Trusted End Host Monitors for Securing Cloud Datacenters

Alan Shieh†‡
Srikanth Kandula‡
Albert Greenberg‡
Cloud workload is dynamic and hostile

**Traditional datacenters**
- Infrastructure supports small # of internal clients
  - Software and topology change *slowly*
  - Can exploit natural network chokepoints
  - Feasible to audit app code

**Cloud datacenters**
- Infrastructure is shared among many untrusted tenants
  - Rapidly changing config
  - Chokepoints torque network topology
  - Too many apps to audit!

- Scaling requires more agility & flexibility
- Exploits more likely
- Exploits can use cloud resources to do more damage
  - Attack other tenants
  - External/internal DoS

Need new approach
Insight: Cloud datacenters can help!

• Cloud data centers tend to be:
  – Centrally controlled
  – Homogeneous hardware & software
    • Clean slate feasible
  – Have strongly isolated, trusted functionality
    • VMs, TPMs, management coprocessors

• Our approach: **Trust end host monitors**
  Push enforcement from network to end hosts
  – Distributed across many hosts
  – Runs in trusted layers
In-network enforcement

- Deep Packet Inspection Appliance
- Firewall
- DoS protection
- Allow to
- Trusted component
Summary

- Cloud DCs have unique challenges & opportunities
  - Address, exploit these with trusted end host monitors
- Runs on commodity network & end host hardware
  - Simplifies controller design
  - Improves scalability
  - Reduces cost
- Status: Built prototype from VMs, trusted NIC (Intel AMT)