Indian Journal of Science and Technology, Vol 9(24), DOI: 10.17485/ijst/2016/v9i24/96072, June 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Method of Secure App user Authentication from Auto-Login in the Mobile Device

Hyung-Jin Mun[1], Yong-zhen Li[2*] and Kwangyoun Jin[3]

[1]Division of Information and Communication Engineering, Baekseok University, Korea; jinmun@gmail.com
[2]Network and information Security Lab, Department of Computer Science and Technology, Yanbian University, Yanji, China; lyz2008@ybu.edu.cn
[3]Department of Computer Engineering, Kangwon National University, Korea; kyjin@kangwon.ac.kr

Abstract

Background/Objectives: At the present_where services are provided using devices, the importance of mobile device authentication is increasing. We propose secure authentication method from auto-login function. **Methods:** Mobile carriers remotely prevent using the device after the process getting the report of missing cellphone, but that can't be a complete solution when the USIM is removed or connection is made via wifi. This paper suggests a method with which when the service is requested by an app from mobile device, Service Provider decides to provide services after checking whether the device is lost through a trusted authority. **Findings:** A user, the owner of a cellphone, registers serial information of Phone, pSN, and reports when the cellphone is lost, and carries out a process to withdraw services. The service provider, whenever a service is requested, decides whether to provide the service through lost device checking process. In this way, the vulnerability of auto-login function of a lost phone can be fixed. Proposed method with the process to check the loss added authentication time compared to existing methods, but in terms of security and privacy protection, proposed method is superior because it provides services only when the device is not lost. **Application/Improvements**: With regard to solution to BYOD vulnerability and secure SSO, which have been recent issues, proposed method can be utilized as an effective method.

Keywords: BYOD, Mobile Authentication, Mobile Device, Mobile Security, Privacy, Smart Phone

1. Introduction

With the development of ICT, the life forms are rapidly changing. Especially, the specification of the mobile device has been highly improved and the era has come, in which the device replaces PC. Since the main components like CPU and RAM of the mobile device are comparable to those of PC, the second PC is used without limit of time and space. At the point where services are provided by the authentication through the device, the importance of mobile device authentication is increasing. Especially, the mobile device equipped with camera and GPS stores a lot of personal and account information. In addition, the occasion to use mobile device in workplace has been increased. Therefore, the researches on the weakness of BYOD have been conducted[1,2].

Despite of the convenient aspect of mobility, there are risks of being stolen and lost because mobile device itself is expensive. Mobile device users have become concerned about sensitive information that can be leaked from being stolen and lost of the device and many studies have been in the process[3-6].

At present, when the mobile device is lost and the report is made, the moving route can be found and remote control to stop the device usage and initialization can also be possible. However, if the third party who found the device removed USIM or tried to access Internet or used the device abroad, it is not easy for the mobile carriers to remotely control the device. This paper suggests the method with which the vulnerability of the auto-login

*Author for correspondence

function can be fixed regardless of the cases with wifi or 3G. Proposed method, by interworking with TA through Secure App, restricts services after checking whether mobile device is lost or not. The sequence of this paper is as follows; Chapter 2 introduces the related technologies that have been used; Chapter 3 introduces a safe authentication method using Secure App; Chapter 4 compares and analyzes the security with existing method; Chapter 5 concludes.

2. Related Works

2.1 Existing Model

Apps downloaded from Google Play or app store provides services after ID and PW are given when they access the server. However, to input the ID and PW with mobile devices is not easy so most of accounts are stored in the auto-login function so that they are to be given the services. Figure 1 describes the process from the request of the device to the service provided.

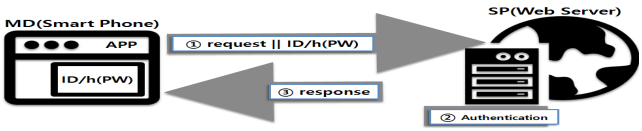

Figure 1. Existing Model.

