Insider Threat Detection Based on Users' Mouse Movements and Keystrokes Behavior

Yassir Hashem, Hassan Takabi and Ram Dantu
Department of Computer Science and Engineering
University of North Texas
Denton, TX, USA
YassirHashem@my.unt.edu, {Takabi, Ram.Dantu}@unt.edu

***Abstract*—Insider threat is considered as one of the most serious threats in cybersecurity and has been a prime security concern for government and industry. Traditional approaches can't provide efficient solutions, and the threat keeps raising. In this paper, we propose a new approach to insider threat detection and prediction based on the user's mouse movements and keystrokes behavior. We conduct human subject experiments with 30 participants and capture their mouse movements and keystroke dynamics as they perform several computer-based activities in both benign and malicious scenarios. We extract features and evaluate our approach using several classifiers and statistical analysis measures. The results show that participants performing malicious tasks showed faster speed and longer mouse movements, and long left click and keystroke duration than the benign tasks. Our results suggest that users' mouse movements and keystrokes behavior can reveal valuable knowledge about their malicious behavior and can be used as indicators in the insider threat monitoring and detection frameworks.**

***Index Terms*—Insider Threat; Biometrics**

I. Introduction

Insider threat has become a significant security risk for organizations and poses enormous harm to their information systems and assets. Malicious insiders normally have authorized access to the organization's computer systems, information, and networks and due to these accesses, malicious insiders are capable of infiltrating information, stealing or damaging data and sabotaging the facilities and the information system [3]. Insider threats are on the rise. For example, the results of the 2014 US State of Cyber-crime Survey shows that 32% of organizations have experienced an insider threat attack and 76% of compromised or stolen confidential records are attributed to insiders. In 2016, the report from the Ponemon Institute based upon a representative sample of 237 organizations in six countries found that the most costly attacks were conducted by insiders and cost companies an average of $167,890 per year [22]. Earlier this year, Alphabet Inc. the owner of Waymo a formerly Googles self-driving car project filed a lawsuit against its former engineer accusing him of copying more than 14,000 internal files about the Waymo's self-driving technology and taking them directly to his new company Uber [11].

Preventing and detecting insider threat incidents is a challenging task because malicious insiders regularly follow legal paths to launch their attacks and current intrusion detection systems are mostly for detecting external attacks and are insufficient in safeguarding against insider threats. However, many approaches based on technical, behavioral and psychological perspectives have been proposed to prevent and mitigate the insider threats [9] [10] [15] [9] [34] [32]. Most of these approaches monitor the insiders voluntarily activities on using the organization's computer information system resources. However, a well-skilled insider can always forge his activities and deceive the detection system.

On the other hand, user behavioral measures such as the computer-based behaviors when a user interacts with computer peripherals (e.g., mouse; keyboard) and user psycho-physiological measures such as electroencephalography (EEG), electrocardiogram (ECG), and eye movements dynamics can provide good indicators to mitigate the insider threat problem. These behaviors and measures are involuntarily generated and can carry a wealth of knowledge about the users mind states that are otherwise not available by other traditional behaviors measures.

In cybersecurity domain, the mouse movements and keystroke dynamics are considered a behavioral or soft biometric and have been studied mainly for authentication and identification [24] [2] [27] [36] [38] [6] [39] [33].

In this paper, we propose an approach that can prevent insider attacks by predicting the possibility of an insider threat using the behavioral analysis of users mouse movements and keystroke dynamics. Our approach aims to introduce an unbiased, noninvasive, and automatic technique to identify unusual behavior for a user within the organization's computers system. It provides an initial foundation for building future insider threat detection and mitigation mechanisms based on the real-time features that can automatically infer a user's computer-based behaviors and determine if whether or not the user is committing a malicious act.

In this work, we extend our previous work [12] that uses the Electroencephalogram (EEG) and eye movement dynamics to reveal valuable knowledge about users malicious intent and utilize them to build a multi-modal neuro-physiological insider threat monitoring and detection framework. However, in this work, we analyze the users mouse and keystroke dynamics and aim to find correlation between computer based behavior and the neural response while users perform different tasks. We use the same experiments, but we focus on the participants' interactions with computer peripherals (mouse and keyboard) during the experiment tasks.

The experiment was performed with 30 participants and the mouse movements and keystrokes were recorded while participants performed different tasks including both malicious and benign activities. We analyze the recorded data, extract useful features and use classification and statistical analysis to evaluate our experimental results.

