PURDUE
UNIVERSITY

School of Electrical and Computer Engineering
Inter-office Memorandum

Scheduling of Examinations:

Student's Name: Gaspar Modelo Howard
Degree: Doctor of Philosophy
Type: Final Exam

Major Professor: SAURABH BAGCHI
Advisor 1: GUY LEBANON
Advisor 2: SONIA A. FAHMY
Advisor 3: VIJAY S. PAI

Examination Date: 12-11-2012
Examination Time: 2:00 PM
Building & Room: MSEE 239

Thesis Title: Secure Configuration of Intrusion Detection Sensors for Changing Enterprise Systems

Abstract: To secure today's computer systems, it is critical to have different intrusion detection sensors (IDS) embedded in them. In spite of that, the complexity of distributed computer systems makes it difficult to determine the appropriate choice and placement of these detectors. For our work, we first describe a method to evaluate the effect a detector configuration has on the accuracy and precision of determining the system's security goals. The method is based on a Bayesian network model, obtained from an attack graph representation of the target system. Using Bayesian inference, we implement a dynamic programming algorithm for determining the optimal detector settings in a large-scale distributed system and compare it against a greedy algorithm, previously developed.
In the work described above, we take a static snapshot of the distributed system to determine the configuration of detectors. But distributed systems are dynamic in nature and current attacks usually involve multiple steps, called multi-stage attacks. For the second part of our work, we present a distributed detection framework based on a probabilistic reasoning engine that communicates to detection sensors and can achieve two goals: (1) protect a critical asset by detecting multi-stage attacks and (2) tune sensors according to the changing environment of the distributed system monitored by the distributed framework.
Each node in the Bayesian Network model represents a detection signature to an attack step or vulnerability. We extend our model by developing a system called pSigene, for the automatic generation of generalized signatures. It follows a four-step process based on a biclustering algorithm to group attack samples we collect from multiple sources, and logistic regression model to generate the signatures. We implemented our system using the popular open-source Bro IDS and tested it for the prevalent class of SQL

injection attacks. We obtain True and False Positive Rates of over 86% and 0.03%, respectively, which are very competitive to existing signature sets.

Committee Members: If you are unable to attend this examination, please contact Mr. Modelo Howard.