A FRAMEWORK FOR ROLE-BASED MONITORING OF INSIDER MISUSE

Aung Htike Phyo, Steven M. Furnell, and Francisco Portilla
Network Research Group, School of Computing, Communications and Electronics, University of Plymouth, Drake Circus, Plymouth, PL4 8AA, United Kingdom, nrg@plymouth.ac.uk

Abstract: Many security incidents involve legitimate users who misuse their existing privileges, such that they have the system-level right to perform an action, but not the moral right to do so. Current Intrusion Detection Systems (IDSs) are ineffective in this context, because they do not have knowledge of user responsibilities, normal working scope of a user for a relevant position, or the separation of duties that should be enforced. This paper considers examples of the forms that misuse may take within typical applications, and then outlines a novel framework to address the problem of insider misuse monitoring. The approach argues that users with similar roles and responsibilities will exhibit similar behaviour within the system, enabling any activity that deviates from the normal profile to be flagged for further examination. The system utilises established access control principles for defining user roles, and the relationships between them, and proposes a misuse monitoring agent that will police application-level activities for signs of unauthorised behaviour.

Key words: Misuse Detection, Insider Misuse, Intrusion Detection, Role-based Monitoring.

1. INTRODUCTION

The need for information security is increasing as organizations depend on IT infrastructures for the smooth functioning of their businesses. While the media has highlighted the threat brought about by external intruders and viruses, it has not promoted the awareness of the threat to the organization's IT infrastructure from its own employees. In reality, however, insiders are

very often the cause of the most significant and costly security incidents, and a significant proportion of cybercrime can be attributed to them.

This paper examines the problem of insider misuse, and outlines a framework for monitoring of user activity in order to detect potential misuse. The literature review section examines the scale of insider misuse and explains why current Intrusion Detection Systems are unable to detect some of the insider misuses, particularly improper data access and fraud. In the methods section, the common forms of application-level misuse are listed, and the abuse of features within database applications is analysed as a more specific example. The detection strategies employed by current intrusion detection systems are evaluated, and the requirements for effective inside misuse monitoring are identified. The results section presents a conceptual framework that would allow role-based monitoring of insider misuse. This framework would allow the detection of users violating the principle of least privileges and separation of duties.

2. INSIDER MISUSE AND DETECTION ISSUES

Examining computer crime literature and surveys dating up to the mid-90s, suggests that the main threat was to be found from one's own staff (with as much as 80% of computer crime believed to be the result of insider activity). For example, in discussing the findings of the 1995 survey from the Computer Security Institute (CSI), Power (1995, p.5) observes that "the greatest threat comes from inside your own organisation". Although more recent years have revealed a different picture in terms of the incident proportions (e.g. by 2002, the CSI results reported that, for the fifth year running, more respondents had cited their Internet connection as a frequent point of attack (74%), than had cited internal systems (33%) (Power, 2002)), the financial impact of insider incidents is still clearly greater. Table 1 presents the figures from these CSI/FBI surveys, and compares the dollar amount lost due to outsider attacks to that of insider net abuse and unauthorised insider access. The figures relating to insider abuse of network access clearly suggest that, as well as bringing considerable advantages in terms of web and email communication, Internet access has also ushered in a whole range of new problems. This can be further evidenced by a survey of 544 human resources managers, conducted in 2002 and targeting large UK companies (i.e. employing an average of 2,500 people). The results revealed that almost a quarter (23%) had felt obliged to dismiss employees in relation to Internet misconduct (with the vast majority of these cases – 69% - being linked to the downloading of pornographic materials) (Theregister, 2002). Many other cases resulted in less severe courses of action, such as verbal

warnings or a discreet word in the ear of the person concerned, and in total the results indicated that 72% of respondents had encountered Internet misuse in some form.

