International Journal of Bio-Science and Bio-Technology
Vol.5, No.5 (2013), pp. 187-196
http://dx.doi.org/10.14257/ijbsbt.2013.5.5.20

PDT-BI: Proactive Detection Technology based on the Biometric Information for Preventing Internal Information Leakage

Seung-Hyun Lee[1], Min-Woo Park[1], Jung-Ho Eom[2*] and Tai-Myoung Chung[3]

[1]*Dept. Electrical and Computer Engineering, Sungkyunkwan Univ, Suwon, Republic of Korea*
[2]*Dept. Military Studies, Daejeon Univ, Daejeon, Republic of Korea*
[3]*School of Information Communication Engineering, Sungkyunkwan Univ, Suwon, Republic of Korea*
{shlee87, mwpark, jheom}@imtl.skku.ac.kr, tmchung@ece.skku

Abstract

National Industrial Security Center of National Intelligence Service has announced that information leakages by insiders occurred at the total of 294 cases during the last 8 years. Difficulty of acquiring omen of a security incident and the fact that insiders usually have legitimate privileges make prevent security defense. Therefore, we need to research about developing methods to obtain factors for prediction of information leakage by insiders in a whole new different perspective. When an insider tries to do something malicious, biometric information of the body changes due to tension. This means that biometric information can be used as factor for detecting malicious activities of an insider. In this paper, we propose the proactive detection technique that can detect malicious behaviors of an insider by biometric information. Additionally, we compare proposed technique with other techniques that use biometric information in the security field.

Keywords: *Biometric Information, Proactive Detection, Internal Information Leakage*

1. Introduction

With the development of IT technology, the information in cyberspace became very diverse and valuable. Moreover, people can collect and share the information as they want to in anywhere, at anytime. Accordingly, life has become very convenient through IT technology. IT technology is applied in variety of fields such as education, health, and other areas of human life. However, as information gets valuable and accessibility of IT technologies increase, disclosure of critical business and personal information through malicious activities has increased. Among such increasing malicious acts, 'Cyber Security Watch Survey' announced that information leakage by an insider has increased from 21% in 2011 to 24% in 2012[1]. In addition, National Industrial Security Center of National Intelligence Service announced that in the last eight years total of 294 cases of insider information leakage have occurred [2]. With a rise of the number of information leakages by insiders, the society began to the internal information security technology. Incident by an insider who is knowing confidential information is more critical than other security incident. Corporation usually uses Data Leak Protection (DLP) or Digital Rights Management(DRM) solution to defend against information leakage by insiders[3, 4]. Such solutions detect

* He is corresponding author of this paper.

ISSN: 2233-7849 IJBSBT

network transmission of internal data or encrypt valuable data to protect the actual information against adversaries. However, these solutions cannot detect and terminate information leakage in the real time or prevent such information leakage before it actually occurs. Therefore existing solutions are not appropriate for preventing information leakages by an insider. Thus, we need security techniques that are able to detect information leakage by an insider before it occurs and to prevent information leakages in advance.

In this paper, we propose an information leakage prevention system based on biometric information and explain the system architecture. We also describe the effectiveness of the biometric factors used in the system and provide a survey of related works with regard to systems using biometric information. Finally, we will evaluate the proposed system comparing to other biometric information based systems.

2. Demand and Effectiveness of a Security Technique based on Biometric Information

2.1. Demand of Proactive Detection Technique based on Biometric Information

Recently, as increasing damage by information leakage, security technologies for protecting internal information is becoming important. The security incident by an insider is difficult to prevent, and when it occurs, it results in massive damage. Therefore, to detect and countermeasure against information leakage by insiders in advance is an important security issue. However, factors for predicting such incidents are very limited because a malicious insider also has appropriate privileges. It is difficult to detect information leakage in terms of access control. Moreover, as companies started deploying IT technologies, data copy and modification became much easier than the past and the possibility of information leakage is higher. In fact, rate of information leakages by insiders is increasing. Figure 1 displays number of corporate information leakage by insider [2]. Figure 2 shows percentage of people who leaked confidential information in the last 5 years. 60 percentages among them were former employees, and current employees were up to 20 percentages. Employees of cooperative company were 12 percentages [1]. It can be said that the approximate 92 percentages of the cases were happened by former or current employees.

