The Implementation of Secure Mobile Biometric System

Yong Wan Ju and Byung Hee Lee

KISA (Korea Internet & Security Agency)
ywju@kisa.or.kr, bhlee@kisa.or.kr

Abstract

As the usage of mobile device is increased, it is started to appear various mobile service such as mobile payment, e-healthcare, etc. Identification and authentication are essential functions to use secure mobile service. As a means of user identification and authentication, password based method is used for long periods. However, password based method has some disadvantages like difficulties for remembering, leakage to others, etc. To solve these problems, biometrics technologies began to receive attention in virtue of user convenience.

In this paper, we describe some mobile biometric authentication model and examine threats. On the basis of this, we summarize possible countermeasures to provide secure telebiometric service. Then, we show our telebiometric system and analyze that system's security.

Keywords: *mobile telebiometric, user identification, authentication model, telebiometric vulnerabilities*

1. Introduction

As the usage of mobile device is increased, it is started to appear various mobile service such as mobile payment, mobile banking, *etc*. Identification and authentication are essential functions to use secure mobile service. As a means of user identification and authentication, knowledge-based method is the most widely used method for long periods. Recently, however, this method began having some problems such as difficulties for remembering, leakage to others, *etc*. To make up for these weak points, biometrics technologies are beginning to receive attention.

Biometrics is the science of establishing the identity of an individual based on the physical, chemical or behavioral attributes of the person [1]. Unlike identification and authentication measures such as token-based systems (*e.g.*, driver's license, passport) and knowledge-based systems (*e.g.*, password, personal identification number), since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods [2]. Furthermore, in biometrics based system, user don't need to remember or carry some passwords or tokens because identification and authentication are performed by using their own bio-information like fingerprint, face, iris, *etc*., and user convenience can be maximized. These characteristics are big factor why biometrics technologies has more attractive in mobile area.

The remainder of this paper is organized as follows: In Section 2, we examine telebiometric and authentication model for mobile biometrics in Section 3. In Section 4, we show our mobile biometric system and analyze the developed system's security in Section 5. Finally, we conclude this work in Section 6.

2. Telebiometric

Telebiometric applies biometrics to telecommunications and telecommunications to remote biometric sensing [3]. Through this, user which locates on remote place can utilize various services based on biometric technologies. Figure 1 shows environment of the telebiometric applications using mobile devices [4].

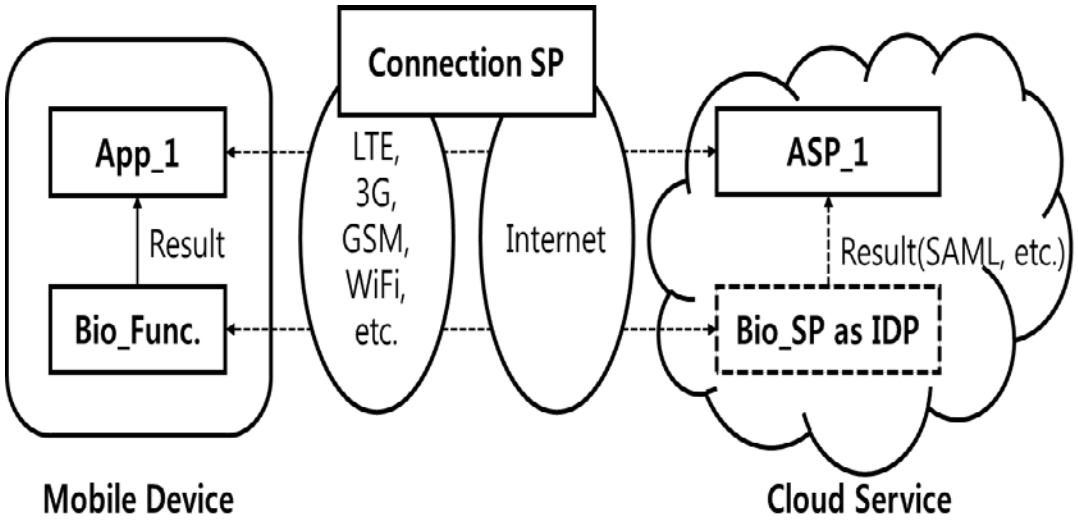

Figure 1. Environment of the Telebiometric Applications using Mobile Devices

Remote user inputs his/her bio-information into mobile device which has or connects biometric sensor. The inputted information may be processed in mobile device or transmitted to service provider and received the results via communication channel. Because telebiometric is based on remote connection, security issues should be considered to provide secure service.

3. Authentication Model for Mobile Biometrics and Threats

Various standard activities for biometric are in progress by standard groups such as ISO/IEC JTC1 SC27/37, ITU-T SG17 Q.9, *etc*. Especially, ITU-T SG17 Q.9 is performing standards for telebiometric in communication network environment. Among the progressing standard in ITU-T SG17 Q.9, X.1087, a guideline to technical and operational countermeasures for telebiometric applications using mobile devices, describes 12 authentication models for mobile biometrics which composed of three components: biometric sensor, mobile device, server [4]. This models depict all possible forms which telebiometric could be implemented using mobile device.

