Isolated Mini-domain for Trusted Cloud Computing

Jaewon Choi, Jongse Park, Jinho Seol, Seungryoul Maeng
Department of Computer Science, KAIST
jwchoi, jspark, jhseol, maeng@camars.kaist.ac.kr

**Related Work**

- **Trusted Computing**
  - The computer system running as expected
    - Developed by Trusted Computing Group
    - Enforced by components in Trusted Computing Base (TCB)
  - **Trusted Computing Base (TCB)**
    - The set of all hardware and software components that are critical to the system security
    - **TCB verification**
      - A great expense is needed when TCB size is large
      - It is better to reduce TCB size as much as possible
      - Developed by Trusted Computing Group
    - **Trusted Platform Module (TPM)**
    - Tamper-resistant hardware
    - Used to assure the integrity of platform

- **Cloud Computing**
  - Infrastructure-as-a-Service (IaaS) Cloud
    - User data and computation on IaaS are processed on remote machines managed by the cloud provider
    - **User must completely trust the cloud provider**
  - **Cloud User**
    - Cloud Manager
    - Cloud Provider
    - VM
    - Hypervisor
    - Node

- **Motivation**
  - **Goal**
    - Separates device drivers from the management domain
    - Minimizes Trusted Computing Base (TCB)
  - **Challenges**
    - **Integrity of Mini-domain**
      - Minimized by the management domain
    - **Mini-domain should be included in TCB**
      - **Management domain contains**
        - Device drivers
        - VM management tools
        - User level processes
      - **Problems of the mngmt domain**
        - Large code size
        - Vulnerabilities
        - Malicious administrator
      - **Management domain is untrustworthy!**

- **Protocol Placement**
  - **Vulnerable authentication protocol**
    - Only management domain directly accesses hardware devices
    - Protocol must request CA certificate from management domain
    - CA certificate is required for authentication protocol

  - **The management domain should be trustworthy**

**Proposed Architecture**

- **Management Domain**
  - Protocol
  - Trusted Hypervisor
  - Hardware

- **Trusted Cloud Computing Platform (TCCP)**
  - Minimizes code size of the mini-domain

**Prototype Implementation**

- **Management domain**
  - VM
  - Hypervisor
  - Trusted Hypervisor
  - Protocol

- **Guest VM**
  - Virtual memory
  - Guest virtual memory
  - Guest physical memory
  - Hypervisor encrypts guest memory

**Conclusion**

- **Conclusion**
  - **Identifying problems on TCCP implementation**
    - Entire code of management domain should be trusted
  - **Isolated Mini-domain**
    - Accesses PCI devices directly
    - Secures secret data under the malicious management domain
    - Runs node authentication protocol on mini-domain
    - Reduces hypervisor complexity
  - **Limitation & Future work**
    - Fine-grained code size analysis of the mini-domain
    - Minimizing the code size of the mini-domain