ISSN 2234-4438
중소기업융합학회 논문지 제6권 제4호 pp. 31-36, 2016 DOI : http://dx.doi.org/10.22156/CS4SMB.2016.6.4.031

New Authentication Methods based on User's Behavior Big Data Analysis on Cloud

Sunghyuck Hong*
Baekseok University, Div. Information and Communication

클라우드 환경에서 빅데이터 분석을 통한 새로운 사용자 인증방법에 관한 연구

홍성혁*
백석대학교 정보통신학부

Abstract User authentication is the first step to network security. There are lots of authentication types, and more than one authentication method works together for user's authentication in the network. Except for biometric authentication, most authentication methods can be copied, or someone else can adopt and abuse someone else's credential method. Thus, more than one authentication method must be used for user authentication. However, more credential makes system degrade and inefficient as they log on the system. Therefore, without tradeoff performance with efficiency, this research proposed user's behavior based authentication for secure communication, and it will improve to establish a secure and efficient communication.

Key Words : user behavior, authentication, access control, cloud storage

요 약 사용자 인증은 네트워크 보안하는 첫 번째 단계이다. 인증의 유형은 많이 있으며, 하나 이상의 인증 방식은 네트워크 내의 사용자의 인증을 보다 안전하게 한다. 하지만 생체 인증 제외하고, 대부분의 인증 방법은 복사 할 수 있다. 또한 다른 사람이 타인의 인증을 악용 할 수 있다. 따라서, 하나 이상의 인증 방식은 안전한 인증을 위해 사용되어야한다. 보안을 너무 강조하게 되면 비효율적이기 때문에, 효율적이면서 안전한 시스템을 구축하기 위한 연구가 많이 진행되고 있다. 본 논문은 사용자의 행동에 기초하여 인증 방안을 제시한다. 본 논문에서 제시한 방법은 안전하고 효율적인 통신을 제공하여 클라우드 기반의 모든 시스템에서 사용자 인증에 적용될 수 있으며, 빅데이터 분석을 통한 보다 정확한 사용자 인증을 통해 안전한 통신에 기여할 것으로 기대한다.

키워드 : 사용자 행위, 인증, 접근 제어, 클라우드 저장소

1. Introduction

Authentication is the first step of a security method. After authentication, access control and authorization steps will be established securely. There are three types of authentication1[1]: The first one is that authentication is a first step to prove the proof of its identity which has been given by credible people who can claim who they are. As authentication required to physical objects, this proof is able to be a friend,

Received 2016-09-03 Revised 2016-10-18 Accepted 2016-12-02 Published 2016-12-31
*Corresponding author : Sunghyuck Hong (sunghyuck.hong@gmail.com)

acquaintance, member or peer attesting to the item's origin by getting witnessed the item in its owner's belongings. Authentication is the process of determining what the right thing or the person who actually report (or just those things). Certification of the public network including the Internet or the individual is through the use of a password to log usually. Those who know the password is considered to be one reliable user. However, the weakness of this system is involved in significant transactions, such as money exchange, there is often password or accidentally be known or forgotten or stolen. For this reason, the Internet business and many other transactions require a more stringent to the certification process. The use of public-key based digital proof issued by a certificate authority and verified, part of the structure is becoming a standard way to perform authentication on the Internet. Inevitably, certification is granted to the first (and often even look like the two combined) [2, 3].

The second method is that the authentication is compared with the attribute of the object itself, as known for an object of its origin [3]. For example, art experts have identified the location and type of investigation signature on the similarity of style or painting can be compared to the object in the photo [4,5]. Archaeologists can use carbon dating to compare the style of construction or decoration materials used in chemical analysis to prove the age of the artifacts to other artifacts in performing or similar origin [6]. You can examine the known physical environment and the sound and light as compared Physics audio recordings, photographs, the authenticity of the video [7]. When implied the creation of a document item can be found to have been created in ink or paper immediately available [8].

Password is, by in a way that is most widely used as the user authentication technology to enter information that only the user knows (password), to perform user authentication. This method is the most vulnerable authentication technologies on the simplest, and at the same time security, other users can be prevented can guess the password, which is the most important security. Therefore, at the time of the setting of the password, but difficult others to guess, the person must use an easy-to-remember passwords. Using a secure and strong password, only by changing the cycle of passwords periodically, it is possible to prevent security incidents [6,7,8].

