Response Mechanisms for Intrusion Response Systems (IRSs)

N.B.Anuar, S.M.Furnell, M.Papadaki and N.L.Clarke

Centre for Security, Communications and Network Research (CSCAN),
University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

The rise of network attacks and incidents need additional and distinct methods of response. This paper discusses the different type of responses in Intrusion Detection Systems (IDSs), Intrusion Prevention Systems (IPSs) and Intrusion Response Systems (IRSs). Using characteristics of responses and the relationship between responses, a more effective model is proposed. The characteristics of responses include the level of operations, the speed and time of responses, the ability to learn and the ability to cooperate with other devices. Using an attack time frame, the relationship between active and passive response are discussed. The response mechanism model distinguishes between active, passive, and different approaches and stages of active responses.

Keywords

Intrusion Response Systems, active, proactive, reactive and passive response

1. Introduction

In recent years, statistics have shown that there are a growing number of intrusion cases reported to the Malaysian Computer Emergency Response Team (MyCERT) (MyCERT, 2008). The latest 6 month report for 2009 indicated a 100% increment on the cases reported to the MyCERT. Moreover, Schouwenberg (2008), a senior anti-virus researcher from Kaspersky Lab BNL, reported about attacks to financial institutions. He described about the possible attacks, overview of the current attack methods and detailed attack trend statistics for financial institutions. Schouwenberg's report shows that the financial institutions are also open to intrusion problems and pointed out that the problem is unavoidable. Also, the Washington News revealed that a part of a $5.4 million contract was repaid to the Pentagon from a security company, Apptis Inc., after the company failed to provide adequate computer security services (Capaccio, 2009). The high cost of the contract indicates the serious financial committed made by the Pentagon to prevent and secure their infrastructure from being attacked from other country.

From those examples, it can be seen that the vulnerability from attackers is unavoidable. Since the problem is unavoidable and in conjunction with the continuation of attacks and intrusion problem, computer security scientists and

researchers are now continuously searching for the better and safer methods to prevent, minimize and overcome the dilemma.

Since Anderson's (1980) research in Intrusion Detection Systems (IDSs) and strengthened by the model and discovery by Denning (1987) and Denning and Newman (1985), researchers have been actively looking for the best method to make sure IDSs perform better and more efficiently.

To date, studies have shown that there are hundreds of published works related to IDSs, IPSs and IRSs (Sherif, Ayers and Dearmond, 2003; Sherif and Dearmond, 2002). Presumably, as a result of these studies, the process of detection, prevention and response could be advanced in order to increase the level of efficiency and reliability. Whilst IDS technologies have advanced there are still areas to explore, particularly with respect to the need to improve and enhance the response method.

However, there are still many limitations in the existing IDSs research. These limitations include: the problem of identifying false alarms (Tjhai et al., 2008), defining which asset is critical to be secured (Huiying and Yuanda, 2008), selecting which threat needs to be urgently neutralized (Zhi-tang et al., 2007), which incident needs investigation or which incident needs to be prioritized (Dondo, 2008) and so forth. In this particular context, the term incident refers to a cyber attack and normally starts when something suspicious is detected (Hacking-Lexicon, 2009).

This paper discusses the multiple types of responses in intrusion detection, prevention and response systems. In addition, using an attack time frame, a response model is proposed to distinguish between active and passive zone.

This paper is divided into five sections. The second section discusses the concept of intrusion detection, prevention and response systems. Using examples from published literature and the concept of active and passive responses, the movement from traditional IDSs to modern IRSs with multiple types of responses are discussed. The third part of this paper describes the proposed response model. Using the attack time frame, the active and passive zones are classified and new definitions of active and passive responses are proposed. In addition, the forth part of this paper describes a small survey and study conducted with an objective of presenting evidence that there are multiple types of responses applied in the existing commercial and research products. Final section discusses the future direction in enhancing IRSs.

2. Detection, Prevention and Response System

Before discussing the multiple types of response it is important to define the term Intrusion Detection System (IDS), Intrusion Response System (IRS) and Intrusion Prevention System (IPS). Currently, the distinctions and differences between these terminologies are still vague. In terms of response, all response mechanism in IPSs, IDSs, and IRSs use the same approach. For example, IDSs which perform an automatic active response could sometimes also be addressed as IPSs and using automatic reactive response IRSs also perform the similar responses.

