The Scheme of 3-Level Authentication Mechanism for Preventing Internal Information Leakage

Sang-Pil Cheon
Dept. of Military Studies
Daejeon University
Daejeon, Republic of Korea
skyfeel69202@naver.com

Jung-Min Kang
Dept. of Military Studies
Daejeon University
Daejeon, Republic of Korea
flytothe-jm@nate.com

Min-Woo Park
Department of Electrical and Computer Engineering
Sungkyunkwan University
Suwon, Republic of Korea
mwpark@imtl.skku.ac.kr

Jung-Ho Eom*
Dept. of Military Studies
Daejeon University
Daejeon, Republic of Korea
eomhun@gmail.com

Abstract—**In this paper, we proposed 3-level authentication technique to prevent internal information leakage in network system. When system authenticates users, it requires user's ID&P/W firstly. Then, it requires a secondary authentication component to check whether he/she is legitimate user. By doing so, it can implement a more robust authentication system. The secondary authentication components are usually a security card, an encryption key and bio-information such as iris, face, fingerprint etc. But there is a problem related to ID&P/W exposure and bio-information copy. Especially, nobody knows can check whether ID&P/W are exposed, whether bio-information is copied. So, we propose another authentication way using biometric signals. A biometric signal is essentially a pattern recognition factor that operates by acquiring biometric signals from an individual, extracting a feature set from the acquired signal pattern, and comparing this feature set against the template set in the database. We decided to use skin conductivity in the biometric signals as 3rd authentication element. The skin conductivity is used as an indication of psychological or physiological arousal. So, there is no risk because it never exposes or copies.**

Keywords*— *authentication, biometrics, information leakage

I. INTRODUCTION

2012 cyber security watch survey [1] said that 51% of respondents answered damage caused by insider attacks more damaging than outsider attacks. Top-10 guide for protecting sensitive data from malicious insiders [2] also said that database security is one of the most important areas for critical data protection from insiders because it saves the attractive data insiders want. Insiders are capable of saving data in USB memory stick and their portable disk, and they can illegally use the data for people who need it. Most security techniques are focused on detects information leakage from outside, not necessarily by insiders. When user tries to access database, system checks user's identity. It is an authentication. Authentication techniques prevent forgery and unauthorized access as well as identity check. In the first, the common authentication approach is the use of passwords. But, as password has been used for a long time, it is possible to copy by hacker [3]. In that order, smart card appears to resolve security problem of password in a secondary authentication techniques. This also proved to be vulnerable to attack impersonation attack [4]. Nowadays, we are using human factors as reliable authentication components. Human factors include iris, face, fingerprint, etc. Authentication by biometric information is automated method of verifying or identifying the identity of user physical characteristics [5]. Recently, an authentication mechanism using biometric signals is actively researching. When a hacker tries to access in the database saved critical information for the purpose of internal information leakage, even if he/she requests to access permission with the stolen user's ID&P/W and copied biometric information, it is denied by user's biometric signals. A biometric signal is a pattern recognition that uniquely identifies humans based on their physiological traits. So, no anybody can copy them. In the paper, we use these characteristics to authentication mechanism. We also focus on insider authentication because internal information leakage by insider has increased.

In section 2, we explain the related works, and present 3-level authentication mechanism in section 3. We conclude in section 4.

II. RELATED WORKS

A. The aspects of internal information leakage

Insiders can access database with legitimate access authorization. When insiders misuse their authorization to leak internal information from database, it is not easy to detect his/her behavioral anomalies. Internal information leakage caused by insiders is considered the most critical risk to organization. The reason of information leakage by insiders is that they have a legitimate access authorization to database and can bypass logical & physical security systems. And they know well ID&P/W to log-in at database, security systems and the main location of sensitive data.

Recently, in Korea, three of the country's major credit card firms are stolen personal information of tens of millions of their customers. The thief was authorized by the firms to access the database. He accessed the card firm's network system and simply copied the data to a USB stick when he

* He is a correspondent author.

ISBN: 978-1-4799-3724-0/14/$31.00 ©2014 IEEE

worked as a dispatch duty in 3 card firms. The following table shows the examples of data leakage by insiders in Republic of Korea[6].

