The Trend of the Security Research for the Insider Cyber Threat

Jaeseung Hong, Jongwung Kim, Jeonghun Cho
School of Electrical Engineering and Computer Science,
Kyungpook National University. 1370, Sangyuk-dong, Buk-gu,
Daegu, Korea {psman2, brewer, jcho}@ee.knu.ac.kr

Abstract

In this paper, we discuss an insider security which has been one of the biggest issues in the network security. By surveying and analyzing an issue of previous studies, we suggest an effective approach for future research. Approximately 90% of the information leakage incidents are recently being performed by internal workers. It is coming as a more serious problem than outsider attacks. The information leakage incident makes an organization or a company not only loses information but also gives a hard blow to the image. To prevent economic loss and damage to the image in advance, we need various research and development for effective solution.

Keywords: *insider threat, insider security, malicious intent*

1. Introduction

Until recently, the cyber security considers just external attacks for protecting inside resource. Firewall, IDS/IPS, VPN and antivirus are used as a protection device for the system and the network from Cracking, viruses or worm. However, such as the core technology leakage, customer information leakage or embezzlement is frequently performed by most of the insiders at companies and financial institutions. According to the Small Business Administration in Korea, 90% of the information leakage incidents are made by internal staff. Because the damage is getting serious with the information leakage incident, insider security study has become one of the big issues in the network security.

Internal workers have access rights to various inside resources for those own business. They have a lot of knowledge about system of an organization. Therefore, they know where resource or information they want is and how to access them. If they want, they can avoid security system to obtain the desired resource and information. It is possible to give serious damage to an organization, if these insiders have a malicious intent.

Although a research for the insider security is actively in progress by the academic world and a company's laboratory, it is difficult to solve every problem with one solution because of a feature of the insider security.

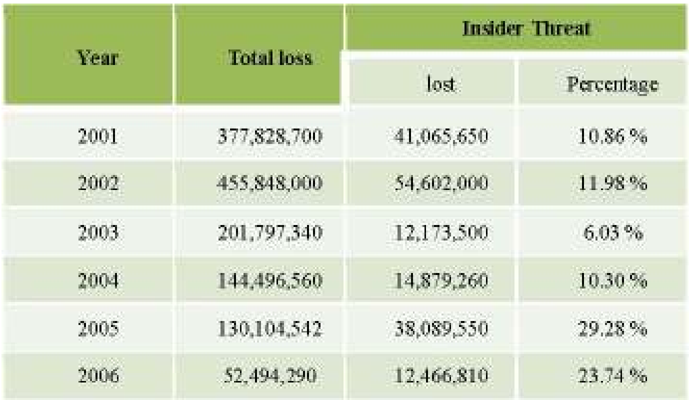
In this paper, by analyzing and surveying the results of recent research for the insider security in the academic, we identify the problems of existing research to present an effective approach for the future insider security research.

2. The insider security

In modern society, most of the employees essentially use a computer for their own business. They have access to use internal resources of an organization through computer networks, and any time they can access to necessary internal resources. Likewise, we call a direct or an indirect member of the organization the insider, who has access right to access to internal resources. There is a top secret data, like the organization's core technology or customer information among the organization's resources, which the insider access. If these resources are disclosed to outside, it can bring fatal results to the organization.

The insider accesses everyday internal resources for their work using a computer. Like this, information of organizations is stored and passed to a server through a computer network. An organization and a large corporation have invested a lot of money and effort to defend external attacks, which are for the purpose of seizing important information or destroying simply a system. They have used various solutions from a basic firewall to an intelligent defense system, such as IDS/IPS, for actively dealing with external attacks. Because defense technology becomes more improved by more intelligent outside attacks, today we have had a significant defense solution against outside attacks. According to Computer Crime and Security Survey[1,2,3,4] announced by CSI/FBI in the United States, the damage by outsider attacks has decreased continuously since 2001 years. However, the damage by an insider threat has increased relatively, although external attacks have decreased at total damage.

