

## Where Are the Nuggets in System Audit Data?

Wenke Lee (Georgia Tech)  
wenke@cc.gatech.edu

### Abstract

Intrusion detection, the process of identifying malicious activities in network and systems, is a very important area of research. Data mining approaches can be applied to network and system audit data to learn normal usage profiles and attack patterns, and to construct intrusion detection models. These (semi-)automated approaches have many advantages over the traditional hand-coding approaches. In this talk, I will first give an overview of current techniques in mining audit data. I will then discuss the research challenges and opportunities in data mining-based intrusion detection.