2008

Can intrusion detection implementation be adapted to end-user capabilities?

Patricia A. Williams
Edith Cowan University

Renji J. Mathew
Edith Cowan University

DOI: 10.4225/75/57b56702b8775
Originally published in the Proceedings of the 6th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 1st to 3rd December 2006.

Can intrusion detection implementation be adapted to end-user capabilities?

Patricia A H Williams
Edith Cowan University,
trish.williams@ecu.edu.au

Renji John Mathew
Edith Cowan University
rmodayil@student.ecu.edu.au

Abstract

In an environment where technical solutions for securing networked systems are commonplace, there still exist problems in implementation of such solutions for home and small business users. One component of this protection is the use of intrusion detection systems. Intrusion detection monitors network traffic for suspicious activity, performs access blocking and alerts the system administrator or user of potential attacks. This paper reviews the basic function of intrusion detection systems and maps them to an existing end-user capability framework. Using this framework, implementation guidance and systematic improvement in implementation of this security measure are defined.

Keywords

Intrusion detection, network security, capability models.

INTRODUCTION

Intrusion Detection System (IDS) is an alarm system for a computer or network. The concept of IDS was first introduced by Anderson in 1980. Anderson identified the reasons for intrusions as: to access information, alter information or render a system unusable. Therefore, intrusion detection is a security measure which monitors network traffic and alerts the system if there is any suspicious activity occurring in the network. Thus, its role in security is to detect, log and raise alarms when intrusion events are detected. Intrusion events can be computer attacks or unauthorised access attempts. IDS is similar to burglar alarm in a vehicle. The vehicle is protected by a lock system and if this lock is broken, it will alert the user by raising an alarm which indicates that someone is trying to steal the car. Intrusion detection systems are often compared with firewall security. A firewall protects an organization from malicious attacks outside the network and an intrusion detection system alerts the administrator if someone passes through the firewall and accesses the network (Innela & Mcmillan, 2001).

An IDS monitors for unusual activity and events based on the set-up policy defined by the organisation. It can perform certain actions to avoid unauthorized entry by blocking the user or source IP address from accessing the network (Sundaram, 1996). Many IDS systems are proprietary, making the setup and configuration of them complex and therefore difficult to an end-user to install and maintain correctly (Whitman, Mattford, & Shackleford, 2006). In this paper, the necessity for such a system is presented together with an overview of the types of IDS available. Subsequently, the key processes involved in IDS configuration and use are discussed. Since IDS is a defensive security measure that is complex to configure and maintain from an end-user perspective, a mapping of these processes to the Security Capability Operational Framework developed by Williams (2008) is proposed.

THE NEED FOR INTRUSION DETECTION

As the complexity of networks increase and access to the unregulated Internet environment, so does the intricacy of network attacks. Thus preventing adverse events becomes increasingly difficult. However, mitigation and deterrence of malicious hacking and unauthorised intrusions can be put into effect by the use of an IDS (Rosenthal, 2002). As such, an IDS is a constituent part of a total security solution and not a total solution in itself. However, it is essential for protecting an organization from unauthorized users and should be a part of every comprehensive security solution because it detects vulnerabilities in the network and alerts the administrator to the possibility of an attack. When an attack pattern is detected and the administrator advised, it is vital to include new rules for the IDS and distribute them (Lear, 2000). Consequently, extensible IDS can help to install these new rules quicker to all machines without having to reinstall the rules onto each system. Furether, there is a need for proper use and maintenance of IDS to ensure they do not negatively impact security over time (Adams, 1996). When an IDS detects a potentially adverse event it sends out alerts and logs activity. However,

whilst an IDS allows for supervision of a network, it still requires appropriate implementation and maintenance. IDS technology cannot be effective and operate at an optimum level if implemented haphazardly. To date this implementation by end-users has been undertaken poorly (Northcutt & Novak, 2002; Rosenthal, 2002). To understand why this is an issue, it is first necessary to appreciate how an IDS functions.

