech ecosystem, notable crowdfunding applications in the corporate world by public companies and what lies ahead for private brands as the regulatory environment changes for equity crowdfunding. FinTech has many segments including but not limited to Digital Wealth Management (aka Robo-Advisors), Crowdfunding (Rewards, Donations, Equity), Alternative Lending (P2P), Digital Currencies (aka Bitcoin) and Payments [10-11].

2.2. Authentication Factors

Authentication can be classified into three major base authentication technologies 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 its high level of security, because of privacy problem it's mainly used only as access control [6, 9].

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 Table 1 shows the classification of authentication factors [7, 9].

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 Authentication	Knowledge based + Property based + Features based	Password + OTP + fingerprint

Recently as mobile devices develop, high usability authentication technologies 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 [7, 9].

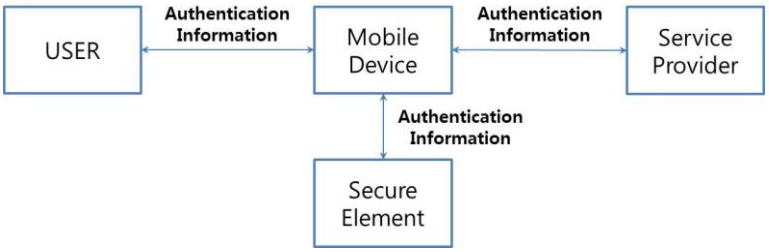

Figure 2. Concept Diagram of Multi-Factor Authentication Technique Based on Mobile Device

As in the Figure 2, 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. In order to do this multi-factor authentication is required to meet the security requirements for object authentication framework in ITU-T X.1254 [9].

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 required 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 providers who want to introduce real services [8-9].

3. Design of Micro-payment to Strengthen Security by 2 Factor Authentication

NFC-based electrical micro-payment system for revitalizing traditional markets corrects the shortcomings of POS in traditional markets and expands business area for retailers from cash to mobile transaction. The Figure 3 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 Figure 5 [9].

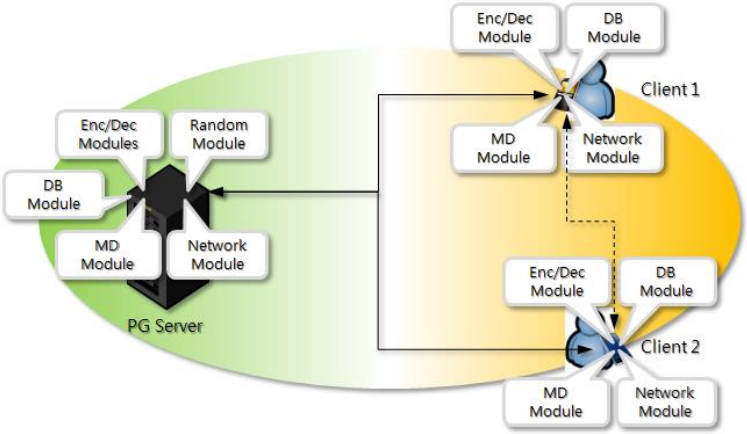

Figure 3. NFC-based Micro-Payment Process by Knowledge-Based Authentication

For the 2-factor authentication using the smart watch as a 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 Figure 5, NFC-based micro-payment system can strengthen the security by double factor authentication. The new business model establishment of existing NFC-based electrical micro-payment system by 2-factor authentication in the Figure 5 and the designs of various payment types according to the absence of multi factor elements are needed [9].

