

A Framework of Defense System for prevention of Insider's Malicious Behaviors

Jung-Ho Eom, Min-Woo Park, Seon-Ho Park and Tai-Myoung Chung

Internet Management Technology Laboratory,
School of Information and Communication Engineering, Sungkyunkwan University,
Suwon, Kyunggi-do, Republic of Korea
{jheom, mwpark, shpark}@imtl.skku.ac.kr, tmchung@ece.skku.ac.kr

Abstract— In this paper, we proposed a framework of defense system by applying attack tree and misuse monitor for prevention of insider's malicious behaviors. Recently, a major interest of network security is the threat from insiders who execute their authorization legitimately to leak information on network system. If insider threats his/her system, he/she has caused a severe damage and loss to compromise information assets. Our proposed framework is consisted of 3 prevention modules. It prevents abnormal behaviors by monitoring all activities according to each prevention techniques. The main keys to prevention are attack tree and misuse monitor. An attack tree is conceptual diagrams of insider threats on systems and possible attacks to reach those goals. And a misuse monitor can prevent the misuse of resources by matching the actual running process pattern to the expected processing pattern in pre-defined current insider executed process profile.

Keywords— Insider threat, defense system, attack tree, misuse monitor

I. INTRODUCTION

According to 'The 2010 Cyber Security Watch Survey' [1], twenty-six percents of an electronic crime were committed by insiders. An insider is a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data. A malicious insider is intentionally exceeded or misused his/her authorized access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or systems. They have the greatest potential threat to information system(IS) security because they understand the information of their system, network structure, and security policies [2,3]. Insider threat has occurred across all computing environments, causing severe damage to their IS and organization. And it has a higher probability of success of penetrating into IS and extracting organization's sensitive information on IS [4,5].

We proposed a framework of defense system by applying attack tree and misuse monitor for preventing insider malicious activities. Our framework prevents insider abnormal activities on IS by matching her/his behaviors with attack tree. It is useful model to construct risks and security threats of systems against attack. Also, our framework prevents resources misuse from

insider by comparing insider actual behavior to the expected processing pattern in current insider process profile.

We describe related work in section 2, and propose our framework in section 3. Finally, we conclude in section 4.

II. RELATED WORKS

A. Insider threat

It is difficult to define 'insider threat' because of lack of a common understanding and definition of the term 'insider threat'. Insiders have a profitable advantage over outsiders who might want to cause damage to an organization. Insiders can bypass physical and logical security safeguards designed to prevent unauthorized access. Insiders are known the security policies and procedures, and technology used in their organizations as well as the vulnerabilities such as inappropriate enforced policies and procedures or technical flaws in IS [3,6,7]. A malicious insider is one who motivate to adversely impact on an IS through a range of actions that compromise information confidentiality, integrity, and/or availability.

Their goals are financial gain, revenge to their organization, transference to the better other organization, and so on. The leaked information from them or the impact of interruption and destruction may be used for commercial, military, political, or other purpose which could be collapsed their organization or nation [6,7,8]. An insider threats have occurred across all organizational divisions, such activities as the following [5].

- Low-slow threat, such as modifying or leaking confidential or sensitive data for monetary gain.
- Theft of business secrets or customer information to be used for business advantage or to give to a foreign government or organization.
- Technically sophisticated crimes that sabotage the organization's data, systems, or network.

B. The characteristics of insider threats

Insider threat is typically attributed to authorized users who maliciously use their privileges, and familiarity and proximity to IS environment to compromise sensitive information or impact damage. The recent study report [9] describes insider threats

becomes the most severe threats in the real IS environment. However, there is no solution which addresses this problem effectively. The following characteristics show why insider threat is more serious than outsider threat [10,11,12,13,17].

