How Much is Risk Increased by Sharing Credential in Group?

Hiroaki Kikuchi(✉), Niihara Koichi, and Michihiro Yamada

Graduate School of Advanced Mathematical Sciences, Meiji University,
4-21-1 Nakano, Tokyo 164-8525, Japan
{kikn,niihara}@meiji.ac.jp

Abstract. Insider threats are one of the biggest issues in information management. In practice, the hardest challenge is protecting information assets from malicious insiders. There have been many studies to clarify the factors influencing insiders to perform malicious activities. However, a user study based on a questionnaire cannot be expected to reveal the honest opinions of potential malicious insiders who may give false answers to such studies. In addition, it is hard to observe the comprehensive searches of malicious activities in insider incidents, because available data about incidents are limited. To overcome the difficulties in studying malicious activities in insider threats, we propose a new approach employing epidemiological methodologies with (1) risk amplification, and (2) a logistic model for malicious insiders. We employed a total of 200 subjects from crowd-sourcing services and observed every step that they employed to perform a given task in an environment motivating them to malicious activities (risk amplification). We applied a logistic regression to identify the odds ratio of in favor of malicious activity among those exposed to a factor divided by the odds when not exposed to it. Our experiment shows that a credential shared in group increases the risk of malicious insiders by 3.28 with statistical significance ($p < 0.1$).

1 Introduction

Insider threats are one of the biggest issues in information management. In practice, the hardest challenge is to protect information assets from malicious insiders. There have been many studies to clarify the factors influencing users to perform malicious activities. Leon et al. showed through an online survey how privacy practices affect users' willingness to allow the collection of behavioral data and identified classes of information that most people would not share [4]. Fagan and Kahn introduced a rational decision model and identified key gaps in perception between people who follow common security advice and those who do not [1]. They collected 290 survey responses to the known security recommendations, i.e., updating software, a password manager, two-factor authentication, and changing passwords frequently. Hausawi conducted a survey study to ask security experts about the behavior of end-users [7]. According to these studies, the most negative behavior is sharing credentials in groups. Individuals may

© Springer International Publishing AG 2017
G. Livraga and C. Mitchell (Eds.): STM 2017, LNCS 10547, pp. 103–117, 2017.
DOI: 10.1007/978-3-319-68063-7_7

behave maliciously when they are grouped under group credential and so can *hide* their individual identity within a group umbrella.

However, a user study [2,3] based on questionnaire should not be exposed to reveal the honest opinions of potential malicious insiders who may give false answers to such studies. In addition, it is hard to observe the comprehensive searches of malicious activities in insider incidents, since available data about incidents are limited.

To overcome the difficulties in studying malicious activities in insider threats, we propose a new approach using epidemiological methodologies with (1) risk amplification, and (2) a logistic model for malicious insiders. Our goal is to identify the significant factors in motivating employees to conduct malicious activities. Employees' willings to follow security policies may be affected by environmental conditions. For example, they are likely to ignore security rules with too many requirements, under tight schedule, and with low payment. Among environmental factors, we focus on those that help an employee feel free to use arbitrary activities without monitoring. If employees find that no equipment monitors their activities, they are more likely to cheat on their duties without detection.

In this study, we conducted an experiment in which subjects were asked to complete a given task under varying monitoring conditions. We employed a total of 200 subjects from crowd-sourcing services and observed steps that they performed a given task in an environment motivating them to malicious activities. We applied a logistic regression to identify the odds ratio of the malicious activity among those exposed to a factor divided by the odds when not exposed to that factor. Our experiment shows that sharing credentials in group increases the risk of malicious insiders by 3.28 with statistical significance ($p < 0.1$).

2 Background and Related Work

There were many studies on insider threats.

Capplli *et al.* classified insider threats into three groups: insider IT sabotage, insider theft of intellectual property, and insider fraud [19]. The present work deals with insider fraud.

Cohen and Felson [15] presented the 'routine activity theory,' which argues that most crimes have three necessary conditions: a likely offender, a suitable target, and the absence of a capable guardian. Cressey [16] proposed the fraud triangle model to explain the factors present in every fraud situation: perceived pressure, perceived opportunity, and rationalization. Greitzer *et al.* [13,17] provided some indicators of insider threats based on published case studies and discussions with experienced human resources professionals. According to these studies, various hypothesized causes of insider threats exist. However, because there are so many potential causes of malicious insider threats, which ones have the greatest effect on insider behavior remains unclear [5,6].

