An investigation and survey of response options for Intrusion Response Systems (IRSs)

Nor Badrul Anuar[1, 2], Maria Papadaki[1], Steve Furnell[1] and Nathan Clarke[1]

[1]Centre for Security, Communications and Network Research, University of Plymouth, Plymouth, UK
cscan@plymouth.ac.uk
[2]Faculty of Computer Science and information Technology, University of Malaya, Kuala Lumpur, MY
badrul@um.edu.my

Abstract— **The rise of attacks and incidents need additional and distinct methods of response. This paper starts a discussion by differentiating the type of operation mode such as Intrusion Detection Systems (IDSs), Intrusion Prevention Systems (IPSs) and Intrusion Response Systems (IRSs). Using characteristics of response and attack time frame, a response model is proposed to distinguish between active and passive response options. The characteristics of response include level of operations, speed and time of response, ability to learn and ability to cooperate with other devices. This paper uses the attack time frame as a response model to show the relationship between active and passive response. Furthermore, the Response Model for Intrusion Response Systems shows some other different approaches and stages of active response. Finally, in order to investigate the most common response used by security practitioner and to justify the response model, studies involving 34 samples products from both commercial and non-commercial are analysed. As a result, this paper shows a clear distinction between the options of responses.**

Intrusion Response Systems (IRSs), active, proactive, reactive and passive response

I. INTRODUCTION

In recent years, statistics have shown that number of reported intrusions in the Symantec Global Internet Security Threat Report is growing [1]. In Malaysia, the latest 6-month report for 2009 indicated a 100% increment on the number of reported cases [2]. Moreover, in another continent, 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 [3]. The high cost of the contract indicates the serious financial commitment made by the Pentagon to prevent and secure their infrastructure from being attacked from other country. In the UK, a survey on UK businesses, conducted by PricewaterhouseCoopers between October 2007 and January 2008, reveals an increasing number of incidents [4], with 94% of very large companies encountered an incident and 76% of them had at least one serious incident. With an average of more than 400 incidents per year, the financial cost is substantial, and it ranges in between £1 to £10 million for larger organizations. This is not surprising, as there were 1,656,227 new malicious code detected by Symantec in 2008, which is increased by more than 250% from the previous year [1]. In addition, Symantec also observed an average of 75,158 active bot-infected computers per day, which shows an increase of 31 percent from the previous period. From those examples, it can be seen that the impact from attackers is unavoidable. Hence, computer security scientists and researchers are now continuously searching for better and safer methods to prevent, minimize and overcome incidents.

In order to counter the problem of attacks, tools such as Intrusion Detection, Prevention, and Response Systems (IDPRS), have emerged. Their aim is to monitor system and/or network activity and detect, prevent, and/or counter suspicious incidents. The early steps towards intrusion detection were made with Anderson's [5] research in automated log collection and management. The concept was further developed by Denning and Newman [6, 7], and since then, it has received extensive interest by the research community.

To date, studies have shown that there are hundreds of published works [8, 9], focusing on increasing the level of efficiency and reliability of intrusion detection systems. Whilst IDS technologies have advanced, there are still areas to explore, particularly with respect to incident response. Specifically, some challenges in the area include the problems of identifying false alarms [10], defining which asset is critical [11], selecting which threat needs to be urgently neutralized [12], identifying which incident needs investigation or which needs to be prioritized [13], and so forth.

As a first step towards studying and improving incident response, it is important to investigate the response options of such systems. The aim of this paper is to present a response model that provides the basis for understanding different response actions, and to present an analysis of the available response options in Intrusion Response Systems (IRSs).

The paper is divided into five sections. The second section presents the different modes, in which Intrusion Prevention, Detection, and Response Systems can operate. The third section focuses on responses, and highlights the evolution from passive Intrusion Detection Systems (IDSs) to modern IRSs with active response options. The fourth part describes the proposed response model, in relation to the attack time frame. Using the attack time frame, the active and passive zones are classified and new stages of active and passive responses are proposed. The fifth part of this paper investigates the state of

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

the art in existing IRSs, in order to assess the response capabilities of existing commercial and research products. Overall thoughts are then presented to conclude the discussion.

