Self-repairing software tackles malware

November 13 2014

Eric Eide, University of Utah research assistant professor of computer science, stands in the computer science department's "Machine Room" where racks of web servers sit. It is on these computers that Eide, U computer science associate professor John Regehr, and their research team created and tested A3, a suite of computer applications that defeat malware and automatically repair the damage it causes. The project could help lead to better consumer software defenses. Credit: Dan Hixson/University of Utah College of Engineering

University of Utah computer scientists have developed software that not only detects and eradicates never-before-seen viruses and other malware,

but also automatically repairs damage caused by them. The software then prevents the invader from ever infecting the computer again.

A3 is a software suite that works with a virtual machine—a virtual computer that emulates the operations of a computer without dedicated hardware. The A3 software is designed to watch over the virtual machine's operating system and applications, says Eric Eide, University of Utah research assistant professor of computer science leading the university's A3 team with U computer science associate professor John Regehr. A3 is designed to protect servers or similar business-grade computers that run on the Linux operating system. It also has been demonstrated to protect military applications.

The new software called A3, or Advanced Adaptive Applications, was co-developed by Massachusetts-based defense contractor, Raytheon BBN, and was funded by Clean-Slate Design of Resilient, Adaptive, Secure Hosts, a program of the Defense Advanced Research Projects Agency (DARPA). The four-year project was completed in late September.

There are no plans to adapt A3 for home computers or laptops, but Eide says this could be possible in the future.

"A3 technologies could find their way into consumer products someday, which would help consumer devices protect themselves against fast-spreading malware or internal corruption of software components. But we haven't tried those experiments yet," he says.

U computer scientists have created "stackable debuggers," multiple de-bugging applications that run on top of each other and look inside the virtual machine while it is running, constantly monitoring for any out-of-the-ordinary behavior in the computer.

Unlike a normal virus scanner on consumer PCs that compares a catalog of known viruses to something that has infected the computer, A3 can detect new, unknown viruses or malware automatically by sensing that something is occurring in the computer's operation that is not correct. It then can stop the virus, approximate a repair for the damaged software code, and then learn to never let that bug enter the machine again.

While the military has an interest in A3 to enhance cybersecurity for its mission-critical systems, A3 also potentially could be used in the consumer space, such as in web services like Amazon. If a virus or attack stops the service, A3 could repair it in minutes without having to take the servers down.

To test A3's effectiveness, the team from the U and Raytheon BBN used the infamous software bug called Shellshock for a demonstration to DARPA officials in Jacksonville, Florida, in September. A3 discovered the Shellshock attack on a Web server and repaired the damage in four minutes, Eide says. The team also tested A3 successfully on another half-dozen pieces of malware.

Shellshock was a software vulnerability in UNIX-based computers (which include many web servers and most Apple laptops and desktop computers) that would allow a hacker to take control of the computer. It was first discovered in late September. Within the first 24 hours of the disclosure of Shellshock, security researchers reported that more than 17,000 attacks by hackers had been made with the bug.

"It is a pretty big deal that a computer system could automatically, and in a short amount of time, find an acceptable fix to a widespread and important security vulnerability," Eide says. "It's pretty cool when you can pick the Bug of the Week and it works."

Now that the team's project into A3 is completed and proves their

concept, Eide says the U team would like to build on the research and figure out a way to use A3 in cloud computing, a way of harnessing far-flung computer networks to deliver storage, software applications and servers to a local user via the Internet.

The A3 software is open source, meaning it is free for anyone to use, but Eide believes many of the A3 technologies could be incorporated into commercial products.

Other U members of the A3 team include research associate David M. Johnson, systems programmer Mike Hibler and former graduate student Prashanth Nayak.

Provided by University of Utah