A Response Strategy Model for Intrusion Response Systems

Nor Anuar, Maria Papadaki, Steven Furnell, Nathan Clarke

A Response Strategy Model for Intrusion Response Systems

Nor Badrul Anuar[1,2], Maria Papadaki[1], Steven Furnell[1,3], Nathan Clarke[1,3]

[1]Centre for Security, Communications and Network Research (CSCAN), Plymouth University, United Kingdom
info@cscan.org
[2]Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur, Malaysia
badrul@um.edu.my
[3]School of Computer and Security Science, Edith Cowan University, Perth, Western Australia

Abstract. There are several types of security systems, which focus on detecting, mitigating and responding to incidents. Current response systems are largely based on manual incident response selection strategies, which can introduce delays between detection and response time**.** However, it would be beneficial if critical and urgent incidents are addressed as soon as possible before they jeopardised critical systems. As a result, the Risk Index Model (RIM) has been proposed earlier in our previous study, as a method of prioritising incidents based upon two decision factors namely impact on assets and likelihood of threat and vulnerability. This paper extends RIM by using it as the basis for mapping incidents with various response options. The proposed mapping model, Response Strategy Model (RSM) is based on risk response planning and time management concepts and it is evaluated using the DARPA 2000 dataset. The case study analysis upon the dataset has shown a significant result in mapping incident into different quadrants. In particular, the results have shown a significant relationship between the incident classification with incident priorities where false incidents are likely to be categorised as low priority incidents and true incidents are likely to be categorised as the high priority incident.

Keywords:intrusion response systems, risk response planning, response strategy model

1 Introduction

At present, there are several types of security systems like Intrusion Detection Systems (IDSs), Intrusion Prevention Systems (IPSs) and Intrusion Response Systems (IRSs), which focus on detecting, mitigating and responding to incidents. There are many well-known and widely-recognised response options in mitigating incidents such as blocking traffic, terminating user and notifying system administrators. Therefore, to mitigate incidents effectively, it is important to have a proper response strat-

egy in place, in order to minimise the delay between detection and response. Hence, an automated approach is preferred. To illustrate the importance of timely response, [1] highlights that the longer the delay between detection and response, the higher the attack success rate is. Therefore, it is important that critical and urgent incidents are addressed as soon as possible before critical systems are jeopardised.

The paper is organised as follows. Section 2 presents the related works that have had significant impact to this paper. Section 3 presents the proposed response strategy model. Section 4 presents a case study to illustrate how the model can be used.Finally, the last section concludes the paper.

2 Related work

There are two types of decision-making models in response selection; a static and a dynamic mapping [2]. To mitigate incidents, the dynamic mapping provides more efficient results in comparison to the static mapping. In addition to the dynamic mapping in a response model, different response strategies are adopted, such as response goal strategy [2, 3], response stopping power [4] and adaptive response strategy [5, 6].

An article in [3] proposed a response goal strategy where a sequence of actions (also called subtasks) is arranged to achieve a specific goal. One or multiple goals need to be selected from the list and normally the selection of them is done manually by security analysts. Similarly with [3], a proposal in [2] developed an automated intrusion response system by adopting the hierarchical task network planning approach in their response decision-making model. An approach in [4] used a rule based module to identify the most appropriate response characteristics based on a Response Policy. The policy aimed to determine the most appropriate Response Phases and it is similar to the response goals used in [3]. Furthermore, the cost-sensitive model proposed in [5] applied an adaptive response strategy and updated response options based upon the status of the previous triggered response and the value of cost as a decision factor. Their approach closely follows the approach proposed in [6].

This paper proposes an alternative approach by considering risk assessment as decision factors in Risk Index Model [7], risk response planning as well as time management concept in improving the timeliness of response. In addition, this paper improves the response strategy by grouping incidents into a similar group based on their priority and it also allows a simultaneous response. With a static policy with a dynamic decision-making, the proposed model reduces the delay problem upon making an appropriate decision and response; hence it is more suitable and practical to be applied in live traffic network with online monitoring systems.