Capplli et al. proposed a MERIT model related to insider threats based on investigations of criminal records [20]. Nurse et al. proposed a framework

for characterizing insider attacks [21]. Their models are convenient for administrators in solving the problems and analyzing the risks associated with insider threats. We demonstrated experimentally that placing participants in environments with low levels of surveillance is more likely to lead to insider threats [14]. There were many studies for detecting typical behaviors of malicious insiders [8–12]. Hausawi conducted an interview study to survey security experts about the behavior of end-users [7]. According to these studies, the most negative behavior is sharing credentials in group. However, how much group sharing credentials increases the risk of insider threats remains unclear.

In this paper, we investigate the relationship between sharing credentials in group and the risk of malicious insider threats.

3 Methodology

3.1 Study Design

Our goal is to identify the significant factors in motivating employees to conduct malicious activities. An employee's willings to follow security policies may be affected by environmental conditions. For example, they are likely to ignore security rules that have too many requirements when schedules are too tight, and salaries are too low. Among environmental factors, we focus on those that help an employee feel free to perform arbitrary activities without monitoring. If employees find that no equipment monitors their activities, they are more likely to cheat without detection.

In this study, we conducted an experiment in which subjects were asked to complete a given task under varying conditions of monitoring. We observed how they behaved in a given environment and quantified the risk of malicious insiders by counts of malicious activities in each of environment. The set of subjects was divided into the following (mixed) groups;

- Group **sharing credentials**. Subjects are given a single common credential, e.g., "administrator" or "guest", to have access to resources. Even if a subject makes a mistake, the activity is logged with the common identity and the subject cannot be identified, except that one of the group did it. Hence, sharing credentials could spoil the traceability of transactions. Knowing that their activities cannot be distinguished, a potential insider might frequency perform malicious activities more frequently.
- Group assigned to **individual credentials**. Ordinarily, subjects are given individual credentials (identity and password) and use them to sign in to a website before completing a task. Hence, they are supposed to follow an instruction of task and no malicious activity would be taken in the group.
- Group with **ID indicated**. The website explicitly indicates the subject's identity at the top of the page so that subjects can notice that they sign-in with individual credentials. The indication of identity reminds them to consider that all behaviors will be logged with their identity.

– Group **no ID indicated**. This is the opposite of the ID indicated group. Because no identity is indicated, subjects may not be sure whether their activities are monitored.

We investigate differences in the number of malicious behaviors in these groups. Our research question is *whether individuals do behavior more malicious behaviors when group identity is shared than individual can be identified.* To determine the question, we test the null hypothesis

H_0**:** The proportion of subjects who behave maliciously among the group where subject share a common credential is identical to the proportion of malicious subjects assigned in individual credentials.

against the following alternative hypothesis:

H_1**:** The subjects sharing common group credentials are more likely to perform malicious activities.
H_2**:** The subjects without their identities indicated are more likely to perform malicious activities.

3.2 Subjects

To investigate the differences between groups, we collected a total of 198 subjects using Lancers Inc.[1], the Japanese crowd-sourcing service, in October 2016. We required Lancers' certified workers who had enrolled in the service with their official certificates of Japanese residence. All subjects who completed the given task were paid 250 JPY (equivalent 2.2 USD), which is typical for a task that takes approximately 20 min to complete.

We assigned subjects round robin to one of four groups, A, B, C, and D, corresponding to hypotheses H_1 and H_2 as defined in Table 1. For example, all subjects in group A shared the same identity "Guest" which was not identified while they completed a task. If both hypotheses are true, group A is most likely and group D is least likely to participate in malicious activities. For groups B and D, we assigned individual identities of the form "user*nnnnn*" where n is a random decimal digit. The number of subjects in group D is the smallest because some of them withdrew from the task.

After reviewing and signing to a consent form, subjects answered demographic questions. Table 3 shows the demographics of our subjects[2]. We found that the subjects' attributes were randomly distributed over the four groups without any significant skew.

[1] http://www.lancers.jp.