The distinction between these three systems is still unclear. However, in order to create distinctions between them, the simple basic terminologies for the systems can be described as follows:

a) An Intrusion Detection System is a system which is able to perform an intrusion detection process and traditionally may produce a simple warning and alarm when the intrusion is detected. Ultimately, the main goal of IDS is to detect the unauthorized use, misuse and abuse of computer systems by both system insiders and external intruders (Aickelin et al., 2003). The final goal for IDSs is to assist system administrators to estimate the state of system and suggest an appropriate response (Zhang, Ho and He, 2009). In the early days, IDS responses would only produce a passive response such as producing a log or notifying an administrator about suspicious activity. Moreover, the early stages of research in IDS are mainly focussed upon research in enhancing the detection processes rather than the response process (Sherif, Ayers and Dearmond, 2003).

b) Intrusion Prevention Systems share similarities with IDSs in terms of system deployment and the detection method, but perform an additional response by blocking potential intrusion or terminating network traffic for the current intrusion. Therefore they can be considered as an extension to the traditional IDS. Normally, in order to block malicious traffic, an IPS is positioned in-line with the networks and conceptually is deployed together with firewalls or access control appliances (Papadaki and Furnell, 2004). Perhaps similar to proactive response in IRSs, the only unique characteristic for IPS is its non collaboration with other security appliances.

c) An Intrusion Response System performs a similar function like an IDS and IPS by maintaining several approaches to detection and response, but use in addition multi types of responses with further analysis to minimize incident impacts. Unlike IDSs and IPSs, IRSs offer additional functions and exhibit multiple characteristics of response to mitigate intrusion impacts. Not just a passive response, IRSs concentrate on response functions by showing characteristics such as proactive and reactive responses. In addition, with the variety of characteristics, IRSs are able to initiate collaboration between other security appliances, such as working with firewalls to block and terminate suspicious traffic, working with honeypots to collect attackers' information and trace attackers sources (Wang et al., 2001), and redirect connections for other precautions (Yue and Cakanyildirim, 2007).

Without differentiating the aforementioned terminologies between IRSs, IDSs and IPSs, from literature, the response mechanism for all these types of systems are the same. Using different perspectives of response taxonomy, both the IDSs taxonomy and IRSs taxonomy (Stakhanova, Basu and Wong, 2007; Fisch, 1996; Debar, Dacier and Wespi, 1999; Wang et al., 2006; Axelsson, 2000) can be clearly divided into two main types; active and passive responses.

An active response refers to a response which is used to counter an incident in order to minimize a vulnerabilities impact to victims (Papadaki et al., 2002). Yue and Cakanyildirim (2007) described proactive response and reactive response as something related to active response. Particularly, for proactive response, which refers to an action that can only be taken if there is a trusted decision made by IDS itself and in special cases the action can be taken immediately. In this case an active response can be referred to as an immediate response (Yue and Cakanyildirim, 2007) and for some other case the response taken is automatic and fast (Lewandowski et al., 2001). In addition, some adaptive, learning, and intelligent methods are involved in this type of action (Ragsdale et al., 2000).

Active responses sometimes produce worst results if the response systems are not configured correctly. For example, an active response can generate Denial of Service attacks to the networks itself. In order to avoid this, the system must be configured confidently so that it responds with confidence. The overconfidence is one of the problems discussed in the decision making and is known as a decision trap (Russo and Schoemaker, 1989). In addition, an active response must have the capacity to engage a corrective response such as updating system patches automatically, logging off a user, reconfiguring firewall or disconnecting a port (Jackson, 1999).

Based on different characteristics such as the level of operations, speed and time of response, ability to learn, and ability to cooperate with other devices, active responses can be divided into two main categories; proactive and reactive response. Proactive response is an approach that controls a potential incident activity before it happens rather than waiting to respond after the incident has happen. Fundamentally, the proactive response approach prevents a predicted intrusion incident based on analysis, investigation, reasoning and scientific methods. For example, a probability measurement is used to value the possibility of an attack happening (Stakhanova, Basu and Wong, 2007). In addition, a proactive response approach can predict a new intrusion and confidently know the method of how to prevent the intrusion from spreading fast.

