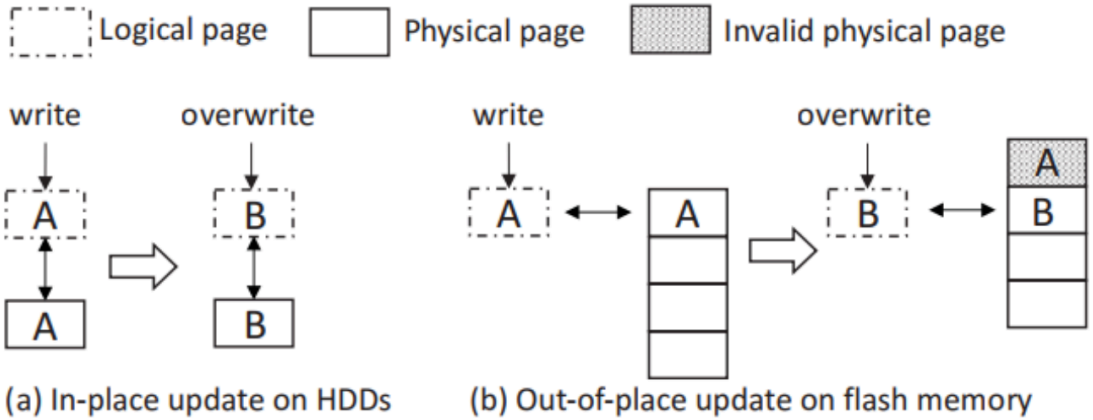
Supporting Transparent Snapshot for Bare-metal Malware Analysis on Mobile Devices

Le Guan, Shijie Jia, Bo Chen, Fengwei Zhang, Bo Luo, Jingqiang Lin, Peng Liu, Xinyu Xing, Luning Xia

Background

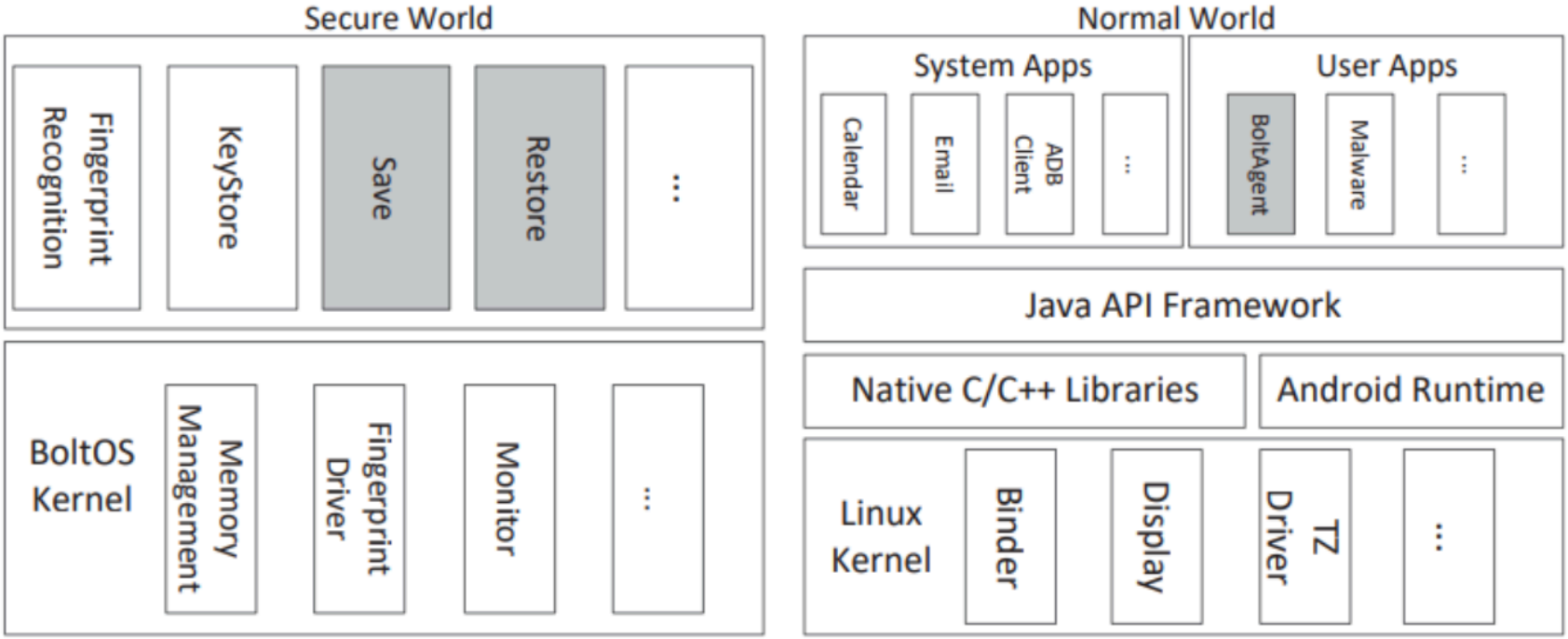
- ARM TrustZone and Its Usage in Android
- Flash-based Block Devices



