SMU SINGAPORE MANAGEMENT UNIVERSITY

LARC LIVING ANALYTICS RESEARCH CENTRE

Carnegie Mellon University

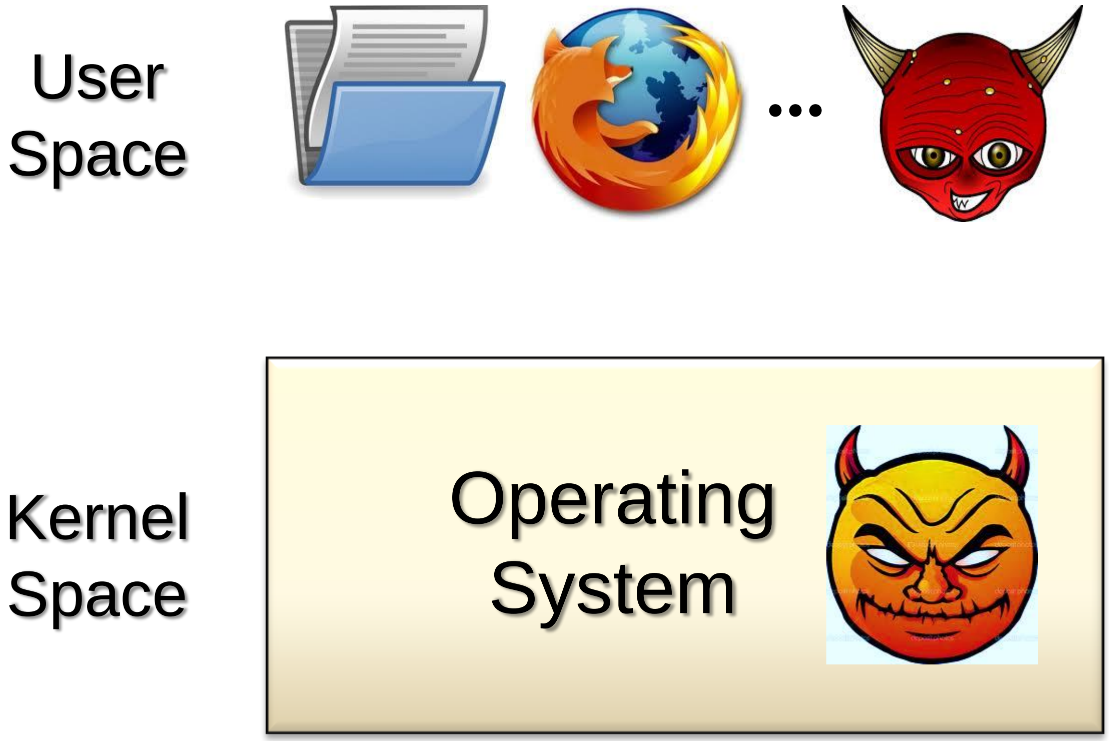
Guardian: Hypervisor as Security Foothold for Personal Computers

Yueqiang Cheng, Xuhua Ding

Singapore Management University (SMU)

The International Conference on Trust & Trustworthy Computing (TRUST),
17-19 Jun 2013, United Kingdom (London)

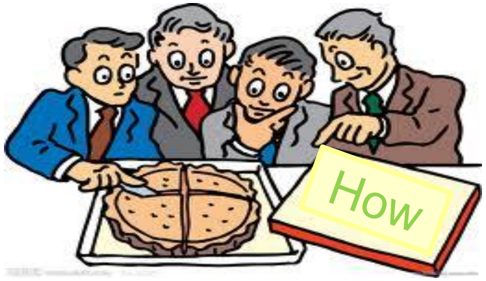
Background



Foothold Needed!!

Possible Solutions

- Rewriting OS
  - – Too costly to be practical



- Adopting new security-capable devices
  - – Compatibility
  - – Difficult to widely deploy

- Adopting hypervisor
  - – Without ***availability*** guarantee
  - – No “secure” user interface

Xen

KVM

Our Goals

- A lightweight and reliable hypervisor
  - Small size
  - Integrity and availability guarantee
  - Secure user interface
- Demonstrate two practical security utilities based on Guardian.

