http://dx.doi.org/10.14400/JDPM.2013.11.11.795

모바일 장치에서 신체정보기반의 효용성 분석을 이용한 인증기법에 관한 연구

이근호
백석대학교 정보통신학부

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

Keun-Ho Lee
Division of Information Communication, Baekseok University

요 약 과거의 오프라인에서만 이루어졌던 생활이 온라인에서의 활동으로 발전함으로 인해 온라인상에서 사용자가 올바른 사용자인지의 여부는 중요한 문제이다. 온라인상이나 나아가 일반 생활에서도 사용자 인증을 보다 정확하게 하기 위하여 생체인식 기술을 도입하고 있다. 생체인식 기술은 개인의 고유한 특징을 이용하여 인증을 수행하는 방법으로 비밀번호를 대체하는 차세대 인증 기술로 각광받고 있다. 인간의 고유한 특징의 종류는 매우 다양하며 이러한 특징을 추출하는 생체인식 기술도 다양한 장치와 알고리즘을 이용하여 이루어진다. 본 논문에서는 첫째로 이러한 다양한 장치인 스마트폰, 스마트와치, M2M 플랫폼을 분석하고 적용하였을 경우 어떤 효용성이 있는지 분석한다. 둘째로, 다른 장치 플랫폼에서 포괄적인 인증인 효용성기반의 AIB를 제안한다. 제안 인증기법은 신체정보를 이용한 효율적인 인증을 포함한다.

주제어 : 인증, 신체정보, 효용성, 이동장치, 보안

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

ISSN: 1738-1916

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 1〉 Smartphone platform popularity

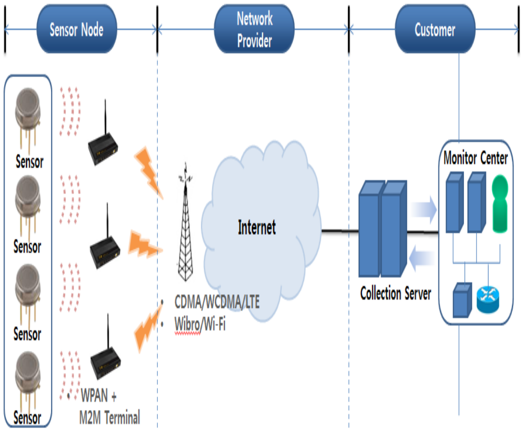
Operating System	Sample Popularity	Gartner Popularity
Android	38.4% (1)	50.9% (1)
BlackBerry	9.2% (5)	8.8% (4)
iOS	23.8% (2)	23.8% (2)
Symbian	16.6% (3)	11.7% (3)
Windows	12.0% (4)	1.9% (5)
Other	0% (6)	2.9% (6)

〈Table 2〉 Comparison of the smartwatch specs

Sony Smartwatch2	Samsung Galaxy Gear
1.6-inch, 220×176 display Aluminum body Micro USB charging Compatible with most Android phones NFC and Bluetooth 3.0 for connectivity 3 to 4 days battery under normal use €199($262 U.S), Ships in late September No camera, mic or speakers	1.63-inch, 320×320 display Stainless steel body Snap-on, proprietary USB 3.0 charger 800MHz Exynos single-core processor Bluetooth 4.0 LE Compatible with new Galaxy devices, previous gen Galaxy support coming soon Around 1 day of use 4GB of onboard storage $299 Ships in September (October for U.S.) 1.9 megapixel camera, 720p video recording, speaker + 2 mics Gyroscope and accelerometer for workout tracking

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, SDcards 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].

M2M service is defined as Machine to Machine, Machine to Man, Man to Machine. As depicted in figure 1, various devices are installed to communicate and collect information from surrounding equipment and devices. Its concept is to provide information service to people and surrounding machines. M2M is utilized in the sectors of sensor network, Tracking, c, and emerging device. Core technologies in M2M are identification, information collection, communication, intelligence and minimization, and every devices and system should be maintained autonomously and securely through control and information exchange between machines [7][8][9].



[Fig. 1] M2M Architecture

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 accessaries-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, health care, 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

〈Table 3〉 Symbol of the AIB

Symbol	Contents
BKDC(Biometrics Key Distribution Center)	Reliable BKDC which can manage the user's account and provide biological information of the user
CBK (Center Biometrics Key)	Biometric recognition-based personal key of BKDC
UBK (User Biometrics Key)	Biometric recognition-based personal key of user
SBK (Server Biometrics Key)	Biometric recognition-based personal key of the server user uses
TGT (Ticket-Granting Ticket)	Ticket having information on user's name and finish time
SA	TSession key between user and BKDC
KAB	Session key between user server and BKDC

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.

