Design of Intrusion Detection System Preventing Insider Attack

Kyusuk Han[1], Hyeran Mun[1], Chan Yeob Yeun[2], and Kwangjo Kim[1]

[1] Information and Communications, KAIST, Korea
[2] Computer Engineering, KUSTAR, UAE

Abstract. Recent reports show that the loss from the malicious intrusion by insiders is more serious than by outsiders. Despite that the various attacks are occurred by insiders and outsiders, most work has been focused on the intrusion detection against outsider attacks. In this paper, we improve the Wang *et al.*'s insider predection model [15] and propose the combined model with access control for the efficient insider intrusion detection. We delegate the role of insider intrusion detection to users that reduces the malicious trial of insiders and the overhead on the centralized intrusion detection system. We also define the separated access privilege that requires insiders to find the witness for accessing the information. We show that the combination of the concept of access control enables more practical deployment of insider intrusion detection system.

1 Introduction

The malicious intrusion cases on the company assets and the overall networks are increasing every year. While the attack cases occur from outsiders, several attacks from malicious insiders also happen. In CSI/FBI report [8], incidents from outsider attack occur more than insider attack, as shown Table 1. However, the attacks by malicious insiders are more severe than the attacks from outsiders, while the number of insider attacks are quite small as you can see from Fig.1. Thus, the necessity of the intrusion detection against insider attacks is obvious to reduce the loss from attacks.

To detect and prevent the intrusion, the Intrusion Detection System (IDS) are extensively studied and deployed in many systems. 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. Deploying IDS, many outside attacks are successfully detected and prevented.

While most work on IDS focused on the intrusion detection against outsider attacks, research on IDS against insider attacks is rare so far. Wang *et al.*[15] 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 are functioning 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 has the weakness on the practical deployments. If a malicious user with a high authority may kill the predicting agent using his/her authority, the intrusion detection will be failed. In practical application, a malicious user may execute buffer overflow or race condition attack to kill the prediction agent of Wang *et al.*'s model.

In this paper, we propose an efficient model that combines the concept of 'access control' with the intrusion detection to enhance Wang *et al.*'s model for practical application. We focus ourselves on the scenario protecting documents which are one of the important assets in an organization. We delegate the role of intrusion detection to users in order to improve the previous model and detect the malicious insiders more efficiently. When a user tries to access to the documents, other users detect the malicious intrusion of the user. Limiting the time duration of the access permission on the document, our model decreases system overhead and increases efficiency for insider intrusion detection.

The rest of the paper is organized as follows: Section 2 presents the previous work on the insider threats. In Section 3, we present our model. In Section 4, we show the advantage of our model. Finally, Section 5 gives the conclusion and future work.

Table 1. Incident cases from outsider and insider in [8]

Outsider	1 - 5	6 - 10	Over 10	Unknown
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 - 5	6 - 10	Over 10	Unknown
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

2 Previous Work on Insider Attacks

In this section, we briefly review the previous work on the insider attacks. We show the previous insider threat prediction models and Wang *et al.*'s model [15] that provides the agent based insider prediction model.

Insider Attacks Numerous definitions for the term insider attack have been proposed. According to Maybury *et al.* [5], malicious insider is one motivated to

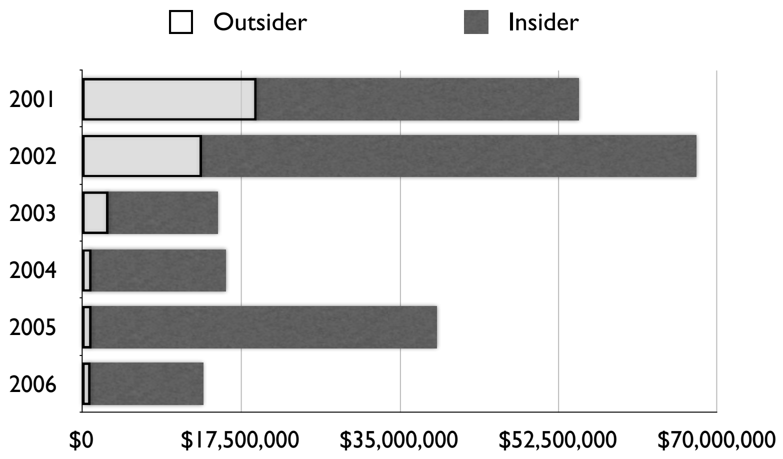

Fig. 1. Annual Losses from attacks in [8]

adversely impact an organization's confidentiality, integrity, and/or availability. According to Tugular and Spafford [11], insider attackers are those who can use a given computer system with a level of authority granted to them and violate their organization's security policy. According to Aleman-Mezal, *et al.*[1], 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 definitions involve the common notion of assigned privileges to an insider. Thus we can assume that the insiders have access privileges on the valuable information in their organization and that the insider attack is done by the insider.

