A Study of Authentication Scheme using Biometric-Based Effectiveness Analysis in Mobile Devices

Keun-Ho Lee
Division of Information Communication, Baekseok University

Abstract As the life which existed only offline has changed into a life part of which is led online, it is an important problem to identify whether an online user is legitimate one or not. Biometric authentication technology was developed to identify the user more correctly either online or in offline daily life. Biometric authentication is a technology where a person is identified by his or her unique characteristics, and is highlighted as a next-generation authentication technology replacing password. There are various kinds of traits unique to each individual, and biometric authentication technologies drawing on such traits use various devices and algorithms. Firstly, this paper classified such various biometric authentication technologies, and analyzed the effects of them when they are applied on smartphone, smartwatch and M2M of the different devices platforms. Secondly, it suggested the effectiveness-based AIB(Authentication for Integrated Biometrics) authentication technique, a comprehensive authentication technique, which can be used in different devices platforms. We have successfully included the establishment scheme of the effectiveness authentication using biometrics.

Key Words : Authentication, Biometric, Effectiveness, Mobile Device, Security

Received 1 November 2013, Revised 20 November 2013 Accepted 20 November 2013 Corresponding Author: Keun-Ho Lee (Baekseok University) Email: root1004@bu.ac.kr

Ⓒ The Society of Digital Policy & Management. All rights reserved. This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (http://creativecommons.org/licenses/by-nc/3.0), which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.
1. Introduction

In the Internet-based modern information society, there is an increasing demand for automated means of identify and certify different persons. While all the life was led offline in the past, currently much part of it is led online. Thus, it has become an important problem to know whether the user online where people interact without seeing each other is the proper user or not. User authentication methods can be divided into the following kinds: what uses the information the user knows like password or PIN, etc.; what uses the equipment the user possesses like smartcard; what uses unique information about the user such as fingerprint or voice. Since the kinds of information the user knows, and the user possesses are in danger of being forgotten or stolen, they do not provide perfect security functions. But, as biometrics uses unique biological information of the user, it does not have any danger of being lost or stolen, and can provide higher security than existing user authentication methods. Biometric authentication is the technology which, using the automated apparatus, measures human physical, behavioral characteristics, and uses them as means of identification and authentication of individuals. Typical examples are authentication of fingerprint, face, iris, retina, vein, and signature, etc. Biometric authentication systems are used in daily lives such as entry and exit control, crime investigation, data management, missing child search, and departure from and entry into the country control, etc. [1][2].

This paper tries to describe trends of smartphone, smartwatch and M2M technologies, the user authentication method which can satisfy the requirement of convenience and security in the networked environment, analyzes its effectiveness when a variety of smartphone, smartwatch and M2M platforms are applied, and suggest appropriateness of models applying biometric authentication on various M2M devices, when authentication method is changed into biometrics.

2. Related Work

The popularity of smartphone platforms in the sample is depicted in Table 1. The second column presents the proportion of users in each platform, along with the popularity rank amongst the platforms. The platform popularity that was discovered in the Greek sample is comparable to a recent Gartner report4 concerning global smartphone popularity. Android, iOS and Symbian were the dominant smartphone platforms in both surveys, while in our sample Windows Phone had more popularity than Blackberry[3].

A smartwatch is a computerized wristwatch with functionality that is enhanced beyond timekeeping, and is often comparable to a personal digital assistant (PDA) device. While early models can perform basic tasks, such as calculations, translations, and game-playing, modern smartwatches are effectively wearable computers. Many smartwatches run mobile apps, while a smaller number of models run a mobile operating system and function as portable media players, offering playback of FM radio, audio, and video files to the user via a Bluetooth headset. Some

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Sample Popularity</th>
<th>Gartner Popularity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android</td>
<td>38.4% (1)</td>
<td>50.9% (1)</td>
</tr>
<tr>
<td>BlackBerry</td>
<td>9.2% (5)</td>
<td>8.8% (4)</td>
</tr>
<tr>
<td>iOS</td>
<td>23.8% (2)</td>
<td>23.8% (2)</td>
</tr>
<tr>
<td>Symbian</td>
<td>16.0% (3)</td>
<td>11.7% (3)</td>
</tr>
<tr>
<td>Windows</td>
<td>12.0% (4)</td>
<td>1.9% (5)</td>
</tr>
<tr>
<td>Other</td>
<td>0% (6)</td>
<td>2.8% (6)</td>
</tr>
</tbody>
</table>

