

# On Evaluation of Response Cost for Intrusion Response Systems (Extended Abstract)

Natalia Stakhanova<sup>2</sup>, Chris Strasburg<sup>1</sup>, Samik Basu<sup>1</sup>,  
and Johnny S. Wong<sup>1</sup>

<sup>1</sup> Department of Computer Science, Iowa State University, USA  
{cstras,sbasu,wong}@cs.iastate.edu

<sup>2</sup> Faculty of Computer Science, University of New Brunswick, Canada  
natalia@unb.ca

**Abstract.** In this work we present a structured and consistent methodology for evaluating cost of intrusion responses. The proposed approach provides consistent basis for response evaluation across different systems while incorporating security policy and properties of specific system environment. The advantages of the proposed cost model were evaluated via simulation process.

The proliferation of complex and fast-spreading intrusions against computer systems brought new requirements to intrusion detection and response, demanding the development of sophisticated and automated intrusion response systems. In this context, the cost-sensitive intrusion response models have gained the most interest mainly due to their emphasis on the balance between potential damage incurred by the intrusion and cost of the response. However, one of the challenges in applying this approach is defining consistent and adaptable measurement of these cost factors on the basis of policy of the system being protected against intrusions.

We developed a structured and consistent methodology for the evaluation of intrusion response cost based on three parameters: (a) *the impact of a response on the system* that quantifies the negative effect of the response on the system resources, (b) *the response goodness* that measures the ability of the corresponding response to mitigate damage caused by the intrusion to the system resources and (c) *the operational cost of a response in a given environment*.

Within this methodology, we assess response impact with respect to resources of the affected system. Our model takes into account the relative importance of the system resources determined through the review of the system policy goals according to the following categories: *confidentiality*, *availability* and *integrity*. One of the important steps in this process is the analysis of the system resources. Based on this analysis, the evaluation algorithm assesses the *response goodness* in terms of the resources protected by the response, the *response damage* in terms of the resources impaired by the action and the *operational cost* with respect to its environmental impact.

This methodology does not substitute the response selection process in case of detected intrusion, but rather allows to evaluate the available responses on the consistent basis. The proposed methodology includes the following steps:

1. **The system classification:** The first step in quantifying the cost of a response involves determining the characteristics of the computing environment where the response will be deployed which includes evaluating system security policy priorities, defining level of tolerable risk, etc.
2. **The system policy goals:** The next step is to determine the importance of the system policy goals, and subsequently, to assess the potential risks according to the following categories: *confidentiality*, *availability* and *integrity*.
3. **The system resources:** System resources can be broadly viewed as the system assets (e.g., host, network, etc.), services provided by the system (e.g., HTTP, file system) and users served by the system. The analysis of system resources includes the enumeration of the available resources and their classification according to the importance for the system policy goals.
4. **The intrusion responses:** The responses are deployed to either counter possible attacks and defend the system resources or regain secure system state. Thus, the selection of applicable responses primarily depends on the identified system resources.
5. **The response operational cost:** The assessment of operational cost is generally independent from the system policy. We assess the involved operational expenses on the basis of three requirements: *human resources*, i.e., administrator time, *system resources*, i.e., storage, network bandwidth, processor time, etc., and *direct expenses* i.e., data processing fees by a third party, subscription service fees, cost of components replacement, etc.
6. **The response goodness:** Often the detection mechanism of the intrusion detection system (IDS) provides administrators with a set of alerts indicating potential attacks rather than a specific intrusion. When this situation arises, the response needs to be deployed preemptively on the basis of high likelihood of possible intrusions. In these cases, the response goodness is evaluated based on the number of possible intrusions it can potentially address, and consequently, the number of resources that can be protected by the response.
7. **The response impact on the system:** The impact of a response on the system is evaluated based on the defined system goals and their importance. The impact assessment process for a specific response includes three steps: (1) identifying the system resources affected by each response, (2) for each resource determining the priority of responses based on their effect on the resource, and (3) computing the negative impact of the responses on the associated resource using the ordering obtained in step 2. Eventually, the impact of a response on the system as a whole is an aggregation of the response's impact on the system resources.

The proposed methodology for assigning response costs essentially presents the first roadmap for defining *standardized metrics* for response cost evaluation. These response metrics provide a *consistent basis* for evaluation across systems, while allowing the response cost to be *adapted with respect to the security policy and properties of specific system environment*. Importantly, this approach is *practically implementable* in a real-world environment, making response cost assessment accessible to system administrators with a range of system expertise.