Cabrera et al. (2002) described two main characteristics in proactive responses such as temporal rules and the reporting of incoming danger. Therefore, proactive responses can be reconstructed into two different approaches:

i. Using a prediction method by producing an early response to an information security administrator or intelligent agent system, and at the same time able to minimize potential intrusion impacts in the future. This approach can use any machine learning approaches either supervised or unsupervised (Kotsiantis, 2007). At least, one solution proposed by Schultz (2002) showed the capabilities of predicting a new attack and this technique perhaps can be extended to be used as input for future response models.

ii. Using a case-based reasoning method to pre-empt incidents based on historical data. For example, any incident detected in real time is stored and later can be used as an input for future responses. Similar to the case-based reasoning approach used in an IDS (Esmaili et al., 1996), but for proactive

response, any previous incident response will be used as a reference point in order to prevent a future similar intrusion. In extension, COBRA (Gangadharan and Kai, 2001), RedAlert (Anuar, Yaacob and Idna, 2004) and ADEPTS (Wu et al., 2007; Foo et al., 2005) provide a proactive response in order to minimize the intrusion impact on other neighbouring systems. Similarly to COBRA and RedAlert, a recent research by Thames, Abler and Keeling (2008a; 2008b) uses proactive response by updating and reconfiguring the firewall dynamically and periodically.

The second category for active response is reactive response. Fundamentally, there is no clear definition on reactive response but it accepted as an approach where the system is maintained in a real-time interaction environment or by using human experts with automated tools to assist in finding the best responses (Fessi et al., 2007).

With similar objectives to proactive response, reactive response is a subset of active response that reports any incident detected directly to information security analyst or a response action is taken immediately or in real-time. Reactive response reacts only after the intrusion is detected. Therefore, it is suggested that there are two stages of responding in a reactive response situation; the first stage involves confident responses after an incident is detected, and the second stage, involves investigating and learning about the uncertain incident before further responses can be applied.

The first stage of response acts only after an incident is detected and aims at least to reduce incident impacts. This first stage of reactive response is still considered within the active zone, a transition between proactive and reactive. The only difference between this stage and the proactive response is this response responds to the incident confidently after the incident is detected. For example, an automated response system using an automated system can be considered as a reactive response. Cooperating Security Managers (CSM) proposed by White (1996), proactively detect intrusions but reactively responding to the incident (Wu et al., 2007). In addition, the response at this stage collaborates with other security appliances such as firewall in order to reduce incident impacts (Hong et al., 2006).

The second stage of reactive response applies to incidents with high uncertainty where the incident will be investigated and the behaviour of the incident will be learned before a further response can be applied. The concept is fundamentally proposed by Yue and Cakanyildirim (2007) who suggest that reactive response is defined as a response of sending alarms to the security analyst. At this stage, unlike the first stage, to reduce uncertainty on incident, the response is not taken immediately but waits for the incident to be investigated, such as, tracing the incident (Chen et al., 2006) or using a honeypot (Feng et al., 2003) to collect additional incident data for investigation purposes. This stage is a bit similar to the passive stage, where there is no action taken to minimize intrusion but only provides incident feedback to minimize intrusion impact. However, literature generally states that responses in this stage are categorised as an active response (Wang, Reeves and Wu, 2001; Jang and Kim, 2002; Feng et al., 2003; Chen et al., 2006; Stakhanova, Basu and Wong, 2007).

Finally, a passive response normally aims to notify other parties about the occurrence of an incident and relies on the information security administrator to take further action (Papadaki et al., 2002). This type of response is one of the earlier responses introduced in IDSs and is therefore vulnerable and exposed to the disadvantage where the action produced sometimes gives an advantage to attackers. The case study which explains the disadvantage is clearly explained by Cohen (1999). For certain cases, ignoring incident is also one of the examples for passive response (Yu and Rubo, 2008).

3. Response Mechanism Model for Intrusion Response Systems

In a broader context of Intrusion Response Systems (IRSs), the system is actually a part of an IDS. Whilst IDSs perform the process of detection, IRSs perform an additional type of response. In order to propose a model for response mechanism for IRSs, the relationships between passive, reactive and proactive responses using attack time frame are depicted in Figure 1 below.