2.2 CA(Certificate Authority)

As an alternative to the problem of symmetric key transmission and management, public key code algorithm is proposed. However, because the public key can be obtained by anyone, the falsification of the key is possible. Thus, to verify the subject of the public key has difficulty. With this weakness, there can be always Man in the middle attack in the system that adopts the public key. In order to solve the problem, subjects have trustworthy organization, CA, and CA sends a signature that proves the subjects are the owners of the key so that the problem can be solved. For secure message transmission, subjects send and receive the public key in the form of certificate one another (Figure 2).

The below describes the step to make a secure channel to transmit messages safely.

Step1. Receiver → CA: Receiver sends his public key to CA

Step2. CA: CA signs the receiver's key into a public key, that is he generates the certificate.

Step3. CA → Sender: He obtains the certificate from CA or Receiver.

Step4. Receiver → Sender: Sender obtains the public key from the certificate, and using the key, makes the secure channel and safely transmits the message.

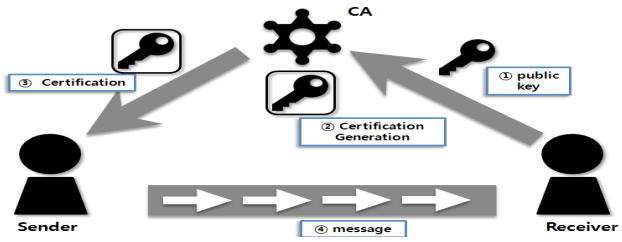

Figure 2. Secure Channel using certificate made by CA.

Once Sender obtains Receiver's public key, secure channel forms between Sender and Receiver. Certificate trusts the other's public key as much as CA does. However, there is a confirmation process to verify the certificate before using it. That is called CRL check. After checking if there is any certificate lost or expired, it utilizes the public key in a certificate to transmit secure messages[7].

3. Secure Authentication Method using Secure APP

The authentication app that applies the proposed method is defined as Secure APP. In Secure APP, the telecommunication subjects need to check the loss through CA. As CA manages CRL in PKI, proposed method suggests the structure in which TA manages the list of lost mobile devices[8]. In the case of smartphone, mobile carriers can be CA. Search engine sites called portal sites can be the object of Secure APP. A lot of information and data of the user are stored in portals and email account, and lots of services provided by apps begin with the account of portal sites and authentication in apps and PW losses occur in e-mail based portals.

In order for the apps like portals to apply the proposed method, firstly, one has to register his phone Serial Number (pSN), for Service Provider (SP) such as portals. The registration process is described as follows.

3.1 The Process to Register pSN for Service Provider

Figure 3 shows the stored information in SP when registering phone Serial Number (pSN) information, which

is the distinct identity number of Mobile Device (MD), in an invisible form into Service Provider (SP). ID_{12} registered MD, ID_{25} joined the website but didn't register MD.

no	ID	h(PW)	phoneSerialNumber	…
11	ID_{11}	$h(PW_{11})$		…
12	ID_{12}	$h(PW_{12})$	$h(ID_{12} \oplus pSN_{12})$	
…	…	…		
24	ID_{24}	$h(PW_{24})$	$h(ID_{24} \oplus pSN_{24})$	…
25	ID_{25}	$h(PW_{25})$		…

Figure 3. member table in the DB of Service Provider.

Below is the descriptions of steps to register pSN of MD into SP

Step 1. Joins membership after access to the website of Service Provider

Step2. Installs Secure APP that is provided by Service Provider through a market like "Google Play" in the mobile device; Allows permission to access of pSN in the process of installation; User accesses Service Provider(SP) through Secure APP installed in the device.

Step 3. Service Provider authenticates with given ID and PW. MD→SP : ID/PW || h(ID⊕pSN). Provides hash value as seen in Figure 4a; Provides ID and the result of hash value for Service Provider; At this point, the information of h(ID⊕pSN) is stored in the table of SP.

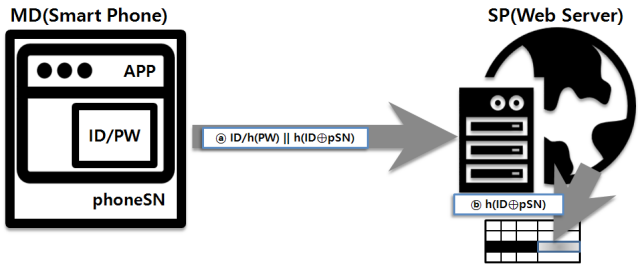

Figure 4. The process in which pSN information is stored in Web Server of SP.