IDS TECHNOLOGY

IDS consist of two components namely a management console and sensors. The management console is the reporting console for when an attack occurs, and the sensors are agents that detect and monitor the hosts in a network (SANS, 2008). In essence, IDS works by maintaining a database of attack signatures which have been obtained from previous malicious activity. These attack signatures are matched with the potentially malicious packets that are detected.

IDS Types

There are two types of intrusion detection system namely, host based intrusion detection and network based intrusion detection system (Innela & Mcmillan, 2001).

Host-based intrusion detection system

Host-based intrusion detection works by collecting information from individual computers by detecting and monitoring the activities of an attack on an operating system by collecting data from the host computer. Host-based detection only monitors inbound and outbound packets from the system device. They use two sources of information obtained from operating system audit trails and system logs. Operating system audit trails are obtained from the kernel of the operating system and system logs give a description about the system activities on the network.

Network-based intrusion detection system

Network-based of intrusion detection systems work by analysing and capturing the packets in a network. This type of IDS monitors traffic patterns and alert the system administrator about potential malicious activity (Innela & Mcmillan, 2001). The sensors used in this type of IDS usually run in ‘stealth mode’, hiding their presence and avoiding discovery of their presence by attackers. Network intrusion detection system monitors all the inbound and outbound packets to and from the devices in the network.

Detection Approaches.

Within these types of IDS, two approaches can be adopted for analysing malicious activities to detect attacks. There are advantages and disadvantages for both the approaches but the most commonly used method is signature based intrusion system (Bradley, 2008).

Signature Based

Signature-based IDS work by monitoring packets in the network and comparing them with pre-defined attack signatures in a database. The signature detection records each pattern of events as a separate attack signature. They are used for detecting attacks whilst minimizing the number of false alarms (Bradley, 2008). Signature based detection system also help security managers to track security problems in their systems. Therefore, signature based intrusion detection system detects malware the same way as antivirus software’s detect viruses and worms.

Anomaly Based

Anomaly-based IDS work by analysing any unusual behaviour of the host in the network. The traffic patterns for a normal activity are different from the patterns of an attack. The anomaly-based category of IDS monitors the traffic and compares it with a known baseline. The baseline provides information about vectors such as the bandwidth, protocols used, ports and devices that connect with each system.

Regardless of the type of IDS employed, standard key processes can be identified for the standard functions of IDS.

KEY IDS PROCESSES

In investigating existing IDS standards, such as NIST and Standards Australia, a number of common key processes have been identified (Saiglobal, 2004; Scarfone& Mell, 2007). These processes can be included in the deployment of an efficient intrusion detection system, as shown in the process model in Figure 1.

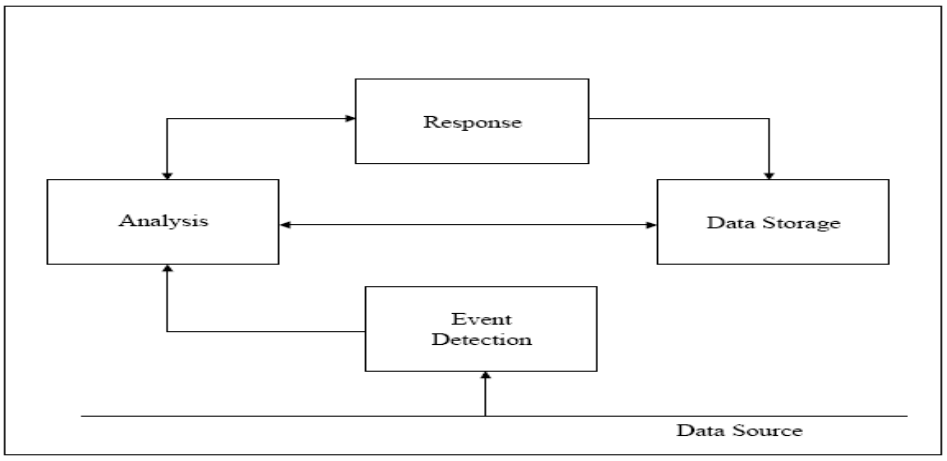

Figure 1: Process model for efficient intrusion detection systems (Saiglobal, 2004).