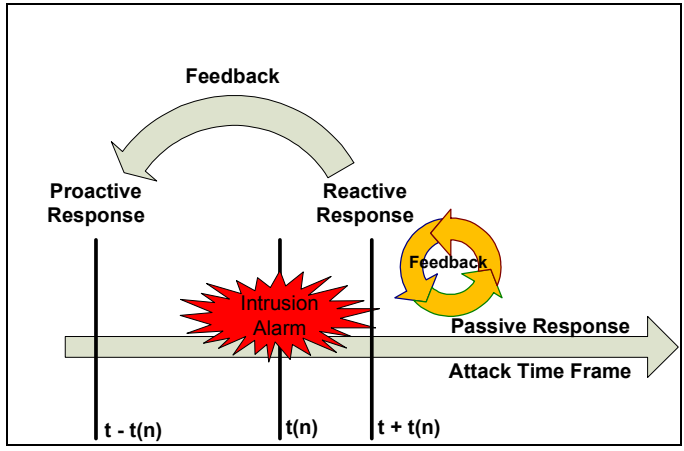

Figure 1: Relationship between passive, proactive and reactive responses using attack time frame

Figure 1 shows the relationship between passive, proactive and reactive response in line with the attack time frame. The relationship between responses is made based on the attack time frame and contains three main lines t-t(n), t(n) and t+t(n).

Figure 1 shows a typical time line for attack time frame where t(n) is denoted as a reference point of an intrusion alarm produced by the IDS. The intrusion alarm can be a false alarm, an uncertain alarm or a true alarm. Since t(n) denote the reference point for an incident, the attack time frame produces another two stages; (i) before intrusion alarm, t – t(n) and (ii) after intrusion alarm, in between t(n) and t + t(n). In addition to the two stages, there is another stage of the attack time frame, after t + t(n), which refers to a stage after a reactive response.

With a total of three stages, the attack time frame is appropriate to describe a new response mechanism particularly for Intrusion Response Systems. The attack time

frame starts from stage t – t(n), where, at this stage before an incident is detected by an IDS, t(n). In this stage, the proactive response plays a big role in defending hosts and networks from being attacked. In this stage, before any intrusion is detected, a precaution action such as blocking any predicted potential incident and adjusting system configuration are some examples that can be taken. Based on the aforementioned two approaches on proactive response, this stage provides two critical response actions; (i) prevent any future potential incident based on prediction analysis and (ii) prevent attack for current and future potential attack based on incident feedback from passive and active response.

In the second stage, between t(n) and t + t(n), a reactive action contributes a more significant response to minimize incident impact. In this stage, countermeasures like terminating the user, process or network traffic that has direct influence with the attacker is taken but only for an intrusion with a high level of confidence. At the same time, some collaboration between other security appliances by limiting the user, process and or network traffic can be another example. If there is a 24x7 information security administrator present at the time of an incident detected, an immediate manual response by changing the security configuration is a crucial activity. However, since this is a critical stage, all processes can only be taken if the confidence level of the incident is very high. This stage ends immediately at the line of t + t(n), and if any incident cannot be solved at this stage, the escalation process will be sent to the next stage, which is the second stage of the reactive response.

Unlike the previous two stages, the last stage after t + t(n) is an investigation phase. The stage is a continuous stage with no ending line for this stage; hence this stage is suitable for a non critical system. This stage uses the second stage of a reactive response by waiting, investigating and learning about incidents that occur before a further response can be applied. This stage is quite similar to the passive stage and previous research has categorized the responses as an active response.

In addition at stage t + t(n), some incident feedback can be collected from passive responses. The responses will be combined with the current stage and act as an input for reactive and proactive responses. Furthermore, the feedback cycle between reactive and passive responses provide a bidirectional feedback from each other; therefore both responses communicate continuously in order to provide better investigation and analysis on any incident.

In conclusion, the definition above clearly indicates that response model for IRSs can be divided into two main response zones; active and passive zones with additional four different stages in active responses (i) two approaches of proactive responses, and (ii) two stages of reactive responses.

4. Product Comparison

In continuation with the definition on the responses model, a simple comparison study is conducted. The objective of the study is to show evidence that there are multiple types of response applied in the commercial and research products. The study involves 27 samples of commercial and non-commercial products. The study

compares between multiple ranges of IDSs which apply multiple types of response mechanisms. The study categorizes active and passive responses into multiple and different types. Figure 2 lists all related products considered in the study.

