Virtualization Security Discussion

Paul Moore

August 2012

Threats to a Virtualized System

- Attacks from the host system
  - Host system has full access to local guests and data
- Attacks from other guest systems on the host
  - Malicious guests can exploit host vulnerabilities
  - Other guests are vulnerable once the host is exploited
- Attacks from the network
  - The network is a scary place, virtualization or not
  - All systems are vulnerable to malicious guest traffic

Protecting the Guest Against Malicious Hosts

- Difficult problem to solve due to host/guest relationship
  - Host has full access to the guest resources
  - Host can modify guest execution at will
    - Ability to circumvent guest's security functionality
- Guests need to be able to verify/attest the host
  - No verification means no guarantee of guest security
  - Authentication, authorization, and integrity are critical
- Guests need to be able to protect data when offline
  - Data is accessible, even when the guest is not

Protecting the Host Against Malicious Guests (1)

- With QEMU/KVM a guest is just another process
  - We should assume is malicious from the beginning
- Virtualization does isolate, but isn't bulletproof
  - Every piece of software has bugs, including QEMU
- QEMU is no different than any process once exploited
  - Guest can directly access the host system
  - Launching point for further exploits, privilege escalation

Protecting the Host Against Malicious Guests (2)

- Host must provide confinement of QEMU/KVM guests
  - Restrict guest access to only guest owned resources
    - Disk images, network interfaces, USB/PCI devices, etc.
  - Limit the available kernel interfaces
    - System calls, netlink, /proc, /sys, etc.
  - Libvirt/sVirt and seccomp help provide confinement
- Move privileged ops from QEMU to management layer
  - Leverage libvirt infrastructure when available
    - Guest network setup and configuration
    - Disk image FD passing

Protecting the Guest Against Hostile Networks

- Anyone can use the network as an attack vector
  - Guests are vulnerable both directly and indirectly
    - Applications running inside the guest are always vulnerable
    - Remote management interfaces vulnerable as well
  - Quality of service can be an issue on loaded systems
- Host and guest firewalls can solve a lot of problems
- Extending the guest separation across the network
  - Network virtualization for multi-tenant solutions
  - Guest IPsec and VPN services on the host

More Information

- My Contact Information
  - Paul Moore
  - pmoore@redhat.com

- Linux Security Summit
  - Thursday and Friday during LinuxCon
  - Information in the LinuxCon schedule booklet
  - http://kernsec.org/wiki/index.php/Linux_Security_Summit_2012