The IDS process model (Figure 1) is underpinned by the data sources it has access to. The data sources are important because this data is used to detect intrusions into the network. These data sources can be obtained from different levels of the system. Some of the data sources from which intrusions can be found are (Bace & Mell, 2007):

- Auditing the system resources by checking the audit log file of the operating system which includes system events and activities. Some of the information such as file access and method of access attempts may also be useful.
- Recording some of the information such as system parameters, memory use and network connections are useful for detecting intrusions.
- Network management logs give information about device status and transition.

In order to implement, and more importantly maintain, an effective IDS it is necessary to identify and describe the key processes involved. Ten key processes are described here.

1. **Activity monitoring and automation.** This is the process for monitoring all user and system activities in a network. The system and network configuration are checked for any intrusions. The main two tasks of active monitoring are to detect system and network intrusions, and to detect abnormal attack patterns and user policy violations (White, 2003). The main purpose of activity monitoring is to alert the administrator of the problems caused by crashed servers, overload, malware infection and failed connections.

2. **Configuration check.** This check is done to identify the system and network configuration. It checks whether the systems and network have any detectable vulnerabilities. Configuration checking also looks for hosts that do not belong to the network. All machines in the network should be checked periodically for malware attack. There are also different types of sniffing tools that can be used in this configuration checking process.

3. **File authorizations.** File authorization checking identifies file, user and group authorizations modifications. One possible attack vector is to modify the user and group authorization allowing various attacks on the network. One way of checking the file settings is to place an expected file setting outside the network and then comparing it with the original file settings.

4. **Log file examination.** Log files record actions and events that take place on a network. Log files can be obtained from various devices such as servers and routers. They are mainly used for checking who has accessed the network and at what time and from which location.

5. **Packet sniffer check.** A packet sniffer, often referred to as a network monitor or analyser, can be used to detect and troubleshoot network traffic. By analysing the captured packets and identifying the malicious packets, the administrator can use this information for protecting the network (Bradley, 2008). A packet capture usually captures all the packets passing through the network interface. There are various ways to undertake this, either by capturing packets to the machine only or capturing all the

packets in promiscuous mode. The issue with promiscuous mode is that any intruder can also capture and analyse traffic.

6. **Password files check.** Password file checking is done periodically to ensure users change passwords regularly, since unauthorized users try to obtain the passwords and usernames for creating accounts. If new unauthorised accounts are detected, the accounts should be deleted from the system password file together with all compromised files. Passwords should be checked and changed frequently by the system administrator.

7. **Services check.** These checks are done to identify any unnecessary services running on the operating system. Many services may create backdoors for hackers to exploit the vulnerabilities in the system (Saiglobal, 2004). A service check is done to identify these services and remove the services that are not needed.

8. **File integrity assessment.** The file integrity assessment is important to determine if a file has been tampered with. Usually such assessments methods can be done manually, however utilising an automated detection method will increase reliability and therefore effectiveness (Saiglobal, 2004). Automated IDS is an effective and efficient method of performing statistical analysis and integrity checking.

9. **Response.** Response is the action that a system takes when detecting intrusions on a network. It is most usefully employed when presenting the event analysis results using a graphical user interface. There are several methods to alert administrators of events such as via email or pagers (Saiglobal, 2004). A system administrator can then ascertain the severity of the response and make decisions on the most appropriate countermeasures. In some IDS, the reaction-response is also able to perform preventive actions such as locking the account that was attacked and therefore reducing additional potential damage to the system.

10. **Data storage.** Data storage is required for storing all detected activities, audit logs and other relevant information in a database. This database will contain collection of attacks, unusual behaviour patterns and other attacks that can be used for future detection of intrusions. It can also store the detected malicious activity for subsequent use as evidence.

