



DARPA program seeks early detection of insider threats

Powerful algorithms will search online user records for anomalies.

- By [Henry Kenyon](#)
- Nov 17, 2011

Usually the pattern of events that leads to a person becoming an insider threat is only discovered after the fact. Now a team of researchers funded by the Defense Advanced Research Projects Agency (DARPA) and the Army Research Office is developing a set of algorithms to detect anomalous activity before the damage is done.

DARPA's [Anomaly Detection at Multiple Scales](#) (ADAMS) program seeks to create a software-based approach to track a person's online work activity — everything from e-mail messages to instant messages, file access, and Web traffic — to detect anomalous behavior, explained David Bader, the project's co-principal investigator and a professor at the Georgia Tech School of Computational Science and Engineering and the Georgia Tech Research Institute.

The project is led by Science Applications International Corporation (SAIC) and includes researchers from Oregon State University, the University of Massachusetts, and Carnegie Mellon University.

The project also seeks to determine how trusted insiders become radicalized; but doing so requires sifting through terabytes of data. This is a big challenge, one that requires powerful algorithms running on high performance computers, Bader said. One of the ADAMS program's predictive aspects will be to find and flag suspicious behavior before a security breach occurs. "Our system tries to find these individuals who have gone down that slippery slope, but before they've done any crime or anything illegal," he said.

ADAMS will collect data and put the pieces together for analysts by highlighting potential threats. Researchers want the system to boil down the number of anomalies to a short list for an analyst to investigate. "Today an analyst is overwhelmed with thousands of anomalies per day," said Bader.

The team is taking a different approach from traditional methods that use pattern matching and profiling by working on algorithms to identify suspicious user activities through change detection. Because an anomaly is an unexplained event in the context of a person's work routine, the algorithms being developed for ADAMS will allow analysts to understand a user's behavior. "Unlike pattern matching, which has many false positives, we're using a different approach to understand humans within an organization," he said.

The system will detect anomalies in job behavior and study an organizational chart to understand how users relate to their organizations. However, individuals and organizations must explicitly agree to undergo the constant monitoring and deep analysis of terabytes of data, Bader said. To do this, the team is developing large scale parallel algorithms to understand communities in an organization. This will also require machine learning and graph analysis to understand the complex interaction of individuals and any changes in their behavior, he said.

ADAMS is in its first two-year development phase. The program was launched this summer and an early version of the framework was demonstrated in October. In this initial demonstration, Bader said the prototype was able to detect some types of threat scenarios. Over the course of the program, this capability will be expanded to detect more types of anomalies and operate with larger datasets, he said.

About the Author

Henry Kenyon is a staff writer covering enterprise applications.



EHR use is driving health care plan **transformation.**

[LEARN MORE HERE](#)

Sponsored by: General Dynamics Information Technology



© 1996-2011 1105 Media, Inc. All Rights Reserved.