Detecting Migration of Virtual Machines

The Challenge: Detect Malicious Migration of Virtual Machines in the Cloud

- Virtualization technologies are fundamental for the cloud
- Prototypes of Virtual Machine-based Rootkits (SubVirt, BluePill) proved feasibility of attacks based on virtualization technologies
- How to detect malicious migration of virtual machines as basis for security mechanisms?

The Approach: Distant Monitoring of Roundtrip-time to Virtual Machines

- Hypothesis: migrating a virtual machine causes characteristic patterns in roundtrip-time
- Experimental setup: distant monitoring of migration of Ubuntu virtual machine based on Proxmox hypervisor
- Parameters: different load conditions (CPU, network, etc.) of migrated virtual machine

The Results: Distant Detection of Malicious Migration Feasible

- Migration processes produce characteristic patterns in roundtrip-time that are detectable with reasonable overhead
- Characteristic patterns of roundtrip-time are not affected by load conditions of migrated machine
- Distant monitoring as basis for detecting malicious behavior feasible