II. Detection, Prevention and Response System

Research initially focused upon enhancing the detection processes rather than response [8]. However, since the beginning of the 21st century, more attention has been given to the intrusion response research, particularly using combination with other approach like decision-making [14]. Moreover, the response model nowadays is not only static, but also provides a dynamic mapping in selecting various types of responses [14].

Before discussing the multiple types of response, it is important to distinguish the different modes, in which Intrusion Detection, Prevention and Response Systems can operate. Therefore, the mode of the system can be described as follows:

- A system running in IDS mode is able to perform an intrusion detection process and traditionally may produce a simple warning and alarm when the intrusion is detected. IDS could be a software, hardware or combination of both to detect intrusion using various techniques and algorithm [15]. 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 [16]. The final goal for IDSs is to assist system administrators to estimate the state of the system and suggest an appropriate response [17]. In the early days, IDS would only produce passive responses such as producing a log or notifying an administrator about suspicious activity.

- Systems running in IPS mode 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 it 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 [18]. The idea of combining firewall and IDSs have been researched by Jin *et al.* [19] and five types of the combination introduced by Desai [20] include inline NIDS, application-based, firewalls/IDS, layer seven switches, network-based application IDS and deceptive applications. Perhaps similar to proactive response in IRSs, the only unique characteristic for IPS is its non collaboration with other security appliances. In addition, host-based IPS uses a security enhancement on OS application system interfaces (API) and OS kernel. According to Rash et al. [21], the host-based IPS is able to stop any initial exploit.

- Systems running in IRS mode perform a similar function to IDS and IPS by maintaining several approaches to detect and response, but use multi types of responses with further analysis to minimize incident impacts. Knowingly, IRS is tightly coupled with an IDS and take over after signs of an intrusion to either record the attack passively or attempt to minimize the impact actively [22]. Research aims to have IRSs which are able to run automatically plus reconfigure, regenerate and rejuvenate systems once an intrusion occurs [23]. Unlike IDS and IPS mode, IRS mode offers additional functions and exhibits multiple characteristics of response to mitigate intrusion impacts. Not just a passive response, IRS concentrates on response functions by showing characteristics such as proactive and reactive responses. In addition, with the variety of characteristics, IRS is 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 [24], and redirect connections for other precautions [25].

It can be seen that the three modes share similarity in terms of detection. In terms of response, the three modes are not limited to passive response and can actively use multiple techniques and approaches to limit and reduce intrusion impact. In order to manage multiple appliances, Security Information and Event Management (SIEM) is a technology which provides real-time monitoring and historical reporting of security events from network, system and/or applications [26] and can be seen as a new approach in enhancing IDPRS. Comprehensively, the SIEM technology can not only collect hundreds of incident events from various types of appliances, but also respond to security incidents. Given its relevance to response, SIEM technologies will be included in this research.

III. Incident Responses: Active vs. Passive

According to various existing IDS and IRS taxonomies, [27, 28, 29, 30, 31], a response can be clearly divided into two main types; active and passive.

- An active response is used to counter an incident in order to minimize a vulnerability's impact to victims;

- A passive response normally aims to notify other parties about the occurrence of an incident and relies upon them to take further action.

Yue and Cakanyildirim [25] 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 the case of the action taken immediately, an

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

active response can also be referred to as an immediate response [25]. Similarly, active response operates automatically as well as run fast [32]. In addition, in order to do this, Ragsdale *et al.* [33] uses some adaptive, learning, and intelligent methods in this type of response.