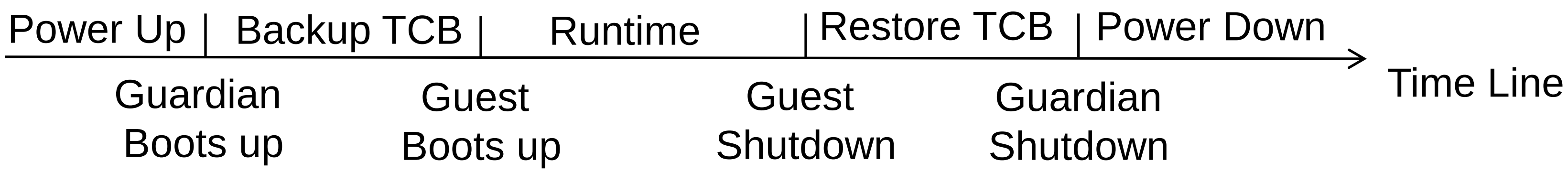
Threat Model

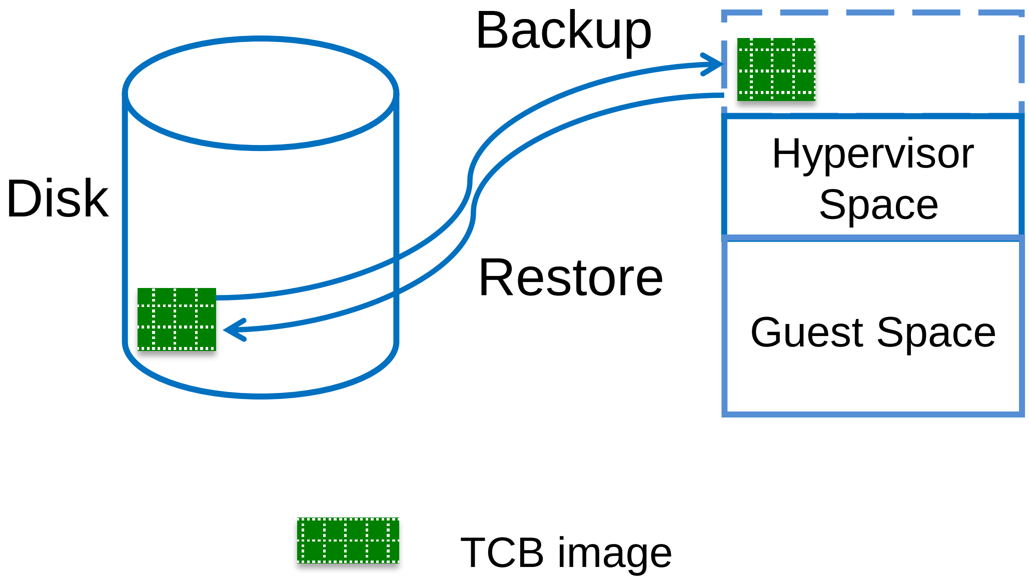
- Untrusted guest OS
  - – Launch arbitrary code with kernel privilege
  - – Issue any possible DMA requests
- Trusted BIOS and firmware
- Trusted hardware
  - – No physical attacks
- Security-conscious end users

Design Rationale

- Small size
  - – Bare-metal hypervisor - Guardian
- Integrity and availability guarantee
  - – Secure Boot and Shutdown (SBS)
- Secure User Interface (SUI)
  - – BIOS services (bootup) and trusted path (runtime)