A. Threat Model

Insiders can be current or former employees who have the privileged access to organization's computers and information system in addition to the knowledge of the internal organizational processes that may allow them to exploit weaknesses [37]. In general, insiders can be categorized into three types: unintentional (apathetic) insiders, intentional (malicious) insiders, and exploited insider (external control of insider workstation). In unintentional insider scenarios, users accidentally abuse the information system by deleting or modifying sensitive information or sharing them with unauthorized parties or social media sites. User's negligence in following the organization security policies can lead to this form of insider threat.

In intentional insider scenarios, the user intentionally abuses the information system by damaging or manipulating the organization sensitive information. These malicious activities include but not limited to data fraud and theft, sabotage of facilities' equipments and information systems. The exploited insider scenario happens when user's account is compromised by an external attacker. An attacker can use social engineering, malware or phishing attacks to compromise user's credentials. All of the three categories can cause significant financial losses and damages to organizations in both industry and government sectors.

In this paper, we focus on the second type of insider threat and our approach addresses the threats coming from the intentional malicious insiders.

B. Related Work

As insider threat incidents have become one of the most critical challenges to the organizations' information system in both government and industry sectors. researchers have proposed numerous approaches tackling the threat and providing solutions. These solutions can be classified to technical and behavioral solutions [28] [26] [35] [16] [32]. They focused on two methods. First, the user behaviors analysis [34] [9], by using psychological approaches to predict and detect the insider threat. For example, Theoharidou et al. presented several different theories from criminology and related social science fields on the behaviors of insiders [34].

Second, the user activities analysis includes user interaction with networks, documents, and social networks. And provides technical solutions include segregation of duties and least privilege, anomaly detection and introduce decoys to entrap insiders [28] [26] [35] [16]. For example, Thompson et al. present a content-based framework to detect insider anomalies in accessing documents and queries [26]. Kaghazgaran et al. proposed a model to consolidate honey permissions into role-based access control [16]. Furthermore, some studies start to utilize the users' psychophysiological measures for data leakage prevention frameworks. For example, Lee et al. proposed a real-time data leakage prevention framework based on the biometrics signals [19].

On the other hand, the computer-based behaviors when a user interacts with computer peripherals (e.g., mouse; keyboard) can provide a dynamic traces of insider mind and can reveal concealed cognitive states that cannot be achieved using the traditional behaviors. The mouse and keystroke dynamics are soft biometrics and haven't been explored enough for the insider threat detection and mitigation purposes. However, they have been mainly used for authentication and identification [24] [2] [27] [36] [38] [6] [39] [33]. For example, Karimi et al. introduced an online authentication system using mouse dynamic and extracted features from the mouse movements, clicks, and scrolls [38]. Zhang et al. proposed a keystroke biometrics model that authenticate a users identity using statistical methods applied to the keystroke features [39].

In addition, the mouse and keystroke dynamics were explored for emotional and mental state prediction, and deception and fraud detection [29] [20] [21] [18] [17] [25] [8]. For example, Nahin et al. proposed an approach to determine user emotion state by analyzing his typing patterns on a standard keyboard [25] [23] [30].

Closely related to our work, Valacich et al. proposed a polygraph technique implemented within an online survey environment to differentiate between how innocent people and guilty insiders respond to concealed information test (CIT) using selected mouse movement features [36]. Unlike our work which focuses on intentional malicious insider threats, this study is targeting a very specific case of insider threat using a controlled experiment where the participants react to visual stimuli displayed on the screen (online survey). However, in our work, we do not use any stimuli in the experiments, and instead, we focus on developing tasks that are close to real-world scenarios.

In this paper, we extend our previous works [13] [14] [12], by conducting a human study experiments include a larger number of participants and more complex activity tasks, and investigate the participants mouse movements and keystrokes behaviors and the capability of using these behaviors to detect the users malicious activities.

II. Experimental Design

Our experimental design includes six different tasks that are a mix of regular computer-based activities such as data entry, browsing the Internet, using applications, etc. and malicious activities that are usually carried out by insiders such as accessing unauthorized information, copying, modifying or deleting sensitive data, etc. Each task emulates a real-world scenario very close to a typical work environment as described in section II-B and II-C.

