Prerequisites for monitoring insider IT misuse

A.H.Phyo, S.M.Furnell and A.D.Phippen
Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: aung@jack.see.plymouth.ac.uk

Abstract

Although the problem of insider misuse of IT systems is frequently recognised in the results of computer security surveys, it is less widely accounted for in organisational security practices and available countermeasures. The countermeasures available today are oriented towards the prevention and detection of outsider attacks on the organisation's IT systems and services. However, we argue that it is possible to apply similar mechanisms and strategies towards monitoring of insider IT misuse. However, there are requirements that need to be satisfied before insider misuse monitoring can be put in to practice and it is recommended that a misfeasor monitoring system should include features for monitoring file access through arbitrary applications, file replication, partial data replication, file transfer, file deletion, user management, settings/configuration management, database access, and Internet access.

Keywords

Intrusion, Detection, Misuse, Misfeasor

1. Introduction

Frequent headlines reporting intrusions to computer networks and rapidly spreading computer viruses have steadily increased public awareness of the threats posed to information security. However, external hackers and malicious software are far from being the only threats to the security of an organisation's IT systems and valuable data. CSI/FBI survey results, detailed in Table 1, have consistently shown that a significant amount of financial loss can be attributed to insider IT misuse.

Year	System penetration by outsider	Insider abuse of Internet access	Unauthorised insider access
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
2004	$901,500	$10,601,055	$4,278,205
2005	$841,400	$6,856,450	$31,322,100
2006	$758,000	$1,849,810	$10,617,000
Total	$49,002,900	$155,455,905	$133,877,105

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

Supporting results from the ICT Fraud and Abuse 2004 survey (Audit Commission, 2005) also reveal that the majority of the perpetrators (over 80%) originate from inside the organisation, with operational staff 37%, administrative/clerical staff 31%, and managers 15%.

From the organisation's point of view, insiders can be full- or part-time employees, consultants, contractors and staff from partner firms. From the IT system's perspective, insiders are users with a valid login account and have legitimate rights and privileges to access the resources it manages. Within the scope of this paper, the discussion concerns individuals who have legitimate access to the organisation's IT system and resources, but abuse their access rights. Anderson (Anderson, 1980) termed such users as *misfeasors*. The insider abuse can be more damaging than many outsider attacks, since the perpetrators have a good idea of what is valuable within the company. Knowing where these resources are stored, and what security mechanisms are used to protect them, also helps insiders in circumventing controls and evading detection (Einwechter, 2002). A survey commissioned by Microsoft has revealed that amongst the 2,226 UK employees who responded, if there was an opportunity 54% would be willing to gain illegal access to sensitive information stored on their employer's IT systems, while 22% admitted to have already done so (Microsoft, 2006).

This paper evaluates the applicability of existing security mechanisms towards prevention and detection of misfeasor activities. The discussion begins with the motivations involved in misfeasor activities, and associating the motivation with the type and nature of the activities. It then proceeds to analysis of currently available Intrusion Detection Systems, how these tools function and their applicability within the context of misfeasor monitoring. The paper then discusses the requirements that need to be satisfied in order to enable effective monitoring of misfeasor activities in practice.

2. Background

2.1. The definition and the scope of the terms (Insider and Misuse)

Within the scope of this paper an insider is an individual with valid login account and legitimate access to the system and its resources. Therefore, one may ask what is misuse, when the user accesses the system and the resources that he/she has legitimate system level access rights? Within the scope of this paper, misuse can be defined as any activity that the user has legitimate system level rights to perform, however the activity may not be acceptable within the context of the application, organisation, or moral or ethical conduct. While the type of activities may vary, motivation behind misfeasor activities can be classified into three distinct categories:

> **Vengeance**: Former/disgruntled employees may be motivated to carry out damaging/disruptive or generally unethical activities upon an organisation's IT systems and data. The activities motivated by vengeance may include denial of service attacks on company servers, or sabotage of organisation's IT systems and/or resources, and exposure of confidential information (Gaudin, 2000). For example, deleting critical business databases or configuring critical servers in such a way that they become vulnerable to

attacks, become easily accessible to unauthorised users, or becomes inaccessible to authorised users. Another example is intentionally exposing confidential information so that it may damage the reputation of the organisation or cause embarrassment to an employee/customer. Sometimes the activity may not be directed towards the organisation, but rather a colleague, or an acquaintance that happens to be one of the organisation's customers. However, the organisation may still be held liable for failing to protect the data.

