Security and Privacy in Public Clouds

David Lie
Department of Electrical and Computer Engineering
University of Toronto

Cloud Computing

- Cloud computing can (and is) applied to almost everything today.

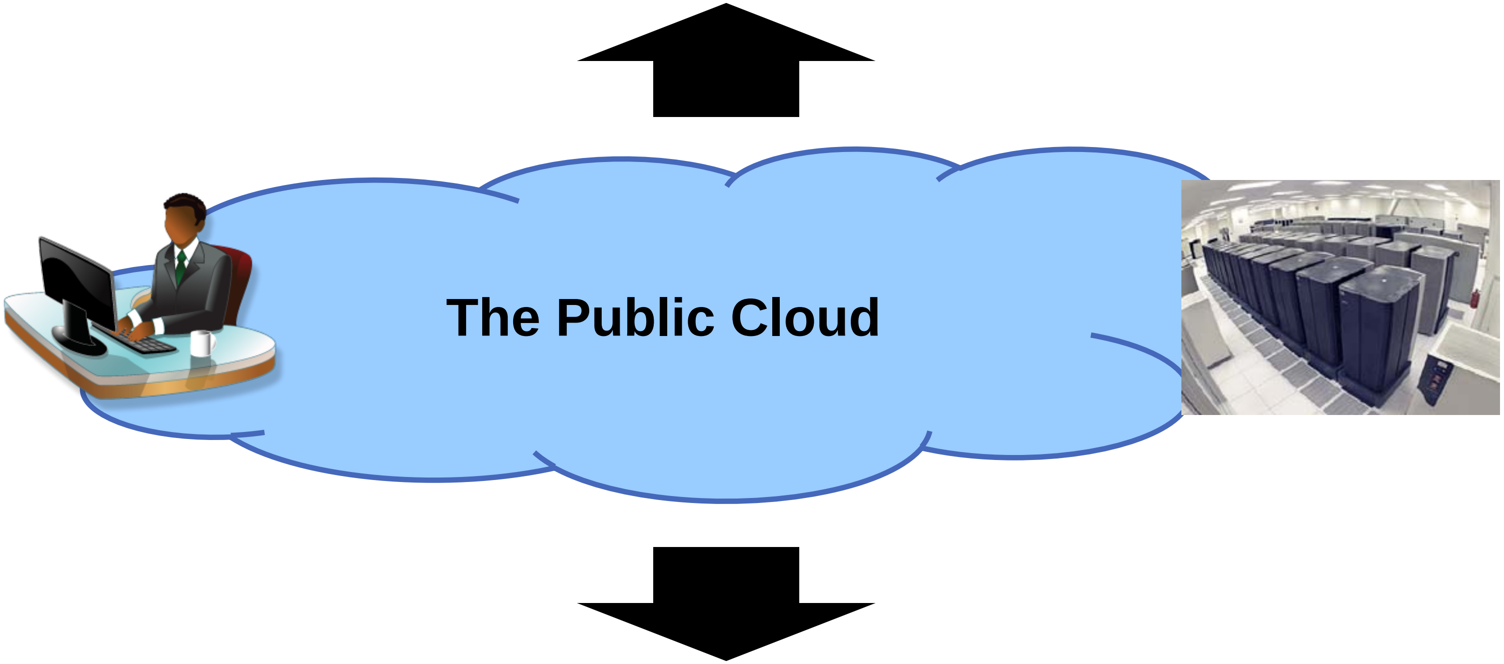
- NIST is working on a definition:

"Cloud computing is a model for enabling convenient, on-demand **network access** to a **shared pool of configurable computing resources** (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction ..."