[2] We plan to make all data publicly available from our website http://windy.mind.meiji.ac.jp/kiknlab2014/paper.html in a way that does not compromise anyone's privacy.

3.3 Micro-task of Testing Website

To simulate the experience of working in an IT company, we instructed the subjects to evaluate the performance of a target website providing a search service and gave them a specified query list of 70 (Japanese) words to test. We explained to them that the aim was to test the usability of a developed website and we wished to know the performance when many queries were sent in a short period. Subjects were required to test at least 50 queries out of the given 70 words, but were allowed to complete their task even though they had not yet tested the minimum number of queries.

After testing the query search of the website, the subjects were asked some questions such as the correctness of the query, the performance of the response, and their experience using the website. The search service was implemented using Google API and the query lists were collected randomly from websites. For experimental purposes, we added a few unusual words to the list.

3.4 Difficulties in Observation

Although we could see all of the steps that our subjects took in the given task, it was not easy to observe malicious activities for several reasons. The followings are difficulties that we faced in observing malicious activities in our experiment.

- *No motivation.* The subjects were hired on an experimental and short-term contract. Hence, they were not motivated to take risks to perform malicious activities that could be detected easily and result in canceling their payment. If they found any difficulty in their task, they could simply cancel their agreement. These are differences between the experiment and a real business environment. Without suffering persistent long-term stress in the working environment, people may not want to behave maliciously.
- *Monitor without identity.* We wanted to observe how subjects behave when they find that no one monitors them. This is a contradictory requirement. Without assigning unique identities, there is no way to distinguish some subjects. Alternatively, we may use Http cookies or hidden links embedded in the website to track target subjects. However, if we use this tracking technique, an advanced subject could suspect the use of tracking and behave as if they were monitored.
- *Small effect of individual credentials.* We expected that subjects assigned individual credentials would be less likely to work maliciously. However, they did not take the credentials serious, even when unique identities were given because they knew the identities were issued for an experimental purpose and only for one-time use. In an experiment, there is little difference between shared and individual credentials.

3.5 Risk Amplification

To overcome the difficulties caused by limited motivation of malicious behavior in the experimental environment, we used a distorted environment, called *risk*

Table 1. Hypotheses and groups

Group	H_1 (account)	H_2 (ID indication)	N
A	Shared	No	52
B	Individual		52
C	Shared	Yes	46
D	Individual		48

Table 2. Schedule of delays with respect to iteration s

Iteration s	Delay [s]	Copy-and-paste
1–4	0	
5–12	1	
13–18	2	
19–22	3	
23–30	4	
31–32	20	
33–36	2	
37–40	9	
41–42	20	Disabled
43–44	5	Disabled
45–46	9	Disabled
47<	5	Disabled

Table 3. Demographics of our subjects

Demographic	A	B	C	D	Total
Gender					
Male	28	30	23	28	109
Female	24	22	23	20	89
Age					
<19	0	0	1	0	1
20–29	8	2	7	6	23
30–39	18	19	17	22	76
40–49	16	24	14	14	68
50–59	6	5	6	5	22
60<	4	2	1	1	8
Occupation					
Office worker	16	17	6	9	48
Government	1	0	0	0	1
Self-employed	13	13	15	16	57
Part-time worker	7	5	2	5	19
Homemaker	6	10	13	8	37
Student	0	0	1	1	2
Unemployed	5	6	4	6	21
Other	4	1	5	3	13
N	52	52	46	48	198

amplification, in which subjects are required to work in an environment with some obstacles. If a subject behaves maliciously under the risk amplification condition with a certain probability, he or she could act malicious in an ordinary condition with smaller but proportional probability. The observed probability is useful to estimate the true magnitude of risk in arbitrary conditions. Risk amplification allows us to make small probabilities look larger so that we can examine risks of relevant conditions.

Scheduled Delay. To frustrate subjects with the website response, we manipulated the performance of the website as scheduled in Table 2. The duration of delay varies with iteration of query, s. For example, the response is delayed by 20 s at the 31st and 32nd iterations. Meanwhile, subjects might consider that some intensive computations were happening at the web server and thus be motivated to complete their task before testing the minimum number of queries, which is treated as a malicious activity.

