Decision tree analysis on environmental factors of insider threats

Michihiro Yamada, Koichi Niihara, Hiroaki Kikuchi (Meiji University, Japan)

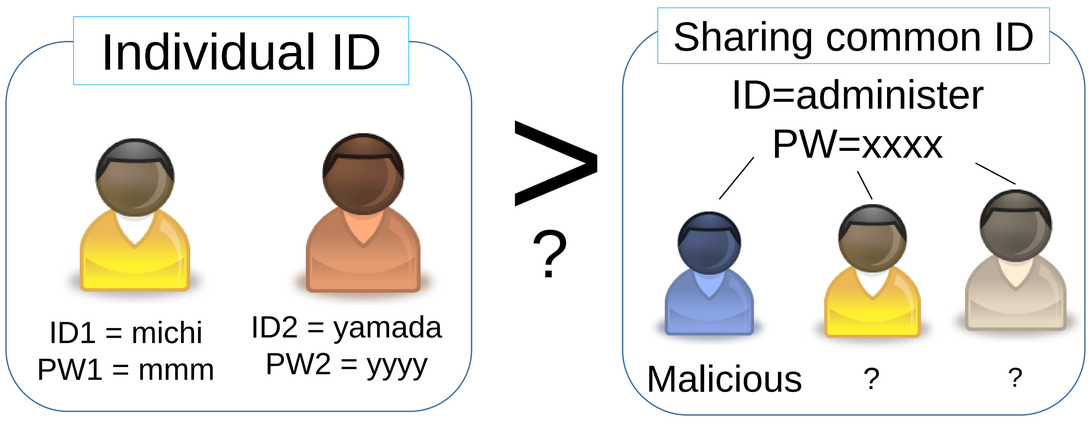
明治大学 MEIJI UNIVERSITY

Background

In information security management, insider threat is one of the biggest threats.

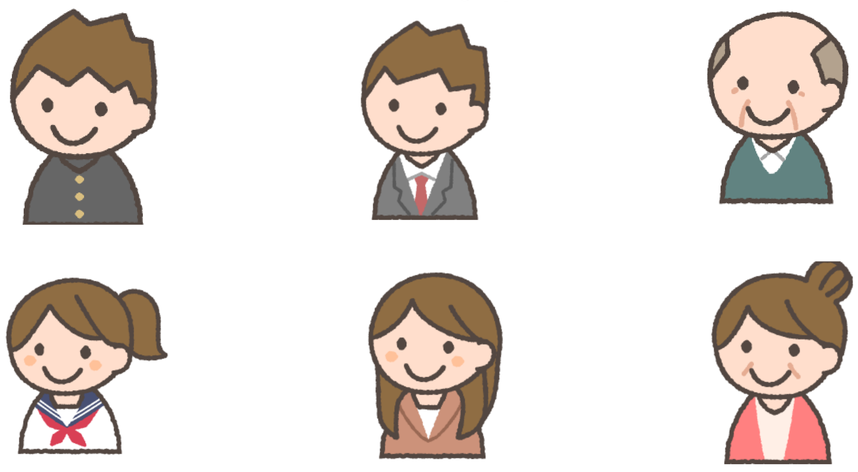
Since there are too many involved factors, it is not clear which factor plays the most significant role in malicious activities.

Research Question 1:



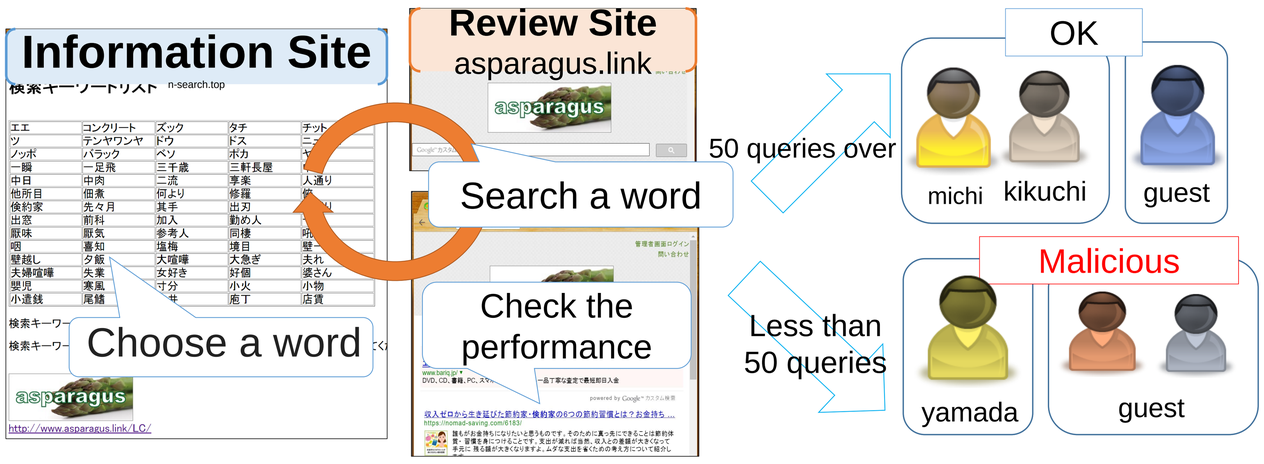
How much risk?

Question 2:
Who is the most risky person ?



