Trusted Computing in Cloud Computing and Virtualization

CSC 495/680 Lecture
December 1 and 6, 2010

What is Cloud Computing

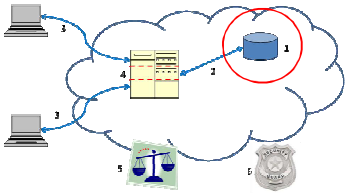
- First, a video to explain cloud computing and relation to virtualization:

  http://www.youtube.com/watch?v=XdBd14rjcs0

- Things to note:
  - Sending data to a remote provider
  - Importance of virtualization and "run anywhere" goal

Areas for Security Concerns

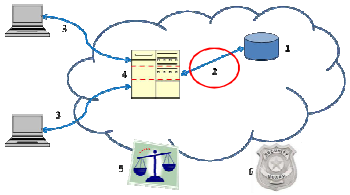
From "Cloud Computing and Security – A Natural Match", by the TCG



1. Data at rest. Encryption works great for stored data.
   - Paper talks about "self-encrypting drives" (i.e., hard drives that encrypt at the hardware level).
     - Is this sensible in the cloud?
     - Who are you protecting from?
     - Does the same person "own" all data on a drive?

Areas for Security Concerns

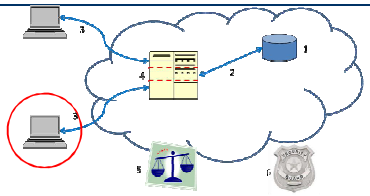
From "Cloud Computing and Security – A Natural Match", by the TCG



2. Securing data in transit.
   - Confidential communication is easy (SSL/TLS)
   - Authentication is tricky (and the next point)

Areas for Security Concerns

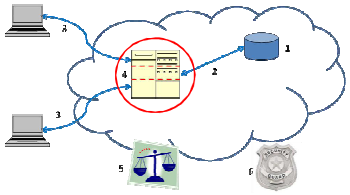
From "Cloud Computing and Security – A Natural Match", by the TCG



3. Authentication – some new challenges in the cloud!
   - Company "owns" authentication info – cloud run by someone else
   - Secure distributed authentication is needed!
     - TPM key management can provide stronger solutions than passwords
   - Communication between auth and resource: IF-MAP (Interface for Metadata Access Points)

Areas for Security Concerns

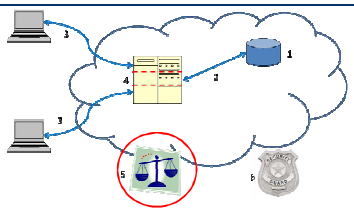
From "Cloud Computing and Security – A Natural Match", by the TCG



4. Separation between customers – customers could be competitors!
   - Strongly depends on virtualization
   - TPM attestation can build trust in hypervisor / VM infrastructure

Areas for Security Concerns

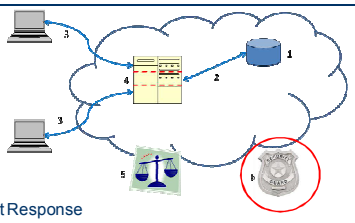
From "Cloud Computing and Security – A Natural Match", by the TCG



5. Cloud legal and regulatory issues.
   - Outsourcing to "best practice" security implementations helps in compliance
   - Provider practices policy can be backed up with hardware enforcement

Areas for Security Concerns

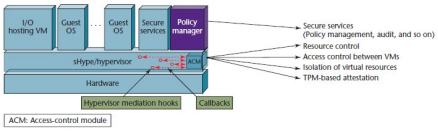
From "Cloud Computing and Security – A Natural Match", by the TCG



6. Incident Response
   - For automated response (limit damage), need real-time notification
     - IF-MAP works for this!

sHype Architecture

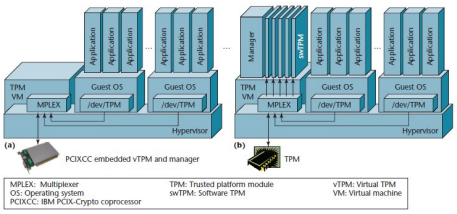
From: "Virtualization and Hardware-Based Security" (Perez, Sailer, and van Doorn)



- Hypervisor can enforce strong separation between virtualized containers.
- sHype is simple enough to enable sensible attestation

TPM Virtualization in sHype

From: "Virtualization and Hardware-Based Security" (Perez, Sailer, and van Doorn)



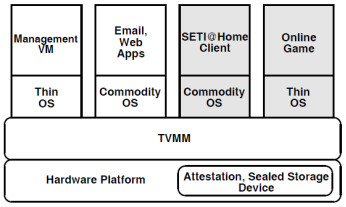
- Big question: How can you "virtualize" a hardware device that gets security from being a HW device?!?!
- Answer: Simulate, but use attestation (and underlying HW) to ensure simulation is secure

sHype: Other Notes

- sHype is the basis of a complete solution: IBM Research's "Trusted Virtual Data Center"
- TPM virtualization can actually use a more powerful cryptographic module (the PCIXCC) when it is available, and it might be worth the investment in a server environment
- Some talk about peripherals supporting secure virtualization in their design

Terra Architecture

From: "Terra: A Virtual Machine-Based Platform for Trusted Computing" (Garfinkel, Pfaff, Chow, Rosenblum, and Boneh)



- Terra predates IBM work on sHype (2003 vs 2008)
  - Clearly influenced sHype
- One interesting point: "Closed box VM" vs "Open box VM"

Notes on Terra

- Designed in the TPM v1.1 days, so required full static root of trust / trusted boot up through Terra's TVMM
  - Although could easily be adapted to DRTM
- Was proposed not long after details of Microsoft's NGSCB were released
  - NGSCB relied on a single OS (not virtualization)
  - NGSCB had a single "open box" – everything else closed
- Paper describes several trusted apps
  - "Trusted Quake"
  - Trusted Access Points