Financial gain: Activities motivated by financial gain may include providing proprietary or confidential information to unauthorised parties or configuring the systems in such a way that unauthorised parties could gain access to proprietary and confidential information, in return for financial benefits. In addition, the misfeasors may also defraud the organisation and/or its customers for financial gain (Dhillon and Moores, 2001).

Recreation & Curiosity: Activities including recreational web surfing, downloading illegal software, perusing and writing personal emails and chatting through instant-messengers. While performing these activities, users may be unable to carryout productive work. In addition, media downloaded from the Internet may be copy protected, or contain inappropriate content such as pornography. This may damage the organisation's reputation and the organisation may also be held liable. Misfeasors may also access an organisation's business databases for personal reasons, which may result in breach of privacy to an employee or a customer.

In addition, accidental misuse may also occur as a result of negligence or users' lack of IT security awareness (Furnell, 2006).

In summarising the above discussion, legitimate activities in the system and network context that may be deemed unacceptable/inappropriate in the organisation/business and application context include:

1. Internet access
2. File access through arbitrary applications
3. File replication (copy, paste, save as)
4. Partial data replication (print screen, copy, paste)
5. File/data transfer through communication applications
6. Settings/configuration changes
7. User management
8. Database access

In developing this argument, we consider whether current Intrusion Detection Systems (IDS) can be employed to detect misfeasor activities in the following section.

2.2. Intrusion Detection Systems (IDS)

Intrusion detection systems are generally categorised based upon the data analysed in order to recognise an attack.

Network IDS: analyse network packets, network protocols and network statistics in order to detect attempts to exploit network protocols and network applications. A successful attack may result in legitimate users being unable to access an organisation's network services, or the attacker may gain access to the machine on which the server application is run.

Host IDS: analyse resource utilisation (CPU/memory/disk usage, number of files opened, number of system calls made), and behaviour of applications (system calls, file access) to detect attempts to exploit system/application vulnerabilities. A successful attack may result in the attacker gaining access to the machine, or the attacker gaining higher privileges.

There is also another category of hybrid systems that analyse both network and host data in order to determine attacks.

IDS can also be categorised based upon the detection strategy employed (Amoroso 1999).

Misuse Detection: This approach relies upon knowing or predicting the intrusion scenario 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. With this approach the detection system is only as good as the database of attack signatures, and may not be able to detect variations of an attack. The problem is that misfeasor activities do not demonstrate the same characteristics as external penetration attacks (Schultz 2002).

Anomaly Detection: This approach relies upon detecting activities that do not look normal when compared to typical user behaviour within the system. The assessment of abnormality is based upon a comparison of current activity against a historical profile of user (or system) behaviour that has been established over time. With this approach, variations of an attack or novel attacks may be detected. However, characterising normal behaviour is difficult and, deciding the variables to be involved for characterisation still requires insight knowledge of the system and the application environment.

IDS may employ a variety of techniques, including expert systems, neural networks and statistical analysis for detecting attacks. Earlier in this paper, we have proposed that existing techniques and monitoring strategies may also be applied to detecting misfeasor activity. However, the majority of currently available IDS are designed to detect network penetrations and privilege escalation attacks. Misfeasors do not need to perform network penetration attacks, since misfeasors already have legitimate access to the network and systems. And by definition, misfeasors do not perform privilege escalation attacks, and do not violate system level controls. However, misfeasor activities may be deemed unacceptable within the application, business, or organisation context. Therefore, any inherent ability to detect misfeasor activity by current IDS would be a coincidence rather than by design. The fact that misfeasors do not violate system level and application level controls makes it extremely difficult to identify misfeasor activity due to lack of reference data/information in order to conclude whether violation of (security or acceptable usage) policy has occurred. In addition some misuses may not be evident at network or host level alone, and misuse may only be recognised when analysed in the context of the application, business rules surrounding the operation, and within the context of the organisation. A correlation of network, host, application, contextual information and rules is needed for analysing the possible occurrence of misuse. Therefore, the data required for successful detection of misfeasor activities need to be identified first.