Figure 4. Mobile & Wearable Device-Based 2 Factor Authentication Technique

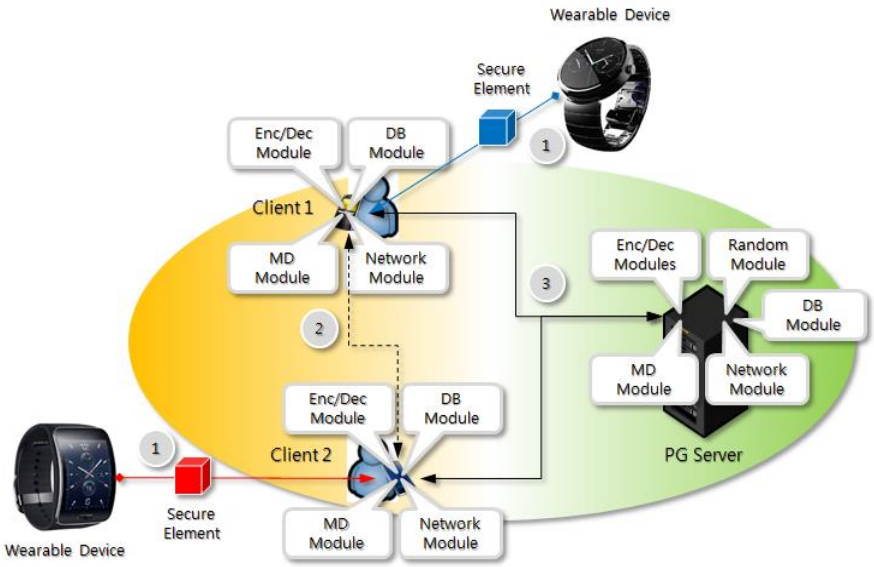

Figure 5. NFC-Based Micro-Payment Process by 2 Factor Authentication

4. Prototype Design of Micro-Payment Process by 2-factor Authentication

In this paper, we described the prototype design of mobile micro-payment process by 2-factor authentication to enhance the security strength, as compared with existing mobile micro-payment process. This section describes the differences between the proposed system and existing system in aspect of the components and payment processing of mobile micro-payment (Figure 3 and Figure 6 vs. Figure 5 and Figure 7).

4.1. Micro-Payment Process between Purchaser and Retailer

In this subsection, we describe the detailed payment process of existing mobile micro-payment system with NFC. Figure 6 illustrates the micro-payment process among retailers, purchasers, PG servers, and banks. Initially both a retailer and a purchaser authenticate with the PG server. Then, by using the public key of PG server via NFC, the retailer transfers the encrypted token of retailer to the purchaser. The purchaser sends the PG server the encrypted data, which are the retailer's token, purchaser's token, and purchaser's account. Next, the PG server converts the token with account information by referring the lookup DB. It also transfers to the bank the monetary transaction between the purchaser and the retailer. Lastly, bank returns the result of monetary transaction to the PG server, and the PG server sends the account information to both purchaser and retailer.

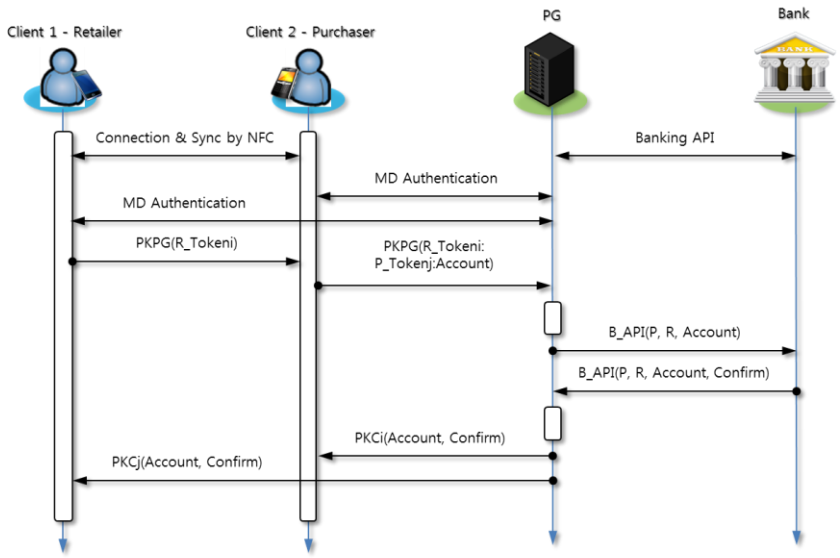

Figure 6. Payment Process of Existing Mobile Micro-Payment

4.2. Micro-Payment Process between a Purchaser and a Retailer with 2-factor Authentication

To compare with the existing mobile micro-payment system, we draw the proposed mobile micro-payment process with 2-factor authentication in Figure 7. Figure 7 illustrates the micro-payment process among retailers, purchasers, PG servers, banks, and wearable devices. Initially both retailer and purchaser with wearable devices authenticate with the PG server. Then, by using the public key of PG server via NFC, the retailer transfers the secure elements (encrypted tokens) of retailer to the purchaser. The purchaser sends the PG server, the encrypted data, which are the retailer's secure element, purchaser's secure element, and purchaser's account. At this point, 2-factor authentication between retailer and purchaser is completed. The remainder of payment process is conducted by the same process as shown in Figure 6.