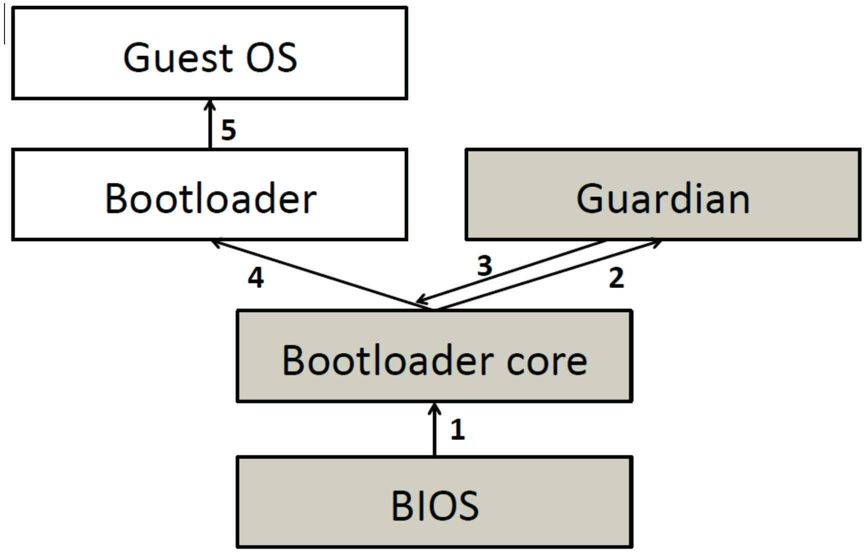
SBS Overview





Secure Boot

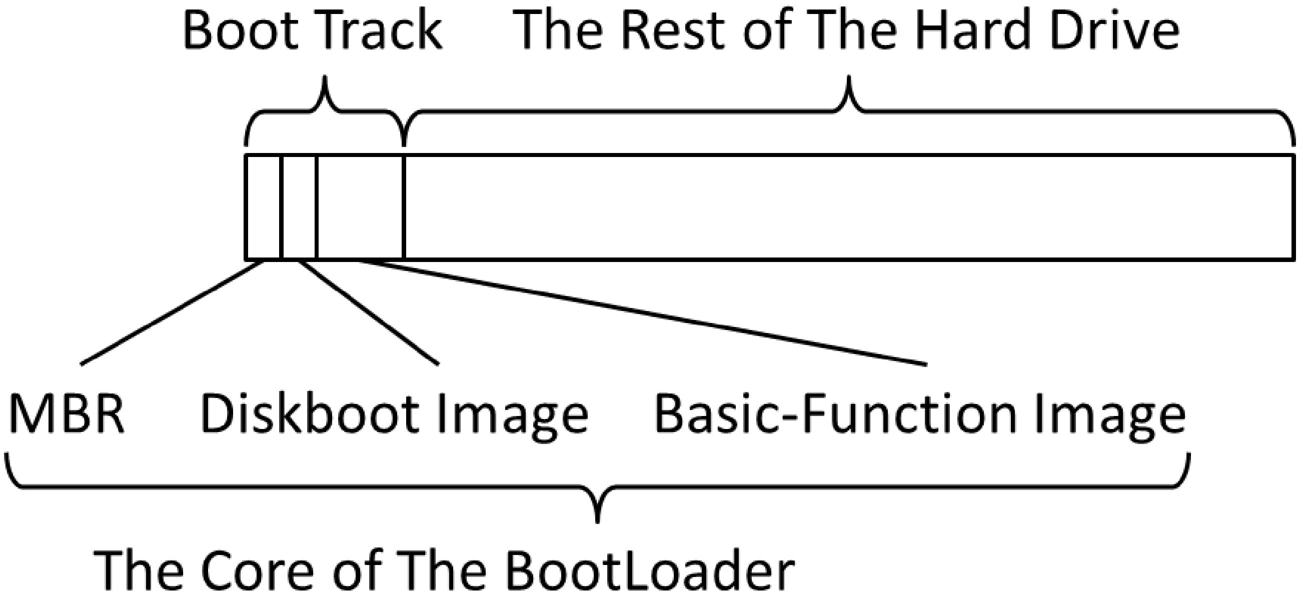
- TPM-based Secure Boot integrated into the secure boot sequence



