
Computer Science Colloquium

Detection of Malicious Insider Activity Using Models of Insider Behavior

Mark Maybury
The MITRE Corporation

Wednesday, 9 February 2005

Olsen 311

Refreshments at 2:30, Talk from 3:00-4:00

This talk reports results from a six month long ARDA NRRC funded challenge workshop to create methods to counter sophisticated insider threats faced by the United States Intelligence Community. Based upon a systematic analysis of actual past and projected future cases of malicious insider activity, we report a generic model of malicious insider behaviors, distinguishing motives, (cyber and physical) actions, and associated observables. We describe a collaborative initiative to design and evaluate tools and techniques to provide early warning of insider activity, including novel algorithms for honeytokens, structured analysis, and data fusion. We assess their performance in an operational network, measuring timeliness and accuracy of detection. The talk will conclude outlining future areas for research.

Biography:

Dr. Mark Maybury is Executive Director of the Information Technology Center at the MITRE Corporation, where he directs and conducts research in human computer interaction, geospatial information systems, collaborative computing, intelligent training, speech and natural language processing, knowledge based software, and advanced databases. Mark received his BA in Mathematics from the College of the Holy Cross in 1986 where he was valedictorian. As a Rotary Scholar at Cambridge University, England he received his M.Phil. in Computer Speech and Language Processing in 1987 and his Ph.D. in Artificial Intelligence in 1991. Mark was awarded an MBA from RPI in 1989.