Disabled Copy-and-Paste. Similar to the scheduled delays in Table 2, we used Javascript to disable the copy-and-paste function of the browser for iterations greater than 40 ($s > 40$). We chose a few unusual long words for the query list so that subjects would want to copy and paste to test them without carefully typing the long word. Hence, they might become irritated by the suddenly disabled

copy-and-paste and be motivated to replace the annoying unusual word with random words, which is regarded as a malicious activity.

No Indication of Iteration. The iteration counts s were not available to subjects to make them believe that the iterations were not significant in completing task. We accepted any completion report before or after the minimum number of queries (50) and allowed subjects to answer questions about usability of the website, even if they had not tested the full 50 queries, which is counted as a malicious activity.

3.6 Tracking Subjects

To track subjects sharing credentials in group and monitor all activities made without unique individual identities, we assigned unique query lists to subjects. By matching the log of tested queries with the query lists assigned to the subjects, we could identify exactly who sent the queries and examine whether they performed any malicious activities while testing the target website.

For those who had individual credentials, tracking was trivial. We required them to sign in to the target website using their Lancers ID for which the payment was made. The use of the official ID helped convince them that their activities were monitored by their employer, and that any fault in their duties could cancel the payment. Thus, individual credentials encouraged subjects to refrain from behaving maliciously.

In these ways, we enlarged the difference of effect in malicious activities between shared and individual credentials and quantify how much risk is increased with sharing group credential against assigning individual ones.

3.7 Malicious Activities

1. *Completing a task with fewer iterations.* In this activity, the task was completed earlier than expected by testing fewer than the minimum 50 iterations.
2. *Replacing given words (queries) with random ones.* When a query does not exactly match any of the words assigned to the subject, we regard it as malicious behavior by the subject who typed in a random word. This malicious activity occurs when the subject wishes to proceed without typing a long unusual word. Similar activities such as querying with null strings or typing error are also classified into this category.
3. *Privileged Access.* Subjects were instructed that privileged access was prohibited in the experiment where we prepared a fake "administrator" link. Therefore, if a subject tried to click a privileged link to modify the records of the task, we regarded it as malicious.

4 Study Results

4.1 Elapsed Time

Figure 2 shows the cumulative processing time T_i [s] with respect to iterations s of querying (indicated as search count). We show typical behaviors of four

representative users in different colors. In general, the elapsed time increases monotonically with iteration, but it sometime increases sharply. For example, the blue line rises at $s = 41$, which was caused by the scheduled delay mentioned in Sect. 3.5.

The typical behaviors of the subjects are classified into the following four patterns:

1. Terminating task before testing the required number of iterations ($s < 50$). User 1 indicated in red is malicious.
2. Terminating the task when a constrains is encountered (scheduled delay or disabled copy-and-paste). User 3 in green stops querying at around $s \geq 41$ when a response is delayed by 20 s. This is labeled as malicious.
3. Completing a task as soon as the minimum iteration is satisfied. User 2 indicated in blue is legitimate.
4. Completing task by testing all 70 words in a given list. User 4 indicated in blue, plotted always as the highest of the four, is legitimate (Fig. 1).

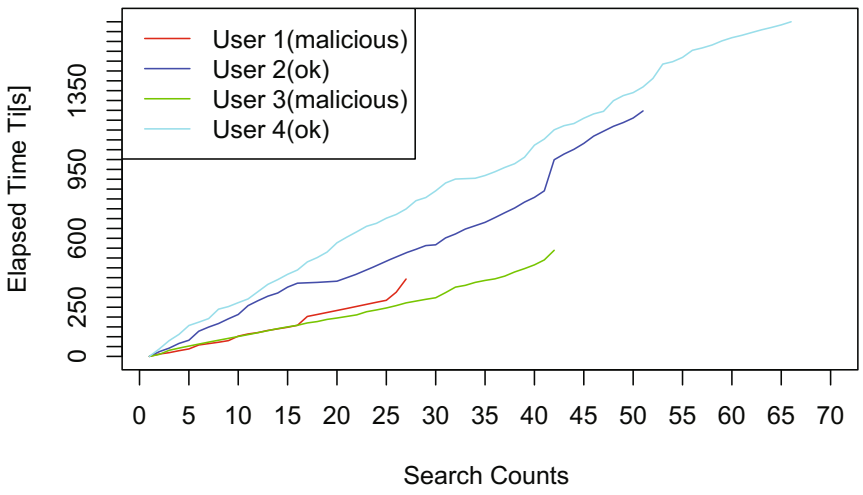

Fig. 1. Elapsed times for a sample of users against iteration (Color figure online)