3 Response Strategy Model (RSM)

This paper presents Response Strategy Model (RSM) which can be used as an alternative to the existing model that applied a dynamic response mapping model. The model creates a relationship between incidents and different types of response option with different levels of priority. Based upon attack metrics and system states as decision

factors proposed in the earlier proposal in [7], this paper uses an alternative approach in exclusively mapping an appropriate response option with an appropriate incident by considering risk response planning and a time management concept in addressing the importance of response time. In addition, this paper proposes the response strategy by grouping incidents into a similar group based on their priority and it also allows for a simultaneous response.

The time management concept applied in RSM aims to create effective responses to critical incidents. In time management concepts, [8] presents four categories of tasks which are mapped onto four different quadrants; Q1: important and urgent, Q2: important but not urgent, Q3: not important but urgent, and Q4: not important and not urgent. However, in order to fit with the model, this paper modifies the quadrant to address the time management in responding to incidents. Instead of using "important", this paper uses "critical" to show the relationship between time and impacts; therefore, the new quadrants consider the combination between urgent and critical incidents. The quadrants for the time management concept contain four different quadrants as tabulated in Table 1.

In order to establish a strategic RSM, this paper uses the risk response planning concept. It contains four different strategies: avoidance, transfer, mitigation and acceptance. According to [9], the risk response planning can be prioritised where avoidance can be the first option followed by transfer, mitigation and acceptance. With the response categorisation proposed by our study in [10], Table 1 shows the relationship map between them and their correspondent quadrants as well as some related examples for their response options.

Table 1. Response Strategy Planning with Response options

Risk Response Planning (Threshold)	**Quadrants**	**Response options**
Avoidance (0.75-1.00)	1st Quadrant: Urgent incident and for a critical asset	• Block users, processes or network traffic in preventing future attacks. • Adjust users, processes or network traffic configuration in minimising impacts but maintain system's performances.
Mitigation (0.50-0.75)	2nd Quadrant: Not an urgent incident but for a critical asset	• Collaborate with other appliances by limiting users, processes or network traffic for delaying the process of attacks (Example: using access control, firewall, enabling other countermeasures or antivirus). • Terminate users, processes or network traffic in preventing continuous attacks (Example: locking OS, resetting connection, dropping user and kill-

		ing process).
Transfer (0.25-0.50)	3rd Quadrant: Urgent incident but for a noncritical asset	• Collect information about incidents for passive responses, proactive responses as well as forensic evidence (Example: trace connections, decoy systems, honeypots, forensic evidence, recovery, incidents' blacklisting and white listing). • Escalate to administrator for a further investigation (Example: attack verification, damage recovery and assessment).
Acceptance (0.00-0.25)	4th Quadrant: Not an urgent incident and not for a critical asset	• Establish passive responses like enabling a notification via syslog, console alert, email, pager, PDA or mobile.

4 Case Study

In order to investigate the effectiveness of the proposed model, this paper discusses one case study and aims to satisfy two goals. Firstly, the case study used to investigate the distribution of incidents using RSM in comparison with other approaches like CVSS v2 [11] and Snort Priority [12]. Secondly, the case studies used to investigate the relationship between the response strategies and its ability to differentiate between true and false incidents in the classification of incidents. The case study were conducted using the MIT 2000 DARPA (i.e. LLDOS 1.0) intrusion detection data set [13]. In order to further discuss the case study, this paper uses the incident rating results from a prioritisation model,Risk Index Model (RIM) [7] and also use the rating threshold as in Table 1.