However, active response sometimes produces negative results if the response systems are not configured correctly. For example, an active response can generate Denial of Service (DoS) attacks to the networks itself by blocking or terminating a legitimate connection or user. In order to avoid this, the system must be configured correctly so that it can respond with confidence. In addition, an active response must have capacities to engage a corrective action such as updating system patches automatically, logging off a user, reconfiguring firewall or disconnecting a port [34].

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 response is divided into two main categories of proactive and reactive:

- Proactive response is an approach that controls a potential incident activity before it happens rather than waiting to respond after the incident has happened.

- Reactive response reports any incident detected directly to information security analyst or a response action is taken immediately or in real-time. Contradicting to proactive response, reactive response reacts only after the intrusion is detected.

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 [27]. In addition, a proactive response approach can predict a new intrusion and confidently know the method to use to prevent the intrusion from spreading fast.

Proactive responses can be reconstructed into two different approaches:

- 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 [35]. At least, one solution proposed by Schultz [36] showed the capabilities of predicting a new attack and this technique perhaps can be extended to be used as input for future response models.

- 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 [37], but for proactive response, any previous incident response will be used as a reference point in order to prevent a future similar incident. For example, COBRA [38], RedAlert [39] and ADEPTS [23, 40] provide a proactive response in order to minimize the intrusion impact on other neighbouring systems. Similar to COBRA and RedAlert, a recent research by Thames, Abler and Keeling [41, 42] 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 of this, 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 [43]. As defined earlier, reactive response reacts only after the intrusion is detected. Therefore, it is suggested that there are two stages of responding in this situation;

- issuing confident responses immediately after an incident is detected;

- 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. For example, an automated response system using an automated system can be considered as a reactive response. Cooperating Security Managers (CSM) proposed by White [44], proactively detect intrusions but reactively responding to the incident [23]. In addition, to reduce incident impacts, the response at this stage collaborates with other security appliances such as firewall; for example the Taichi [45]. The Taichi is a system which combines heterogeneous IDSs with improved distributed firewall system and able to detect and prevent intrusion automatically.

The second stage of reactive response applies to incidents with high uncertainty where the incident need to be investigated and the behaviour of the incident needs be learned before a further response can be applied. The category is fundamentally made based on paper published by Yue and Cakanyildirim [25] 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 [46] or using a honeypot [47] 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 [24, 27, 46, 47, 48, 49].

Finally, passive response does not react to minimize the impact but only notify and collect information about the intrusion. Passive response is one of the earlier responses

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

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 exposed by Cohen [50]. For certain cases, ignoring incident is also one of the examples for passive response [51].

IV. Response Model for Intrusion Response Systems

Based on earlier discussion, it can be seen that response can be divided into several different categories and stages. Therefore, in order to show the relationship between the responses, this paper uses attack time frame as illustrated in Figure 1. This shows the common time frame when attack or intrusion is detected and responded by any security appliances. In differentiating the type of response and describing the response model, the attack time frame clearly depicts the stages of the response. In the figure, the relationship between responses is made based upon the attack time frame and contains three main lines t(n)-t, t(n) and t(n)+t, where t(n) denotes the time of the intrusion alarm. Based on t(n), the following two stages appear;

(i) Before intrusion alarm, between t(n) - t and t(n),

(ii) After intrusion alarm, in between t(n) and t(n) + t.

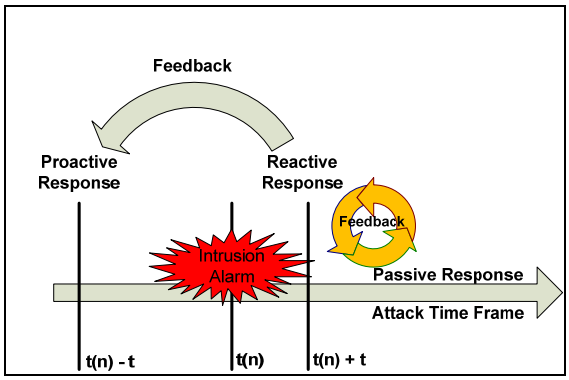

Figure 1. Relationship between passive, proactive and reactive response using attack time frame

In addition to the two stages, there is another stage of the attack time frame, after t(n) + t, which refers to a stage after reactive response. The stage before t(n) – t is assumed as a normal stage where no intrusion is detected. With a total of three main stages, the attack time frame in Figure 1 is considered appropriate to describe the variety of responses, which have been explained in the previous section. Therefore this will be used as the Response Model for Intrusion Response Systems.

