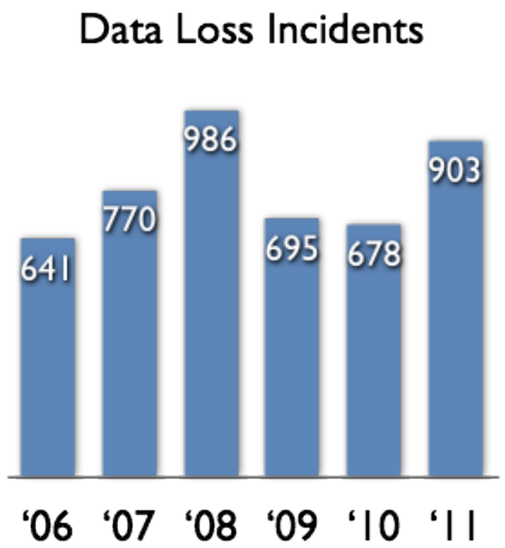
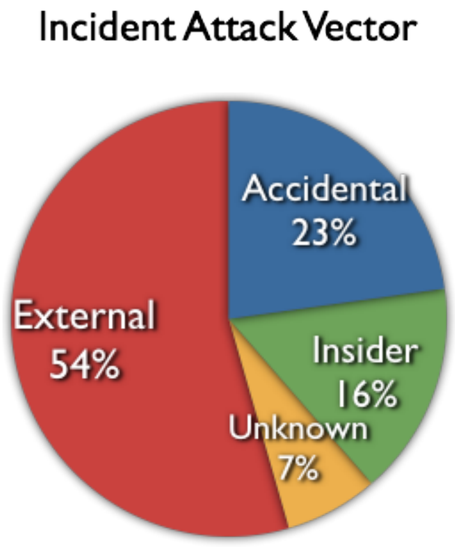
COMPREHENSIVE SYSTEM VERIFICATION IN CLOUD COMPUTING PLATFORMS

Joshua Schiffman, Hayawardh Vijayakumar,
Yuqiong Sun, and Trent Jaeger

- Cloud computing offers on-demand resources with reduced administrative effort for developers
- However, fears of **data loss** and **security breaches** have stifled adoption by businesses and governments
- Current system verification mechanisms are **inflexible** and **ill-suited for the complexity** of cloud platforms
- We present a cloud architecture that **efficiently** verifies **comprehensive** integrity requirements

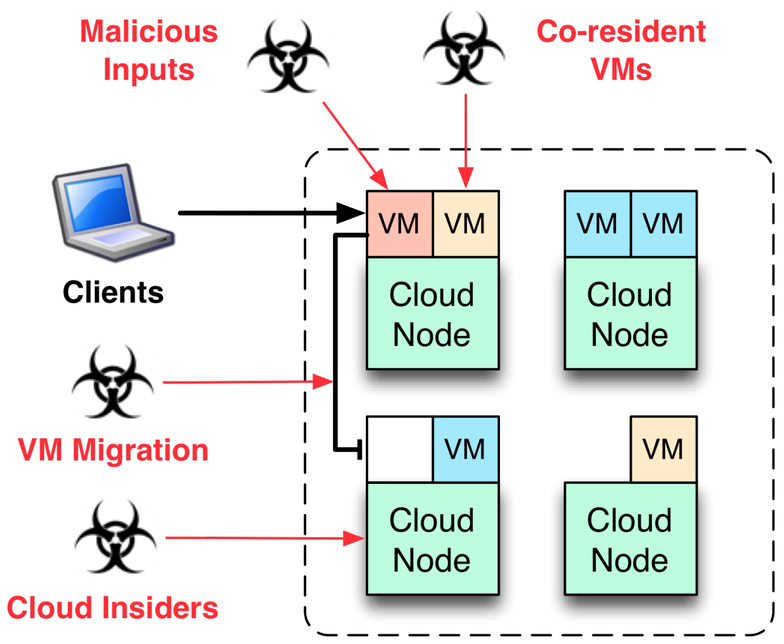




CLOUD VERIFICATION CHALLENGES

Clouds **complicate** system verification

- Clouds **hide** physical machine identity
- Application VMs **depend on cloud nodes**
- Hosted applications may be affected by **co-resident VMs**
- VM **migration** requires verification of new cloud node
- Difficult to inspect **runtime changes** to VM configurations



Multiple administrative domains with differing integrity requirements:

