Advanced Science and Technology Letters
Vol.107 (Ubiquitous Science and Engineering 2015), pp.5-8
http://dx.doi.org/10.14257/astl.2015.107.02

A Study on Service Architecture for Secure Authentication System

Sung Jin Kim[1], Myung Chul Ma[2], Hyeon-Kyung Lee[3] and Jong-bae Kim[4*]

[1,2]Dept. of IT Policy and Mgmt., Graduate School of Soongsil Univ., Seoul 156-743, Korea
[3,4*]Graduate School of Software, Soongsil University, Sangdo-dong,
Dongjak-gu, Seoul, Korea

Abstract. Recently, mobile field draws much attention and it is used for most means of living for users like purchase of commodity, payment, and user certification. Mobile economy also grows by this trend, but hacking accidents or financial crimes are also in full swing. It is expected that the service for mobile in the future will ever more be increased, but, in security aspect we still use problematic certification and security system. Data control service in the future is expected to done with the service which basically stores all services, based on cloud service, in phones as well as service providers. Data control service will lead to expansion of IoT (Internet of Things) service, as it substitutes existing off-line backup and safely provide user data regardless of location or kinds of devices. To use this data safely, establishing of certification system of users will be an ever more important factor. Therefore, this treatise is going to suggest the plan that, especially the certification among several threats, we can conduct it in safer way. This treatise is going to suggest the model that service provider can provide safe certification service by performing verification of transaction and data through electronic certification.

Keyword: Certificate, ISP, Authentication, Mobile, Payment

1 Introduction

Data control service will lead to expansion of IoT (Internet of Things) service, as it substitutes existing off-line backup and safely provide user data regardless of location or kinds of devices. That is, users can use data from the devices connected to internet without copying or moving to devices users want to use. To use this data safely, establishing of certification system of users will be an ever more important factor. Therefore, e-notarization for electronic data will be also revitalized. The size of internet shopping market is expected to be over 5 trillion won, according to the survey of KOLSA (Korea On-line Shopping Association) in 2015, and this is an about 12% increase compared with 2014, and especially, the uptrend of mobile sector appears noticeably [1]. With emerging of companies in which this mobile gravity occupies

[*] Jong-Bae Kim (kjb123@ssu.ac.kr) is the corresponding author of this paper.

ISSN: 2287-1233 ASTL

over 70% of entire internet shopping, mobile market is expected to be increased more. However, the measure for mobile security is now being used by existing method, appearing as the biggest threat to mobile economy, and when side effect by this is realized, even the outlook, which normal operation of mobile economy ecosystem would be impossible, is coming out [2]. Therefore, this study is going to suggest a plan that, especially the certification sector among several threats to mobile, we can conduct it in safer way. Mobile hacking is a very serious and important issue, as it could directly lead to monetary loss. In particular, when certification is insufficient, we will get to allow illegal benefit of 3rd party, not of actual users, through hacking. This study is going to suggest the model that service provider can provide safe certification service by performing verification of transaction and data through electronic certification.

2 Related Researches

Certificate verification is a kind of certificate of seal impression for cyber trade, as electronic information issued by licensed certificate authorities in order to check identity in e-commerce, and prevent forgery and alteration of document and denying of transactions fact. Hacking incidents which snatch certificate verification is being increased now after decades since introduction of certificate verification, reaching 15,386 cases in 2014. According to ‘ destruction status due to leakage of certificate verification in each bank’ submitted by Financial Supervisory Service to Assemblyman Kim Taewhan in Saenuri Party on the 16th, the cases destroyed by leakage of certificate verification were rapidly increased to 5871 cases in 2013 from 15 cases in 2011, and 8 cases in 2012, and also this year 15,376 cases occurred until the end of August[3]. Active-X is a technology developed by MS so that Windows users can use the document written by existing application program as it is with internet access. For instance, internet banking is available only on PC on which financial transaction and security program are installed, and Active-X is a means to distribute this program. In many cases normal internet service is difficult with other web browsers like Firefox, as majority of domestic internet sites are based on Active-X of IE, and government abolished this Active-X in March 2015 because many targets of hacking occurred due to Active-X. What Active-X became another criticism is that it made a loophole in security. A representing damage case is 7.7 DDOS case which made a noise to entire country in 2009. At that time Active-X was pointed out as it was misused in making zombie PC which simultaneously attacked Blue House and others[4]. OTP, a certification method based on ownership, has a very strong safety as it creates password through its only OTP token. However, purchasing OTP token, registering it to bank in person, and always carrying for use cause inconvenience for users to use OTP. Smart OTP means creation of one time password in software without OTP token to overcome these problems and raise user efficiency, and it is classified as knowledge-based certification as one time password is created based on confidential information, which is basically shared between user and computer [5].

3 Main Subject

3.1 System Concept

Combined certification means a type which individuals receive certification through online or offline, or a 3rd certification provider acts for certification for transaction. A problem occurred in the past, which had to confirm the person himself in case of hacking, as the person himself in person performed certification. Also in case of existing 2-channel certification, the current picture is that problems still exist with indirect method like using reproduced instrument. In order to solve this, this study is going to suggest a more perfect type of certification by making use of existing certificate verification and removing indirect method.

3.2 System Configuration

Users who will have identification or transaction through internet can do as such safely by submitting certification for transaction to trade institution through certification device. The concept suggested by this study is different in that user receive certification in real time through outside institution at the point of transaction, unlike existing public certification type. Though user just enters arbitrary value for transaction, this part is technically available for automation without limit. That is, when using the device, owned by both Smart Phone and user, for certification with mutual recognition, reproduction or hacking is impossible.

4 Conclusions

Combined certification suggested by this study solved problem of certificate verification type as well as security and convenience by suggesting additional certification device. It is expected that future certification device will be expanded more. With abolition of certificate verification system employer or institution who provides transaction service should prepare a separate certification type. It is judged that if we perform combined certification service by providing certification device that user can conveniently own, non-facing service can also perform as much as facing service. But, we should prepare a plan that can make more convenient initial registry procedure to save open key in certification server.

References

1. http://news1.kr/articles/?1906344
2. http://opennet.or.kr/e-finance-e-signature-reform.pdf

3. http://www.hidomin.com/news/articleView.html?idxno=249918
4. http://view.asiae.co.kr/news/view.htm?idxno=2015032509531946839
5. Seongmin Yoo, Jinseung Yu, Haegjin Jang and Jaecheol Ryou, "A Study on OTP Generation Method based on Software", Journal of the HCI Society of Korea, HCI 2011, No. 1, pp. 173-176 (2011)