We recruited a total of 30 participants to participate in our experiments, but we use data of 25 participants in our data analysis; the data records of the other 5 participants were incomplete and were removed from the analysis. Out of 25 participants, 15 were male, and 10 were female. All participants were between the age of 18 and 34 years old and were a graduate or undergraduate students at the University of North Texas. As in real-world scenarios, a malicious insider can be a highly skilled or a script kiddie user (an unskilled user who uses codes or programs developed by others), we made sure to include participants with different levels of programming skills and cybersecurity knowledge. We also made sure to have a fair distribution of participants w.r.t gender, race and age.

Participants performed the tasks in two sessions, three tasks per each session. The sessions conducted on two different days and at a different time during the day. The experiments were conducted with the approval of the University of North Texas Institutional Review Board (IRB) and the participants were compensated $30 for one hour of their time. The participants were briefed on the objectives of the study and given a written informed consent form to read and sign. The consent form included a precise information about the experiment procedure and participant's right to participation. In the following, we describe the experiment in more detail.

A. Experiment Setup and Procedure

The experiments were conducted in our lab room which was set up to keep the same environmental conditions for all tasks and all participants. We used a regular personal computer for conducting the experiments with Intel Core i5-4210U Processor, 6GB PC3 DDR3L SDRAM and Windows 10 Home operating system and a 24-inch screen with a 1920x1200 resolution.

To record the mouse movements and keystrokes, we used a Mini Mouse Macro Pro software [31] that record the mouse position on the screen (X,Y coordinates), the event (drag, click, move, key press), and the event time-stamp in milliseconds (ms).

The experiment was divided into six different tasks for a period of 10 minutes per task. There were four benign activity tasks and two malicious activity tasks. In the following, we describe each of the six tasks in detail.

B. Benign Activities Scenarios

1) Task 1 : benign daily activities: This task emulates the benign daily activities performed by most employees in any organization such as browsing Internet, using computer applications or using an email account. In this task, the participating participant received through email an excel sheet containing names of students who participated in a previous survey and their associated information. The participant needed to use the browser to login to the database system and find out the students' names and update their missing data using the excel sheet. In this task, we did not require the participants to finish all the students' record and there was no pressure or stress introduced during the task.

2) Task 2: benign daily activities under stress: In this task, we repeat the previous task with some changes to introduce stress to the participants in order to emulate the scenario where employees work under pressure or emotional stress. The reason behind this experiment is to differentiate between the regular work pressure, fatigue or stress and the malicious intent of the users.

To do this, we conducted the experiment at the end of the working day, so the participants came to the lab after attending classes, exams or labs during the day causing them to have more mental workload compared to Task 1. The participants were also given twice the number of the records compared to the first task and asked to make sure to finish all the records during the 10 minutes experiment. In addition, we removed some of the students' names from the database to add more pressure as the participants were not able to find those names. The participants were told that there will be a special prize for the participant who finished his/ her report faster than the others adding more stress and time pressure to the experiment.

3) Task 3: high mental workload activities: This task emulates the professional job activities when the employees perform some activity involving high mental interaction. We try to show that our approach covered all the possible activities. The participants were asked to complete a short coding project (Designing a calculator) which requires more mental workload compared to the benign daily activities in Task 1. The participants were allowed to choose any programming language they felt comfortable with (C++, Java, Python). They were also allowed to browse Internet for help if needed. However, the participants were told that copying the code from Internet was not allowed and they had to write their own code. The participants were encouraged to finish the code project. However, the task did not require them to complete the project and there was no pressure or stress introduced to the experiment.

4) Task 4: high mental workload activities under stress: In this task, we repeated the previous task with some changes to introduce stress to the participants in order to emulate situations where employees work under pressure or emotional stress. To do this, we conducted the experiment at the end of the working day, so the participants came to the lab after attending classes, exams or labs during the day causing them to have more mental workload compared to Task 3. The participants were asked to repeat the same project but with another programming language. Participants were still able to browse the Internet for help. However, the participants had to complete the code and test it in 10 minutes. The participants were told that there will be a special prize for the participant who completed his/her code faster than the others.

C. Malicious Activities Scenarios

1) Task 5: remote access attack: This task emulates the malicious activities that could be performed by an insider. We used the remote access control scenario where an insider accesses to another computer in the network which he is not authorized to access. The insider can steal the credential information using shoulder surfing and use it to login to the victim's device. So, in this task the participants were asked to remotely access the teaching assistant's computer and steal data related to the exams, quizzes, projects etc.