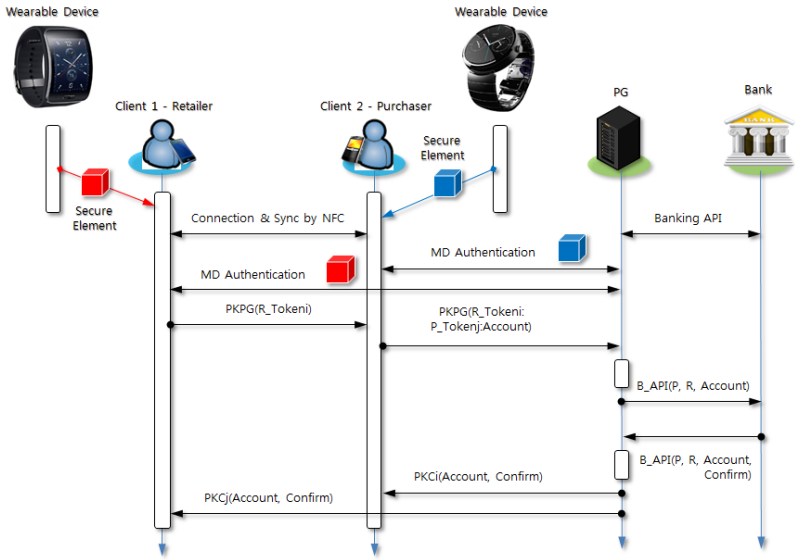

Figure 7. Payment Process of the Proposed Mobile Micro-Payment with 2-factor Authentication

4.3. Business Model for Compatibility

The trend of changes in traditional market is very slow and this trend is evident in the demand and supply of technology. It means that we need to consider the compatibility among the mobile devices of retailers and purchasers. To show you, we have derived the following business mode in Figure 8. That is, business model for compatibility in Fig. 8 was designed using combination between existing mobile payment in Figure 6 and the proposed mobile payment by 2-factor authentication in Figure 7.

Figure 8 presents the payment processing between retailer and purchaser with wearable devices. As shown in Figure 8, the retailer is a passive object and purchaser is an active subject in mobile payment process. The object that is willing to pay is the subject in payment processing. To have the wearable device indicates a willingness to pay. Specially, the purchaser with wearable device has a willingness to pay. This mean is that this payment process between a retailer without the wearable device and a purchaser with a wearable device shall prove legal.