McAfee IntruShield, Snort IDS, Cisco IDS, Bro IDS, FlowMatrix, IBM Proventia Network IPS Series, Prelude Hybrid, DefensePro (APSolute Immunity), StoneFate IPS, TippingPoint, SecureNet IDS/IPS, Security Metrics, iPolicy, Juniper IDP, Strata Guard (StillGuard), DeepNines IPS, netfence sintegra, Proventia Desktop, CA-Host Based IPS, PHPIDS, SAMHAIN, Symantec Critical System Protection, Osiris, McAfee Host Intrusion Prevention for desktops, Untangle, Dragon Intrusion Prevention, OSSEC

Figure 2: List of products involve in the study

The products surveyed are chosen based on the product details found in white papers and articles published in the Internet. The details about the products vary and additional information about the product can be found directly from the product websites. Presumably, misclassification of the responses in the survey is considered low, but there still is some minor error. The product detail is correct on the day the data is collected which was until 18 April 2009.

The study found that most of the products apply passive response and active response but not all products have reactive and proactive response. The study also found that there are fewer systems which adjust their real time configuration to proactive response, but most of them do collaborate with other system to minimize the intrusion impacts. The approach is still the same where additional appliances are used to support the response from an IDS.

The study also found that there are only 4 out of 27 products which use a mobile as a passive response, and most of the products are using HTML (100%) and Syslog (96%) as the main approach of the passive response. In addition, the percentages of the total 27 products using other approaches of passive response are: 48% for email (13 products), 11% for pager (3 products), and 33% for SNMP (9 products).

For the active response, the study is divided into 6 categories, which are, blocking, adjusting, collecting, collaborating, manual alteration and escalation to senior administrator for further investigation. For blocking, the product has the capability of blocking traffic and user from accessing the system. In addition to that, for adjusting, the study looked at the ability of the product to adjust the configuration and system automatically. For collecting, the study looked at the ability of the product to collect incidents information actively. For collaborating the study looks at the product's ability to collaborate with other appliances such as firewalls or other central monitoring systems. Finally, for system's manual response, the study will count if the product studied contains a manual response and allowed an administrator to adjust the configuration manual. Out of 27 products, the study shows that the percentages are 89% for blocking, 41% for adjusting, 100% for collecting, 70% for collaborating and 100% for both manual alteration and escalation to senior administrator for further investigation.

5. Future works and Conclusion

This paper studied the IRS by explaining and comparing the response mechanism. Even though the response mechanism model is not complete, especially on defining the other influencing factors for the model, the model clearly defined that response can be divided into two main responses, active and passive and other stages of proactive and reactive response.

In addition, using multiple literature comparisons, different perspectives, taxonomies, comparisons and relationship studies between types of responses, active response clearly can be divided into two other responses, proactive and reactive. Proactive is a response responding before an incident happen and reactive response is a respond after an incident happen. Moreover, the different examples of response mechanism, proactive and reactive response can be extended to have two other approaches and stages. Using attack time frame, the distinction between proactive and reactive response is explained.

This is the early stage of the discussion on enhancing IRSs. The response model is derived from the discussion made above. Clearly, there are many other issues which are not addressed in this paper, especially on the influencing factor for the IRSs. There are also issues that need to be explored and there are other practical issues that need to be addressed, such as an estimation of potential threats and how to define and increase the confidence level for each incident and estimation process.

6. References

Aickelin, U., Bentley, P., Cayzer, S., Kim, J. and McLeod, J. (2003), "Danger theory: The link between AIS and IDS?" *Proceeding of the Second International Conference on Artificial Immune Systems*, Vol. 2787, pp. 147-155.

Anderson, J.P. (1980), *"Computer Security Threat Monitoring and Surveillance",* James P. Anderson Co., Box 42, Fort Washington, PA, 19034, USA.

Anuar, N.B., Yaacob, M. and Idna, M.Y. (2004), "RedAlert: Approach for Firewall Policies Update Mechanism", *Wseas Transaction on Computer*, Vol. 3 No. 5, pp. 1451-1454.

Axelsson, S. (2000), *"Intrusion Detection Systems: a Survey and Taxonomy",* Department of Computer Engineering, Chalmers University, Gothenburg, Sweden.

Cabrera, J.B.D., Lewis, L., Qin, X., Lee, W. and Mehra, R.K. (2002), "Proactive Intrusion Detection and Distributed Denial of Service Attacks—A Case Study in Security Management", *Journal of Network and Systems Management*, Vol. 10 No. 2, pp. 225-254.

Capaccio, T. (2009), "Contractor returns money to Pentagon". *The Washington Times*, 25 July 2009.