3. Relevant Data for Misfeasor Analysis

Within the IT environment, users access and manipulate the data stored and managed by the computer system through the use of application programs. The entities involved in the data access are the machines involved (server-client, peer-peer), the data, the users, and the application utilised. Therefore, information regarding these entities will certainly be relevant for misfeasor analysis.

Machine Details: Files and databases are stored, processed, manipulated, managed, and transferred to and from computer systems. Although a user has legitimate access rights to the data, the machine utilised to access the data may not satisfy security requirements of the data. For example, a user who has access to the data transfers the file to an external machine. Although, the user at the receiving end might be also authorised to access the data, the machine utilised at the receiving end may not be regulated by organisation's security mechanisms. Therefore, the security requirements of the system to which users have access, which computers can access the file/database server, and other details such as location and physical security of each machine will be relevant for detecting misfeasor activities.

File and Database Security Requirements: Data is stored within files and databases on computer systems. Since the aim is to ensure the security of the data, it is essential that the security requirements of the file/databases be provided to the monitoring system for reference. Control mechanisms determine only whether the user has read or write access the data (Escamilla 1998). In order to detect data theft/leakage, information regarding whether partial/whole replication of data is acceptable, and whether the data can be saved to a removable media needs to be defined. It is more difficult to manage the security of multiple copies of confidential data on various machines. Therefore, it is also important to keep track of how many copies of a critical file exist, and where they are located. Keeping track of critical files will also become useful when recovering deleted data, or verifying whether it is the only copy prior to deletion. Since the business managers have better knowledge of the sensitivity, and the users who needs access to the data and the validity of access, it is they who should be given the responsibility of defining the security requirements of the data, instead of the system administrator who may not have equivalent knowledge of the contents and security requirements of the file/data in the business context. In addition, if an event does not satisfy the security requirements of the data, the business manager should be alerted. Therefore, the information regarding who the file custodian is will also be useful for alerting the right person in the event of suspicious activity. It may not be practical to monitor all data files as a computer system may also contain system files and user's personal files. Therefore files regarded as intellectual property of the organisation and files that require misfeasor monitoring should be listed and tagged with security policy.

User Details: A misfeasor that has access to the file may transfer the file to someone who is not authorised. The file may be transferred through email, instant messaging, or some other programs with communication capability. Therefore, contact addresses of organisation's employees, customers, or contractors should be provided to the monitoring system to determine misfeasor activity. Information regarding, the user's responsibilities and roles within the organisation will also be useful when alerting the system administrator or file custodian, so that the file custodian will be able to make better decision regarding the validity of the activity within the business context.

Application function and capabilities: The application utilised determines what the user can do with the system or data accessed. Therefore, data regarding user activity within the application environment will be relevant for detecting misuse. However, it may not be practical to monitor all applications and application functions. Applications that require monitoring can be divided into two categories based on the data access capabilities.

> **Applications with access to file or databases**: Applications with direct access to file and databases include file managers, word processors, document readers, image editors, media players and database programs. File managers do not have direct access to the contents of the file, but provide capability to replicate, move, and delete the file. User activities regarding file replication, relocation, and deletion need to be monitored to detect misuse. Document readers and processors have direct access to the entire contents of the file, and also provide capability to edit, and replicate partial or entire contents of the file. It may not be possible to automate the integrity checking of the contents of documents if various users are allowed to update the document, as the structure of the data within the documents may vary with each update. Database programs access small part of the file; however a single record may contain critical information regarding the organisation, a business transaction, an employee, or a customer. User access to each record, for both viewing and updating needs to be verified. If possible, access to each record should be validated, and the integrity of the record should be verified after each update. To be able to automate this validation and verification process, reference information needs to be provided to the monitoring system.