The stage of the attack time frame for the response model starts from stage t(n) – t, where this is a stage before incident is detected by IDSs, t(n). Within this stage, proactive response is playing a big role in defending hosts and networks from being attacked. For example, 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 of proactive response, this stage provides two critical response actions; (i) prevent any future potential incident based on prediction analysis and (ii) prevent current and future potential attacks based on incident feedback from passive and active response.

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

Unlike the previous stages, the last stage after t(n) + t is an investigation phase. The stage is continuous with no specific ending point; hence this stage is suitable for non critical system. The moment is a continuous stage and only finish once the incident has been investigated and action has been taken. This stage is using the second stage of reactive response by waiting, investigating and learning about incident before further response can be applied.

In addition at stage t(n) + t, some incident feedback can be collected from passive responses. This can be combined with the feedback on 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 which is from both responses; therefore both responses communicate continuously in order to provide better investigation and analysis on any incident.

Finally, as a conclusion from the discussion above, it clearly indicates that response model for IRSs can be divided into two main response zones; active and passive zone with additional four different stages in active response (i) two approaches of proactive response, (ii) two stages of reactive response.

V. Product Comparison

In understanding the model, this paper presents a comparison study. This study helps to investigate the level of response applied in commercial and research products, looking at IDS, IPS and IRS technologies, as well as Security Information and Event Management (SIEM) products.

A total of 34 systems were compared, including both commercial and non-commercial products. The commercial products were selected based on two reports from Gartner, namely the Magic Quadrant for Network Intrusion Prevention System Appliances [52] and Magic Quadrant for Security Information and Event Management [26]. As a guideline, the non-commercial products were selected based on online ratings of open source products published by several experts in the area [53, 54, 55].

