A Model for Estimating the Benefits from Network Security Systems

Soumyo D. Moitra, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, USA

ABSTRACT

Estimating the benefits of network security systems is important for security decisions since considerable resources are spent on them and organizations need to know the returns on their investments. The objective of the model presented here is to improve management decisions. Better decisions imply greater security for the budget. This model has a number of novel features such as a probabilistic sub-model for the detection and response process, a new attack/damage matrix based on damage-type and cyber-attacks by category, and extensive sensitivity analyses. The results suggest a number of insights into the factors affecting the benefits from sensors such as the effects of non-linear relationships between the rate of attacks and the damages caused. The key role of the value of sensitive information is identified. The model helps identify the conditions under which a new security system provides enough benefits to justify its purchase.

Keywords: Benefits from Sensors, Cyber Defense, Impact of Cyber Attacks, Information Assurance, Network Security Economics, Return On Security Investments

INTRODUCTION

In view of the importance of network and information security to organizations today, there is a need for a methodology to assess the value of investments in network security. Network security depends heavily on monitoring traffic to detect and mitigate intrusions and attacks. Monitoring requires network sensors and associated systems to observe and analyze the traffic. Sensor systems are therefore extremely important to cyber security and are widely deployed. In addition to technical considerations, there are a number of critical managerial issues related to decisions regarding the acquisition and deployment of sensors that we address in this paper. We shall use the term sensor in a broad sense to include Intrusions Detection and Prevention Systems (IDPSs) and Security Information Event Managers (SIEMs) that complement sensors. These systems monitor traffic, alert analysts about possible cyber attacks, and can help incident handlers in preventing or mitigating the impacts of attacks. Sensors

DOI: 10.4018/ijban.2014070101
can be very expensive in relation to constrained security budgets and managers need to know whether expenditures on sensors are justified, how much to invest in them and how best to deploy them. This includes prioritization across alternative locations and how the deployment fits in with defense-in-depth or other security strategies. Although we use the term “sensors” for concreteness, all analyses discussed here are applicable to network security systems generally.

These decisions require the assessment of the value of sensors to the organization and thus organizations need metrics to evaluate the benefits from sensors. This paper focuses on the issues of measuring the effectiveness of sensors at a particular location and develops a comprehensive model for such metrics. Purely technical analysis does not provide a complete answer to the managerial question of how best to plan the deployment of sensors. An economic and financial perspective is also needed. There is currently a gap between discussions about the value of network security systems and the evaluation of the benefits of deploying them. On one hand there is a general acceptance that network security systems should be deployed (and in fact are widely deployed). But on the other hand, there is no standard methodology to evaluate how useful they are to network defense and how to assess the returns an organization might get from them. Real dollars are spent on network security systems and managers would naturally like to know what returns they get from them. These expenditures are significant and are being made on a regular basis (usually annually). Since this will likely continue in the foreseeable future, making the decision process more effective can make a major difference. The model and methodology developed in this paper is illustrated with an example showing how the value of sensors (and network security systems in general) can be estimated. One major reason why organizations are very concerned about protecting their networks is the sensitive information that resides on many of its hosts and hence we examine the significance of having sensitive information at risk on the network.

Resources are inevitably limited and there are always competing demands. A further issue of importance is how best to utilize the resources allocated for sensors in terms of prioritizing the possible locations where they might be placed so as to be most beneficial. Of course there will be a spectrum of potential benefits across the possible locations, and based on the budget, the most deserving set of locations would be provided with sensors during a planning horizon. Thus it is very important to have a comprehensive and consistent methodology to value a sensor that will monitor a network at a particular location.

This value comes from the reduction in potential damages (to the organization’s network systems) that might have been caused by cyber attacks but which are mitigated by having a new or additional sensor – by detection of attacks that might not have been otherwise detected. Having a new sensor may also help in better response and more efficient incident handling (that is, prevention, protection, mitigation, etc.) and this process is modeled here as well. There could be other benefits from sensors, such as better network management or improved forensics, but that is beyond the scope of this paper.

The rest of the paper is organized as follows. The next section reviews the relevant research on security metrics and considers some of the outstanding issues. The following section develops the model that has many novel features for estimating sensor metrics. We then present a numerical example to illustrate the approach. The example values are entirely hypothetical and are based on publicly available data. The intent of the example is to illustrate the approach and indicate how it could be applied by an organization. The model was designed to facilitate sensitivity analysis in view of the various uncertainties in the parameters, and we present extensive sensitivity analyses. We discuss the significance of the results. Finally we have a summary and conclusions.
Principled Reference Data Management for Business Intelligence
Ivan Milman, Martin Oberhofer, Sushain Pandit and Yinle Zhou (2014). Information Quality and Governance for Business Intelligence (pp. 219-235).
www.igi-global.com/chapter/principled-reference-data-management-for-business-intelligence/96152?camid=4v1a