1-1-2011

A risk index model for security incident prioritisation

Nor Badrul Anuar
Plymouth University, United Kingdom

Steven Furnell
Edith Cowan University

Maria Papadaki
Plymouth University, United Kingdom

Nathan Clarke
Edith Cowan University

DOI: 10.4225/75/57b52a66cd8b5
9th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 5th -7th December, 2011

A RISK INDEX MODEL FOR SECURITY INCIDENT PRIORITISATION

Nor Badrul Anuar1,2, Steven Furnell1,3, Maria Papadaki1, Nathan Clarke1,[3]
[1]Centre for Security, Communications and Network Research, Plymouth University, United Kingdom
[2]Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur, Malaysia
[3]School of Computer and Security Science, Edith Cowan University, Perth, Western Australia
info@cscan.org, badrul@um.edu.my

Abstract

With thousands of incidents identified by security appliances every day, the process of distinguishing which incidents are important and which are trivial is complicated. This paper proposes an incident prioritisation model, the Risk Index Model (RIM), which is based on risk assessment and the Analytic Hierarchy Process (AHP). The model uses indicators, such as criticality, maintainability, replaceability, and dependability as decision factors to calculate incidents' risk index. The RIM was validated using the MIT DARPA LLDOS 1.0 dataset, and the results were compared against the combined priorities of the Common Vulnerability Scoring System (CVSS) v2 and Snort Priority. The experimental results have shown that 100% of incidents could be rated with RIM, compared to only 17.23% with CVSS. In addition, this study also improves the limitation of group priority in the Snort Priority (e.g. high, medium and low priority) by quantitatively ranking, sorting and listing incidents according to their risk index. The proposed study has also investigated the effect of applying weighted indicators at the calculation of the risk index, as well as the effect of calculating them dynamically. The experiments have shown significant changes in the resultant risk index as well as some of the top priority rankings.

Keywords
Incident prioritisation, risk assessment, Analytic Hierarchy Process, Risk Index Model

INTRODUCTION

The landscape of security threats continues to evolve and attacks are becoming more sophisticated (Symantec, 2011). The number of vulnerabilities is also rising. Based upon daily statistics published by the National Vulnerability Database, by the third quarter of 2011, the number of registered vulnerabilities is approximately 50,000. In 2010, Symantec (2011) encountered more than 286 million variants of malware; giving further evidence that the numbers are rising. Threats are evolving and numbers are rising, which means better ways are needed to manage them.

With security appliances identifying thousands of incidents every day, relying upon manual processes to determine their importance and urgency is difficult, error-prone and time-consuming. Therefore, an automated operation is needed. This paper proposes a new Risk Index Model (RIM) as a method of rating, ranking and prioritising incidents, and validates it via comparison to existing approaches, such as the Common Vulnerability Scoring System (CVSS) (NIST, 2011) and Snort Priority (Caswell and Roesch, 1998).

This paper is divided into three main parts: the first part discusses the background and related work in incident prioritisation; the second part presents the proposed Risk Index Model and the indicators that are used to support it; the third part presents the methodology and experimental results in validating the proposed approach, and then discusses the significance of the results.

BACKGROUND

Common approaches in prioritising incidents include static prioritisation, vulnerability pre-prioritisation and post-incident prioritisation. The static prioritisation approach tags and tunes signatures and prioritises known vulnerabilities based on the current characteristics of the vulnerabilities and experts' experience. Snort 2.1, for example, provides the Severity Identifier Option and this can be used to set a priority tag for some rules (Caswell and Beale, 2004). The vulnerability pre-prioritisation offers a similar approach to the static prioritisation but uses additional systematic methods like risk assessments and expert systems on analysing potential incidents. In the vulnerability pre-prioritisation, a potential risk for potential vulnerabilities is estimated before any real incidents are detected. Dondo (2008) applied a fuzzy system approach in accessing relative potential risks by associating potential vulnerabilities with computer network assets. Post-incident prioritisation inherits advantages similar to the previous approaches but extends the usage of risk assessment and cost-sensitive analysis. Lee and Qin (2003) estimated risks by associating three criteria: computer network assets, attacks and vulnerabilities. The M-Correlator proposed by Porras *et al.* (2002) is an alert ranking system based on the likelihood of attacks to succeed, the importance of targeted assets and the amount of interest in the type of attack. Alsubhi *et al.* (2008) proposed a fuzzy system based on metrics such as the importance of victims and the relationship between alerts.

The aforementioned approaches all have the ability to prioritise incidents, but they also have limitations. The use of Snort Priority groups similar critical incidents into similar groups of priorities (e.g. high, medium and low priority), with the consequence that security analysts face a challenge in analysing and differentiating which incidents are urgent and important. In addition, the use of CVSS in the vulnerability pre-prioritisation does not provide a full coverage of new incidents and limits itself to incidents with CVE-ID; this consequently produces incomplete results that security analysts have little confidence in. Furthermore, other studies such as Alsubhi *et al.* (2008) and Porras *et. al* (2002), have other limitations, particularly in the technical aspects of the methods adopted in their proposal. For example, although existing approaches consider multiple decision factors, they do not consider different weightings based upon the importance of different decision factors. The use of different weightings could provide more flexibility and allow the incident prioritisation process to reflect different organisational policies.

A popular prioritisation method is the Analytic Hierarchy Process (AHP), which is a theory of measurement through pair wise comparisons and relies upon the judgement of experts to derive priority scales, and which has already been successfully applied in several non-security contexts (Zahedi, 1986; Saaty, 2008a). This method is a systematic approach to making decisions and the use of the method in general can help to identify which incidents are important and which are trivial. To the best of the authors' knowledge, this study is the first attempt to evaluate the feasibility of adopting AHP in the incident prioritisation process.

RISK INDEX MODEL (RIM)

The proposed model estimates the risk index for every single incident based upon indicators and input obtained from asset environments and attributes within the incidents themselves. The Risk Index Model is a post-incident prioritisation, and the model rates each of the incidents to produce a risk index value. Based on the value, incidents are ranked quantitatively from the highest to the lowest index.

The model uses a combination of two decision factors: impact on asset and likelihood of threat and vulnerability. In addition, the aforementioned factors use several other indicators such as criticality, maintainability, replaceability, etc., as listed in

Table 4 and *Table 5*. These indicators were determined by reviewing existing literature. In order to reduce the uncertainty within the factors, the model uses a decomposition approach which has been applied in other security metrics studies (Wang and Wulf, 1997; Heyman *et al.*, 2008) and has proven useful in identifying basic components from higher level requirements (Savola and Abie, 2009). For instance, the basic components in the model refer to the elements that contribute input into the decision factors, also called an indicator, such as the type of incidents, time of incidents, cost of maintenance, replacement, and other related data.

The lists in the tables also specify the most significant references, on which each indicator is based. There are two main categories in differentiating the indicators: essential and desirable. An essential indicator (labelled as 'E' in the tables) is a main indicator and it has been applied in many previous frameworks and actively flagged by more recent studies. Desirable indicators (labelled as 'D' in the tables) are categorised as a secondary indicator, previously used by fewer studies. In order to reflect this difference, essential indicators are given a higher weight in the estimation of the risk index, whereas desirable indicators receive a lower weight.