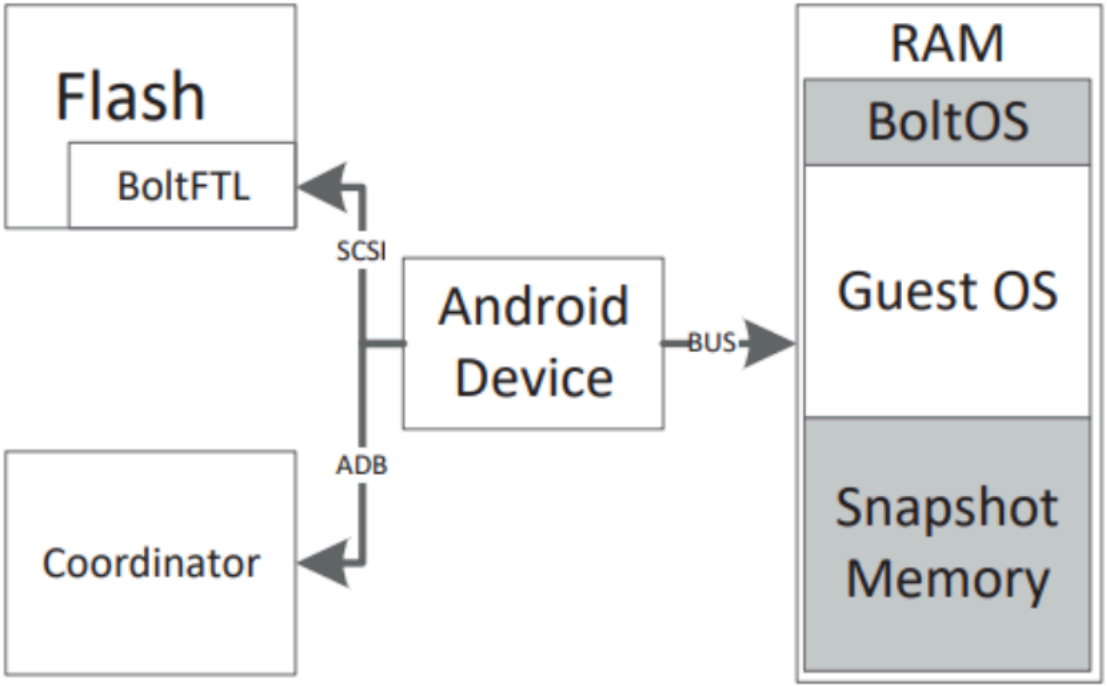
Design

- Threat Model and Assumptions
  - Malware can obtain ultimate privilege in the normal-world Android system
  - Secure world is resilient to attacks from normal world