Chen, C.M., Jeng, B.C., Yang, C.R. and Lai, G.H. (2006), "Tracing denial of service origin: Ant colony approach", *EvoWorkshops 2006*, Budapest, HUNGARY, pp. 286-295.

Cohen, F. (1999), "Simulating cyber attacks, defences, and consequences", *Computers & Security*, Vol. 18 No. 6, pp. 479-518.

Debar, H., Dacier, M. and Wespi, A. (1999), "Towards a taxonomy of intrusion-detection systems", *Computer Networks*, Vol. 31 No. 9, pp. 805-822.

Denning, D. (1987), *"A Prototype IDES: A Real Time Intrusion Detection Expert System",* Technical Report, Computer Science Laboratory, SRI International.

Denning, D.E. and Neumann, P.G. (1985), *"Requirements and Model for IDES - A Real-time Intrusion Detection Expert System",* Technical Report, CSL, SRI International.

Dondo, M.G. (2008), "A vulnerability prioritization system using a fuzzy risk analysis approach", *Proceeding of the 23rd International Information Security Conference*, Milano, ITALY, pp. 525-539.

Esmaili, M., Balachandran, B., Safavi-Naini, R. and Pieprzyk, J. (1996), "Case-based reasoning for intrusion detection", *Proceedings of the 12th Annual Computer Security Applications Conference*, pp. 214-223.

Feng, Z., Shijie, Z., Zhiguang, Q. and Jinde, L. (2003), "Honeypot: a supplemented active defense system for network security", *Proceedings of the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies*, pp. 231-235.

Fessi, B.A., Hamdi, M., Benabdallah, S. and Boudriga, N. (2007), "A decisional framework system for computer network intrusion detection", *European Journal of Operational Research*, Vol. 177 No. 3, pp. 1824-1838.

Fisch, E.A. (1996), *"Intrusion Damage Control and Assessment: A Taxonomy and Implementation of Automated Responses to Intrusive Behavior",* Ph.D. Dissertation, Texas A&M U.

Foo, B., Wu, Y.S., Mao, Y.C., Bagchi, S. and Spafford, E. (2005), "ADEPTS: adaptive intrusion response using attack graphs in an e-commerce environment", *Proceedings of the International Conference on Dependable Systems and Networks (DSN 2005)*, pp. 508-517.

Gangadharan, M. and Kai, H. (2001), "Intranet security with micro-firewalls and mobile agents for proactive intrusion response", *Proceedings of the International Conference on Computer Networks and Mobile Computing*, pp. 325-332.

Hacking-Lexicon (2009), "Linux Dictionary", Available at: http://www.tldp.org/LDP/Linux-Dictionary/html/i.html (Accessed: 19 July 2009).

Hong, H., Xian-Liang, L., Li-Yong, R. and Bo, C. (2006), "Taichi: An Open Intrusion Automatic Response System Based on Plugin", *Proceedings of the International Conference on Machine Learning and Cybernetics*, pp. 66-77.

Huiying, L. and Yuanda, C. (2008), "Research on Network Risk Situation Assessment Based on Threat Analysis", *Proceedings of the International Symposium on Information Science and Engineering*, Shanghai, China, pp. 252-257.

Jackson, K. (1999), *"Intrusion detection system product survey",* Technical Report LA-UR-99-3883, Los Alamos National Laboratory.

Jang, H. and Kim, S. (2002), "Real-time intruder tracing through self-replication", *Proceeding of the 5th International Information Security Conference (ISC)*, Sao Paulo, Brazil, pp. 1-16.

Kotsiantis, S.B. (2007), "Supervised Machine Learning: A Review of Classification Techniques", *Informatica*, Vol. 31 No. 3, pp. 249-268.

Lewandowski, S.M., Van Hook, D.J., O'Leary, G.C., Haines, J.W. and Rossey, L.M. (2001), "SARA: Survivable Autonomic Response Architecture", *Proceedings of the DARPA Information Survivability Conference & Exposition II (DISCEX '01)*, Vol. 1, pp. 77-88.

MyCERT (2008), "Malaysian Computer Emergency response Team Incident Statistic", Available at: http://www.mycert.org.my/en/services/statistic/mycert/2008/main/detail/566/index.html (Accessed: 16 October 2008).

Papadaki, M. and Furnell, S. (2004), "IDS or IPS: what is best?", *Network Security*, Vol. 2004 No. 7, pp. 15-19.