TABLE 1. THE LEAKAGE CASES OF INTERNAL INFORMATION

Date	Financial company	Criminal	Leakage Information	Path
Apr. 2013	Citibank	Local Employee	Personal information of 34,000 users	Printed Paper
Feb. 2012	Standard chartered Bank	Subcontractor employee	Personal information of 100,000 users	Access database
Feb. 2012	Meritz Fire & Marine Insurance	Employee	Personal information of 164,000 users	E-mail and USB
June 2011	NH NongHyup Securities		Personal information of 15,000 users	Program Error
May 2011	Leading Investment & Securities	Hacker	Personal information of 12,000 users	Homepage hacking
Mar. 2011	Hanwha Life Insurance	Hacker	Personal information of 150,000 users	Homepage hacking

It is difficult to predict internal information leakage by insider because it happened by insider with legitimate access authorization. Also, information leakage by insider can't be detected accurately because it is not easy to perceive it. The path of information leakage by insiders is variable as following figure[7].

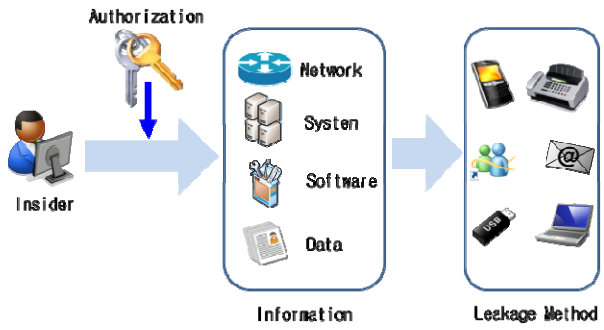

Figure 1. The path of informtaion leakage by insiders

B. Biometrics information security

A system using biometrics information provides an automated technique of identifying an individual based on his/her biometric traits. Biometrics are a unique, measurable a trait of a human being for automatically recognizing or verifying identity. The types of biometrics commonly include face, iris, retina, fingerprint, voice, signature, vein pattern, and hand geometry [8-10]. The existing security systems used at companies are using ID&P/W for an individual identification. For more powerful security configuration, double authentication provide by using any one of the biometrics information. The biometric security systems offer several advantages. The information security gives the protection of information ensuring only authorized users can access the database stored needed information. Authentication method using biometrics information is more secure system because it provides a more reliable than traditional authentication method. They are used to access control in physical security like building, gate, office, and so on.

A biometric security system is essentially individual characteristics recognition system that operates by extracting biometric data from a person, and compares these characteristics set with the template set in the database. A biometric system operates in a simple manner as following figure 2 [9,10].

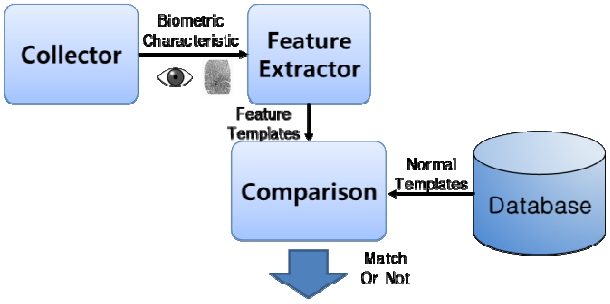

Figure 2. Biometric Security System

The collector collects biometric characteristics using any sensors. The feature extractor converts biometric characteristics into feature templates for next comparison step. And then new feature template is compared with stored templates in a database. If new feature template is matched with stored individual templates in a database, it permits user's requested actions [11].

III. 3-LEVEL AUTHENTICATION MECHANISM

A. 3-level authentication process

Biometrics security systems are limited to the authentication system because it has disadvantage. Firstly, it is the false rejection rate. It is the probability that the system fails to match between the input template and a normal template in the database. Secondly, it is impossible that all biometrics always keep a normal condition. For example, it is difficult to keep a normal condition if human eats the food before sleeping. Some biometric information collection sensors have a limited function. Lastly, biometric security systems may violate user's privacy because biometric characteristics contain much personal information [8].

