Transactions of the Korean Nuclear Society Autumn Meeting
Gyeongju, Korea, October 27-28, 2016

A New Framework to Minimize Insider Threats in Nuclear Power Operations

Young A Suh [a], Man-Sung Yim [a]*

[a] Nuclear Environment & Nuclear Security Lab, Department of Nuclear And Quantum Engineering, Korea Advance Institute of Science and Technology(KAIST)
[*]Corresponding author: msyim@kaist.ac.kr

1. Introduction

With the on-going global war on terror, potential terrorist attack in a nuclear power plant is getting a lot of attention. In particular, potential threat of an insider that could lead into a serious outcome deserves serious consideration. In a 2008 report, IAEA presented preventive and protective measures against such threat [1]. These are summarized as : (1) Exclude potential insiders by identifying undesirable behavior or characteristics, which may indicate motivation, prior to allowing them access; (2) Exclude further potential insiders by identifying undesirable behavior or characteristics, which may indicate motivation, after they have access; (3) Minimize opportunities for malicious acts by limiting access, authority and knowledge, and by other measures; (4) Detect, delay and respond to malicious acts, and; (5) Mitigate or minimize consequences. Implementation of these measures requires further deliberations. Building on the recommendations of the IAEA, this study proposes a framework for detection and exclusion of potential insiders as described below.

2. A New Framework for Detection of Potential Insiders

To suggest a new insider monitoring framework into detection and prediction of insider threat, it is necessary to develop conceptual understanding of the insider threats. First, understanding why a worker becomes the insider is important. There are several theories for understanding insider behavior. Among those, General Deterrence Theory (GDT) [2] tells that a person commits crime if the expected benefit outweighs the cost of action. Theory of Planned Behavior (TPB) [3] explains that person's intention such as attitude; subjective norms and perceived behavior control towards crime are key factor in predicting behavior Situational Crime Prevention (SCP) [4]. Using SCP and TPB theory, insider threat can be predict if their motivation, capability and opportunity are revealed before committing crimes. Since the human act mostly through rational assessment such as cost-benefit analysis, a normal worker may not consider being an insider unless he gets a pressure over their threshold, i.e. suggestion of a large sum of money beyond expectation or a blackmail of endangering their family member's life from terrorists. In these cases, it is possible for a normal worker to become the potential insider according to the GDT theory.

The risk of insider threat is a function of motivation, intention and opportunity (capacity). Motivation is divided into two divisions: internal or external and strong or weak. The internal motivation is to become an insider by himself/herself due to personal issues such as family problems, financial need and job dissatisfaction, etc. The external motivation is related to 'unwanted insider' because of blackmail from outsiders. These motivations can be strong or weak depending on the individual's personality and cultural environment. Depending on the intention, the insider becomes a passive or violent-active, or non-violent insider. Even though insider has strong motivation and intention, the consequence of their malicious action is also different because their opportunity (capacity) is different by the position on vulnerability to blackmail, skill, knowledge and authorities. The consequence varies, depending on the levels of the tasks, such as from borrowing ID card to sabotage. Therefore, detection of insider threat requires monitoring of both internal and external motivation as well as monitoring the intention and capacity, perhaps through examining stimulus to the individual.

To predict and detect the insider threats, a reliable technology to determine internal motivation is necessary. If we can notice the change of psychological signals associated with motivation, such technology can be available. Such psychological signals can be combined with the results of background checkup and abnormal behavior indicators. The framework suggested in this study for the detection of potential insiders is based on integration of three monitoring strategies: (1) Behavior monitoring, (2) Cognitive monitoring, and (3) Stimulus monitoring. This is depicted in Figure 1.

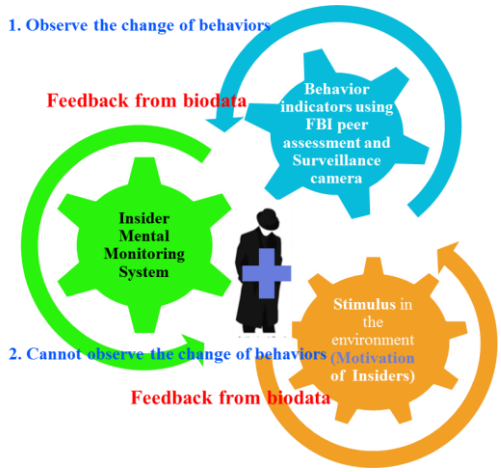

Fig. 1. A new framework to detect and predict the insider threats

Figure 1 show a new conceptual model for monitoring cognitive, behavioral, and environmental (stimulus) signals for predicting and detecting the insider threat. This framework integrates behaviorist, cognitivist, and environmental approaches.

