

## Hardware, software advances help protect operating systems from attack

January 26 2011

The operating system (OS) is the backbone of your computer. If the OS is compromised, attackers can take over your computer – or crash it. Now researchers at North Carolina State University have developed an efficient system that utilizes hardware and software to restore an OS if it is attacked.

At issue are security <u>attacks</u> in which an outside party successfully compromises one computer application (such as a Web browser) and then uses that application to gain access to the OS. For example, the compromised application could submit a "system call" to the OS, effectively asking the OS to perform a specific function. However, instead of a routine function, the attacker would use the system call to attempt to gain control of the OS.

"Our goal is to give the OS the ability to survive such attacks," says Dr. Yan Solihin, an associate professor of electrical and computer engineering at NC State and co-author of a paper describing the new system. "Our approach has three components: attack detection; security fault isolation; and recovery."

The concept is to take a snapshot of the OS at strategic points in time (such as system calls or interrupts), when it is functioning normally and then, if the OS is attacked, to erase everything that was done since the last "good" snapshot was taken – effectively going back in time to before the OS attack. The mechanism also allows the OS to identify the source of the attack and isolate it, so that the OS will no longer be vulnerable to



attacks from that application.

The idea of detecting attacks and re-setting a system to a safe state is a well-known technique for restoring a system's normal functions after a failure, but this is the first time researchers have developed a system that also incorporates the security fault isolation component. This critical component prevents the OS from succumbing to the same attack repeatedly.

The concept of taking snapshots of the OS and using it to replace the OS if it is compromised was previously viewed as impractical, since taking these snapshots and running such a system significantly slowed <u>computer</u> operating speeds. "But we've developed hardware support that allows the OS to incorporate these survivability components more efficiently, so that they take up less time and energy," Solihin says. The researchers say the survival system takes up less than 5 percent of the OS's operating overhead.

**More information:** The paper, "Architectural Framework for Supporting Operating System Survivability," was co-authored by Solihin and former NC State Ph.D. student Xiaowei Jiang. The paper will be presented Feb. 16 at the IEEE International Symposium on High-Performance Computer Architecture in San Antonio, Texas.

## Provided by North Carolina State University

Citation: Hardware, software advances help protect operating systems from attack (2011, January 26) retrieved 27 April 2024 from <u>https://phys.org/news/2011-01-hardware-software-advances.html</u>

This document is subject to copyright. Apart from any fair dealing for the purpose of private



study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.