However, password authentication is easy to be exposed [11, 12]. The method of authenticating the user, large, a method of utilizing that the user knows, a method utilizing the fact that the user owns, a method of utilizing the characteristics of a user. The method of utilizing that the user knows, IDs / Password, passphrases, Personal Identification Number, S / Key Canada, include OTP, the method utilizing the fact that the user owns is. The IC card (Smart card), there is a magnetic card (Memory card), the methods utilizing the characteristics of a user, there is authentication method using fingerprints, voice, measuring retinal and biometric features, such as signature operation [9,10].

2. Proposed Work

The behavior analysis of people can verify by principles, which analyzes variables which can influence on people's behavior [12]. For acting scientific analysis of people to determine the dimensions of the event of the characteristics or symptoms, environment, and some knowledge of the event isolation start time and the opportunity to define the resulting changes by the space [10, 11]. Therefore, it will be able to mention that the environment and both the virtual and physical environment establish conditions for a specific behavior9,10. The people's behaviors are based on conceptual information, based on previous behavioral history, the previous history of behavior reinforcement

and conduct of the people to interact with the environment immediately13. Conditioning and conditioning operation until adjusted, so they connect the need for an operation, a mechanism to compensate for the user's response. Operation operating environment changes the likelihood of similar future and change is generate a result of the re-work [7]. Environmental variables in the air conditioning process are a method for modeling behavior of the user [7]. In a similar manner, for a software application, session, user behavior is electrical and electronic devices and software applications and the condition when the mutual function3. According to the law of effect are, people they are connected to people and situations similar experience, generalize the learning process and will expand to the larger context of life [5,9,12]. People tend to repeat the operation in [6] repeating situation. This may be considered the application of the other10 in the context of a person authentication system and security. When a person is identified and access to the software applications with hours of capture user behavior information in an environment when the user is close a, it is carried out in time [11].

According to basic authentication methods[7], there are 4 types of authentication which are password-based, software-based, hardware-based and biometric-based authentication. Basic factors in the authentication can be an authenticator, an authentication mechanism, or the environment. The overview of the authentication systems is in Table 1.

Table 1. Authentication System

Authentication Element	Passwordbased Authentication	Softwarebased Authentication	Hardwarebased Authentication	Biometricbased Authentication
Authenticator	Password	Certificate	Secure Card	Biometric information
Authentication Mechanism	Password Validation Software	Certificate Validation Software	Card Validation Software	Biometric Recognition Device
Environment	Client-Server	Web-based Client-Server / Multicast	Client-Server	Client-Server

2.1 Software based key authentication

Not only the recent e-commerce, in order to provide a reliable online system over the main pillar industries and the service sector, such as government and health care, the task of trying to establish a public key infrastructure has been promoted to worldwide. Public Key Infrastructure of wired present is a situation which has been promoted around the X.509 of ITU-T. Recently, in mutual research has been conducted for interlocking, discussed in terms of the technical aspects and the business model and legal elements is proceeding situation between countries with different public key infrastructure structure is there. Furthermore, studies have been conducted of the authentication method for a wireless environment, have been proposed a method in consideration of a wireless environment, such as WTLS, research has been actively conducted. One is a certified mediation, and the other is directly certified. Mediation Certification There are two types of symmetric and asymmetric encryption. A symmetric encryption scheme Nideom Schroeder protocol [12] and Kerberos authentication scheme. Asymmetric cryptography is Denning-Sacco protocol, Woo-Lam protocol, and the international standard X.509 (ITU-T 1993)which is basedupon a key certificate, and it does not need online participation of a Trust Third Party (TTP).

2.2 Changes in a member's biometric data and environment

Recent human fingerprint, face, voice, iris, vein such as the specific physical characteristics and the signature, the new identity authentication system because of the excellent safety of biometrics technology to the field of use of the behavioral characteristics, such as how to walk for identification and authentication. It is the considerable attention as. Bio-recognition systems, the users themselves are divided on the recognition that the user find out who the in the authentication and the database, which is confirmed to be his. Recognition technology that uses

a single bio-information, in an ideal environment, but you deserve to trust, in a real situation, there is a disadvantage that the environment is very sensitive. As an example, the speech recognition is the noise environment, rapid recognition rate is lowered, face recognition also illumination intensity and direction, greatly affected by the user's pose. An attempt to overcome these limitations of a single bio-recognition, research relating to a plurality of bio-recognition to provide a complement each other by using the integration of different types of bio-recognition technology has been actively promoted. Fusion of two or more single bio recognition systems, there are to occur in several stages, it can be divided into the stage of the three fusion, and fusion at the feature extraction stage of fusing data obtained from the sensor and a feature vector, and fused at the stage of the matching score for fusing outputter matching score from each of a single biometric matching module, respectively there is a fusion of a single decision stage to fuse has been approved or rejected decision output from bio-metric determination module.

