New Research Offers Security For Virtualization, Cloud Computing

April 27 2010, by Matt Shipman

Virtualization and cloud computing allow computer users access to powerful computers and software applications hosted by remote groups of servers, but security concerns related to data privacy are limiting public confidence - and slowing adoption of the new technology. Now researchers from North Carolina State University have developed new techniques and software that may be the key to resolving those security concerns and boosting confidence in the sector.

"What we've done represents a significant advance in security for cloud computing and other virtualization applications," says Dr. Xuxian Jiang, an assistant professor of computer science and co-author of the study. "Anyone interested in the virtualization sector will be very interested in our work."

Virtualization allows the pooling of the computational power and storage of multiple computers, which can then be shared by multiple users. For example, under the cloud computing paradigm, businesses can lease computer resources from a data center to operate Web sites and interact with customers - without having to pay for the overhead of buying and maintaining their own IT infrastructures. The virtualization manager, commonly referred to as a "hypervisor," is a type of software that creates "virtual machines" that operate in isolation from one another on a common computer. In other words, the hypervisor 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. This is the technique that enables concepts like

cloud computing to function.

One of the major threats to virtualization - and cloud computing - is malicious software that enables computer viruses or other malware that have compromised one customer's system to spread to the underlying hypervisor and, ultimately, to the systems of other customers. In short, a key concern is that one cloud computing customer could download a virus - such as one that steals user data - and then spread that virus to the systems of all the other customers.

"If this sort of attack is feasible, it undermines consumer confidence in cloud computing," Jiang says, "since consumers couldn't trust that their information would remain confidential."

But Jiang and his Ph.D. student Zhi Wang have now developed software, called HyperSafe, that leverages existing hardware features to secure hypervisors against such attacks. "We can guarantee the integrity of the underlying hypervisor by protecting it from being compromised by any malware downloaded by an individual user," Jiang says. "By doing so, we can ensure the hypervisor's isolation."

For malware to affect a hypervisor, it typically needs to run its own code in the hypervisor. HyperSafe utilizes two components to prevent that from happening. First, the HyperSafe program "has a technique called non-bypassable memory lockdown, which explicitly and reliably bars the introduction of new code by anyone other than the hypervisor administrator," Jiang says. "This also prevents attempts to modify existing hypervisor code by external users."

Second, HyperSafe uses a technique called restricted pointer indexing. This technique "initially characterizes a hypervisor's normal behavior, and then prevents any deviation from that profile," Jiang says. "Only the hypervisor administrators themselves can introduce changes to the

hypervisor code."

More information: The research, "HyperSafe: A Lightweight Approach to Provide Lifetime Hypervisor Control-Flow Integrity," will be presented May 18 at the 31st IEEE Symposium On Security And Privacy in Oakland, Calif.

Provided by North Carolina State University