Outsourcing of critical infrastructure to a common third party

Cloud Security

Threats to the Cloud Provider



The Public Cloud

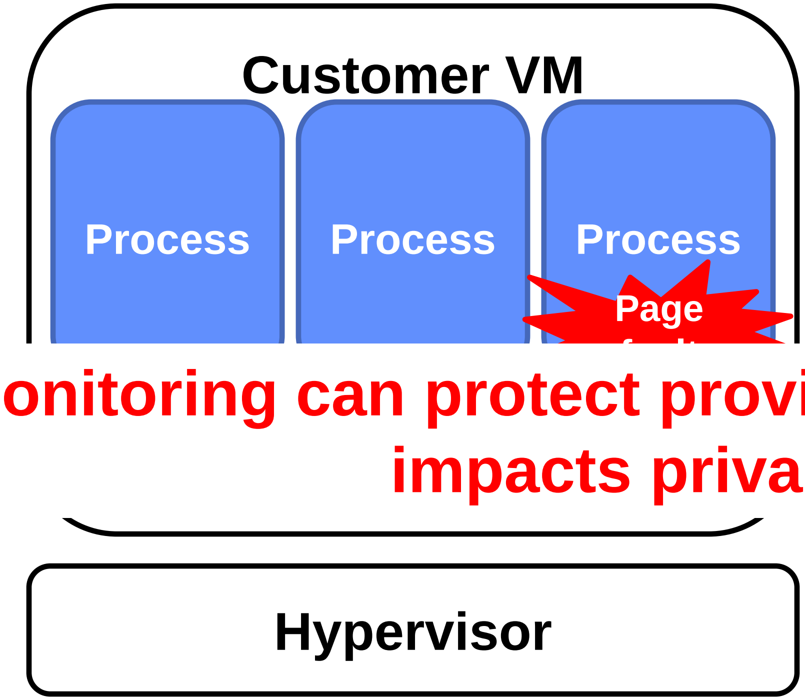
Threats to the Cloud User

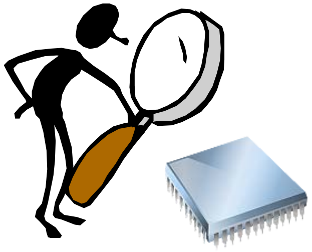
Threats to the Cloud Provider

- Miscreants can abuse the cloud provider’s resources:
  - Spam
  - Use infrastructure to attack other computers
  - Hosting illegal content

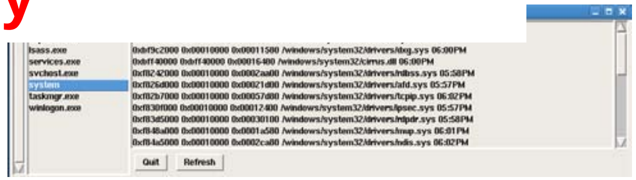
- This has consequences for the cloud provider:
  - Damage to reputation. Customers are leery of sharing infrastructure with questionable parties
  - Technical consequences: Shared IPs blacklisted
  - Legal ambiguity

Solution: Monitoring Users





Monitoring can protect provider and user but impacts privacy



```
lsass.exe      0xbf9c2000 0x00010000 0x00011580 /windows/system32/drivers/dxg.sys 06:00PM
services.exe   0xbff40000 0xbff40000 0x00016400 /windows/system32/cirrus.dll 06:00PM
svchost.exe    0xf8242000 0x00010000 0x0002aa00 /windows/system32/drivers/ndbss.sys 05:58PM
system         0xf826d000 0x00010000 0x00021d00 /windows/system32/drivers/afd.sys 05:57PM
taskmgr.exe    0xf82b7000 0x00010000 0x00057d80 /windows/system32/drivers/tcpip.sys 06:02PM
winlogon.exe   0xf830f000 0x00010000 0x00012400 /windows/system32/drivers/ipsec.sys 05:57PM
               0xf83d5000 0x00010000 0x00030100 /windows/system32/drivers/rdpdr.sys 05:58PM
               0xf848a000 0x00010000 0x0001a580 /windows/system32/drivers/nmp.sys 06:01PM
               0xf84a5000 0x00010000 0x0002ca80 /windows/system32/drivers/ndis.sys 06:02PM
```

- Patagonix (Usenix Security, 2008)
  - Identify malware
  - Identify misconfigured or vulnerable machines

