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
# Hypervisor ACM: comparison

<table>
<thead>
<tr>
<th></th>
<th>sHype [SAI05]</th>
<th>XSM [COK06]</th>
<th>Xen ARM ACM</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access Control Policies</strong></td>
<td>Flexible based on Flask (TE and Chinese Wall)</td>
<td>Flexible based on Flask (TE and Chinese Wall, RBAC, MLS, and MCS)</td>
<td>Flexible based on Flask (TE and other policy)</td>
</tr>
<tr>
<td><strong>Objects of Access Control</strong></td>
<td>Virtual resources and domain management</td>
<td>Physical/virtual resources and domain management</td>
<td>Physical/virtual resources and domain management</td>
</tr>
<tr>
<td><strong>Protection against mobile malware-based DoS attacks</strong></td>
<td>N/A</td>
<td>N/A</td>
<td>Memory, battery, DMA, and event channels are controlled by ACM</td>
</tr>
<tr>
<td><strong>Access control to objects in each guest domain</strong></td>
<td>Enforced by ACM at hypervisor</td>
<td>Enforced by ACM at Xen x86</td>
<td>Enforced by ACM at each domain</td>
</tr>
</tbody>
</table>
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
Secure Xen ARM for Performance Isolation: case of DoS attack (1/3)

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

**Test Environment**

- **SGH-i780**
- **Power Meter**

**Test Cases**

<table>
<thead>
<tr>
<th></th>
<th>Network I/O Test Cases</th>
<th>Storage I/O Test Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Attack</td>
<td>TcN0</td>
<td>TcS0</td>
</tr>
<tr>
<td>Under Attack (No I/O ACM)</td>
<td>TcN1</td>
<td>TcS1</td>
</tr>
<tr>
<td>Under Attack (20% I/O ACM Policy)</td>
<td>TcN2</td>
<td>TcS2</td>
</tr>
<tr>
<td>Under Attack (10% I/O ACM Policy)</td>
<td>TcN3</td>
<td>TcS3</td>
</tr>
</tbody>
</table>

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

**CPU Utilization: Network**

**CPU Utilization: Storage**
Secure Xen ARM for Performance Isolation: case of DoS attack (3/3)

- Throughput increase and power consumption decrease even under malware attack

**Effectiveness**

### Throughput: Network

![Throughput Network Chart]

- Throughput: Storage

![Throughput Storage Chart]

- Power Consumption

![Power Consumption Chart]
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.