2.1 Stimulus Monitoring

The stimulus monitoring is that checking the insider's motivation from both internal and external. The insider in this framework is contained within both initiating insider and a "non-initiating insider" (insider who has not yet committed an action). The motivation of insider can occur from various factors such as personality like strong self-esteem, ego and problems at work (i.e., a lack of recognition, disagreements with co-workers or managers) as shown in Figure 2 (purple box). Among these, the red bold words in Figure 2 indicate the motivation factors strongly influenced on culture difference in multicultural environment. In the case of nuclear security culture, it may be affected by cultural differences, especially employee screening/staff trustworthiness, training for emergency and non-emergency procedures, organizational structure, manager style, communication effectiveness, review/feedback, authority, change, decision-making, creating motive to increase security, teamwork and cooperation [5], adherence to procedures and commitment, striving to improve and integrity. Job dissatisfaction is also the one of the significant factors affected by multiculturalism. There are examples such as coworker relations, financial stability, account for personal beliefs and climate effect on foreigners [6]. In addition, different styles of English will make the miscommunication between workers [7]. This may imply the importance of language selection in emergency situations and increase of the insider threat in multicultural environment.

Fig. 2. Description of general motivation factors and type of insider related to capacity

Motivation can be checked up from background investigation in the screening system at recruiting to periodic mental check up every 6 months. Manager or peer can also report insider's abnormal status from family problem to finance need. It can be worked on tracing the motivation of initiating insider and a potential insider who needs to watch carefully at workplace. However, it is difficult to monitor the non-initiating insider, especially externally coerced into attacking the organization. This is because we cannot observe the evidence during the periodic mental checkup or screening system, so it means the needs of real-time monitoring of worker's mental status (cognitive and mental status monitoring system).

In this new framework, we focused on the insider's motivation [8] and environment assessment (stimulus assessment) [9]. We can observe the worker's motivation and narcissism behavior using big data analysis via social medium, i.e. twitter. In addition, MBTI test, which is famous for identifying the personality, will be adapted in recruiting periods to prevent the high aggressive person. To assess the environmental stimulus, before a worker enters the workplace, psychological states, i.e. alcohol, amount of sleep, fatigue, and simple background survey relating to outsider contact will employed to identify the motivation of insider. Figure 3 shows the action flow of stimulus monitoring (purple circle).

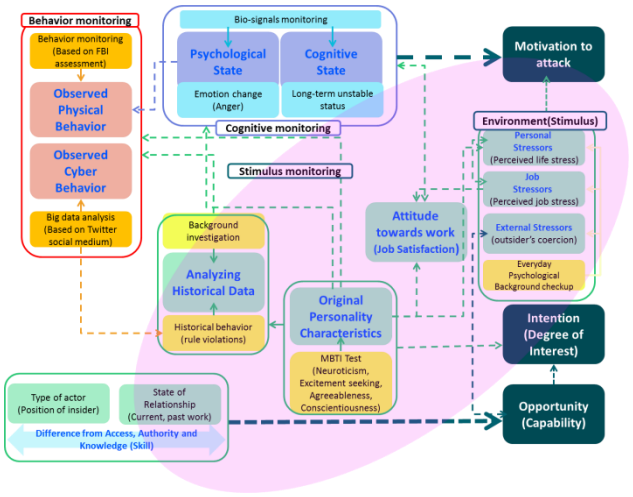

Fig.3. A specific framework for insider action monitoring highlighted on Stimulus monitoring (Purple circle)

2.2 Cognitive Monitoring

Cognitive monitoring is that checking the non-initiating insider's mental status and cognitive process for predicting and detecting the initiating insider. For

cognitive and mental status monitoring, this study suggests the real-time measurement of bio-signals. Generally, bio-signals can represent human nature like their personality and individuals' physiological and mental status. There are various bio-signals such as respiratory rate, skin temperature, Galvanic Skin Response (GSR), Electroencephalogram (EEG), Electromyogram (EMG), Electrooculogram (EOG) and Phonocardiogram (heart sounds) [10]. Among these, three typical signals, i.e. GSR, EEG and ECG, appear to be useful for measuring the mental status of workers or potential insiders. ECG and GSR are usually used to the principle of a lie detector. Because of limitation of a lie detector, EEG becomes famous to supplement the existing lie detector [11]. Brain is in charge of the cognitive process and the intentional wrong decision behavior, emotion change and motivation of insider may be related to cognitive process represented by EEG. Nevertheless, these signals can be helpful to measure the emotion change when a normal worker suddenly goes through a change to become an insider.

In addition, a new insider mental monitoring system can be implemented through the use of simple wearable devices such as a watch or a safety helmet. With the innovative technological advancement in health wearable system, the three signals such as GSR, EEG, and ECG can be obtained from a simple wire or wireless devices. For the investigation of applicability of biodata for detecting and predicting insiders, a pilot study is underway [12] using the equipment in Figure 4.