Table 1. Annual losses for selected incidents from CSI/FBI surveys

Year	System penetration by outsider	Insider abuse of Net access	Unauthorised insider acess
1998	$1,637,000	$3,720,000	$50,565,000
1999	$2,885,000	$7,576,000	$3,567,000
2000	$7,104,000	$27,984,740	$22,554,500
2001	$19,066,600	$35,001,650	$6,064,000
2002	$13,055,000	$50,099,000	$4,503,000
2003	$2,754,400	$11,767,200	$406,300
Total	$46,502,000	$136,148,590	$87,659,800

The main difference between insider misuse and outsider attacks is that the insiders have legitimate access to the system and resources, but abuse their privileges by using the resources in an inappropriate manner or for an unapproved purpose. Anderson (1980) classifies such users as 'misfeasors'. The fact that insiders are already within the organisation often puts them in an ideal position to misuse a system if they are inclined to do so, as they have insight knowledge of what security mechanisms are employed and how to evade detection. Current Intrusion Detection Systems (IDS) are geared towards detecting attacks by outsiders, as well as insiders who employ the same methods to mount an attack. The types of attacks the IDS can detect depend on the type of data collected for analysis. The data for intrusion analysis can be collected at three varying levels of the IT systems, i.e. Network, Host OS, and application (Phyo and Furnell, 2003). Different types of misuse can manifest themselves at varying levels within the system. Therefore the data needs to be collected at the appropriate level in order to detect various types of misuses. Many of the currently available intrusion detection systems are Network-based (Roesch, 1999; Paxson, 1998), and Host-based (Anderson *et al.,* 1994; Lindqvist and Porras, 2001). Previously mentioned IDSs can detect network penetrations, exploitation of network protocols, and anomalous process behaviour. However, insiders may not need to exploit network protocols or system vulnerabilities in these ways because they already have legitimate access to it (Audit Commission, 1990). In reality many security incidents involve legitimate users abusing their existing privileges, such that they have the system-level right to perform an action, but not the moral right to do so. This is especially true in database applications as database management systems are rich in functionality and varying classes of users can manipulate the data in many different ways. One of the main problems of insider misuse is the improper access of data within

databases, which can result in data theft, breach of privacy, fraud, and compromised data integrity. Database level misuses can have severe impact on the organisation as many businesses employ database systems for record management, accounting, trading, business analysis and strategic planning. The authors have identified two notable approaches amongst previous work that detect anomalous behaviour at the application level. The first of these, DIDAFIT (Detecting Database Intrusions Through Fingerprinting Transactions), monitors anomalous SQL queries by generating fingerprints of authorised queries (Low *et al.,* 2002). These fingerprints are sequences of SQL queries, along with variables that the users should not change, ensuring that the queries are executed in proper order and only on the restricted range of records. Another example is (Detection of Misuse In Database Systems) DEMIDS (Chung, Gertz, and Levitt, 1999), which attempts to profile working scopes based on user access patterns in relational databases, and assumes that a user will not typically access all attributes and data in a database schema. Therefore user access patterns will form some working scopes, which are sets of attributes usually referenced together with some values. Based upon this assumption, Chung *et al.* (1999) defined the notion of a distance measure between sets of attributes that consider both the structure of the data and user behaviour. This notion is then used to guide the search for regular patterns that describe user behaviour in a relational database. However, to be able to detect, data theft and potential occurrence of fraud in complex transaction/trading systems, the detection system also needs to have the knowledge of user responsibilities, work patterns, separation of duties and organisation hierarchy. Knowledge of job positions and segregation of duties are important as the opportunity for misuse arises when the individual is in a position of trust and the controls are weak. Many of the misuses in Audit Commission (1990) survey are the result of lack of application level controls and proper segregation of duties. Therefore, there is a need to provide the detection system with knowledge of required separation of duties, business processes, and working scope in order to enable more effective monitoring.

3. OPPORTUNITIES FOR APPLICATION-LEVEL MISUSE

Commercial applications include more features than the users may actually need to perform the task, and such features may sometimes be misused. In feature rich applications where users of varying responsibilities may access different features and the mechanism to control access to the features may not be present. Again, some of the features may not be easily

disabled. Therefore, the detection system needs to monitor the features/functionality accessed by each user. In order to be able to prevent and monitor insider misuse, the nature of potential misuses must firstly be identified and analysed. This section analyses how features in common applications can be misused, and suggests a functional classification. Table 2 list the possible misuses with regard to the type of application commonly available on most computers, with the right-hand column indicating the means by which misuse would be achieved (Portilla, 2003).

