Pentagon aims to detect network intruders by their strange behavior

By Dawn Lim

July 23, 2012

The military venture capital wing has tapped scientists to build computer systems that can detect intruders by picking out abnormal behavior from familiar patterns generated by authorized users.

Defense Advanced Research Projects Agency has awarded a contract to security software developer Coveros to research methods to validate the identity of a computer user by detecting unauthorized uses of computer accounts, the firm announced.

"Our research on this project is examining system call patterns" – requests made to an operating system to command tasks to be performed -- "to determine whether a computer user is legitimate or not," CEO Jeffery Payne said in an email.

The research is being funded under DARPA's Active Authentication program, he said.

The aim of the DARPA funding project is "developing novel ways of validating the identity of the person...that focus on the unique aspects of the individual through the use of software-based biometrics," according to the DARPA tender, released in January.

The idea is to devise a unique "cognitive fingerprint" of a user by tracking how they interact with their computers -- through, say, how they command and search for data -- in order to ensure users of computer systems are exactly who they claim to be, the document said.

Loudoun County, Va.-based Coveros has previously received funding in June from the Air Force for work involving anomaly detection and authentication, contract databases indicate.

(Image via hfuchs/Shutterstock.com)