SCIS 2008 The 2008 Symposium on
Cryptography and Information Security
Miyazaki, Japan, Jan. 22-25, 2008
The Institute of Electronics,
Information and Communication Engineers

Yet Another Intrusion Detection System against Insider Attacks

Hyeran Mun[*] Kyusuk Han [*] Chan Yeob Yeun [*] Kwangjo Kim [*]

Abstract— Intrusion Detection System (IDS) originated as a mechanism for managing the detection of system misuse through the analysis of activity [5]. Despite that the various attacks are occurred by insiders and outsiders, most studied focused on IDS against outsider attacks. However, the loss from insider attacks is more severe than outsider attacks as shown in [10]. In this paper, we improve the Wang *et al.*'s insider predection model [17] and propose the combined model with access control for the efficient insider intrusion detection. We delegate the role of intrusion detection to users, in order to detect the malicious insiders more efficiently. If the insiders want to access to the information, they should have the permission from several users in organization. By combining the concept of access control in Wang *et al.*'s model, our scheme is believed to be more secure.

Keywords: Intrusion Detection, Insider Attack, Access Control

1 Introduction

Intrusion Detection System(IDS) is used to detect malicious behaviors that can compromise the security and trust of a computer system, such as network attacks against vulnerable services, data driven attacks on applications, host-based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and malware like viruses, trojan horses, and worms.

In CSI/FBI report [10], incidents from outsider attack occur more than insider attack, as shown Table 1. So, most studies on IDS focused themselves on the intrusion detection against outsider attacks. As a result, many outside attacks are successfully detected and prevented.

However, Fig.1 shows the attacks by malicious insiders are more severe than the attacks from outsiders, while the number of insider attacks are quite small. Thus, the necessity of the intrusion detection against insider attacks is obvious to reduce the loss from attacks.

Wang *et al.*[17] proposed the prediction model of Insider Threat Based on Multi-agent, which consists of central agents, interactive agents, predicting agents, response agents and communication services agents. The notion of agents is defined to be software systems that function autonomously to achieve desired objectives in their environment. The central agents generate the customized minimal attack tree, and the predicting agents monitor the users operations. However, Wang *et al.*'s model did not consider the concept of access control. If user who has a high authority and malicious propose kills the predicting agent using his/her authority, the intrusion detection will be failed. For example, user

Table 1: How many incidents from outsider and insider in [10]

Outsider	1 to 5	6 to 10	Over 10	Don't know
2001	41	14	7	39
2002	49	14	9	27
2003	46	10	13	31
2004	52	9	9	30
2005	47	10	8	35

Insider	1 to 5	6 to 10	Over 10	Don't know
2001	40	12	3	44
2002	42	13	9	35
2003	45	11	12	33
2004	52	6	8	34
2005	46	7	3	44

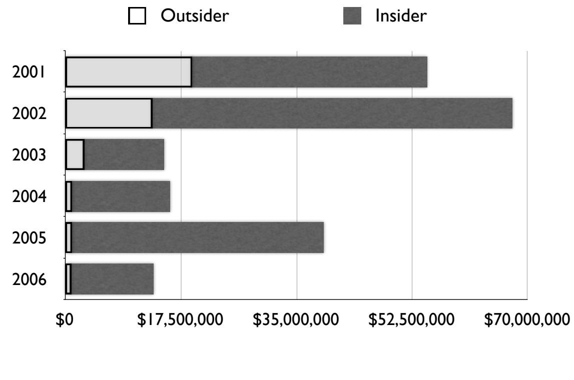

Figure 1: Annual Losses from attacks in [10]

[*] Information and Communications University, 119, Munjiro, Yuseong-gu, Daejeon, 305-732, Korea {smartran, hankyusuk, cyeun, kkj}@icu.ac.kr

executes buffer overflow or race condition attack to kill the prediction agent. If it combines the concept of access control in Wang *et al.*'s model, it will be more secure.