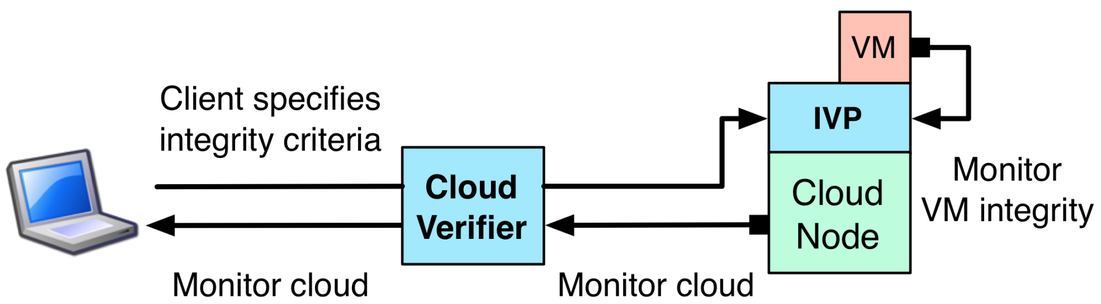
- Cloud administrators
- Application developers
- Data owners
- Clients

Each wishes to **verify** the integrity of the components they rely upon in the cloud

CLOUD VERIFIER

Cloud-wide system integrity verification service

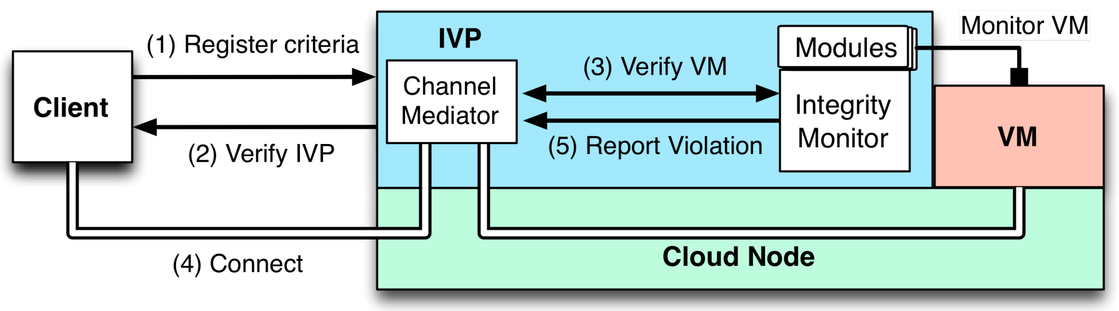
- Ensures **cloud node integrity** based on **cloud's criteria**
- Clients **verify** the cloud verifier's integrity
- Clients own criteria is **pushed** to the target VM's cloud node
- An integrity verification proxy (IVP) **monitors VM integrity**



INTEGRITY VERIFICATION PROXY

Cloud node service to enforce client criteria over connections

- Mediates a TLS tunnel between client and a hosted VM
- Monitors VM integrity both at loadtime and runtime
- Uses VM introspection to track VM integrity enforcement



OPENSTACK INTEGRATION

Currently integrating cloud verifier into the OpenStack cloud platform

- Cloud verifier (CV) is an independent, verifiable service in the cloud
- Added a `nova-verify` project to monitor `nova-compute` servers
- Clients establish persistent tunnel to CV to detect reboots
- IVP implementation being ported over to Intel chips from AMD.
- Evaluating performance on several cloud applications

PUBLICATIONS

- J. Schiffman, H. Vijayakumar, T. Jaeger. **Verifying System Integrity by Proxy**, *5th International Conference on Trust and Trustworthy Computing*.
- J. Schiffman, T. Moyer, H. Vijayakumar, T. Jaeger, and P. McDaniel. **Seeding clouds with trust anchors**. In *Proceedings of the 2010 ACM workshop on Cloud computing security workshop (CCSW '10)*. New York, NY, USA, 43-46.
- J. Schiffman, T. Moyer, T. Jaeger, and P. McDaniel. **Network-based Root of Trust for Installation**. IEEE *Security & Privacy*. 9(1), 40-48, 2011.
- T. Jaeger and J. Schiffman, **Outlook: Cloudy with a Chance of Security Challenges and Improvements**, IEEE *Security & Privacy*, 8(1), 77-80, Jan.-Feb. 2010

Sponsored by National Science Foundation grants CNS-1117692 and CNS-0931914