These key processes can be used to delineate specific activities for end-user maintenance of their IDS. One method to make this accessible and understandable to the end-user is to map these processes to a capability operational framework. One such framework to enable mapping of security activities to end-user capabilities is the adapted CMM Operation Framework (Williams, 2008).

CAPABILITY MATURITY MODEL (CMM) OPERATIONAL FRAMEWORK

A capability maturity model (CMM) is a methodology founded in 1986 by Software Engineering Institute (SEI) at Carnegie Mellon University to develop organizational software development processes. The main purpose of this model is to guide and help organizations to develop and maintain their key process areas. This model has been modified and developed by many companies to improve their capability in key management areas. One of the important factors to be considered for CMM is using the knowledge of the maturity levels and identifying the differences between mature and immature organizational processes.

CMM provides five distinct levels for measuring the maturity of the development of processes. These maturity levels help in providing a well-defined, proper path for achieving improved processes. In this case we are looking at improving the implementation and maintenance processes of intrusion detection systems. The different levels are defined in Table 1.

Table 1. The capability operational framework, maturity levels description (Carnegie Mellon University, 2003).

Level	Heading	Description
1	Initial	Procedures are performed in an *ad hoc* manner
2	Repeatable	Procedures are tracked and follow a regular pattern
3	Defined	Procedures documented and communicated
4	Managed	Procedures monitored and measured
5	Optimized	Best Practice procedures followed and automated

The CMM operation framework (Figure 2) maps specific activities into definable levels of capability. The levels are defined to allow both assessment of the current level of capability and to identify how improvement to a higher level cane attained. Using this model, specific activities can be deconstructed into manageable segments to make them understandable and implemented by the end-user.