- No effective way to identify whether insider is hostile or not: Insiders mean employer and employee who work within a IS environment. They have the least privilege to access to IS with their role and privilege. It is a problem that nobody knows when they change their mind and use their privilege illegally against an organization, which behavior they do maliciously and how they use the leaked information. This is the most difficult part of human factor administration.
- The lack of insider threat recognition: Until a recent date, information security experts almost concentrate on defense attack from outside. So, most of security techniques focus on development of vulnerability /audit analysis tool, firewall and intrusion detection system for detecting outsider attack. On the other hand, insider threat is not perceived accurately because it is difficult to judge whether insider's anomalous behavior is intended or not.
- The difficulty of detection: The behavior is a noisy approximate of insider intent in the absence of sufficient contextual information about the insider and the overall environment. Consequently, such systems are often tuned to minimize false alerts by being less stringent about malicious behaviour. Although it reduces administrators' workload and users' irritation, such tuning can let some malicious behavior undetected.
- Insider's the abundant knowledge about their IS environment: Insiders know IS and network structure, information resources, security policy and safeguard etc. They can easily get other ID&P/W by shoulder smurfing, and know sensitive information location by eavesdropping. Once they decide their target, they can access stealthily to their target system.
- The severe damage: Although insider threats may not occur as frequently as outsider threats, they have a higher rate of success because insiders almost know about their IS environment and security safeguards in place. Insiders don't consider access authorization as outsiders try to gain authorization to access network system. Whenever insiders want to access their target system and information resource, they can access on system and a plenty of sensitive information timeless. So, insider threats impact on IS seriously.

C. The current research for detecting insider threats

The related researches for detecting insider threats have developed rapidly in recent years.

Ray [15] proposed a framework that uses an attack tree to detect malicious behaviors of authorized insiders. He developed algorithms to generate minimal forms of attack tree customized for each user. It can be used efficiently to monitor insider's activities. If the insider's activities progress sufficiently up along

the branches of the attack tree towards the goal of system compromise, it generates an alarm.

Zhang [18] presented an active defense model and framework of insider threat detection and sense. He firstly describes the hierarchical framework which deal with insider penetration from some aspects, and subsequently show a hierarchy-mapping based insider penetrations model, the kernel of the threats detection, and sense and prediction.

Doss [19]'s study was conducted within an enterprise where analysts were observed performing analytical operations to analyze and detect insider threats. Using Grounded Theory(GT) as a research method, data was collected which evolved into a model. This model shows how alerts and events created through some methods can be analyzed to determine if malicious insider behavior is present. This model may allow other analysts to can better identify insider threats to IS in less time than before, and allow identification of insider threats and attacks that had not been identified prior.

III. PROPOSED FRAMEWORK

A. The concept of our proposed framework

We proposed our framework to in depth defense insider threat at each layered prevention step. It performs online monitor to prevent insider malicious activities that have enough potential threat on information system.

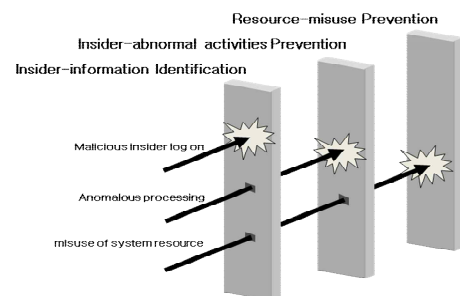


Figure 1. The concept of the layered defense

We approach a framework that defends insider threat at each prevention functions. As executing his process, it defends user-oriented malicious activities by each prevention functions. We can defense high impact on IS from insider malicious activities and mistake to be threat to critical system and sensitive data. The concept of the proposed framework and functions are as following.

- Insider information identification
It is to identify whether insider is authorized or not. Firstly, when insider accesses system, it checks insider information by user profile, and identifies whether he/she has security violation or not.
- Insider-abnormal activities prevention
It focuses on prevention from insider's abnormal behavior using attack tree. Attack trees provide a formal

method of describing the security measures of systems, based on varying attacks. A tree structure is used represent attacks on a system, with the goal as the root node and different ways of achieving that goal as leaf nodes.