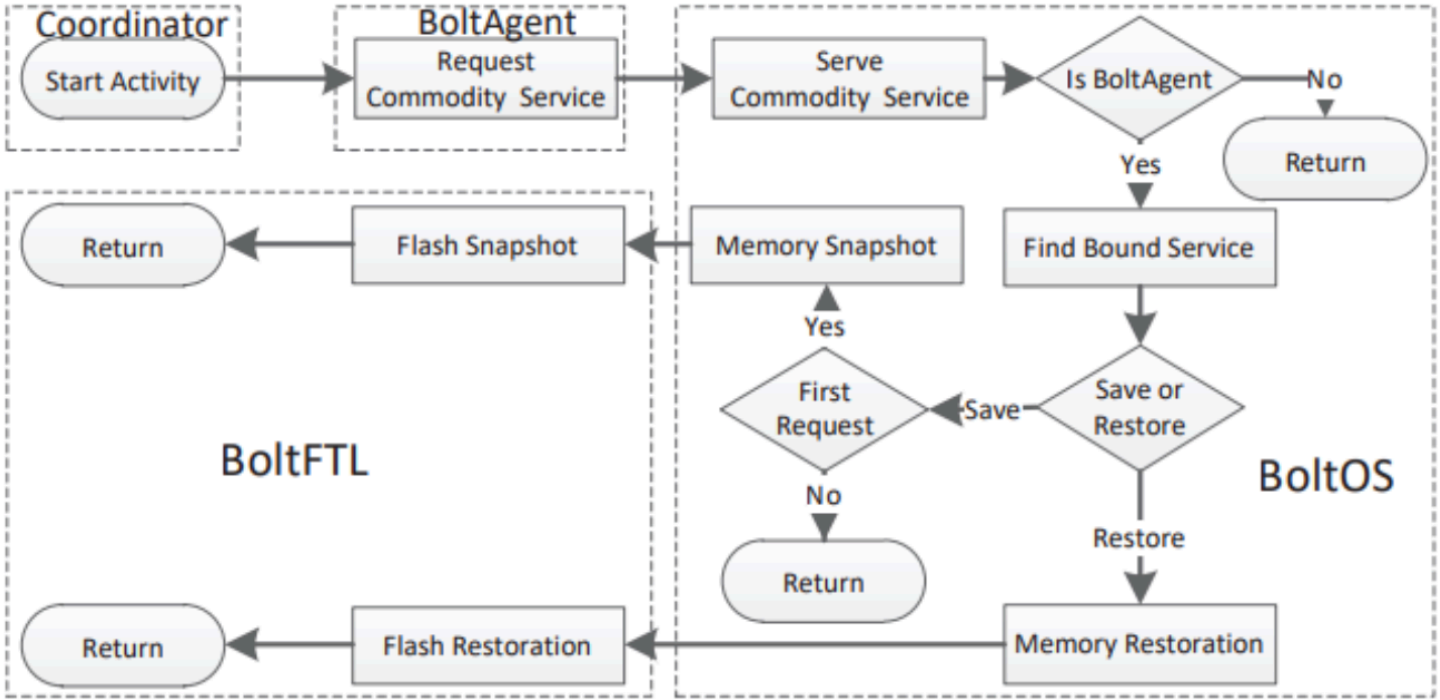
Overview-OS


Secure World
Fingerprint Recognition
KeyStore
Save
Restore
...
BoltOS Kernel
Memory Management
Fingerprint Driver
Monitor
...
Normal World
System Apps
Calendar
Email
ADB Client
...
User Apps
BoltAgent
Malware
...
Java API Framework
Native C/C++ Libraries
Android Runtime
Linux Kernel
Binder
Display
TZ Driver
...

Overview Architecture



Work-flow


Coordinator
Start Activity
BoltAgent
Request Commodity Service
Serve Commodity Service
Is BoltAgent
No
Return
Yes
Find Bound Service
Save or Restore
Save
First Request
Yes
Memory Snapshot
Flash Snapshot
Return
No
Return
Restore
Memory Restoration
Flash Restoration
Return
BoltFTL
BoltOS

Memory Recovery

- partition the physical memory into two regions
  - one is guest system
  - one is snapshot region
- registers, TTBR, SCTLR, ASID

Flash Recovery

- Malware analysis in-preparation
  - back up the valid pages and erases the blocks
- Malware analysis in-motion
  - Read: None
  - Write: page containing clean-state data or backup data is never selected
  - GC: blocks storing clean-state data are never selected as victim blocks
- Recovery from malware analysis

Implementation

- i.MX 6Quad SABRE experiment board
  - ARM Cortex-A9 processor
  - 1GB DDR3 DRAM and 256 KB SoC internal RAM
- Flash board: LPC-H3131

Evaluation

- Memory Restoration
  - 384MB: 2092653
  - 448MB: 2445271
  - 512MB: 2798087
- Flash Restoration
  - 433917

Evaluation

- Flash Runtime Performance