Authentication Models for Telebiometric Applications Using Mobile Devices

Yong-Nyuo Shin[1], Jae-Sung Kim[2],

[1] Dept.of Computer Engineering, Hanyang Cyber University,
222 Wangsimni-ro, Sengdong-gu, Seoul, Korea,
[2] Korea National Biometric Test Center, Korea Information Security Agency,
IT Venture Tower, Garak-dong 78, Seoul, Korea,
ynshin@hycu.ac.kr, jskim@kisa.or.kr

Abstract. In 2012, biometric company AuthenTec announced in a regulatory filing that it had agreed to a $356 million acquisition offer from Apple. The agreement provides Apple with the right to acquire non-exclusive licenses and certain other rights with respect to hardware technology, software technology and patents of the company for commercialization of 2D fingerprint sensors for use in or with Apple products [1]. As this case, the biometric technology based on the mobile device is more frequently used. It is necessary to make efforts to develop a security system that can preemptively cope with potential security threats mobile biometric data security. Also, biometric handles the sensitive personally identifiable information (PII), some of privacy issues for biometric in the mobile device should be considered [2]. This paper is designed to provide authentication models to ensure security and reliability of the flow of biometric information for telebiometric applications using mobile devices.

Keywords: Telebiometric, Mobile device, Biometrics, Authentication Model, Security

1 Introduction

With the widespread diffusion of the Internet, various network services are now in operation. In high value services, such as Internet banking, Internet shopping, Internet trading, etc. , illegal trading by obtaining a PIN by means such as phishing are occurring with increasing regularity. Therefore, high security authentication mechanisms are increasingly required, such as can be provided by biometrics [3]. We have the following problems in biometric authentication on the mobile devices: Firstly, service providers do not have any information regarding what biometric devices are in use at the end-user's end, what security level is this device set at, or how it is operated. Secondly, according to each biometric product, the accuracy (False Accept Rate) determined by the threshold parameter differs between different biometric products. Therefore, the service provider can't claim to maintain a uniform accuracy level. Finally, the accuracy of biometric verification may decline with the aging of end-users, because biometrics uses features of the human body. , biometric

handles the sensitive personally identifiable information (PII), some of privacy issues for biometric in the mobile device should be considered [5].

Chapter 2 explains the Environment of the telebiometirc applications using mobile devices. Chapter 3 explains the biometric hardware security module. Authentication models for the telebiometric applications using mobile devices. Finally, a conclusion is drawn and future study tasks are reviewed.

2 Environment for the telebiometric applications using mobile devices

Vulnerabilities mean weakness of mobile devices and their inabilities to withstand hostile environment effects. Attacks are any attempts to intentional destroy, unauthorized use, malicious modify or illegally obtain mobile devices assets. In other words, vulnerabilities are the internal attributes of mobile devices, while attacks are the external offensive activities to mobile devices. Telebiometric security reference models in operating telebiometric systems using a mobile device including cloud computing and big data environment. The environment of the telebiometirc applications using mobile devices is depicted in figure 1.

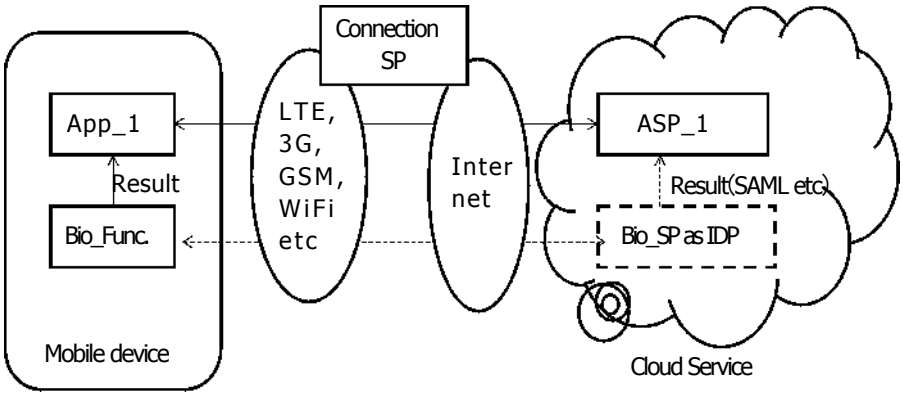

Fig. 1. Environment of the telebiometirc applications using mobile devices

3 Authentication models for the telebiometric applications using mobile devices

In this paper, we takes into account of the three perspectives below, dividing models into eleven categories

