New research improves ability to detect malware in cloud-computing systems

September 21 2010

Researchers from North Carolina State University have developed new software that offers significantly enhanced security for cloud-computing systems. The software is much better at detecting viruses or other malware in the "hypervisors" that are critical to cloud computing, and does so without alerting the malware that it is being examined.

Cloud computing is being hailed as a flexible, affordable way of offering computer resources to consumers. Under the cloud-computing paradigm, the computational power and storage of multiple computers is pooled, and can be shared by multiple users. But concerns exist about hackers finding ways to insert malware into cloud computing systems. A new program called HyperSentry, developed by researchers at NC State and IBM, should help allay those fears.

HyperSentry is security software that focuses on protecting hypervisors in virtual computing clouds. Hypervisors are programs that create the virtual workspace that allows different operating systems to run in isolation from one another - even though each of these systems is using computing power and storage capability on the same computer.

Specifically, HyperSentry enables cloud administrators to measure the integrity of hypervisors in run time - meaning that the administrators can check to see whether a hypervisor has been breached by a third party, while the hypervisor is operating.

"The concern is that an attacker could compromise a hypervisor, giving

them control of the cloud," says Dr. Peng Ning, professor of computer science at NC State and co-author of a paper describing the research. If a hypervisor is compromised, the attacker could do almost anything: access users' sensitive information; use the cloud's computing resources to attack other Internet entities; spread malware; etc.

"HyperSentry solves two problems," Ning says. "It measures hypervisor integrity in a stealthy way, and it does so in the context of the hypervisor." Context is important, Ning explains. To effectively identify hypervisor problems you need to look at the hypervisor program memory and the registers inside the central processing units (CPUs) that are actually running the program. (The registers are the internal memory of CPUs.) This is important because intelligent malware can conceal itself from security programs that look only at the memory where the hypervisor is supposed to be located - they can effectively make themselves invisible to such security programs by modifying certain registers of the CPU and thus relocating the infected hypervisor elsewhere. By ensuring in-context measurement, HypeSentry can successfully track where the infected hypervisor is actually located and thus defeat such intelligent malware.

The fact that HyperSentry can check the integrity of a hypervisor in a stealthy way - checking the hypervisor without the hypervisor being aware of it - is important too. If a hypervisor is aware that it is being scrutinized, and has already been compromised, it can notify the malware. The malware, once alerted, can then restore the hypervisor to its normal state in order to avoid detection. Then the malware effectively hides until the security check is over.

Once a compromised hypervisor has been detected, a cloud administrator can take action to respond to the compromise, such as shutting down the computer, performing additional investigations to identify the scope of the problem and limiting how far the damage can

spread.

More information: The research is being presented Oct. 5 at the 17th ACM Conference on Computer and Communications Security in Chicago, Ill.

Provided by North Carolina State University