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.

2.1 Insider Threat Prediction Model

Several techniques have been proposed for insider intrusion detection. In order to detect insider attacks, several studies were based on the attack tree [10] or attack graph [16]. Althebyan and Panda [2] proposed a knowledge-base model and Chinchani *et al.* [3] proposed a target-centric formal model based on the attack tree and attack graph.

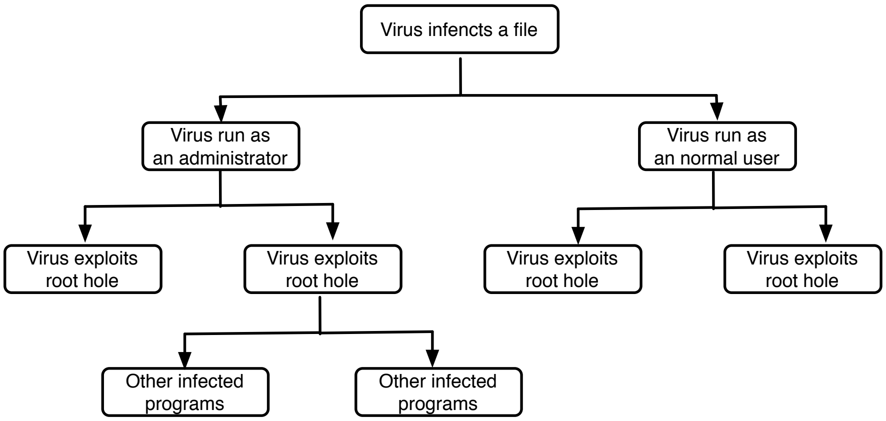

Fig. 2. Example of the attack tree for computer viruses

We show an attack tree for computer virus as a typical example in Fig. 2. It is represented tree structure, root node indicates attacker goal, leaf node indicates different ways of achieving goal. In Fig. 2, the goal of attacker is to infect a file with virus and several different ways are available to achieve the goal.

In [4, 10, 14], attack trees provide a formal and methodical way of describing the security of systems, based on various attacks. An attack tree can help organizations to establish attack scenarios by analyzing system vulnerabilities and dependencies among these vulnerabilities.

An attack graph [7, 12, 13] allows representation of a computational environment and subsequent analysis for security vulnerabilities. Also, the attack graph offers an elegant alternative in terms of symbolic machinery to appropriately represent a computational environment and to analyze it for security weaknesses.

Comparing between attack tree and attack graph, the representation of states and actions is different. Approach by attack graph seems to be too complicated. According to Ritchey and Ammann [9], a major drawback of attack graph is its scalability. So it is exactly the advantage of attack tree.

2.2 Wang *et al.*'s Model

Wang *et al.*[15] proposed the prediction model of Insider Threat Based on Multi-agents that consist of 'central agent', 'interactive agent', 'predicting agent', 'response agent' and 'communication services agent'. The notion of agents is defined to be software systems that function autonomously to achieve desired objectives in their environment.

Their model is based on the agent and the distribute intrusion detection system (DIDS) with several advantages such as flexibility, scalability, and so on. In the model, a user must have a session with interactive agent before the user can login into system successfully. Interactive agents generate the intended operations and submits them to central agents. Then, the central agents generate the customized minimal attack tree and the information of tree structure are stored in local rule database. Each user will be allocated the unique corresponding minimal attack tree. The rule database can be created in run-time that is obviously different from traditional static rule database. Predicting agents monitor users' operations and compute the probability of attacks based on the minimal attack tree. When an attack is detected, response agents will report the information to central agents. The overall framework of this model is shown in Fig. 3.

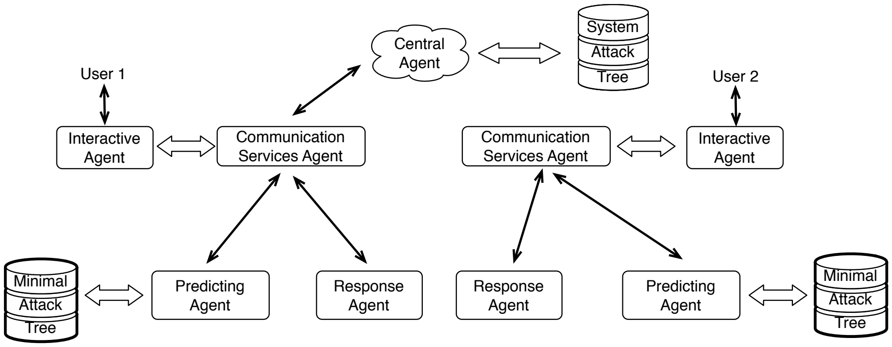

Fig. 3. The framework of Wang *et al.*'s model [15]

However, Wang *et al.*'s model has weakness on the practical application. The model does not prevent a malicious user kill the predicting agent that fails the intrusion detection. For example, a malicious user may executes buffer overflow or race condition attack to kill the prediction agent.

