Security Enhancement on Xen ARM

April 19, 2018 | Case study: Protection of Smartphone using Xen ARM Hypervisor

Dr. Sang-bum Suh

CEO, Perseus Co., Ltd, GENIVI Alliance

Email: sbsuh@cyberperseus.com

This work is licensed under a Creative Commons Attribution-Share Alike 4.0 (CC BY-SA 4.0)

GENIVI is a registered trademark of the GENIVI Alliance in the USA and other countries.

Copyright © GENIVI Alliance 2018.

Contents

- Feature for secure smartphone
- Hypervisor ACM: comparison
- Xen ARM with Access Control: Secure Xen ARM
- Secure Xen ARM for Performance Isolation: case of DoS attack

Features for secure smartphone

- Isolation of services
  - Services of which security should be guaranteed run in a secure domain, while other downloadable services in a normal domain
- Secure boot
  - Integrity measurement of hypervisor’s and guest domains’ images during system booting
- Secure storage
  - Secure ROM in a SoC for a bootloader and a master key, and a secure partition of flash memory for hypervisor and guest domains
- Access control
  - Access control of physical/virtual resources and domain management functions

 Copyright © GENIVI Alliance 2018

Hypervisor ACM: comparison

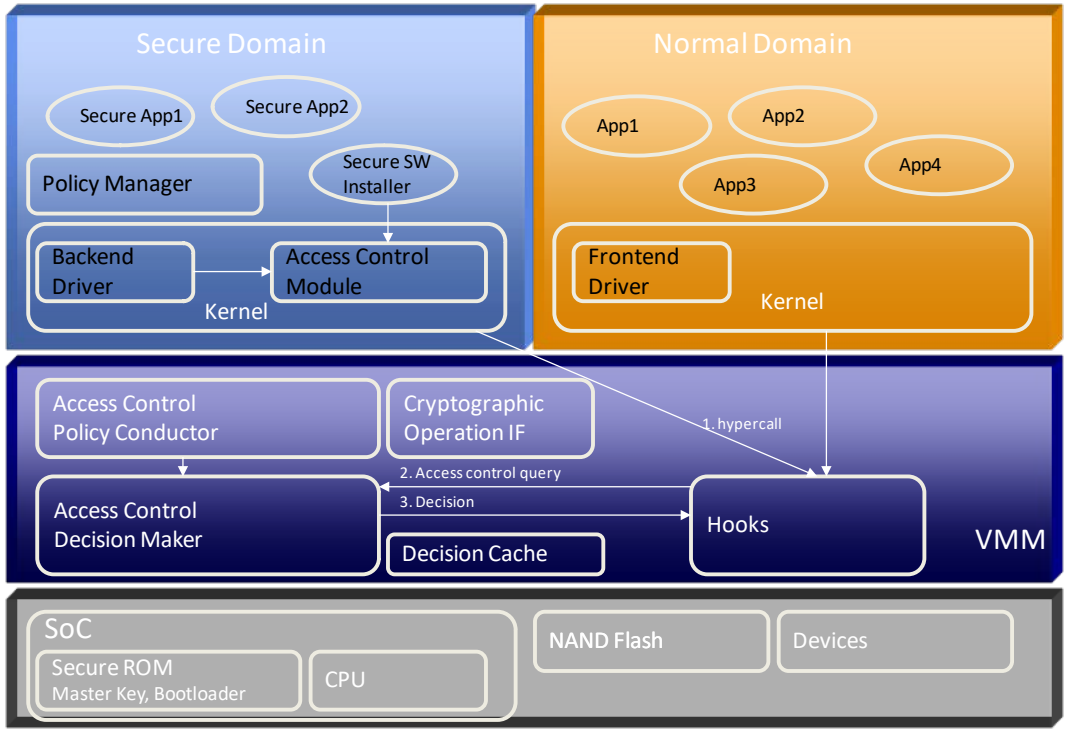
sHype, XSM and Xen ARM ACM

	sHype[SAI05]	XSM [COK06]	Xen ARM ACM
Access Control Policies	Flexible based on Flask(TE and Chinese Wall)	Flexible based on Flask(TE and Chinese Wall, RBAC, MLS, and MCS)	Flexible based on Flask(TE and other policy)
Objects of Access Control	Virtual resources and domain management	Physical/virtual resources and domain management	Physical/virtual resources and domain management
Protection against mobile malware-based DoS attacks	N/A	N/A	Memory, battery, DMA, and event channels are controlled by ACM
Access control to objects in each guest domain	Enforced by ACM at hypervisor	Enforced by ACM at Xen x86	Enforced by ACM at each domain

