Advanced Science and Technology Letters
Vol.99 (ITCS 2015), pp.176-179
http://dx.doi.org/10.14257/astl.2015.99.43

Scenario for Secure Transmission of Bio-information between Mobile application and Health Server[1]

Jong Tak Kim[1], Hee Jun Pan[1], Young Ho Lee[2], Un Gu Kang[2], Byung Mun Lee[2],

[1] Research and Development Center, Medical Solution for People C & S, Incheon, Korea
[2] Dept. of Computer Engineering, Gachon University, Incheon, Korea
jongtakkim@gmail.com, panheejun@nate.com, {bmlee, ugkang}@gachon.ac.kr

Abstract Most mobile health management application stores and manages user's health information in local memory. However, in u-Health Service, healthcare information is transmitted to healthcare server and provides integrated analysis and care service. Therefore, in mobile healthcare, it is necessary to transmit healthcare information to server. If healthcare information is not safely transmitted to server, there is a risk of being tapped, counterfeited or modified. In order to solve such problems, it is necessary to introduce a secure data transmission model between mobile device and server to facilitate safer data transmission. Therefore, this research paper proposes a data transmission model so that confidentiality of healthcare information is not compromised during transmission process.

Keywords: mHealth, security, eavesdropping, bio-information.

1 Introduction

With explosive growth in use of smartphones, the number of applications that provide healthcare information is increasing. This phenomenon appears to reflect a greater increase in health and diseases according to population aging. Growth of wireless communications technology led to a research on wearable devices, increasing the case of mobile devices handling healthcare information [1][2]. Mobile health applications are divided into behavior tracing, physical monitoring, weight reduction diet prescription, exercise methods, medical/healthcare information service, physical management program and integrated healthcare program [3][4][5]. Among them, since personal healthcare information can be transmitted to physical monitoring program [6], medical/healthcare information service and physician management program, there is a possibility of infringement on personal information between server and mobile device [7]. In general, infringement type during data transmission process includes infringement on data confidentiality such as tapping and infringement on data integrity such as counterfeiting and modification of transmitted data [8]. This

[1] This research was supported by the MSIP(Ministry of Science, ICT & Future Planning), Korea, under supervised by Incheon Information Service

ISSN: 2287-1233 ASTL
Copyright © 2015 SERSC

research deals with secure transmission model to solve infringement accident that occurs between server and mobile device application.

2 Vulnerability between mobile application and server

In order to prevent unauthorized user from leaking, damaging or modifying information, confidentiality, integrity and usability of data must be maintained. Infringement risk can be reduced if confidentiality and integrity of data can be preserved when personal healthcare information is transmitted from mobile application to server. The example in Figure 1 shows the types of data infringement. In (a), an application creates and transmits a http message that contains blood pressure values in SBP = 138 and DBP = 82. Http message is text-based and can be leaked during transmission via sniffing tools such as Wireshark.

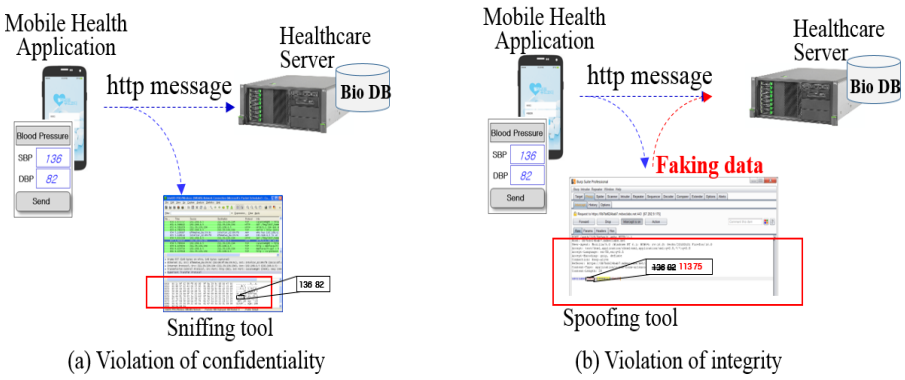

Fig. 1. Scenario of violation data between application and server

In (b), when the blood pressure value (138,82) entered in mobile device is transmitted over http message, spoofing tools such as burp suite can tap the http message and modify it to different values (113,75). It results in infringement on data integrity as the counterfeited values are stored in Bio DB.

