Georgia Tech Helps to Develop System That Will Detect Insider Threats From Massive Data Sets

Researchers at the U.S. Defense Advanced Research Projects Agency (DARPA), the Army Research Office, and Georgia Tech are developing new approaches for identifying insider threats before a data breach occurs.

The researchers are developing a suite of algorithms that can detect different types of insider threats by analyzing massive amounts of data for unusual activity. "Our goal is to develop a system that will provide analysts for the first time a very short, ranked list of unexplained events that should be further investigated," says Georgia Tech professor David A. Bader.

The researchers also are developing a prototype Anomaly Detection at Multiple Scales (ADAMS) system, which they say could revolutionize the capabilities of counterintelligence professions by prioritizing potential malicious insider threats against a background of normal network activity.

The ADAMS system will analyze terabytes of data using new algorithms to quickly find anomalies. "We need to bring together high-performance computing, algorithms, and systems on an unprecedented scale because we're collecting a massive amount of information in real time for a long period of time," Bader says.

From Georgia Tech News
View Full Article
Georgia Tech Helps to Develop System That Will Detect Insider Threats From Massive D...