Advanced Science and Technology Letters
Vol.63 (NT 2014), pp.1-5
http://dx.doi.org/10.14257/astl.2014.63.01

An Application of Data Leakage Prevention System based on Biometrics Signals Recognition Technology

Hojae Lee[1], Junkwon Jung[1], Taeyoung Kim[1], Minwoo Park[1], Jungho Eom[2*], and T. M Chung[1]

[1] Department of Computer Engineering,
School of Information and Communication Engineering,
Sungkyunkwan University, Suwon-si, Republic of Korea
hjlee72@gmail.com, {jkjung, tykim, mwpark}@imtl.skku.ac.kr, tmchung@ece.skku.ac.kr
[2] Military Studies, Daejeon University,
62 Daehakro, Dong-Gu, Daejeon, Republic of Korea
eomhun@gmail.com

Abstract. In this study, we researched internal information leakage prevention system by insiders based on biometrics signals recognition technology. We turned attention to the attack subject as detection target. We focused on the insider's the change of biometrics signals when they try to conduct unusual behavior. In other words, we applied biometrics signals recognition technology to detection algorithm. When Insider tries to leak internal information, they may seem the unusual changes of biometrics signals such as pulse, electrocardiogram, and skin conductivity. We demonstrated our proposed system by a 'BioGraph Infiniti' program.

Keywords: Detection; Insider Threat; Biometrics Signals

1 Introduction

We tried to apply the new approach to detection system, unlike conventional detection method. We focused on human biometrics signals that represent human's unique characteristics. They are changed when human conducts unusual thoughts or behavior. In other words, we applied biometrics signals recognition technology like a polygraph [1] to anomaly detection algorithm. When insider tries to leak critical data in the database, he/she may seem abnormal emotional condition such as tension, agitation, anxiety and so on. It could be detected by biometrics signals such as pulse, electrocardiogram, and skin conductivity. This paper is expanded and detailed from Jungho Eom et al, 'An Architecture of Emotional Recognition Based Internal Information Leakage Prevention System [2]. We sufficiently explained the related works. So, we will skip the related works in this paper.

* *Corresponding Author*

ISSN: 2287-1233 ASTL

In this paper, we will explain architecture of proposed system in Section 2, and describe the application of data leakage prevention system using user's biometrics signals in Section 3. And we conclude in the last section.

2 Data Leakage Prevention System based on Biometrics Signals Recognition Technology

2.1 Biometrics Signals

According to the general emotion classification of psychologists, they are classified into joy, sadness, anger, surprise, and fear disgust. Thy could be distinguished by biometrics signals such as brain waves, pulse, EEG(Electroencephalography), voice, and skin conductivity etc. Biometrics signal is a natural, unique feature and an important physiological characteristic in the human body. It is difficult to replicate or imitate because it can collect from only inside of human body in real time. In this paper, we will select emotional recognition elements which have proven effectiveness in polygraph technique and previous researches [3].

Up to now, the biometrics is commonly used to identify and authenticate humans because it provides a more reliable authentication than traditional authentication elements such as P/W, ID cards, and keys. It is also used to control access to physical assets or logical data. A biometrics system is essentially a personality recognition system that operates by extracting biometric data from an individual, and compares this personality set with the template set in the database.

2.2 Design of Data Leakage Prevention System

Our proposed security system is a data leakage prevention system based on biometrics signals recognition technology. Our proposal was conceived from a polygraph technique and an authentication system using biometrics. A polygraph technique [4] records the change values of biometrical signals such as blood pressure, pulses, skin conductance, and reflex due to the fear which detection may be come out when human deliberately attempt to lie. It is composed of biometrics signals recognition based prevention system that is installed on the user's PC, security manager that manages the security policy of internal system, and human interface that is input device attached sensors for collecting insider's biometrics signals.

Biometrics signals recognition based prevention system is a core part that analyzes insider's biometrics state based on insider's biometrics signals collected from sensors, and determines the possibility of information leakage. It is composed of a detection system and a countermeasure module. A detection system monitors the changes of insider's biometrics signals during he/she works, and identifies an unusually rapid

change. It is composed of user behavior monitor, authentication module, biometrics signals recognition module, and local biometrics signals recognition database.

- Insider behavior monitor: monitors actions related to data leakage such as sensitive files copy, uploading, sending mail attachments and prints, etc.
- Authentication module: authenticate insider with authentication tools before user does any action on a sensitive file. Insider can access to sensitive files after authenticating by the authentication process.
- Biometrics signals recognition module: detects anomalous behavior as comparing and analyzing the change values of collected insider's biometrics signals with his/her normal (average) values saved in a database when received biometrics signals from human interface.
- Local biometrics signals recognition database: stores the value of insider's biometrics signals received from human interface while insider performs a task.