 Copyright © GENIVI Alliance 2018

Xen ARM with Access Control: Secure Xen ARM

- To protect unauthorized access to important system resources from hacker's attack



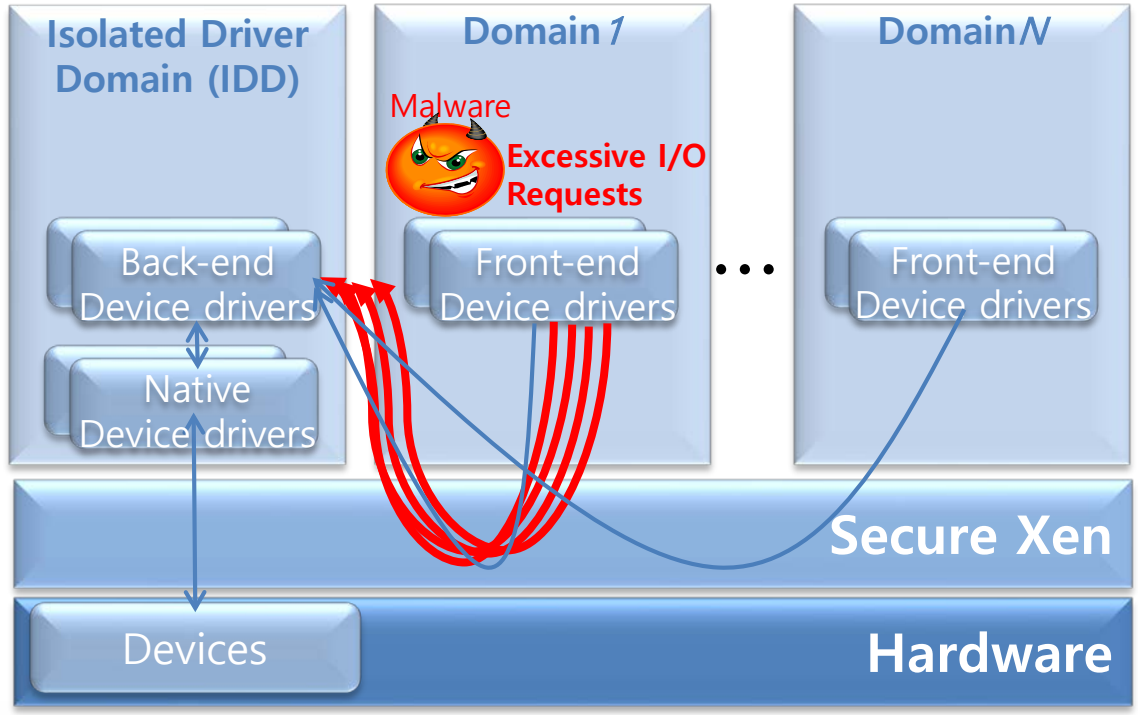
- **37 access control enforcers in hypercalls**
- **Flexible architecture based on Flask**
  - **access control models supported (TE, BLP, Biba, CW)**
- **Access control of the resources**
  - **Physical resources (TE)**
    - **Memory, CPU, I/O space, IRQ**
  - **Virtual resources (TE, BLP, Biba)**
    - **Event-channel, grant table**
  - **Domain management (CW)**
    - **Domain creation/destroy**

 Copyright © GENIVI Alliance 2018

Secure Xen ARM for Performance Isolation: case of DoS attack (1/3)

Needs for performance isolation

- **If availability threat: denial of service (DoS) attack from a compromised domain in a mobile device**
  - **CPU overuse:** a greater share of CPU time than initial allocation
  - **Performance degradation:** The Performance of other domains that share the same I/O device with the compromised domain
  - **Battery drain**