Table 4: Indicators for impact on asset

Indicator	Type	Description	References
Criticality	E	Criticality estimates the importance and value of the asset. Criticality is based on three main and common attributes in security such as confidentiality, integrity and availability. Criticality also uses an asset value in estimating the final rating. Generally, the higher the criticality, the higher the impact on the asset.	Lee *et al.* (2002) Porras *et al.* (2002) Gregg and Kim (2005) Rogers *et al.* (2005) Davis *et al.* (2007) Zhang *et al.* (2007) Dondo (2008) Fenz and Neubauer (2009) Mu *et al.* (2008) Zhang *et al.* (2009)
Maintainability	D	Maintainability measures the cost of maintaining assets and is based on monetary value. Maintainability is similar to operational costs where it used in maintaining the operation of the asset. The cost of maintenance is measured by calculating the average cost in maintaining an asset annually. Generally, the higher the maintainability, the higher the impact on the asset.	Lee *et al.* (2002) Munteanu (2006) Zhang *et al.* (2009) Strasburg *et al.* (2009)
Replaceability	D	Replaceability refers to the ability to replace an asset in terms of cost and time. There is a trade-off between replaceability and asset criticality. Unlike the asset criticality, the higher the asset replaceability, the lower the impact on the asset. The sooner the replacement is placed, the less impact on the asset.	Lee *et al.* (2002) Munteanu (2006) Haslum *et al.* (2007) Pak and Cannady (2009) Zhang *et al.* (2009) Strasburg *et al.* (2009)
Dependability	D	Dependability determines whether the asset is operated alone or if it depends on other assets or applications. The more connections an asset has with other assets, the higher its dependability is. In other words, the more connections between assets and applications, the higher the impact on the asset.	Porras *et al.* (2002) Toth and Kruegel (2002) Lee and Qin (2003) Nicole *et al.* (2004) Kheir *et al.* (2010)
Control	D	This measures the control factors that are implemented by an asset or application. Controls are used to mitigate potential vulnerability and threats. Generally, the higher rating of asset control, the lower the impact on the asset.	Lee *et al.* (2002) Lee and Qin (2003) Dondo (2008) Ekelhart *et al.* (2009)

Table 5: Indicators for the likelihood of threats and vulnerability

Indicator	Type	Description	References
Severity	E	Severity refers to the severity of the potential incidents and the estimation of it may relate to the extent of vulnerability. As such, the extent of vulnerability can be obtained from other sources such as the Common Vulnerability Scoring System (CVSS). Generally, the higher the likely incident severity, the higher the potential risk.	Abedin *et al.* (2006) Lai and Hsia (2007) Alsubhi *et al.* (2008) Ahmed *et al.* (2008) Ausibal and Gallon (2008) Lin *et al.* (2008) Dondo (2008) Mu *et al.* (2008) Houmb and Franqueira (2009) Subramanian *et al.* (2009) Zhang *et al.* (2009) Fenz and Neubauer (2009)
Exploitability	D	Exploitability measures the general level of exploitability of incidents at a specific time. It shows the current state of the related vulnerability and verifies the impact to a specific asset at any specific time. Generally, the higher the status of the incident exploitability, the higher the risk.	Mell *et al.* (2006) Dondo (2008) Houmb and Franqueira (2009) Hausrath (2011) Clark and Stavrou (2011)
Sensitivity	D	Sensitivity measures the initial priority of incidents. The sensitivity shows the seriousness of the incident which is detected by certain detectors or appliances. Generally, the higher the rating of the incident sensitivity, the higher the risk.	Årnes *et al.* (2005) Årnes *et al.* (2006) Haslum and Årnes (2007) Alsubhi *et al.* (2008) Noel and Jajodia (2008) Zhang *et al.* (2009)
Similarity	D	Similarity represents the similarity between incidents' attributes within a particular period of time. The attributes are obtained from the detail between attacker and victim and they are the IP address, protocol, services and time of occurrence. The similarity between incidents' attributes can be used to estimate the seriousness of the incident. Generally, the higher the incident similarity, the higher the risk.	Valdes and Skinner (2001) Xu and Ning (2005) Alsubhi *et al.* (2008) Xiao *et al.* (2008) Yu and Rubo (2008)
Frequency	D	Frequency represents the frequency of the similar incidents that occurred within a particular period of time. Unlike similarity, the frequency identifies the similarity between vulnerabilities in terms of the number of occurrences within a particular period of time. Generally, the higher the incident frequency, the higher the risk.	Ning *et al.* (2004) Haslum and Årnes (2007) Alsubhi *et al.* (2008) Yu and Rubo (2008) Houmb *et al.* (2009)

Figure 1 depicts a block diagram with the indicators that are used to estimate the risk index, and the three level decision hierarchies involved:

1. Level 1 is the goal of the model. In this particular context, the model aims to rate, quantify and estimate the risk index for incidents. The model uses the risk index result produced with the aid of AHP as a value to rank and prioritise incidents.
2. Level 2 is the decision attributes of the model. These are the factors that influence the goal (e.g. the consequence, in terms of the impact on the asset, and likelihood of the event, based in turn upon the likelihood of associated threats and vulnerabilities).
3. Level 3 details the decision attributes defined in level 2. Five indicators influence the impact on asset and a further five inform the likelihood of threat and vulnerability. Each indicator uses quantitative values obtained from information metrics (e.g. incident information, criticality, incident severity and sensor sensitivity).