In this paper, we combine the access control with the intrusion detection to improve Wang *et al.*'s model and propose an efficient model to detect insider attacks. We focus ourselves on protecting documents which exist in organization. We delegate the role of intrusion detection to users, when insider try to access to the documents which exist in organization, in order to improve previous model and detect the malicious insiders more efficiently. Using limitation time for accessing documents, our model decreases system overhead and increases efficiency for intrusion detection.

The rest of the paper is organized as follows. Section 2 presents related work in this area. In Section 3, we present the our model. In Section 4, we analyze our model. Finally, Section 5 gives the conclusion and future work.

2 Related Works

In this section, we describe the concept of intrusion detection system firstly. After that, we also describe the insider attacks and several previous works for the insider intrusion detection.

2.1 Intrusion Detection System

Intrusion Detection System (IDS) is used to detect malicious behaviors that can compromise the security and trust of a computer system, such as network attacks against vulnerable services, data driven attacks on applications, host-based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and malware like viruses, trojan horses, and worms.

IDS is categorized by 'Data source' or 'Intrusion detecting method'[1] as shown in Fig. 2.

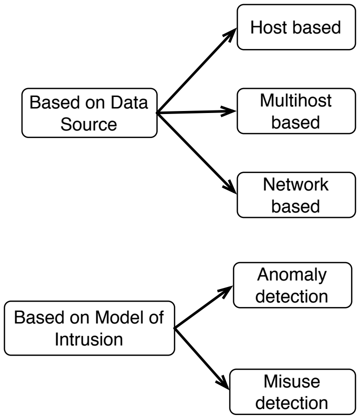

Figure 2: Categorize of IDS by COAST(Computer Operations, Audit and Security Technology)

- **Host based** audit data from a single host is used to detect intrusions
- **Multihost based** audit data from multiple host is used to detect intrusions
- **Netwrok based network** traffic data, along with audit data from one or more hosts, is used to detect intrusion
- **Anomaly detection** the intrusion detection system detects intrusions by looking for activity that is different from a users or systems normal behavior
- **Misuse detection** the intrusion detection system detects intrusion by looking for activity that corresponds to known intrusion techniques (signatures) or system vulnerabilities

2.2 Insider Attacks

Numerous definitions for the term insider attack have been proposed. We present three of the definitions for insider threat presented by other researchers.

According to Maybury *et al.* [8], malicious insider is one motivated to adversely impact an organization's confidentiality, integrity, and/or availability. According to Tugular and Spafford [13], insider attackers are those who are able to use a given computer system with a level of authority granted to them and who in so doing violate their organization's security policy. According to Aleman-Mezal, *et al.*[3], insider threat refers to the potential malevolent actions by employees within an organization, a specific type of which relates to legitimate access of document.

The above definition involves the notion of assigned privileges to an insider. So general definition of insider has privileges through which he/she can access different information in his/her organization.

2.2.1 Analyzing method

Several techniques have been proposed for insider intrusion detection. In order to detect insider attacks, many authors use the attack tree or attack graph. The previous work [4, 6] was suggested to use.

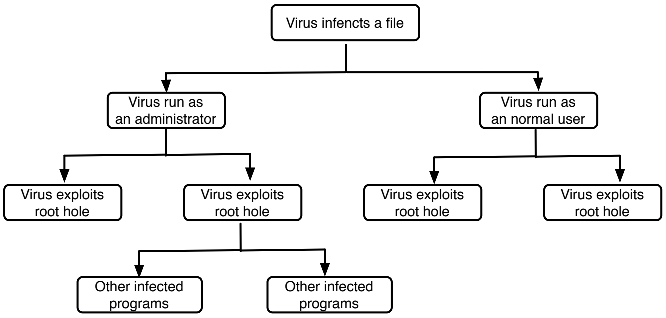

Figure 3: Example attack tree for computer viruses [2]

In Fig. 3, we generate a typical example for computer virus. It is represented tree structure, root node indicates attacker goal, leaf node indicates different ways of achieving goal. In Fig. 3, the goal of attacker is to infect a file with virus, in order to achieve goal exist many different ways.