TCB: BIOS, Bootloader core, Guardian hypervisor

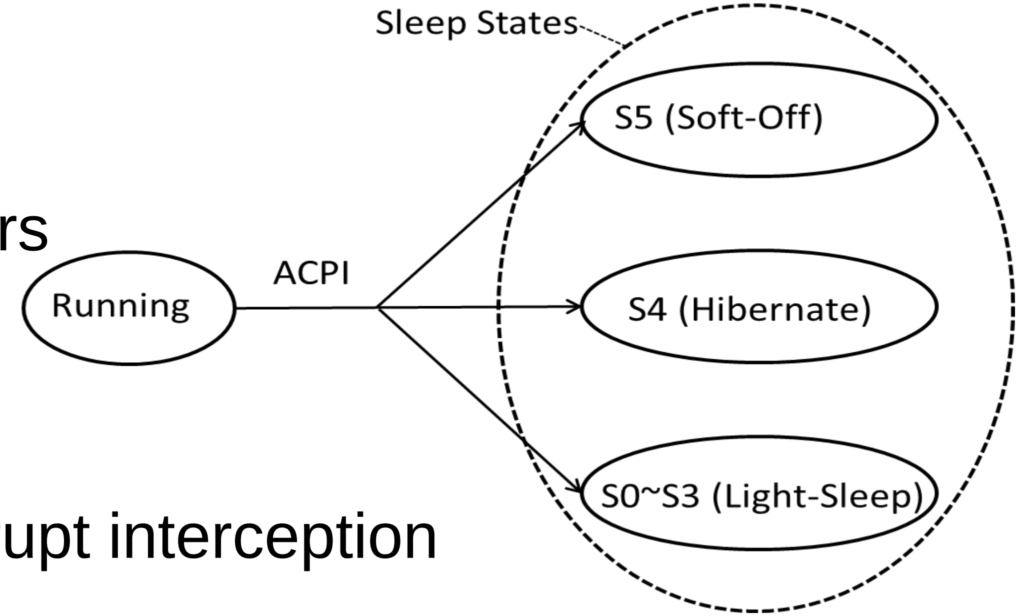
The Core of BootLoader

- Bootloader usually dynamically loads other (potentially malicious) modules



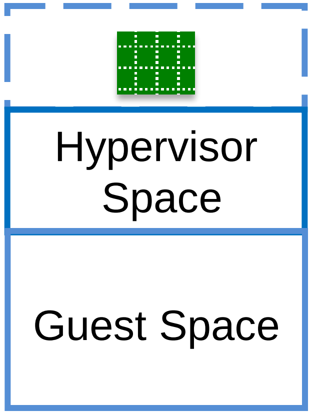
Secure Shutdown

- Intercept all shutdown events, and restore the TCB images
  - – Advanced Configuration and Power Interface (ACPI) sleep
    - Intercept the sleep and control registers
  - – System reboot
    - CPU INIT-IPI interrupt interception



TCB Images Backup/Restore

- TCB images are bootloader core and Guardian image
- The images are protected in a reserved memory at runtime
  - Use EPT/NPT
- Raw disk I/O
  - ***Not need file system***
  - Reuse bootloader’s functionality



Recovery

- The recovery mechanism is used when system crashes
  - – E.g., Power failure
- Boot up from a trusted-storage
  - – CD, read-only USB-token
- Restore the TCB images
  - – Restore the TCB images to the disk
  - – Reuse bootloader’s functionality

Secure User Interface

- Boot Up Secure User Interface(BUSUI)
  - – Bootup phase
  - – Built upon ***BIOS services***

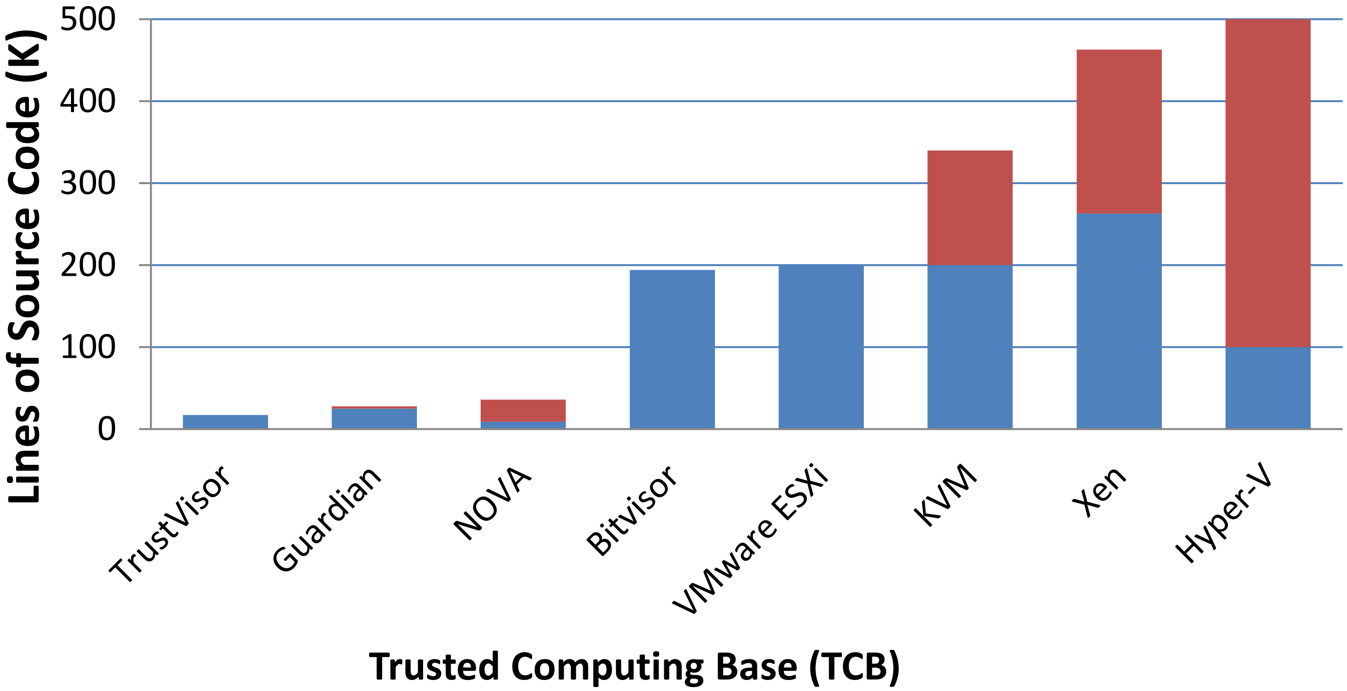
- Run Time Secure User Interface (RTSUI)
  - – Runtime phase
  - – Based on the ***trusted path***
    - Keyboard -> Guardian -> Monitor