> **Application with no access to file or databases**: The applications that do not have direct access to the contents of the file yet may affect the security of the system and data include security applications, configuration managers, user management applications, and applications with communication capability. Security applications can be used to harden or weaken the security of a system or an application that may result in unauthorised users gaining access or authorised users being unable to access. Therefore, changes to security settings need to be verified against security requirements of the system or application as defined in the policy. The correct execution of a system or an application depends on the correct configuration, and therefore changes to configuration need to be verified against an appropriate reference. Adding users to a system or a role in effect allows the user to gain access to the system or the files accessible for the assigned role. Therefore system administrators and role managers should be asked to authorise the addition of a user. Applications with communication capabilities, such as email and messenger may be used to transfer files, or partial data. In order to detect misuse, the monitoring system needs to determine whether the server mediating the communication is managed by the organisation, whether the recipient is authorised to access the file, and whether the machine utilised by the recipient satisfy security requirements for accessing the file transferred. Therefore, the details of the file, the sender, the server, the recipient, and the machines utilised for communication is required for analysis of possible misfeasor activity.

Before misfeasor monitoring can be put in to practice, the applications need to provide the monitoring system with the information described previously in order to enable misfeasor activity detection.

Contextual rules related to operations: Sometimes, certain conditions may need to be satisfied for an operation to be legitimate within the application and business context. Required conditions may vary from one business to another, and one operation to the next. When an operation does not conform to the required conditions, the activity may result in fraud/misuse. There may be pre-requisite conditions to be satisfied. For example, when a user account is created, a business rule may require that the user of the account exists in the human resource database as an employee of the organisation. There may also be post-requisite conditions to be satisfied. For example, when a user is added to a role, the policy may state that the role manager must verify the addition of the user to the role, and the time period for verification to be made may also be defined. Within certain applications, other contextual rules may exist. For example, in some businesses if the payment is made within fifteen days of a purchase, the customer is entitled to a prompt payment discount. Depending upon whether the organisation is the customer or the supplier, there may be opportunities for employees to commit fraud in such cases, and the organisation and the supplier/customer may be defrauded. For the monitoring system to be able to detect misfeasor activity, the system needs to be provided with the knowledge of contextual rules relating to the operation. For certain operations, the value entered by the user may determine whether/when the verification of the operation takes place. For example, the loss/profit calculation date may determine when the loss/profit calculation for a business takes place and phoney profits may be generated or verification of losses may be delayed.

Questions have been raised as to why the aforementioned contextual rules are not used as access control for operations, rather than monitoring. There are a number of reasons for this: in some cases the application developers could not have foreseen the contextual requirements; and it is not practical to hard-code contextual rules within the application because the rules may not apply to all business transactions; and the rules may change within a short period as the business practice evolves in order to be competitive.

4. A Generic Misfeasor Monitoring Tool

The following proposes a design for a generic misfeasor monitoring too based upon the requirements discussed above. Deriving from this analysis, the user activities that should be monitored are database access, data replication, data transfer through communication programs, user management, and settings/configuration management of system and applications. The information required to determine possible misuse concerning the described activities will be discussed in detail.

File Access: The application utilised by the user to access the file determines what the user can do with it. In addition, if an arbitrary application is utilised, the user may by pass application level controls embedded within the normal application. Therefore, the monitoring system should be able to determine whether the application utilised is the normal application for accessing the file concerned. For the monitoring system to be able to determine the correct file access, the system needs to be provided with the information regarding the application normally used for accessing the file, and the application utilised by each user for accessing the file. Thus each file listed for misfeasor monitoring needs to be tagged with the identifier of the application normally used for access, so that the monitoring system can compare it against the application utilised by the user for accessing the file, in order to determine possible occurrence of misfeasor activity.

File replication: When a user copy and pastes a file, the monitoring system needs to determine whether the source file is listed for misfeasor monitoring. If the source file is listed then, the system needs to determine whether replicating the entire file is acceptable, or saving the file to a removable disk is acceptable. If replicating the entire file, and/or saving the file to a removable disk are acceptable then no further analysis needs to be made and no one needs to be alerted of the activity. However, if replicating the entire file is not acceptable the monitoring system needs to alert the file custodian of the activity with the details. The details of the event that should be provided are the source file ID, the machine on which the copy is saved, the exact file path of the copy, and the user who performed the activity. Thus each file listed for misfeasor monitoring needs to be tagged with the policy regarding whether replicating to removable disk is acceptable, whether replicating the file is acceptable, and who should be alerted in the event of policy violation.

