The University of Alabama
Department of Computer Science
Colloquium Series Speaker

Prof. Wenke Lee
College of Computing
The Georgia Institute of Technology

"Architectural Considerations for Anomaly Detection"

Friday, November 12th
11:00 a.m., HO 108

Abstract:

The most commonly used intrusion detection system (IDS) performance metrics are detection rate and false alarm rate. From a usability point of view, a very important measurement is Bayesian detection rate, which indicates how likely there is an intrusion when the IDS outputs an alert. It depends on detection rate, false alarm rate, and base rate (the prior probability of intrusion). Typically, an anomaly detection system has a low Bayesian detection rate because it has a non-zero false alarm rate and the base rate in the target environment is very low.

We argue that we need better system architecture to improve Bayesian detection rate. The main objective is to increase the base rate of data stream analyzed by complex detection modules. The general principle is to use *layered* architecture.

One approach is to use a cascade of successively more complex detection modules. We show that base rate increases from one layer to the next. In many cases, the overall false alarm rate of the cascade can be very low. We describe a worm detection system with cascade architecture. In DSC, the lower layer module identifies hosts with “infection-like” behavior and the higher layer module detects anomalous outgoing connection behavior of these hosts. Our experiments showed that DSC can detect fast scanning worms very accurately.

Another approach is to deploy multiple simple or low-level sensors and correlate the observations or alerts from these sensors. HoneyStat is a worm detection system with such architecture. In HoneyStat, each low-level sensor detects “interesting” events in a honey pot. The correlation module uses logistic analysis on the event data from multiple sensors to detect worms. We show that by deploying sufficient number of low-level sensors, HoneyStat can reliably detect worms.