(Table 1) Smartphone platform popularity
smartphone models, feature full mobile phone capability, and can make or answer phone calls. Such devices may include features such as a camera, accelerometer, thermometer, altimeter, barometer, compass, chronograph, calculator, cell phone, touch screen, GPS navigation, Map display, graphical display, speaker, scheduler, watch, SD cards that are recognized as a mass storage device by a computer, etc. and Rechargeable battery. It may support wireless technologies like Bluetooth, Wi-Fi, and GPS. However, it is possible a “wristwatch computer” may just serve as a front end for a remote system, as in the case of watches utilizing cellular technology or Wi-Fi. The Galaxy Gear smartwatch from Samsung is the company’s first attempt to enter a market in which the industry has adopted as the next opportunity for growth. Sony’s new smartwatch, which is actually named the Smartwatch 2, has been a known quantity since its official announcement in June at the Mobile Asia Expo in Shanghai, and now the Samsung Galaxy Gear has been itemized by its creators in Berlin at IFA. Meaning it’s time for the two to square off in our blogger arena of champions for a spec and feature showdown in Table 2.[4][5][6].

3. Analysis of Effectiveness per Platform Environment

3.1 Smartphone

Smartphone exists with the user anywhere and
anytime, and generates various big data. Various sensors existing in smartphone allow the user to authenticate himself or herself. Recently, sensors which can identify biological information of the user such as fingerprint authentication of iPhone 5S of Apple are appearing in the market. Such a phenomenon is possible to be a trend in the mobile market, and it is expected that various applications will be introduced in the market. Currently in smartphone platforms, user authentication is done by applying authentications using password, pattern, face, or fingerprint. Existing simple user authentication methods have been developed into models applying biometric authentication. The biometric authentication makes it possible to authenticate the user correctly. However, since the biological information cannot be revised, if the key is stolen in a broader authentication service process, the result would be to provide hacker with a life-long master key. Thus, it is necessary to have a secure countermeasure against it. As a countermeasure, it is necessary to develop a authentication model which uses authentication through the terminal serves as the basis, and also additional authentication stage which makes it possible to authenticate real biological information.

3.2 Smartwatch

Smartwatch is currently provided as accessories-based one through convergence service linked with smartphone. However, given the situation that wearable computing is expected to be active in the future, application to smartwatch is judged be to applied rapidly. Since smartwatch has merits such as being convenient to carry around and easy for using various functions, many models will be developed through frequent uses. Especially, as smartwatch is worn around wrist, it is effective to authenticate the user of it with the physical information which can be acquired from the wrist. Such physical information includes vein and electrocardiogram (ECG), etc. And, with the development of physical information-sensing technologies, various methods for acquiring the information will be developed. Currently, authentication methods through vein or ECG are in the initial research stage, and they will be developed into technologies which make it possible to generate unique keys through vein or ECG authentication. And, the authentication method using comprehensively various kinds of physical information will heighten the strength of security, and have higher possibility to guarantee safety. However, when physical information used for authentication is exchanged through close range network, it is at risk of being bugged. To prevent such bugging, sturdy password protocols should be applied to secure close range communication- and wearable computing-based safety. As close range wireless environment deals with light-weight data, it is important to raise effectiveness of resources and recognition rate through designing light-weight protocols optimized to physical information.

3.3 M2M(Machine to Machine)

M2M is matter intelligence communication, and has settled down as the next-generation mobile communication paradigm. M2M is being developed to the stage where various devices are structured to provide convergence service. Especially, as examples applying M2M, there are models for inter-device service in various fields such as intelligent car, healthcare, and smart grid, etc. Among various fields where M2M is applied, U-Healthcare where core data for biometric authentication can be used is expected to be the most active in applying M2M technologies. When various service models are developed in the U-Healthcare application field, those models are expected to develop into services used to monitor real time data on physical information. In an environment where physical information can be exchanged, the technologies capable of authenticating unique biological information of the user will be used as important
A Study of Authentication Scheme using Biometric-Based Effectiveness Analysis in Mobile Devices

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>BKDC(Biometrics Key Distribution Center)</td>
<td>Reliable BKDC which can manage the user’s account and provide biological information of the user</td>
</tr>
<tr>
<td>CBK (Center Biometrics Key)</td>
<td>Biometric recognition-based personal key of BKDC</td>
</tr>
<tr>
<td>UBK (User Biometrics Key)</td>
<td>Biometric recognition-based personal key of user</td>
</tr>
<tr>
<td>SBK (Server Biometrics Key)</td>
<td>Biometric recognition-based personal key of the server user uses</td>
</tr>
<tr>
<td>TGT (Ticket-Granting Ticket)</td>
<td>Ticket having information on user’s name and finish time</td>
</tr>
<tr>
<td>SA</td>
<td>TS; Session key between user and BKDC</td>
</tr>
<tr>
<td>KAB</td>
<td>Session key between user server and BKDC</td>
</tr>
</tbody>
</table>