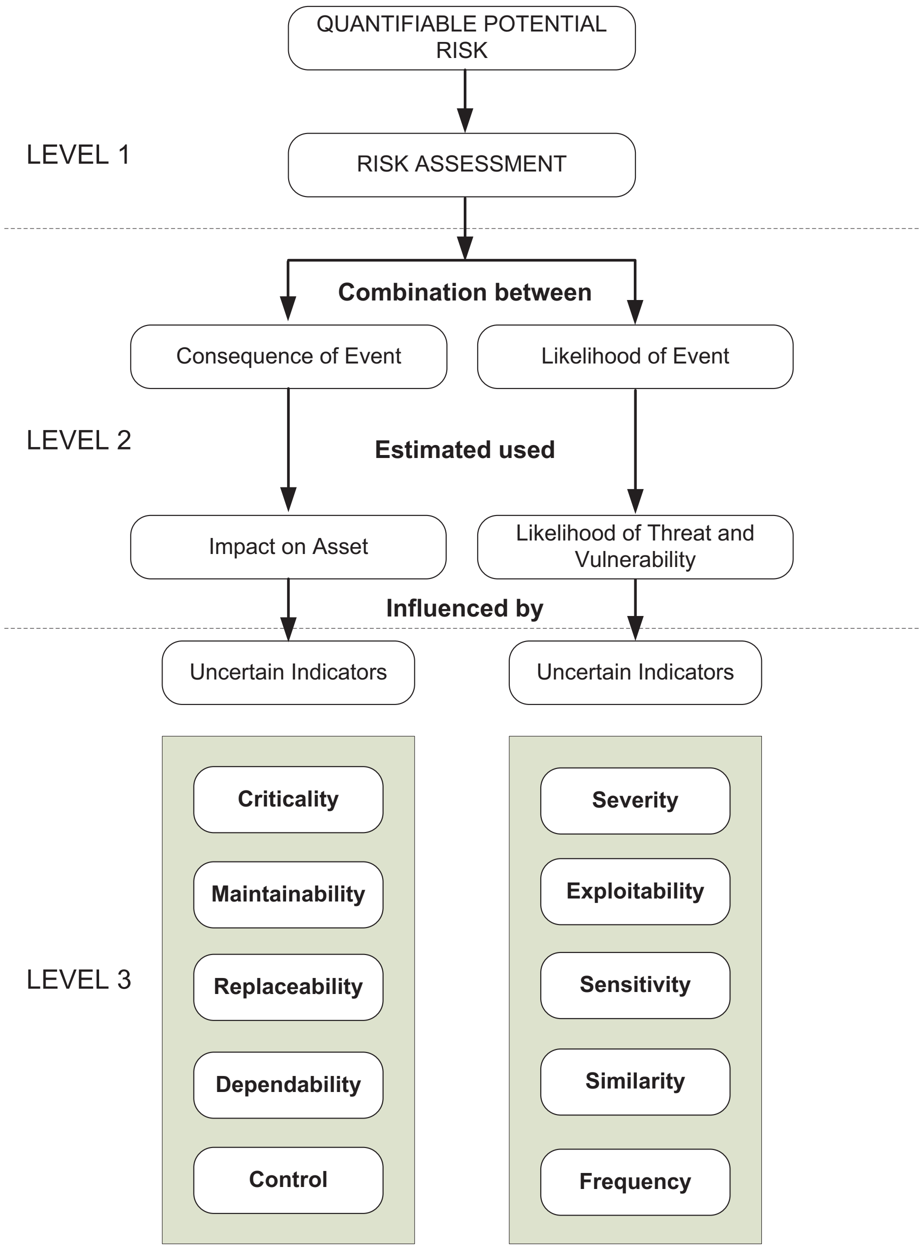

Figure 1: Decision hierarchy for the Risk Index Model

EXPERIMENTAL EVALUATION

Two experiments were used to validate the use of the Risk Index Model and AHP. Using the RIM, the experiment rates as well as ranks incidents. The experiments were conducted using one of the MIT 2000 DARPA (i.e LLDOS 1.0) data sets (DARPA, 2011), with some modifications. Specifically, given the lack of specific information on assets, some assumptions had to be made on the values of assets that related to the incident scenario in the dataset. The rationale behind the selection of the specific dataset is due to the multi-stage attacks it contains. This is important as it allows the model to evaluate and analyse the effectiveness of ranking and prioritising incidents over different phases.

EXPERIMENTS

The first set of experiments aimed to investigate the effect different weights for indicators can have on the calculation of the risk index. Initially an equal weight was used, whereas the next stage used different weights. Both experiments rate incidents only one time when the incidents are detected. Essentially, the rating for the risk index for each incident is unchanged and remains static until the end. Theoretically, the changes of the risk index periodically could give another implication such as it would affect the performance of the estimation process but perhaps it gives more accurate risk indexes. It is suggested that the estimation process must be done periodically (Lee *et al.*, 2002). However, the first set of experiments does not consider the changes of the risk index over time.

The second set of experiments aims to overcome this limitation by considering a risk index that is calculated dynamically. In order to achieve this, the following conditions were applied:

(a) The incident risk index is updated each time when a new alert is detected.

(b) The position of incidents is ranked again after a change to a risk index.

In order to compare the results, and validate the RIM, the experiment was based on some assumptions. In particular, with the DARPA 2000 LLDOS 1.0 dataset, there are different attacks in different stages of attacks, as shown in *Table 6*. To analyse the dataset, this paper made assumptions as follows:

(a) A true incident in every stage is assumed as a critical incident in that particular stage.

(b) Due to the multi-staged attack in the dataset, true incidents in the latest stage are assumed as more critical incidents compared to incidents in other previous stages.

Table 6: Attack phases

Phase	Attacker Schemes	Description
Phase 1	***IPsweep***	Sending ICMP echo-request for live hosts
Phase 2	***Probe***	Probe of live IP's to look for the sadmind daemon running on Solaris Hosts
Phase 3	***Break-in***	Break-ins via the sadmind vulnerability, both successful and unsuccessful on those hosts
Phase 4	***Install Virus***	Installation of the Trojan mstream DDoS software on three hosts using telnet
Phase 5	***DDos***	Launching the DDoS attacks

Furthermore, in order to show the result of the weight for each indicator, this paper adopts the AHP approach using the rating mode in order to rate incidents. The different weights for the indicators used in Experiment 2 were obtained using estimation in three judgement matrices: the judgement matrix of the influence factor, the judgement matrix of the main indicator for the consequence of an event (i.e. impact on asset), and the judgement matrix of the main indicator for the likelihood of an event (i.e. the likelihood of threats and vulnerability). The judgement matrices were used to evaluate the different results of the risk index. In this particular experiment, the judgement matrices were just an assumption made to manually fit with the model. Generally, they can be altered and the assumption in this particular experiment is not definitive and subject to reassessment. *Table 7*, *Table 8* and *Table 9* show the judgement matrices for the decision factors and indicators used in the RIM. Since there are two types of indicators, this study controls the essential indicators by giving a slightly higher value compared to the desirable indicator values. The valuation of the indicator is easy because the essential indicator for both decision factors always becomes a higher priority.

Although the judgement matrices were manually assigned, they need to be tested in order to maintain their consistency. Thus, they are tested using the random index (RI), consistency index (CI) and consistency ratio (CR) formulas (Saaty, 2008b). On the bottom of the tables there are three variables: λ_{max}, consistency index and consistency ratio. According to some studies (Zahedi, 1986; Saaty, 2008b), if the consistency ratio value is less than 10%, then the value can be considered as a reasonable and acceptable judgement or otherwise the judgement matrix is not consistent.

Table 7: Judgement matrix of the influence factor

	Consequence of Event	Likelihood of Event	**Priorities**
Consequence of Event	1.0000	0.8000	**0.4444**
Likelihood of Event	1.2500	1.0000	**0.5556**

λ_{max} = 2.0000; Consistency Index= 0.0000; Consistency Ratio = undefined

Table 8: Judgement matrix of the main indicator for the consequence of an event (impact on asset)

	Criticality	Maintainability	Replaceability	Dependability	Control	**Priorities**
Criticality	1.0000	5.0000	3.0000	2.0000	2.0000	**0.3859**
Maintainability	0.2000	1.0000	0.5000	0.2500	0.3333	**0.0659**
Replaceability	0.3333	2.0000	1.0000	2.0000	2.2000	**0.2210**
Dependability	0.5000	4.0000	0.5000	1.0000	1.5000	**0.1834**
Control	0.5000	3.0000	0.4545	0.6667	1.0000	**0.1437**

λ_{max} = 5.2684; Consistency Index= 0.0671; Consistency Ratio = 6.05%

Table 9: Judgement matrix of the main indicator for the likelihood of an event (likelihood of threats and vulnerability)