In [7, 12, 16], attack trees provide a formal, methodical way of describing the security of systems, based on various attacks. Attack tree can help organizations establish attack scenarios by analyzing system vulnerabilities and dependencies among these vulnerabilities.

Attack graph [9, 14, 15] allows representation of a computational environment and subsequent analysis for security vulnerabilities. Also, attack graph offers an elegant alternative in terms of symbolic machinery to appropriately represent a computational environment and analyze it for security weaknesses.

Comparing between attack tree and attack graph, the representation of states and actions is different. Approach of attack graph seems to be too complex. According to Ritchey and Ammann [11], a major drawback of attack graph is its scalability. So it is exactly the advantage of attack tree.

2.2.2 Wang *et al.*'s Model

Wang *et al.*[17] proposed the prediction model of Insider Threat Based on Multi-agent, which consists of central agents, interactive agents, predicting agents, response agents and communication services agents. The notion of agents is defined to be software systems that function autonomously to achieve desired objectives in their environment.

The model is based on the agent and the distribute intrusion detection system (DIDS). Therefore, the model is of many advantages, such as flexibility, autonomy, scalability, and so on. User must have a session with interactive agent before user can login into system successfully. Interactive agents generate intended operations and submits it to central agents. Central agents will generate the customized minimal attack tree. The information of tree structure will be stored in local rule database.

With users changing, the corresponding minimal attack tree will be different, too. The rule database can be created in run time, and it is obviously different from traditional static rule database. Predicting agents are monitoring users operations on-line and compute the probability of attack in terms of the minimal attack tree. If attack generates, response agents will report the information to central agents. The framework of this model is shown in Fig. 4.

However, Wang *et al.*'s model did not consider access control. If user who has a high authority and malicious propose kills the predicting agent using his/her authority, the intrusion detection will be failed. For example, user executes buffer overflow or race condition attack to kill the prediction agent. If it combines the concept of access control in Wang *et al.*'s model, it will be more secure.

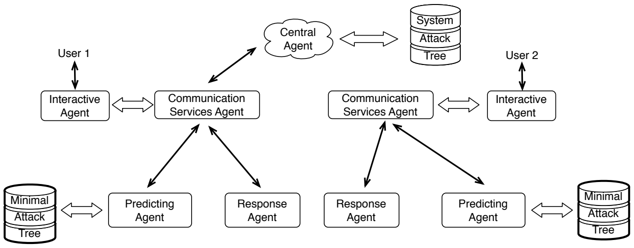

Figure 4: The framework of insider threat model

3 The model of Insider Intrusion Detection System

With rapid advances in computer technologies, organization's documents are changed into digital documents to achieve high responsiveness and ease of management. Therefore, these digital documents are the most important asset of an organization. Insiders has the knowledge of the organization's system and privilege for access to the documents which exist organization.

In this paper, we propose efficient model for insider intrusion detection system (IIDS). We delegate the role of intrusion detection to several users, when insider try to access to the documents which exist in organization, in order to improve previous model and detect the malicious insiders more efficiently. Administrator manages database which stores all possible system vulnerability and administrator is unnecessary to monitor users actions. So, if the insiders want to access to the information, they should have the permission from the several user in orgnization.

3.1 Our Framework of IIDS

Intrusion Detection Model is composed of user group, documents, whole of vulnerability scan(WVS), subset of vulnerability scan(SVS) and subset of pattern(SP). The framework of insider intrusion detection model is shown in Fig. 5.

- P_1. **User Group** Users in organization are divided into user grade and assign privilege by user grade. We strongly believe that as the grade of a user increases, the privilage of the user also have to do. The user grade by privilege is shown in Table 2.