3 Insider Intrusion Detection System

In this section we proposed the efficient model for insider intrusion detection system (IIDS) model with the concept of 'access control'. We combines the concept of access control in Wang *et al.*'s model for the practical model. We define the model that a user (an insider) in a organization accesses to a document. 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 one of the most important asset of an organization. Insiders have the knowledge of the organization's system and the privilege for access to the documents of the organization.

In the following section, we show the framework of our model and the workflow with an attack scenario. We delegate the role of intrusion detection to several users, when an insider tries to access to the documents which exist in an organization, in order to improve the previous model and detect the malicious insiders more efficiently. An administrator manages a database that stores all the possible system vulnerability does not 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 Framework of IIDS

Our 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. 4.

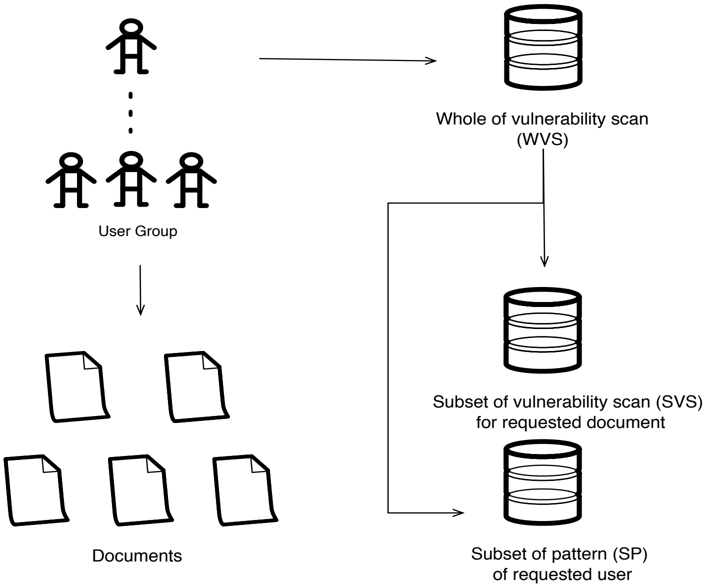

Fig. 4. The framework of insider intrusion detection model

- P_1. **User Group** Users in organization are divided into user grade and its assigned privilege. It is quite natural that as the user grade increases, the privilage of the user also increases. We show the user grade by its privilege in Table 2. The privilege may differ in applications.
- P_2. **Documents** Each document is assigned important value as 'security grade'. The user should require minimum privilege in order to access to

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	$8U_1$

the documents. It is quite natural that as the security grade increases, the minimum privilege of the user also increases. The security grades of documents and minimum privileges are shown in Table 3. The value may differ in applications.

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 not solely access 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), the user should not require other user's acceptances.

- 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) can 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 is represented as a 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 workflow of IIDS is as follows: 1) An administrator manages WVS and gets all the possible system vulnerabilities from WVS. 2) When a user requests document, he should select other users as witnesses for suitable privilege using P_1 and P_2. After receiving access permission on the document from witnesses, he can access the document. 3) The administrator generates SVS and SP from WVS. 4) Witnesses are monitoring requested user's actions examining SP and SVS while requested user accesses to the document. 5) When any attacks are generated, witnesses will report the information to administrator, then the administrator suspends the access of the user. Witnesses will update to SP and SVS. 6)Finally, the reported information is used to update to the WVS. The workflow diagram is shown in Fig. 5.