4.2 Malicious Activities

Table 4 shows the number of malicious subjects, defined as those who performed at least one of the malicious activities, defined in Sect. 3.7. We find slightly decreasing tendency of malicious activities in the order of groups $A > B > C > D$, as assumed in hypothesis, H_1: subjects sharing a common group credential (A, C) are more likely to behave maliciously than those who sign-in with individual credentials (B, D).

Table 4. Malicious activities

Activity	*A*	*B*	*C*	*D*	Total
(1) Fewer iteration	11	8	9	7	35
(2) Random queries	5	3	1	2	11
(3) Privileged access	1	1	0	0	2
N	17	12	10	9	

Table 5. Malicious subjects with fewer iteration

Demographic	*A*	*B*	*C*	*D*	Total
Gender					
Male	7	5	6	6	24
Female	4	3	3	1	11
Age					
<19	0	0	1	0	1
20–29	1	0	1	2	4
30–39	6	1	3	3	13
40–49	0	3	2	1	6
50–59	1	2	1	0	4
60<	3	2	1	1	7
Occupation					
Office worker	3	3	2	2	10
Government	1	0	0	0	1
Self-employed	4	0	3	3	10
Part-time worker	1	0	0	0	1
Homemaker	1	2	1	0	4
Student	0	0	1	1	2
Unemployed	1	2	0	1	4
Other	0	1	2	0	3
N	11	8	9	7	35

The most frequent malicious activity is (1) completing task with fewer iterations, which is followed by (2) replacing required with random words, and (3) privileged access. We show the demographics of malicious subjects in Table 5. The number of malicious subjects is generally proportional to the population of each demographic groups (we show hypothesis testing later). However, note that older subjects are more frequently detected as malicious than younger ones. For instance, the seven (87.5%) out of eight subjects over 60 years of age were malicious users. By investigating the log of their behaviors, we observed that they usually spent a longer time on and often duplicated the same query.

Since they might be unfamiliar with this type of task and might have lost their way before completing it, we should exclude the older subjects as outliers and focus on the younger ones.

4.3 Cumulative Relative Frequency

A cumulative relative frequency, $Cu(s)$, defined as the fraction of subjects who completed the task at iteration s as a proportion of the group, gives more detailed malicious behaviors. Figure 2 shows the changes in cumulative relative frequencies of the four groups A, B, C and D. We show a vertical dotted line at $s = 50$ which is the threshold iteration for regarding subjects as malicious.

The higher the frequency is, the more subjects completed the task, and more malicious activity occurred in the group. For example, group A has $Cu(s < 50) = 0.21 = 21/52$, which means that 21 subjects out of 52 members of A did not satisfy the minimum requirement of 50 queries (malicious subjects). The tendency of increased malicious activities with shared credentials is enhanced when we examine the subset of workers aged 30 through 39, as shown in Fig. 3. The fractions of malicious subjects, $Cu(s < 50)$, of groups A, B, C and D are $0.33, 0.05, 0.18$, and 0.14, respectively. We note that there were more malicious subjects in group A than any other group. Therefore, the environmental condition of the group, i.e., sharing group credentials without ID indication, must have an effect in increasing the risk of insider threats.