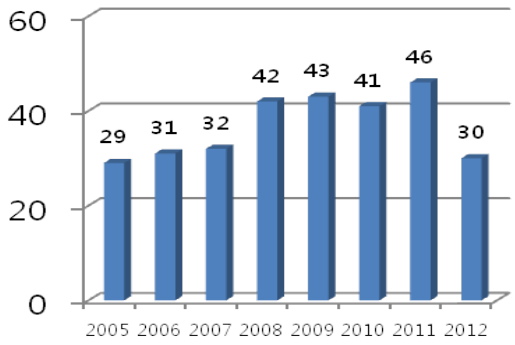

Figure 1. The Number of Information Leakage by an Insider in Korea

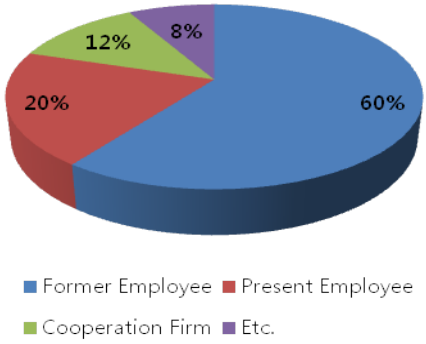

Figure 2. The Percentage of People who Leaked Confidential Information

2.1.1. Security Incidents by Insiders in Republic of Korea

In 2007, former and current employees of Posdata were arrested by illegally leaking core WIBRO technologies, and trying to sell them to a US communication company. When they had worked as researchers, they constantly leaked internal information such as WIBRO development procedure analysis information, design specification of WIBRO device and test results since 2006. If core WIBRO technologies were actually leaked to the US, exportation chance of base stations related devices will be lost [5].

In 2007, employees and ex-employees were prosecuted for leaking car-manufacturing technologies of Hyundai-Kia Motors. Leaked information was 54 confidential information including car body building technology of Sorento and a new model. The leakage plan was to leak the information by email in the company that were in their charge and then transfer technologies to a Chinese company for money. Estimated damage of the leak was twenty-two trillion won of loss [6]. Following Table 1 shows the examples of information leakage by insiders [7].

Table 1. The Examples of Information Leaks

Date	Incident	Method
May. 2012	Lieutenant Colonel working in Army Training Command leaked a total of 38 hard copy military secrets	Physical Access
Sept. 2011	A support staff responsible for Hana-SK Card telemarketing leaked a total of 90,000 the personal information	E-mail
Aug. 2011	Samsung Card customer care sales staff hacked queried and leaked customer information by hacking server for 8 months	Server Hacking
Mar. 2010	The staff working Samsung Electronics Semiconductor cooperation supplier leaked the business proprietary documents and core technology under A/S	Physical Access

2.1.2. Security Incidents by an Insider in Foreign Countries

In 2004, US Nuclear Research Lab's emails were hacked. It was found that Los Alamos National Nuclear Research Lab's confidential information was transmitted by Internet for several times [8]. After internal investigation, confidential information related to the nuclear weapon facilities were transmitted by email to the outside, and this raised social attention about securing information by internal information protection system. There was another case that an insider leaked customer information from the data processing center in Arizona Tucson. The insider had access to the card information of customers in the corporate network and leaked them. A total of forty million credit card information was leaked. In Japan, an insider leaked user information of Yahoo. He is a employee retired from Yahoo in Japan, used ID and password that he can access while working in the past and accessed the database to leak 46 million user account information [9]. In case of Russia, new generation nuclear capability submarine-launched ballistic missile(SLBM) and other technical information was leaked to China. Two professors from Russia Saint Petersburg State University leaked the information and transmitted to China for financial gain.

