Technology Review PUBLISHED BY MIT

Friday, November 20, 2009

Self-Policing Cloud Computing

IBM security tool searches for and destroys malicious code in the cloud.

By David Talbot

Cloud computing presents inherent privacy dangers, because the cloud provider can see a customer's data and leased computational apparatus, known as "virtual machines." New research suggests that as long as the cloud can see things, it might as well check that its customers aren't running malicious code, new research suggests.

Researchers at IBM's Watson Research Center (http://www.watson.ibm.com/index.shtml) in Yorktown, NY, and IBM's Zurich Research lab (http://www.zurich.ibm.com/) have developed a system for cloud computing "introspection monitoring," in which elements of the cloud would act as a kind of virtual bouncer. They'd frisk virtual machines to check what operating systems they're using, whether they are running properly, and whether they contain malicious code, such as root-kits.

"It works by looking inside the virtual machine and trying to infer what it does. You don't want malicious clients to give you all kinds of malware in their virtual machines that you will run in the cloud," says Radu Sion (http://www.cs.sunysb.edu/~sion) , a computer scientist at Stony Brook University, who was not involved in the research. "Today the cloud does not offer privacy, so we might as well use the lack of privacy for introspection."

The work by IBM was one of several papers presented last Friday at the ACM Cloud Computing Security Workshop (http://crypto.cs.stonybrook.edu/ccsw09/) , a first-of-its-kind event. The paper extends earlier research on introspection to make it more applicable to cloud settings such as Amazon's EC2 (http://aws.amazon.com/ec2/) service. "In clouds, the barrier to entry is lower, and the thing customers are most concerned about is their information. We want to make sure their information is handled in a manner consistent with their expectation of security and privacy," says J.R. Rao (http://domino.research.ibm.com/comm/research_people.nsf/pages/jrrao.index.html) , senior manager for secure software and services for IBM.

One specific way that clouds could present hazards is if hackers figure out how to place their malicious virtual machines on the same physical servers as those of their victims, as recent research (http://people.csail.mit.edu/tromer/papers/cloudsec.pdf) has shown is possible. Cloud providers use multiple data centers and many thousands of servers, so finding the right one could be a crucial first step to a cloud computing attack. (Earlier research has shown that hackers using a given operating system can steal data from other users of the same operating system, and that similar vulnerabilities can exist when operating systems share the same servers.)

The next step could be data-theft from cache memory on multicore systems within the server. These caches, or temporary memory, are shared between different virtual machines, presenting a theoretical risk. At the conference, Microsoft proposed a system that would create hierarchies within the cache memory. Such a system would serve as a kind of partition and could guard against cache attacks of this kind.

The IBM and Microsoft papers are representative of new research that's important to the future of cloud computing because it points to ways of making fundamental cloud infrastructure more secure. "They are particularly good at fixing problems in the core, as opposed to just discussing the security of applications in the cloud," such as e-mail, says Sion of the two companies. The proposed solutions could be ready for commercialization within a year, he added.

Also at the conference, combined research by PARC (http://www.parc.com/) and Fujitsu (http://www.fujitsu.com/us) pointed out other ways that clouds could help provide security. Specifically, clouds can provide convenient places to cheaply and easily do computing that helps diagnose and solve security threats.

For example, consider a scenario in which mobile devices start acting strangely, possibly because a virus is spreading via text messages or e-mails. A wireless carrier could aggregate data from these mobile phones and, in a cloud setting, analyze the problem and devise the best response. "All of that work is done outside the mobile device. It allows dramatic speed-up in how you can respond to threats," says Markus Jakobsson (http://www.parc.com/about/people/89/markus-jakobsson.html) , a principal scientist at PARC, in Palo Alto, CA.

"When people use the words 'cloud' and 'security' together--it is often with a frown. But we are saying it is a huge boon," in enabling easy processing of security-related tasks, Jakobsson added. "If we don't use it, we are missing out on something truly amazing."