	Severity	Exploitability	Sensitivity	Similarity	Frequency	**Priorities**
Severity	1.0000	6.0000	7.0000	3.0000	4.0000	**0.4954**
Exploitability	0.1667	1.0000	2.0000	0.3333	0.3333	**0.0716**
Sensitivity	0.1429	0.5000	1.0000	0.1667	0.2000	**0.0426**
Similarity	0.3333	3.0000	6.0000	1.0000	2.0000	**0.2300**
Frequency	0.2500	3.0000	5.0000	0.5000	1.0000	**0.1604**

λ_{max} = 5.1574; Consistency Index = 0.0394; Consistency Ratio = 3.55%

RESULTS

There were 1,068 incidents detected and the critical incidents are highlighted in bold. *Table 10* and *Table 11* show the incidents and tabulated them into several phases: group, number of incidents, time, risk index and priority of the incident ranked at the specific time. In order to analyse the results, the table summarises the time detected and risk index into two different values (high/max and low/min). The ranking process was ranked at 12 different periods starting from 09:51:35 and ending at 12:35:48. To give a simple view, the incidents are grouped into a similar type of signature and ranked based on the highest and lowest risk indexes.

As can be seen in both tables*,* most true and critical incidents, except in the last phase, were ranked at the top priority ranking. In addition, this trend is consistent with the assumption made earlier, whereby a new critical incident in a new phase is considered more critical to the incident in the previous phases. To look at them closer, incidents detected in the 3rd phase were ranked at the top priority until the end of the scenario. Although there were new critical incidents (i.e. Bad Traffic Loopback IP) detected in the 5th phase, it was ranked lower than the critical incident in the 3rd phase because it was considered not critical enough in comparison. In this particular scenario, the result is consistent with the dataset because the incidents were considered failed (DARPA, 2011).

Furthermore, *Table 11* shows the partial results of Experiment 2 and it shows some significant changes compared to the result of Experiment 1. The results are slightly different because the experiment was performed with different weights of indicators. In general, Experiment 2 has shown some significant changes to the risk index value as well as the top priority ranking.

Table 10: Partial result of risk index and ranking for Experiment 1

							Time Interval																							
Phase	Incidents' Signature	No. of Incidents	Time		Risk Index		09:51:35		09:52:00		10:08:06		10:18:06		10:33:09		10:35:01		10:50:00		10:50:54		11:26:14		11:34:21		12:23:39		12:35:48	
			Min	Max	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High
Pre 1	FTP Bad login	1	09:32:34	09:32:34	0.3142	0.3142	1	1	4	4	4	4	114	114	114	114	149	149	149	149	149	149	153	153	153	153	153	153	153	153
1	**ICMP Echo Reply**	**20**	**09:51:36**	**09:52:00**	**0.0939**	**0.3542**			**65**	**2**	**86**	**2**	**317**	**66**	**321**	**66**	**385**	**95**	**413**	**95**	**423**	**95**	**435**	**99**	**1014**	**99**	**1042**	**99**	**1056**	**99**
	ICMP PING	**20**	**09:51:36**	**09:52:00**	**0.0942**	**0.3542**			**64**	**1**	**85**	**1**	**316**	**65**	**320**	**65**	**384**	**94**	**412**	**94**	**422**	**94**	**434**	**98**	**1013**	**98**	**1041**	**98**	**1055**	**98**
Pre 2	ATTACK-RESPONSES Invalid URL	1	09:52:10	09:52:10	0.1135	0.1135					84	84	315	315	315	315	376	376	398	398	408	408	415	415	422	422	450	450	464	464
	ATTACK-RESPONSES 403 Forbidden	2	09:54:45	09:58:36	0.1345	0.1345					83	82	311	310	311	310	372	371	392	391	396	395	401	400	408	407	412	411	414	413
2	**RPC portmap sadmind request UDP**	**76**	**10:08:07**	**10:18:05**	**0.0802**	**0.3412**							**329**	**68**	**333**	**68**	**397**	**103**	**425**	**103**	**435**	**103**	**447**	**107**	**1026**	**107**	**1054**	**107**	**1068**	**107**
	RPC portmap Solaris sadmin port query udp request	**76**	**10:08:07**	**10:18:05**	**0.2802**	**0.5412**							**141**	**1**	**141**	**1**	**184**	**7**	**184**	**7**	**188**	**7**	**192**	**7**	**196**	**7**	**196**	**7**	**196**	**7**
Pre 3	ATTACK-RESPONSES directory listing	4	10:22:43	10:31:30	0.1061	0.1061									319	316	380	377	408	405	418	415	430	427	437	434	465	462	479	476
3	**RPC portmap sadmind request UDP**	**14**	**10:33:10**	**10:34:59**	**0.1959**	**0.3462**											**267**	**97**	**267**	**97**	**271**	**97**	**275**	**101**	**282**	**101**	**282**	**101**	**282**	**101**
	RPC portmap Solaris sadmin port query udp request	**14**	**10:33:10**	**10:34:59**	**0.3959**	**0.5462**											**22**	**1**	**22**	**1**	**22**	**1**	**26**	**1**	**26**	**1**	**26**	**1**	**26**	**1**
	RPC sadmind query with root credentials attempt UDP	**14**	**10:33:10**	**10:34:59**	**0.1573**	**0.3076**											**357**	**150**	**357**	**150**	**361**	**150**	**365**	**154**	**372**	**154**	**374**	**154**	**376**	**154**
Pre 4	TELNET login incorrect	2	10:36:34	10:46:04	0.1361	0.1362													390	389	394	393	398	397	405	404	409	408	411	410
	ATTACK-RESPONSES 403 Forbidden	2	10:46:28	10:46:28	0.1315	0.1315													394	393	404	403	411	410	418	417	434	433	441	440
4	**RSERVICES rsh root**	**8**	**10:50:02**	**10:50:38**	**0.1334**	**0.2835**															**400**	**173**	**405**	**177**	**412**	**179**	**416**	**179**	**418**	**179**
	ATTACK-RESPONSES 403 Forbidden	2	10:50:15	10:50:54	0.1318	0.1323															402	401	409	408	416	415	420	419	427	426
Pre 5	TELNET login incorrect	1	11:00:11	11:00:11	0.1355	0.1355																	399	399	406	406	410	410	412	412
	ATTACK-RESPONSES Invalid URL	1	11:05:11	11:05:11	0.1116	0.1116																	416	416	423	423	451	451	465	465
5	**(snort decoder) Bad Traffic Loopback IP**	**572**	**11:27:51**	**11:27:56**	**0.0984**	**0.1027**																			**1012**	**441**	**1040**	**469**	**1054**	**483**
Post 5	TELNET login incorrect	4	11:39:07	12:33:25	0.1578	0.1702																					358	356	368	356