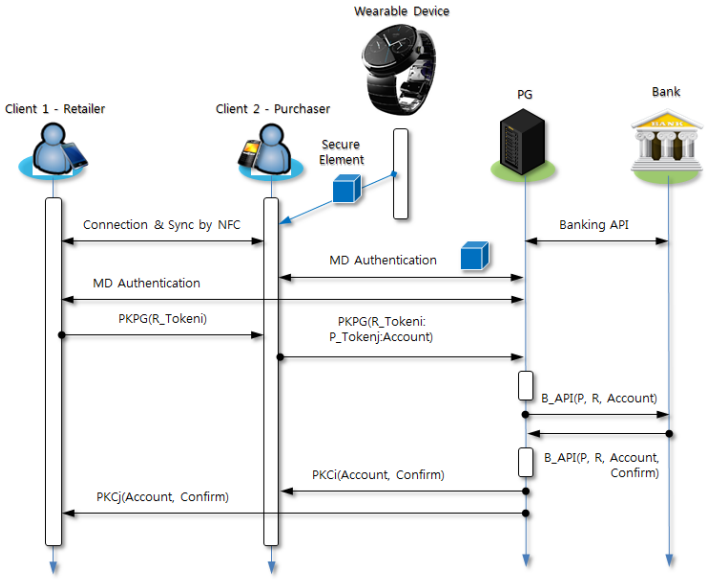

Figure 8. Business Model for Compatibility

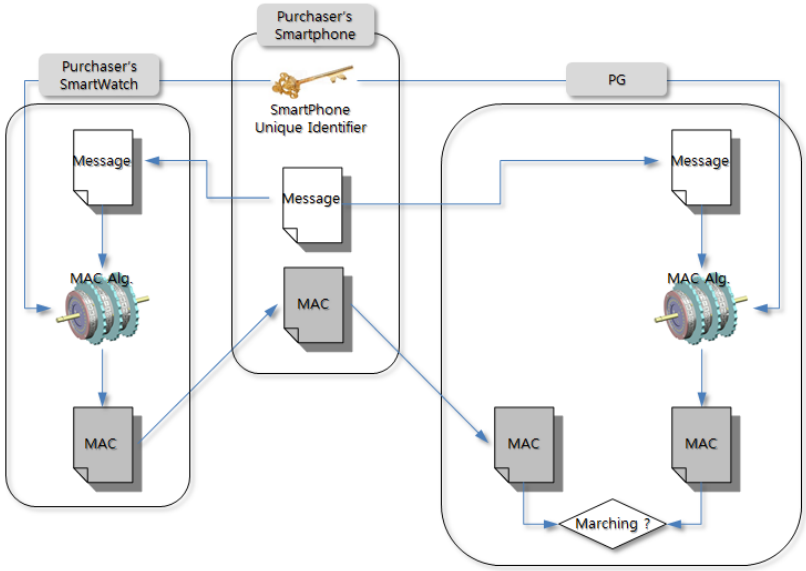

Figure 9. Relation among Security Modules for 2-Factor Authentication

In order to draw Figure 8, the logical agreement among security modules in components of 2-factor authentication is required in Fig. 9. The payment information is generated in purchaser's mobile device by user's willingness to pay. The secure element is generated using message (payment information) from purchaser's mobile device in purchaser's wearable device. That is, the message is made into the secure element in wearable device and transfer to Payment Gateway. Lastly, Payment Gateway authenticates and authorizes the payment transaction between a retailer and a purchaser.

5. Conclusions

As an increase in the services using mobile devices, various authentication technologies 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 proposed 2-factor authentication technology with knowledge-based authentication by user and possession-based authentication by smart watch.

Acknowledgments

This research was supported by the Dongshin University research grants.

References

[1] T. F. Smith and M. S. Waterman, "Identification of Common Molecular Subsequences", J. Mol. Biol. vol. 147, **(1981),** pp. 195-197.
[2] C. Ntantogian, S. Malliaros and C. Xenakis, "Gaithashing: A two-factor authentication scheme based on gait features", Journal of Computer & Security, vol. 52, **(2015),** pp. 17-32.
[3] Apple touch ID, http://support.apple.com/kb/HT5883
[4] S. Argyropoulos, D. Tzovaras, D. Ioannidis and M. A. Strintzis "Channel coding approach for human authentication from gait sequences," IEEE Trans Information Forensics Security, **(2009)** September.
[5] Y.-K. Ji and B.-R. Cha, "Prototype design of NFC-based electronic coupon ecosystem with object memory model", Contemporary Engineering Sciences, vol. 7, no. 22, **(2014),** pp. 1105-1112.
[6] C.-T. Li, C.-Y. Weng and C.-I Fan, "Two-Factor user Authentication in Multi-Server Networks", International Journal of Security and Its Applications, vol. 6, no. 2, **(2012),** pp. 261-268.
[7] S. Ullah, Z. Xuefeng and Z. Feng, "TCLOUD: A Multi-Factor Access Control Framework for Cloud Computing", International Journal of Security and Its Applications, vol. 7, no. 2, **(2013),** pp. 15-26.
[8] S. Yoo, S.-j. Shin and D.-H. Ryu, "An Innovative Two Factor Authentication Method: The QRLogin System", International Journal of Security and Its Applications, vol. 7, no. 3, **(2013),** pp. 293-302.
[9] B.-R. Cha, S.-H. Lee, S.-B. Park, G.-K. Lee and Y.-K. Ji and T.-h. Kim (Ed.), "Advanced Science and Technology Letters", Design of Micro-payment to Strengthen Security by 2 Factor Authentication with Mobile & Wearable Devices, Proceedings International Workshop Security, Reliability and Safety 2015, **(2015)** August 19-22; Jeju, Korea.
[10] J.-K. Park, "Fintech and Information Security", Journal of KIISE, vol. 33, no. 5, **(2015),** pp. 23-32.
[11] Emst and Young, "Landscaping UK Fintech Commissioned", UK Trade & Investment" August, **(2015).**
[12] C. Lan and W. Brown, "Data Security Considerations for FinTech Companies", BNA's Banking Report, **(2013)** April.