Table 2. Misuse of typical application features

LEGITIMATE ACTION	MISUSE
Client/Server Applications	
Message Exchange	Unusual exchange of messages hat degrades performance
Connectivity to Server	Exceeding possible number of connections to cause a denial of service
Execution of Tasks	Executing privileged procedures
Word Processors	
Writing a Document	Insertion of illegal content Insertion of malicious code
Mail Clients	
Sending and receiving emails	Distribution of illegal content Setting up remote attack Private use/gain Spamming
Browsers	
Browsing the Internet	Access to illegal content
Access to cached files and history	Displaying other user's view files and previous accesses
Programming tools	
Developing programs	Creation of malware
Debugging	Access to memory segments containing sensitive data
General purpose applications	
Input to programs	Buffer overflow for elevation of privileges Buffer overflow for cod execution Buffer overflow for denial of service
Database Applications	
Data access	Anomalous browsing of database Inference attacks Inappropriate modification of data

Despite controls established in databases, authorised users may misuse their legitimate privileges. Possible misuses associated with legitimate visualisation rights are:

- Data aggregation: users could try to collect information about one or more individuals, transactions or products for different purposes.
- Displaying data in an improper way (conditioned or sorted): when information is not displayed in a manner that exclusively serves the purpose of the database system, it can provide additional information and capabilities. For example, displaying a telephone directory sorted by number.
- Retrieval of a large amount of data: users could attempt a partial reconstruction of the database by retrieving a large amount of information. This reconstruction could possibly provide more operations over the data that were initially restricted.
- Discovering the existence of restricted information: unsuccessful attempts to display restricted fields could allow users to identify records with sensitive information or to guess part of them.
- Inference: Data within a database is semantically related. Therefore, sometimes users can come to know an unknown value without accessing it directly by inferring it from known values.

Misuses associated with legitimate creation and modification rights are:

- Deliberate insertion of false data: users can insert erroneous content in the database in order to damage its integrity or to corrupt the supported procedures.
- Misuse of coherence mechanisms: users can exploit mechanisms that check for coherence and compatibility of related values in the database. They may be able to discover the structure of the database, by displaying error messages when attempting to perform a writing operation. Besides, inserting false information into particular fields might be used to change the values of initially restricted fields.

Considering the list of potential misuses listed in the table, it is possible that appropriate controls could be used to prevent some of them, but even these will not be sufficient for all contexts (consider, for instance, the case in which the misfeasor has legitimate access to the payroll database, but modifies records to raise his own salary). In this example, even though the user has the system right to modify the data, it should require someone else to authorise the modification. Many of the insider misuse cases in Audit Commission surveys are a result of lack of separation of duties and application level control (Audit Commission, 1990). Therefore, insider misuse is not only a technical problem, but also a managerial problem, because in some cases it is the improper segregation of duties that presented the problem. One of the main problems of insider misuse is the improper

access of data in database environments, which can result in data theft, breach of privacy, fraud, and compromise of data integrity, depending on the motive of the perpetrator.

4. A COMPARISON OF DETECTION STRATEGIES

IDS employ two main strategies to identify attacks, namely misuse-based and anomaly-based detection (Amoroso, 1999), and it is possible to see how each of these could be applied to the insider problem.

Misuse-based detection. This approach relies upon knowing or predicting the incident that the system is to detect. Intrusions are specified as attack signatures, which can then be matched to current activity using a rule-based approach. A similar approach could potentially be incorporated for misfeasor incidents, based upon those methods that employees have been known to exploit in the past, or those that can be anticipated they would attempt based upon the privileges and resources available to them. For example, at a conceptual level, one such misuse signature might relate to a user who is identified as attempting to modify a record about him/her in a database. The rule here is that no one should modify their own records without someone else's authorisation. The problem with applying misuse-based detection to insider misuse is that the possible misuse scenarios for insiders are wide ranging and could be extremely organisation-specific. Thus it would be difficult to catalogue them all. Misuse-based detection is only as good as the database of signatures it relies upon for detection. Therefore, the database would need to be updated constantly to detect new attack methods. This approach would not be suitable for insider misuse detection as it would be too time-consuming in person-hours to create misuse signatures for all possible scenarios and to continually keep them updated.