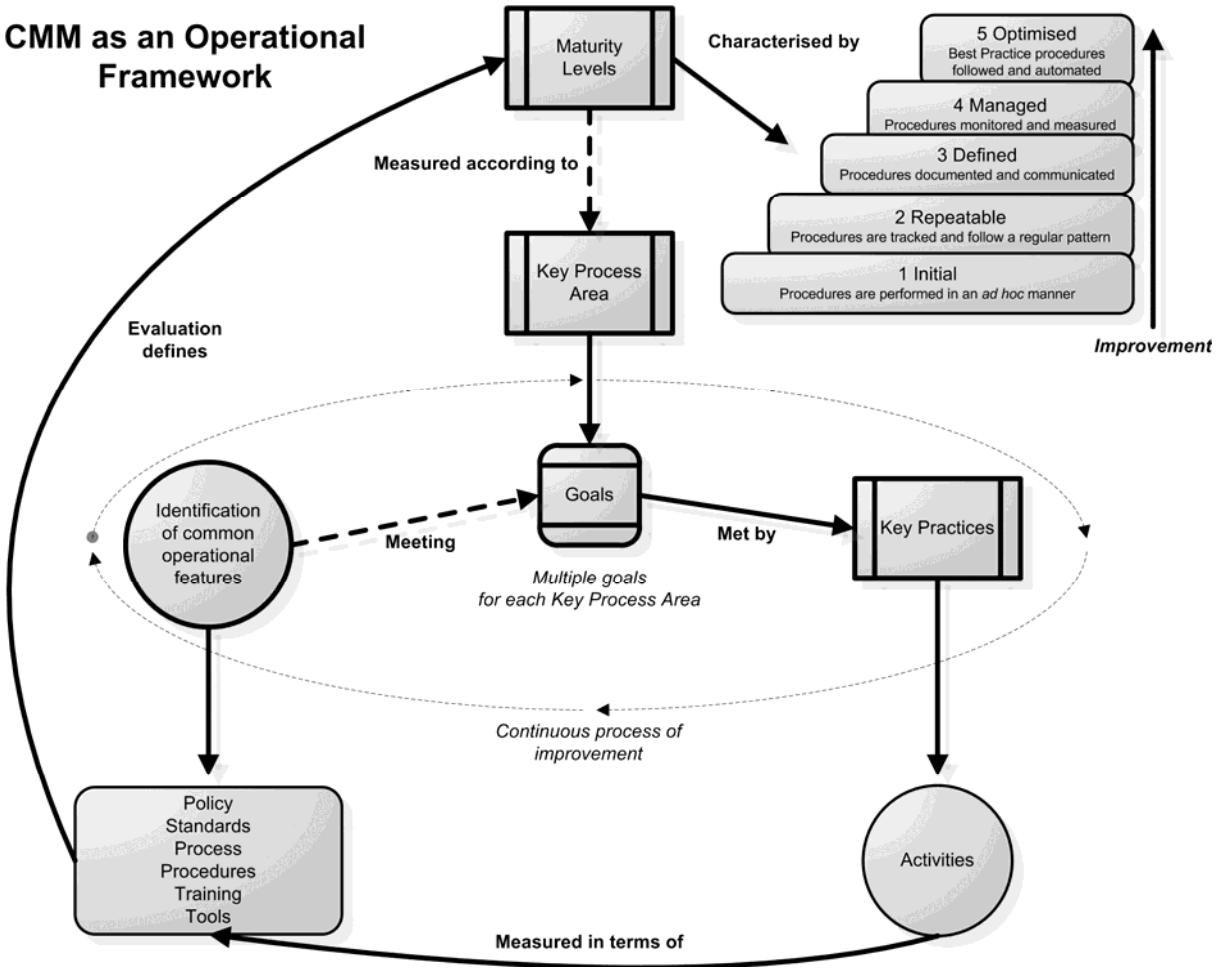

Figure 2. An apapted Capability Maturity Model (CMM) operational framework for mapping security activities to capability (Williams, 2008).

The results below show how a mapping of IDS key processes can be translated into this oprtational framework.

RESULTS

Using the key processes for IDS identified by the standards (as discussed above), a mapping was created to elucidate on the activities involved and the capability level these can be attributed to (Table 2). Each key process listed above was deconstructed into its constituent activities and defined at increasing levels of effectiveness. These constituent activities are placed in the table against one of the five defined levels of capability where assessment of complexity of the activity is matched to the capability levels 1-5 (Table 1).

The construction of the table and allocation of each activity at each level is an informed but somewhat arbitrary process. However it does enable clear identification of each task for each process. Key processes at level 1 are either non-existent or of limited implementation. Similarly, those at level 5 are well developed, mostly automated and reflect best practice. For instance, the key process of ‘configuration checking’ is not undertaken at level 1 and is automated using scanning tools at level 5. The mapping in Table 2 also indicates the support required and the tools available for deploying an IDS. It should be noted that whilst ‘policy’ is not listed as a key process, “security policies and procedures go hand-in-hand with technological countermeasure such as firewalls and intrusion detection systems (IDSs), towards leveraging the organization’s security posture, mitigating risk, and maintaining financial and competitive viability” (Rosenthal, 2002).

Table 2: IDS key process mapping to CMM operational framework capability levels.