Table 1. Annual losses from CSI/FBI surveys



Year	Total loss	Insider Threat	
		lost	Percentage
2001	377,828,700	41,065,650	10.86 %
2002	455,848,000	54,602,000	11.98 %
2003	201,797,340	12,173,500	6.03 %
2004	144,496,560	14,879,260	10.30 %
2005	130,104,542	38,089,550	29.28 %
2006	52,494,290	12,466,810	23.74 %

The occurrence of external via a network attacks is higher than an insider threat. Therefore, until now the focus of network security is defense from external attacks. However, according to a survey of CSI/FBI [1], computer security incidents by the insider occupy 15.37% in Table 1. This percentage is a higher loss for occurrence rate. The security incidents by the insider are not high occurrence probability, but if a security incident occurs, it is fatal damage to the organization and difficult to analyze and cope to the cause. Recently, a company and an organization do many investments for preventing a secret outflow by the insider, but it has still many problems. The insiders have a lot of knowledge about the system structure of an organization and know well where resource they want is. If the insiders have a malicious purpose to obtain organization's resource, it is possible to gain the information using their knowledge for avoiding the security system. All of the employee's behavior could be controlled by a strong security policy for internal security, but it is able to significantly make loss of work efficiency.

When the insiders have a malicious purpose, they show some of the visible signs that they try to access the unauthorized resources or store necessary information to personal database. By removing the insider threat using analysis of these behavioral patterns, we prevent a security incident by the insider in advance. In this paper, we analyze various modeling techniques about the insider's behavioral patterns, and then we present how to prevent and detect the potential insider threat effectively.

3. The previous researches for the insider threat

Through the result of existing studies, we will discuss the significance issue of the insider security and some of the problems, which are showed during developing an insider security system.

3.1 Domain Oriented Approach

Qutailbah Althebyan and Brajendra Panda propose a domain oriented approach for predicting and mitigating an insider threat at [7]. The more internal resource an insider access s, the more information of an organization he//she take. This accumulated knowledge can be used to obtain confidential information of thee organization, if the insider has malicious intent. Therefore, if thee knowledge, which the insider is getting, is not controlled , it is not easy to keep the organization's confidential information safely.

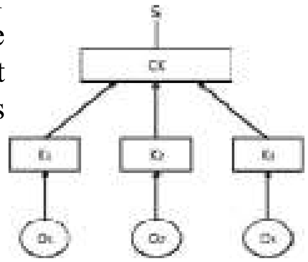


Figure 1.. A knowledge Graph(KG)

- SS*i* - the insider
- CCK – the Composed Knowledge is the total knowledge acquired by the insider
- KK*i* – a knowledge unit
- OO*i* – an object the insider has approached

In this paper, a system i s separated to necessary domains, and a set of objects which are resources such as a document are place on the related domain. We predefine an ontology using the knowledge units [5] which are created by analyzing the features and related terms. When the insider approaches an internal resource, a knowledge graph, denoted by KGG, are configured. Fig 1 represents a Knowledge Graph .

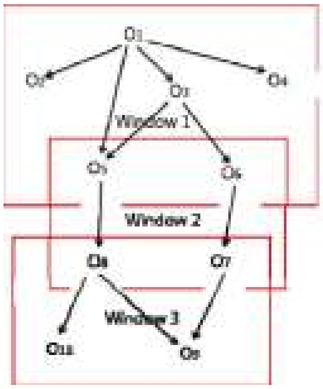


Figure 2. A Dependency GGraph of Objeect

A Ki is predefined about an Oi, and then when a Si accessed an Oi, it regards Si as acquiring knowledge of Ki and updates KG. Internal resources can have inter-dependence directly or indirectly. The insider can access unauthorized resources due to inter-dependence, and it is possible to make the insider threat. Therefore, for managing the inter-dependence, dependency Graph, denoted by DG, is represented such as figure 2

In order to mitigate the insider Threat, the author predefines priority values as follows.