Participants were instructed to perform this task without the TA noticing and to incentivize them, they were told that they would receive extra reward if they could complete these tasks without leaving any trace. For this task, we added a timer on the computer desktop showing the time remaining to complete the task.

2) Task 6: SQL injections attack: In this task, we emulate the scenario of the script kiddie insider (an unskilled system user who uses codes or programs developed by others to attack computer systems and networks participants). More specifically, we used the scenario when an insider uses SQL injections to access to information he has no permission to access. In this task, the participants were asked to use SQL injection to bypass the authentication for the database system. Then update, delete and copy the student's information in the database. The participants were told that successfully completing this task without leaving any trace will result in extra reward. We also added a timer on the computer screen showing the time remaining to to complete the task.

III. Data Analysis

The mouse and keyboard activities were recorded while the participants were performing the task. We recorded the X and Y coordinates of the mouse position on the screen, the mouse and keyboard event (drag, click, move, key press), and the event time-stamp in milliseconds (ms). Upon the completion of the task, the raw mouse movements and keystrokes data were stored in a text file.

We analyze the data by feeding the text file to our feature extraction component to extract useful features that represent the user behavior and can be used for detecting insider threats. We extract a total of 57 features that include mouse movements' spatial and temporal features, and keystrokes features (as shown in Table I). To calculate the mouse movement speed, we measure the length of the mouse path by adding the total distances between all adjacent path coordinates and dividing by the total time the mouse path took (the summation of the time-stamps in the path). As our experiment doesn't record the mouse and keystroke actions regarding to stimuli and it's entirely free (participants can move the mouse and press the keyboard keys freely during the experiment), we don't have a predefined start and end point to the mouse movement path. To address that, we chose our start and end point by the value of the movement event's time-stamp. We used 800 ms as our threshold to identify the start and end points. The mouse movement event with value 800 ms or above is considered as the stop position, and the next movement event will be the start point for the next path. We also calculate the mouse movement distance or the length of the mouse movement path and subtract that from the direct distance (the Euclidean distance between the first point in the path and the last point). In addition to that, we calculate the mouse left click duration and keystroke duration. We also consider the direction of the mouse movements and the frequency of directions change.

TABLE I
Mouse and keystroke dynamics features extracted from the experiment data

Mouse movement speed Av.
Mouse movement speed Max
Mouse movement speed Min
Mouse movement speed SD
Distance Av.
Distance Max
Distance Min
Distance SD
Distance x-axis Av.
Distance x-axis Max
Distancex-axis Min
Distance x_axis SD
Distance y-axis Av.
Distance y-axis Max
Distance y-axis Min
Distance y_axis SD
Direction
Frequency direction change
Direction Max
Direction Max distance
Left click down Av.
Left click down Max
Left click down Min
Left click down SD
Left click release Av.
Left click release Max
Left click release Min
Left click release SD
Backspace rate
Left click time diff Av.
Left click time diff Max
Left click time diff Min
Left click time diff SD
Right click down Av.
Right click down Max
Right click down Min
Right click down SD
Right click release Av.
Right click release Max
Right click release Min
Right click release SD
Right click time diff Av.
Right click time diff Max
Right click time diff Min
Right click time diff SD
Keypress time Av.
Keypress time Min
Keypress time Max
Keypress time SD
Num-pad press time Av.
Num-pad press time Max
Num-pad press time Min
Num-pad press time SD
Keypress time Av.
Keypress time Max
Keypress time Min
Keypress time SD

IV. Experimental Results

After completing the experiments for all participants, we analyze the recorded mouse and keystroke data for each participant separately. Then, we sample the data into ten seconds time frame (each time frame represents one sample). We extract the features and generate the feature vectors by applying our feature extraction code to each sample and save the output features into a feature vector. Each feature vector then will be labeled to the experiment tasks that generated from. In more detail, we label the feature vectors extracted from each participant by the activity he/she performed. So, the feature vectors obtained from the benign activities tasks (tasks 1, 2, 3, 4) have a label negative ”0”, and the feature vectors extracted from the malicious activity tasks (tasks 5, 6) have a label positive ”1”. Finally, we split each participant's data into 70% tuning and training set, and 30% testing set by dividing the 10 minutes task time to seven minutes for training and three minutes for testing.