Table 11: Partial result of risk index and ranking for Experiment 2

							Time Interval																							
Phase	Incidents' Signature Num	No. of Incidents	Time		Risk Index		09:51:35		09:52:00		10:08:06		10:18:06		10:33:09		10:35:01		10:50:00		10:50:54		11:26:14		11:34:21		12:23:39		12:35:48	
			Min	Max	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High	Low	High
Pre 1	FTP Bad login	1	09:32:34	09:32:34	0.3135	0.3135	1	1	4	4	4	4	141	141	141	141	176	176	176	176	176	176	180	180	183	183	183	183	183	183
1	**ICMP Echo Reply**	**20**	**09:51:36**	**09:52:00**	**0.0950**	**0.3459**			**65**	**2**	**86**	**2**	**317**	**123**	**321**	**123**	**385**	**158**	**413**	**158**	**423**	**158**	**435**	**162**	**1014**	**165**	**1042**	**165**	**1056**	**165**
	ICMP PING	**20**	**09:51:36**	**09:52:00**	**0.0955**	**0.3459**			**64**	**1**	**85**	**1**	**316**	**122**	**320**	**122**	**384**	**157**	**412**	**157**	**422**	**157**	**434**	**161**	**1013**	**164**	**1041**	**164**	**1055**	**164**
Pre 2	ATTACK-RESPONSES Invalid URL	1	09:52:10	09:52:10	0.1177	0.1177					84	84	315	315	315	315	376	376	398	398	408	408	415	415	422	422	450	450	464	464
	ATTACK-RESPONSES 403 Forbidden	2	09:54:45	09:58:36	0.1531	0.1531					83	82	311	310	311	310	372	371	392	391	396	395	401	400	408	407	412	411	414	413
2	**RPC portmap sadmind request UDP**	**76**	**10:08:07**	**10:18:05**	**0.0891**	**0.3408**							**329**	**125**	**333**	**125**	**397**	**160**	**425**	**160**	**435**	**160**	**447**	**164**	**1026**	**167**	**1054**	**167**	**1068**	**167**
	RPC portmap Solaris sadmin port query udp request	**76**	**10:08:07**	**10:18:05**	**0.4041**	**0.6558**							**76**	**1**	**76**	**1**	**105**	**7**	**105**	**7**	**105**	**7**	**109**	**7**	**109**	**7**	**109**	**7**	**109**	**7**
Pre 3	ATTACK-RESPONSES directory listing	4	10:22:43	10:31:30	0.1086	0.1086									319	316	380	377	408	405	418	415	430	427	484	481	512	509	526	523
3	**RPC portmap sadmind request UDP**	**14**	**10:33:10**	**10:34:59**	**0.2195**	**0.3469**											**220**	**151**	**220**	**151**	**224**	**151**	**228**	**155**	**235**	**158**	**235**	**158**	**235**	**158**
	RPC portmap Solaris sadmin port query udp request	**14**	**10:33:10**	**10:34:59**	**0.5345**	**0.6619**											**22**	**1**	**22**	**1**	**22**	**1**	**22**	**1**	**22**	**1**	**22**	**1**	**22**	**1**
	RPC sadmind query with root credentials attempt UDP	**14**	**10:33:10**	**10:34:59**	**0.1826**	**0.3100**											**325**	**177**	**325**	**177**	**329**	**177**	**333**	**181**	**340**	**184**	**342**	**184**	**342**	**184**
Pre 4	TELNET login incorrect	2	10:36:34	10:46:04	0.1550	0.1552													390	389	394	393	398	397	405	404	409	408	411	410
	ATTACK-RESPONSES 403 Forbidden	2	10:46:28	10:46:28	0.1505	0.1505													394	393	404	403	411	410	418	417	422	421	424	423
4	**RSERVICES rsh root**	**8**	**10:50:02**	**10:50:38**	**0.1526**	**0.2797**															**400**	**185**	**405**	**189**	**412**	**192**	**416**	**192**	**418**	**194**
	ATTACK-RESPONSES 403 Forbidden	2	10:50:15	10:50:54	0.1507	0.1514															402	401	409	408	416	415	420	419	422	384
Pre 5	TELNET login incorrect	1	11:00:11	11:00:11	0.1540	0.1540																	399	399	406	406	410	410	412	412
	ATTACK-RESPONSES Invalid URL	1	11:05:11	11:05:11	0.1161	0.1161																	416	416	423	423	451	451	465	465
5	**(snort decoder) Bad Traffic Loopback IP**	**572**	**11:27:51**	**11:27:56**	**0.1036**	**0.1090**																			**1012**	**434**	**1040**	**462**	**1054**	**476**
Post 5	TELNET login incorrect	4	11:39:07	12:33:25	0.1733	0.1890																					329	327	377	327

To look closer, *Table 12* summarises the comparison between them. The table summarises the incidents by grouping them into similar types of signatures with the number of incidents, the time when the incident was detected (i.e. min and max), the risk indexes and ranking of the related incidents. For the risk index and ranking, the table only shows the lowest and highest values for both experiments: E1 represents Experiment 1 and E2 represents Experiment 2. As mentioned earlier, there were some significant changes to the risk index value as well as some of the top priority rankings. For example, the top priority incidents for both experiments were still in the same position. This scenario can be seen in the "*RPC portmap Solaris sadmin port query udp request"* and the "*RPC portmap Solaris sadmin port query udp portmapper sadmin port query attempt*" incidents.

Table 12: Risk index and ranking comparison

Incidents' Signature Name	No. of Incidents	Time		Risk Index				Ranking			
		Min	Max	Low		High		Low		High	
				E1	E2	E1	E2	E1	E2	E1	E2
ATTACK-RESPONSES directory listing	20	09:29:20	11:03:33	0.1061	0.1083	0.1725	0.1956	482	573	329	323
FTP Bad login	1	09:32:34	09:32:34	0.3142	0.3135	0.3142	0.3135	153	183	153	183
TELNET login incorrect	17	09:32:34	12:33:25	0.1302	0.1484	0.2865	0.2828	447	427	175	190
ATTACK-RESPONSES Invalid URL	4	09:37:05	12:23:39	0.1116	0.1161	0.1442	0.1650	465	465	404	401
ATTACK-RESPONSES 403 Forbidden	12	09:45:34	12:31:13	0.1186	0.1252	0.1429	0.1633	463	463	405	403
ICMP Echo Reply	**72**	**09:45:37**	**12:26:16**	**0.0939**	**0.0950**	**0.3542**	**0.3459**	**1056**	**1056**	**99**	**165**
ICMP PING	**72**	**09:45:37**	**12:26:16**	**0.0942**	**0.0955**	**0.3542**	**0.3459**	**1055**	**1055**	**98**	**164**
ICMP Destination Unreachable Port Unreachable	76	10:08:07	11:04:13	0.2100	0.2402	0.5067	0.5292	211	211	14	35
RPC portmap sadmind request UDP	**90**	**10:08:07**	**10:34:59**	**0.0802**	**0.0891**	**0.3462**	**0.3469**	**1068**	**1068**	**101**	**158**
RPC portmap Solaris sadmin port query udp request	**90**	**10:08:07**	**10:34:59**	**0.2802**	**0.4041**	**0.5462**	**0.6619**	**196**	**109**	**1**	**1**
RPC portmap Solaris sadmin port query udp portmapper sadmin port query attempt	**14**	**10:33:10**	**10:34:59**	**0.3799**	**0.5178**	**0.5303**	**0.6452**	**73**	**73**	**8**	**8**
RPC sadmind query with root credentials attempt UDP	**14**	**10:33:10**	**10:34:59**	**0.1573**	**0.1826**	**0.3076**	**0.3100**	**376**	**342**	**154**	**184**
SQL version overflow attempt	1	10:34:57	10:34:57	0.4679	0.5386	0.4679	0.5386	18	14	18	14
RSERVICES rsh root	**8**	**10:50:02**	**10:50:38**	**0.1334**	**0.1526**	**0.2835**	**0.2797**	**418**	**418**	**179**	**192**
(snort decoder) Bad Traffic Loopback IP	**572**	**11:27:51**	**11:27:56**	**0.0984**	**0.1036**	**0.1027**	**0.1090**	**1054**	**1054**	**483**	**476**
SNMP AgentX/tcp request	3	11:27:54	11:27:55	0.2349	0.3592	0.2366	0.3614	199	157	197	155
ICMP PING *NIX	1	11:28:18	11:28:18	0.2811	0.2739	0.2811	0.2739	184	199	184	199
ICMP PING BSDtype	1	11:28:18	11:28:18	0.2811	0.2739	0.2811	0.2739	183	198	183	198