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

TABLE I. PRODUCT COMPARISON ON IDSS/IPSS/SIEM

						Proactive			Reactive			Passive					
	Name of Product	Company /Organization	Commercial (C) Non-commercial (NC)	HIDS/NIDS/SIEM	With SIEM	predicts a new attack	blocks future attack	adjust regularly	collaborates	terminate	collects information	syslog and console	email	pager	SNMP	HTML	PDA/Mobile
1	AlienVault	AlienVault	Both	SIEM			X	X	X	X	X	X	X		X	X	
2	ArcSight Enterprise Security Manager	ArcSight	C	SIEM			X	X	X	X	X	X	X		X	X	
3	Bro IDS with Plugin	Lawrence Berkeley National Laboratory	NC	NIDS			X		X	X	X	X	X	X	X	X	X
4	CA-Host Based IPS	CA Inc	C	HIDS	SIEM		X		X	X	X	X					
5	Checkpoint IPS-1	Checkpoint Inc	C	NIDS			X		X	X	X	X	X				
6	Cisco IDS	Cisco Systems Inc	C	NIDS	SIEM		X		X	X	X	X					
7	Cisco Security Monitoring, Analysis and Response System (MARS)	Cisco Systems Inc	C	SIEM			X	X	X	X	X	X	X	X	X	X	
8	DeepNines IPS	DeepNines Technologies Inc	C	NIDS			X	X	X	X	X	X					
9	Enterasys Intrusion Prevention System	Enterasys Networks, Inc.	C	NIDS HIDS	SIEM		X	X	X	X	X	X	X		X	X	
10	FlowMatrix	AKMA Labs	NC	NIDS							X	X				X	
11	IBM Proventia Desktop	IBM	C	HIDS	SIEM		X		X	X	X	X					
12	IBM Proventia Network IPS Series	IBM	C	NIDS	SIEM		X		X	X	X	X			X	X	
13	IBM Tivoli Security Operation Manager	IBM	C	SIEM			X			X	X		X		X	X	
14	iPolicy Intrusion Detection/Prevention	iPolicy Networks	C	NIDS			X	X	X	X	X	X	X			X	
15	Juniper IDP	Juniper Networks, Inc	C	NIDS			X	X	X	X	X	X			X		
16	Loglogic Exaprotect	Loglogic	C	SIEM			X	X	X	X	X					X	
17	McAfee Host Intrusion Prevention for desktops	McAfee, Inc.	C	HIDS			X	X	X		X					X	
18	McAfee IntruShield	McAfee, Inc.	C	NIDS	SIEM		X	X	X	X	X	X			X	X	
19	McAfee IntruShield® Security Manager (ISM)	McAfee, Inc.	C	SIEM		X	X	X	X	X	X	X	X	X	X	X	X
20	netfence gateways	phion AG	C	NIDS			X		X	X	X	X	X		X		
21	NetIQ Security Manager SIEM	NetIQ	C	SIEM					X		X	X	X	X			X
22	NitroSecurity Guard IPS	NitroSecurity	C	NIDS	SIEM		X	X	X	X	X	X	X	X	X		
23	Osiris	Brian Wotring	NC	HIDS					X		X	X	X			X	
24	OSSEC	Trend Micro, Inc.	NC	NIDS HIDS SIEM			X		X	X	X	X	X	X			X
25	PHPIDS	PHPIDS Team	NC	HIDS						X	X		X			X	
26	Radware's DefensePro (APSolute Immunity)	Radware Ltd.	C	NIDS		X	X	X		X	X	X					
27	SAMHAIN	samhain design labs	NC	HIDS			X		X	X	X	X	X			X	
28	SecureNet IDS/IPS	Intrusion, Inc.	C	NIDS			X			X	X	X				X	
29	Snort IDS (Sourcefire IPS)	Sourcefire, Inc.	NC	NIDS			X		X	X	X	X	X	X	X	X	X
30	StoneGate IPS	Stonesoft Inc.	C	NIDS			X		X	X	X	X	X		X		X
31	Strata Guard	StillSecure	C	NIDS			X			X	X	X	X		X	X	
32	Symantec Critical System Protection	Symantec	C	HIDS			X		X	X	X	X			X	X	
33	TippingPoint IDS/IPS	3Com	C	NIDS			X	X	X	X	X	X	X	X	X		
34	Top Layer Security : IPS	Top Layer Networks	C	NIDS			X	X	X	X	X	X	X		X	X	

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

Using the previous response model in Figure 1, active response is divided into proactive and reactive responses. Proactive responses are further subdivided into ones utilising attack prediction and the ones that do not. As for reactive responses, they are subdivided into 2 stages. Based on the response model, the 1st stage of reactive response refers to the countermeasures like terminating the user, process or network traffic and collaboration between other security appliances by limiting the user, process and or network traffic. Therefore, in comparing the product, the study tabulates the result for the 1st stage of reactive response into two categories; collaborates and terminate. The first category relates to any collaboration that can be established between the product and other products, and the second category refers to the ability of the product to terminate user, process and/or network traffic. In extension, the study tabulates the result for the 2nd stage of reactive response in the "collects information" column. Finally, the study uses six categories of passive responses, namely syslog and console, email, pager, SNMP, HTML and PDA/Mobile.

Product literature and documentation, white papers, and online articles were then investigated during late 2009 in order to determine the response options offered by the selected products. Table 1 shows the results of this survey. However, the detail about the product can be varied and additional information about the product can be found directly from the product website. Misclassification of the response is considered low, but there still is some minor potential for error.