We use several classification algorithms to evaluate our approach. However, the four classifiers: Support Vector Machine (SVM) [7], K-nearest-neighbors (k-NN) [1], Random forests [5], and Bagging predictors [4], show the best performance among the other classifiers using our training dataset. In

TABLE II
RESULTS OF THE MOUSE AND KEYSTROKE DYNAMICS

Features	Benign		Benign under stress		Malicious	
	Mean	SD	Mean	SD	Mean	SD
Mouse movement speed	0.75	0.26	0.82	0.42	0.97	0.34
Mouse distance travel	145.93	44.75	146.57	61.53	181.13	72.10
Mouse left clicks duration	167.63	69.60	226.69	224.20	293.01	152.32
Keystroke duration	218.52	463.96	506.65	937.79	469.32	792.49

general, the four classifiers show an average detection accuracy between 67.5% to 72.5% in detecting the malicious activities using the entire group of the extracted features.

Since the classification results are not very good, and in order to investigate which features are more valuable and useful in detecting the malicious intent among the extracted features, we run the statistical analysis over the mouse and keystroke extracted features and investigate each feature separately. We calculate the mean for each feature among the group of our participants for each task. We evaluate our results by dividing our experiment to three different tasks: the benign tasks, the benign under stress tasks and the malicious tasks.

Of all the features we tested, four features show statistically significant difference between the mean value of the tasks, namely the mouse movement speed, the mouse travel distance, the left mouse click duration, and the keystroke duration.

As shown on Table II the malicious tasks were associated with mouse movement speed at mean of 0.97 (pixels/ms) (SD 0.34). And by comparison, the benign tasks and the benign under stress tasks were associated with slower mouse movement speed at mean of 0.75 (pixels/ms) (SD=0.26) for the benign tasks, and mean of 0.82 (pixels/ms) (SD 0.42) for the benign under stress tasks. To test the hypothesis that there is a statistically significant difference between mouse movement speed of malicious tasks and the benign tasks, a related t-test was performed. The related t-test shows a statistically significant effect on p-value = 0.0000316. Thus the malicious tasks were associated with statistically significantly larger mean than the benign tasks. We also run the related t-test between the mean of the mouse movement speed for the malicious tasks and the benign under stress tasks. The results show that there is a statistically significant difference with p-value = 0.034. These results suggest that users will move the mouse at a relatively higher speed when performing a malicious act than performing benign act even when they involve in stressful conditions.

On the other hand, the participants performing the malicious tasks show longer travel distance than the other two tasks. As shown in the table, the malicious tasks were associated with the longest mouse movements distance among all the tasks with mean of 181.13 pixels (SD 72.10). To ensure these differences are statistically significant, we performed the related t-test over the malicious and benign tasks, and the p-value was about 0.000832. We repeated the same test over the malicious and benign under stress tasks, and the p-value was about 0.00114. From these results, we can conclude that users performing malicious act will tend to make longer mouse movement path than their normal pattern even when they experienced stressful conditions.

The mouse left click duration feature also shows interesting results. As shown on in the table, the mouse left click duration for the malicious tasks were the longest among all the tasks with mean of 293.01 ms (SD 152), while the benign tasks show the shortest mouse left click duration with mean of 167.63 ms (SD 69.60). We performed the related t-test over the two tasks, and the results show there is a statistically significant effect with p-value = 0.000015. The related t-test was also applied to test the difference between the mean of the mouse left click duration on both the malicious tasks and benign under stress tasks, and the p-value was about 0.0451. These results indicate that individuals will click the mouse (left click) at a slower speed when they perform the malicious act than their normal clicks pattern. However, individuals experiencing stressful conditions will also click the mouse (left click) at a slower speed than the normal but this speed still faster than performing a malicious act.

For the keystroke part, the benign under stress tasks show the highest keystroke duration with mean of 506.65 ms (SD 937). However, the results of the malicious tasks were very close to the benign under stress tasks with mean of 469.32 ms (SD 792) and much longer than the benign tasks. We performed the related t-test over the malicious and benign tasks, and the results show the differences were statistically significant with p-value = 0.0385. However, there was no statistically significant difference between the benign under stress, and the malicious tasks and the p-value was about 0.418571. Thus, users experiencing stressful conditions and users performing malicious acts may have similar keystroke duration and slower than their regular pattern. In addition, looking at this feature participants were varied on their keystroke speed as they come from different backgrounds and different computer skills and that can be seen clearly from the high standard deviation value.

Furthermore, other features such as the direction of the mouse movements and the frequency of directions change didn't show statistically significant difference between tasks.