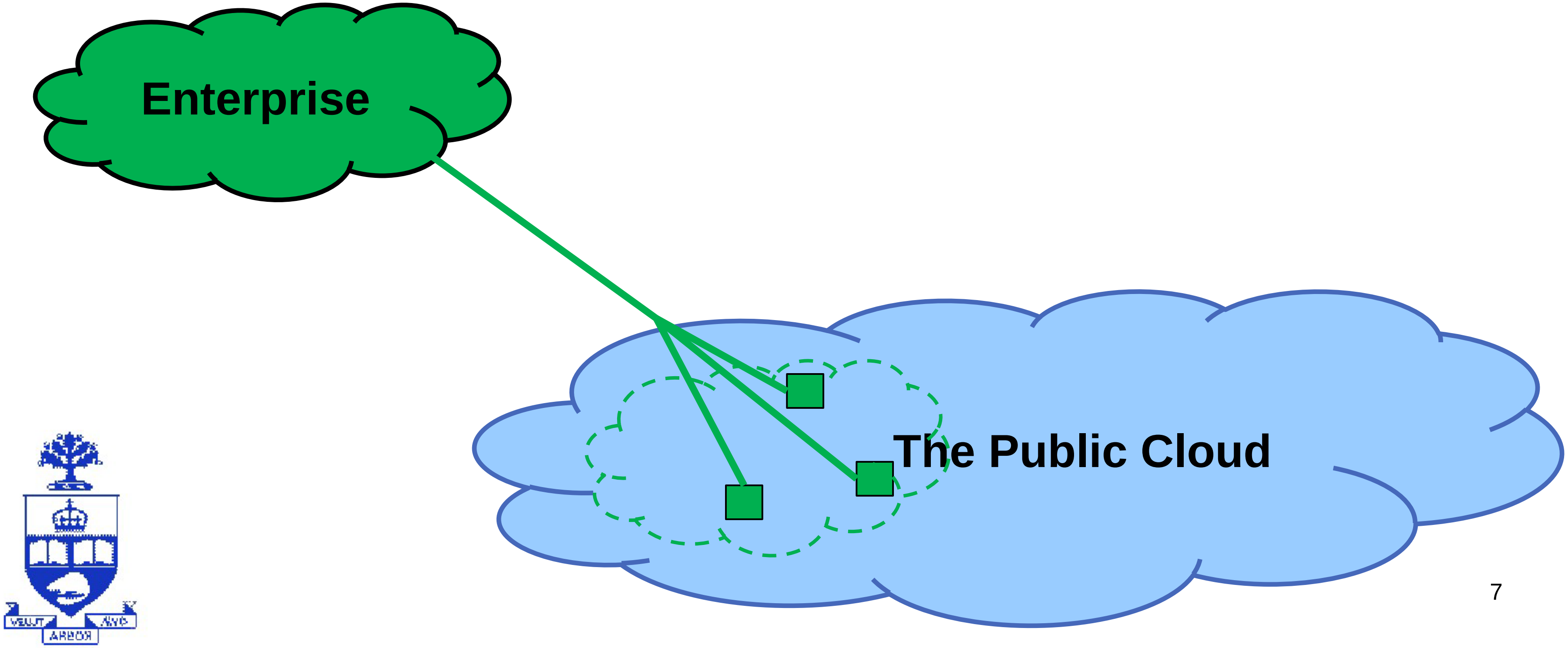
Threats to the Cloud User

- Threats to the cloud user:
  - Loss of control: hardware is no longer under physical control
  - Shared infrastructure: information leaks, privacy
  - Unpredictable behavior: reliance on yet another party may create unforeseen outages or degraded performance
  - Information leakage, loss of privacy and control

Obstacles to cloud adoption by enterprises

Virtual Private Clouds

- Virtual Private Cloud (HotCloud, 2009):
  - Use VPN, VLAN and Virtualization (Xen) to give customers the illusion that they are on a secure private cloud.
    - VPN/VLAN protects all network traffic
    - Virtualization layer provides isolation from other customers