Anomaly-based detection. This approach relies upon watching out for things that do not look normal when compared to typical user activities within the system. In standard IDS, the principle is that any event that appears abnormal might be indicative of a security breach having occurred or being in progress. The assessment of abnormality is based upon a comparison of current activity against a historical profile of behaviour that has been established over time (Anderson *et al.,* 1994). One advantage insider misuse detection system has over outsider attacks is that it is possible to characterise normal activities of insiders according to their job position, as users with the same responsibilities should exhibit similar activities within the system and application environment to complete their daily tasks. The similarities may be profiled to represent normal behaviour for users with the same responsibilities, and different profiles for different job positions. If the

user's behaviour deviates from the normal profile that represents his position, the activity should be flagged as suspicious. An example would be monitoring frequency of access to certain databases can lead to the detection of in insider who browses the database for personal use. Examples of such databases are medical records, and criminal records.

The concept of applying the techniques for the detection of misfeasor activity makes the task more difficult, because we are dealing with legitimate users who are not violating system level access controls. From a misuse-based detection perspective, it is more difficult to identify the ways in which an insider might misuse the resources to which they have legitimate access, while from an anomaly detection perspective the level of behaviour profiling would need to be more precise and comprehensive. When basing the assessment upon a comparison against their behaviour profile, a legitimate user misbehaving will almost certainly be more difficult to identify than a total impostor who is masquerading under the legitimate user's identity, because it is more likely that the impostor's behaviour would deviate by a larger margin, whereas conversely the deviation is likely to be minimal for a legitimate user who abuses existing privileges. In addition, in an adaptive system, the process of profile refinement might be exploited by wily misfeasors who gradually train the system to accept misuse behaviour as normal. Again, when users change positions within the organisation, their behaviour would change to reflect the new responsibilities assigned. A potential solution to counter the exploitation of profile refinement, and improve profile management is to profile common user behaviour based on the role the user takes up within the organisation. Another advantage of role-based profile comparison is that when the users of a particular role are assigned special assignments, the sudden change of user profile may not be considered anomalous, if the changes are similar for all users within the same role. Individual user profiles can be complemented, such that activities associated with job responsibilities are stored in the role profile and the rest in individual user profiles.

5. KNOWLEDGE OF SEPARATION OF DUTIES

Another problem associated with insider misuse detection is that current IDSs lack the necessary knowledge of business processes, organisation hierarchy, separation of duties, and the role of the users within the organisation structure. This knowledge needs to be expressed in the form that is understandable to the detection system, if effective misfeasor monitoring is to take place. Role management principles specified by (Gavrila and Barkley, 1998) are utilised in Role-Based Access Control

(RBAC) to support user role assignment, role relationships, constraints and assignable privileges. The idea of role-based access control was introduced by Ferraiolo and Khun (1992). While privileges are assigned directly to users in Discretionary and Mandatory Access Control methods, assignment of privileges is a two stage process in RBAC. Privileges are assigned to roles and the users are assigned to roles, subsequently the user inherits the privileges assigned to the role. A role can be thought as a collection of operations required to complete the daily tasks of a user. This approach simplifies the task of assigning permissions to the user, as the roles for appropriate job functions are created with the least privileges required to complete the relevant tasks and the users are assigned to the role that reflects their responsibilities. Users can be assigned from one role to another, or assigned multiple roles, and permissions can be assigned at role-level to affect all users associated with the role. This use of roles is similar to the use of groups in Discretionary Access Controls (DAC). The main focus of RBAC is to maintain the integrity of the information by defining who can perform what operations on which set of data. The type of operations and objects that can be controlled by RBAC is dependant upon the environment and the level at which it has been implemented. For example, at the OS level, RBAC may be able to control read, write, and execute; within database management systems controlled operations may include insert, delete, append, and update; within transaction management systems, operations would take the form that express the properties of a transaction. The term transaction here means a combination of operation and the data item affected by the operation. Therefore, a transaction can be thought of as an operation performed on a set of associated data items. The ability to control specific transactions, rather than restricting simple read and write operations are very important in database environments. For example, a clerk may be able to initiate a transaction and the supervisor may be able to correct the completed transactions, for which both users need read and write access to the same fields in the transaction file. However, the actual procedures for the operations and the values entered may be different. Meanwhile, the clerk may not be allowed to correct the completed transactions and the supervisor may not be allowed to initiate the transactions. The problem is that determining whether the data has been modified in the authorised manner, for it can be as complex as the actual procedures that modified the data. This is where SQL fingerprinting techniques utilised in DIDAFIT can be employed. However, transactions need to be certified and classified before associating them with the roles. To characterise the required transactions for a role, duties and responsibilities of the users need to be specified first.