- Very low importance : assigned a priority value : 1
- Low importance : assigned a priority value : 2
- Medium importance : assigned a priority value : 3
- High importance : assigned a priority value : 4
- Very high importance : assigned a priority value : 5

To calculate the risk between each resource, the following formula [5] is used with priority

$$\mathrm{Risk} = \left[\sum_{i=1}^{\mathrm{N}} (ni * di)/\mathrm{N}\right] \qquad (1)$$

ni represents the number of resources with importance value di, di is importance value of the resources, and N is total number of resources. In addition, the threshold is predefined to all of the knowledge units. When a clustering occurs due to access of resources by the insider, the possibility of the insider threats is determined by comparing the threshold with the calculated risk by corresponding knowledge units.

3.2 Prediction Model

For predicting the insider threat, Hui Wang, Shufen Liu and Xinjia Zhang proposed an approach using a tree structure at [9]. In this paper, the authors referred to the attack tree of Bruce Schneier [10] for their own approach. The Attack tree is able to be used for detecting various internal or external attacks. They introduced the System Attack Tree in a new way, which was more improved than the Attack tree. The System Attack Tree configures a tree after collecting all of the attack paths in a system, and detects the insider threat.

If we grasp all of the insider's intents when the insider access internal resources, we are able to intercept and detect the insider threat. The insider gives information to a system regarding a purpose of using before entering. By given, information the Signature Powered Revised Instruction Table, denoted by SPRINT, is configured, and the system makes Aos, which is a set of intended operations according to the insider's SPRINT plan. Finally, based on the Minimal Attack Tree generated by Aos, the security system observes an actual user action to detect a malicious intent. The overall configuration is shown below.

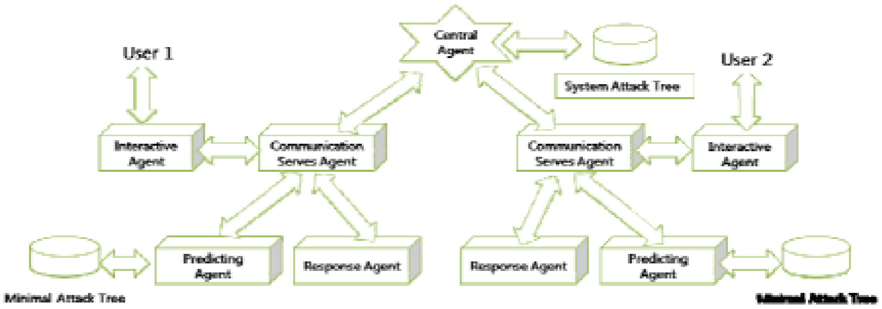


Figure 3. The framework of insider threat model

As shown in Figure 3, when the insider is connected to a system, the Interactive Agent requests some information regarding a purpose of using, and the n the user has to wait for a while. After configuring Aos with given information, thee Central Agent makes the Minimal Attack Tree by comparing Aos with the System Attack Tree. Inn this phase, the insider can work and the Predicting Agent observes a user's behavior bby the Minimal Attack Tree to detect an attack possibility. If detecting a malicious intention, the Predicting Agent halts the insider 's behavior.

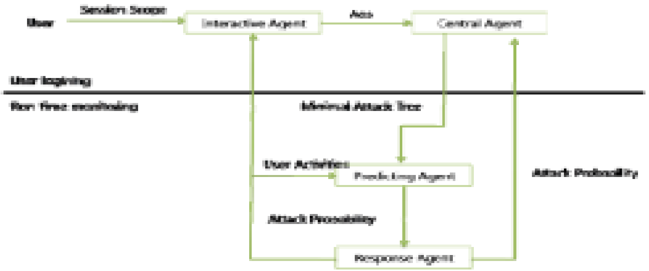


Figure 4. Flow diagram for insider threat model

3.3 Intent-driven Insider Threat Detection

Santos E., Hienn Nquyen andd Fei Yo propose an intent-driven framework, which consist s of a user model and insider detection metrics, to automatically detect the insider threats at [11]. Many traditional studies of the insider threat have focused an action-based, a social network, and a document-based, however the authors talked about grasping the intent of the user.