2.2. Effectiveness of Factors in Proposed Biometric Information Based System

Our system based on biometric information predicts user behaviors by measuring and analyzing the change of user's biometric signals. These could be identified by brain waves, pulse, voice, and temperature *etc*. We used the elements such as pulse, temperature, and skin conductivity based on the results of the existing researches. Effectiveness of each biometric information factor is measured in the following Table 2.

Table 2. Effectiveness of Factors Used in the Proposed System

Factors	Characteristics	Effective-ness (%)
Pulse [10]	- Periodic artery wave by the heartbeat - Pulse rate is 60~80BPM in relaxed state (Adult) - Increase in pulse rate by tension and stress means that user is in an unstable state	87~97
Temperature [11][12]	- The general temperature: 36.5℃ - Skin temperature: 30~32℃ - Capillary extends by tension and stress - The skin temperature increases by extension of the capillary	78~90
Skin Conductance [13][14]	- Electrical activity in skin - Skin conductance changes by sweat in tension status - Change in user's emotions can be detected by the alteration of skin conductance	88~98
Brain Wave [15][16]	- Potential that measures electric signal that occurs from brain's neuron cell - The brain wave shows change in frequency between 1~60Hz and in potential between 5~300 μN	80~97

3. Current Status of Biometric Information Techniques

Biometric information can be applied for use in a authentication system, validating the user trying to access or a lie detector confirming whether criminal's statement is true or not. Such biometric techniques acquire its objectives by comparing measured biometric information statistics of user during activities. These technologies are actively being researched to be applied in other various fields that are not mentioned in this paper. In this chapter, we explain techniques using biometric information in various fields. Table 3 shows biometric information technologies, used factors and characteristics.

3.1. Polygraph Technique

Polygraph is based on physiology and medicine which records human feelings, physiology phenomenon such as breath, pulse, blood pressure and skin conduction. It is a useful method to figure out the truth of testimonies done when answering certain questions by collecting and analyzing biometric information[17].

3.2. Authentication Technique

Most of biometric information researches done in the field of information security are authentication techniques. Biometric information contains signals such as pulse and temperature that cannot identify users, but there are other signals such as fingerprint and iris that can identify users by their unique characteristics. Authentication exploits these user-unique information and validates whether user has privileges to access certain resources. Such factors are fingerprints and iris. Authentication technologies using face and vein are in development[18, 19].

3.3. Emotion Measure Technique

One of the representative examples of measuring emotional state using stress, fatigability, level of concentration, sleepiness and tension is measuring physical and mental state of pilots. In order to grasp physical and mental state of pilots, it is regulated for pilots to have periodic checks, and their information is utilized for safety supervision. In this research, questionnaire and biochemical & physiological examination are implemented for measuring physical and mental condition of pilots. The questionnaire checks mental health by various questions. Biochemical examination measures physical status by performing serum and urine cortisol experiment. Finally, physiological examination measure physical and mental condition of pilots by checking sensorimotor responses, heart rate change, blood pressure and body temperature [20].

Table 3. The Characters of Used Factors in Biometric Information Technology

Technologies	Used Factors	Characteristics
Polygraph Technique	Pulse wave	Pulse wave measures the volume change of the blood in the arm by pressuring artery via blood pressure measurement stand.
	Skin conduction	Skin conductance measures change in electrical resistance of the skin by connecting silver electrodes. Extremely sensitive device capable of measuring small changes in resistance of the skin must be used which is the key element of getting high ratings in determining authenticity.
	Breath	Breathing records respiratory, volume, degree of inhibition while stopping and change in breathing and intake by recording device. Rubber tube is put around the chest and abs and pen writes to the paper by sensing motion in the chest and abs.
Authentication Technique	Fingerprint	Measuring biometric information using fingerprints is most widely used and it can be used as an authentication factor since it is unique to each person.
	Iris	Measuring biometric information by iris is the second most widely used method and iris is also unique to each person. It can be used as an authentication factor.
	Vein	Measuring biometric information by vein is done by touching the