From the table, the Network Intrusion Detection Systems (NIDS) category is dominated by the commercial products, and only 4 out of 19 products are non-commercial products. A part from that, the result shows 26 products are stand-alone IDSs or IPSs product and the rest are SIEM products or a combination of the SIEM and IDSs/IPSs products. However, not all surveyed organisation produce SIEM and IPSs products together. This report highlights at least 7 IDS/IPS products use Security Information and Event Management from same company or organisation (namely Trend Micro, McAfee, IBM, Enterasys Networks, NitroSecurity, Cisco Systems and CA Inc).

Interestingly, the study highlights the following findings;

- This report identified that only 2 products used the 1st type of proactive response. The products were McAfee IntruShield® Security Manager (ISM) and Radware's DefensePro (APSolute Immunity).

- Most of the products apply the 2nd stage of the proactive response. 80% of the products apply blocking mechanism techniques as a proactive response, but only 44% of products had the capability to automatically adjust the configuration regularly.

- Not all products have capability on making connection or collaboration with other security appliances, only 82% of the products surveyed has the ability on the 1st stage of reactive response.

- 30 products (88%) had an ability to terminate the connection.

- All products have an ability to collect information about the incident, which is the 2nd stage of the reactive response.

- All products support passive responses, with 88% using console or syslog as a main notification method.

- Email, HTML and SNMP are supported by the majority of products to notify security analysts.

- Pager and mobile notification are relatively rare, with less than 10% using these types of notification.

However, the study also has some limitations as follows;

- The comparison study only focused on the commercial product based on Gartner's report. In addition, there are other products listed in Table 1 are not covered in the Gartner's report; for example the non-commercial products.

- Since the comparison study aims to provide basic analysis of available responses options in IRSs, the result of the study can not be used as an evidence for selecting the best product in mitigating intrusions or attacks, as other factors such as performance, detection accuracy, etc would need to be considered for such a decision. The study does not necessarily show the best product for IDSs/IPSs/IRSs/SIEM, as aspects such as performance, detection accuracy, and so on have not been taken into account. In this case, if the product listed has more than 1 type of responses or satisfy all the response, it does not mean and refer to the best product.

VI. CONCLUSION

This paper studied incident response by explaining and comparing the variety of responses guided by response model, attack time frame and some literature studies. Even though the response model is not scientifically proved by experiments, it clearly defined that response can be divided into two main categories of active and passive, and further stages of proactive and reactive response.

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.

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

Using attack time frame, a clear distinction between proactive and reactive response is explained.

In addition, using this response model, the research on the intrusion response can be enhanced, particularly in selecting and mapping appropriate response with appropriate incidents. For the time being, intrusion response relies on the multi and variety type of responses. The response model can be used as a model to map the current existing responses by arranging them into appropriate stage. For example, a serious incident can be mapped into proactive or reactive response and the other incident can be mapped into the passive response.

In addition, the comparison study has shown that the response model can be applied to current commercial and non-commercial products. The study noted that the current products can be categorised into appropriate type of responses. In addition, the availability of the current response option is considered appropriate because at least one response applied in commercial or research product. The study has provided a clear distinction between the options of responses.

There are many other things need to be done before Intrusion Response Systems (IRSs) can become reliable, efficient and matured technology. One of the objectives of this paper is to show that the response model can be used to map the appropriate response with appropriate incident; therefore in the future, by arranging and prioritizing incidents, the model can ensure that serious incidents can be assured to receive correspondingly serious responses.

ACKNOWLEDGMENT

The authors are thankful to the Ministry of Higher Education in Malaysia and the University of Malaya for providing scholarship to the first author of this paper.

REFERENCES

[1] Symantec, "Symantec Internet Security Threat Report Trends for 2008 Volume XIV," Symantec Corporation 2009. Available: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf.

