1. Motivation

- Cloud computing seen as the next **architectural shift** in computing.
- Multiple products already available, e.g., Amazon EC2/S3 and Microsoft Azure.
- Dell plotted a $1 billion investment in the cloud in 2011.
- Considerable amount of research around the cloud.

2. Malicious Insider Threat

- Biggest shift in the cloud is having data processing and storage **entrusted** to the cloud provider.
- #3 in the Cloud Security Alliance (CSA) top threats list.
- Consider the risks when facing a typical rogue administrator, but **amplified** by the architecture.
- Is there an impact on confidentiality/privacy?

3. Malicious Insider threat – facts

- Data processed in the cloud is **not protected**, e.g., a malicious insider can **compromise private keys** [RC11].
- Powerful attacks can be orchestrated using virtual machine introspection, e.g., **compromise confidentiality** of a private inter-VM channel.
- Cryptography on its own is **not enough**, not even with Fully Homomorphic Encryption (FHE) [VDJ10].

4. Preventing Malicious Insiders - our solution

- Deploy **integrity-protected** virtual machine monitors (VMMs), a.k.a., hypervisors.
  - Respect security design requirements [VMQ+10].
  - For the malicious insider threat ensure that the **principle of least privilege** is respected in the memory access model used for the management VM [RvM12].
- Use trustworthy computing to provide integrity measurements of hypervisors to remote clients.
  - **Integrity measurement**, cryptographic hash of software/binary code.
  - **Remote attestation**, enables a verifier to establish trust in an initially untrusted platform.

5. Solution Explained

- This solution prevents malicious insider attacks against inter-VM channels.
- The xen_gntalloc driver performs an hypercall to register the shared page in Xen (1).
- Following, Xen flags that page has not accessible to the management VM or domain-0 (2).
- When attack code running in domain-0 tries to obtain access to that page (3), Xen rejects it based on the security flag (4).

6. Limitations and Future Work

- Depends on the kernel, which **increases** the trusted computing base.
- It **only protects** inter-vm communication the rest of a virtual machine’s memory still vulnerable to attack.
- Implement a solution that applies the **principle of least privilege** to the memory access model of domain-0.

7. References

- Francisco Rocha and Aad van Moorsel, *Refining the memory access model for xen’s domain-0*, May 2012.