Step 4. After authentication, Service Provider stores h(ID⊕pSN) into pSerialNumber field of member's table like the Figure 4b.

3.2 The Process to Report MD Loss of user

As a user reports his loss of smartphone to a mobile carrier's agent, when MD is lost, he needs to report that to TA. Because TA trusts the mobile carrier like Figure 5, it registers the pSN information provided by the mobile carrier on the revocation list. User doesn't go through the mobile carrier, but reports the loss to SP after log-in. At this point, after an additional authentication with I-PIN and accredited certificate is made, TA registers the loss into CRL after finding ID in the table of SP.

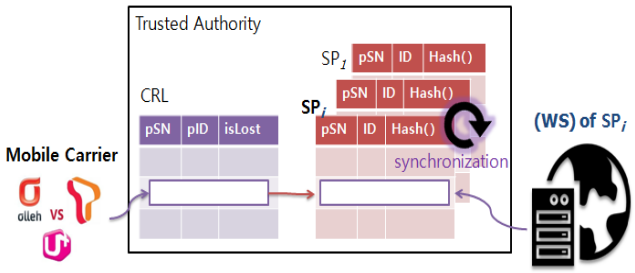

Figure 5. Registration at CRL in case of losses.

Through the system, although there are different SPs in MD, once SP registers the loss, TA automatically performs synchronization, which secures the safety from all the auto-login functions with only one report of the loss.

3.3 Checking Process of the Loss when Service Request is made after pSN Registration

Figure 6 describes the method by which after checking authentication process through the mobile device and confirming the loss from TA, it provides services with no problem found; if not, it stops providing services.

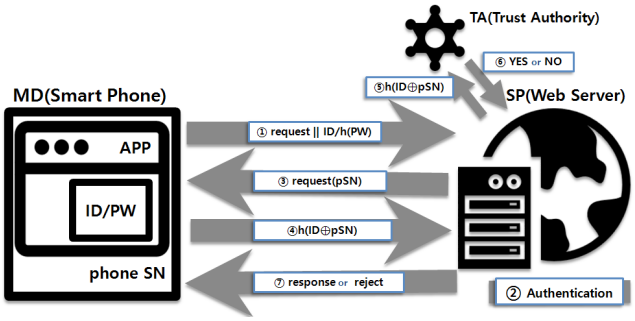

Figure 6. Proposed Method.

The below describes the step by step process to confirm the loss in the process of request.

Step 1. MD→WS : service request || ID/auto-login(PS). To request services, log-in is made by using auto-login function in the mobile device.

Step 2. WS : Authentication. Server tries to authenticate after checking the loss of the device to find out

whether it is MD or not; If not, the server doesn't check the loss and provides services. If it is MD, next step begins.

Step 3. WS→MD : pSN request. It requests pSN (phone serial number) to check the loss.

Step 4. MD→WS : h(ID⊕pSN). MD calculates the hash values about the information of ID⊕pSN and send them to the server. The reason to transmit them with hash values is to secure the pSN information from service provider.

Step 5. WS →TA: h(ID⊕pSN). WS provides h(ID⊕pSN) that is hash value for TA.

Step 6. TA : pSN_RL (revocation list in TA) searching. TA checks the loss after investigating h(ID⊕pSN) in the table of WS.

Step 7. TA →WS: checking the loss. TA notifies either the loss when the is Lost value is "yes" in the revocation list or that the loss hasn't occurred when the value is "no" to WS.

Step 8. WS →MD : service response or service reject. It rejects to provide services if it is a lost device, if not, it provides services.

3.4 Withdrawal Process

Withdrawal from the service implies two meanings. They are divided into the withdrawal from SP service, stop using Secure APP. First, the withdrawal from SP service proceeds by the request to withdraw from SP's website. At this point, SP removes not only given information but the information of TA. Second, regarding how to stop using Secure APP, it requires application for withdrawal, which is similar to the registration process. After that, it is necessary to delete Secure APP in the smart phone. In case it is not the withdrawal from the service provider but to stop using in certain device, the application for withdrawal should be made in the device, after that, it is necessary to register MD to be provided with services in another device. In case of the change in user, registered user stops using services and the other user should register. If the registered user didn't stop using services, the new user could not register.