When users access the internal resources, they will have intentions, which are malicious or not. If some insiders have a malicious intent, it shows some of the features as the follow s [11]: they may use many non-supporting queries or put more constraints on non-supporting queries, when the insiders search for information; they may neglect noon-supporting documents, use old documents when supporting documents are not enough, or even fabricate pieces of information; when drawing reports, the insider may quote the same documents, and overstate record information. Through the experiments and the analysis, malicious intents can be classified by grasping the insider’s intents.

In this paper, the user models are based on the IPC mode l [12, 13] which includes an interest list, a preference network and a context network. Especially, a context network is important one. It is a document graph (DG), which is used to model a user’s knowledge context. A DG is generated for each document from the textual deliverables.

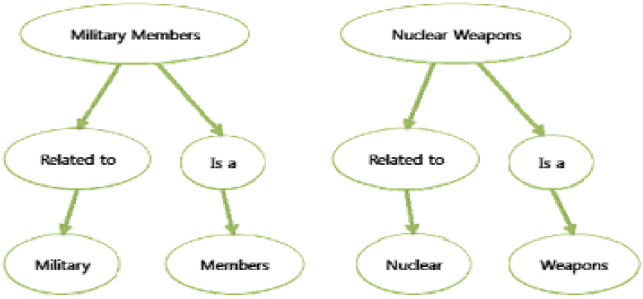


Figure 5. An example of a Document Grraph

A DG consists of concept nodes and relations between them. Two sort of relations are defined by the “Is a” relation and the “Related too” relation as shown in Figure 5. Users’ context networks are tracked and analyzed by detection metrics.. A similarity value between a document viewed by the analyst and their context network can b be computed by the following equation [14].

$$\mathrm{Similarity}(\mathrm{DG}_1, \mathrm{DG}_2) = \frac{n}{2N} + \frac{m}{2M} \qquad (2)$$

In the equation, n denotes the number of concept nodes shared by DDG1 and DGG2. N denotes the total number of concept nodes in DG1. Likewise, m and M are parallel to n and N except they count the relation nodes instead of the concept nodes.

3.4 Sensitive Information Dissemination Detection

The Sensitive Information Dissemination Detection was proposed by Yali Liu, Cherita Corrbet and Renie Archibald, Biswanath at [15]. This study uses network traffic to detect the insider threat. It is similar to a traditional method, which compares traffic c statistics at each hour. When someone accesses specific internal data,, its patterns are analyzed.

As the following figure 66, it can image one of the scenarios: A company X outsources its customer service to another company Y by establishing a shared (enterprise) network connecting their corporate LANs. In the service process, X needs to provide proprietary documents and manuals too Y, but it does not wish to share some sensitive/proprietary information. A malicious insider Z seeks to create backdoor networks to enable loss or damage of protected information and infiltrate sensitive/proprietary information using the enterprise’s network resources.

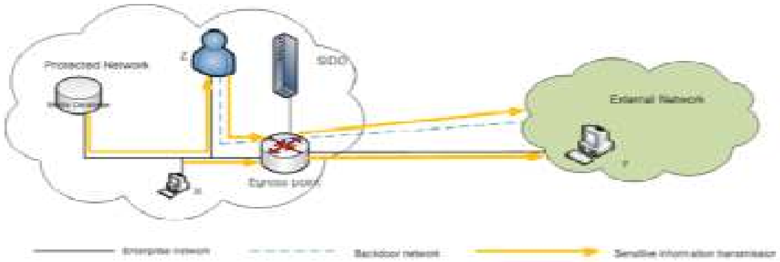


Figure 6.A motivating example for sensitive data exfiltration and detection

To detect and prevent the leakage of sensitive information, SIDD is placed at the network egress to monitor the traffic flow outbound from the protected network. First step, the captured network traffic is filtered into the application identification system to extract traffic features. And second step, after the traffic flow passes through the application identification checking process, it will pass into the Content Retrieval process and the content of application will be analyzed by the content detection stage.

