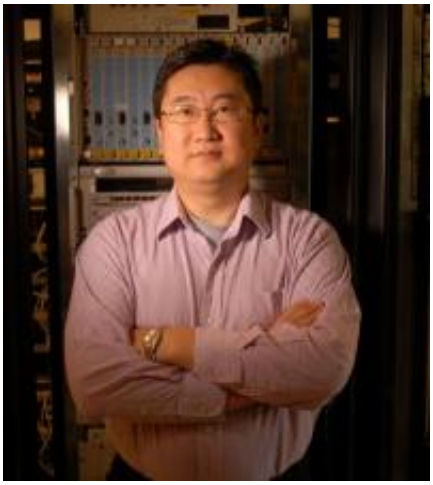
New technique offers enhanced security for sensitive data in cloud computing

October 5 2011



The research team, led by Peng Ning, has developed a new approach to cloud security, to protect sensitive information and workload. Credit: Roger Winstead, North Carolina State University

Researchers from North Carolina State University and IBM have developed a new, experimental technique to better protect sensitive information in cloud computing – without significantly affecting the system's overall performance.

Under the cloud-computing paradigm, the computational power and storage of multiple computers is pooled, and can be shared by multiple users. 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. A longstanding concern in cloud computing is that attackers could take advantage of vulnerabilities in a hypervisor to steal or corrupt confidential data from other users in the cloud.

The NC State research team has developed a new approach to cloud security, which builds upon existing hardware and firmware functionality to isolate sensitive information and workload from the rest of the functions performed by a hypervisor. The new technique, called "Strongly Isolated Computing Environment" (SICE), demonstrates the introduction of a different layer of protection.

"We have significantly reduced the 'surface' that can be attacked by malicious software," says Dr. Peng Ning, a professor of computer science at NC State and co-author of a paper describing the research. "For example, our approach relies on a software foundation called the Trusted Computing Base, or TCB, that has approximately 300 lines of code, meaning that only these 300 lines of code need to be trusted in order to ensure the isolation offered by our approach. Previous techniques have exposed thousands of lines of code to potential attacks. We have a smaller attack surface to protect."

SICE also lets programmers dedicate specific cores on widely-available multi-core processors to the sensitive workload – allowing the other cores to perform all other functions normally. A core is the brain of a computer chip, and many computers now use chips that have between two and eight cores. By confining the sensitive workload to one or a few cores with strong isolation, and allowing other functions to operate separately, SICE is able to provide both high assurance for the sensitive workload and efficient resource sharing in a cloud.

In testing, the SICE framework generally took up approximately 3

percent of the system's performance overhead on multi-core processors for workloads that do not require direct network access. "That is a fairly modest price to pay for the enhanced security," Ning says. "However, more research is needed to further speed up the workloads that require interactions with the network."

More information: The paper, "SICE: A Hardware-Level Strongly Isolated Computing Environment for x86 Multi-core Platforms," was co-authored by Ning; NC State Ph.D. student Ahmed Azab; and Dr. Xiaolan Zhang of IBM's T.J. Watson Research Center. The paper will be presented at the 18th ACM Conference on Computer and Communications Security, Oct. 17-21 in Chicago, Ill.

Provided by North Carolina State University