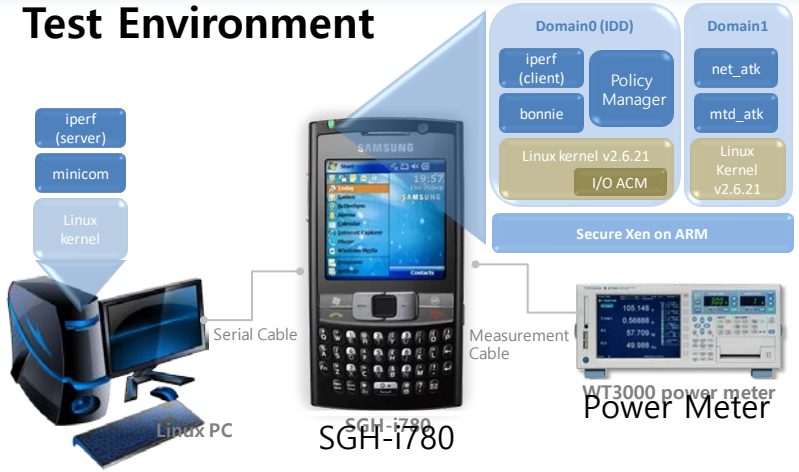


 Copyright © GENIVI Alliance 2017

Secure Xen ARM for Performance Isolation: case of DoS attack (2/3)

Effectiveness

Test Environment

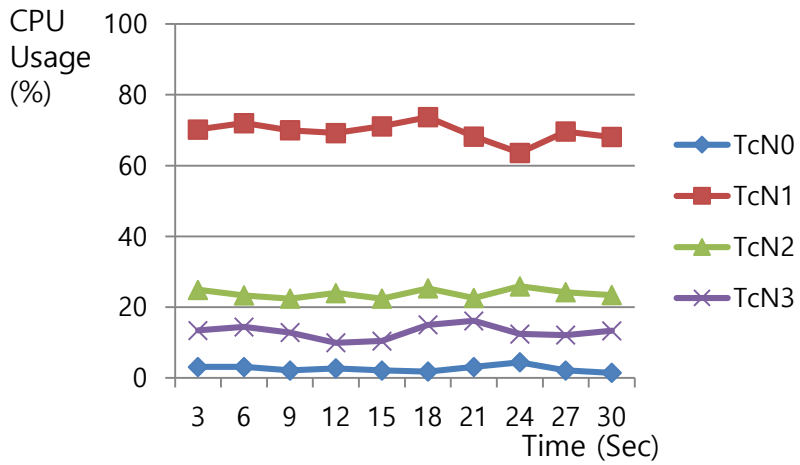


net_atk: UDP packet flooding (sending out UDP packets with the size of 44,160 bytes every 1msec)
mtd_atk: excessive NAND READ operations (scanning every directory in the filesystem and reading file contents)

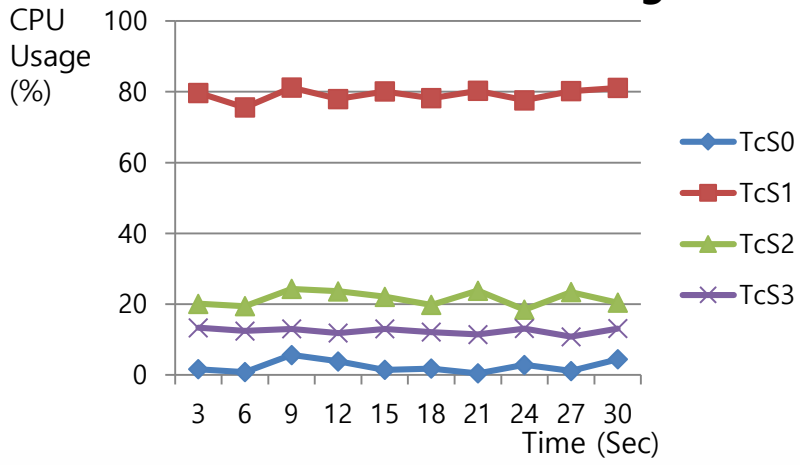
Test Cases

	Network I/O Test Cases	Storage I/O Test Cases
No Attack	TcN0	TcS0
Under Attack (No I/O ACM)	TcN1	TcS1
Under Attack (20% I/O ACM Policy)	TcN2	TcS2
Under Attack (10% I/O ACM Policy)	TcN3	TcS3