Virtual Private Clouds

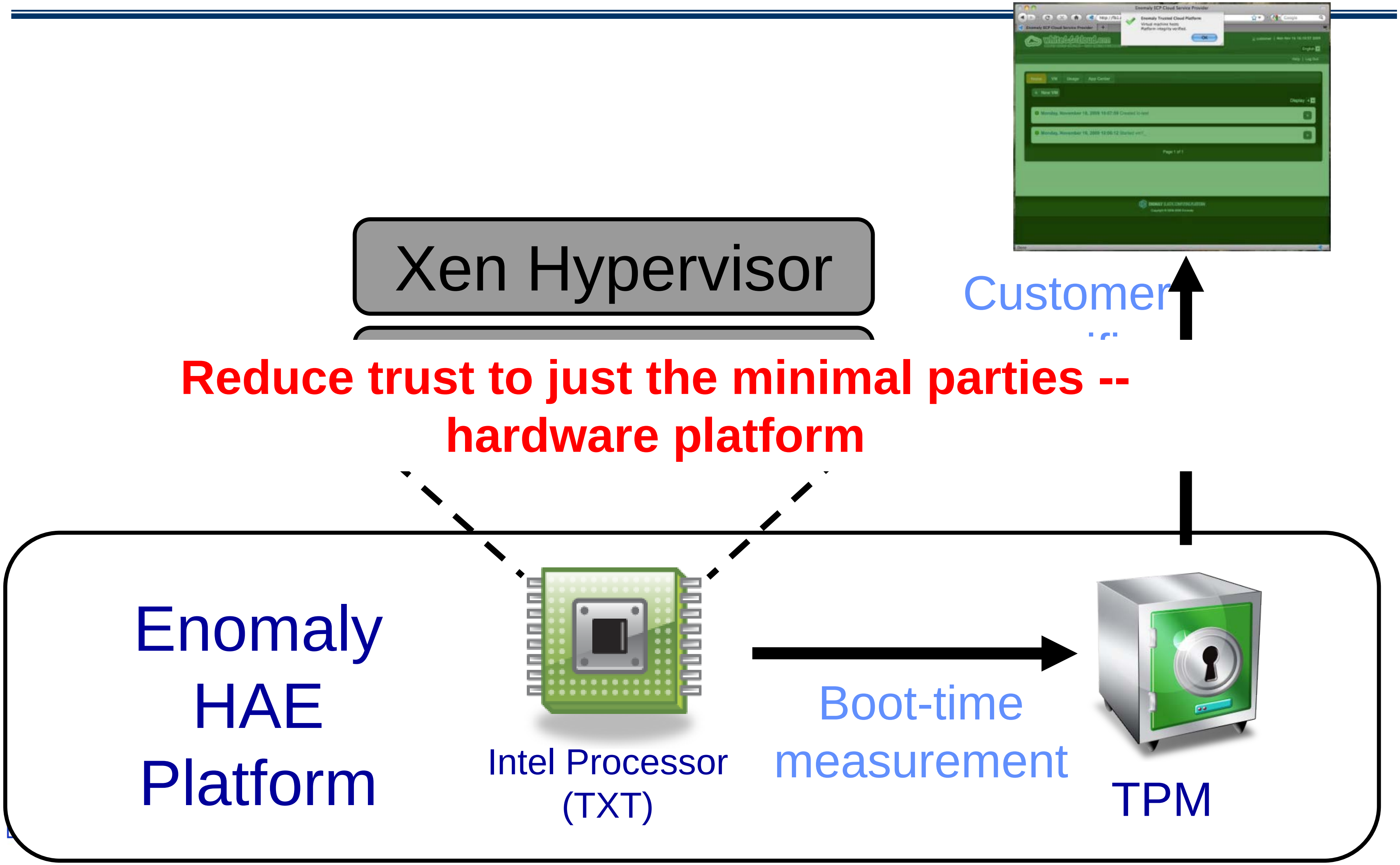
- However, this assumes an almost ideal threat environment:
  - Hypervisor could have a vulnerability:
    - Malicious customer could compromise other VMs
  - Cloud provider could confuse customer VMs/data/configurations:
    - Data could be leaked to other customers

Current solution: “Trust us” – not acceptable

cleanup:

- Data could be left in memory or on disk and accessible to next user
- Cloud provider could be malicious:
  - Disgruntled employees could cause damage

Enomaly HAE Platform



Enomaly Trusted Cloud Platform
Virtual machine hosts
Platform integrity verified.