4.1 Case study results

Table 2 shows the distribution of incidents using the DARPA dataset. It contains 1,068 incidents. The first column on the left refers to the phases of the dataset and is followed by the total of incidents. The incidents are divided into two classes of incidents: true and false incidents. The other columns summarise the percentage of incidents with regards to specific rows; either they are true or false incidents. The distribution is separated between Snort Priority, CVSS v2 and the Response Strategy Model. The Snort Priority is divided into 3 different priorities which are high, medium and low. With CVSS v2, there are three main categories and there are high, medium and low. The last column is an additional column and it refers to incidents without priority. Response Strategy Model (RSM) divides its priority into four quadrants, including avoidance, mitigation, transfer and acceptance.

In general, a total of 904 incidents or 84.64% of incidents are considered as true incidents and this includes critical incidents as well as non-critical incidents. Only 15.36% or 164 incidents are considered as false incidents. As can be seen in the table, there is a clear distribution between true and false incidents. With RSM, an average of 92.68% of the false incidents was prioritised as the lowest quadrant in the acceptance strategy column. This percentage is better compared to only 67.07% of the false incidents being prioritised under low priority with Snort Priority.

Table 2. With the DARPA datasets

Phase	Time	No. of Incidents	Type	No. of Incidents	Snort Priority			CVSS v2			Response Strategy Model				
					High	Medium	Low	High	Medium	Low	None	Avoidance	Mitigation	Transfer	Acceptance
Pre 1	09:21:36 - 09:51:35	25	TRUE	-	-	-	-	-	-	-	-	-	-	-	-
			FALSE	25	-	36.00%	64.00%	-	-	-	100.00%	-	-	**4.00%**	**96.00%**
1	09:51:36 - 09:52:00	40	TRUE	40	-	-	100.00%	-	-	-	100.00%	-	-	**7.50%**	**92.50%**
			FALSE	-	-	-	-	-	-	-	-	-	-	-	-
Pre 2	09:52:01 - 10:08:06	21	TRUE	-	-	-	-	-	-	-	-	-	-	-	-
			FALSE	21	-	14.29%	85.71%	-	-	-	100.00%	-	-	-	**100.00%**
2	10:08:07 - 10:18:05	243	TRUE	224	-	67.86%	32.14%	33.93%	32.14%	-	33.93%	-	**17.86%**	**43.30%**	**38.84%**
			FALSE	19	-	15.79%	84.21%	-	-	-	100.00%	-	-	-	**100.00%**
Pre 3	10:18:06 - 10:33:09	4	FALSE	4	-	100.00%	-	-	-	-	100.00%	-	-	-	**100.00%**
3	10:33:10 - 10:35:01	64	TRUE	60	-	100.00%	-	46.67%	-	-	53.33%	-	**46.67%**	**23.33%**	**30.00%**
			FALSE	4	25.00%	75.00%	-	25.00%	-	-	75.00%	-	-	-	**100.00%**
Pre 4	10:35:02 - 10:50:00	28	TRUE	-	-	-	-	-	-	-	-	-	-	-	-
			FALSE	28	-	35.71%	64.29%	-	-	-	100.00%	-	-	-	**100.00%**
4	10:50:01 - 10:50:54	10	TRUE	8	100.00%	-	-	-	-	-	100.00%	-	-	**50.00%**	**50.00%**
			FALSE	2	-	100.00%	-	-	-	-	100.00%	-	-	-	**100.00%**
Pre 5	10:50:55 - 11:26:14	12	TRUE	-	-	-	-	-	-	-	-	-	-	-	-
			FALSE	12	-	66.67%	33.33%	-	33.33%	-	66.67%	-	-	**33.33%**	**66.67%**
5	11:26:15 - 11:34.21	579	TRUE	572	-	100.00%	-	-	-	-	100.00%	-	-	-	**100.00%**
			FALSE	7	-	42.86%	57.14%	42.86%	-	-	57.14%	-	-	**100.00%**	-
Post 5	11:34:22 - 12:35:48	42	TRUE	-	-	-	-	-	-	-	-	-	-	-	-
			FALSE	42	-	19.05%	80.95%	-	-	-	100.00%	-	-	-	**100.00%**
Total	09:21:36 - 12:35:48	1068	TRUE	904	0.88%	86.73%	12.39%	11.50%	7.97%	-	80.53%	-	**7.52%**	**13.05%**	**79.43%**
			FALSE	164	0.61%	32.32%	67.07%	2.44%	2.44%	-	95.12%	-	-	**7.32%**	**92.68%**