Papadaki, M., Furnell, S.M., Lee, S.J., Lines, B.L. and Reynolds, P.L. (2002), "Enhancing Response in Intrusion Detection Systems", *Journal of Information Warfare*, Vol. 2 No. 1, pp. 90-120.

Ragsdale, D.J., Carver, C.A., Jr., Humphries, J.W. and Pooch, U.W. (2000), "Adaptation techniques for intrusion detection and intrusion response systems", *Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics*, Vol. 4, pp. 2344-2349.

Russo, J.E. and Schoemaker, P.J.H. (1989), "*Decision traps: Ten barriers to brilliant decision-making and how to overcome them",* New York: Simon & Schuster. pp 304.

Schouwenberg, R. (2008), "Attacks on banks", Available at: http://www.viruslist.com/en/analysis?pubid=204792037 (Accessed: 18 October 2008).

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

Sherif, J.S., Ayers, R. and Dearmond, T.G. (2003), "Intrusion detection: the art and the practice. Part I", *Information Management & Computer Security*, Vol. 11, pp. 175-186.

Sherif, J.S. and Dearmond, T.G. (2002), "Intrusion detection: systems and models", *Proceedings of Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE 2002)*, pp. 115-133.

Stakhanova, N., Basu, S. and Wong, J. (2007), "A taxonomy of intrusion response systems", *International Journal of Information and Computer Security*, Vol. 1 No. 1/2, pp. 169-184.

Thames, J.L., Abler, R. and Keeling, D. (2008a), "A distributed active response architecture for preventing SSH dictionary attacks", *Proceedings of the IEEE Southeastcon 2008*, Vol. 1 and 2, Huntsville, Alabama, pp. 84-89.

Thames, J.L., Abler, R. and Keeling, D. (2008b), "A Distributed Firewall and Active Response Architecture Providing Preemptive Protection ", *Proceedings of the 46th ACM Southeast Conference 2008*, Auburn, AL, USA.

Tjhai, G.C., Papadaki, M., Furnell, S.M. and Clarke, N.L. (2008), "The Problem of False Alarms: Evaluation with Snort and DARPA 1999 Dataset". *Trust, Privacy and Security in Digital Business.* pp 139-150.

Wang, H.Q., Wang, G.F., Lan, Y., Wang, K. and Liu, D.X. (2006), "A new automatic intrusion response taxonomy and its application", *Proceedings of the 8th Asia-Pacific Web Conference and Workshops (APWeb 2006)*, Harbin, People R China, pp. 999-1003.

Wang, X., Reeves, D.S., Wu, S.F. and Yuill, J. (2001a), "Sleepy Watermark Tracing: An Active Network-Based Intrusion Response Framework", *Proceedings of the IFIP TC11*

Sixteenth Annual Working Conference on Information Security: Trusted Information: The New Decade Challenge, Vol. 193, pp. 369 - 384.

Wang, X.Y., Reeves, D.S. and Wu, S.F. (2001b), "Tracing Based Active Intrusion Response", *Journal of Information Warefare*, Vol. 1 No. 1, pp. 50–61.

White, G.B., Fisch, E.A. and Pooch, U.W. (1996), "Cooperating security managers: A peer-based intrusion detection system", *IEEE Network*, Vol. 10 No. 1, pp. 20-23.

Wu, Y.S., Foo, B., Mao, Y.C., Bagchi, S. and Spafford, E.H. (2007), "Automated adaptive intrusion containment in systems of interacting services", *Computer Networks*, Vol. 51 No. 5, pp. 1334-1360.

Yu, S. and Rubo, Z. (2008), "Automatic intrusion response system based on aggregation and cost", *Proceedings of the International Conference on Information and Automation (ICIA)*, pp. 1783-1786.

Yue, W.T. and Cakanyildirim, M. (2007), "Intrusion prevention in information systems: Reactive and proactive responses", *Journal of Management Information Systems*, Vol. 24, pp. 329-353.

Zhang, Z., Ho, P.-H. and He, L. (2009), "Measuring IDS-estimated attack impacts for rational incident response: A decision theoretic approach", *Computers & Security (2009)*.

Zhi-tang, L., Jie, L., Li, W. and Dong, L. (2007), "Assessing Attack Threat by the Probability of Following Attacks", *Proceedings of the International Conference on Networking, Architecture, and Storage (NAS 2007)*, pp. 91-100.