[2] MyCERT. (2009). Malaysian Computer Emergency Response Team. [Online]. Available: http://www.mycert.org.my/en/.

[3] T. Capaccio, "Contractor returns money to Pentagon,", The Washington Times, 25 July 2009.

[4] BERR, "2008 Information Security Breaches Survey - Technical Report," Department for Business Enterprise and Regulatory Reform 2009. Available: http://www.pwc.co.uk/pdf/BERR_ISBS_2008(sml).pdf.

[5] J. P. Anderson, "Computer Security Threat Monitoring and Surveillance," James P. Anderson Co., Box 42, Fort Washington, PA, 19034, USA 1980.

[6] D. Denning, "An Intrusion-Detection Model," *IEEE Transaction on Software Engineering,* vol. 13, pp. 222-232, 1987.

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

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

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

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

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

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

[13] M. G. Dondo, "A vulnerability prioritization system using a fuzzy risk analysis approach," in *23rd International Information Security Conference*, Milano, ITALY, 2008, pp. 525-539.

[14] C. Mu and Y. Li, "An intrusion response decision-making model based on hierarchical task network planning," *Expert Systems with Applications,* vol. 37, pp. 2465-2472, 2010.

[15] J. McHugh, A. Christie, and J. Allen, "Defending yourself: the role of intrusion detection systems," *IEEE Software,* vol. 17, pp. 42-51, 2000.

[16] U. Aickelin, P. Bentley, S. Cayzer, J. Kim, and J. McLeod, "Danger theory: The link between AIS and IDS?," in *Second International Conference on Artificial Immune Systems*, 2003, vol. 2787, pp. 147-155.

[17] Z. Zhang, P.-H. Ho, and L. He, "Measuring IDS-estimated attack impacts for rational incident response: A decision theoretic approach," *Computers & Security,* vol. 28, pp. 605-614, 2009.

[18] M. Papadaki and S. Furnell, "IDS or IPS: what is best?," *Network Security,* vol. 2004, pp. 15-19, 2004.

[19] H. Jin, F. Xian, Z. F. Han, and S. L. Li, "A distributed dynamic mu Firewall architecture with mobile agents and KeyNote trust management system," in *4th International Conference on Information and Communications Security (ICICS 2002)*, Singapore, Singapore, 2002, pp. 13-24.

[20] N. Desai. (2003). Intrusion Prevention Systems: the Next Step in the Evolution of IDS. [Online]. Available: http://engsci.aau.dk/kurser/ETC/Nap/Papers/Ips/Sub/Intrusion%20Prevention%20Systems%20-%20the%20Next%20Step%20in%20the%20Evolution%20of%20IDS.pdf.

[21] M. Rash, A. Orebaugh, G. Clark, B. Pinkard, and J. Babbin, *Intrusion Prevention and Active Response: Deploying Network and Host IPS*: Syngress, 2005.

[22] T. Toth and C. Kruegel, "Evaluating the impact of automated intrusion response mechanisms," in *18th Annual Computer Security Applications Conference*, 2002, pp. 301-310.

[23] Y. S. Wu, B. Foo, Y. C. Mao, S. Bagchi, and E. H. Spafford, "Automated adaptive intrusion containment in systems of interacting services," *Computer Networks,* vol. 51, pp. 1334-1360, Apr 2007.

[24] X. Y. Wang, D. S. Reeves, and S. F. Wu, "Tracing Based Active Intrusion Response," *Journal of Information Warefare,* vol. 1, pp. 50–61, 2001.

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

[26] M. Nicolett and K. Kavanagh, "Magic Quadrant for Security Information and Event Management," Gartner RAS Core Research Note G00167782 2009.

[27] N. Stakhanova, S. Basu, and J. Wong, "A Cost-Sensitive Model for Preemptive Intrusion Response Systems," in *21st International Conference on Advanced Information Networking and Applications (AINA '07)*, 2007, pp. 428-435.