Reduce trust to just the minimal parties -- hardware platform

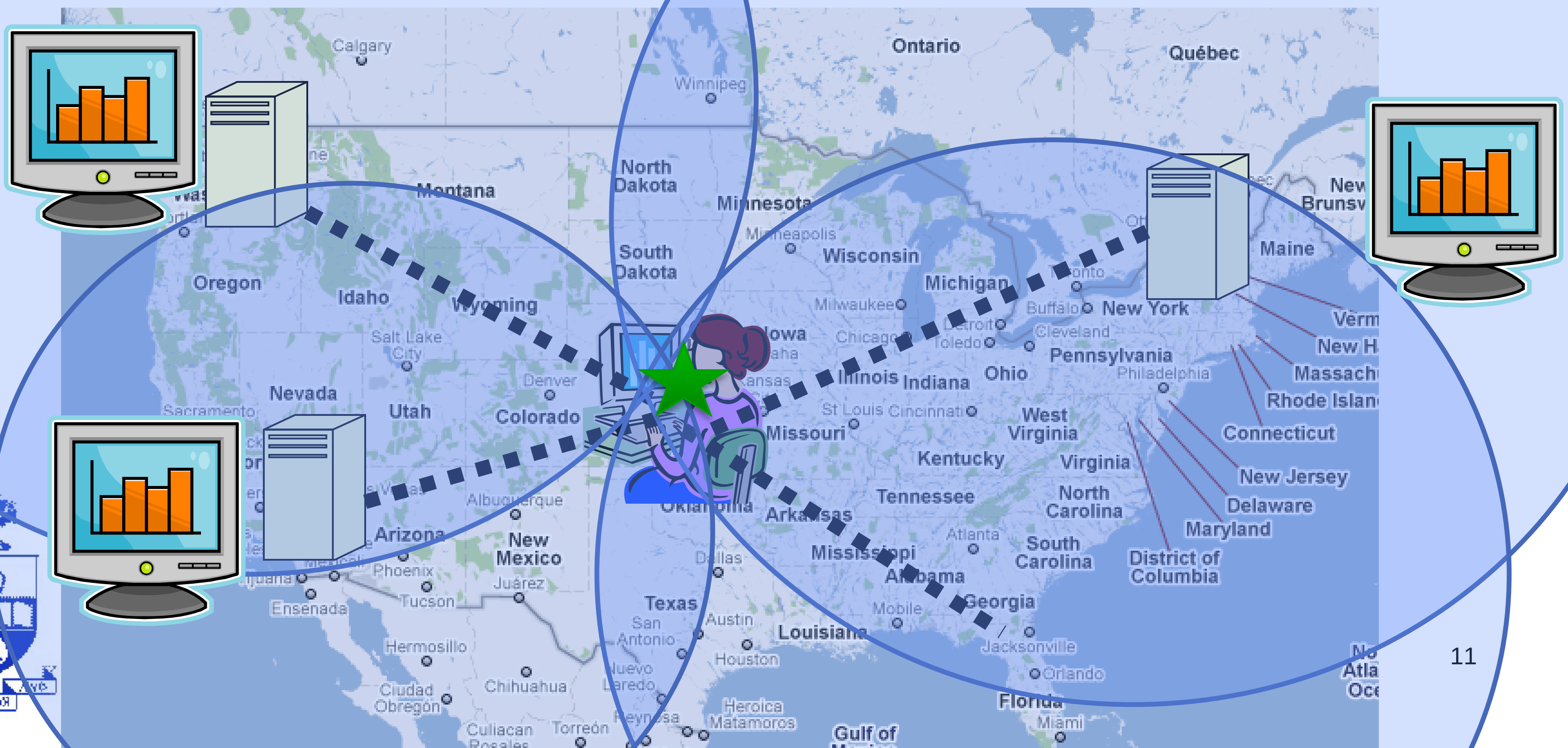
Even stickier issues

- Even if the cloud provider is competent and benign, many non-technical issues:
  - Electronic Discovery
  - Compliance and Audit
  - Jurisdiction and Legal
  - Termination

Users will want or be required to restrict cloud services to be hosted in certain geographic regions

Measurement-based geolocation

- Delay-based geolocation example
  - Constraint-based geolocation [Gueye et al. ToN '06]



Summary

- Cloud providers are exposed to the security competencies of their customers:
    - This has implications for not only the provider but the provider’s other customers
    - Cloud providers need *robust* and *non-intrusive* monitoring techniques. Tension with user privacy.

- Security for cloud users also is a big problem:
    - Users need to maintain control of information, protect privacy
    - A lot can be achieved through cryptography but open problems still remain:
        - How to ensure that keys are never leaked (swap, transferred over network during migration)
        - How to permit checkpointing of VMs for HA, but prevent replay attacks