- **Resource-misuse prevention**
It prevents to misuse system resources from insider with authorized rights as comparing insider actual process to the expected processing pattern [14]. The insider has specific patterns to execute process and resource usage related to current his task/role.
- **Defense manager**
It manages all modules in defense system. It manages security policy and updates database related to attack tree and misuse monitor.

B. A framework of defense system for preventing from insider's malicious behavior

We considered such a complicated operation factors such as insider behavior, systems, process, roles and file, etc to monitor malicious insider behavior. We concentrated our framework on insider abnormal behavior and resource misuse.

For example, programmer is normally expected to access certain project applications for working hours. If he attempts to access on audit trail analysis program, it is inferred a deviation from normal behavior pattern. Programmer also executes program related to his project in the directory. If he executes program in the plan directory, we can presume that he does unauthorized access any sensitive data. The reason to occur it, an insider may use the privileges of a program to execute in which he is interested. Namely, an insider can execute program in abnormal ways for achieving his attack goal.

We explain the function of each prevention module. Our framework consists of 3 modules and a manager such as insider information checker, insider behavior monitor, resource misuse monitor, and defense manager. Our framework prevents user's abnormal activities, resources misuse and mistake by each prevention modules.

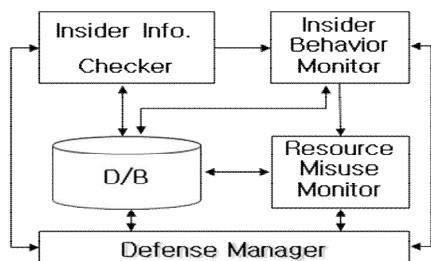


Figure 2. The proposed framework of defense system

1) Insider Information Checker

Insider information checker decides to permit connection to system when an insider logs on, as comparing insider information such as his/her ID&P/W and security violation, his/her current process and the log of system usage, etc. Once

insider's ID&P/W is matched to user profile, it checks the record of his malicious activities on system. If he has the record of malicious activities, it informs to a defense manager for monitor thoroughly. This module marks 3 types of security label to insider according to the experience of security violation. The security label is as following table.

TABLE I. THE SECURITY LABEL OF INSIDER

Security Label	Description
Red	Sometimes abnormal activities and security violation
Yellow	No malicious activities, Sometimes the violation of security rule
Blue	No malicious activities, The compliance of security rule

It can reduce the load of monitor related to all insider activities on system by security label. It also minimizes the usage of resource and runtime for preventing insider threat. Lastly, this module sends the log of check results to defense manager.

TABLE II. THE EXAMPLE OF INSIDER PROFILE

NAME: Tom Washington	Duty Directory: /user, /user/affair, /etc
DEP.: General Affairs	DutyFile: /user/affair/manager/schedule/*.c
Position: manager	Favorite Command: vi, ls, grep. Etc
Duty: Scheduling	Favorite Website: www.eventact.com
Office hours: AM 0900 – PM 0500	www.racquetball.com
Sys. Info.: Intel Pent4 CPU 2.4GHz	Exchange email: info@eventact.com
2.39GHz 256MB RAM	sandblack@sarion.net
IP Address: 10.1.1.65	Chief-kim@affairs.
Gateway: 10.1.1.1	Concerns;
ID&P/W: tomwash&not34qaz	Security violation: 1 times
Rights in the DCD: r, w, e	Promotion Fall-off: 2 times
Favorite Software: Unix,	High social activity
Microsoft office	

For example, once Tom does log on system, insider information checker grants 'Yellow' because he has a record of security violation. And if Tom tries to log on other system which has IP address 10.1.1.62 with his ID&P/W during office hours, this module issues warning message to him. If he continues to enforce his task on other system, this module rejects his query and disconnects, and reports to defense manager. Defense manager updates and modifies insider profile, and sends new data to insider profile D/B. Though Tom normally logs on his system, he is continuously monitored by each module because he has security violation history.