The most interesting feature of RBAC is the ability to define relationships between roles and enforce separation of duties. In RBAC, separation of duties can be applied by specifying mutually exclusive roles, and allow administrators to regulate who can perform what actions, when, from where, in what order and sometimes under what circumstances. Access controls only allow or deny access to certain resources, however there is a need to monitor and analyse the user actions after the access has been gained and the operations had been carried out. In theory the idea of roles and role-management principles can be applied to misfeasor monitoring. Instead of allowing or denying operations to be performed, common user operations can be associated with roles, and the users can be assigned to appropriate roles. If the user's operations deviate from the common profile, a thorough investigation can be carried out to clarify if the user has misused the system in an inappropriate manner or for unapproved purpose.

6. PROPOSING A FRAMEWORK FOR MISUSE MONITORING

It has been mentioned previously that anomaly detection is more suitable for insider misuse detection, because employees' normal behaviour can be profiled. It is assumed that the users with the same responsibilities within the organisation will exhibit similar activities within the system, and their working-scopes may be established. The idea of establishing working-scopes for users with same responsibilities has been tested in relational database environments by Chung *et al.* (1999). However, in order to be able to detect violation of separation of duties, the detection system needs to be provided with the knowledge of organisation hierarchy and relationships between roles. RBAC utilises role-relationship management principles to define role-hierarchy and separation of duties. The authors' proposed system combines the ability of RBAC to provide knowledge of role- relationships, with intrusion detection techniques to effectively detect users who abuse their existing privileges.

Figure 1 presents the framework of the conceptual insider misuse detection system. Functional modules are explained in subsequent paragraphs.

6.1 Management Functions

All management functions, such as defining roles, characterisation of operations, association of operations to roles and user assignment to roles,

are carried out from the Management Console. The working scope of a user is defined by the operations associated with the role(s) the user assumes. Once the separation of duties between roles has been defined, it is expressed in the Role-Relations Matrix, such as inheritance, static separation of duties, and dynamic separation of duties. Static separation of duties occurs at the role level by specifying mutually exclusive roles. When the two roles are in static separation of duties, a user may not be assigned both roles. Dynamic separation of duties occurs at the operations level and the conditions can be that operations within dynamically separated roles are mutually excluded, disallowed to execute concurrently, or disallowed to be performed on the same set of data.

When the two roles are in dynamic separation of duties, the user may not execute the operations that are mutually exclusive or on the same set of data. The relationships expressed in the Role-Relations Matrix are checked against the rules specified by (Gavrila and Barkley, 1998) for consistency.

