Advanced Science and Technology Letters
Vol.51 (CES-CUBE 2014), pp.180-183
http://dx.doi.org/10.14257/astl.2014.51.41

Authentication Techniques for Privacy Protection in N-Device Environment

[1]Si-Jung Kim, [2]Byong-Kwon, Lee, [3]Sohyun Sim, [4]An Na Kang

[1]College of General Education, Hannam University, Korea
sjkim6183@gmail.com.
[2,3,4]Department of multimedia engineering, Dongguk University, Korea,
sonic747@daum.net,ssh12510@naver.com,anakang37@gmail.com

Abstract. as well as a variety of communication environment using the present communication network. Thus, it is required to investigate the authentication techniques for safer access control considering the access device. This paper proposed the authentication technique guaranteeing the security against existing attack techniques using OPT server as well as the authentication server using OPT value generated on a user's side. The proposed authentication technique will realize safe service and authentication control by providing safer service access procedure.

Keywords: N-Device, Privacy Protection, Privacy Policy, Authentication.

1 Introduction

The users have been getting access to the service including web or application through a variety of equipment as receiving the IT service at present. The integrated display device called "N-Screen" supply a quantity of contents and applications to users on the basis of customized interface[1]. Diverse kinds of services including authentication and payment in online shopping malls or internet banking using N-Device have been actively used. Such services require the safe authentication before getting access to those services. Then, it is necessary to investigate the authentication services with a variety of potential security problems.

Section 2 of this paper introduces the researches related to authentication techniques for information security service. Section 3 analyzes the security in N-Device and authentication techniques. Section 4 explains the safe authentication techniques in N-Device as proposed in this paper. Section 5 summarizes the analysis results.

2 Related Work

User authentication technique using N-Device varies on security level to each service. The following Table 1 describes the problems of existing service authentication [2,3].

ISSN: 2287-1233 ASTL
Copyright © 2014 SERSC

Table 1. Problems of Authentication using N-device

Authentication Type	Problems	Security Vulnerability
OTP Authentication	Waiting time. Risk of encryption algorithm exposureInconvenient purchase of device	Private information exposure and message encoding
Mobile Authentication	Risk of security key loss	Message encoding Messagefalsification/fabrication

Such issues will be more aggravated through internet or a variety of information media. Thus, it is required to reduce input of excessive private information for authentication techniques and to strengthen the security by more strict authentication technique[4].

3 Authentication in N-Device Environment

3.1 Security Analysis according to N-Device Service Access

N-Device has the risk of being lost depending on types. Mobile Device Management(MDM)[4] service can become available depending on the service providers, but there is the risk which others illegally use the service using exposed password including payment by authentication before the service by the device is suspended. For smart phones, the credentials including user password can be saved in several devices and exposed even though malignant codes are installed. Thus, both dispersed and centralized storage have the security risk.[5,6]

3.2 User Authentication Techniques

(1) UICCAuthentication.

UICC supports Wideband Code Division Multiple Access(WCDMA) access authentication through mobile internet subscriber authentication module mounted on a device. UICC supports additional services including financial management, security management and privacy management.[7]

(2) EAP-AKAAuthentication.

.

N-Device applies Privacy and Key Management(PKM) mechanism for authentication and key management for mobile internet. PKM mechanism was used in early times. It is classified into PKMv1 for Rivest Shamir Adleman(RSA)-based authentication and PKMv2 for RSA and EAP-based authentication which supplemented demerits of PKMv1. PKMv1 was vulnerable against the replay attack. So PKMv2 has been used. The standard mechanisms available include EAP-MD5, EAP-TLS, and EAP-AKA.

[8].

4 Safe Authentication Techniques in N-Device

4.1 Proposed Authentication Technique

This paper proposed the authentication technique with high security through authentication between OTP generated by N-Device and the authentication server and the authentication with OPT authentication server. The authentication technique above may secure privacy protection and enables to use a variety of services more safely through N-Device, including mobile internet, financial transaction or private information management, provided that the user authentication is provided.

Figure 1 below illustrates the authentication technique proposed in this paper. The symbols in the figure have the following meanings:

N-Device: User N-Device

AA(Authentication, Authorization, Accounting) : Authentication server for authentication service

OTP : OTP value H(SK||AC||r) generated on N-Device with One-Time Password for authentication between N-Device and the authentication center.