We used biometric signals to decide insider's conditions when he/she access critical information in database. As 3rd authentication process, it determines whether he/she performs a normal operation. If he/she is performing a normal work, biometric signals will be in the ordinary boundary. If he/she is performing abnormal work, biometric signals will be out of

ISBN: 978-1-4799-3724-0/14/$31.00 ©2014 IEEE

ordinary boundary. The reason is that biometric signals are closely associated with emotion recognition. When insider does unusual behavior, insider's biometric signals change because insider represents emotions such as anxiety, agitation, and tension. In this paper, we skin conductivity to identify the emotion changes.

Skin conductivity is the electrical conductance of the skin, which varies with skin moisture. It can be seen the level of skin moisture by the response for stimulation occurred in the skin. Thus, skin conductivity is used as an indication of psychological or physiological arousal. By Ahyoung Choi's paper[12] 'Feature extraction for emotion analysis based on physiological signal', when the emotion change is recognized, technique using the skin conductivity has the effectiveness 87.5% or 98%.

Our proposed 3-level authentication process is as follow figure 3.

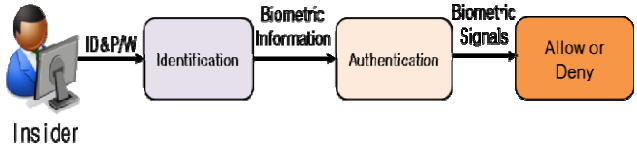

Figure 3. 3-level authentication process

Insider enters his/her ID&P/W when he/she access to company network system. Next step, insider sends his/her biometric information for access server stored critical data to authentication server. Last step, when insider tries to operate on critical data, security system checks insider's biometric signal in this time. If measured biometric signal is within the normal boundary, insider's requested operation will be allowed.

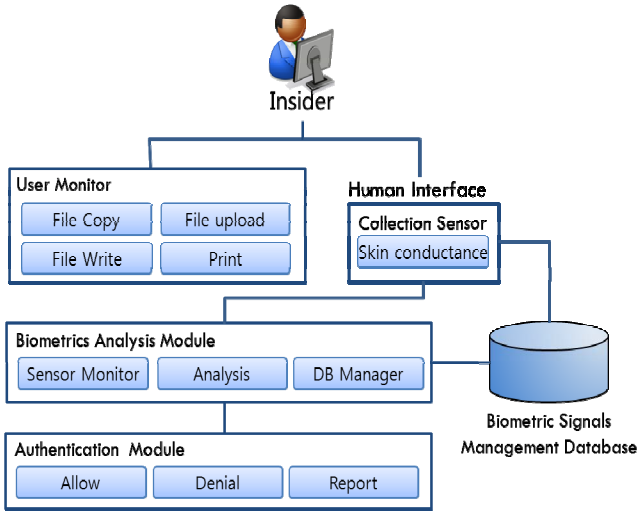

Figure 4. Authentication mechaniam using biometric signals

Our proposed authentication mechanism is a security-enhanced authentication system using biometric signals. A 3-level authentication system using biometric signals offers more reliability over traditional authentication systems because of unique biometric signal characteristics.

The concept of proposed 3-level authentication mechanism is as above figure 4. It monitors insider's biometric signals when he/she tries to operate a critical data in database, and compares measured insider's biometric signals in real time with stored the normal boundary of biometric signals in biometric signals management database. If measured value of biometric signals is out of normal boundary, system checks the status of insider's operation. If the change of biometric signals relates to insider's abnormal behavior, it alerts to security manager, and deny requested operation.

Our proposed system composes of user monitor, biometrics analysis module, authentication module, human interface, and biometric signals management database.

- User monitor: monitors behaviors related to data leakage such as critical data copy, uploading, and prints, etc. Critical data are determined by the security policy, and monitoring is done by hooking the main system call.

- Human interface: input devices that attached sensors to collect insider's biometric signals. Collection sensor periodically measure insider's skin conductivity. It sends measured value to biometrics analysis module. If biometrics analysis module requests the measured value, collection sensor immediately measures insider's biometric signals and report it to sensor manager in biometrics analysis module.