[28] H. Debar, M. Dacier, and A. Wespi, "Towards a taxonomy of intrusion-detection systems," *Computer Networks,* vol. 31, pp. 805-822, 1999.

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

[30] S. Axelsson, "Intrusion Detection Systems: a Survey and Taxonomy," Department of Computer Engineering, Chalmers University, Gothenburg, Sweden 2000.

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

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

[33] D. J. Ragsdale, C. A. Carver, Jr., J. W. Humphries, and U. W. Pooch, "Adaptation techniques for intrusion detection and intrusion response systems," in *IEEE International Conference on Systems, Man, and Cybernetics*, 2000, vol. 4, pp. 2344-2349.

[34] K. Jackson, "Intrusion detection system product survey," Technical Report LA-UR-99-3883, Los Alamos National Laboratory 1999.

[35] S. B. Kotsiantis, "Supervised Machine Learning: A Review of Classification Techniques," *Informatica,* vol. 31, pp. 249-268, 2007.

[36] E. E. Schultz, "A framework for understanding and predicting insider attacks," *Computers & Security,* vol. 21, pp. 526-531, 2002.

[37] M. Esmaili, B. Balachandran, R. Safavi-Naini, and J. Pieprzyk, "Case-based reasoning for intrusion detection," in *12th Annual Computer Security Applications Conference*, 1996, pp. 214-223.

[38] M. Gangadharan and H. Kai, "Intranet security with micro-firewalls and mobile agents for proactive intrusion response," in *International Conference on Computer Networks and Mobile Computing*, 2001, pp. 325-332.

[39] N. B. Anuar, M. Yaacob, and M. Y. Idna, "RedAlert: Approach for Firewall Policies Update Mechanism," *Wseas Transaction on Computer,* vol. 3, pp. 1451-1454., 2004.

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

[41] J. L. Thames, R. Abler, and D. Keeling, "A Distributed Firewall and Active Response Architecture Providing Preemptive Protection," in *46th ACM Southeast Conference 2008*, Auburn, AL, USA, 2008, pp. 220-225.

[42] J. L. Thames, R. Abler, and D. Keeling, "A distributed active response architecture for preventing SSH dictionary attacks," in *IEEE Southeastcon 2008*, Huntsville, Alabama, 2008, vol. 1 and 2, pp. 84-89.

[43] B. A. Fessi, M. Hamdi, S. Benabdallah, and N. Boudriga, "A decisional framework system for computer network intrusion detection," *European Journal of Operational Research,* vol. 177, pp. 1824-1838, 2007.

[44] G. B. White, E. A. Fisch, and U. W. Pooch, "Cooperating security managers: A peer-based intrusion detection system," *IEEE Network,* vol. 10, pp. 20-23, 1996.

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

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

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

[48] X. Wang, D. S. Reeves, S. F. Wu, and J. Yuill, "Sleepy Watermark Tracing: An Active Network-Based Intrusion Response Framework," in *Proceedings of the IFIP TC11 Sixteenth Annual Working Conference on Information Security: Trusted Information: The New Decade Challenge*, 2001, vol. 193, pp. 369 - 384.

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

[50] F. Cohen, "Simulating cyber attacks, defences, and consequences," *Computers & Security,* vol. 18, pp. 479-518, 1999.

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

[52] G. Young and J. Pescatore, "Magic Quadrant for Network Intrusion Prevention System Appliances," Gartner RAS Core Research Note G00167309 2009.

[53] SECTOOLS. (2010). Top 5 Intrusion Detection Systems. [Online]. Available: http://sectools.org/ids.html.

[54] R. Bejtlich, *The Tao of Network Security Monitoring: Beyond Intrusion Detection*: Addison Wesley, 2004.

[55] B. Wotring, *Host integrity monitoring: using Osiris and Samhain*: Syngress 2005.

978-1-4244-5494-5/10/$26.00 ©2010 IEEE