Table 2: User grade and privilege

User grade	Symbol of grade	Privilege
Lowest user	U_1	U_1
Low user	U_2	$2U_1$
Medium user	U_3	$4U_1$
High user	U_4	$6U_1$
Supreme user	U_5	$8U_1$

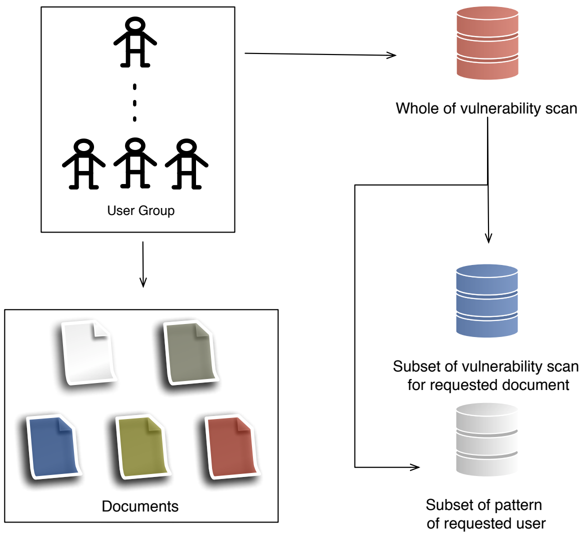

Figure 5: The framework of insider intrusion detection model

- P_2. **Documents** Each document is assigned important value (Security grade). The user should require minimum privilege in order to access to the documents. We strongly believe that as the grade of a security increases, the minimum privilege of the user also have to do. The important value of document(Security grade)and minimum privilege is shown in Table 3.

Table 3: Security grade of document and minimum privilege

Document grade	Security grade	Minimum privilege
5-grade secrecy	D_5	U_1
4-grade secrecy	D_4	$3U_1$
3-grade secrecy	D_3	$9U_1$
2-grade secrecy	D_2	$15U_1$
1-grade secrecy	D_1	$21U_1$

P_1 and P_2 assign privilege by user grade and minimum privilege by document. Therefore, when low-grade user accesses to high-grade document, user requests for many users. The supreme user can't access with an independence in 1-grade secrecy document. Because U_5 has privilege $8U_1$, in order to access to the D_1, U_5 needs more $13U_1$. Also, if user requests a permission to several users for using the public documents(=5- grade secrecy), it is inefficient. Therefore, when accessing 5-grade secrecy(=public documents), user should not require different user accept.

- P_3. **Whole of vulnerability scan** Utilizing vulnerability scanner can scan all possible system vulnerabilities. After dependencies are analyzed, all attack scenarios can be represented in form of attack tree. Whole of vulnerability scan(WVS) is able to represent several subsets of tree by tree theory. Administrator only manages WVS and need not monitoring users actions.

- P_4. **Subset of vulnerability scan** When one user requested documents, WVS customizes to generate the subset of vulnerability scan for requested document. SVS are represented in form of attack tree. If attacks are generated, search the point about attack occurred and update the information to WVS using the attack tree.

- P_5. **Subset of pattern** When one user requested documents, WVS customizes to generate the subset of pattern for requested user. This pattern includes limitation time for accessing document, decreases system overhead and increases efficiency for intrusion detection.

3.2 The Workflow of IIDS

The manager suspends the access of the user This part focus on the following steps. 1) Administrator manages WVS and get all possible system vulnerability from WVS. 2) When user requests document, user should receive access permission to several users for accessing document. Using P_1 and P_2, user selects random users which have suitable privilege 3) Administrator generates SVS and SP from WVS. 4) Selected users are monitoring requested user's actions examining SP and SVS while requested user accesses to the document. 5) If attacks are generated, selected users wil report the information to administrator, then administrator suspends the access of the user. Selected user will update to SP and SVS. 6)Finally, reported information is used to update to the WVS. The workflow diagram is shown in Fig. 6