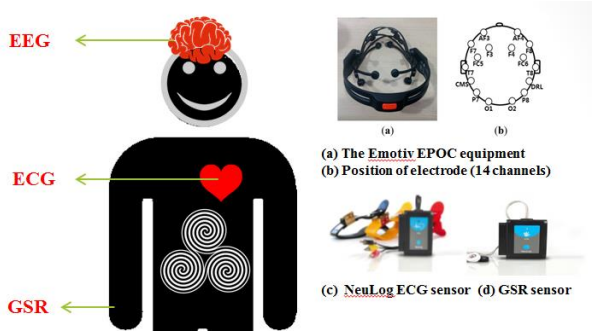

Fig. 4. A new insider mental monitoring system

2.3 Behavioral Monitoring

Behavioral monitoring will be checked by peer or manager assessment and surveillance camera. The principle of behavioral monitoring is based on TPB theory. Some behaviors may be a clue that an employee is spying and/or stealing from the organization's important asset. FBI [13] and other researchers [14] suggest the several behavioral indicators for detecting and predicting the insider threats. In this study, among these, possible behaviors indicators can be used in NPPs are selected. The behavior indicators are: (1) remotely accesses the network while on vacation, sick or at odd times, (2) works odd hours without authorization, (3) notable enthusiasm for overtime, weekend or unusual work schedules, (4) unnecessarily copies material, especially if it is proprietary or classified, (5) Interest in matters outside of the scope of their duties and (6) signs of vulnerability, such as drug or alcohol abuse, financial difficulties, gambling, illegal activities, poor mental health or hostile behavior, should trigger concern. Be on the lookout for warning signs among employees such as the acquisition of unexpected wealth, unusual foreign travel, irregular work hours or unexpected absences.

Despite the behavior indicators, we cannot judge the abnormal behavior of a worker into an insider completely. According to criminal researchers, many people experience or exhibit some or all of the above to varying degrees; however, most people will not cross the line and commit a crime. Although behavior monitoring itself is conventional approach dealing with detection and prevention on insider threats, there are limitations on misjudgment and discrimination. Thus, a new integrated framework suggested in this study is needed to compensate the lacks of behavior monitoring itself.

3. Conclusions

The nuclear security risk, i.e. insider threat, has concerned continuously because the existing physical protection system is only for outsider threats. In addition, with high possibility of use of multicultural workforce in newcomers' NPPs, the detection and prediction of insider threat is a hot potato. Thus, this paper suggested a new framework for predicting and detecting the insider threat. This framework integrates the behavioral indicators, stimulus monitoring and cognitive monitoring. Specially, cognitive monitoring developed newly based on human biodata which are reliable signals. This framework open a chance to detect and predict the insider before commits a crime accurately. This model can be direct application to reduce the security risks in multicultural environment.

REFERENCES

[1] Guide, Implementing. "Preventive and Protective Measures against Insider Threats."
[2] Theoharidou, Marianthi, et al. "The insider threat to information systems and the effectiveness of ISO17799." Computers & Security 24.6 (2005): 472-484.
[3] Mathieson, K. (1991). Predicting user intentions: comparing the technology acceptance model with the theory of planned behavior. Information systems research, 2(3), 173-191.
[4] Guerette, R. T., & Bowers, K. J. (2009). Assessing the extent of crime displacement and diffusion of benefits: a review of situational crime prevention evaluations. Criminology, 47(4), 1331-1368.
[5] Ogbonna, E., & Harris, L. C. (2006). The dynamics of employee relationships in an ethnically diverse workforce. Human Relations, 59(3), 379-407.

[6] Marschan-Piekkari, R., Welch, D., & Welch, L. (1999). In the shadow: The impact of language on structure, power and communication in the multinational. International Business Review, 8(4), 421-440.
[7] Boyle, W. F., & Charles, M. (2012). EDUCATION IN A MULTICULTURAL ENVIRONMENT: EQUITY ISSUES IN TEACHING AND LEARNING IN ENGLAND. Living on the boundaries: urban marginality in national and international contexts, 8, 143.
[8] Nurse, Jason RC, et al. "Understanding insider threat: A framework for characterising attacks." Security and Privacy Workshops (SPW), 2014 IEEE. IEEE, 2014.
[9] Axelrad, Elise T., et al. "A Bayesian network model for predicting insider threats." Security and Privacy Workshops (SPW), 2013 IEEE. IEEE, 2013.
[10] Anandanatarajan, R. (2011). Biomedical Instrumentation and Measurements. PHI Learning Pvt. Ltd..
[11] Abootalebi, V., Moradi, M. H., & Khalilzadeh, M. A. (2009). A new approach for EEG feature extraction in P300-based lie detection. Computer methods and programs in biomedicine, 94(1), 48-57.
[12] Y.A. Suh and M.S Yim, “An Investigation into the Applicability of Biodata, from Health Wearable Devices, to Insider Threat Detection in Nuclear Power Plants”, 2016 annual INMM Conference, Atlanta, USA, July, 2016 (Prearranged)
[13] FBI, “The Insider Threat: An introduction to detecting and deterring an insider spy”, 2012. http://www.fbi.gov/about-us/ investigate/counterintelligence/ the-insider-threat
[14] Gelles, M. G., Brant, D. L., & Geffert, B. “Building a Secure Workforce”.2012