Countermeasure module defenses the insider anomalous behaviors related to data leakage with response method such as alert, service delay and block according to the risk degree. Security manager consists of two databases such as a security policy database and a main biometrics signals database. The former is stored user information related to insider security guideline, rule, and policy. The latter is stored the value of insider's normal (or average) biometrics signals and threshold of biometrics signals change regulated leakage possibility. Human interface is input devices that attached sensors to collect insider's biometrics signals. Sensors periodically measure insider's pulse, temperature, and skin conductivity

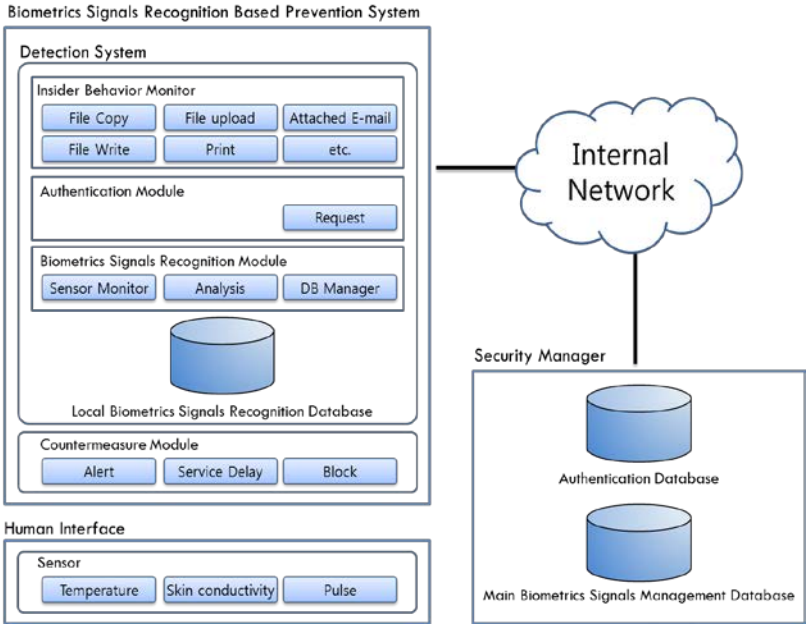

Fig. 1. The Architecture of Data Leakage Prevention System

3 Application

We will show the detection process of insider's anomalous behaviors as using biometrics signals measuring system that is a 'BioGraph Infiniti' program used in [5]. This system measures user's biometrics signals such as HRV (Heart Rate Variability), a core body temperature, and a skin temperature. We measured the change of the test subject's biometrics signals during he watches a horror movie. In other words, we observed the change of the test subject's biometrics signals when he/she suddenly watches a dreadful scene in a horror movie. Figure 2 shows the test results.

Fig. 2. The measurement results of the test subject's biometric signals

In above figure, first graph describes HR (Heart Rate), two graphs of second step describe HR variance (left) and HR average (right). A third graph shows a core body temperature (upper) and a skin temperature (under). A last graph shows temperature subtraction between a core body temperature and a skin temperature. In this paper, we use a graph of heart rate to identify the change of biometrics signals. Figure 3 shows the change in HR of the test subject when a dreadful scene suddenly emerges from horror movie.

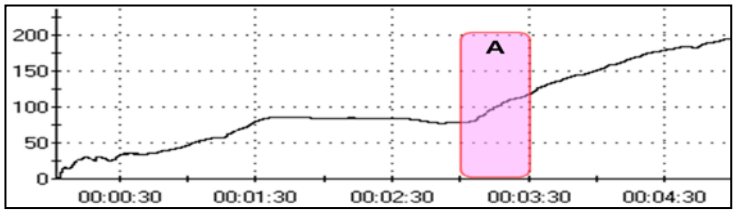

Fig. 3. The Change of HR

In figure 3, the change of the test subject's HR started to happen in three minutes later. The test subject felt a sense of fear when scary scene emerges from horror movies around the three minutes, and biometrics signals was accordingly reacted at that time. In this study, we knew attributes that an insider's psychological state is identified by the change of biometrics signals.

The 'BigGraph Infiniti' sensor is very sensitive to the movement of the test subject because it is used to check the health condition of the patients. So, motion tolerance sensor, which is not sensitive to user's action, is needed for our proposed system. If noise occurs, filtering technology could remove the unusable value is required. This part is needed for the ongoing research in this study.

4 Conclusion

In this paper, we proposed a real-time data leakage prevention system based on biometrics signals recognition technology. We applied insider's biometrics signals to a detection mechanism. When insider performs anomalous behavior to sensitive data, the change of biometrics signals occur. In other words, we applied the change of biometrics signals to detection algorithm.

Proposed system is composed of biometrics signals recognition based data leakage prevention system that is installed on the user's PC, security manager that manages the security policy of internal all systems, and human interface that is sensors attached input device for measuring insider's biometrics signals.

In future, we have to solve the problem of the biometrics signals collection sensor.

Acknowledgments. This paper is an expanded version of a paper entitled [An Architecture of Emotional Recognition Based Internal Information Leakage Prevention System] presented at [SUComS 2013, Poland and 14~17 Aug.].

References

1. Byoung Sun Cho : Lie detector : J. Notice, Vol.549, pp.5-16 (2002)
2. Jungho Eom, Seunhyun Lee, Junkwon Jung, Minwoo Park, TaiMyoung Chung : An Architecture of Emotional Recognition Based Internal Information Leakage Prevention System In : The 4th International conference on Security-enriched Urban Computing and Smart Grid, pp.60-63, (2013)
3. Kim Hyun, Heo Chang-Wook, Choi Jun-Hyung : Evaluation of Reliability of the Emotional Function Mouse : J. the Korean Society of Jungshin Science, Vol.5 No.1, pp.28~36 (2001)
4. Byoung Sun Cho : Lie detector : J. Notice, Vol.549, pp.5-16 (2002)
5. Jung ho Eom, et al : Application of pilot's biomedical signals for safety management : ROKAF Research Report, pp.18-19 (2013)