Implementation

- Experiment setup
  - Dell OptiPlex 990 MT desktop
  - Intel(R) Core (TM) i7-600CPU, 3.40GHz processor
  - 4GB main memory
  - USB Logitech web camera with EHCI host controller
  - Intel Corporation 82579LM Gigabit Network Card

Guardian Implementation

- Guardian 25K SLOC



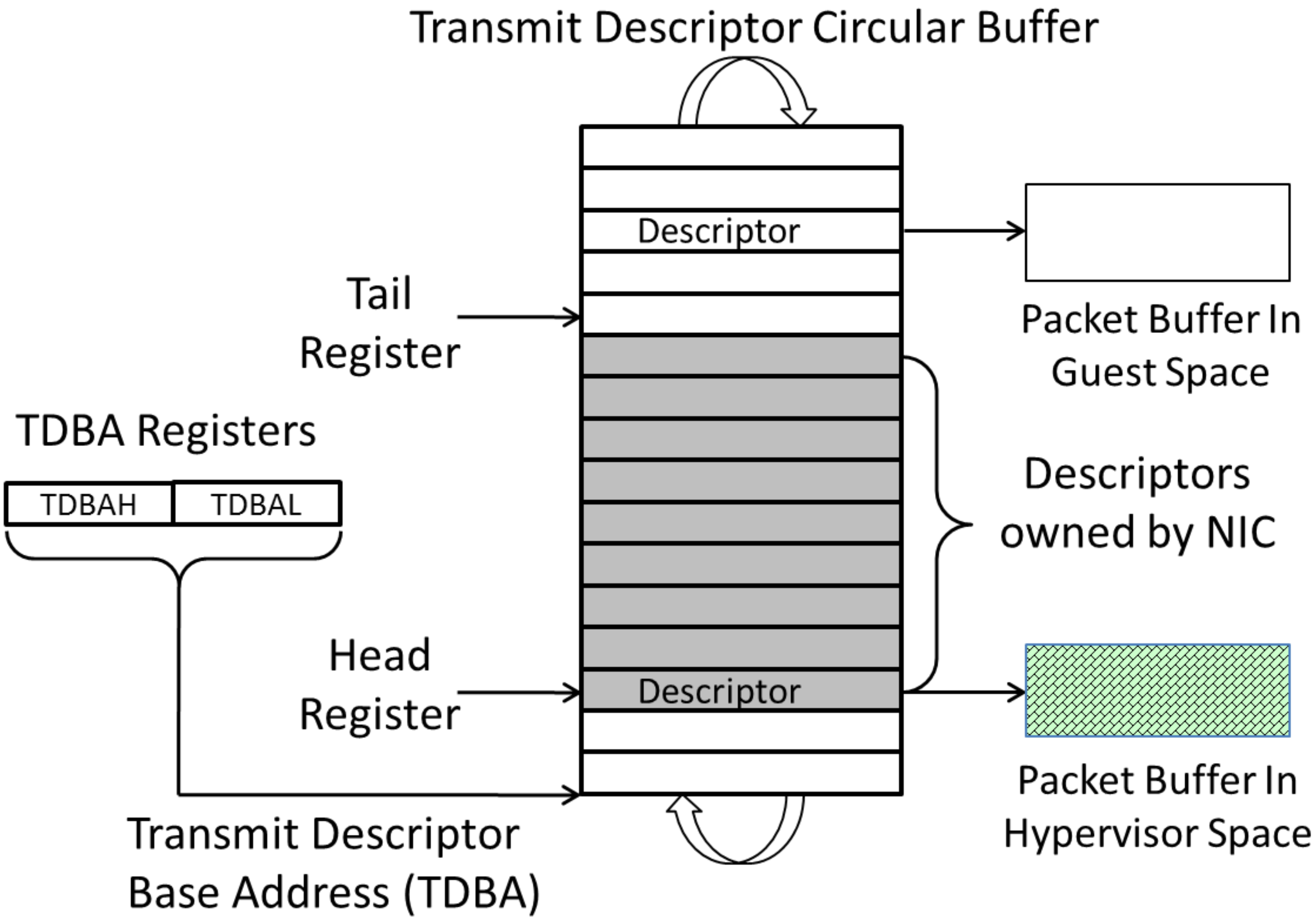
Blue: Hypervisor code

Red: Other TCB code

Two Security Utilities

- Device Monitoring
  - Camera control
    - Monitoring if the web camera is open without user’s consent
- Hyper-Firewall