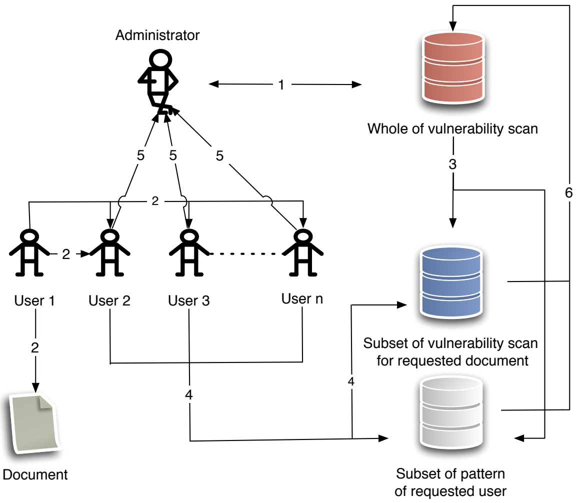

Figure 6: The workflow of insider intrusion detection model

3.3 Example: Attack Scenario

In this section, we present an example scenario of our model for insider attack detection. Medium user(=U_3) accesses to document assigned important values D_2. Refer to P_1 and P_2, U_3 has privilege $4U_1$ and D_2 assigns $15U_1$ minimum privilege. In order to access to the D_2, U_3 needs more $11U_1$ privilege. Therefore, U_3 selects random users, $1 \cdot U_4$, $2 \cdot U_2$, $1 \cdot U_1$. So U_3 has $15U_1$ privilege($4U_1$ + $6U_1$ + $(2 \cdot 2U_1)$ + U_1), U_3 can access the D_2. Fig. 7 is shown after U_3 accessed to the D_2.

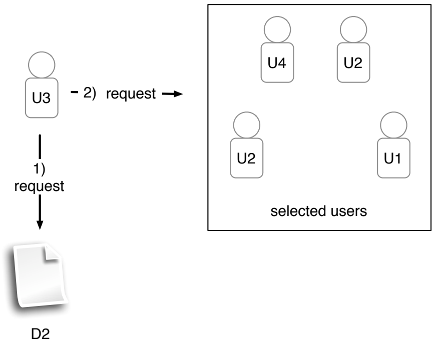

Figure 7: After U_3 accessed to the D_2

Administrator who managed WVS generates SVS for D_2 and SP of U_3 based on attack tree. It referred to P_5, SP of U_3 includes limitation time for accessing document. It limits a detection time at information use permission duration.

Selected users are monitoring U_3's action examining SP of U_3 and SVS for D_2, while U_3 accesses to the D_2. SVS for D_2 and SP of U_3 which are configured of an attack tree have a same structure as Fig.7.

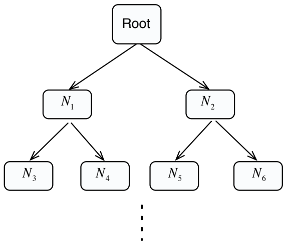

Figure 8: Structure of attack tree

Attack tree contains all possible attack scenarios. So, SVS for D_2 and SP of U_3 which are configured of attack tree to detect the malicious actions of U_3. If selected users detect the malicious actions, they will report the information to administrator, then administrator suspends the access of the user. Selected user will update to the SP of U_3 and SVS for D_2. Finally, reported information is used to the WVS.

4 Analysis of our model

In this section, we compare our model with Wang *et al.*'s model [17] as in Tables 4 and 5.

Wang *et al.*'s model does not considered access control. If user who has a high authority and malicious propose kills the predicting agent using his/her authority, the intrusion detection will be failed. For example, user executes buffer overflow or race condition attack to kill the prediction agent.

Our model combines concept of access control in Wang *et al.*'s model. Therefore, our model is more secure than Wang *et al.*'s model. We assign privilege by user grade and minimum privilege by document. Therefore, when low-grade user accesses to high-grade document, user requests for many user. The supreme user(U_5) will not able to access with an independence in 1-grade secrecy document(D_1). Also, SP includes limitation time for accessing document. It limits a detection time at information use permission duration. System overhead decreases and efficiency increases for intrusion detection.