Intrusion detection system key processes		Level 1(Initial)	Level 2(repeatable)	Level 3(defined)	Level 4(managed)	Level 5(optimized)
IDS Policy		Does not exist	Verbal	Written	Written for packet sniffer, monitoring and response.	Policy is written for monitoring, packet sniffer, response and backup storage.
Policy communication		Not communicated	verbally communicated	Written and provided to some staff	Policy in written form; training provided for some staff	Policy is communicated to all employees and training provided
Activity monitoring and automation		Monitoring does not take place	Manual monitoring of some system activities	Manual monitoring of all the system activities	Automated monitoring for user, system and policy violations	Automated monitoring of abnormal attack patterns on the system and all user activities and policies.
Configuration check		No configuration check takes place	Manual checking of some system vulnerabilities monthly	Periodic automated check of some system and network vulnerabilities	Periodic automated check of all systems and networks	Automated configuration checking of each system and networks daily using port scanning tools
File authorization check		No manual checking of files done	Manually file checking takes place for user authorization	File authorization takes place automatically to check tampering of user data periodically	File authorization takes place automatically to check tampering of user and group authorization periodically	Automatic file authorization check for tampering for user and group authorization daily and maintain file access settings for comparing with the current settings to detect any modification.
Log file examination		Log file examination not done	Manually basic security log files are examined	Automatically log files are examined for router periodically	Automatically log files are examined for router and server periodically	All the log files for router, server, process and other security logs are examined automatically per day
Packet sniffer check		Sniffing tools are not monitored	Manually analyse packets	Monitoring the system and its configuration for packet sniffer.	Automated system and network done for monitoring sniffing tools	Automated system and network checking is done for identifying unauthorized sniffing tool, packet analysis is done for detecting malicious activities.
Password files check		Password file not checked	Passwords files checked for unauthorized accounts only	Automated checking of accounts deletion of user accounts not required.	Automated deletion of all unauthorized accounts and other files with change of passwords periodically	Automated deletion of all unauthorized accounts and files that are compromised from the systems password file on a regular basis. The system passwords are changed regularly.
Services check		No unwanted services are checked.	Manually uninstalling all the unwanted services installed.	Automated checking of some unwanted services done periodically	Automated checking of all services weekly.	Automated checking of all the unwanted services installed in the operating system. The service files are analyzed for intrusion and unnecessary files are removed by users.
File integrity assessment		Integrity of file not checked	Integrity of file checked monthly	Integrity of file checked weekly	Integrity of file checked daily	Integrity of file checked daily and countermeasures taken for it.
Response		Response detected without any measures.	Response send to management console only	Response is send to management console and administrator	Response is send to senior administrator giving a graphical user interface of events detected.	Response is send to specified senior administrator by email, pager etc, management console and preventive measures taken.
Backup storage		Storage is done near the system	Near the locker onsite	Backup data taken home by staff and returned	Backup data is taken offsite and stored	Backup data is taken offsite and multiple copies are made
Backup data security access		Only employees	Specified employees	Specified administrator assigned.	Senior staff and administrator	Senior administrator and manager.
Training		Training not provided	Intrusion detection procedures are included	Intrusion detection and training provided for newcomers	Understanding all the basic Intrusions detection methods, initial training and disaster recovery plan,	Full training provided on various sections of intrusion detection, disaster recovery plan implemented, proper induction for all the newcomers.
TOOLS	**Support**	Support is not available	Ad hoc is supported	Support is available	Support is contracted and available	In house contract and support available
	Software					Airdefense or similar used

DISCUSSION

Table 2 demonstrates how intrusion detection implementation can be clarified into manageable steps using the capability operational framework and matched to the end-users' capabilities. The application of the activity mapping in Table 2 can be used for two activities. Firstly to assess the current level of security capability in the use of IDS and secondly to identify potential improvements in security practice. The table could be enhanced when applied to a specific end-user profession by identifying the legal and ethical requirements of that profession in relation to IDS implementation. In this case, correlation of professional and legal requirements with the defined levels of capability would be undertaken. Using the mapping, the current level of capability of the end-user can be assessed and improvement is based upon this starting point.

Table 2 provides information to the user about the CMM operational maturity levels which can be achieved and how to achieve them. The levels are defined as increasing in complexity and effectiveness in terms of IDS implementation and maintenance. For instance, the initial level to the optimized level gives a new user who is not skilled in intrusion detection system to develop and maintain it. The process of intrusion detection system can improve depending upon each level. The initial level shows that all the processes are in ad hoc manner and the optimized level indicates the best practice. Best practice (level 5) is the ultimate target for every implementation of IDS. Most of the processes can be done manually or automated. Automated processes work quicker and are more efficient than manually performing tasks.