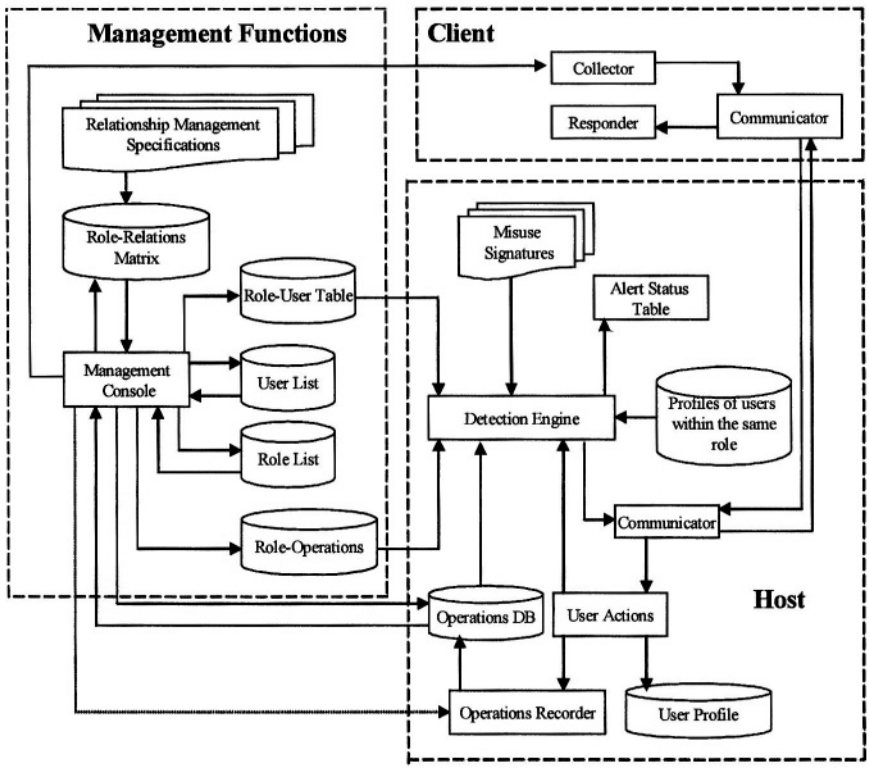

Figure 1. Conceptual Framework for Role-Based Monitoring of Insider Misuse

6.2 Host

This is where the actual profiling of user(s) and the detection process takes place. Characteristics of each operation are stored in the *Operations DB* along with an appropriate name for each operation. The characteristics are dependent upon which level of the system they are being profiled at. Characteristics of the operations may be in the form of file access, sequence of system calls, SQL queries, API calls, User interactions, and Network access. Recording the characteristics of each operation is controlled from the *Management Console.*

The profiling should be done at all three levels of the system namely: network, system, and application level. The *Detection Engine* checks the roles available to the active user, and next checks the *RoleOperations* table for the names of the operations available to the user. After this, the characteristics of the available operations from the *Operations DB* are compared to the current user actions. If current user actions do not match the characteristics of operations available to the user, the administrator is alerted. This alert may indicate the user performing a totally new operation, or performing a valid operation in the *Operation DB* but is violating separation of duties because the operation is not listed under any roles the user may assume.

The envisaged detection flow is as follows:

1. Detection Engine gets the name of the user from the Client. Looks for the roles the user's name is associated with, in the Role-User table.
2. After acquiring the list of roles for the user, the Detection Engine looks for the names of the operations associated with each role in the Operations DB (Note: only names of the operations are associated with the Roles.)
3. After acquiring the names of operations available to the user, the Detection Engine reads the characteristics of available operations from the Operations DB and they are compared against current user actions.
4. If the current user action matches with the characteristics of operations available to the user, then the user is not in breach of static separation of duties.
5. If OpA belongs to RoleA, OpB belongs to RoleB, and RoleA and RoleB are in dynamic separation of duties. Condition of the separation is checked to clarify whether the operations are: mutually

excluded; disallowed to execute concurrently; or disallowed to perform both operations on the same set of data.

If the user violated the specified condition, the system security officer is alerted. In addition, the misuse rules employed in expert systems within traditional IDSs can also be included. These rules may then be associated with an operation, such as modifying the payroll database to increase one's own wages. In this case, the process is as follows: If modification is performed on the payroll database, check that the employee ID of the user is not the same as that of the record being modified. (Note: This will require the inclusion of system user ID in the personnel records.)

6.3 Client

This is where the actual data is collected and transferred to the Host for analysis. The *Clients* can be network server systems or end-user workstations. The nature of the data collected may vary depending on the type of the *Client.* For example, mail logs can be collected from the mail server, user queries from the database server, and application logs from user workstations. The data to be collected is specified by the system administrator from the *Management Console.* The collected data can then be refined to a standard format by the *Communicator* module before sending the data to the *Host,* so that data from heterogeneous *Client* systems is in a standard format. The *Client* may also have a *Responder* module to respond to detected incidents, and the appropriate response for each incident can be specified from the *Management Console.* For example, when a misuse is detected, the *Responder* may be configured to terminate the user session, revoke privileges, deny further access, alert the security officer, or terminate the anomalous process (Papadaki *et al.,* 2003).