To extend the evaluation, the next set of experiments considers the changes to the risk index over time. Using E2 as the result for the comparison study,

Table 13 compares the rank position for selected incidents. The new position for each incident was ranked with the second set of experiments, where the incident risk indexes were updated dynamically. The old position for each incident was extracted from *Table 10* and *Table 11.* When comparing the position of the incidents, the majority of them were influenced. For example, the position of the *CID 4* incident changed from the old position of 183rd to the new position of 158th due to the changes of the risk index (i.e. 0.3135 to 0.3139); this trend is consistent with the other incidents.

Table 13: Position for critical incidents between two different studies

		Time Interval											
Incident ID		**09:51:35**	**09:52:00**	**10:08:06**	**10:18:06**	**10:33:09**	**10:35:01**	**10:50:00**	**10:50:54**	**11:26:14**	**11:34:21**	**12:23:39**	**12:35:48**
CID 4	Risk Index	0.3135	0.2954	0.2935	0.2862	0.2869	0.2875	0.2886	0.2888	0.2899	0.3147	0.3140	0.3139
	Position	1	4	4	141	141	182	182	182	186	158	158	158
	Old Position	1	4	4	141	141	176	176	176	180	183	183	183
CID 52	Risk Index		0.3459	0.3410	0.3325	0.3315	0.3320	0.3305	0.3287	0.3276	0.2844	0.2855	0.2859
	Position		1	2	124	124	159	159	159	163	188	184	184
	Old Position		3	3	124	124	159	159	159	163	166	166	166
CID 88	Risk Index				0.6558	0.6547	0.6615	0.6562	0.6542	0.6527	0.6037	0.6031	0.6028
	Position				1	1	7	7	7	7	5	7	7
	Old Position				1	1	7	7	7	7	7	7	7
CID 353	Risk Index						0.6619	0.6565	0.6546	0.6531	0.6038	0.6032	0.6029
	Position						1	1	2	1	3	5	5
	Old Position						1	1	1	1	1	1	1
CID 428	Risk Index								0.2797	0.2796	0.2856	0.2851	0.2849
	Position								188	191	185	187	187
	Old Position								187	191	194	194	194

Table 14: Snort Priority, CVSS v2 Base Score, Exploitability Subscore and Risk Index

						Risk Index			
						Low		High	
Incidents' Signature Name	**Snort Priority**	**CVE ID**	**CVSS v2 Base Score**	**Exploitability Subscore**	**No. of Incidents**	**E1**	**E2**	**E1**	**E2**
ATTACK-RESPONSES directory listing	2	-	-	-	20	0.1061	0.1083	0.1725	0.1956
FTP Bad login	2	-	-	-	1	0.3142	0.3135	0.3142	0.3135
TELNET login incorrect	2	-	-	-	17	0.1302	0.1484	0.2865	0.2828
ATTACK-RESPONSES Invalid URL	2	-	-	-	4	0.1116	0.1161	0.1442	0.1650
ATTACK-RESPONSES 403 Forbidden	2	-	-	-	12	0.1186	0.1252	0.1429	0.1633
ICMP Echo Reply	**3**	**-**	**-**	**-**	**72**	**0.0939**	**0.0950**	**0.3542**	**0.3459**
ICMP PING	**3**	**-**	**-**	**-**	**72**	**0.0942**	**0.0955**	**0.3542**	**0.3459**
ICMP Destination Unreachable Port Unreachable	3	CVE-2005-0068	5	10	76	0.2100	0.2402	0.5067	0.5292
RPC portmap sadmind request UDP	**2**	**-**	**-**	**-**	**90**	**0.0802**	**0.0891**	**0.3462**	**0.3469**
RPC portmap Solaris sadmin port query udp request	**2**	**CVE-2003-0722**	**10**	**10**	**90**	**0.2802**	**0.4041**	**0.5462**	**0.6619**
RPC portmap Solaris sadmin port query udp portmapper sadmin port query attempt	**2**	**CVE-2003-0722**	**10**	**10**	**14**	**0.3799**	**0.5178**	**0.5303**	**0.6452**
RPC sadmind query with root credentials attempt UDP	**2**	**-**	**-**	**-**	**14**	**0.1573**	**0.1826**	**0.3076**	**0.3100**
SQL version overflow attempt	1	CVE-2002-0649	8	10	1	0.4679	0.5386	0.4679	0.5386
RSERVICES rsh root	**1**	**-**	**-**	**-**	**8**	**0.1334**	**0.1526**	**0.2835**	**0.2797**
(snort decoder) Bad Traffic Loopback IP	**2**	**-**	**-**	**-**	**572**	**0.0984**	**0.1036**	**0.1027**	**0.1090**
SNMP AgentX/tcp request	2	CVE-2002-0013	10	10	3	0.2349	0.3592	0.2366	0.3614
ICMP PING *NIX	3	-	-	-	1	0.2811	0.2739	0.2811	0.2739
ICMP PING BSDtype	3	-	-	-	1	0.2811	0.2739	0.2811	0.2739

The experimental results are encouraging as the majority of true and critical incidents received a high ranking. The proposed method was further validated by comparing the experimental results with the Snort Priority and the CVSS v2 Base Score, as tabulated in

Table 14. The first column in the table is the type of incident, which is followed by the Snort Priority, as obtained directly by Snort IDS. The next three columns are the CVE-ID, CVSS v2 Base Score and exploitability sub score which were taken directly from the National Vulnerability Database (NIST, 2011). The last four columns are the experimental results that were directly taken from *Table 12*.

The experimental results show that the approach in this study is better than the Snort Priority and CVSS v2 Base Score in terms of its results. All incidents were 100% successfully rated in this study and produced risk indexes between 0 and 1. In comparison, it seems that the result have shown a significant improvement because the CVSS v2 Base Score can rate only 17.23% or 184 out of 1068 incidents.

Furthermore, the ranking approach performed in this study is better than the Snort Priority because the latter prioritises incidents only into several groups, specifically three. To look at them closer*, Figure 2* plots the distribution of incidents. For example, there were 72 incidents for the "*ICMP Echo reply*" and the Snort Priority labelled all of them as a low priority or three within the same groups. However, in Experiment 1, the risk indexes given were between 0.0939 and 0.3542. The different risk indexes between the incidents allow security analysts to rank and prioritise incidents more effectively. This limitation of the group priority can also be seen with the CVSS and can be seen clearly between *Table 12* and

Table 14.