A task and definition of malicious activity

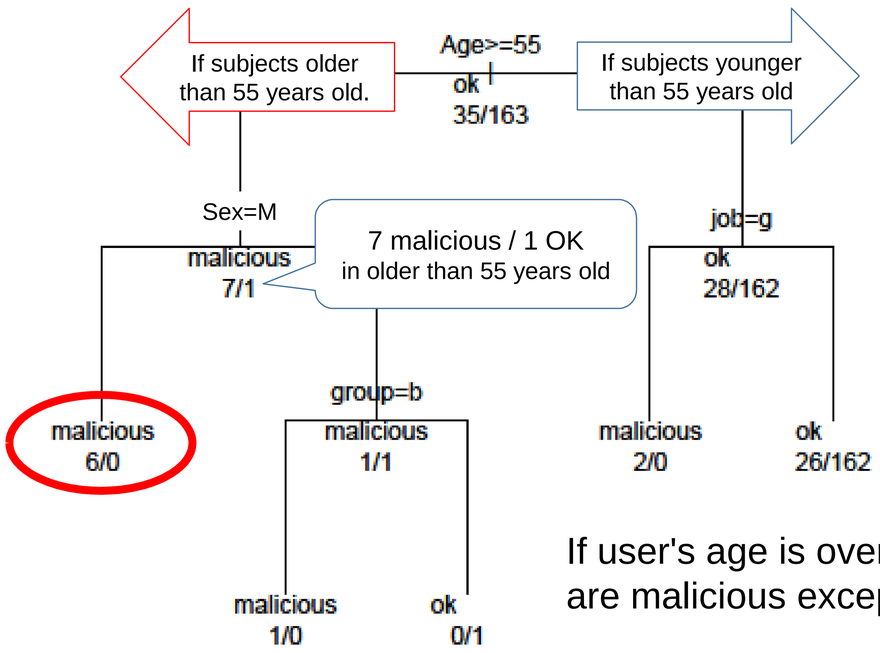
We collected 198 workers from cloud sourcing service.
We divided them into two groups; one is individual ID and the other is sharing common ID.
A task is to check performance of search engine with more than 50 queries chosen from the list.



Summary of experimental result

Group	Sharing common IDs Malicious	Sharing common IDs N	individual IDs Malicious	individual IDs N	total Malicious	total N
Sex male	13	51	11	58	24	109
Sex female	7	47	4	42	11	89
Age -19	1	1	0	0	1	1
Age 20-29	2	15	2	8	4	23
Age 30-39	9	35	4	41	13	76
Age 40-49	2	30	4	38	6	68
Age 50-59	2	12	2	10	4	22
Age 60-	4	5	3	3	7	8
Job office worker	5	22	5	26	10	48
Job public servant	1	1	0	0	1	1
Job self employed	7	28	3	29	10	57
Job parttime worker	1	9	0	10	1	19
Job houseworker	2	19	2	18	4	37
Job student	1	1	1	1	2	2
Job unemployment	1	9	3	12	4	21
Job others	2	9	1	4	3	13
total	20	98	15	100	35	198

Decision Tree

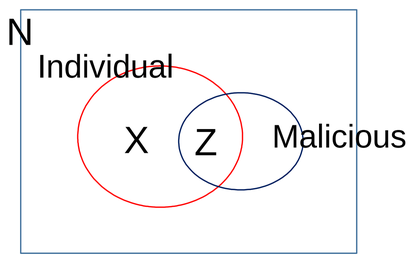


If user's age is over 55 then 7 subjects are malicious except 1 honest (at Sex=b).

Association rule

No.	Left Hand Side	Right Hand Side	support	confidence	lhs.support	lift
1	individual IDs, self-employed ⇒	Judge=ok	0.131	0.896	0.146	1.089
2	individual IDs, 40's ⇒	Judge=ok	0.171	0.894	0.191	1.086
3	individual IDs, 30's ⇒	Judge=ok	0.186	0.902	0.207	1.096
4	individual IDs, Male, self-employed ⇒	Judge=ok	0.111	0.916	0.121	1.113
5	Sharing common ID ⇒	Judge=malicious	0.101	0.204	0.494	1.154

90% of 30's people who use individual ID, didn't play insider. (Confidence)



Support = Z/N

Confidence = Z/X

Logistic regression

	Estimate	Pr(>|t|)	Odds
(Intercept)	-0.107	0.384	2.41E-02
Group individual IDs	-0.054	0.306	6.78E-01
Sex male	0.048	0.465	1.41E+00
Age	0.006	0.023	1.05E+00
Job office worker	0.097	0.297	2.18E+00
Job public servant	0.668	0.082	2.90E+07
Job self employed	0.031	0.735	1.38E+00
Job parttime worker	-0.060	0.566	4.41E-01
Job others	0.087	0.476	1.86E+00
Job student	1.012	0.000	3.37E+08
Job unemployment	0.064	0.558	1.74E+00

$$log\frac{Pr(malicious \mid x)}{1-Pr(malicious|x)} = -1 - 0.05x_1 + 0.048x_2 \cdots + 0.064x_{10}$$

Sharing common ID could increase a risk of malicious insider by 1/0.67 than without sharing.

Conclusion

We studied the factor analysis of malicious insider in total of 198 subjects with some conditions.

Older than 55 years old men played malicious activity with 6 out of 6.

Our experiment showed that sharing ID could increase a risk of malicious insider.

Sharing identity could increase a risk of malicious insider by 1/.68 from odds.

References

S137: Human Behaviour in Security and Privacy (Thursday, 13 July 2017 13:30 – 15:30 Room: 111)
Sharing or Non-sharing Credentials: a Study of what Motivates People to be Malicious Insiders
Koichi Niihara, Michihiro Yamada, Hiroaki Kikuchi, Meiji University, Japan