Risks and Challenges of Live Virtual Machine Migration

Presenter:
Jon Oberheide
University of Michigan
Live VM Migration

- Transfer of a VM from one physical machine to another with little or no service downtime

High Availability
Enhanced Mobility
Dynamic Load Balancing
Live Migration Methodology

- Methodology
  - Copy machine state (memory) over network

- Goals
  - Minimize service downtime and migration duration

- Iterative Precopy
  - VMotion (Vmware VI3), XenMotion (Xen Server)

---

Stop and Copy  Iterative Precopy  Demand Migration

High Downtime  Hybrid  Low Downtime
Low Duration   Hybrid   High Duration
A Trip Down Memory Lane

• Physical machines
  • Machine state protected by MMU/hardware
  • Physical attacks (firewire device DMA)

• Virtual Machines
  • VM state protected by VMM/hypervisor
  • Software attacks (weak VMM isolation)

Can we further weaken isolation boundaries?
Isolation of Machine State

- Virtual machine migration
  - Full VM state exposed to network
  - Trade off of increased risk for functionality and management
  - Authentication, confidentiality, isolation concerns
VM Migration Security

- (In)security of migration protocol
  - Unauthenticated, insecure migration data plane
  - VMotion/XenMotion susceptible to MITM attacks

- Full access granted to VM state
  - OS/kernel memory
  - Application state
Exploiting VM Migration

- Passive Attacks
  - Snarf sensitive data, passwords, keys in memory

- Active Attacks
  - Manipulate auth. services
    - sshd, /bin/login, etc
  - Manipulate kernel structures
    - slip rootkits into memory
VMBR Hoisting

- Virtual Machine-Based Rootkits
  - Slip in extra virt layer (a la SubVirt/Blue Pill/Vitriol)
Addressing the Risks

- Encrypt it?
  - Requires authentication to ensure integrity
  - PKI adds deployment and key management complexity
  - Not implemented by vendors

- Isolate it?
  - Separate networks for migration data
  - Physical or virtual (VLAN segmentation)
  - Recommended by VMware best practices guide
Lessons Learned

“Ok, I configured VLANs for isolation, hacked in PKI/TLS support myself, and trained kittens to migrate my VMs. Am I still at risk? Is this even important any more?”

• Yes and no:
  • Isolation not a feature of virtualization, it's a challenge
  • Beware of hidden risks in new functionality
  • Best practices and configuration audits are key
Questions?

Q&A

• Contact info:
  • Jon Oberheide <jonojono@umich.edu>
  • PhD candidate, University of Michigan
  • Advisor: Farnam Jahanian
  • Research Group: http://www.eecs.umich.edu/fjgroup/