New Advances in Self-Policing Cloud Computing

Vahab Pournaghshband
Computer Science Department
University of California, Los Angeles
vahab@cs.ucla.edu

Cloud computing is a style of computing in which dynamically scalable and often virtualized resources (e.g., CPU, memory, storage, and network bandwidth) are provided as a service over the Internet. This model is considered affordable for cloud users as they avoid the significant financial overheads associated with deploying, maintaining, and managing datacenter environments, and instead pay just for the usage of these resources (the you-pay-as-you-use model). However, this benefit comes at a price: the cloud user, who is concerned about the privacy of its information, now needs to trust the cloud provider since it has no control over the computing infrastructure. This indeed has been a major concern in cloud computing.

Currently, the trusted cloud providers, to guard against malicious users, are using Virtual Machines (VM). Virtual machines are primarily used to isolate computing processes for each cloud user. Now the question is will the malicious user be able to retrieve the private information belong to the victim, assuming he correctly manages to discover that his code runs on the same server as the victim customer (given each user is running in separate VMs)? Unfortunately, Virtual machines still do not achieve complete isolation since some resources may be implicitly shared among VMs, such as the Last Level Cache (LLC) on multi-core processors and memory bandwidth which could potentially be exploited by the attacker. Microsoft, however, recently claimed that cache hierarchy aware core assignment and page coloring based cache partitioning could potentially defend against such attacks.

To further secure cloud computing infrastructure, we can monitor the executable to be run in the cloud and detect malicious activities. However,

integrity of the monitor is itself requires verification. This is also the case for a running OS, which ensuring its integrity must be validated by some independent source. This problem has been studied over years, and as a result, using Trusted Platform Modules (TPM) is widely used solely for this purpose. The approach is to take information needed for the OS integrity validation and store the result in TPM (a separate trusted co-processor whose state cannot be compromised by a potentially malicious host system). In case of cloud computing, due to virtualization, the integrity measurements are potentially done in out- of-reach of the attackers, so the attacker cannot corrupt the VM monitor. However, even with the help of a VM monitor, a new potential challenge is the semantic gap between the level of details that the VM monitor is observing and the level of details required to make any security decision. As the worst case, the source code of the guest OS (the operating system running in the VM) running on a cloud server is not available (e.g. Windows), making the elimination of this gap a daunting task.

A recent research performed by IBM introduces a secure introspection technique as a number of steps to both determining the guest OS and validating its integrity. Its first step requires reading Interrupt Descriptor Table (IDT) from the virtual CPU registers. It further determines the running guest OS by analyzing the content of IDT as well as the use of white-list of known operating systems (i.e. cryptographic hashes of normalized executable code). By continuous analyzing of all discovered data structure used in the guest OS, it can detect if any unauthorized modification occurred at its run-time.

At last, the idea is to use the unique properties of cloud computing, lack of privacy and many available resources, to create a more secure cloud computing infrastructure as Markus Jakobsson, a principal scientist at Palo Alto Research Center (PARC), says: "if we don't use it, we are missing out on something truly amazing."

References

[1] Christodorescu, M., Sailer, R., Schales, D. L., Sgandurra, D., and Zamboni, D. *Cloud security is not (just) virtualization security: a short paper.* In Proceedings of the 2009 ACM Workshop on Cloud Computing Security (Chicago, Illinois, USA, November 13 - 13, 2009). CCSW '09. ACM, New York, NY, 97-102.

[2] Ristenpart, T., Tromer, E., Shacham, H., and Savage, S. *Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds*. In Proceedings of the 16th ACM Conference on Computer and Communications Security (Chicago, Illinois, USA, November 09 - 13, 2009). CCS '09. ACM, New York, NY, 199-212.

[3] Raj, H., Nathuji, R., Singh, A., and England, P. *Resource management for isolation enhanced cloud services*. In Proceedings of the 2009 ACM Workshop on Cloud Computing Security (Chicago, Illinois, USA, November 13 - 13, 2009). CCSW '09. ACM, New York, NY, 77-84.