4ZD-05

An Importance Estimation Method Based on Resource Lineage

Yingtao Zhou† Hirokazu Hasegawa† Hiroki Takakura‡

Nagoya University† National Institute of Informatics‡

1 Introduction

Targeted attacks are the problem frequently faced by various organizations today. These attacks are optimized for targets and designed to capture sensitive information. Therefore, recent countermeasures have focused on reducing the damage that occurs after malware intrusion.

We have proposed A Countermeasure Recommendation System for Indicating Residual Risks [1] to increasing ability that handling the cybersecurity incident. Subsequently, the concept that risk of information leakage remaining in the internal network, so-call Residual Risks, was advocated.

There have been studies on security risk assessment. Masoud et al. proposed a Bayesian Decision Network-Based Security Risk Management Framework [2] which includes a risk assessment method based on attack graphs and temporal probability. However, this framework is unable to reduce or eliminate the residual risk.

We have designed an assessment System for Residual Risks of Information Leakage in Incident Countermeasures [3]. The system includes a resource importance estimation method to help calculating residual risks.

However, the existing importance estimation method is only suitable for importance calculation of internal company information resource. Therefore, we proposed a new importance estimation method based on resource lineage in this paper, which fulfills importance calculation in both internal and external sensitive information.

2 Previous System

2.1 Existing Formula

The existing importance estimation equation, as shown in (1), uses the number of all employees ($|N_{ALL}|$), the number of employees who can access the limited resource i ($|N_i|$) and the weight of accessible employees (W_p) to calculate the importance of resource i (I_i). The weight is derived from the position of accessible employees as shown in Figure 1. However, it will introduce incorrect result when we calculate importance of the sensitive information resource which is external lineage if we use existing method.

$$I_i = \frac{|N_{ALL}|}{|N_i|} \times max\{W_p : p \in N_i\} \quad (1)$$

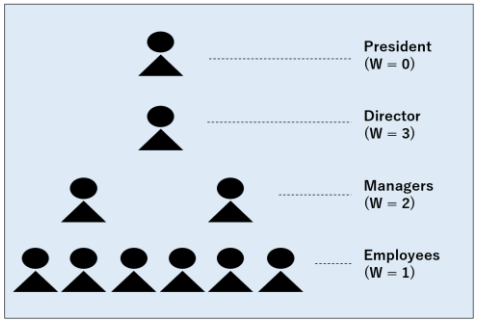

Figure 1: Company Position and Weight

2.2 Issue of Weight

The correlation between position of employees and the importance of the resource that employees can access is not always a positive correlation. In particularly, there are not an explicit correlation between a position in company and the importance of external resource. In other word, existing weight is invalid when we implement importance calculation of external resource.

2.3 Issue of Max Function

In existing papers, it is assumed that there is no case where the person with the highest position can access all resources. Consequently, using max function does not fix importance value. However, in external resource case, the project manager has access to all resource about his project. Therefore, the output of max function be fixed if we used existing method.

3 Proposed Method

3.1 General Design

We proposed an importance estimation method

based on resource lineage to complete with external resource. The new equation (2) adopts new setting of position and its weight (W'_p), which based on project, shown as Figure 2. We keep calculation of internal resource unchanged and use the number of all employees who can access the limited resource as existing method did. On the other hand, we use average function instead of max function, and new setting of position inside project and its weight instead of using company position and its weight.

$$I_i = \frac{|N_{ALL}|}{|N_i|} \times \begin{Bmatrix} max\{W_p : p \in N_i\}, if\ i \in internal\ data \\ avg\{W'_p : p \in N_i\}, if\ i \in external\ data \end{Bmatrix} \quad (2)$$

Remark: Avg = Average

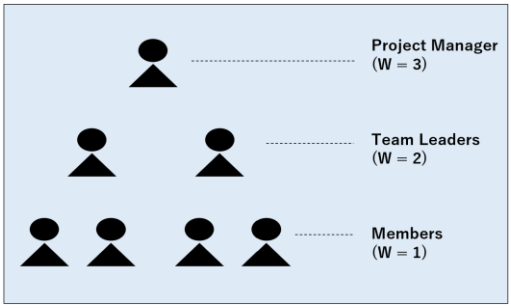

Figure 2: Project Position and Weight

3.2 Average Function

The graph of the average function, whose input are weights of project position, matches the negative correlation between the number of people who can access the limited resource and the importance of this resource.

For instance, number of project people is totally 10, PM and TL are 1 person each, and the remaining 8 people are members. Based on these cases, we did a simulation and results shown as Table 1. The result confirmed our expectation.

3.3 Project Position and Its Weight

First, we make the position in the project, the same as the position in the company, in a hierarchical structure. In addition, the project manager (PM) as responsible personnel for the project. Finally, the weight of PM is set to 3, and the weight is deducted by 1 as the position goes down.

Previous setting guarantee that the correlation between the project position and the importance of external resource is positive.

Table 1: Simulation Result of Average Function

Case	Accessible personnel	Average function
1	Tanaka PM	**3.0**
2	Tanaka PM, Yamada TL	**2.5**
3	Tanaka PM, Yamada TL, Nakamura	**2.0**
4	Tanaka PM, Suzuki(finance)	**2.0**
5	Whole project member	**1.3**

Remark: PM: Project Manager (weight = 3) TL: Team leader (weight = 2)

4 Conclusion

We proposed an importance estimation method based on resource lineage to complete with both internal and external resource. With this proposal, we made calculation of resource importance more accurate, consequently increased calculation accuracy of residual risks. In part 3.3, we created the position of project to suit external resource. In part 3.2, simulation show that average function guarantees positive correlation between the position of project and the importance of external resource, and negative correlation between the number of people who can access the limited resource and the importance of this resource.

However, related problem remains to be discussed. That is the relation between company position and project position. For without loss of generality, we try to avoid setting up this relation in human resource server. Therefore, we want creating an algorithm to calculate this relation automatically in future.

5 Reference

[1] H. Hasegawa, Y. Yamaguchi, H. Shimada, and H. Takakura, “A Countermeasure Recommendation System for Indicating Residual Risks,” The 33rd International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC2018), No.33, pp.856-859, 2018.

[2] Masoud Khosravi-Farmad, Abbas Ghaemi-Bafghi, “Bayesian Decision Network-Based Security Risk Management Framework,” Journal of Network and Systems Management, vol.28, pp.794-1819, 2020.

[3] Tomohiro Noda, Hirokazu Hasegawa and Hiroki Takakura, “Assessment System for Residual Risks of Information Leakage in Incident Countermeasures,” The 4th International Conference on Information Science and Systems (ICISS 2021), pp.41-46, 2021.