3.1. Authentication Model

The authentication models are divided into 12 categories according to each component's role. Description about these models is shown in Table 1.

Table 1. Authentication Models

	Biometric Sensor	Mobile Device	Server
Model 1	Capturing	Comparison, Reference	-
Model 2	Capturing	Comparison	Reference
Model 3	Capturing	-	Comparison, Reference
Model 4	Capturing, Comparison	-	Reference
Model 5	Capturing, Comparison	Reference	-
Model 6	Capturing, Comparison, Reference	-	-
Model 7	Capturing, Reference	Comparison	-
Model 8	Capturing, Reference	-	Comparison
Model 9	Capturing	Reference	Comparison
Model 10	-	Capturing, Comparison, Reference	-
Model 11	-	Capturing	Comparison, Reference
Model 12	-	Capturing, Comparison	Reference

As shown in Table 1, authentication model is divided based on role which each component performs: “Capturing”, “Reference”, “Comparison” means bio-information acquisition, the already enrolled bio-information, comparison acquired with enrolled bio-information, respectively.

3.2. Security Threats and Countermeasures

In this section, we examine security threats and countermeasures for each authentication model. Threats and countermeasures against these threats for each model which is described the above section is described in Table 2 [5].

Table 2. Security Threats for each Model

	Threats by unauthorized users	Countermeasures
Model 1	- Replace illegal capture data, such as stolen or altered data - Use illegal biometric reference template data - Use illegal comparison program - Leaked templates through the loss of the mobile devices	- Mutual authentication between sensor and mobile device - Encryption for the reference data

Model 2	- Replace illegal capture data, such as stolen or altered data - Alter illegally when the captured data is transferred - Use an illegal biometric reference template data - Use illegal comparison program - Leakage for the reference - transfer data to illegal server - Leaked templates through the loss of the mobile device or by having central server lost or stolen	- Authentication for the sensor, mobile device and server - Encryption for the transmission channel - Encryption for the references data
Model 3	- Replace illegal capture data, such as stolen or altered data - Alter illegally when the captured data is transferred - Attack the transmission channels - Transfer data to illegal server - Leaked templates by having a central server lost or stolen	- Authentication for the sensor and server - Encryption for the transmission channel - Encryption for the transferred data
Model 4	- Replace illegal capture data, such as stolen or altered data - Use an illegal Biometric reference template - Use an illegal comparison program - Leaked templates by having a sensor lost(or central server) or stolen - Attack the transmission channels	- Authentication for the sensor and server - Encryption for the reference data - Encryption for the transferred data
Model 5	- Replace illegal capture data, such as stolen or altered data - Use an illegal biometric reference template data - Use an illegal comparison program - Leaked template by having a sensor lost or stolen	- Authentication for the sensor and mobile device - Encryption for the reference data
Model 6	- Replace illegal capture data, such as stolen or altered data - Use an illegal biometric reference template data - Use an illegal comparison program - Leaked template by having a sensor lost or stolen	- Encryption for the reference data
Model 7	- Replace illegal capture data, such as stolen or altered data - Alter illegally when the captured data is transferred - Use an illegal biometric reference template data - Use an illegal comparison program - Leaked template through the loss of the mobile device	- Authentication for the sensor and mobile device - Encryption for the reference data

Model 8	- Replace illegal capture data, such as stolen or altered data - Alter illegally when the captured data is transferred - Attack the transmission channels - Transfer data to illegal server	- Authentication for the sensor and server - Encryption for the transmission channel
Model 9	- Misuse for the sensor by irrelevant application - Use the captured data by irrelevant application - Use an illegal biometric reference template data - Use an illegal comparison program - Leaked template through the loss of the mobile device	- Authentication for the sensor and application - Encryption for the reference data
Model 10	- Misuse for the sensor by irrelevant application - Use the captured data by irrelevant application - Attack the transmission channels - Transfer data to illegal server - Leaked template by having a central server lost or stolen	- Authentication for the sensor and application - Authentication for the application and server - Encryption for the transmission channel - Encryption for the transferred data
Model 11	- Misuse for the sensor by irrelevant application - User the captured data by irrelevant application - Use an illegal biometric reference template data - Use an illegal comparison program - Leaked template through the loss of the mobile device - Attack the transmission channels - Transfer data to illegal server - Leaked template by having central server lost or stolen	- Authentication for the sensor and application - Authentication for the application and server - Encryption for the reference data - Encryption for the transmission channel - Encryption for the transferred data
Model 12	- Misuse for the sensor by irrelevant application - Use the captured data by irrelevant application - Attack the transmission channels - Transfer data to illegal server	- Authentication for the sensor and application - Authentication for the application and server - Encryption for the transmission channel

As mentioned in Table 2, there can be various forms for telebiometric system. To provide secure telebiometric service, threats analysis should come before implementing the systems and proper countermeasures should be established based on that analysis.

