



Presenter's name : Kenichi Kourai
Technical Session :
Category : Oral

Secure Monitoring of Virtual Machines with Memory Split into Multiple Hosts

Kenichi Kourai^{1*} and Kouki Yamato¹

¹ Kyushu Institute of Technology, 680-4 Kawazu, Iizuka, Fukuoka 820-8502, Japan

* kourai@ksl.ci.kyutech.ac.jp

Abstract: Recently, Infrastructure-as-a-Service clouds provide virtual machines (VMs) with a large amount of memory. To enable such VMs to be flexibly migrated to other hosts, a technique called split migration has been proposed. Split migration divides a large-memory VM into small pieces and transfers them to multiple hosts, i.e., one main host and one or more sub-hosts. After split migration, the VM runs across these hosts and exchanges memory data between the main host and a sub-host when necessary. Such a VM is called a split-memory VM. However, it becomes difficult to run intrusion detection systems (IDSes) outside a split-memory VM for securely monitoring its internal state because its memory is split.

We present VMemTrans for secure monitoring of split-memory VMs. Using VMemTrans, IDSes can monitor a split-memory VM as if its memory were not split. To achieve this, VMemTrans enables IDSes running in the main host to transparently access the memory of sub-hosts. VMemTrans provides two methods for obtaining memory data from sub-hosts. One is that VMemTrans obtains necessary memory data and passes it to IDSes. The other method is that VMemTrans makes a VM itself exchange necessary memory data. We have implemented VMemTrans in KVM and examined the execution performance using the above two methods. As a result, it was shown that the two methods have a trade-off.

Keywords: virtual machines, migration, clouds, security, monitoring, intrusion detection systems