Hamilton Institute

Feedback Control of Network Intrusion Detectors

Joao B. D. Cabrera,
Scientific Systems Company, Inc.
Woburn, MA, USA

Tuesday, March 7th, 2006

Abstract

Intrusion Detection Systems (IDSs) are relatively complex devices that monitor information systems in search for security violations. Network-based IDSs process packets entering the system, while host-based IDSs process audit data from individual hosts. In this presentation, we describe recent efforts by the author and collaborators at the Georgia Institute of Technology in which techniques from Applied Statistics and Systems Science were applied for designing an adaptive network-based IDS. It builds upon our work on constructing statistical models for the processing times along the four stages of Snort, a commonly used network-based IDS. These models are used to describe network-based IDS processing as a queuing system with four stages.

This queuing system is further abstracted to produce a design model for the purpose of control. The control objective is to provide the IDS with the ability of effecting performance adaptation, that is to achieve the best possible performance for a given operating environment. During normal operation, the IDS utilizes a full rule set, covering all known intrusions. The control strategy is centered on estimating the probability of buffer overflow, and switching to less inclusive rule sets whenever this probability crosses a given threshold. Experimental results are provided, based on real datasets collected at the network entry point of the College of Computing at Georgia Tech. While the focus of the current work concerns network-based IDSs for high-speed networks, the methodology is applicable to any resource-constrained system performing pattern matching of some sort. Other applications of the method are discussed.

Venue: Seminar Room, Hamilton Institute, Rye Hall, NUI Maynooth

Time: 1.00 - 2.00pm (followed by tea/coffee)

Travel directions are available at www.hamilton.ie

IEEE
CC Ireland Chapter