Secure Virtualization Infrastructure

John McDermott  NRL  john.mcdermott@nrl.navy.mil

4 December 2012
Does anyone know how we discovered the International Date Line?
*Important cloud security infrastructure problems this talk is not about:

* Network security
* Protection from insiders and rogue administrators
* Pixie dust cryptographic solutions
* Governance and security standards
* Geopolitical security
* Legal
* Incident handling
* Web / SOA security

* It is about the hard problem of co-residence attacks
*Cloud computing breaks hardware separation

*Hardware separation (separate clouds) breaks cloud computing

*“Whoever gets to the interface first wins.”
Cloud computing breaks hardware separation

Host Hardware

Control Plane

Networks

Attack

Virtualization Technology

Host Virtual Machine
Cloud computing breaks hardware separation

- Attack
- Network
- Control Plane
- Host Virtual Machine
- Virtualization Technology
- Platform Hardware

6 December 2012
Hardware separation breaks cloud computing
* “Whoever gets to the interface first wins.”
* Type 1 VMM does not mean “runs on bare metal.”
* Privileged (not the same as sensitive) instructions are instructions that can be managed for security, by the hardware
* Sensitive instructions are instructions that could be used to tamper with virtualization ≠ privileged instructions
  * Not just synchronous machine instructions but also interrupts and configuration commands, e.g. UEFI, ACPI, and IO/APIC
  * NUMA configuration, e.g. inter-socket communication fabrics like Intel Quick Path Interconnect
  * SR/IOV configuration commands

What Does **Type 1** Really Mean and Do I Have One?
* When a VM migrates, what does it leave behind?
* When a VMM recycles memory from one VM to another, is all recycled memory always cleared first?
* Caching

or is it mostly cleared?

Resource Reuse
* Can you mark different VMs so that they never run at the same time on the same platform?
* Is your VMM designed to resist hypercall flooding attacks?
* Is your VMM designed to mitigate covert timing channels and other forms of information leakage via shared hardware?
* Does your VMM log and report internal events or just what the control plane sees?
* Can you whitelist internal resources such as hypercalls and privileged instructions on a per VM basis?

* Do you have a VMM feature that internally responds to repeated policy violations or do violations require external network-based intervention?

* Does your VMM have a security feature that lets you partition your cloud to contain the spread of intrusions or malware while you wait for a patch?
How significant is the network address of a VM that migrates a dozen times in 1 hour, such that it co-resides with more than 100 different VMs?
* Latest commodity architectures have switching point-to-point interconnection, with an MMU for each core.
  * AMD Hyper Transport
  * Intel Quick Path Interconnect

* reads/writes (interrupts?) pass through multiple CPUs and sockets - locking your VM to a specific socket does not always keep its data and instructions within that socket

* cache snooping?