Title: Strengthening the Security and Privacy of Virtualized Computing Infrastructures

Ping (Julie) Yang and Kartik Gopalan
Computer Science, Binghamton University

Virtualization can enhance the security in a shared cloud computing infrastructure through greater isolation between virtual machines (VM). However, virtualization also gives rise to new security challenges for which the current technology is inadequately prepared. For example, VM management techniques can increase the vulnerability of confidential data in ways not anticipated by the users of VMs. Massive consolidation of VMs in data centers can increase the potential for successful attacks that can rapidly propagate through the shared infrastructure.

Out team is investigating ways to strengthen the security and privacy guarantees provided by virtualization technologies that are fundamental to the success of future cloud computing infrastructures. This includes ways to secure the cloud platforms as well as help developers build better applications that limit the lifetime of confidential data in virtualized settings. Our current investigations are along the following directions:

- ***Protecting privacy and confidentiality:*** VM checkpointing can store confidential user data (such as passwords or credit card numbers) in a persistent "snapshot" without users' knowledge. VM checkpoints are usually stored for a long time and may be shared among users, which drastically prolongs the lifetime and vulnerability of confidential data in the VM. We are developing techniques to limit the exposure of confidential data by safely excluding such data from VM checkpoints while maintaining stability and consistency of VMs when restored later from the checkpoint.
- ***Strong and scalable isolation:*** Sensitive VM workloads can become vulnerable when VMs with different trust levels are co-located on the same physical server. Current approach is to retrofit and patch traditional access control mechanisms from non-virtualized settings into virtualized environments, which can quickly become complex and unscalable. We are developing new techniques for maintaining strong isolation and scalable trust management while retaining the benefits of consolidation using co-location.
- ***Securing the trusted computing base:*** Shared cloud environments can expose VMs to potential attacks by third parties. For instance, attackers may be able to modify the memory contents of a VM in migration, or subvert its applications and the operating system. In addition, implicit sharing of data among VMs result in security breaches and unintended information leakage. We are investigating new approaches to maintain security of the trusted computing base against such vulnerabilities while minimiznig the performance impact of the security mechanisms.