4. Development of mobile Telebiometric System

In this section, we describe development of mobile biometric system based on smartphone. Our system adopts model 1 among the authentication models which is described in the previous section. Figure 2 shows the diagram of our system.

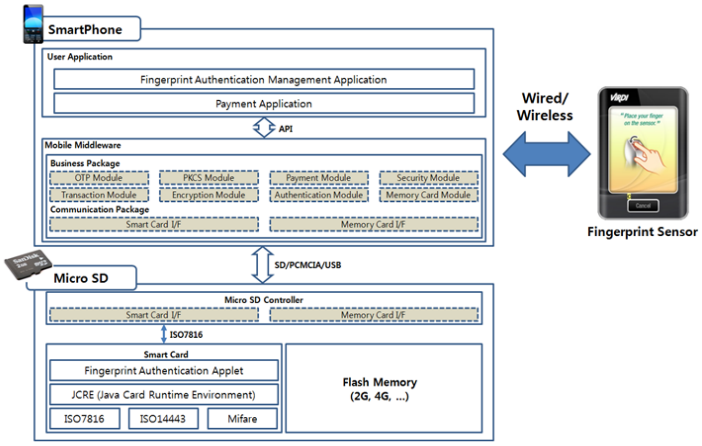

Figure 2. Overall Diagram of the Developed System

Figure 3. The Developed Mobile Biometric System

As mentioned in the above that our system adopts authentication model 1, the most of main functionalities (such as enrollment, template store and comparison, *etc*.,) are operated on smartphone except capture function. Bio-information is captured by external biometric sensor(in our case, we use fingerprint sensor) which connected to smartphone through Bluetooth [6]. The acquired information is compared with reference data and decided whether the inputted information is legal user or not (in other words, identification is proceed). After identification is succeeded, user can use additional services such as mobile payment, e-banking, *etc.*, as shown in Figure 3.

5. Security Analysis

Because the developed system is based on authentication model 1, threats which applied to our system are also related to those of model 1. Most of these threats have relevance to forge for template data or program. So, to solve these threats, we adopt MoC (Match-on-Card) [7] and financial microSD [8]. Through these technologies and standard, the developed system store critical information on SE (Secure Element) area included in microSD card and performed matching algorithm in only SE area. Therefore, our system can prevent data or algorithms from leaking to the other person and secure telebiometric service can be provided.

6. Conclusions

It is stared to appear various mobile service such as mobile payment, e-banking, *etc.*, because of increasing the usage of mobile device. However, security aspects as well as user convenience should be considered with deliberation to provide secure mobile service.

To address these problems, we examine authentication model for mobile biometric and threats for each model. According to this examination, we develop mobile biometrics system which equivalent of the model 1. Furthermore, we adopt MoC technology and financial microSD standard to implement secure mobile biometrics system. By applying these technology and standard, it is possible that leakage of crucial information such as user's bio-information or specific algorithm can be prevented and secure mobile biometric service can be provided.

Acknowledgements

This research was supported by the ICT Standardization program of MISP(The Ministry of Science, ICT & Future Planning).

References

[1] A. K. Jain, P. Flynn and A. Ross, Handbook of Biometrics, Springer, pp. 1-22, ISBN 978-0-387-71040-2, **(2008)**.
[2] Wikipedia, Biometrics, http://en.wikipedia.org/wiki/Biometrics, **(2010)**.
[3] Wikipedia, Telebiometrics, http://en.wikipedia.org/wiki/Telebiometrics, **(2009)**.
[4] Y.-N. Shin and J.-S. Kim, "Authentication Models for Telebiometric Applications using Mobile Devices", Advanced Researches on Software Technology, vol. 19, **(2013)**, pp. 61-64.
[5] ITU-T SG17 Q.9, A guideline to technical and operational countermeasures for telebiometric applications using mobile device, **(2012)**.
[6] Wikipedia, Bluetooth, http://en.wikipedia.org/wiki/Bluetooth, **(2011)**.
[7] J. Nilsson and M. Harris, "Match-on-Card for Java Cards", Precise Biometrics, **(2004)**.
[8] Bank of Korea, Standards for financial microSD v1.0, **(2012)** October.

Authors

Yong Wan Ju

1997: Graduated H.U.F.S in business management (bachelor's degree)
2002: Graduated H.U.F.S in Global Business (master's degree)
2007: Soongsil University in Computer Science & Engineering (doctor's degree)
1997-1999: National Information Society Agency (NIA)
2000-Current: Korea Internet & Security Agency (KISA)

Byung Hee Lee

2005: Graduated Sungkyunkwan University in Computer Engineering (bachelor's degree)
2007: Graduated Sungkyunkwan University in Computer Engineering (master's degree)
2012: Graduated Sungkyungkwan University in Information and Communication Engineering (doctor's degree)
2012-Current: Korea Internet & Security Agency (KISA)