Table 1 Authentication Models

	Biometric Sensor	**Mobile Device**	**Server**
Model1	Capturing	Comparison Store*	
Model2	Capturing	Comparison	Store
Model3	Capturing		Comparison Store
Model4	Capturing Comparison		Store
Model5	Capturing Comparison	Store	
Model6	Capturing Comparison Store		
Model7	Capturin g Store	Comparison	
Model8	Capturin g Store		Comparison
Model9		Capturing Comparison Store	
Model10		Capturing	Comparison Store
Model11		Capturing Comparison	Store

* Biometric reference template location

4 Conclusion

To attack mobile devices, hackers must have a prior understanding of the specific mobile devices OS, as there are a larger number of mobile devices OSs than PC OSs [6]. In most cases, the scope of mobile devices security incidents is limited to individuals, such as personal information leaks, device disabling, and financial information loss. As mobile devices handle sensitive information and dedicated mobile devices security software is not sufficient, it seems that security measures need to be established. Types of mobile devices security incidents include personal information leaks, limited device use, illegal billing generation, and mobile DDoS. This paper is designed to provide authentication models to ensure security and

reliability of the flow of biometric information for telebiometric applications using mobile devices. These eleven telebiometrics authentication models depending on the configuration of the biometric sensor, the mobile device, and the server were defined. Future work will specify threat in operating telebiometric systems based on the mobile device and proposes a general guideline for security countermeasures from both technical and managerial perspectives in order to establish a safe mobile environment for the use of telebiometric systems. Also, we will include more detailed threats for cooperation of PKI, and a biometric authentication. Also we plan to standardize on this topic in ITU-T SG17 Q.9.

Acknowledgments. This research was supported by the ICT Standardization program(2012-PM10-27) of MKE(The Ministry of Knowledge Economy).

References

1. Why Apple really bought AuthenTec: It wanted “new technology” for upcoming products, and quickly, http://thenextweb.com/apple/2012/08/16/the-real-reason-apple-acquired-authentec-because-needed-new-technology-quickly-products/, August 2012.
2. Yong-Nyuo Shin, "Standard Implementation for Privacy Framework and Privacy Reference Architecture for Protecting Personally Identifiable Information", International Journal of Fuzzy Logic and Intelligent Systems , 2011, Vol 11, No 3, pp. 197-203.
3. International Standard ITU-T SG17, Telebiometrics system mechanism - Part 1: General biometric authentication protocol and system model profiles for telecommunications systems
4. Apple iPhone, http://www.apple.com/iphone/
5. Yong-Nyuo Shin, Woo Chang Shin, "A Security Reference Model for the Construction of Mobile Banking Services based on the SmartPhone”, International Journal of Fuzzy Logic and Intelligent Systems , 2011, Vol 11, No 4, pp. 229-237.
6. Giles Hogben, Marnix Dekker, "Smartphones: Information security risks, opportunities and recommendations for users", European Network and Information Security Agency, 2010.
7. Hahmin Jung, Dong Hum Kim, "Control of a Mobile Robot Based on a Tangible Interface using iPhone", Journal of Korea Institute of Intelligent Systems , 2011, Vol 21, No 3, pp. 335-340.
8. Yong-Hyun Cho, "System Development for Guiding Job Information Based on Android Smart-Phone", Journal of Korea Institute of Intelligent Systems , 2011, Vol 21, No 5, pp. 588-594.