		device with a finger and it is easy to collect data.
	Face	Measuring biometric information by face recognition has less resistance on input and the interface device is not complex.
Emotion Measure Technique	Motor response	Measures the speed of reaction on visual stimulus for tiredness, concentration, stress tests and etc.
	Heartbeat, blood pressure	Measures body signals that represent stress and tiredness of the body related to cardiovascular of autonomic nervous system, which is controlled by heartbeat and blood pressure.
	Body temperature	Body temperature can be divided into the core temperature and skin temperature. Core temperature does not alter meaninglessly. It can be used to check the results of the disease, occurrence of inflammation or infection, status of user.

4. Design of Proactive Detection Technique based on Biometric Info.

The proactive detection technique is consisted the detection module, the response module, the security controller module, and the human interface. Figure 3 shows the structure of proposed system [21].

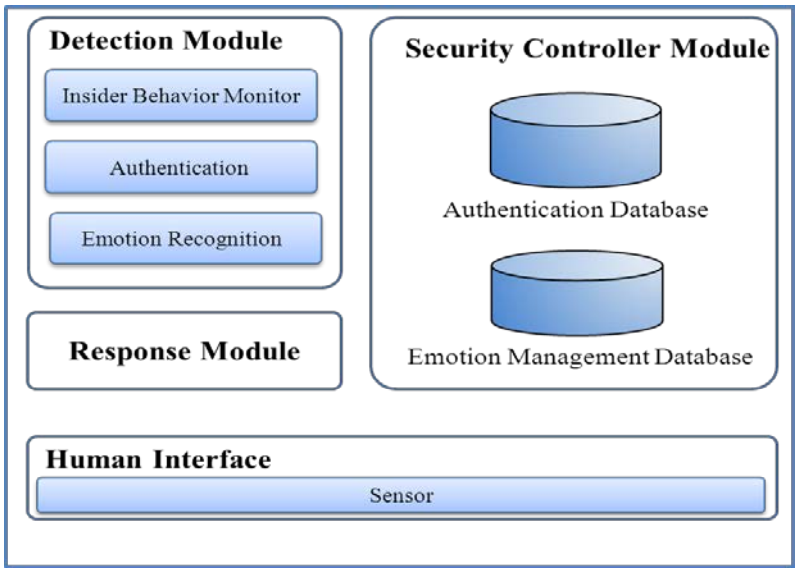

Figure 3. The Basic Structure of Proposed Technique

In the detection module, insider behavior monitor monitors the user behavior, and identifies abnormal behavior. It monitors actions related to the leakage of sensitive information. Authentication function authenticates insider by ID and password before insider does any action on a sensitive file. Emotion recognition detects insider's abnormal behaviors by comparing and analyzing the value of insider's collected biometric signals with insider's average value stored in a database when biometric signals are received from the human interface. It periodically calls insider's biometric signals from human interface, and generates the average value of biometric signals after collecting insider's biometric signals for about a month. Then it compares the value of biometric signals with insider's average value in the database. If the value of collected biometric signals exceeds the threshold of the average value, it determines that there is a possibility of data leakage.

The response module countermeasures the insider's abnormal behaviors related to data leakage with reacting methods such as alerting, delaying and blocking services, etc. according to the degree of leakage severity. For example, if the risk degree of data leakage is high, the system delays or blocks requested service.

The security controller module is consisted with authentication database and emotion management database. The authentication database applies the authentication information for distinguish whether user has access privilege or not. The emotion management database saves the measured values of insider's biometric signals, average values of measured user biometric information, and threshold values of biometric information.

The human interface collects insider's biometric signals by sensors. Sensors periodically measure insider's biometric signals. It sends collected signals to the detection module if detection module requests the measured data of any insiders. Sensors immediately measure insider's biometric signals, and report them to the detection module.