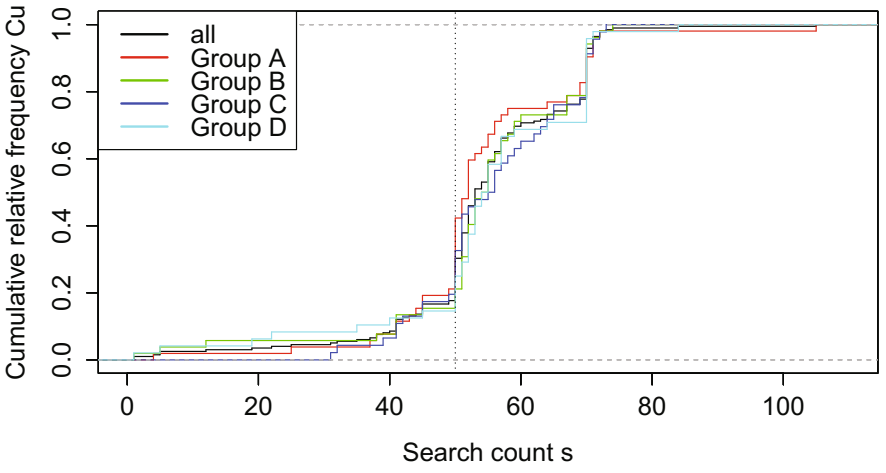

Fig. 2. Cumulative relative frequencies of groups (all members)

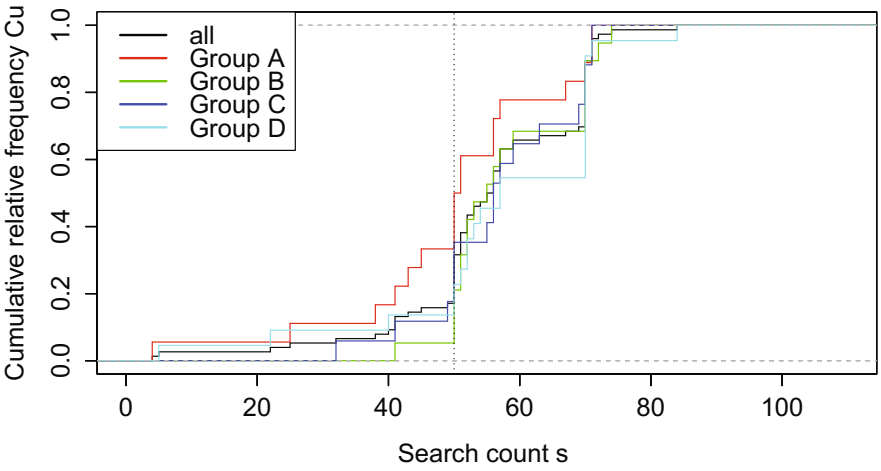

Fig. 3. Cumulative relative frequencies of groups (for subjects aged 30–39)

4.4 Hypothesis Testing (Fisher's Exact Testing)

To test the null hypothesis H_0 that two proportions of malicious subjects with/without sharing group credentials (groups A plus C) are identical, we used the Fisher's exact test. To carry out the test, we have the 2×2 contingency tables for each malicious activity as shown in Table 6, where there are total of eight contingency tables computed to test hypothesis H_1 (sharing identity) and H_2 (indication of identity). Based on the observation in Sect. 4.3, we added another table for the subset of malicious subjects restricted to 30–39 years of age.

For a hyper-geometric distribution with 1 degree of freedom, we have the probabilities followed by the counts in the contingency tables in Table 7.

Table 6. Contingency tables of counts of malicious subjects

Activities	Malicious	H_1 (shared ID)		H_2 (no ID indicated)	
		Shared $A+C$	Individual $B+D$	Not Indicated $B+D$	ID indicated $C+D$
Fewer iteration	Yes	20	15	19	16
	No	78	85	85	78
Random query	Yes	6	5	8	3
	No	92	95	96	91
Privileged access	Yes	1	1	2	0
	No	97	99	102	94
Fewer iteration (30's)	yes	9	4	7	6
	No	26	37	30	33

Table 7. Results of Fisher's exact test

Activities	Hypothesis	p
Fewer iteration	H_1 (shared)	0.3551
	H_2 (no ID indicated)	0.8539
Random query	H_1 (shared)	0.7662
	H_2 (no ID indicated)	0.2201
Privileged access	H_1 (shared)	1.0000
	H_2 (no ID indicated)	0.4987
Less iteration (30s)	H_1 (shared)	**0.0763**
	H_2 (no ID indicated)	0.7659

With the significance level $p < 0.05$, the probabilities are too high to reject the null hypothesis for this case. However, with $0.05 < p < 0.1$, we can reject the null hypothesis that there is no association between the malicious activities in the subset in their 30s and the condition of sharing group credential, hence we conclude that there is evidence of an association between sharing group credentials and malicious activities.