The limitations of the framework mapping need to be considered as do the limitations of the IDS technology itself. IDS is only part of the security management solution and thus taking this framework mapping in isolation to other security will not result in effective security. However, the mapping of an activity using the CMM operational framework provides a straightforward representation of the essential processes for IDS implementation and maintenance. Further, it creates a structure for improvement based on small defines steps where improvement in security can be incremental. This is important in the application of security measures which are complex and difficult for the end-user to put into practice.

CONCLUSION

Intrusion detection systems have been widely accepted as an essential security measure as part of a total security solution. They are an important component because IDS helps identify threats to a network by comparison to known signatures. Further, it is important that all component processes of effective IDS use are implemented correctly. The automated monitoring which IDS provides can greatly assist organisations in their security efforts by logging events, gathering information about network activity, detecting potential unauthorised intrusions and attacks, preventing actions using blocking and alerting the systems administrator of potential adverse intrusion events.

The IDS capability mapping (Table 2) presented is being used in current research to assess the capability of end-users in security implementation in the primary care medical field. Whilst the IDS security activity defined in this paper provides guidance for improvement in security practices, expansion of the mapping table would be required to identify potential accreditation to national and international standards for IDS security. Further, for application in specific professional area, correlation of professional endorsement standards related to IDS should be added to the CMM operation framework table of activities. This would provide an uncomplicated method for assessment of current IDS capability for the end-user and provide evidence of best practice for accreditation purposes.

REFERENCES

Adams, D. G. (1996, 2-4 Oct. 1996). *Operational tips for improving intrusion detection system performance.* Paper presented at the Security Technology, 1996. 30th Annual 1996 International Carnahan Conference, Lexington, KY.

Bace, R., & Mell, P. (2007). *NIST Special Publication on Intrusion Detection System*. Retrieved May 8, 2008 from http://www.21cfrpart11.com/files/library/reg_guid_docs/nist_intrusiondetectionsys.pdf.

Bradley, T. (2008). *Introduction to Packet Sniffing.* Retrieved May 2, 2008 from http://netsecurity.about.com/cs/hackertools/a/aa121403.htm.

Carnegie Mellon University. (2003). *Systems Security Engineering Capability Maturity Model (SSE-CMM): Model Description Document Version 3.0*. Retrieved October 1, 2005, from http://www.sse-cmm.org/docs/ssecmmv3final.pdf.

Innela, P., & Mcmillan, O. (2001). *An introduction to Intrusion detection system*. Retrieved May 10, 2008 from http://www.securityfocus.com/infocus/1520.

Lear, A. (2000). *Axent's Rob Clyde. Why you need intrusion detection system*. Retrieved May 10, 2008 from IEEEXplore database.
Northcutt, S., & Novak, J. (2002). *Network intrusion detection* (3rd Ed.). Indianapolis, Indiana: New Riders.
Rosenthal, D. A. (2002). Intrusion detection technology: leveraging the organization's security posture. *Information Systems Management* (Winter), 35-44.
Saiglobal (2004). *AS ISO/IEC 15947-2004. Information Technology-security techniques- IT intrusion detection framework*. Retrieved May 10, 2008 from http://www.saiglobal.com/shop/script/Details.asp.
SANS. (2008). Intrusion Detection Framework. Retrieved 2008, 16 March, from http://www.sans.org/resources/idfaq/.
Scarfone, K. & Mell, P. (2007). *NIST Guide to intrusion detection and prevention systems (IDPS) SP800-94.* Retrieved May 13, 2008 from http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf.
Sundaram (1996). *An Introduction to Intrusion Detection*. Retrieved May 10, 2008 from http://www.acm.org/crossroads/xrds2-4/intrus.html.
White, D. (2003). *What is Network Monitoring?* Retrieved May 8, 2008 from http://www.wisegeek.com/what-is-network-monitoring.htm.
Whitman, M. E., Mattford, H. J., & Shackleford, D. M. (2006). *Hands-on Information Security Lab Manual*. Australia: Thompson Course Technology.
Williams, P. A. H. (2008). A practical application of CMM to medical security capability. *Information Management & Computer Security, 16*(1), 58-73.