4. Analysis and Discussion

Due to the electronic device which is portable and convenient, it is often lost and it is rare to retrieve the device. For this, in order to control a lost device the USIM of which is removed, the user needs to change passwords in the websites that he joined before and to log-out in other devices by using PC or other terminals, which are inconvenient actions.

With this proposed method, however, because the app checks the loss when authentication is requested, the user needs to simply register the loss. It can be an alternative to BYOD that has vulnerability caused by frequent use of mobile devices. Especially, the proposed method using auto-login function makes secure authentication possible.

Table 1. Existing Method VS Proposed Method

	Existing Method	Proposed Method
Authentication Time	short time	long time
Authentication Safety	poor	good
Privacy protection	-	good
BYOD vulnerability	high	low
SSO security	weak	strong

Table 1 compared and analyzed both of existing method and proposed method. Proposed method with the process to check the loss added authentication time, but in terms of security and privacy protection, proposed method is superior because it provides services only when the device is not lost. In addition, proposed method is more efficient in terms of BYOD vulnerability and SSO security which has been an issue nowadays.

5. Conclusions

At this point where services are provided using devices, the importance of mobile device authentication is increasing. At present, to convert existing app into secure APP takes additional expense. However, as for companies, because of the frequency to use mobile devices in the workplace increasing, BYOD vulnerability is always exposed. In this situation, the proposed method can be an alternative. In case the leakage of photos or videos taken with cameras in MD occurs, necessity to encode is raised. Regarding access to personal sensitive information or data, corresponding access control methods have been studied[9,10].

In this paper, the alternative for secure authentication in Secure APP using auto-login function is proposed. Proposed method works in MD applied with auto-login in Secure APP no matter what Internet method is used, for example wifi, 3G, LTE. A follow-up study would deal with either a method by which operation system in MD checks the loss, or a method to prevent illegal data leakage

by using SD memory card and cable. Especially, to design a system which blocks access to files in SD card with the security module not working after Android system recognizes any change when SD memory card is attached or detached is necessary.

6. References

1. Miller KW, Voas J, Hurlburt GF. BYOD: security and privacy considerations. IT Professional. 2012; 14(5):53–5.
2. Morrow B. BYOD security challenges: control and protect your most sensitive data, Network Security. 2012; (12):5–8.
3. Enck W, Octeau D, McDaniel P, Chaudhuri S. A study of android application security. Proceedings of the 20th USENIX Conference on Security. 2011; 21–21.
4. Friedman J, Hoffman DV. Protecting data on mobile devices: A taxonomy of security threats to mobile computing and review of applicable defenses, Information-Knowledge-Systems Management. 2008; 7(1/2):159-180.
5. Hyung-Jin Mun. Real Time User Location Information Protection Model Using Anonymity. Journal of the Korea Institute of Information and Communication Engineering. 2013; 17(10), 2316-2322. Doi no: 10.6109/jkiice.2013.17.10.2316.
6. R. Danu. Tracking Theft Mobile Application. Indian Journal of Science and Technology, 2016 Mar; 9(11), Doi no:10.17485/ijst/2016/v9i11/89381
7. W. Stallings, Cryptography and Network Security, ISBN 0-13-091429-0. Prentice Hall. 2002; 258-268
8. Hyun-Gon Kim. CRL Distribution Method based on the T-DMB Data Service for Vehicular Networks. Journal of the Korean Institute of Information Security and Cryptology. 2011; 21(4), 161-169.
9. Hyung-Jin Mun, Sejong Oh. Injecting Subject Policy into Access Control for Strengthening the Protection of Personal Information. Wireless Personal Communications. 2015 (first published online). Doi no: 10.1007/s11277-015-3094-7
10. Hyung-Jin Mun, Kun-Hee Han. A Study on Design for Efficient Personal Policy of Service based RBAC. Journal of Digital Convergence. 2016; 14(2), 191-196.