Journal of Network and Computer Applications 55 (2015) 89–107

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

ORCEF: Online response cost evaluation framework for intrusion response system

Alireza Shameli-Sendi *, Michel Dagenais

Department of Computer and Software Engineering, École Polytechnique de Montréal, Montreal, Canada

ARTICLE INFO

Article history:
Received 2 December 2013
Received in revised form
31 March 2015
Accepted 6 May 2015
Available online 21 May 2015

Keywords:
Intrusion response
Response cost
Resource dependency
Decision-making
Fuzzy logic

ABSTRACT

Response cost evaluation is a major part of the Intrusion Response System (IRS). Although many automated IRSs have been proposed, most of them use statically evaluated responses, avoiding the need for dynamic evaluation of response cost. However, by designing a dynamic evaluation for the responses we can alleviate the drawbacks of the static model. Furthermore, it will be more effective at defending a system from an attack as it will be less predictable. A dynamic model offers the best response based on the current situation of the network. Thus, the evaluation of the positive effects and negative impacts of the responses must be computed online, at attack time, in a dynamic model. We evaluate the response cost online with respect to the resources dependencies and the number of online users.

In this paper, we present a practical framework with relevant factors for response cost evaluation. The proposed framework is a platform that leads us to account for the user's needs in terms of quality of services (QoS) and the dependencies of critical processes. Compared with other response evaluation models, the proposed framework consists of not only a novel online mechanism for response cost evaluation in complex network topologies, but also more detailed factors to evaluate responses positive effect and negative impact. In addition, we discuss the main challenges to evaluate response cost with respect to the attack type.

1. Introduction

Today, cyber attacks and malicious activities are rapidly becoming a major threat to the security of organizations (Sawilla and Wiemer, 2011). It is therefore crucial to have appropriate Intrusion Detection Systems (IDSs) and Intrusion Response Systems (IRSs) to continuously monitor and react against malicious or unauthorized activities by applying appropriate countermeasures. Unfortunately, IRS receives considerably less attention than IDS (Shameli-Sendi et al., 2012).

Usually, the attacker exploits security goals: the *confidentiality* and *integrity* of data, and the *availability* of service (referred to as *CIA*), by targeting vulnerabilities in the form of flaws or weak points in the security procedures, design, or implementation of the system (Shameli-Sendi et al., 2010). The main issues in designing security defence models are to correctly identify the security problem and choose the right set of countermeasures. If we fail to do so, our automated IRS will needlessly reduce network/host performance, wrongly disconnect users from the network/host, and eventually results in a DoS attack on our network. Thus, implementing an appropriate algorithm in IDS and IRS must take this into account. It is essential that we counterattack with more advanced features, a complete list of responses, accurate evaluation of those responses in a network model, and an understanding of the cost of each response in every network element.

The selected response by the IRS should increase the security performance against the attacker. However, a good response decreases the service quality (service availability). Therefore, the objective is increasing the security performance and decreasing the negative impact of the response simultaneously. We interpret this problem as a multi-objective optimization problem. The main contribution of this work is to prepare a proper online response cost evaluation for automated IRS with respect to all elements of a network, the dependency between resources, and system users based on multi-objective optimization algorithms. The optimal response, in the optimization mechanism, is selected with respect to these constraints: the damage cost, confidence level of attack happening, and the attacker target value. It is very important to explain the rationale behind the online calculation in this paper. If we assume that our service dependency graph is static, and there is no crash, migration nor dependency changes over time, all responses can be evaluated offline in all defence points. Since we consider the number of online users in our formula, we do not know where the load is high at attack time. Our goal is to provide a

* Corresponding author
E-mail addresses: alireza.shameli-sendi@polymtl.ca (A. Shameli-Sendi), michel.dagenais@polymtl.ca (M. Dagenais).

http://dx.doi.org/10.1016/j.jnca.2015.05.004
1084-8045/

mechanism to balance the response cost and the potential attack damage cost in online mode and protect the quality of service in terms of total user's needs.

The paper is organized as follows: first, we will investigate earlier work and several existing methods for intrusion response. Fuzzy modeling is illustrated in Section 3. The proposed framework will be discussed in Section 4. Experimental results are given in Section 5. We provide a discussion of ORCEF limitations in Section 6. Finally, Section 7 concludes the paper.

2. Related work

2.1. Intrusion response system

Software systems, information systems, distributed applications, and so on usage is continuously growing in size and complexity. Today, many services are offered to the users and organizations try to provide the best service quality. Any disruption of service causes users dissatisfaction. This could be one of the important criteria for the competition between organizations. Thus, to design a new generation of IRS, it is extremely important to maintain the user's QoS, the response time of applications, and critical services in high demand when a set of responses are being applied by the IRS.