5. Comparison of Proposed System with Other Security Systems

In this paper, we measured biometric information of an insider and analyzed the measured information and proposed a security technique which protects the information from leaking by insiders. The proposed technique, which is based on biometric information, differs from other past researches in the biometric security field. Until recent, it is not a technique that can proactively detect information leakages by insiders using the biometric information of insiders and report the omen of information leakage by insiders to security administrator. Furthermore, security techniques based on biometric information are used for authentication purposes by identifying biometric information such as iris and fingerprint. It only compares the information whether the insider is legitimate user or not. We compared existing techniques based on biometric information with our proposed detection technique as Table 4. Through this comparison, we present that proposed security system can detect malicious behavior of insiders proactively.

Table 4. Comparison of Proposed Technique with Other Techniques

Factors	classification	Description
Main Functiona -lity	**Polygraph Technique**	To discern the authenticity of suspects statement, and such process is used for criminal investigations
	Authentication Technique	To identify the user by biometric information and issues a user's ID. ID is compared with the collected biometric information.
	Emotion Measure Tech.	To measure the current situation of the user and it is widely used in the medical area. By using the collected biometric information, we can confirm emergencies of patients.
	Proposed Technique	To detect and terminate internal information leakage by an insider. We measured the change of biometric signals with biometric factors such as pulse, skin conduction. So, proposed technique can more securely manage internal information.

Character-istics	**Polygraph Technique**	A polygraph technique 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.
	Authentication Technique	An authentication technique offers more reliability over traditional authentication systems because of biometric characteristics.
	Emotion Measure Tech.	In the medical field, biometric information is used to check the status of patients. Also, The information is transformed into emotion information for checking stress and tiredness of patients.
	Proposed Technique	The proposed technique monitors insider's biometric signals when he/she tries to access or leak a sensitive data in database, and compares the change values of collected insider's biometric signals with stored the normal values of biometric signals in database. If collected biometric signals are out of normal boundary, it checks insider's status.
Subject	**Polygraph Technique**	This is typically used for the police and prosecutor's office to choose truth or falsehood of criminal suspects.
	Authentication Technique	This is used when a user enters and exits the building, or at border checkpoint and E-commerce.
	Emotion Measure Tech.	This is used to check the status of patients or workers in medical fields and dangerous job field.
	Proposed Technique	This is used to detect malicious behaviors of insiders. It is not objects tried to leak but insider.

6. Conclusion

We proposed the technique for detects information leakage based on biometric signals of an insider. We architected the basic structure of this technique. Also, we investigated the effectiveness of factors which uses the biometric technique, and we studied the trends in security technique related to biometric information. Finally, we compared the proposed technique with other techniques related to biometric signals and information. As comparing proposed technique with other security techniques, we can know that proposed technique suggest new security paradigm which monitor target is not object but users. When an insider tries to leak internal information, proposed technique can detects the omen of information leakage.

In future research, we will implement the proactive detection system based on biometric information. Through this system, we can expect more secure, simple, and effective the information security environment. We also expect to reduce the security incidents by insiders.

