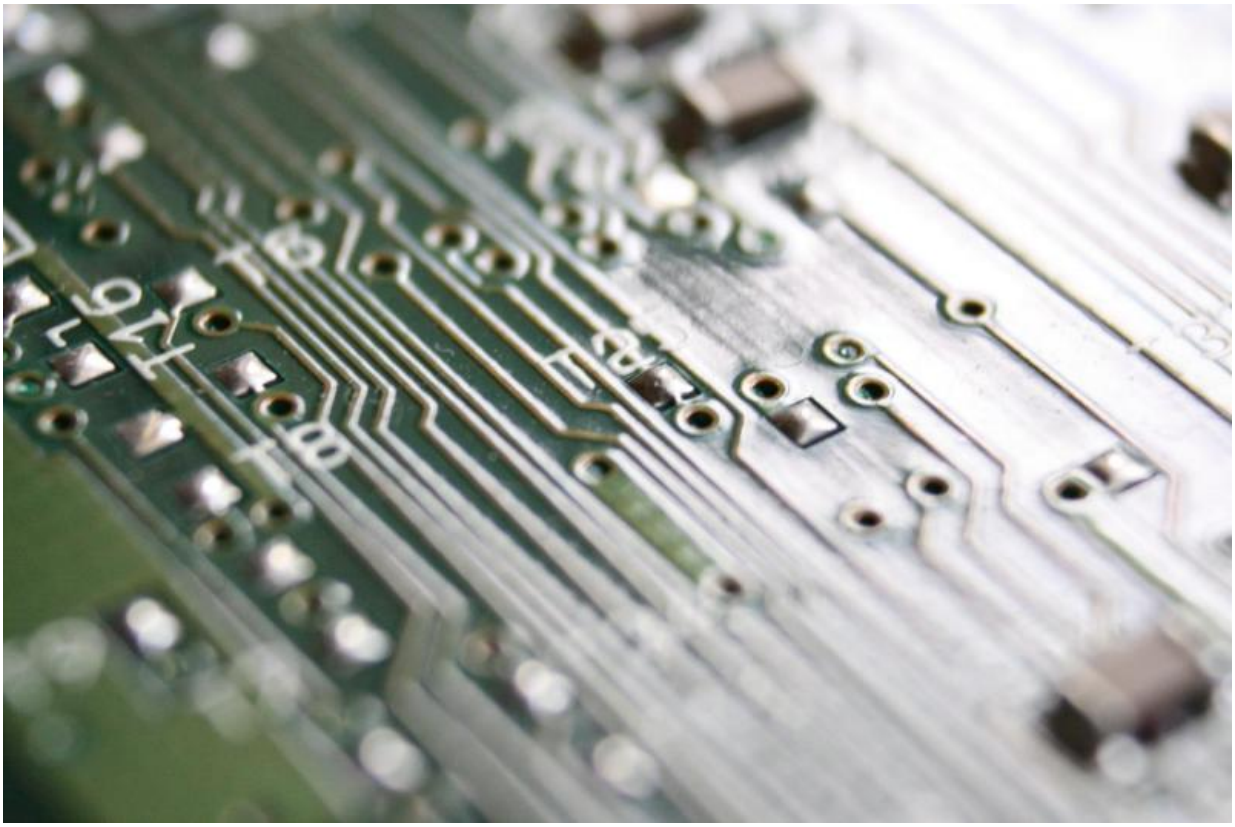
New research method identifies stealth attacks on complicated computer systems

October 13 2015



Credit: Public Domain

Three Virginia Tech computer scientists are unveiling a novel approach to discovering stealth attacks on computers at the annual ACM Conference on Computer and Communications Security.

Imagine millions of lines of instructions. Then try and picture how one extremely tiny anomaly could be found in almost real-time and prevent a cyber security attack.

Called a "program anomaly detection approach," a trio of Virginia Tech computer scientists has tested their innovation against many real-world attacks.

One type of attack is when an adversary is able to remotely access a computer, bypassing authentication such as a login screen. A second example of attack is called heap feng shui where attackers hijack the control of a browser by manipulating its memory layout. Another example of attack is called directory harvesting where spammers interact with vulnerable mail servers to steal valid email addresses.

The prototype developed by the Virginia Tech scientists proved to be effective and reliable at these types of attacks with a false positive rate as low as 0.01 percent.

Their findings are reported today in an invited presentation at the 22nd Association of Computing Machinery (ACM) Conference on Computer and Communications Security, Denver, CO, Oct 12-16, 2015.

"Our work, in collaboration with Naren Ramakrishnan, www.cs.vt.edu/user/ramakrishnan is titled, "Unearthing Stealthy Program Attacks Buried in Extremely Long Execution Paths," said Danfeng (Daphne) Yao, www.cs.vt.edu/user/yao associate professor of computer science at Virginia Tech. Xiaokui Shu, a computer science doctoral student of Anqing, China, advised by Yao, was the first author.

"Stealthy attacks buried in long execution paths of a software program cannot be revealed by examining fragments of the path," Yao, who holds the title of the L-3 Communications Cyber Faculty Fellow of Computer

Science, said.

Yao explained, "Modern exploits have manipulation tactics that hide them from existing detection tools. An example is an attacker who overwrites one of the variables before the actual authentication procedure. As a result, the attacker bypasses critical security control and logs in without authentication."

Over time, these stealthy attacks on computer systems have just become more and more sophisticated.

The Virginia Tech computer scientists' secret formula in finding a stealth attack is in their algorithms. With specific matrix-based pattern recognition, the three were able to analyze the execution path of a software program and discover correlations among events. "The idea is to profile the program's behavior, determine how often some events are supposed to occur, and with which other events, and use this information to detect anomalous activity," Ramakrishnan said.

"Because the approach works by analyzing the behavior of computer code, it can be used to study a variety of different attacks," Yao added. Their anomaly detection algorithms were able to detect erratic program behaviors with very low false alarms even when there are complex and diverse execution patterns.

Yao and Ramakrishnan have lengthy portfolios in the study of malicious software and data mining.

In 2014, Yao received a U.S. Army Research Office Young Investigator award to detect anomalies that are caused by system compromises and malicious insiders. This award allowed her to design big data algorithms that focused on discovering logical relations among human activities. In 2010 she won a National Science Foundation CAREER award to

develop software that differentiated human-user computer interaction from that of malware, commonly known as malicious software.

Ramakrishnan, who holds the Thomas L. Phillips Professorship of Engineering, directs Virginia Tech's Discovery Analytics Center www.dac.cs.vt.edu, supported by the Institute for Critical Technology and Applied Science www.ictas.vt.edu . A Distinguished Scientist of the ACM, Ramakrishnan has concentrated his research on data mining, the science of processing massive quantities of data to discover patterns and to produce new insights.

More information: 22nd Association of Computing Machinery (ACM) Conference on Computer and Communications Security, Denver, CO, Oct 12-16, 2015. www.sigsac.org/ccs/CCS2015/

Provided by Virginia Tech