Furthermore, the result in this study has shown some improvement. In particular, the incident in the 5^{th} phase is rated with a low rating and the same time ranked it at a suitable position and placed it better compared to the results by Alsubhi *et al.* (2008). In contrast, their model gave a very high score for the incidents, although they were considered as failed incidents.

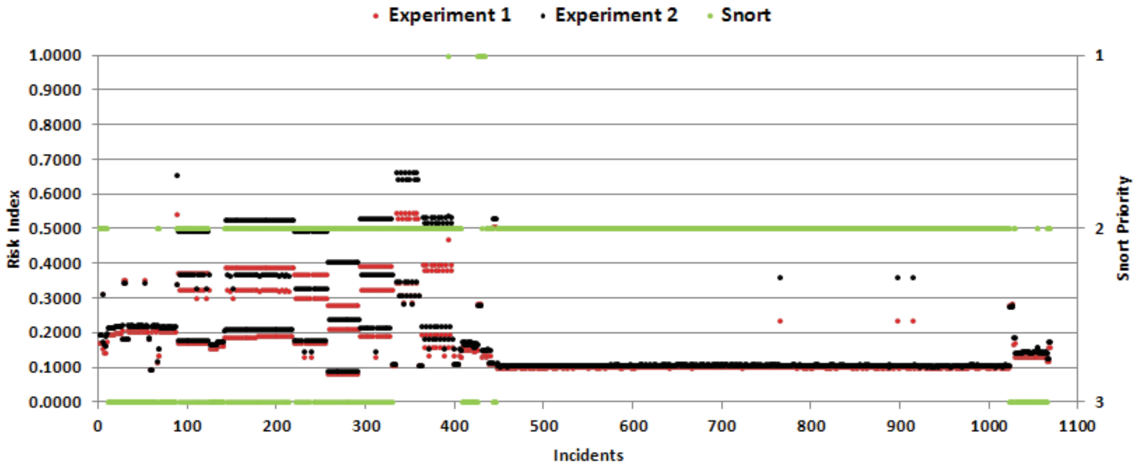

Figure 2: Experiment 1, Experiment 2 and Snort Priority

CONCLUSION AND FUTURE WORK

The study highlighted some significant findings in incident prioritisation. The experiments identified different risk indexes using similar and different weights of indicators. The different weights used by the indicator showed some significant changes in risk indexes as well as the position of incidents. In addition, comparison studies have been made to compare Snort Priority and CVSS in order to investigate the model improvement. The result has shown an improvement upon the comparison. Furthermore, the study also highlighted the effect of the changes of risk indexes over time and the incidents' position, where the majority of them were influenced.

In conducting the experiments, this study found some limitations. The experiment used assumptions to derive the values in estimating the risk index, particularly in rating the value of assets. Future work should focus on strengthening the estimation process for rating every indicator which is involved in the model. It is suggested to extend the indicator by giving a precise and detailed metric for measuring incidents, especially in reducing uncertainty amongst indicators. Furthermore, this study did not discuss the performance of the process, as the prioritisation process may induce an overhead in estimating the risk index. However, based on the preliminary results which can be simulated within a few seconds, it is estimated that the effect will be less. The result has provided a clear distinction between the ways in which incidents are rated and ranked. However, the experiments do not consider any countermeasures or responses to control the critical incident. With the promising results, we intend to investigate a response strategy that can work with the RIM in selecting appropriate responses for incidents with different ranks and priorities.

ACKNOWLEDGEMENT

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

Abedin, M., Nessa, S., Al-Shaer, E. and Khan, L. (2006), "Vulnerability analysis for evaluating quality of protection of security policies", *Proceedings of the 2nd ACM workshop on Quality of protection*, Alexandria, Virginia, USA, pp. 49-52.

Ahmed, M.S., Al-Shaer, E. and Khan, L. (2008), "A Novel Quantitative Approach For Measuring Network Security", *Proceedings of the 27th IEEE Conference on Computer Communications (INFOCOM 2008)*, pp. 1957-1965.

Alsubhi, K., Al-Shaer, E. and Boutaba, R. (2008), "Alert prioritization in intrusion detection systems", *Proceedings of the IEEE Network Operations and Management Symposium*, Salvador, Brazil, pp. 33-40.

Årnes, A., Sallhammar, K., Haslum, K., Brekne, T., Moe, M.E.G. and Knapskog, S.J. (2005), "Real-time risk assessment with network sensors and intrusion detection systems", *Proceedings of the International Conference on Computational Intelligence and Security*, Vol. 3802, Xian, China, pp. 388-397.

Årnes, A., Valeur, F., Vigna, G. and Kemmerer, R. (2006), "Using Hidden Markov Models to Evaluate the Risks of Intrusions: System Architecture and Model Validation", *Proceedings of the International Symposium on Recent Advances in Intrusion Detection (RAID)*, pp. 145–164.

Aussibal, J. and Gallon, L. (2008), "A New Distributed IDS Based on CVSS Framework", *Proceedings of the IEEE International Conference on Signal Image Technology and Internet Based Systems (SITIS '08)*, pp. 701-707.

Caswell, B. and Beale, J. (2004), "*Snort 2.1 Intrusion Detection",* 2nd edition, Syngress.

Caswell, B. and Roesch, M. (1998), "Snort: The open source network intrusion detection system", Available at: http://www.snort.org (Accessed: 20 August 2010).

Clark, J.W. and Stavrou, A. (2011), "Breaching & Protecting an Anonymizing Network System", *Proceedings of the 6th Annual Symposium on Information Assurance*, New York, USA, pp. 32-44.

DARPA (2011), "DARPA Intrusion Detection Data Sets", Available at: http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/index.html (Accessed: 1 July 2011).

Davis, C., Schiller, M. and Wheeler, K. (2007), "*IT Auditing: Using Controls to Protect Information Assets",* McGraw-Hill.

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

Ekelhart, A., Fenz, S. and Neubauer, T. (2009), "AURUM: A Framework for Information Security Risk Management", *Proceedings of the 42nd Hawaii International Conference on System Sciences*, pp. 1-10.

Fenz, S. and Neubauer, T. (2009), "How to determine threat probabilities using ontologies and Bayesian networks", *Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies*, Oak Ridge, Tennessee.

Gregg, M. and Kim, D. (2005), "*Inside Network Security Assessment: Guarding your IT Infrastructure",* Sams.

Haslum, K., Abraham, A. and Knapskog, S. (2007), "DIPS: A Framework for Distributed Intrusion Prediction and Prevention Using Hidden Markov Models and Online Fuzzy Risk Assessment", *Proceedings of the Third International Symposium on Information Assurance and Security*, Trondheim, Norway, pp. 183-190.

Haslum, K. and Årnes, A. (2007), "Multisensor Real-Time Risk Assessment Using Continuous-Time Hidden Markov Models", *Proceedings of the International Conference on Computational Intelligence and Security*, Vol. 4456, Guangzhou, China, pp. 694-703.