2 Scenario for secure transmission

In order to prevent infringement on data confidentiality and integrity, data must be encrypted for transmission. Data confidentiality between mobile application and server can be maintained using RC4 encryption algorithm. RC4 is a method used in WET, TLS and RDP. It has faster processing speed but has a weakness in security. Spritz method is adopted in this paper to improve upon this weakness. As a response to infringement on data integrity, MD5 encryption algorithm was used to obtain and transmit the hash key values of the message being transmitted. Unlike RC4 method,

Copyright © 2015 SERSC

MD5 uses hash key values to verify if the message has been damaged in an attempt to check if the message being transmitted has been counterfeited or modified. If these two methods are used simultaneously, both data integrity and confidentially can be maintained

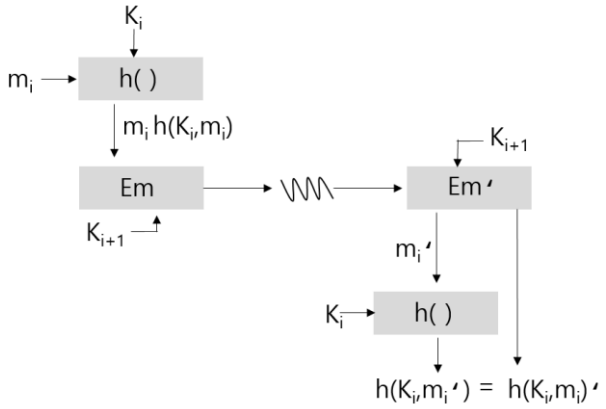

Fig. 2. Encryption and Decryption between application and server

As shown in Figure 2, mi, bio-information inputted into mobile application (e.g., blood pressure and blood sugar), is hashed along with the key Ki using MD5 method to create MAC(Message Authentication Code). The created code is integrated into mi and encrypted as Em using Spritz algorithm and then transmitted to the server. The server receives encrypted message Em and goes through decryption process in reverse direction to verify if the original message mi has been counterfeited. The MAC value obtained by hashing the original message is compared to MAC value within the message. If they do not match, it is judged a counterfeit and the server rejects the transmitted message. Thus, infringement on confidentiality and integrity of data is prevented.

4 Conclusion

Recently, there has been an increase in the number of mobile healthcare management applications. As a result, privacy infringements are expected to occur during transmission of healthcare information. This paper, as a solution to solve data confidentiality and integrity during transmission of personal healthcare information such as blood sugar and blood pressure using mobile application, proposed an encryption transmission scenario based on the method that integrates Spritz encryption method and MD5 method. There should be further empirical researches and experiments on preventing privacy infringement under a variety of situations with various types of infringement scenario in mobile devices

 Copyright © 2015 SERSC

References

1. Zhihan Lv: Wearable Smartphone: Wearable Hybrid Framework for Hand and Foot Gesture Interaction on Smartphone. Proc. of International Conference on Computer Vision Workshops (ICCVW), 2013 IEEE International Conference on. 436--443 (2013)
2. G. Bailly, J. Müller, M. Rohs, D. Wigdor and S. Kratz.: Shoe-sense: a new perspective on gestural interaction and wearable applications. Proc. of the SIGCHI Conference on Human Factors in Computing Systems, 1239--1248, (2012)
3. Silva, Bruno M.; Lopes, Ivo M.; Rodrigues, Joel J. P. C.; Ray, Pradeep Sapo Fitness: A mobile health application for dietary evaluation. Proc. of International Conference on e-Health Networking Applications and Services (Healthcom), 375--380, (2011)
4. Google fitness platform service web, https://developers.google.com/fit/
5. Fitbit One™ Wireless Activity, Sleep Tracker.: https://www.fitbit.com/#i.1o9dth 18wleh8r
6. N. Ukita and M. Kidode: Wearable virtual tablet: fingertip drawing on a portable plane-object using an active-infrared camera. Proc. of the 9th international conference on intelligent user interfaces, IUI '04, 169--176, (2004)
7. W.D. Yu, L. Davuluri, M. Radhakrishnan, M. Runiassy: A Security Oriented Design (SOD) Framework for eHealth Systems. Proc. of international workshop on Computer Software and Applications Conference. 122--127 (2014)
8. K. Knorr, D. Aspinall : Security testing for Android mHealth apps. Proc. of IEEE 8th International Conference on Software Testing, Verification and Validation Workshops, 322--325 (2015)

Copyright © 2015 SERSC