Our experiment did not reveal quite strong confidence to the hypothesis that sharing group credential increases malicious behaviors. We think the reason of this caused by small subsets of subjects such as over-60-years group in Table 5. We don't think that they intended to do maliciously but unfortunately they were recognized as malicious according to our criteria of malicious behaviors. Moreover, they are not eligible for our study that aims to identify significant factor in insider threats in industry. Hence, we should design an experimental condition more carefully for selection proper subset of workers.

4.5 Logistic Regression

To quantify the risk introduced by sharing credentials, we performed a multivariable logistic regression analysis on the subset of subjects aged their 30s. Our logistic regression model has a dependent variable for the outcome of malicious activity of (1) fewer iteration and multiple independent variables; x_1, a sharing group credential, x_2, a gender, occupations such as x_3, "part-time worker", x_4, "office worker", and so on, as shown in Table 8. Let p be probability that individuals in their 30s will perform malicious activity of completing the task with fewer iteration. The logit of our model is

$$\log \frac{p}{1-p} = -16.75 + 1.189x_1 + 1.165x_2 + \cdots + 12.90x_7,$$

where the coefficient of x_1 (sharing group credential) is statistically significant with 90 % ($Pr < 0.1$) confidence level. Therefore, the estimated odds ratio of

Table 8. Results of logistic regression (* shows the significant level of $Pr < 0.1$)

	Variables	Coefficient	Std. Error	z value	$Pr(>\|z\|)$
	(Intercept)	−16.75	1455.39	−0.012	0.991
1	sharing ID	**1.189**	0.675	1.760	0.0784*
2	Male	1.165	0.902	1.292	0.196
3	Part-time worker	14.40	1455.40	0.010	0.992
4	Office worker	13.94	1455.40	0.010	0.992
5	Self-employed	13.80	1455.40	0.009	0.992
6	Homemaker	14.17	1455.40	0.010	0.992
7	Unemployed	12.90	1455.40	0.009	0.993

having malicious activity (fewer iteration) for subjects sharing credentials versus those who have individual credentials is

$$\begin{aligned}\widehat{OR} &= \frac{Pr(mal.|sharing)}{1 - Pr(mal.|sharing)} \Big/ \frac{Pr(mal.|individual)}{1 - Pr(mal.|individual)} \\ &= e^{1.189} = 3.28,\end{aligned}$$

which implies that the risk of malicious activity when credentials are shared is about three times higher than when they are not.

5 Conclusions

We have proposed a new approach to identify significant factors in insider threats. In our proposed method, a set of subjects work on a simple task, and we observes how many malicious activities are performed in varying conditions. We propose a distorted environment, called *risk amplification*, in which subjects are required to work in the presence of some obstacles. Subjects who behave maliciously under the risk amplification condition with a certain probability can be expected to behave maliciously in ordinary conditions with smaller but proportional probability. The observed probability is useful to estimate the true magnitude of risk in arbitrary conditions.

We quantified the risk introduced by sharing group credentials, by performing a multi-variable logistic regression analysis. Our experimental results showed that the estimated odds ratio of having malicious activity among subjects who share credentials is 3.28 compared with those who do not. We conclude that the risk of malicious activity occurring when sharing credentials is about three times higher than that when not.

Our future works include a future investigate primal factors to make subject motivate malicious activities, and a generalization of our experimental results to real one. Since our experiment has some limitations, e.g., the duration of observation, the number of subjects, the kinds of tasks, and the environment, we plan to conduct a long-term experiment where subjects have more chances to behave maliciously.

