

## Detecting and Mitigating Security Anomalies

Mladen Vouk  
*North Carolina State University*  
*vouk@ncsu.edu*

Network and information security is of increasing concern as intruders utilize more advanced technologies, and attacks are occurring much more frequently. A simple intrusion can cause an enterprise financial disaster, a threat to national safety, or loss of human life. Network-based and computer-based intrusion detection systems (IDS's) started appearing some twenty years ago. Now, there are various synchronous and asynchronous tools for external and internal network and host intrusion detection and mitigation using models ranging from signature scanning and pattern matching, to statistical anomaly detection. Although modern tools are much more advanced, they still have many limitations, shortcomings, and open issues. Most tend to be focused on matching known patterns as opposed to discovery of new anomalies through, for example, inductive reasoning about potential anomaly signals. This talk discusses the issues, and the place of pro-active reasoning in the context of identification of security-related anomalies and issues.