

Proactive network defense via Bayesian learning

Jian Zhang
Ph.D., Yale University

Date: Feb 29th, 2008
Time: 1:00 PM
Venue: 256 Coates Hall

Abstract

A recent development in computer and network defense is the establishment of large-scale security information sharing systems that collect security-log data from thousands of participants across the Internet. One intended benefit from such a system is to enable proactive defense: a participant can be informed of potential attacks that have been observed by the others so that it can take measures accordingly to fend off the attacks. A central problem in realizing such a proactive defense system is the identification of potential attacks for each individual participant. The information sharing system often receives millions of reports daily but a participant has resources to address only a limited number of possible threats. Therefore, it is essential to identify the most important and imminent threats (may be different for different participants). In this talk, I will present several learning-based approaches to tackle this problem. In particular, I will discuss the use of (hierarchical) Bayesian models that may combine the observations in the sharing system and our domain knowledge to make attack identification and prediction.