Computer hardware 'guardians' protect users from undiscovered bugs

September 30 2008

(PhysOrg.com) -- As computer processor chips grow faster and more complex, they are likely to make it to market with more design bugs. But that may be OK, according to University of Michigan researchers who have devised a system that lets chips work around all functional bugs, even those that haven't been detected.

Firms such as Intel find functional bugs by simulating different scenarios, commands and configurations that their processor might encounter. Bugs only show themselves when they're triggered by certain configurations. When firms find major bugs, they fix them. But because it would be virtually impossible to simulate all possibilities, engineers don't find all the bugs.

Buggy hardware inadvertently released to customers could fail. Short of replacing the product, there isn't much a company can do to fix the problem today.

The U-M researchers' system would eliminate this risk by building a virtual fence that prevents a chip from operating in untested configurations. The approach keeps track of all the configurations the firm did test, and loads that information onto a miniscule monitor that would be added to each processor.

The monitor, called a semantic guardian, keeps the chip operating within its virtual fence. It works by switching the processor into a slower, bare-bones, safe mode when the chip encounters a configuration that has not

been validated. In this way, the monitor would treat all untested configurations as potential threats.

This guardian isn't as controlling as it may sound, the researchers say.

"If you consider all the possible configurations of the processor, only a tiny fraction of them is verified. But that tiny portion accounts for the configurations that occur 99.9 percent of the time," said Valeria Bertacco, assistant professor in the Department of Electrical Engineering and Computer Science.

"Users wouldn't even notice when their processor switched to safe mode," Bertacco said. "It would happen infrequently, and it would only last momentarily, to get the computer through the uncharted territory. Then the chip would flip back to its regular mode."

Bertacco says this system would be akin to turning a motorcycle into a bicycle briefly when a rider encounters a rough patch of road. Then the rider could pedal over the bumps without crashing.

The vast majority of a processor's components are there for speed, Bertacco says. A chip in safe mode still operates properly and can perform all necessary functions.

The guardian would take only a small fraction of the microprocessor's area with a imperceptible performance impact, which the researchers assert is a small price to pay to eliminate the risks of buggy hardware.

This system could also protect against what could be hackers' next frontier: exploiting hardware design bugs in order to gain control of other computers. This threat has been in the news lately, as independent security researcher Kris Kaspersky announced plans to demonstrate a hardware bug exploit that can take over a machine, independent of its

applications, operating system, or patch level. He is scheduled to demonstrate this attack at the upcoming Hack in the Box Security Conference, Oct. 27-30.

"Semantic guardians would stop these security attackers dead in their tracks, since the processor would no longer be able to execute the buggy configurations that they were planning to exploit, said Ilya Wagner, a doctoral student in the Department of Electrical Engineering and Computer Science.

Wagner presents this research Sept. 29 at the Gigascale System Research Center's annual meeting, where industry and government funding agencies come together to learn about new research results. He and Bertacco are authors of a paper called Engineering Trust with Semantic Guardians, which they presented at the Design Automation and Test in Europe Conference in April 2007.

Engineering Trust paper (.pdf): www.eecs.umich.edu/~valeria/re … /DATE07Guardians.pdf

Provided by University of Michigan