

ICDM Workshop on Data Mining for Computer Security (DMSEC 03)

November 19, 2003

8:50am	Introductory Remarks
9am	Invited Talk: <i>Authenticating Users by Profiling Behavior</i> Tom Goldring (National Security Agency)
10am	Anomaly Detection: <i>Learning Rules from System Call Arguments and Sequences for Anomaly Detection</i> Gaurav Tandon and Philip Chan (Florida Institute of Technology)
10:30am	Morning Break
11am	Anomaly Detection: <i>One Class Support Vector Machines for Detecting Anomalous Windows Registry Accesses</i> Katherine Heller, Krysta Svore, Angelos Keromytis, and Salvatore Stolfo (Columbia University) <i>One Class Training for Masquerade Detection</i> Ke Wang and Salvatore J. Stolfo (Columbia University) <i>Detection of Novel Network Attacks Using Data Mining</i> Levent Ertoz, Eric Eilertson, Aleksandar Lazarevic, Pang-Ning Tan, Paul Dokas, Vipin Kumar, and Jaideep Srivastava (University of Minnesota)
12:30pm	Lunch
2pm	Invited Talk: <i>Behavior-based Security</i> Salvatore J. Stolfo (Columbia University)
3pm	Misuse Detection: <i>Detecting Privilege-Escalating Executable Exploits</i> Jesse C. Rabek, Robert K. Cunningham, and Roger I. Khazan (MIT Lincoln Laboratory)
3:30pm	Afternoon Break
4pm	Feature Extraction and Visualization: <i>Passive Operating System Identification from TCP/IP Packet Headers</i> Richard Lippmann, David Fried, Keith Piwowarski, and William Streilein (MIT Lincoln Laboratory) <i>Boundary Detection in Tokenizing Network Application Payload for Anomaly Detection</i> Rachna Vargiya and Philip Chan (Florida Institute of Technology) <i>A Prototype Tool for Visual Data Mining of Network Traffic for Intrusion Detection</i> William Yurcik, Kiran Lakkaraju, James Barlow, and Jeff Rosendale (NCSA/University of Illinois at Urbana-Champaign)
5:30pm	Concluding Remarks