In this final step, SIDD may only be able to detect the presence of hidden content and not fully recover the content for comparison.

When the internal network traffic passes through, SIDD parses the flow and waits for the server response. It may perform up to three-phase checks in a response time to determine how to filter outgoing traffic to prevent exfiltration of sensitive information.

3.5 Honeypot

The honeypot is able to not only detect a malicious external attack and lure an attacker for intercept but also to analyze attacker's patterns for corresponding new attack techniques. We lure an outside attacker to a vulnerable system to security, and collect their attack techniques, tools, and behavioral patterns so on. The hoenypot was originally developed for defending external attacks, but Lance Spitzner showed a detection technique with the hoenypot for the insider threat at [8].

Middle of 1990's, David Clock first proposed the honeypot. When an external attack occurs, by attracting this attack to the honeypot, we can intercept the attack and collect information, which is the attacker's behavioral patterns, techniques and tools. Especially, when IDS and IPS are powerless in the zone day, the honeypot collect attacker's information and new attack techniques, and protect an internal system. Lance Spitzner moved the honeypot, which was developed for protecting the system form external attacks, into the system for detecting the insider threat. The insider with malicious intent might be interested in ID, password, confidential information or so on. So, Honeytoken [8] is configured by documents or e-mail, which includes like confidential information, and placed into the system. All of the insiders have the access right to approach Honeytoken, however that is not true. If someone accesses Hoenytoken, we need to suspect that person's malicious intent. Also, Hoenytoken can be placed into a search engine for observing the insider threat. If the insider searches specific confidential information in the organization's intranet, the search engine shows Hoenytoken link to the insider. Because the insider has the access right for the intranet, a search does not cause the insider threat. However, clicking Hoenytoken link is that the insider is interested in the confidential information. It is possible to make the insider threat.

4. Problems of the current insider security system

Now a lot of research is still in progress, and many insider security solutions have been released based of the research. However, the result of the insider security solution is still not as satisfactory as external security solution. The biggest problem of the insider security solution for development is that the insider has a lot of the information about the organization, and understands the organization's structure. The insider not only knows where desired information is but also has sufficient knowledge about internal security system. If one of the insiders has a malicious intent to take confidential information, it is not difficult. It is very difficult to protect internal resource from the malicious insider using any excellent algorism and technique. Especially, it is actually impossible to prevent the insider security incidents by a system manager. Because the system managers manage all of the systems as well as the insider security system, if they have a malicious intent, it is the biggest insider threat.

5. Conclusions

To prevent the insider threat, we need a security system, which not only simply protects internal resources but also have to grasp the insider's behavioral patterns or intents in advance. Also, if the insider security incident happens, the security system has to grasp a cause and track the attacker deficiently. For preventing the insider threat by the system manager, management domains and permissions of the system manager have to be divided according to related work, and business has to have interdependence between each works to prevent that one person has a lot of the permission.

A malicious insider becomes more intelligent because of improving an insider security system. We have to think why the insider threat happens. If the malicious insider is just not a spy, he/she is a person, who is discontented with various reasons. Sometimes, the insiders have dissatisfaction because of employment, wages, and promotion and so on. The more these dissatisfaction grow bigger, the more the insider will have malicious intents by compensatory mentality. Establishing a powerful insider security system is important, however through appropriate evaluation and compensation system according to business ability, forming mutual trust relationship between the insider and the organization to lower the possibility of the insider threat is also important.