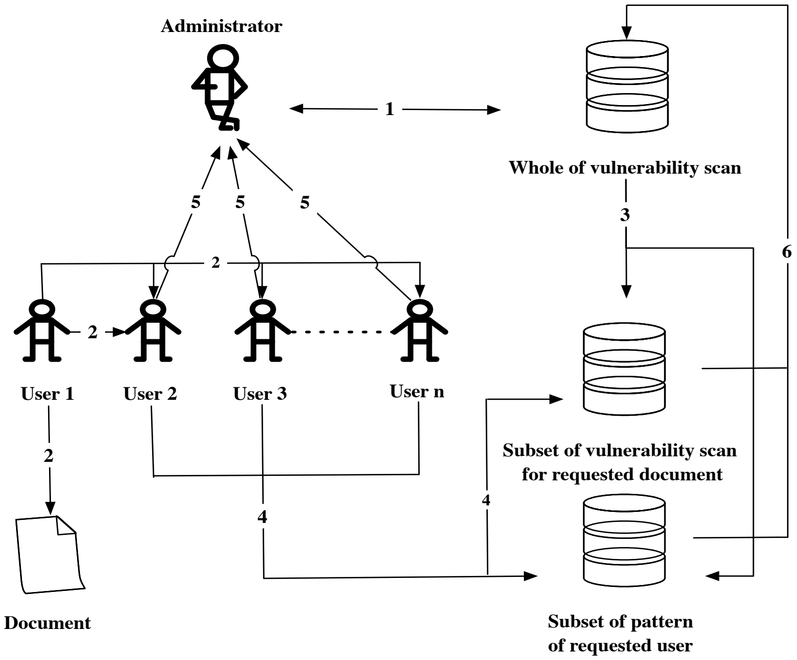

Fig. 5. The workflow of insider intrusion detection model

3.3 Example: Attack Scenario

In this section, we present an example scenario of our model for the insider attack detection.
A medium user(=U_3) accesses to document assigned important values D_2. Refer to P_1 and P_2, U_3 has privilege $4 \cdot U_1$ and D_2 assigns $15 \cdot U_1$ minimum privilege. In order to access to the D_2, U_3 needs more $11 \cdot U_1$ privilege. Therefore, U_3 randomly selects other users, $1 \cdot U_4$, $2 \cdot U_2$, and $1 \cdot U_1$ as witnesses. Thus, U_3 can has the enough access privilege on D_2 with $15 \cdot U_1$ $(4 \cdot U_1 + 6 \cdot U_1 + (2 \cdot 2 \cdot U_1) + U_1)$. Fig. 6 is shown after U_3 accessed to the D_2.
The administrator who manages WVS generates SVS for D_2 and SP of U_3 based on the attack tree. SP of U_3 includes the time limits for accessing document based on P_5. It enables the time for the detection can be also limited.
Witnesses 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 that consist of an attack tree have a same structure as Fig.6.

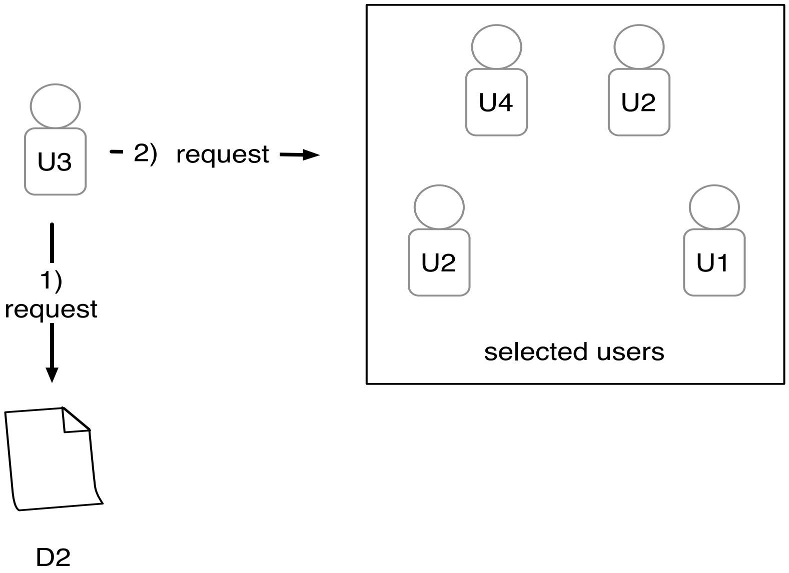

Fig. 6. After U_3 accessed to the D_2

The attack tree contains all possible attack scenarios. So, SVS for D_2 and SP of U_3 which are configured of the attack tree to detect the malicious actions of U_3. When selected users (witnesses) detect the malicious actions, they will report the information to administrator, then administrator suspends the access

