A Real-time Recurrent Alert Correlation Model for Intrusion Detection Systems

Reza Sadoddin[1](UNB, Fredericton), Ali. A Ghorbani[2](UNB& NRC, Fredericton)

Abstract

Complementary security systems are widely distributed in networks to protect digital assets. These systems may include intrusion detection systems (IDSs), firewalls, antivirus tools, file integrity checkers, and so forth. They usually serve for different security purposes, or serve for the same purpose through different methods. Analyzing raw alerts is not an easy task with a large volume of alerts generated by low-level sensors. The problem is exaggerated with well-known weaknesses of intrusion detection systems in generating high rate of false alerts. The primary goal of alert correlation is to provide system support for a global and condensed view by analyzing raw alerts.

In this poster, we explain a novel framework of alert correlation which takes into account all aspects of correlation. As shown in figure 1, the framework is consisted of six steps: Normalization, Aggregation, Correlation, False Alert Reduction, Attack Strategy Analysis and Prioritization. The purpose of each step and our methodology for accomplishing each are presented in the poster. In addition to proposing a novel correlation model, we anticipate to achieve a new online clustering technique for grouping similar hyper-alerts and a novel multi-layer filtering technique for reducing false alerts.

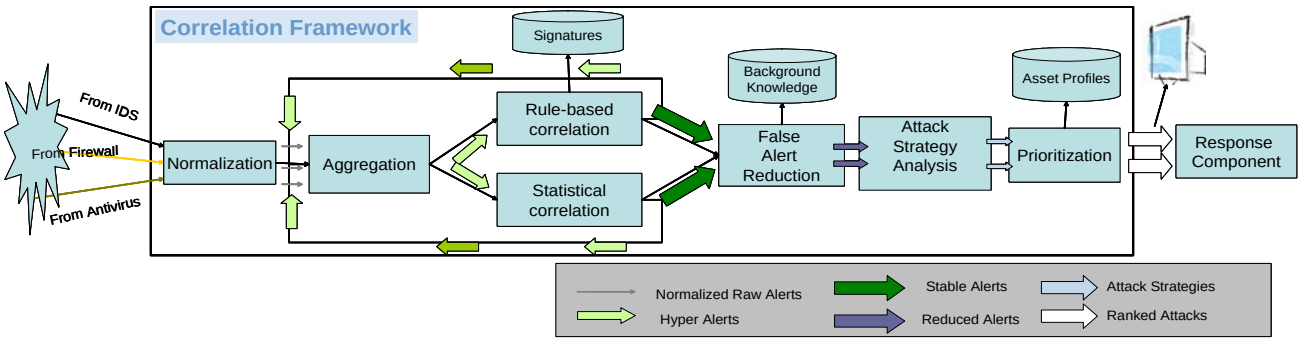

Figure 1 – Alert Correlation Framework

[1] Reza.sadoddin@unb.ca
[2] Ghorbani@unb.ca