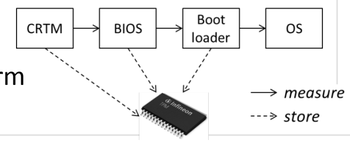
Isolated Mini-domain for Trusted Cloud Computing

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

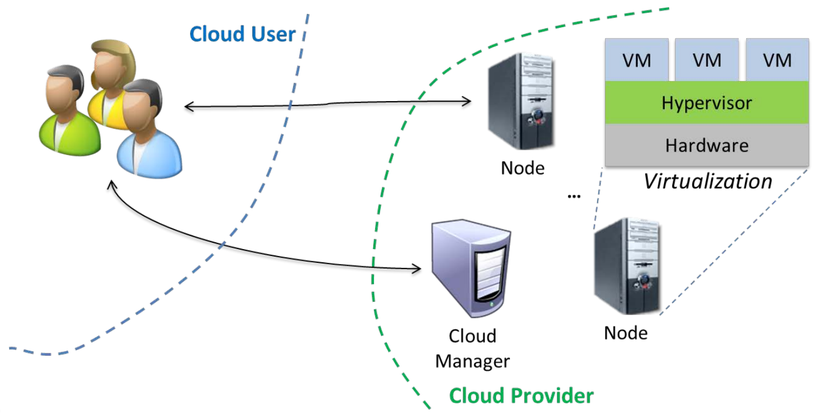
Trusted Computing

- 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 *[Michael Hohmuth'04][Lenin Singaravelu'06]*
  - Trusted Platform Module (TPM)
    - Tamper-resistant hardware
    - Used to assure the integrity of platform



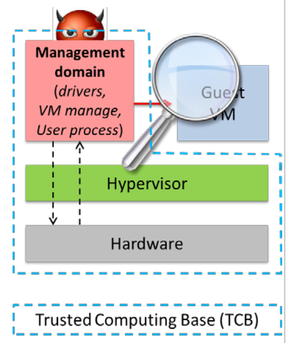
Cloud Computing

- 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



Trusted Computing in Virtualization

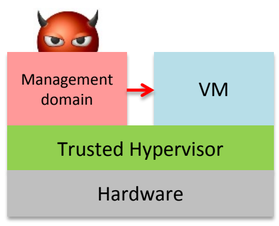
- Hypervisor
  - Manages guest VMs on the virtualized environment
- Management domain contains
  - Device drivers
  - VM management tools
  - User level processes
- Problems of the mngmt domain
  - Large code size
    - Vulnerabilities *[Lenin Singaravelu'06]*
  - Buggy device drivers
    - 7 times larger bug rate than that of kernel *[Andy Chou'01]*
  - Malicious administrator
    - Privilege to access guest VM memory *[Bryan D. Payne'07]*



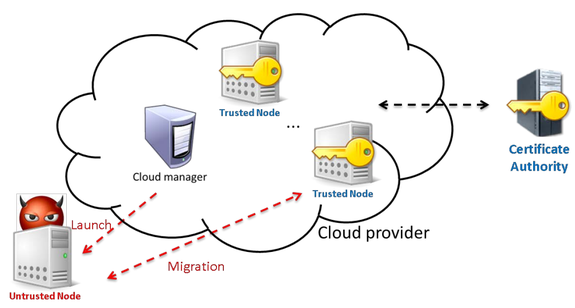
-> *Management domain is untrustworthy!*

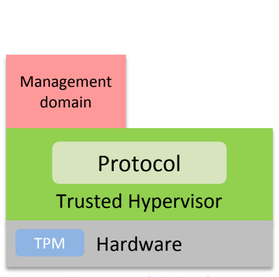
Related Work

- Trusted Hypervisor
  - Protects VMs from a malicious management domain
    - Disaggregation *[Derek G. Murray'08]*
      - Domain building process
    - Memory encryption *[Chunxiao Li'10]*
      - Hypervisor encrypts/decrypts guest VM memory
  - Protects guest VMs under a single system