There is a huge percentage or 79.43% of true incidents identified under the acceptance quadrant and this figure can be considered as misclassification, as in the ideal situation a true incident should be classified under the first or second quadrant. However, this percentage clearly shows that those true incidents are not really critical; therefore it is acceptable to be considered under that quadrant. The results are also consistent with the DARPA dataset where most of the true incidents were identified as failed incidents, especially in the last main phase.

Furthermore, the distribution of true incidents using RSM is better compared to Snort Priority and CVSS v2. To look at them closer, in the 3rd phase, the true incidents were prioritised into three different groups using RSM compared to only one group with Snort Priority. In this case, the distribution allows any automated response systems to initiate multiple actions on incidents. This means incidents will have different types of response depending on their criticality and priority.

5 Conclusion

The results presented in the previous section are encouraging, as the Risk Index Model (RIM) works well with the Response Strategy Model (RSM) by mapping all incidents into their appropriate quadrants. The model has also shown a significant result in mapping between the quantitative indexes with the qualitative group of pri-

orities. In addition, the results presented have shown a significant relationship between incident priorities and their classification. The case studies in this stage have shown a significant relationship in addressing false and true incidents.

6 References

1. Cohen, F.: Simulating cyber attacks, defences, and consequences. Computers & Security. 18(6), 479-518 (1999)
2. Mu, C. and Li, Y.: An intrusion response decision-making model based on hierarchical task network planning. Expert Systems with Applications. 37(3), 2465-2472 (2010)
3. Carver, C.A.: Adaptive Agent-Based Intrusion Response. PhD Dessertation. Texas A&M University (2001)
4. Papadaki, M. and Furnell, S.M.: Informing the decision process in an automated intrusion response system. Information Security Technical Report. 10(3), 150-161 (2005)
5. Stakhanova, N., Basu, S., and Wong, J.: A Cost-Sensitive Model for Preemptive Intrusion Response Systems. In: 21st International Conference on Advanced Information Networking and Applications (AINA '07). pp. 428-435. Niagara Falls, Canada (2007)
6. Foo, B., Wu, Y.S., Mao, Y.C., Bagchi, S., and Spafford, E.: ADEPTS: adaptive intrusion response using attack graphs in an e-commerce environment. In: International Conference on Dependable Systems and Networks (DSN 2005). pp. 508-517. Yokohama, Japan (2005)
7. Anuar, N.B., Furnell, S., Papadaki, M., and Clarke, N.: A Risk Index Model for Security Incident Prioritisation. In: 9th Australian Information Security Management Conference. pp. 25-39. Perth, Australia (2011)
8. Covey, S.R.: 7 Habits of Highly Effective People, 15th Anniversary edition, Simon & Schuster Ltd. (2004)
9. Hillson, D.: Developing Effective Risk Responses. In: 30th Annual Project Management Institute 1999 Seminars & Symposium Philadelphia, Pennsylvania, USA (1999)
10. Anuar, N.B., Papadaki, M., Furnell, S., and Clarke, N.: An investigation and survey of response options for Intrusion Response Systems (IRSs). In: Information Security for South Africa (ISSA). pp. 1-8. Johannesburg, South Africa (2010)
11. Mell, P., Scarfone, K., and Romanosky, S.: Common Vulnerability Scoring System. IEEE Security & Privacy. 4(6), 85-89 (2006)
12. Snort: The open source network intrusion detection system, http://www.snort.org
13. DARPA Intrusion Detection Data Sets, http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/index.html