Partial data replication: When a user performs Print Screen, Cut, or Copy activity when a file is accessed, the monitoring system needs to determine whether the source file from which the data is copied has been listed for misfeasor monitoring. If the source file is listed, then the clipboard data needs to be associated with the source file ID. When the user Paste/Inserts the clipboard data, the file custodian should be alerted the details of the event. The details of the event include source file ID, the user responsible for the activity, file path of the document into which the copied data is pasted, the machine on which the file is saved. The files listed for misfeasor monitoring needs to be tagged with the policy whether partial replication of the contents is acceptable.

File transfer: When a user transfers a file, the monitoring system first needs to determine whether the file is listed for monitoring, and whether saving the file to a removable disk is acceptable. If the file is listed and saving the file to a removable disk is not acceptable the monitoring system needs to determine whether the server mediating the transfer is managed by the organisation, i.e. if it is an internal server. If it is not an internal server the file custodian and the server administrator should be alerted of the activity. If the server is internal the monitoring system needs to determine whether the recipient is also an insider. If the file is transferred through the email application, the recipient's email should be checked against the employee email address list to determine whether the recipient is an insider. If the recipient is not an insider then the file custodian should be alerted. If the recipient is an insider then, the monitoring system needs to determine whether the recipient is authorised to access the file. If the recipient is not authorised to access the source file the file custodian should be alerted with the details. If the recipient is authorised to access the source file the monitoring system needs to determine whether the machine utilised by the recipient to retrieve the file satisfy security requirements, i.e. whether the machine is authorised to access the File server where the source file is located on. If the machine utilised by the recipient to retrieve the file is not authorised to access the server of the source file the system administrator of the server and file custodian should be alerted of the activity along with the details.

The monitoring system also needs to be provided with the list of internal machines for it to determine whether the communication server involved is managed by the organisation. The monitoring system then needs the username/addresses of insiders, so that it can determine whether the recipient's username/address is that of an insider's. The monitoring system then needs to be provided with the role(s) and users allowed to access the file, so that it can determine whether the recipient is authorised to access the file transferred. The monitoring system then needs to determine whether the machine utilised by the recipient for retrieving the file is an internal or external machine. The monitoring system also needs information regarding which machines are allowed to access the server from which the file originated, so that it can determine whether the machine utilised by the recipient is authorised to access the file server.

File Deletion: When a file is to be deleted, the monitoring system should be able to determine whether it is the only copy that exists within the organisation's IT systems. The list of files that need to be monitored is required, and information regarding how many copies of each file exists, where each file is stored, and who is responsible for the security and availability of the file is needed in order to determine possible sabotage, and to inform the right personnel.

User management: When an account is created or a user is added, the added user will gain access to the system, application, file, or records depending upon the list to which the user has been added. If the user is added to the users of a server then they will gain access to the server if the user is added to a role then the user will gain access to the resources given access to the role members. Therefore, the List Custodian should be informed of the addition of users to the list. Thus, the monitoring system first needs to identify to which list the user has been added. Once it has been identified then the custodian of the list should be alerted for verification.

Settings/configuration management: Changing the settings of a system/application may also be a stepping-stone towards a misfeasor activity. When a system is first set up, the required settings for both security and functionality should be defined. When a user activity affects settings/configurations the monitoring system needs to determine whether current/attempted settings of the system/application satisfy the required settings defined when it was first set up. If the current/attempted settings vary from required settings defined by the policy, then the administrator of the system/application should be alerted with the details. The details should include, the affected machine, the affected application, the user responsible, current settings, and required settings stated by the policy. The monitoring system needs to be provided with the required settings for each application installed on each machine, so that analysis can be made to determine whether the changes made by the user conforms to requirements.

