Technology
PUBLISHED BY MIT Review

Friday, October 23, 2009

Vulnerability Seen in Amazon's Cloud-Computing

New research reveals how to find would-be victims within cloud hardware.

By David Talbot

Leading cloud-computing services may be vulnerable to eavesdropping and malicious attacks, according to research that shows it is possible for attackers to precisely map where a target's data is physically within the "cloud" and then use various tricks to gather intelligence.

The study probed Amazon's industry-leading Elastic Computer Cloud (EC2) (http://aws.amazon.com/ec2/) service, but "we firmly believe these vulnerabilities are generic to current virtualization technology and will affect other providers as well," says Eran Tromer, a postdoctoral researcher at MIT's Computer Science and Artificial Intelligence Laboratory, who performed the work with three colleagues from the University of California at San Diego.

Ron Rivest (http://people.csail.mit.edu/rivest) , a computer science professor at MIT and pioneer in cryptography, says the four researchers have "discovered some troubling facts" about cloud-computing services, which rent out computing resources, including storage and processing power, on a by-the-hour basis. Specifically, the potential weaknesses were found in the basic computing infrastructure services that are provided by Amazon and Rackspace and are widely used within many in-house corporate datacenters.

These technologies involve "virtual machines"--remote versions of traditional onsite computer systems, including the hardware and operating system. The number of these virtual machines can be expanded or contracted on the fly to meet demand, creating tremendous efficiencies. But the actual computing is, of course, performed within one or more physical data centers, each containing thousands of computers. And virtual machines of different customers sit on the same physical servers.

The attack involves first figuring out which physical servers a victim is using within a cloud, then implanting a malicious virtual machine there, and finally attacking the victim.

Hunting down a victim who might be on any of tens of thousands of servers might seem a needle-in-haystack enterprise. But the paper concludes that with some simple detective work, "just a few dollars invested in launching [virtual machines] can produce a 40 percent chance of placing a malicious [virtual machine] on the same physical server as a target." They dub this mapping process "cartography."

Tromer and his colleagues demonstrated that, once the malicious virtual machine is

placed on the same server as its target, it is possible to carefully monitor how access to resources fluctuates and thereby potentially glean sensitive information about the victim. The researchers said it would be possible to steal data this way, though they did not take this next step.

The attack starts by taking advantage of that fact that all "virtual machines" still have internet protocol, or IP, addresses, visible to anyone within the cloud. The researchers found that nearby addresses often share the same hardware on EC2. So, at the simplest level, an attacker can set up lots of his own virtual machines, look at their IP addresses, and figure out which one shares the same physical resources as an intended target.

In practice, though, achieving this co-residence is not so easy; the attacker has a much higher chance of success if he has created his virtual machines at nearly the same time as his victim. To achieve such timing, the paper says, an attacker could perhaps flood the victim's website with requests, forcing the victim to expand his computing capacity by creating new virtual machines. The attacker would then create new virtual machines at the same time and check the IP addresses to confirm that he had landed in the right spots.

In other words, one of the key benefits of cloud computing--the ability to instantly expand or contract computational capacity as required--in this case provides a crucial vulnerability.

Once the researchers achieved such co-residence on Amazon's infrastructure, they were able, by monitoring ebbs and flows of the servers' processing speed and other factors, to indirectly learn what kinds of computing resources a would-be victim uses and when he uses them--often crucial clues that can reveal sensitive information about the victim's activities.

"I might find out all kind of business intelligence with things that these 'side-channels' might leak," says Radu Sion (http://www.cs.sunysb.edu/~sion/) , a computer scientist at Stony Brook University who is cochairing the conference (http://crypto.cs.stonybrook.edu/ccsw09/) at which the paper will be presented. A flurry of heavy computational activity by a company running financial trading models, for example, could provide clues to a pending market movement. Concurrent high levels of activity between two brokers could suggest a pending transaction.

While the researchers said that actual theft of data is possible, they did not go ahead to demonstrate it. "Stealing encryption keys isn't something we have demonstrated in this context yet, but we have demonstrated that the underlying side-channels are capable of that," says Tromer.

It may even be possible to detect the victim's passwords through a so-called keystroke attack, Tromer says. Earlier research has demonstrated that analyzing the timing of keystrokes can reveal which letters have been struck on a keypad. The current paper adapted that insight to suggest that small spikes in activity from a victim's previously idle virtual machine can reveal the activity of a person typing a password. Measuring subtle load-changes provides a way of detecting the timing of the keystrokes and thus,

potentially, the password.

The approach could also be used to perform much cruder attacks. If an attacker sits on the same servers as his victim, a conventional denial-of-service attack becomes possible simply by amping up his resource usage all at once.

In a statement, Amazon spokesman Kay Kinton says Amazon has "rolled out safeguards that prevent potential attackers from using the cartography techniques described in the paper." She added that for security reasons, Amazon could not disclose the details. However, Tromer says that the only full solution available today would be to give customers the option to avoid sharing physical servers with other customers. Creating unbreachable virtual walls between virtual machines that sit on the same server remains "an open research problem that we, and others, are working on," he says.

Amazon's statement also calls the side-channel method implausible. "The side channel techniques presented are based on testing results from a carefully controlled lab environment with configurations that do not match the actual Amazon EC2 environment. As the researchers point out, there are a number of factors that would make such an attack significantly more difficult in practice."

Amazon also said it had tightened access credential procedures, though this is not of direct relevance to the new paper. Rackspace did not return requests for comment made yesterday afternoon.

Upcoming Events

The Tough Get Growing: How to Succeed in a Down Economy (http://enterpriseforum.mit.edu/network/broadcasts/200911/index.html)
MIT Campus, Cambridge, MA
Monday, November 16, 2009
http://enterpriseforum.mit.edu/network/broadcasts/200911/index.html (http://enterpriseforum.mit.edu/network/broadcasts/200911/index.html)

Global Public Policy Summit (http://www.gpps2009.com)
Bermuda
Sunday, November 01, 2009 - Tuesday, November 03, 2009
http://www.gpps2009.com (http://www.gpps2009.com)

Optimizing Innovation 2009 (http://www.connecting-group.com/Web/EventOverview.aspx?Identificador=6)
New York, NY
Wednesday, October 21, 2009 - Thursday, October 22, 2009
http://www.connecting-group.com/Web/EventOverview.aspx?Identificador=6 (http://www.connecting-group.com/Web/EventOverview.aspx?Identificador=6)

Bioengineering Insights 2009 (http://engineering.ucsb.edu/insights2009/TR)

Santa Barbara, CA
Monday, October 26, 2009
http://engineering.ucsb.edu/insights2009/TR (http://engineering.ucsb.edu/insights2009/TR)