2) Insider-Behavior Monitor

This module prevents insider's abnormal activities using attack tree. An attack tree helps organize threats and/or abnormal activities by identifying vulnerabilities and/or weak points in a system and analyzing the weak points and dependencies among the vulnerabilities and representing these dependencies in the form of an AND, OR decomposition. AND-node is a sequence of events all of which must be achieved for a this subgoal to succeed; this is represented by the events being combined by AND decomposition at node. OR-node is a set of

events, any one of which occurring will result in the sub-goal succeeding; this is represented by the events being combined by OR decomposition at the node [15,16].

The basic attack tree is consisted of 3 attributes; Vertex(v), Edge(e), Deomposition(θ).

$Attack\ Tree = \langle v, e, \theta \rangle$

① v is the set of nodes in the tree representing different states of partial compromise or subgoals that an attacker needs to move through in order to fully compromise a system.

② $E \subseteq V \times V$ constitutes the set of edges in the attack tree.

③ θ is a set of tuples of the form (v , AND or OR Decomposition)

We added the minimum attack execution probability (MAEP) to the attributes of attack tree for identifying a new and attack route which has a high rate of attack success. MAEP is defined as a chance of completing the attack when a sub-node goal is achieved. MAEP is calculated with the ratio of all achieved events until the sub-nodes are achieved over all nodes of attack tree. MAEP is the minimum value that the insider needs to compromise the given sub-goal. If the goal G has an AND-decomposition, the least value is the sum of the least value of the child nodes plus all additional unit value, one for each child node to achieve to G . If a goal G has an OR-decomposition, the least value is computed as the minimum least value of its child nodes plus one unit value needed to achieve to G from the child node. The following definition is the steps to compute MAEP for a sub-goal G . A sub-goal G 's child node N_i , MAEP to compromise G is defined as follows.

① If G is a leaf node of the attack tree the MAEP is 0.

② If G is some interior node and is an AND-decomposition, then $MAEP = \text{Sum}(N_i) / \text{Total}(N)$

③ If S is some interior node and is an OR-decomposition, then $MAEP = \text{Min}(N_i) / \text{Total}(N)$

Our extended attack tree is $EAT = \langle v, e, \theta, MAEP \rangle$

For example, let see as following fig 3. If the activities of insider are matched to attack tree, insider-behavior monitor prevents process by the threshold of threat from attack tree. The threshold of threat means a limitation which the system can defense an insider's abnormal behavior.

And if a sub-goal B is to achieve, child node F is executed or both child node G and H is executed together. The MAEP of Sub-goal B are, in case of choice F , 33.3%(2/6), in case of choice G, H , 50%(3/6) by above equations. To achieve sub-goal B , attack path is selected as F node. Insider-behavior monitor can prevent attack path (including F node) in former times as following figure 3.

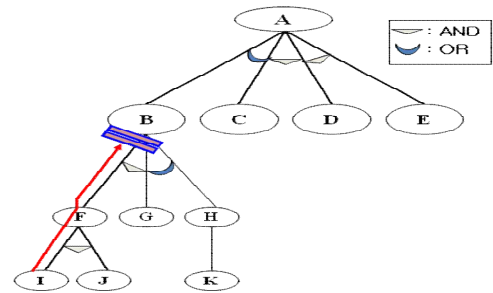


Figure 3. The expression of attack tree

For example, we are supposing that insider compromises system for leaking proprietary secrets. Attack scenario is described as following table 3.