  - Both application-level and OS-level firewalls can be disabled by rootkits
  - Packet-level filter in the hypervisor space
  - ***Not need NIC driver***, while intercepting critical registers to locate the cycle buffer and packet buffer

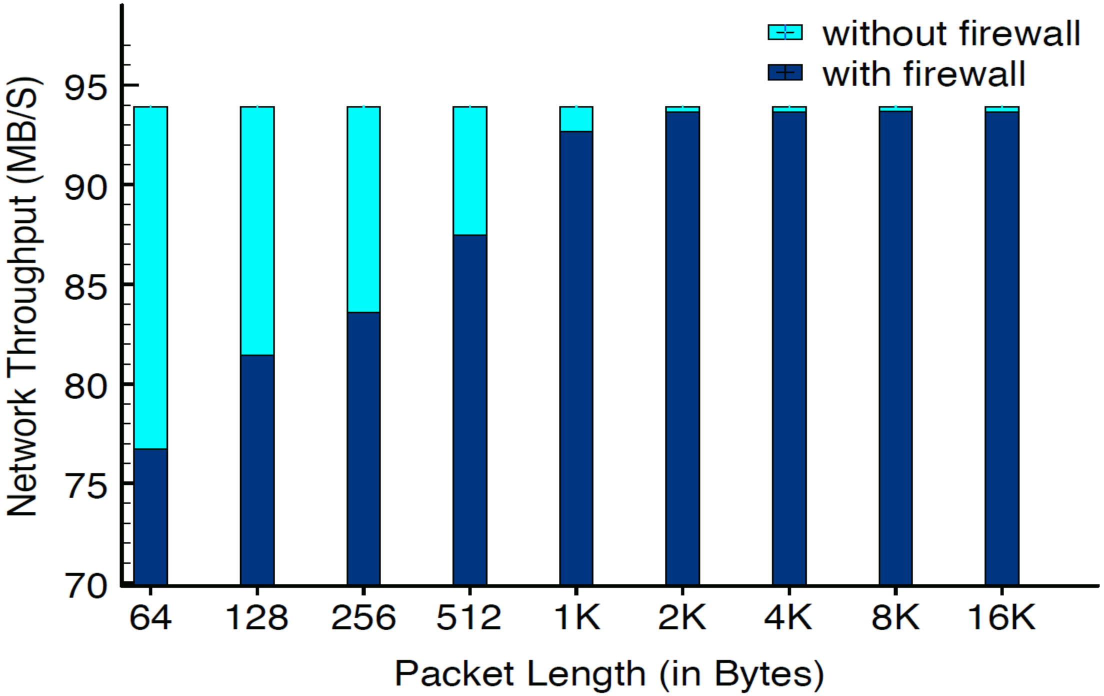
Hyper-firewall



Transmit Descriptor Circular Buffer
Descriptor
Tail Register
Packet Buffer In Guest Space
TDBA Registers
TDBAH
TDBAL
Descriptors owned by NIC
Head Register
Descriptor
Packet Buffer In Hypervisor Space
Transmit Descriptor Base Address (TDBA)