Table 4: Compared Wang *et al.*'s model with our model

	Wang's model	Our model
Who detects attacks?	Predicting Agent	Selected users

Table 5: Advantage of Our model

Policy	Advantage
Assign privilege by user grade and minimum privilege by document	Low-grade user access to high-grade document, user request for many users The supreme user will not able to access with an independence in 1-grade secrecy document
Limitation time for accessing document	- Overhead decreases - Efficiency increases

5 Conclusion and Future Work

In this paper, we presented a new model for insider intrusion detection. Our model uses the two elements:

- It uses attack tree to detect all possible attacks.
- Users in organization divide into user grade and assign privilege by user grade. And each document assigns important value(Security grade). In order to access to the document, it is necessary as minimum privilege. We delegate the role of intrusion detection to several users, we improve Wang *et al.*'s model.

However, our model will expect to have a few shortcoming in the presented model. As future work, we expect to research for resolving the problem and intend to develop a simulation model to verify the performance of our model.

References

[1] Computer operations, audit and security technology. *http://www.cerias.purdue.edu/about/history/coast-resources/idcontent/ids.html.*

[2] Wikipedia - attack tree. *http://en.wikipedia.org/wiki/Attack-tree.*

[3] B. Aleman-Meza, P. Burns, M. Eavenson, D. Palaniswami, and A. Sheth. An ontological approach to the document access problem of insider threat. *In Proceedings of the IEEE International Conference on Intelligence and Security Informations, ISI 2005, Atlanta, Georgia, USA, May 19-20*, pages 486–491, 2005.

[4] Q. Althebyan and B. Panda. A knowledge-base model for insider threat prediction. *Workshop on Information Workshop on Information Assurance United States Military Academy*, Jun 2007.

[5] J. Anderson. Computer security threat monitoring and surveillance. *Technical report, James PAnderson Co., Fort Washington, Pennsylvania, April*, 1980.

[6] R. Chinchani, A. Iyer, H. Ngo, and S. Upadhyaya. A target-centric formal model for insider threat and more. Oct 2007.

[7] X. Ga and C. Yuan-da. Generating ids attack pattern automatically based on attack tree. *Journal of Beijing Institute of Tecbnology*, Jan 2003.

[8] M. Maybury, P. Chase, B. Cheikes, D. Brackney, S. Matzner, T. Hetherington, B. Wood, C. Sibley, J. Marin, T. Longstaff, L. Spitzner, J. Haile, J. Copeland, and S. Lewandowski. Analysis and detection of malicious insiders. *2005 International Conference on Intelligence Analysis,McLean,VA*, Apr 2005.

[9] C. Phillips and L. Swiler. A graph-based system for network-vulnerability analysis. *Proceedings of the 1998 workshop on New security paradigms*, Jan 1998.

[10] R. Richardson. 2001 2006 csi/fbi computer crime and security survey. *Computer Security Institute*, 2006.

[11] R. Ritchey and P. Ammann. Using model checking to analyze network vulnerabilities. *Security and Privacy*, Jan 2000.

[12] B. Schneier. Attack trees: Modeling security threats. *Dr.Dobb's Journal*, Dec 1999.

[13] E. Schultz. A framework for understanding and predicting insider attacks. *2002 Elsevier Science Ltd*, Oct 2002.

[14] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J. M. Wing. Automated generation and analysis of attack graphs. *In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA. May*, 2002.

[15] S.Jha, O.Sheyner, and J.Wing. Two formal analyses of attack graphs. *In Proceeding of 15th IEEE Computer Security Foundations Workshop, Cape Breton, Nova Scotia, Canada*, pages 49–63, 2002.

[16] T.R.Ingoldsby. Understanding risk through attack tree analysis. *CSI Computer Security Journal 2004*, pages 33–59, 2004.

[17] H. Wang, S. Liu, and X. Zhang. A prediction model of insider threat based on multi-agent. *1st International Symposium on Pervasive Computeing and Applications*, Jan 2006.