TABLE III. THE EXAMPLE OF ATTACK SCENARIO

Goal: Leakage of system proprietary secrets
OR 1. Monitor emanations from system
AND 1.1 Survey physical perimeter to determine optimal monitoring position
1.2 Acquire necessary monitoring equipment
1.3 Setup monitoring site
1.4 Monitoring emanations from site
2. Attack system intranet using its connections with Internet
OR 2.1 Monitor comm over Internet for leakage
2.2 Get trusted process to send sensitive information to attacker over Internet
2.3 Gain privileged access to Web server

If an insider executes process such {1.1, 1.2, 1.3, 1.4}, we prospect that he/she tries to monitor emanation from system. This module prevents process before attack achieves the last goals of parent node. In case of attack 2, their sub-nodes are connected by OR decomposition. So, if only one of 3 child nodes achieves, it is easy to achieve node 2. This module monitors positively node 2 process because MAEP is lower. The attack tree of scenario is as following figure 4.

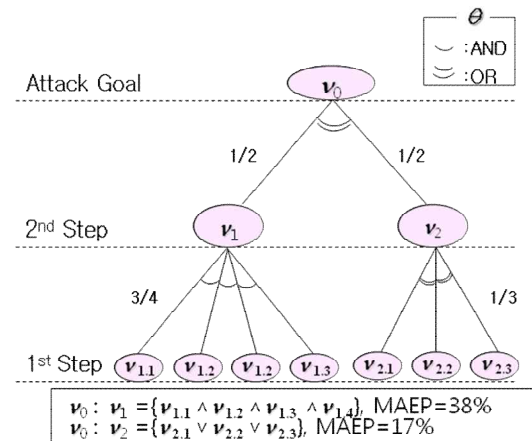


Figure 4. The attack tree of table III

3) Resource-Misuse Monitor

This module prevents insider activities to misuse system resource as comparing the insider's actual behavior to the set of expected processing pattern based on the insider's current process profile. This module operates as following figure 4.

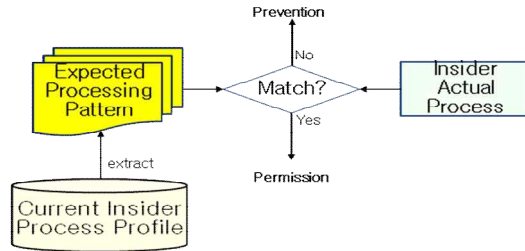


Figure 5. Misuse Monitor

The insider's current executed process profile saves on profile D/B as following table IV.

TABLE IV. THE STRUCTURE OF CURRENT PROCESS PROFILE

Users	Roles	Tasks	Objects	Work Time(H)	Perm
U ₁	R ₁ (S)	T ₁	O ₂	6	W
			O ₂	2	R
			O ₄	3	R
		T ₂	O ₂	2	R
			O ₃	5	R
			O ₃	2	W

For example, this module prevents misuse process like figure 6. If the expected processing pattern extracted from the insider's current process profile is to execute "read mode" in "user-role-task2-object3", this module prevents execution of "write mode" in insider actual process.

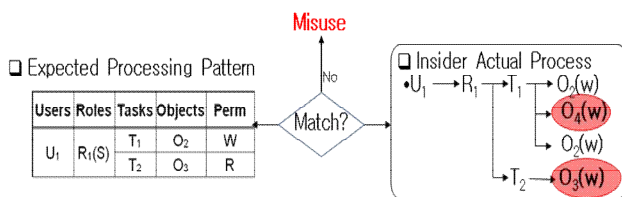


Figure 6. The prevention of insider misuse

4) Defense Manager

This module controls 3 modules; Insider Information Checker, Insider behavior Monitor and Resource Misuse Monitor. It thoroughly examines the process pattern of insider with process log in the past and updates database. If an insider finishes his project and then is assigned new project, defense manager modifies the current executed process pattern profile.

And it solves problem related to prevention mechanism from each module.

IV. CONCLUSIONS

We described a framework of defense system for preventing from insider malicious activities and sophisticated threat. We applied attack tree and misuse monitor mechanism to our proposed framework. The pattern of program and process execution from insider is almost steady when he/she performs his/her task by same pattern daily. So, our framework easily built insider profile, and can identifies insider threat which maliciously does use privilege to execute program and process, matching up attack tree and the expected process pattern in the current executed process profile.