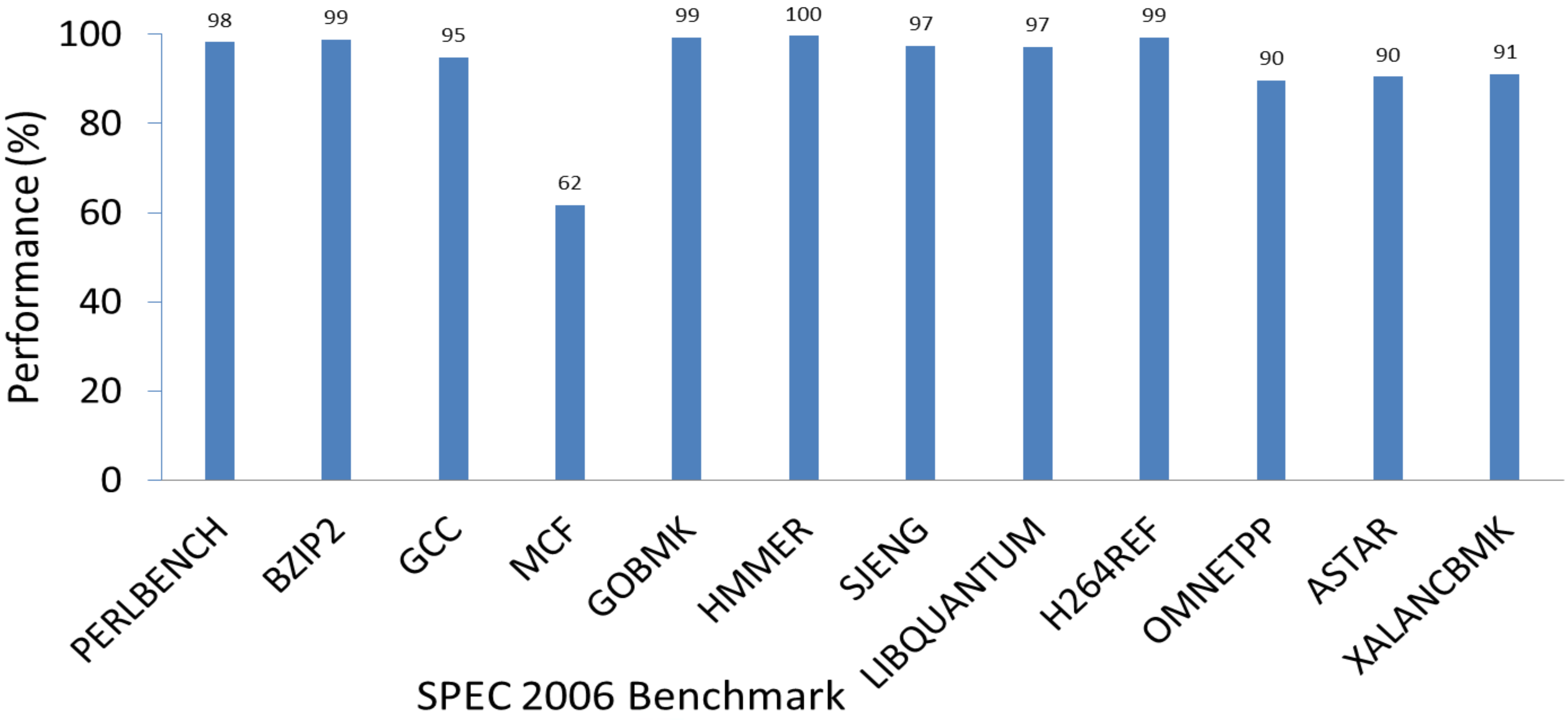
Performance Evaluation

- Device Monitoring has no effect on the camera's performance at runtime
  - No runtime data transferring interception
- Hyper-Firewall



System Benchmarks

- Virtualization effects on CPU and I/O



SMU SINGAPORE MANAGEMENT UNIVERSITY

LARC LIVING ANALYTICS RESEARCH CENTRE

Carnegie Mellon University

Conclusions

- Guardian, as lightweight and reliable security foothold
  - Small size
  - Integrity and availability guarantee
  - Secure user interface
- Two practical security services
  - Device monitoring
  - Hyper-firewall
- Insignificant performance overhead

THANKS~

Guardian: Hypervisor As Security Foothold for Personal Computers

Yueqiang Cheng
Yqcheng.2008@smu.edu.sg

SMU
SINGAPORE MANAGEMENT UNIVERSITY

LARC
LIVING ANALYTICS RESEARCH CENTRE

Carnegie
Mellon
University