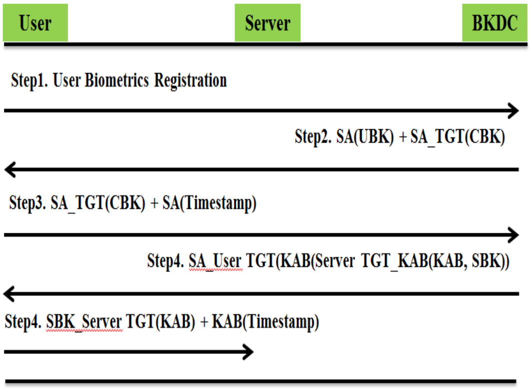
The AIB authentication technique is what integrated the Kerberos authentication technique for existing users and biometric authentication technique, which authenticate users in various platforms from security threats. In the Kerberos authentication technique using existing symmetric-key cryptography, 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
Server
BKDC
Step1. User Biometrics Registration
Step2. SA(UBK) + SA_TGT(CBK)
Step3. SA_TGT(CBK) + SA(Timestamp)
Step4. SA_User TGT(KAB(Server TGT_KAB(KAB, SBK))
Step4. SBK_Server TGT(KAB) + KAB(Timestamp)

[Fig. 2] Scheme Authentication BKDC to User

legitimate owner by confirming that the operator acquired SA by decrypting one's own ticket with CBK and encrypted the time stamp with the acquired SA, and sent it to BKDC. Through such a process, user and BKDC can authenticate each other.

Step 4: One includes the server ticket containing session key KAB between BKDC and server, and is encrypted as SBK into the operator ticket, and encrypts it as SA, and sends it to operator. Operator acquires server ticket and session key KAB through decrypting them through SA.

User sends the server ticket he or she acquired to server, and encrypts time stamp used for time synchronization as session key KAB and sends it. Server acquires KAB through decrypting it by using SBK, his or her personal key, and acquires time stamp by decrypting it using acquired KAB. Server can authenticate operator holding KAB, and rely on BKDC which encrypted it into one's personal key SBK as legitimate biometric key distribution center. In this way, BKDC, user, and server can authenticate one another.

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

[1] Jung-Woo Seo, Dong-Og Min, Jong-Sub Moon, “A study on the Muti-Modal Biometrics System”, Korean Institute of Information Scientists and Engineers”, Spring Conference, Vol.30, No1, pp.301-3020, 2003.

[2] Sung-Hyun Yun, Heui-Seok Lim, “The Biometric based Mobile ID and Its Application to Electronic Voting”, KSII Transactions on Internet and Information Systems, Vol.7, No.1, pp.166-183, 2013.

[3] Alexios Mylonas,Anastasia Kastania,Dimitris Gritzalis,“Delegatethesmartphoneuser?Securityawarenessinsmartphoneplatforms”, Computer & Security, Vol34, , pp.47~66, 2013.

[4] Pascoe, Jason. "The Smartwatch." Proceedings of

the Conference on Mobile and Ubiquitous Systems (CSMU), pp. 203-206, 2006.

[5]http://techcrunch.com/2013/09/04/sonys-smartwatch-2-versus-samsungs-galaxy-gear-two-very-different-smartwatches-face-off/

[6]http://news.cnet.com/8301-19882_3-20087282-250/wimm-launches-platform-for-smart-watches/

[7] Keun-Ho Lee, "Authentication Scheme based on VANET Cluster in M2M", ICCT2012, pp.16~19, Jan 2013.

[8] Gab-Sang Ryu, Keun-Ho Lee, "Authentication based on Cluster in Machine to Machine", Journal of The Korea Knowledge Information Technology Society, Vol 5, No.6, pp.103-110, 2010

[9] Tae Yang Kim, Keun-Ho Lee, "Information System based Authentication Scheme in Intelligent Vehicles", ICCT2012, pp.282-285, 2012.

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, 융합 보안, 개인정보보호, ISMS(정보보호관리체계), 정보보호사전점검
- E-Mail : root1004@bu.ac.kr