The current intrusion response models can be classified into three categories (Shameli-Sendi et al., 2014):

- *Static cost*: The static response cost is obtained by assigning a static value based on expert opinion. Thus, in this approach, a static value is considered for each response.
- *Static evaluated cost*: In this approach, a statically evaluated cost, obtained by an evaluation mechanism, is associated with each response. The response cost, in the majority of existing models, is statically evaluated. A common solution is to evaluate the positive effects of the responses based on their consequences for the confidentiality, integrity, availability, and performance metrics. To evaluate the negative impact, we can consider the consequences for the other resources, in terms of availability and performance (Strasburg et al., 2009). For example, after running a response that blocks a specific subnet, a Web server under attack is no longer at risk, but the availability of the service has decreased. After evaluating the positive effect and negative impact of each response, we then use a technique to calculate the response cost (Mu and Li, 2010).
- *Dynamic evaluated cost*: The dynamic evaluated cost is based on the network situation. We can evaluate the response cost online based on the dependencies between resources and online users. For example, the consequences of terminating a dangerous process varies with the number of interdependencies of other resources on the dangerous process and with the number of online users. If the cost of terminating the process is high, maybe another response would be better. Compared to the statically evaluated cost model, this model better meets the needs of QoS.

The majority of the proposed IRS use *Static Cost* or *Static Evaluated Cost* models (Curtis and Carver, 2001; White et al., 1996; Strasburg et al., 2009; Lee et al., 2002; Stakhanova et al., 2007; Mu and Li, 2010; Wang and Elhag, 2006; Fisch, 1996; Porras and Neumann, 1997; Bowen et al., 2000; Musman and Flesher, 2000; Somayaji and Forrest, 2000; Lewandowski et al., 2001; Schnackenberg et al., 2001; Wang et al., 2001; Tanachaiwiwat et al., 2002; Foo et al., 2005; Papadaki and Furnell, 2006; Kanoun et al., 2010). In contrast, a few models have been presented in the third category, dynamic evaluated cost (Toth and Kregel, 2002; Balepin et al., 2003; Kheir et al., 2010). Since our proposed framework lies in this category, we will subsequently discuss some highly related frameworks.

We first consider service dependencies models in IRS, initially proposed by Toth and Kregel (2002). They presented a network model that accounts for relationships between users and resources, illustrating that they are performing their activities by utilizing the available resources. The response model goal is to keep the usability of a system as high as possible. Each response alternative (which node to isolate) is inserted temporarily into the network model and a calculation is performed to find which one has the lowest negative impact on the services. When the IDS detects an attack coming towards a machine, an algorithm tries to find which firewall/gateway can minimize the penalty cost of the response actions. This approach suffers from multiple limitations. First, they did not consider the positive effect of responses. The evaluation of responses without considering their positive effects leads us to inaccurate evaluation. For example, if the negative impact of response A is greater than response B, it does not mean that response B has to be applied first. Maybe the positive effect of response A is better than B and, if we calculate the response effectiveness, overall response A is better. Secondly, from a security goals perspective (CIA), there is no evaluation in terms of data confidentiality and integrity. Eventually, in the proposed model only the “block IP” response has been considered.

Balepin et al. (2003) presented a local resource dependency model to evaluate responses in case of attack. Like Toth and Kregel (2002), it considers the current state of the system to calculate the response cost. Each resource has common response measures associated with it. They believe that designing a model to assess the value of each resource is a difficult task, so they order the resources by their importance to produce a cost configuration. Then, static costs are assigned to high priority resources. Thus, costs are inflicted into the resource dependency model when associated resources get involved in an incident. A particular response for a node is selected based on three criteria: (1) response benefit: sum of costs of resources that the response action restores to a working state, (2) response cost: sum of costs of resources which get negatively affected by the response action, and (3) attack cost: sum of costs of resources that get negatively affected by the intruder. Thus, unlike Toth and Kregel (2002) this model considers the positive effects of responses. This approach suffers from multiple limitations. First, it is not clear how the response benefits are calculated in terms of confidentiality and integrity. Secondly, restoring the state of resources cannot be the only factor to evaluate the response positive effect (Kheir et al., 2010). Finally, the proposed model is applicable for host-based intrusion response systems. To use for network-based intrusion response, it requires significant modifications in its cost model (Kheir et al., 2010).

Jahnke et al. (2007) proposed a graph-based approach for modeling the effects of attacks against resources and the effects of the response measures taken in reaction to those attacks. The proposed approach extends the idea put forward in Toth and Kregel (2002) by using general, directed graphs with different kinds of dependencies between resources, and by deriving quantitative differences between system states from these graphs. If we assume that G and $\tilde{G}$ are the graphs obtained before and after the reaction, respectively, then the calculation of the responses positive effect is the difference between the availability plotted in the two graphs: $A(\tilde{G})$–$A(G)$. Like Toth and Kregel (2002); Balepin et al. (2003), these authors focus on the availability impact.

Kheir (2010) presented a dependency graph to evaluate the confidentiality and integrity impact, as well as the availability impact. The confidentiality and integrity criteria are not considered in Toth and Kregel (2002), Balepin et al. (2003), Jahnke et al. (2007). In Kheir (2010), the impact propagation process proposed by Jahnke et al. is extended to include these impacts. Now, each service in the dependency graph is described with a 3D CIA vector, the values of which are