References

1. Fagan, M., Khan, M.M.H.: Why do they do what they do?: a study of what motivates users to (not) follow computer security advice. In: Proceedings of 12th Symposium on Usable Privacy and Security (SOUPS 2016), pp. 59–75 (2016)
2. Rao, A., Schaub, F., Sadeh, N., Acquisti, A., Kang, R.: Expecting the unexpected: understanding mismatched privacy expectations online. In: Proceedings of 12th Symposium on Usable Privacy and Security (SOUPS 2016), pp. 77–96 (2016)
3. Ion, I.,Reeder, R., Consolvo, S.: "... no one can hack my mind": comparing expert and non-expert security practices. In: Eleventh Symposium on Usable Privacy and Security (SOUPS 2015), pp. 327–346 (2015)
4. Leon, P.G., Ur, B., Wang, Y., Sleeper, M., Balebako, R., Shay, R., Bauer, L., Christodorescu, M., Cranor, L.F.: What matters to users? Factors that affect users' willingness to share information with online advertisers. In: Proceedings of the SOUPS 2013. ACM (2013)
5. Aurigemma, S., Panko, R.: A composite framework for behavioral compliance with information security policies. In: Proceedings of the 2012 45th Hawaii International Conference on System Sciences, pp. 3248–3257. IEEE Computer Society (2012)
6. Renaud, K., Goucher, W.: The curious incidence of security breaches by knowledgeable employees and the pivotal role a of security culture. In: Tryfonas, T., Askoxylakis, I. (eds.) HAS 2014. LNCS, vol. 8533, pp. 361–372. Springer, Cham (2014). doi:10.1007/978-3-319-07620-1_32
7. Hausawi, Y.M.: Current trend of end-users' behaviors towards security mechanisms. In: 4th International Conference on Human Aspects of Information Security, Privacy, and Trust, pp. 140–151 (2016)
8. Spitzner, L.: Honeypots: catching the insider threat. In: Proceedings of 19th Annual Computer Security Applications Conference, pp. 170–179 (2003)
9. Azaria, A., et al.: Behavioral analysis of insider threat: a survey and bootstrapped prediction in imbalanced data. IEEE Trans. Comput. Soc. Syst. **1**, 135–155 (2014)
10. Legg, P.A., et. al.: Caught in the act of an insider attack: detection and assessment of insider threat. In: IEEE International Symposium on Technologies for Homeland Security (2015)
11. Legg, P.A.: Visualizing the insider threat: challenges and tools for identifying malicious user activity. In: 2015 IEEE Symposium on Visualization for Cyber Security (VizSec), pp. 1–7 (2015)
12. Greitzer, F.L., et al.: Identifying at-risk employees: modeling psychosocial precursors of potential insider threats. In: 2012 45th Hawaii International Conference on System Science (HICSS), pp. 2392–2401 (2012)
13. Greitzer, F.L., Frincke, D.A.: Combining traditional cyber security audit data with psychosocial data: towards predictive modeling for insider threat mitigation. In: Probst, C., Hunker, J., Gollmann, D., Bishop, M. (eds.) Insider Threats in Cyber Security. Advances in Information Security, vol. 49, pp. 85–113. Springer, Boston (2010). doi:10.1007/978-1-4419-7133-3_5
14. Niihara, K., Kikuchi, H.: Primary factors of malicious insider in E-learning model. In: HCI International 2016 - Posters' Extended Abstracts: 18th International Conference. Proceedings, Part I, pp. 482–487 (2016)
15. Cohen, L.E., Felson, M.: Social change and crime rate trends: a routine activity approach. Am. Sociol. Rev. **44**(4), 588–608 (1979)
16. Cressey, D.R.: Other People's Money: A Study in the Social Psychology of Embezzlement. Free Press, Glencoe (1953)

17. Greitzer, F.L., et al.: Identifying at-risk employees: modeling psychosocial precursors of potential insider threats. In: 2012 45th Hawaii International Conference on System Sciences, pp. 2392–2401 (2012)
18. Fagade, T., Tryfonas, T.: Security by compliance? A study of insider threat implications for Nigerian banks. In: Tryfonas, T. (ed.) HAS 2016. LNCS, vol. 9750, pp. 128–139. Springer, Cham (2016). doi:10.1007/978-3-319-39381-0_12
19. Cappelli, D., Moore, A., Trzeciak, R.: The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes. (Theft, Sabotage, Fraud). Addison-Wesley Professional, Boston (2012)
20. Cappelli, D., et al.: Management and Education of the Risk of Insider Threat (MERIT): System Dynamics Modeling of Computer System. Carnegie Mellon University, Software Engineering Institute (2008)
21. Nurse, J.R.C. et al.: Understanding insider threat: a framework for characterising attacks. In: 2014 IEEE of the Security and Privacy Workshops (SPW), San Jose, CA, pp. 214–228 (2014)