Our framework has benefit to prevent in-depth threat to critical system and sensitive data from insider according to each prevention mechanism.

In Future, we will research to reduce false-negative problem with advanced distinction basis of normal, abnormal and suspicious behavior.

REFERENCES

- [1] "2010 CyberSecurity Watch Survey", CSO magazine, The U.S Secret Service and CERT, Jan, 2010. <http://www.csoonline.com/documents/pdfs/2010CyberSecurityResults.pdf>.
- [2] Richard C. Brackney, Pobert H. Anderson, "Understanding the Insider Threat" Proceeding of a March 2004 Workshop, RAND, Mar, 2004. <http://www.rand.org>.
- [3] Dorothy E. Denning, "Information warfare and Security" Addison-Wesley, pp.131-161, 1999.
- [4] Nguyen N., Reiher P., Kuenning G.H., "Detecting insider threats by monitoring system call activity" Information Assurance Workshop, IEEE Systems, Man and Cybernetics Society, pp. 45-52, Jun 2003.
- [5] Dawn Cappelli, Andrew Moore, Timothy Shimeall, "Common Sense Guide to Prevention and detection of Insider Threats" US-CERT, Jan, 2009.
- [6] Mark Maybury, Penny Chase, Brant Cheikes, et al, "Analysis and Detection of Malicious Insiders" International Conference on Intelligence Analysis, Mar. 2005.
- [7] Robert H. Anderson, "Research and Development Initiatives Focused on Preventing, Detecting, and Responding to Insider Misuse of Critical Defense Information Systems", RAND, Aug. 1999.
- [8] Bradley J. Wood "An insider threat model for adversary simulation" Research on Mitigating the Insider Threat to Information Systems Workshop, RAND, pp.41-48, Sep. 2000.
- [9] Marisan Reddy Randazzo et. al "Insider threat study : Illicit cyber activity in the banking and finance sector", Cert/United States Secret Service, Aug. 2004.
- [10] Chinchani, R.; Iyer, A.; Ngo, H.Q.; Upadhyaya, S., "Towards a theory of insider threat assessment" Dependable Systems and Networks(DSN 2005) Proceedings, pp.108-117, Jun. 2005.
- [11] Michael Caloyannides, Carl Landwehr, "Can technology reduce the insider threat?", Research on Mitigating the Insider Threat to Information Systems Workshop, RAND, pp.61-66, Sep. 2000.
- [12] M. Keeney, et. al "Insider threat study : computer system sabotage in critical infrastructure sectors" US-CERT/SEL, May, 2005.

- [13] Phillip G. Bradford, Ning Hu, "A layered Approach to Insider threat Detection and Proactive Forensics" proceeding of ACSAC, Dec, 2005.
- [14] Joon S. Park and Shuyuan Mary Ho, "Composite Role-Based Monitoring(CRBM) for Countering Insider Threats" ISI 2004, LNCS 3073, pp.201-213, 2004.
- [15] Indrajit Ray and Nayot Poolsapassit, "Using Attack Trees to Identify Malicious Attacks from Authorized Insiders" ESORICS2005, LNCS3679, pp.231-246, 2005.
- [16] Nayot Poolsapassit and Indrajit Ray, "Investigating computer attacks using attack trees", IFIP 2007, Vol.242, pp.331-343, 2007.
- [17] Brian M et al, "Designing Host and Network Sensors to Mitigate the Insider Threat" Journal of Security&Privacy IEEE, Vol.7 Issue6, pp.22-29, November, 2009.
- [18] Hongbin Zhang et al, "An Active Defense Model and Framework of Insider Threats Detection and Sense", IAS'09, IEEE, pp.258-261, 2009.
- [19] Gary doss and Guvirender Tejay, "Developing Insider Attack Detection Model: A Grounded Approach", ISI'09, IEEE, pp.107-112, 2009.