Technology, and raise effectiveness. Physical information, core data treated in U-Healthcare, has the merit of not having to move additional authentication data, when it is used for authentication. However, with the increase of convenience in use of it, it contains various and serious risks in security. Leakage of sensitive information like the disease name and treatment records of it of a patient, among personal information of the patient, is likely to seriously violate his or her privacy. It is also possible to attack which can have bad effects on the life and health of the patient by manipulating data on healthcare apparatus. In the comprehensive medical information system as well, biometric authentication methods will be used as means of comprehensive authentication for each individual. As various elements threatening security can be expected in the comprehensive medical information system, it is necessary to analyze different scenarios where security can be threatened from the designing stage of the system, and develop models which can upgrade security levels.

4. Authentication Scheme for Integrated Biometric Recognition

This chapter suggests the AIB (Authentication for Integrated Biometrics) scheme in which security is strengthened in biometric recognition used in each platform for comprehensive biometric identification and authentication. In the existing Kerberos authentication technique using symmetric-key cryptography, reliable KDC (Key Distribution Center) concept is used.

The AIB authentication technique is what integrated the Kerberos authentication technique for existing users and biometric authentication technique, which authenticate users in various platforms from security threats. In the Kerberos authentication technique using existing symmetric-key cryptography, there is reliable KDC (key distribution center). KDC has 3 kinds of personal keys — KA, KB, KKDC — for mutual authentication between server and user.

However, in the AIB authentication mechanism, KDC is replaced by BKDC, biometric recognition-based key distribution center, and KA, KB, and KKDC, personal keys of user, server, and KDC are replaced by values of UBK, SBK, and CBK. The AIB authentication techniques are as follows.

Step 1: Operator sends his or her own biological information to BKDC. As a person’s biological information is unique to the person, even if a third person intercepts it, the third person cannot abuse it.

Step 2: BKDC encrypts SA and sends it to UBK, and encrypts the ticket containing SA, and sends it to UBK. Through this process, the user can trust and authenticate the BKDC holding UBK, his or her own personal key.

Step 3: Operator encrypts the time stamp used for time synchronization with the ticket encrypted as CBK which he or she received from BKDC and SA which he or she acquired through one’s own UBK, and sends it to BKDC. BKDC can authenticate operator as the user by decrypting the time stamp with his or her own key.

The Journal of Digital Policy & Management I 799
and user authentication was done by meeting them. Recently, however, with the development of technology and booming online activities, user authentication has become an important problem. If biometric authentication using fingerprint and voice, etc. is available in smartphone which is evolving further and further, various applications will be created. But, since the security of smartphone is weak, it has demerits of the key being stolen. This paper described what biometric recognition is, and discussed the kinds of biometric authentication and effectiveness of them when they are applied to various platforms. In this paper classified such various biometric authentication technologies, and analyzed the effects of them when they are applied on smartphone, smartwatch and M2M of the different devices platforms. It suggested the effectiveness-based AIB (Authentication for Integrated Biometrics) authentication technique, a comprehensive authentication technique, which can be used in different devices platforms. We have successfully included the establishment scheme of the effectiveness authentication using biometrics.

5. Conclusion

In the past when online activities were not frequent, and user authentication was done by meeting them. Recently, however, with the development of technology and booming online activities, user authentication has become an important problem. If biometric authentication using fingerprint and voice, etc. is available in smartphone which is evolving further and further, various applications will be created. But, since the security of smartphone is weak, it has demerits of the key being stolen. This paper described what biometric recognition is, and discussed the kinds of biometric authentication and effectiveness of them when they are applied to various platforms. In this paper classified such various biometric authentication technologies, and analyzed the effects of them when they are applied on smartphone, smartwatch and M2M of the different devices platforms. It suggested the effectiveness-based AIB (Authentication for Integrated Biometrics) authentication technique, a comprehensive authentication technique, which can be used in different devices platforms. We have successfully included the establishment scheme of the effectiveness authentication using biometrics.

REFERENCES

A Study of Authentication Scheme using Biometric-Based Effectiveness Analysis in Mobile Devices


이 근 호 (Lee, Keun Ho)

• 2006년 8월 : 고려대학교 컴퓨터학과 (이학박사)
• 2006년 9월 ~ 2010년 2월 : 삼성전자 DMC연구소 책임연구원
• 2010년 3월 ~ 현재 : 백석대학교 정보통신학부 조교수
• 관심분야 : M2M 보안, 이동통신 보안, 응답 보안, 개인정보보호, ISMS(정보보호관리체계), 정보보호사전점검
• E-Mail : root1004@bu.ac.kr