CPU Utilization: Network



CPU Utilization: Storage

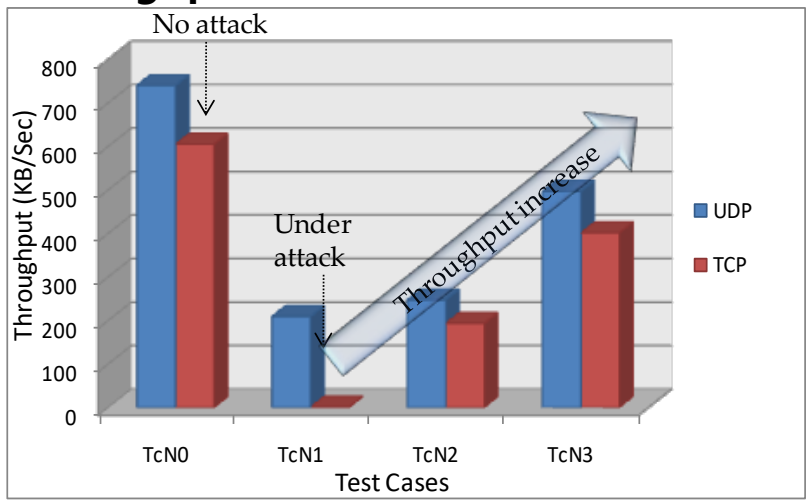


 Copyright © GENIVI Alliance 2018

Secure Xen ARM for Performance Isolation: case of DoS attack (3/3)

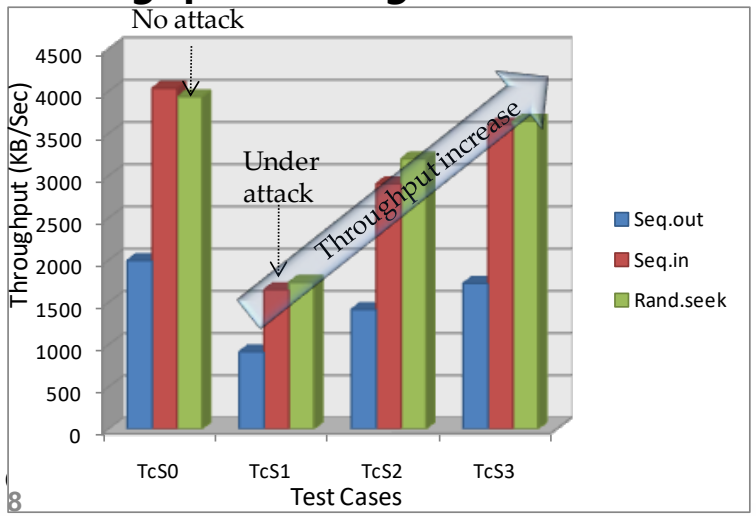
Effectiveness

Throughput: Network

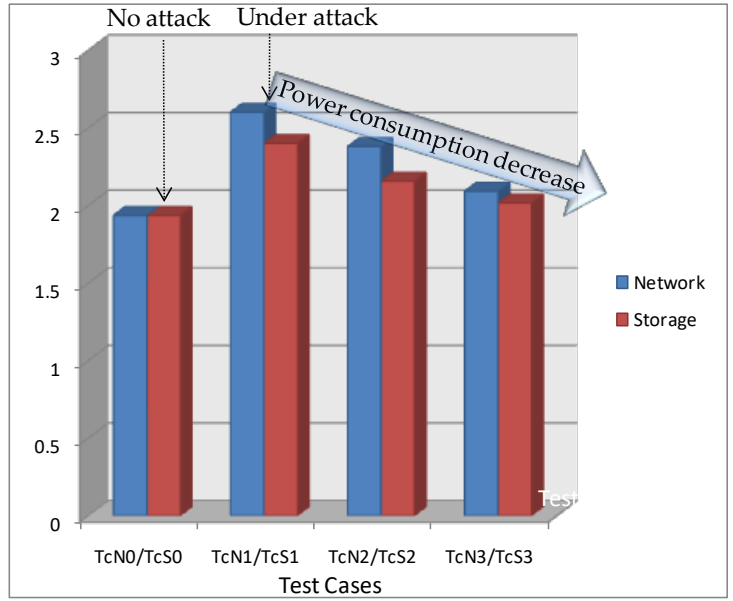


- **Throughput increase and power consumption decrease even under malware attack**

Throughput: Storage



Power Consumption



Thank you!

Visit GENIVI at http://www.genivi.org or http://projects.genivi.org

Contact us: help@genivi.org

This work is licensed under a Creative Commons Attribution-Share Alike 4.0 (CC BY-SA 4.0)
GENIVI is a registered trademark of the GENIVI Alliance in the USA and other countries.
Copyright © GENIVI Alliance 2018.