Autonomic Parameter Tuning of Anomaly-Based IDSs: an SSH Case Study

June 2012 IEEE Transactions on Network and Service Management

Anomaly-based intrusion detection systems classify network traffic instances by comparing them with a model of the normal network behavior. To be effective, such systems are expected to precisely detect intrusions (high true positive rate) while limiting the number of false alarms (low false positive rate). However, there exists a natural trade-off between detecting all anomalies (at the expense of raising alarms too often), and missing anomalies (but not issuing any false alarms). The parameters of a detection system play a central role in this trade-off, since they determine how responsive the system is to an intrusion attempt. Despite the importance of properly tuning the system parameters, the literature has put little emphasis on the topic, and the task of adjusting such parameters is usually left to the expertise of the system manager or expert IT personnel. In this paper, we present an autonomic approach for tuning the parameters of anomaly-based intrusion detection systems in case of SSH traffic. We propose a procedure that aims to automatically tune the system parameters and, by doing so, to optimize the system performance. We validate our approach by testing it on a flow-based probabilistic detection system for the detection of SSH attacks.

Title and author(s) of the original paper in IEEE Xplore:
Title: Characterization of ISP Traffic: Trends, User Habits, and Access Technology Impact
Author: Anna Sperotto, Michel Mandjes, Ramin Sadre, Pieter-Tjerk de Boer, and Aiko Pras
This paper appears in: IEEE Transactions on Network and Service Management
Issue Date: June 2012