7. DISCUSSION AND CONCLUSIONS

Insiders pose a considerable threat and organisations need to give equal priority in detecting insider abuse as well as outsider attacks. Access controls only allow or deny access; however there is a need to monitor what the user does after gaining access to the system and objects. In order to effectively monitor privilege abuse, IDS require the knowledge of organisation hierarchy, managerial controls, responsibilities and working scopes of each user. The methods employed in RBAC to express knowledge of roles, organisation hierarchy, and separation of duties can be coupled with

intrusion detection techniques to detect users who abuse their existing privileges. This paper presented a framework for monitoring users who abuse their existing privileges.

In order to be able to implement the system successfully, separation of duties would first need to be defined at the organisation level. Next, the responsibilities of the users need to be defined. Then it needs to be checked that the operations a user is allowed to perform would not lead to a successful misuse. All of these are more of a managerial (rather than technical) issue. However, these are not trivial and could require considerable amount of time and labour. Again, at a technical level, monitoring of user behaviour at application level may require modification of the software package if appropriate APIs are not included.

The authors' future research will focus on developing the proposed system and testing it against a variety of simulated insider misuses, such as data theft, fraud, net abuse, sabotage, and breach of privacy.

8. REFERENCES

Amoroso, E., 1999, *Intrusion Detection: An Introduction to Internet, Surveillance, Correlation, Traceback, Traps and Response,* First Edition, Intrusion.Net books, NJ, ISBN: 0966670078.

Anderson, D. Frivold, T. Tamaru, A. And Valdes A., 1994, Next-generation intrusion detection system (NIDES): Software users manual, Technical Report. Computer Science Laboratory, SRI International. December 1994.

Anderson, J.P., 1980, Computer security threat monitoring and surveillance. Technical Report, James P Anderson Co., Fort Washington, April 1980.

Audit Commission, 1990, Survey of computer fraud & abuse: Supplement. Audit Commission, 1990.

Chung, C.Y. Gertz, M. Levitt, K., 1999, DEMIDS: A misuse detection system for database systems, in the Proceedings of the 3rd International Working Conference on Integrity and Internal control in Information Systems. 18-19 November, Amsterdam. pp. 159-178.

Ferraiolo, D. Kuhn, R., 1992, Role-based access control, In the Proceedings of the 15th National Computer Security Conference, October 1992, Washington DC. pp. 554-563.

Gavrila, S.I. Barkley, J.F., 1998, Formal specification for role based access control user/role and role/role relationship management, Third ACM workshop on Role Based Access Control, October 22-23, Fairfax, Virginia. pp 81-90.

Lindqvist,U. and Porras, P., 2001, eXpert-BSM: A host based intrusion detection solution for Sun Solaris. 17th Annual Computer Security Applications Conference, New Orleans, December 2001.

Low, W. L. Lee, J. Teoh, P., 2002, DIDAFIT: Detecting intrusions in databases through fingerprinting transactions. In the Proceedings of the 4th Internationsal Conference o Enterprise Information Systems, Ciudal Real, Spain, April 2-6, 2002.

Paxson, V., 1998, Bro: A system for detecting network intruders in real-time, In 7th Annual USENIX Security Symposium, San Antonio, Texas, January 26-29, 1998, pp.31-52.

Phyo, A.H and Furnell, S.M., 2003, Data gathering for insider misuse monitoring, In the Proceedings of the 2nd European Conference on Information Warfare and Security, pp.247-254, University of Reading, UK, 30th June-1st July, 2003.

Portilla, F., 2003, Analysis of insider misuse in commercial applications, MSc thesis, University of Plymouth, United Kingdom, September 2003.

Power, R., 1995, Current and future danger: A CSI primer on computer crime and information warfare. San Francisco, CA: Computer Security Institute.

Power, R., 2002, 2002 CSI/FBI computer crime and security survey. Computer Security Issues & Trends, Vol. VIII, No. 1. Computer Security Institute. Spring 2002.

Richardson, R., 2003, 2003 CSI/FBI Computer Crime and Security Survey, Computer Security Institute. Spring 2003.

Roesch, M., 1999, Snort - lightweight intrusion detection for networks, In the Proceedings of the 1999 USENIX LISA Conference, Seattle, Washington, November 7-12, 1999, pp.229-238.

Theregister, 2002, Leyden, J. (July 9 2002); P45s for porn surfers, http://www.theregister.co .uk/content/6/26098.html.