V. CONCLUSION AND FUTURE WORK

Insider threats have become a growing challenge in the cybersecurity domain, and several solutions have been proposed. However, it remains a major concern. In this work, we have presented an insider threat detection approach based on the user's mouse movements and keystroke behavior. We analyzed the mouse movements and keystroke dynamics for

25 participants while performing different tasks including both malicious and benign activities. We extracted several mouse movements spatial and temporal features, and keystrokes features and used classification and statistical analysis measures to evaluate our results. In our results, we found that individuals show different mouse movements and keystroke behavior patterns when they perform malicious acts than their normal behavior pattern. These changes on behavior include high-speed and high-distance mouse movements, and long-lasting left clicks and keystroke duration. For future work, we plan to integrate our from findings mouse movements and keystroke features into a multi-modal framework that uses other behaviors to efficiently monitor and detect the insider threat activities.

References

[1] N. S. Altman. An introduction to kernel and nearest-neighbor nonparametric regression. *The American Statistician*, 46(3):175–185, 1992.

[2] F. Bergadano, D. Gunetti, and C. Picardi. User authentication through keystroke dynamics. *ACM Transactions on Information and System Security (TISSEC)*, 5(4):367–397, 2002.

[3] E. Bertino and G. Ghinita. Towards mechanisms for detection and prevention of data exfiltration by insiders: keynote talk paper. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, pages 10–19. ACM, 2011.

[4] L. Breiman. Bagging predictors. *Machine learning*, 24(2):123–140, 1996.

[5] L. Breiman. Random forests. *Machine learning*, 45(1):5–32, 2001.

[6] X.-j. Chen, F. Xu, R. Xu, S.-M. Yiu, and J.-q. Shi. A practical real-time authentication system with identity tracking based on mouse dynamics. In *Computer Communications Workshops (INFOCOM WKSHPS), 2014 IEEE Conference on*, pages 121–122. IEEE, 2014.

[7] C. Cortes and V. Vapnik. Support-vector networks. *Machine learning*, 20(3):273–297, 1995.

[8] M. Fairhurst, C. Li, and M. Erbilek. Exploiting biometric measurements for prediction of emotional state: A preliminary study for healthcare applications using keystroke analysis. In *Biometric Measurements and Systems for Security and Medical Applications (BIOMS) Proceedings, 2014 IEEE Workshop on*, pages 74–79. IEEE, 2014.

[9] F. L. Greitzer and D. A. Frincke. Combining traditional cyber security audit data with psychosocial data: towards predictive modeling for insider threat mitigation. In *Insider Threats in Cyber Security*, pages 85–113. Springer, 2010.

[10] F. L. Greitzer, L. J. Kangas, C. F. Noonan, A. C. Dalton, and R. E. Hohimer. Identifying at-risk employees: Modeling psychosocial precursors of potential insider threats. *System Science (HICSS), 2012 45th Hawaii International Conference on*, pages 2392–2401, 2012.

[11] M. Harris. Who is anthony levandowski, and why is google suing him?, Feb. 2017.

[12] Y. Hashem, H. Takabi, R. Dantu, and R. Nielsen. A multi-modal neurophysiological study of malicious insider threats. In *Proceedings of the 9th ACM CCS International Workshop on Managing Insider Security Threats*, MIST '17. ACM, 2017.

[13] Y. Hashem, H. Takabi, M. GhasemiGol, and R. Dantu. Towards insider threat detection using psychophysiological signals. In *Proceedings of the 7th ACM CCS International Workshop on Managing Insider Security Threats*, pages 71–74. ACM, 2015.

[14] Y. Hashem, H. Takabi, M. GhasemiGol, and R. Dantu. Inside the mind of the insider: Towards insider threat detection using psychophysiological signals. *Journal of Internet Services and Information Security (JISIS)*, 6(1):20–36, 2016.

[15] J. Hunker and C. W. Probst. Insiders and insider threats-an overview of definitions and mitigation techniques. *JoWUA*, 2(1):4–27, 2011.

[16] P. Kaghazgaran and H. Takabi. Toward an insider threat detection framework using honey permissions. *Journal of Internet Services and Information Security (JISIS)*, 5(3):19–36, 2015.

[17] A. Kaklauskas, M. Krutinis, and M. Seniut. Biometric mouse intelligent system for student's emotional and examination process analysis. In *Advanced Learning Technologies, 2009. ICALT 2009. Ninth IEEE International Conference on*, pages 189–193. IEEE, 2009.