A_kAK(Authentication Key) : Authentication Key

SK(Secret Key) : Shared secret key

r(Random number) : Generated random number

ACT(Auto CounTer) : Automatic counter providing synchronization by increasing by 1 per 10 seconds.

H( ) : secure hash function

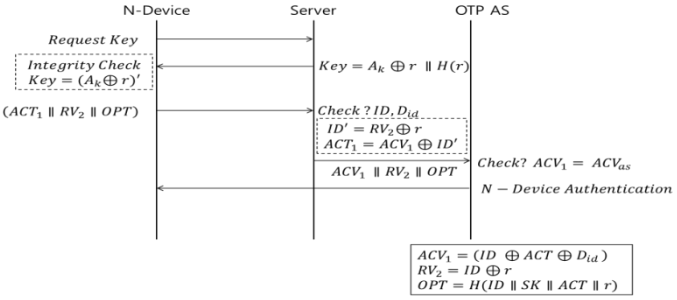
N-Device
Server
OTP AS
Request Key
Integrity Check
$Key = (A_k \oplus r)'$
$Key = A_k \oplus r \parallel H(r)$
$(ACT_1 \parallel RV_2 \parallel OPT)$
$Check ? ID, D_{id}$
$ID' = RV_2 \oplus r$
$ACT_1 = ACV_1 \oplus ID'$
$Check? ACV_1 = ACV_{as}$
$ACV_1 \parallel RV_2 \parallel OPT$
$N - Device Authentication$
$ACV_1 = (ID \oplus ACT \oplus D_{id})$
$RV_2 = ID \oplus r$
$OPT = H(ID \parallel SK \parallel ACT \parallel r)$

Fig.1. Proposed Authentication Technique

5 Conclusion

N-Device can be used in a variety of organizations including companies or government organizations as well as individuals and saves information of each organization.

Copyright © 2014 SERSC

If such information is exposed or falsified, the technologies of the relevant organization can be exposed. For preventing such risk, it is required to secure the service based on safer information protection management system. This paper proposed safer authentication procedure using the data generation in the authentication server and OTP value on a device user side for access to the service on web or application using N-Device. Furthermore, this paper verified the stability against diverse kinds of attack techniques. The authentication technique proposed in this paper will induce safe service and authentication control by providing safer service access procedure. Further study needs to apply the system depending on the security policy and analyze the stability of the proposed authentication techniques.

Acknowledgement. This research was supported by the MSIP(Ministry of Science, ICT and Future Planning), Korea, under the ITRC(Information Technology Research Center) support program (NIPA-2014-H0301-14-1021) supervised by the NIPA(National IT Industry Promotion Agency)

References

1. Choi, D., Kim, S., Jin, S.: Smart Channel : A Method for Processing Transactions in Smartphone for Authentication, Payment and Digital Signature in N-Device Environment," Journal of Korea Institute of Information Scientists and Engineers, No.39, Vol.6, December (2012)
2. Bae, D.H., Kim, C. J.: A Secure SMS Self-Authentication Method in Mobile Networks. Internet and Information Security, No1, Vol.2, pp.24-41, November (2010)
3. Shabtai,A. ,Fledel,Y.,Kanonov,U.,Elovici,Y.,Dolev,S.,Glezer,C.: Google Android: A Comprehensive Security Assessment. IEEE Security & Privacy, Vol.8, Issue.2, pp.35-44, (2010)
4. Bessani,A.,Correia,M.Quaresma,B., Andre,F. and Sousa,P.: DEPSKY: Dependable and Secure Storage in a Cloud-of-Clouds. Proc. of the 6th ACM SIGOPS/EuroSys European Systems Conference, April, (2011)
5. PAKE (Password Authenticated Key Exchange), ISO-IEC 11770-4.
6. T.,Itoh, H., Takahashi, K.: Implement identity provider on mobile phone," Proceeding of the 2007 ACM Workshop on Digital Identity Management, (2007)
7. Kang, A., Lee, J.D., Kang, W. M.,Barolli, L., Park, J. H.: A Study on Prevention of Smishing Attack on the Smartphone. Springer LNEE Proceedings, (2013)
8. Kang, A.,Barolli, L.,Jeong, H. Y., Park, J. H., Choi, H. G. : The Practical Quality Model for Cloud Learning System," Springer LNEE Proceedings, (2013)

Copyright © 2014 SERSC