On September 17, 2009, Amazon Web Services published an article under their Security Bulletin to the report that was published by Thomas Ristenpart, Eran Tromer, Hovav Shacham, and Stefan Savage. Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds. *Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS), ACM, Chicago, IL,* November 2009.

Here is what they wrote in the article.

"

MIT and UC San Diego researchers publish report

September 17, 2009

A recent report describes cloud cartography research methods conducted on Amazon EC2 which could increase an attacker's probability of launching a compute instance on the same physical server as another specific target compute instance. While no specific attacks were identified in this paper, AWS takes any potential security issue very seriously and we are in the process of rolling out safeguards that prevent potential attackers from using the cartography techniques described in the paper.

In addition to investigating how to collocate compute instances on EC2 using cloud cartography, the paper goes on to present hypothetical side channel attacks which attempt to gain information from target instance once an attacker successfully has an instance running on the same physical host. 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.

While this report contained only hypothetical scenarios, we are taking the observations very seriously and will continue to investigate these potential exploits. We will also continue to develop features that create added levels of security for our users. Recent examples include AWS Multi-Factor Authentication (AWS MFA), which provides customers an additional layer of security to the administration of a customer's AWS account by requiring a second piece of information to confirm a user's identity. With AWS MFA enabled, users must provide a six-digit, rotating code from a device in their physical possession in addition to their standard AWS account credentials, before they are allowed to make changes to their AWS account settings.

Additionally, users can rotate access credentials (e.g., an AWS Access Key ID or X.509 Certificate). This enables users to seamlessly replace the existing access credential with the new one without incurring any downtime to applications. Applications can be made more secure by regularly rotating access credentials to further protect an account in the event access credentials are lost or compromised."

The URL for the same – http://aws.amazon.com/security/security-bulletins/mit-and-uc-san-diego-researchers-publish-report/