2.3 Security problems in biometric authentication system

Bio-authentication information usually is the data to be centralized to be stored in the database, the database at the time of the bio authentication. Compared with the bio-data stored in the database, perform authentication

It will be bio-authentication database intrusion. The risk of a large amount of outflow is exposure. It can be information about the bio-authentication database. Protection can be assumed to be very important.

Spoofing attack: In biometrics authentication system, spoofing is a process that cheats a biometric system by providing altered biometric copy of a legal user, for example by using a fake finger, altering a high-resolution iris image, or providing a facemask which put on a someone's face.

Template attack: This is difficult to prevent due to physical attack. It is also modifying, stealing, or adding he template in a self-contained device, or directly on the sensor, local machine, or central database with a physical approach.

To prohibit these two attacks, several counter attack techniques have been developed in hardware and software. One method of counter measure attack is called liveness test that detects physical properties of the live biometric such as electrical, thermal, moisture, and reflection measurements on the surface. However, the biometric information system is not attack free system all time. Thus, the security problem should be resolved shortly.

2.4 Privacy issues

There are various user authentication methods. However, they all have pros and corns. This research paper focuses on efficient user authentication methods [12-15].

Therefore, confidentiality should not affect the availability of the system. Users' behaviors can be predictable because people use user names. For example, access time and access location can be a unique pattern. Therefore, user's behaviors can be the most efficient user authentication method if the system has lots of collects user's pattern logos. Location-based

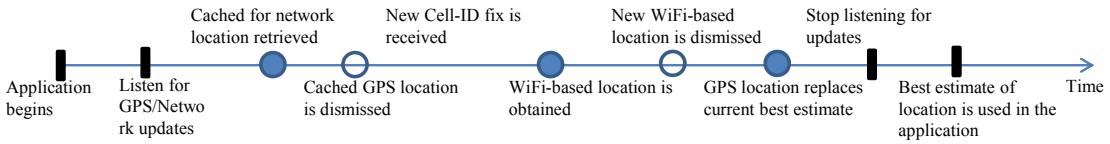

Fig. 1. A timeline in which an application listens for location updates.

applications are now commonly used. To overcome the barriers of obtaining a legitimate user's physical location while preserving battery power, the user should define a consistent model that specifies how your application obtains the user location. This model includes when you start and stop listening for updates and when to use cached location data.

3. Proposed Authentication Method

3.1 Flow on obtaining user location

Here's the typical flow of process for getting the user's physical location:

····· Start application with setting GPS on

Sometime later, start listening for updates from desired location ISPs

Managing a "current best estimate" of location by filtering out.

····· Stop listening for updating location

····· Take the advantage of last best location

Fig. 1 shows this model in a timeline how to work and how to collect the physical user's GPS data [13].

```
#Geocoding a location using
#implement My_Geocoder_View_Controller (Custom_Geocoding_Additions)
(void)geocodeLocation:(CL_Location*) location for Annotation:(Map_Location*)
annotation
{
    if (!geocoder)
        geocoder = [[CL_Geocoder alloc] init];

    [geocoder reverse_Geocode_Location:location completion Handler:
        ^ ( NSArray * placemarks, NSError * error)
{
            if ([placemarks count] > 0)
            {
                annotation.placemark = [placemarks objectAtIndex:0];


                MKPinAnnotationView* view = (MKPinAnnotationView*)[map
viewForAnnotation:annotation];
                if (view && (view.rightCalloutAccessoryView == NULL))
                {
                    view.canShowCallout = Yes;
                    view.rightCalloutAccessoryView = [UIButton
buttonWithType:UIButtonTypeDetailDisclosure];
                }
}];
```

Fig. 2. Geocoding a location using CL_Geocoder

Figure 2 shows geocoding a location using CL_Geocoder [13]. The corn of using a block object in a sample like this is that information can be easily returned and used as the part of the completion handler. Without blocks, the process of wrangling data variables becomes more complicated.

