New Behavioral Data System Could Do Double Duty

May 7 2010

(PhysOrg.com) -- A new behavioral data analysis system under development at UT Dallas focuses on identifying potential Internet threats, but it comes with a nice bonus.

Researchers say the basic idea behind the system - detecting worrisome deviations from normal activity and quickly providing an alert so that immediate measures can be taken - could have application in areas far beyond the Web, such as health-care monitoring.

"We proposed a novel platform that thoroughly analyzes network traffic behavior to identify potential internet threats," said Dr. Mehrdad Nourani, an associate professor of electrical engineering in the University's Erik Jonsson School of Engineering and Computer Science. "But it could have much broader application."

The technology uses two sub-systems functioning in parallel to achieve both high speed and efficient use of memory, thus ensuring fast results and optimal use of resources. The system builds a bell-shaped curve depicting normal traffic/behavior and can then achieve practically zero false positives and false negatives when identifying abnormalities outside the curve.

The happy result is that although the system is designed to identify abnormalities that indicate suspicious interactions among users or the presence of malicious data such as worms or viruses, the abnormality might just as well be health-related data indicating an issue such as heart

arrhythmia, sleep apnea or epileptic seizure.

Titled "A Behavioral Analysis Engine for Network Traffic," the two-year $100,000 project is funded by the Cisco University Research Program Fund, a corporate advised fund of the Silicon Valley Community Foundation.