- Biometrics analysis module: detects suspicious behavior as comparing and analyzing the collected value of insider's skin conductivity with his/her normal values stored in a database when received the value of skin conductivity from human interface. It performs the 3 functions such as sensor monitor, analysis, and D/B manager. A sensor monitor periodically calls insider's the value of skin conductivity by human interface, and generates the normal values of skin conductivity after collected insider's skin conductivity for some months. An analysis function compares the values of skin conductivity received from sensor monitor with insider's normal values in database, and if the value of collected skin conductivity is out of normal boundary, it determines the probability of data leakage. D/B manager manages and decides the normal values of insider's skin conductivity, using data stored in database as the initial value. If there is no data stored in biometric signals management database, it measures the value of insider's skin conductivity to set normal value.

- Authentication module: determines whether insider requested operation will allow or not. The change of insider's skin conductivity is used as an indicator for identifying the potential data leakage. If it receives that the measured value is different from the normal value of skin conductivity from biometrics analysis module, it rejects the operation requested by an insider. And then, it reports to security manager.

- Biometric signals management database: stores the normal value of insider's skin conductivity and normal boundary of insider's skin conductivity changes regulated leakage possibility.

ISBN: 978-1-4799-3724-0/14/$31.00 ©2014 IEEE

IV. CONCLUSION

In this paper, we proposed 3-level authentication mechanism using biometric signals. Insider enters his/her ID&P/W when he/she access to company network system. Next step, insider sends his/her biometric information for accessing server stored critical data to authentication server. Last step, when insider tries to operate on critical data, third authentication mechanism using biometrics signal detects abnormal behavior of insider. In other words, we applied insider's unique biometric signals to authentication mechanism which detects whether he/she tries to leak internal critical information illegally.

Our proposed authentication mechanism monitors insider's skin conductivity when he/she tries to operate a critical data in database, and compares measured insider's skin conductivity in real time with stored the acceptable boundary of skin conductivity in biometric signals management database. If measured value of skin conductivity is out of acceptable boundary, system checks the status of insider's operation and alerts to security manager, and then denies requested operation.

In future, we will consider adding other biometrics signals to third authentication elements for improving FAR(False Accept Rate) and FRR(False Reject Rate).

REFERENCES

[1] Carnegie Mellon University, "2012 Cyber Security Watch Survey", Sof. Eng. Ins., 2013.

[2] "Top-10 Guide for Protecting Sensitive Data from Malicious Insiders", Imperva White Paper, iMPERVA, 2009.

[3] Wen-Her Yang and Shiuh-Pyng Shieh, "Passowrd Authentication Schemes with Smart Cards", Elsevier Computers & Security, vol.18, No.8, pp.727-733, 1999.

[4] Eun-Jun Yoon, "Cryptanalysis of RSA based Password Authentication Scheme with Smart Card", the proceedings of IEIE summer conference, Vol.35. No.1, pp.866-869, 2012.

[5] James Wayman,et. al, "An Introduction to Biometric Authentication Systems", Springer Biometric System, pp.1-20, 2005

[6] Jung ho Eom, "The Quantitative Evaluation of a Level of Insider Activity using SFI Analysis Techniques", Journal of Security Engineering, Vol.10. No.2, pp.113-122, 2013.

[7] Jung ho Eom, Nam uk Kim, Sung hwan Kim and Tai Myoung Chung, "An Architecture of Document Control System for Blocking Information Leakage in Military Information System" International Journal of Security and Its Applications, Vol.6 No.2, pp.109-114, 2012.

[8] Reetu Awasthi and R.A.Ingolikar, "A Study of Biometrics Security System", International Journal of Innovative Research & Development, Vol.2, Issue 4, pp.737-760, 2013.

[9] Neha Dahiya and Chander Kant, "Biometrics Security Concerns, A proceeding of Second International Conference on Advanced Computing & Communication Technologies, IEEE, Press, pp.297-302, 2012.

[10] "Biometrics Security Considerations", System and Network Analysis Center Information, Assurance Directorate, www.nsa.gov/snac.

[11] Jong Yeol, Kim, "A study on a Reinforced Certification Technique Using an Accredited Certificate and Bioinformation", Master's thesis, Graduate School of Information Sciences Soongsil University, 2012.

[12] Ahyoung Choi and Woontack Woo, "Feature extraction for emotion analysis based on physiological signal", the proceedings of 2005 Korea HCI conference, pp.624-629, 2005.

ISBN: 978-1-4799-3724-0/14/$31.00 ©2014 IEEE