Acknowledgments

This research was supported by the MKE(The Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program supervised by the NIPA(National IT Industry Promotion Agency) (NIPA-2010-C1090-1031-0004)

References

[1] Robert Richardson.: 2003 CSI/FBI Computer Crime and Security Survey. Computer Security Institute, 2003

[2] Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn., Robert Richardson.: 2004 CSI/FBI Computer Crime and Security Survey. Computer Security Institute, 2004

[3] Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn., Robert Richardson.: 2005 CSI/FBI Computer Crime and Security Survey. Computer Security Institute, 2005

[4] Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn., Robert Richardson.: 2006 CSI/FBI Computer Crime and Security Survey. Computer Security Institute, 2006

[5] Q. Althebyan, B. Panda.: A Knowledge-Base Model for Insider Threat Prediction. In Proceedings of the 2007 IEEE Workshop on Information Assurance. United States Military Academy, West Point, New York, June 2007.

[6] Q. Althebyan, B. Panda.: A Knowledge-Based Bayesian Model for Analyzing a System after an Insider Attack. To Appear in the IFIP 23rd International Information Security Conference, Milan, Italy, Sept 2008.

[7] Qutaibah Althebyan, B. Panda.: Performance analysis of an insider threat mitigation model. ICDIM 2008: 703-709

[8] Lance Spitzner.: Honeypots: Catching the Insider Threat, 19th Annual Computer Security Applications Conference (ACSAC '03)

[9] Hui Wang, Shufen Liu, injia Zhang.: A Prediction Model of Insider Threat Based on Multi-agent. 2006 1 st

International Symposium on Pervasive Computing and Applications, 2006

[10] B. Schneier.: Attack trees: Modeling security threats. Dr. Dobb's Journal, December 1999. [11] Eugene Santos, Jr, Hien Nguyen, Fei Yu, Keumjoo Kim, Deqing Li, John T. Wilkinson, Adam Olson, Russell Jacob.: Intent-driven Insider Threat Detection in Intelligence Analyses. 2008 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology, 2008.

[12] Nguyen, H.; Santos, E Jr.; Zhao, Q.; and Wang, H. (2004b). Capturing User Intent for Information Retrieval. Proceedings of the 48th Annual Meeting for the Human Factors and Ergonomics Society (HFES-04), new Orleans, LA. Pages 371- 375.

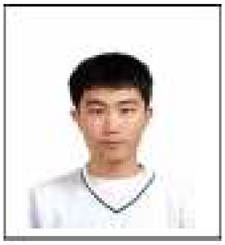
[13] Santos, E Jr.; Nguyen, H.; Zhao, Q. & Wang, H (2003a). User modelling for intent prediction in information analysis. Proceedings of the 47th Annual Meeting for the Human Factors and Ergonomincs Society. Pages 1034–1038.

[14] Montes-y-Gómez, M., Gelbukh, A., and Lópes-López, A. (2000). Comparison of Conceptual Graphs. In Proceeding of MICAI-2000, In 1st Mexican International Conference on Artificial Intelligence

[15] Yali Liu, Cherita Corbett, Rennie Archibald and Biswanath.: SIDD: A Framework for Detecting Sensitive Data Exfiltration by an Insider Attack. Proceedings of the 42nd Hawaii International Conference on System Sciences, 2009

Authors

Jaeseung Hog received the B.S degree in Computer engineering from Dongyang University, Yeongju, Republic of Korea, in 2008. He is currently a M.S degree student at Kyungpook National University. His research interests include embedded system and real-time OS.



Jongwung Kim received the B.S. degree in Electrical engineering and Computer science from Kyungpook National University, Daegu, Republic of Korea, in 2009. He is currently a M.S. degree student at Kyungpook National University. His research interests include embedded system and communication.

Jeounghun Cho received the B.S. and M.S. degree in Electrical Engineering from Korea Advanced Institute of Science and Technology, Daejeon, Republic of Korea, in 1996 and 1998, respectively, and the Ph.D. degree in Electrical Engineering from Korea Advanced Institute of Science and Technology, Daejeon, Korea, in 2003. He is currently an associate professor at Kyungpook National University, Daegu, Korea. His research interests include embedded system software optimization and Operating systems for embedded systems.