Database access: Each user's database access statistics can be monitored on the basis of the number of records accessed per defined period, the number of records accessed per related event/quantity, and comparing the number of records accessed by each user to that of the average accessed by other users belonging to the same role within the organisation. However, the validity of each record accessed by each user should also be verified. When a record is viewed, the monitoring system should be able to determine whether the user had a valid reason to access the record. If a record is added or updated, the monitoring system should be able to determine the integrity of the data within the record. The monitoring system needs to be provided with the list of data tables that require monitoring, and the corresponding data table where the data for reference may be found. The monitoring system also needs to know the attributes that share a common value in both data tables, so that the corresponding reference record may be identified. The monitoring system also needs the information regarding the attributes that need to be verified from the two tables, and the condition of the verification, i.e. check for existence, both values must equal, or a value must be True.

Internet access: Employees may abuse the ability to access the Internet through organisation's IT systems by downloading illegal software, online shopping, and accessing inappropriate content. In order to be able to detect abuse, the monitoring system must be provided with acceptable usage policy. The acceptable usage policy may indicate the acceptable number of bytes downloaded per defined period or per user, the URLs deemed acceptable for access, the acceptable amount of time spent utilising the web browser, and the types of media acceptable for download.

5. Conclusions

Without having relevant data for analysis, the monitoring system will not be able to carry out accurate detection of possible misfeasor activity. The data analysed by current IDS related to network and system level events, and these data may be analysed for detecting network penetrations and privilege escalation attacks. However, the misfeasors do not need to perform network penetrations or privilege escalation attacks in order to gain access to the network and systems. Misfeasors already have legitimate access to network and systems in order to carry out their day-to-day tasks. However, while some of the activities may be perfectly acceptable at network and system level, the activity may be unacceptable within the context of the application and acceptable usage policy defined by the organisation. Therefore, in order to be able to detect violation of contextual rules regarding the application, organisation, or a business process, the monitoring system needs to be provided with the contextual information related to application, organisation, business operations, and acceptable usage policy. Currently, a demonstrator misfeasor monitoring tool is being designed based on the specifications derived from the discussion made in this paper, and developed in order to test the relevance of log data mentioned for the analysis of misfeasor scenarios.

6. 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, J.P. (1980), "Computer Security Threat Monitoring and Surveillance", Technical Report, James P Anderson Co., Fort Washington, April 1980.

Audit Commission. (2005), "ICT Fraud and Abuse 2004 - An Update to yourbusiness@risk", Audit Commission Publications, UK. June 2005

Dhillon, G., Moores, S. (2001), "Computer Crimes: Theorising about the enemy within", Computers & Security, Vol.20, No.8, pp715-723.

Einwechter, N (2002), "Preventing and Detecting Insider Attacks Using IDS", http://www.securityfocus.com/infocus/1558

Escamilla, T. (1998), “Intrusion Detection: Network Security Beyond the Firewall”, John Wiley & Sons, Inc. ISBN 0-471-29000-9, 1998

Furnell, S. (2006), “Malicious or misinformed? Exploring a contributor to the insider threat”, Computer Fraud & Security, September 2006

Gaudin, S. (2000), “Case Study of Insider Sabotage: The Tim Lloyd/Omega Case”, Computer Security Journal, Volume XVI, No.3

Gordon, L.A. Loeb, M.P. Lucyshyn, W. Richardson, R. (2004), “2004 CSI/FBI Computer Crime and Security Survey”, Computer Security Institute, 2004.

Gordon, L.A. Loeb, M.P. Lucyshyn, W. Richardson, R. (2005), “2005 CSI/FBI Computer Crime and Security Survey”, Computer Security Institute, 2005.

Gordon, L.A. Loeb, M.P. Lucyshyn, W. Richardson, R. (2006), “2006 CSI/FBI Computer Crime and Security Survey”, Computer Security Institute, 2006.

Microsoft. (2006), “Survey Finds: Employer may be leaving the door open to internal espionage”, Press Release, Microsoft UK, 30 May 2006.
http://www.microsoft.com/uk/press/content/presscentre/releases/2006/06/PR03635.mspx

Power, R. (2001), “2001 CSI/FBI Computer Crime and Security Survey”, Computer Security Issues & Trends, vol. VII, No.1. Computer Security Institute. Spring 2001.

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.

Schultz 2002, E.E. (2002), “A framework for understanding and predicting insider attacks”, Computers & Security, Vol. 21, No.6, pp.526-531