Hausrath, N.L. (2011), "*Methods for Hospital Network and Computer Security"*. M.Sc. University of Cincinnati.

Heyman, T., Scandariato, R., Huygens, C. and Joosen, W. (2008), "Using Security Patterns to Combine Security Metrics", *Proceedings of the Third International Conference on Availability, Reliability and Security (ARES 08)*, pp. 1156-1163.

Houmb, S.H. and Franqueira, V.N.L. (2009), "Estimating ToE Risk Level Using CVSS", *Proceedings of the International Conference on Availability, Reliability and Security (ARES '09)*, pp. 718-725.

Houmb, S.H., Franqueira, V.N.L. and Engum, E.A. (2009), "Quantifying security risk level from CVSS estimates of frequency and impact", *Journal of Systems and Software*, Vol. 83. No. 9, pp. 1622-1634.

Kheir, N., Cuppens-Boulahia, N., Cuppens, F. and Debar, H. (2010), "A service dependency model for cost-sensitive intrusion response", *Proceedings of the 15th European Conference on Research in Computer Security*, pp. 626-642.

Lai, Y.P. and Hsia, P.L. (2007), "Using the vulnerability information of computer systems to improve the network security", *Computer Communications*, Vol. 30 No. 9, pp. 2032-2047.

Lee, W., Fan, W., Miller, M., Stolfo, S.J. and Zadok, E. (2002), "Toward cost-sensitive modeling for intrusion detection and response", *Journal of Computer Security*, Vol. 10 No. 1-2, pp. 5-22.

Lee, W. and Qin, X. (2003), "Statistical causality analysis of INFOSEC alert data", *Proceedings of the Recent Advances in Intrusion Detection*, Vol. 2820/2003, pp. 73-93.

Lin, C.H., Chen, C.H. and Laih, C.S. (2008), "A Study and Implementation of Vulnerability Assessment and Misconfiguration Detection", *Proceedings of the IEEE Asia-Pacific Services Computing Conference (APSCC '08)*, pp. 1252-1257.

Mell, P., Scarfone, K. and Romanosky, S. (2006), "Common Vulnerability Scoring System", *IEEE Security & Privacy*, Vol. 4 No. 6, pp. 85-89.

Mu, C.P., Li, X.J., Huang, H.K. and Tian, S.F. (2008), "Online Risk Assessment of Intrusion Scenarios Using D-S Evidence Theory", *Proceedings of the 13th European Symposium on Research in Computer Security*, Malaga, Spain, pp. 35-48.

Munteanu, A.B. (2006), "Information Security Risk Assessment: The Qualitative Versus Quantitative Dilemma", *Proceedings of the 6th International Business Information Management Association (IBIMA) Conference*, pp. 227-232.

Nicol, D.M., Sanders, W.H. and Trivedi, K.S. (2004), "Model-based evaluation: from dependability to security", *IEEE Transactions on Dependable and Secure Computing,*, Vol. 1 No. 1, pp. 48-65.

Ning, P., Cui, Y., Reeves, D.S. and Xu, D. (2004), "Techniques and tools for analyzing intrusion alerts", *ACM Transactions on Information System Security*, Vol. 7 No. 2, pp. 274-318.

NIST (2011), "National Vulnerability Database version 2.0", Available at: http://nvd.nist.gov/ (Accessed: 1 April 2011).

Noel, S. and Jajodia, S. (2008), "Optimal IDS Sensor Placement and Alert Prioritization Using Attack Graphs", *Journal of Network and Systems Management*, Vol. 16 No. 3, pp. 259-275.

Pak, C. and Cannady, J. (2009), "Asset priority risk assessment using hidden markov models", *Proceedings of the 10th ACM conference on SIG-information technology education*, Fairfax, Virginia, USA, pp. 65-73.

Porras, P.A., Fong, M.W. and Valdes, A. (2002), "A mission-impact-based approach to INFOSEC alarm correlation", *Recent Advances in Intrusion Detection*, Vol. 2516, pp. 95-114.

Rogers, R., Fuller, E., Miles, G. and Cunningham, B. (2005), "*Network Security Evaluation Using the NSA IEM ",* Syngress

Saaty, T.L. (2008a), "Decision making with the analytic hierarchy process", *International Journal of Services Sciences*, Vol. 1 No. 1, pp. 83-98.

Saaty, T.L. (2008b), "Relative Measurement and Its Generalization in Decision Making Why Pairwise Comparisons are Central in Mathematics for the Measurement of Intangible Factors The Analytic Hierarchy/Network Process", *RACSAM. Rev. R. Acad. Cien. Serie A. Mat*, Vol. 102 No. 2, pp. 251-318.

Savola, R.M. and Abie, H. (2009), "Identification of Basic Measurable Security Components for a Distributed Messaging System", *Proceedings of the Third International Conference on Emerging Security Information, Systems and Technologies (SECURWARE '09)*, pp. 121-128.

Strasburg, C., Stakhanova, N., Basu, S. and Wong, J.S. (2009), "Intrusion response cost assessment methodology", *Proceedings of the 4th International Symposium on Information, Computer, and Communications Security*, Sydney, Australia, pp. 388-391.

Subramanian, D., Le, H.T. and Loh, P.K.K. (2009), "Fuzzy Heuristic Design for Diagnosis of Web-Based Vulnerabilities", *Proceedings of the Fourth International Conference on Internet Monitoring and Protection (ICIMP '09)*, pp. 103-108.

Symantec (2011), *"Symantec Internet Security Threat Report - Trends for 2010"*. Available at: http://www.symantec.com/business/threatreport/index.jsp (Accessed: 16 July 2011).

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

Valdes, A. and Skinner, K. (2001), "Probabilistic Alert Correlation", *Proceedings of the 4th International Symposium on Recent Advances in Intrusion Detection*, pp. 54-68.

Wang, C. and Wulf, W.A. (1997), "Towards A Framework for Security Measurement", *Proceedings of the 20th National Information Systems Security Conference, Baltimore, MD*, pp. 522-533.

Xiao, S.S., Zhang, Y.G., Liu, X.J. and Gao, J.J. (2008), "Alert Fusion Based on Cluster and Correlation Analysis", *Proceedings of the International Conference on Convergence and Hybrid Information Technology*, Daejeon, South Korea, pp. 163-168.

Xu, D. and Ning, P. (2005), "Privacy-preserving alert correlation: a concept hierarchy based approach", *Proceedings of the 21st Annual Computer Security Applications Conference*, pp. 537-546.

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.

Zahedi, F. (1986), "The Analytic Hierarchy Process: A Survey of the Method and Its Applications", *Interfaces*, Vol. 16 No. 4, pp. 96-108.

Zhang, Z., Ho, P. and He, L. (2009), "Measuring IDS-estimated attack impacts for rational incident response: A decision theoretic approach", *Computers & Security*, Vol. 28 No. 7, pp. 605-614.

Zhang, Z., Lin, X. and Ho, P.H. (2007), "Measuring Intrusion Impacts for Rational Response: A State-based Approach", *Proceedings of the Second International Conference on Communications and Networking in China (CHINACOM '07)*, pp. 317-321.