- Trusted Cloud Computing Platform (TCCP) *[Nuno Santos'09]*
  - Confines VMs to be run on trusted nodes

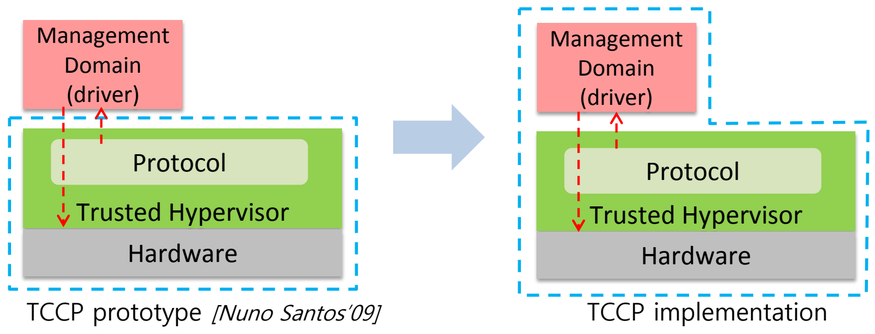




Motivation

- Problems of TCCP implementation *[Nuno Santos'09]*
  - 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



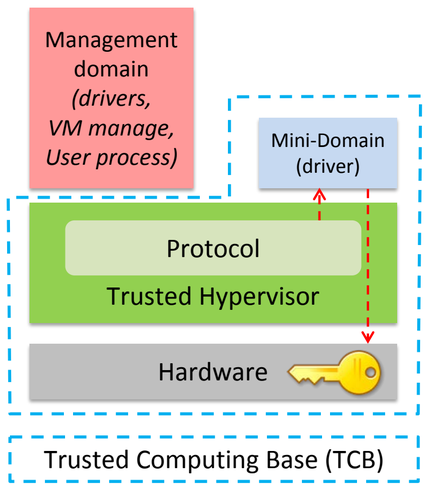
Proposed Architecture

Goal

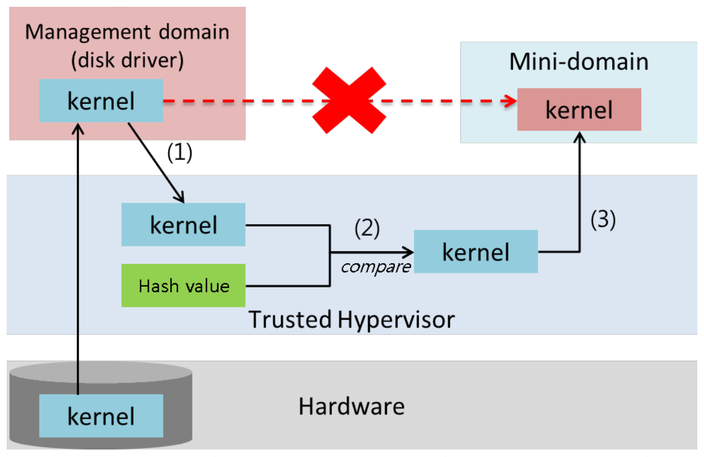
- Separates device drivers from the management domain
- Minimize Trusted Computing Base (TCB)

Challenges

- Integrity of Mini-domain
  - Mini-domain is created by the management domain
  - Mini-domain should be included in TCB on the untrustworthy management domain
- Vulnerable Authentication Protocol
  - Protocol increases hypervisor complexity
  - Hypervisor runs with the highest privilege in the system