References

[1] "2011 CyberSecurity Watch Survey: Organizations Need More Skilled Cyber Professionals to Stay Secure", Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte, **(2011).**
[2] "National Industrial Security Center: Industrial Security Information", National Intelligence Service, **(2012)**.
[3] I. M. Abbadi and M. Alawneh, "Preventing Insider Information Leakage for Enterprises", The Second International Conference on Emerging Security Information, Systems and Technologies (SECURWARE '08), **(2008)**, pp.99-106.
[4] J. ho Eom, "Modeling of Document Security Checkpoint for Preventing Leakage of Military Information", International Journal of Security and Its Applications, **(2012)**, pp.175-182.
[5] "Unsecured Economies: Protecting Vital Information", McAfee, (2009).
[6] H.-G. Park, "IBM Governance and Risk Management: Business alignment, visibility and control", IBM Tivioli Security Consultant, **(2007)**.
[7] J. ho Eom, "The Quantitative Evaluation of a Level of Insider Activity using SFI Analysis Techniques", Journal of Security Engineering, **(2013)**, pp. 113-122.
[8] "Cyber Security Issue", Korea Internet & Security Agency_May, **(2013)**.
[9] "TrendLabs 2Q 2013 Threats Report", Trend Micro, **(2013)**.
[10] H. Zhang and G. Liu, "Research of Emotion Recognition Based on Pulse Signal", Advanced Computer Theory and Engineering, **(2010)**, pp. 20-22.
[11] C. Ah-Young and W.-Tack Woo, "Feature Extraction for Emotion Analysis based on Physiological Signal", HCI Korea 2005, **(2005)**, pp. 624-629.
[12] A. Tefas, "Using support vector machines to enhance the performance of elastic graph matching for frontal face authentication", IEEE Trans.Pattern Anal.Mach.Intell, **(2001)**, pp. 735-746.
[13] J.-Y. and Q.-Y., "Sensor-Based Abnormal Human-Activity Detection", IEEE Transactions on Knowledge and Data Engineering, **(2008)**, pp. 1082-1090.
[14] B. Shahani, J. Halperin, P. Boulu and J. Cohen, "Sympathetic skin response: a method of assessing unmyelinated axon dysfunction in peripheral neuropathies", J Neurol Neurosurg Psychiatr, **(1984)**, pp. 536-542.
[15] K.-M. Cha and H.-C. Shin, "Brain-Computer Interface(BCI) using P300 Brain Wave", Institute of Electronics Engineers, **(2009)**, pp. 1174-1175.
[16] M. Li, Q. Chai, T. Kaixiang, A. Wahab and H. Abut, "EEG Emotion Recognition System", In-Vehicle Corpus and Signal Processing For Driver Behavior, **(2009)**, pp. 125-135.
[17] B. Sun Cho, "Lie detector", The Journal of Notice, **(2002)**, pp. 5-16.
[18] K. Hyun, H. Chang-Wook and C. Jin-Hyung, "Evaluation of Reliability of the Emotional Function Mouse", Journal of the Korean Society of Jungshin Science, **(2001)**, pp. 28-36.
[19] W. Ark, D. Christopher Dryer and D. J. Lu, "The Emotion Mouse", International Conference on Human-Computer Interaction, **(1999)**, pp. 818-823.
[20] S.-H. Choi and D.-H. Lee, "A Study on the Evaluation of Human Alertness for Flight Safety", Ergonomics Society of Korea, **(1998)**, pp. 167-172.
[21] J.-H. Eom, S.-H. Lee, J.-K. Jung, M.-W. Park and T.-M. Chung, "An Architecture of Emotional Recognition based Internal Information Leakage Prevention System", AICT2013, **(2013)**.

Authors

Seung hyun Lee received his B.S. degrees in Computer Information Warfare from Dongyang University, Yeongju, Korea in 2012. He is currently working toward his M.S in Electrical and Computer Engineering at Sungkyunkwan University. His research interests are internal information security, binary analysis, network security, and virtualization security.

Min woo Park received his B.S. AND M.S. degrees in Computer Engineering from Sungkyunkwan University, Suwon, Korea in 2008 and 2010, respectively. He is currently working toward his Ph.D. in Electrical and Computer Engineering at Sungkyunkwan University. His research interests are android security, threat analysis, network security, wireless security, and access control.

Jung ho Eom received his M.S. and Ph.D. degrees in Computer Engineering from Sungkyunkwan University, Suwon, Korea in 2003 and 2008, respectively. He is currently a professor of Military Studies at Daejeon University, Daejeon, Korea. His research interests are information security, cyber warfare, and network security.

Tai myoung Chung received his first B.S. degree in Electrical Engineering from Yonsei University, Korea in 1981 and his second B.S. degree in Computer Science from University of Illinois, Chicago, USA in 1984. He received his M.S. degree in Computer Engineering from University of Illinois 1987 and his Ph.D. degree in Computer Engineering from Purdue University, W. Lafayette, USA in 1995. He is currently a professor of Information Communication Engineering at Sungkyunkwan University, Suwon, Korea. He is now a vice-chair of the Working Party on Information Security & Privacy, OECD.