

Computers get a better way to detect threats

EurekaAlert!

Technique nicknamed 'space travel' allows a machine to travel virtually to another system

UT Dallas computer scientists have developed a technique to automatically allow one computer in a virtual network to monitor another for intrusions, viruses or anything else that could cause a computer to malfunction.

The technique has been dubbed "space travel" because it sends computer data to a world outside its home, and bridges the gap between computer hardware and software systems.

"Space travel might change the daily practice for many services offered virtually for cloud providers and data centers today, and as this technology becomes more popular in a few years, for the user at home on their desktop," said Dr. Zhiquian Lin, the research team's leader and an assistant professor of computer science in the Erik Jonsson School of Engineering and Computer Science.

As cloud computing is becoming more popular, new techniques to protect the systems must be developed. Since this type of computing is Internet-based, skilled computer specialists can control the main part of the system virtually - using software to emulate hardware.

Lin and his team programmed space travel to use existing code to gather information in a computer's memory and automatically transfer it to a secure virtual machine - one that is isolated and protected from outside interference.

"You have an exact copy of the operating system of the computer inside the secure virtual machine that a hacker can't compromise," Lin said. "Using this machine, then the user or antivirus software can understand what's happening with the space traveled computer setting off red flags if there is any intrusion.

Previously, software developer had to manually write such tools.

"With our technique, the tools already being used on the computer become part of the defense process," he said.

The gap between virtualized computer hardware and software operating on top of it was first characterized by Drs. Peter Chen and Brian Noble, faculty members from the University of Michigan.

"The ability to leverage existing code goes a long way in solving the gap problem inherent to many types of virtual machine services," said Chen, Arthur F. Thurnau Professor of Electrical Engineering and Computer Science, who first proposed the

Computers get a better way to detect threats

Published on Electronic Component News (<http://www.ecnmag.com>)

gap in 2001. "Fu and Lin have developed an interesting way to take existing code from a trusted system and automatically use it to detect intrusions."

Lin said the space travel technique will help the FBI understand what is happening inside a suspect's computer even if they are physically miles away, instead of having to buy expensive software.

Space travel was presented at the most recent IEEE Symposium on Security and Privacy. Lin developed this with Yangchun Fu, a research assistant in computer science.

"This is the top conference in cybersecurity, said Bhavani Thuraisingham, executive director of the UT Dallas Cyber Security Research and Education Center and a Louis A. Beecherl Jr. Distinguished Professor in the Jonsson School. "It is a major breakthrough that virtual developers no longer need to write any code to bridge the gap by using the technology invented by Dr. Lin and Mr. Fu. This research has given us tremendous visibility among the cybersecurity research community around the world."

Original release:

http://www.eurekalert.org/pub_releases/2012-09/uota-cga092012.php [1]

Source URL (retrieved on 12/27/2014 - 1:40pm):

<http://www.ecnmag.com/news/2012/09/computers-get-better-way-detect-threats>

Links:

[1] http://www.eurekalert.org/pub_releases/2012-09/uota-cga092012.php