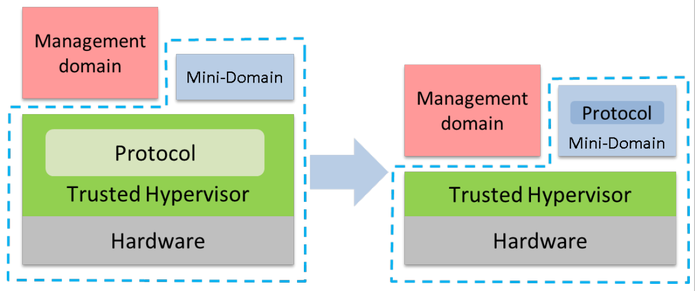
Challenge – Integrity of Mini-domain



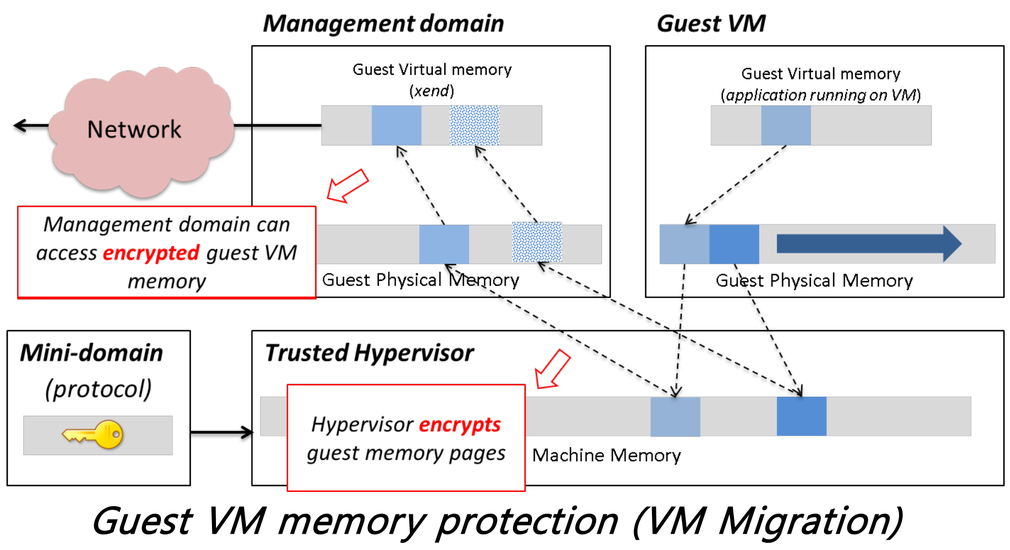
(1) Mngmt domain forwards kernel image to hypervisor
(2) Hypervisor checks integrity of mini-domain kernel
(3) Hypervisor loads kernel image to mini-domain memory

Challenge – Protocol Placement

- Vulnerable authentication protocol
  - Protocol requires cryptographic functions and libraries
- Moving protocol functions to mini-domain
  - Minimizing hypervisor complexity
  - Improving system security *[Udo Stein Berg'10]*



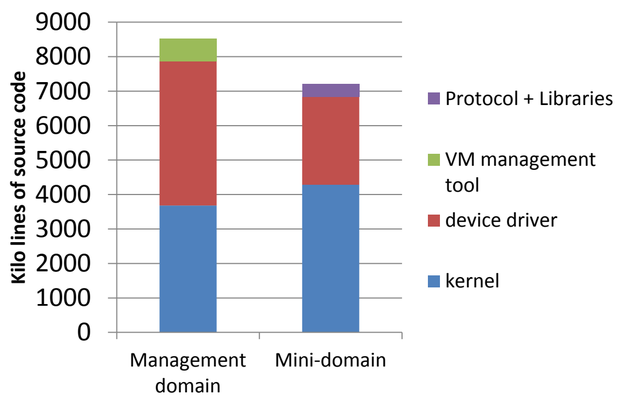
Prototype Implementation



Guest VM memory protection (VM Migration)

Evaluation

Comparison of the TCB size



- The code size of mini-domain is 15.4% compared to the management domain

Conclusion

- Identifying problems on TCCP implementation *[Nuno Santos'09]*
  - The entire code of management domain should be trusted
- Isolated Mini-domain
  - Accesses PCI devices directly
  - Securely gets 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