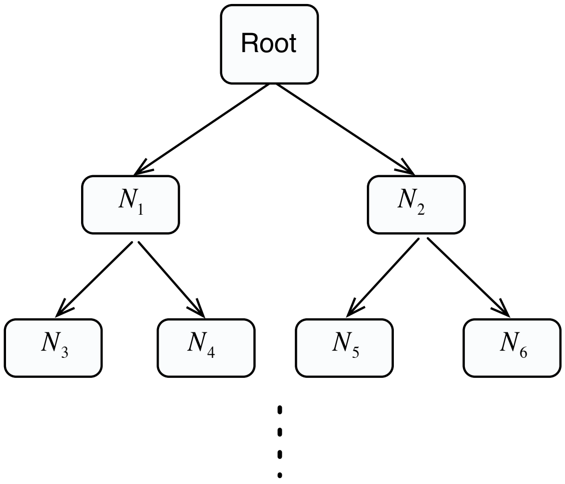

Fig. 7. Structure of attack tree

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 Advantage of our model

In this section, we compare our model with Wang *et al.*'s model [15]. Since Wang *et al.*'s model has no consideration of access control, their model does not prevent malicious users from disabling the predicting agent for themselves. In contrast our model is more applicable in practical deployment with adopting the concept of access control to Wang *et al.*'s model. We assign privilege by 'user grade' and 'minimum privilege' for accessing documents. Thus, when a low-grade user accesses to a high-grade document, the user has requests to many other users as witnesses to gain the enough privilege. Even the supreme user (U_5) will not be able to solely access to the 1-grade document (D_1) that needs to be highly secure. Also the access permission on the document with time limit decreases the overall overhead for the insider intrusion detection. Table 4 shows the overall advantage of our model.

5 Conclusion and Future Work

In this paper, we presented a new model for insider intrusion detection. In our model, we applied the attack tree to detect all possible attacks. Also, we divided users in an organization into user grade and assign privilege by user grade. And each document assigns important value(Security grade). In order to access to the

Table 4. 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

document, it is necessary as minimum privilege. We delegate the role of intrusion detection to several users, we improve Wang *et al.*'s 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. For the practical deployment, the request of users to gain the privilege should be operated randomly. Also, the automated process that minimize the human decision should be considered. Our goal is the human decision is only required for the acceptance on the involvement as a witness.

Acknowledgments. The first draft of this paper was presented in Japanese domestic conference, SCIS 2008 [6].

References

1. 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.
2. Qutaibah Althebyan and Brajendra Panda. A knowledge-base model for insider threat prediction. *Workshop on Information Workshop on Information Assurance United States Military Academy*, Jun 2007.
3. Ramkumar Chinchani, Anusha Iyer, H Ngo, and Shambhu Upadhyaya. A target-centric formal model for insider threat and more. *In Proceedings of the 2005 International Conference on Dependable Systems and Networks*, pages 108–117, Oct 2005.
4. X Ga and C Yuan-da. Generating IDS attack pattern automatically based on attack tree. *Journal of Beijing Institute of Tecbnology*, Jan 2003.
5. Mark Maybury, Penny Chase, Brant Cheikes, Dick Brackney, Sara Matzner, Tom Hetherington, Brad Wood, Conner Sibley, Jack Marin, Tom Longstaff, Lance Spitzner, Jed Haile, John Copeland, and Scott Lewandowski. Analysis and detection of malicious insiders. *2005 International Conference on Intelligence Analysis,McLean,VA*, Apr 2005.
6. Hyeran Mun, Kyusuk Han, Chanyeob Yeun, and Kwangjo Kim. Yet another intrusion detection system against insider attacks. *Proc. of SCIS2008*, Jan 2008.
7. C Phillips and L Swiler. A graph-based system for network-vulnerability analysis. *Proceedings of the 1998 workshop on New security paradigms*, Jan 1998.

8. Robert Richardson. 2001 2006 CSI/FBI computer crime and security survey. *Computer Security Institute*, 2006.
9. R Ritchey and P Ammann. Using model checking to analyze network vulnerabilities. *Security and Privacy*, Jan 2000.
10. B Schneier. Attack trees: Modeling security threats. *Dr.Dobb's Journal*, Dec 1999.
11. E.Eugene Schultz. A framework for understanding and predicting insider attacks. *2002 Elsevier Science Ltd*, Oct 2002.
12. Oleg Sheyner, Joshua Haines, Somesh Jha, Richard Lippmann, and Jeannette M Wing. Automated generation and analysis of attack graphs. *In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA. May*, 2002.
13. 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.
14. T.R.Ingoldsby. Understanding risk through attack tree analysis. *CSI Computer Security Journal 2004*, pages 33–59, 2004.
15. Hui Wang, Shufen Liu, and Xinjia Zhang. A prediction model of insider threat based on multi-agent. *1st International Symposium on Pervasive Computeing and Applications*, Jan 2006.
16. Jeannette M. Wing. Attack graph generation and analysis. In *ASIACCS '06: Proceedings of the 2006 ACM Symposium on Information, computer and communications security*, pages 14–14, New York, NY, USA, 2006. ACM.