4. Conclusion

Relatively weak compared to the PC and mobile devices adopt a general-purpose OS, due to the advent of the App Store, an open platform based on the full-fledged competitive smartphone market with increased security technologies, applying the characteristics of the mobile network, in particular with regard to the mobile user authentication actively the purpose of this study is to contribute to mobile networks, secure communication and enable research realized by a secure mobile network authentication, the authentication of mobile users by leveraging the mobility characteristics of the mobile is used as a certification because it has not been sufficiently studied. Therefore, this research contributes to establish an efficient and secure and user authentication by user's behavior such as user's physical location.

ACKNOWLEDGMENTS

이 논문은 2016학년도 백석대학교 대학연구비에 의하여 수행된 것임

REFERENCES

[1] D. G. Kim and I. G. Song, "Need and Development of u-Healthcare Service," *Journal of Korean Society for Internet Information*, Vol. 1, No. 3, pp. 9-17, Sep. 2009.

[2] H. J. Mun, Y. C. Hwang, H. Y. Kim, "Countermeasure for Prevention and Detection against Attacks to SMB Information System - A Survey," *Journal of the*

Convergence Society for SMB, Vol. 5, No. 2, pp. 1-6, Jun. 2015.

[3] Y. Xie and S. Z. YU, "Anomaly detection based on web users' browsing behaviors," *Journal of Software*, Vol. 18, No. 4, pp. 967-977, Apr. 2007.

[4] B. Tams and C. Rathgeb, "Towards efficient privacy-preserving two-stage identification for fingerprint-based biometric cryptosystems," *Proceedings of the 2014 IEEE International Joint Conference on Biometrics (IJCB)*, pp .1-8, 2014.

[5] B. S. Abhilasha, A. Squicciarini and E. Bertino, "Privacy Preserving Multi-Factor Authentication with Biometrics," *Proceedings of the second ACM workshop on Digital identity*, pp. 63-72, 2006.

[6] C. L. Lin and T. Hwang, "A password authentication Scheme with Secure Password Updating," *Journal of Computers & Security*, Vol. 22, No. 1, pp .68-72, Jan. 2003.

[7] Liqin T, Chuang L,' Yang N., "Evaluation of user behavior trust in cloud computing," *Proceedings of the 2010 International Conference on Computer Application and System Modeling (ICCASM 2010)*, pp. 567-572, 2010.

[8] T. Chattopadhyay, P. Biswas, B. Saha and A. Pal, "Gesture Based English Character Recognition for Human Machine Interaction in Interactive Set Top Box Using Multi-factor Analysis," *Proceedings of the Sixth Indian Conference on Computer Vision, Graphics & Image Processing Computer Vision, Graphics & Image Processing, 2008(ICVGIP '08)*, pp. 134-141, 2008.

[9] Li C T, Hwang M S., "An Efficient Biometrics-Based Remote User Authentication Scheme Using Smart Cards," J. Network and Computer Applications, Vol. 33, No. 1, pp. 1-5, 2010.

[10] R. Ramasamy, A. P. Muniyandi, "New Remote Mutual Authentication Scheme using Smart Cards," *Journal of Transactions on Data Privacy*, Vol. 2, No. 2, pp. 141-152, Aug. 2009.

[11] J. Ze, L. Shuangqing and Y. Chengguo, "Evaluating network user behavior trust based on multiple decisions attributes", *Journal of Application Research of Computers*, Vol. 28, No. 6, pp. 2289-2293, Jun. 2011.

[12] C. H. Liao, H. C. Chen and C. T. Wang, "An Exquisite Mutual Authentication Scheme with Key Agreement Using Smart Card", *Journal of Informatica*, Vol. 33, No. 2, pp. 125-132, May. 2009.

[13] Developer, "Android Developer Guide," https://developer.android.com/guide/topics/location/strategies.html#Challenges, 2016. 4

[15] S. H. Hong and Y. J. Seo, "Countermeasure of Sniffing Attack: Survey", *Journal of Convergence Society for SMB*, Vol. 6, No. 2, pp. 31-36, Jun. 2016

[15] H. J. Mun, G. H. Choi and Y. C. Hwang, "Countermeasure to Underlying Security Threats in IoT communication", *Journal of Convergence Society for SMB*, Vol. 6, No. 2, pp. 37-44, Jun. 2016.

저 자 소 개

Sunghyuck Hong [Regular member]

- Aug, 2007: Texas Tech University, Computer Science (Ph.D)
- Sept, 2007~Feb, 2012: Senior Programmer, Texas Tech University, Office of International Affairs
- March, 2012 ~ Present : Associate Professor at Baekseok University

<Research Interests> : Network Security, Hacking, Anti-fishing technology