[18] P. Lali, M. Naghizadeh, H. Nasrollahi, H. Moradi, and M. S. Mirian. Your mouse can tell about your emotions. In *Computer and Knowledge Engineering (ICCKE), 2014 4th International eConference on*, pages 47–51. IEEE, 2014.

[19] H. Lee, J. Jung, T. Kim, M. Park, J. Eom, and T. Chung. An application of data leakage prevention system based on biometrics signals recognition technology. In *The 3rd International Conference on Networking and Technology*, 2014.

[20] Y. M. Lim, A. Ayesh, and M. Stacey. The effects of typing demand on emotional stress, mouse and keystroke behaviours. In *Intelligent Systems in Science and Information 2014*, pages 209–225. Springer, 2015.

[21] Y. M. Lim, A. Ayesh, and M. Stacey. Using mouse and keyboard dynamics to detect cognitive stress during mental arithmetic. In *Intelligent Systems in Science and Information 2014*, pages 335–350. Springer, 2015.

[22] P. I. LLC. Cost of cyber crime 2016: Reducing the risk of business innovation, 2016.

[23] C. McKinstry, R. Dale, and M. J. Spivey. Action dynamics reveal parallel competition in decision making. *Psychological Science*, 19(1):22–24, 2008.

[24] F. Monrose and A. D. Rubin. Keystroke dynamics as a biometric for authentication. *Future Generation computer systems*, 16(4):351–359, 2000.

[25] A. N. H. Nahin, J. M. Alam, H. Mahmud, and K. Hasan. Identifying emotion by keystroke dynamics and text pattern analysis. *Behaviour & Information Technology*, 33(9):987–996, 2014.

[26] Y. Park and S. J. Stolfo. Software decoys for insider threat. In *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security*, pages 93–94. ACM, 2012.

[27] M. Pusara and C. E. Brodley. User re-authentication via mouse movements. In *Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security*, pages 1–8. ACM, 2004.

[28] M. B. Salem and S. J. Stolfo. Masquerade attack detection using a search-behavior modeling approach. *Columbia University, Computer Science Department, Technical Report CUCS-027-09*, 2009.

[29] S. Salmeron-Majadas, O. C. Santos, and J. G. Boticario. An evaluation of mouse and keyboard interaction indicators towards non-intrusive and low cost affective modeling in an educational context. *Procedia Computer Science*, 35:691–700, 2014.

[30] C. Shen, Z. Cai, X. Guan, and R. Maxion. Performance evaluation of anomaly-detection algorithms for mouse dynamics. *Computers & Security*, 45:156–171, 2014.

[31] T. soft. Mini mouse macro pro, 2016.

[32] H. Takabi and J. H. Jafarian. Insider threat mitigation using moving target defense and deception. In *Proceedings of the 9th ACM CCS International Workshop on Managing Insider Security Threats*, MIST '17. ACM, 2017.

[33] P. S. Teh, S. Yue, and A. B. Teoh. Feature fusion approach on keystroke dynamics efficiency enhancement. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, 1(1):20–31, 2012.

[34] M. Theoharidou, S. Kokolakis, M. Karyda, and E. Kiountouzis. The insider threat to information systems and the effectiveness of iso17799. *Computers & Security*, 24(6):472–484, 2005.

[35] P. Thompson. Weak models for insider threat detection. *International Society for Optics and Photonics,Defense and Security*, pages 40–48, 2004.

[36] J. S. Valacich, J. L. Jenkins, J. F. Nunamaker Jr, S. Hariri, and J. Howie. Identifying insider threats through monitoring mouse movements in concealed information tests. In *Hawaii International Conference on System Sciences. Deception Detection Symposium*, 2013.

[37] R. Willison and M. Warkentin. Beyond deterrence: An expanded view of employee computer abuse. *MIS quarterly*, 37(1):1–20, 2013.

[38] H. Zandikarimi, F. Lin, C. Carlos, J. Correa, P. Dressner, and V. Monaco. Design of a mouse movement biometric system to verify the identity of students taking multiple-choice online tests. *Proceedings of Student/Faculty Research Day*, 2014.

[39] Y. Zhang, G. Chang, L. Liu, and J. Jia. Authenticating user's keystroke based on statistical models. In *Genetic and Evolutionary Computing (ICGEC), 2010 Fourth International Conference on*, pages 578–581. IEEE, 2010.