Researchers show how side-channel attacks can be used to steal encryption keys on Amazon's cloud servers

October 28 2015

Researchers at Worcester Polytechnic Institute (WPI) have demonstrated that RSA encryption keys, which are used by thousands of companies and organizations to protect the data and processes they entrust to cloud-based services, can be obtained using a sophisticated side-channel attack—despite recent efforts by cloud service providers and cryptography software developers to eliminate such vulnerabilities.

The research was described in a paper titled "Seriously, get off my cloud! Cross-VM RSA key recovery in a public cloud," published in the

International Association for Cryptologic Research's Cryptology ePrint Archive by a team led by Berk Sunar, professor of electrical and computer engineering, and Thomas Eisenbarth, assistant professor of electrical and computer engineering.

Supported by a $500,000 award from the National Science Foundation, the team used a combination of techniques to first create a virtual machine (essentially a remote computer running on a cloud server) on the same server as a target machine (a technique known as co-location). They then used the co-located machine to spy on the target. By observing how it accessed information in memory, they could determine when it was retrieving its RSA key (the code that protects data from unauthorized access). Finally, by charting the timing of the memory access they were able to deduce the key's actual numeric sequence.

"We believe this is the first report in the cryptography literature to describe a successful RSA key recovery attack in a commercial cloud environment," Sunar said.

Cloud computing is a service that enables companies and organizations to store information and run computer applications without making their own investments in actual computer hardware or employing IT staff. Instead, the cloud providers maintain large arrays of computer servers that users access through the Internet. Using the cloud instead of investing in dedicated hardware makes it easier and less expensive for companies to scale up their operations. In fact, the cloud has helped enable the rapid expansion of companies like Netflix and Dropbox.

Researchers have been aware of vulnerabilities in public cloud servers since it was demonstrated six years ago that the co-location of virtual machines is possible and that sensitive information can be extracted from a co-located "victim machine." Cloud service providers, like Amazon Web Services, and developers of security software and cryptographic libraries, including Libgcrypt, have responded to published reports of successful attacks with patches that have addressed known vulnerabilities. In fact, a new patch available from Libgcrypt addresses the very vulnerabilities that the WPI team took advantage of, though it is up to the users of cloud services, not the cloud providers, to install the patch. That means many users may still be unprotected.

The focus of the WPI paper is a type of cloud service called infrastructure as a service, or IaaS, in which users run computer applications on virtual machines. Typically, many virtual machines can operate independently on each server. Because providers like Amazon maintain thousands of servers, it was once thought that virtual machines would be more difficult to attack than physical computers, since an attacker would have to be able to determine which server was hosting a target machine and then set up its own "spy" machine on the same server. That was believed to be all but impossible.

In 2009, a team at the University of California San Diego and MIT showed how they could predict which server was likely to host a particular virtual machine. They then created a number of virtual machines until they successfully co-located one on the target's server. While security features in the server environment prevent a co-located virtual machine from directly accessing information on the target, a number of studies have shown that it is possible to observe how a virtual machine loads information into memory caches in the server and glean clues that can be used to deduce sensitive information. These techniques, collectively, are known as cache side-channel attacks.

Security patches have closed off a number of these side-channels and also rendered previous methods for determining co-location ineffective. The WPI team devised a new co-location technique that makes use of what is known as the last-level cache, which is memory shared by all of the virtual machines running on a server. By performing a variety of tests on this cache, they were able to systematically zero in on instances of co-location.

Once co-located with a target machine, the researchers launched a prime-and-probe attack, which involves filling a portion of the cache with data and then observing how the target responds. The cache is designed to hold frequently accessed information and to lessen the need for the CPU to retrieve information from the server's random-access memory (RAM). Since it takes less time to access the cache than it does to retrieve data from RAM, the time it takes the server to access the cache or RAM provides clues about the type of information being retrieved. By observing the patterns of memory access, the WPI team was able to determine when the target machine was retrieving the 2,048-bit RSA code and then to deduce the actual bits of the RSA key.

"Our research has shown that covert channels still exist and may be exploited by side channel attacks," Eisenbarth noted. "Crypto keys are safe if users follow security best practices and stick to well-maintained and fully patched crypto libraries. The efforts of Amazon and other providers to address known vulnerabilities in the public cloud have made it harder for anyone attacking these services."

Provided by Worcester Polytechnic Institute

Citation: Researchers show how side-channel attacks can be used to steal encryption keys on Amazon's cloud servers (2015, October 28) retrieved 24 April 2024 from https://phys.org/news/2015-10-side-channel-encryption-keys-amazon-cloud.html