technology review
Published by MIT





Friday, October 28, 2011

# Security Researchers Rain on Amazon's Cloud

Experts find way to modify controls within Amazon's cloud service, but the hole is quickly plugged.
By David Talbot

A new paper has revealed what its authors call "alarming" vulnerabilities in controls over Amazon's cloud service, but the problems were fixed before anyone could exploit them in real life. If they hadn't been addressed, the weaknesses could have allowed hackers to sidestep cryptographic protections and reprogram or delete customers' virtual computers and steal their data, the researchers say.

The paper—titled "All Your Clouds Are Belong to Us," a play on a decade-old Internet meme—was produced by several researchers based at Ruhr University in Germany. It showed flaws in the client controls of Amazon's Elastic Compute Cloud (EC2) service, which is used by a growing number of large Web companies including Foursquare and Yelp, government agencies including the National Renewable Energy Lab, media companies such as the Washington Post, and academic institutions such as the University of Barcelona and the University of Melbourne.

The principal hack described involves a messaging system that companies use to do things like create and delete virtual computers as needed. The researchers were able to change those messages in a way that Amazon's cryptographic authentication systems failed to detect. And Amazon's service would have executed the malicious instructions along with the proper ones. The approach exploited a specific kind of vulnerability first reported by IBM researchers in 2005.

The effects were potentially devastating. "One eavesdropped message—or a message gained another way—was enough to get control over the whole user's cloud," says Juraj Somorovsky, one of the researchers involved in the study. "Cloud interfaces are generally a prominent attack target. If an attacker compromises a cloud interface, he could misuse its vulnerabilities to get control over users' data." Users' computations could also be manipulated, he adds.

Kay Kinton, an Amazon spokeswoman, said in an e-mail statement that "the potential vulnerabilities reported by researchers [...] have been corrected and no customers have been impacted." She also disputed that data would have been at risk, saying that the process Amazon uses to store customer data would not have allowed even the researchers to see and expose passwords or other information.

This is the latest in a series of concerns over cloud security. In the cloud services offered by Amazon and other providers, computing is done by virtual machines generated in physical data centers, and virtual machines dedicated to different customers may be created on the same server. Other research has shown that it is sometimes possible to deliberately place a malicious virtual machine on the same physical server as a victim's machines, and use that virtual machine to launch various kinds of attacks.

While the ongoing research that exposed these problems strengthens cloud computing overall, the episode shows that the price of a single vulnerability can be potentially enormous as cloud services proliferate and the data they work with mushrooms in value.

"Scale makes things more vulnerable—you have more components interacting with each other," says Radu Sion, a computer scientist at Stony Brook University in New York. That creates a larger and more attractive target. Sion, who did not participate in the new research, heads the Cloud Computing Security Workshop, which was held alongside the ACM Computer and Communications Security Conference in Chicago last week and was where the paper was released.

As the virtual computers hosted by cloud providers grow in number and complexity, new attack methods of that sort are likely to arise, Sion predicts. The German research showed "a pretty serious vulnerability," he adds, "but it can be fixed and has been fixed."

Still, he contends that clouds are inherently more secure—and their operators better able to stay on top of new vulnerabilities—than thousands of millions of distributed users can ever be. And he says ongoing research in consultation with industry players, like that accomplished by the German experts, will work to keep commercial offerings as safe as possible. He adds, "I strongly believe the cloud is the way to go."