Poster:TVisor — A Practical and Lightweight Mobile Red-Green Dual-OS Architecture

Wenhao Li, Liang Liang, Mingyang Ma, Yubin Xia, Haibo Chen
Institute of Parallel and Distributed Systems
Shanghai Jiao Tong University

1. INTRODUCTION

Mobile and embedded system software designer are often torn between choosing security and functionality. In particular, the security of out-of-band execution environment is sensitive to rich functionality. ARM TrustZone has been used to develop a Trusted Execution Environment (TEE), which runs in parallel with rich functionality commodity OS and provides an isolated execution context for trusted applications. TrustZone splits access of the processor, memory and peripherals into two different worlds, namely normal world and secure world. The secure world is more privileged and it's the recommended context to implement TEE. However, despite its security, the functionality is very limited.

Hardware virtualization could balance the tradeoff between security and functionality by creating two VMes atop of the hardware. However, most of embedded and mobile devices lack hardware virtualization support, which makes it hard to deploy.

Red-green dual-OS design, which provides a highly-protected and constrained trusted environment ("green" OS) to perform secure sensitive tasks and a general purpose environment ("red" OS) for all other tasks and applications, is an attractive design to achieve both security and functionality. Red-green dual-OS architecture uses resources partition instead of virtualization to achieve its goal and has been deployed in many mobile devices by running the red OS in normal world and the green OS in secure world of ARM TrustZone. However, even red-green dual-OS provides an isolated environment and rich functionality, the two OSes are not created equally: a compromise of the green OS would also result in the compromise of the red OS since secure world is more privileged.

We show that how TVisor, a lightweight dual-OS architecture that creates two born-equal OS and each of them could still use the secure services of TEE in secure world, balances security and functionality for mobile devices. TVisor could be deployed to many low-cost embedded and mobile devices which are equipped with ARM TrustZone but without hardware virtualization support.

2. DESIGN AND IMPLEMENTATION

Figure 1 shows the overall software architecture when deploying TVisor. In secure world, a secure OS and TEE are deployed, which

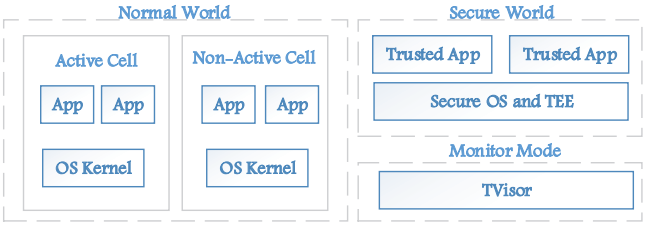

Figure 1: Mobile software architecture with TVisor

provide trusted execution environment for trusted applications and APIs for normal world applications. A Cell is introduced in normal world, which is a wrapper of a commodity OS. There are two Cells running in normal world, corresponding to red and green OS, and at most one Cell is active at the same time. When a Cell is active, its memory is set to be non-secure while the rest memory is set to secure memory so as to prevent the active Cell from tampering with the other Cell and software running in secure world. An active Cell could communicate with the TEE services running in secure world. TVisor runs in monitor mode and is responsible for managing states of the two Cells, including devices partition and management, Cell switching and scheduling. TVisor provides APIs for a Cell to register some real-time tasks notification so that the Cell could handle these critical tasks (i.e., phone call) when it is non-active.

Comparison with hypervisor: TVisor tries to minimize the abstraction layer as much as possible. For memory management, TVisor simply guarantees the isolation between Cells and let the Cell itself do the management. Consider CPU virtualization, hypervisor provides a virtual CPU to a VM while TVisor gives the real CPU view to Cells and manages the external unmarkable interrupts (i.e., secure timer, Cell notification) to schedule Cells. For IO devices sharing, hypervisor virtualizes the devices in a multiplex manner while TVisor takes the dynamic device partitioning way.

The beauty of TVisor is that it is a practical, lightweight and secure solution to meet dual-OS requirement for mobile and embedded devices. We implement a prototype of TVisor in ARM Cortex-A9 processor using Fast Model, which runs two vanilla Linux in Cells and T6 [1] secure OS in secure world. The OS runs at native speed and the switch time between Cells is negligible (3.32 μs).

3. REFERENCES

[1] T6: an arm trustzone based secure os for mobile devices. `http://www.trustkernel.org`, 2015.

MobiSys'15, May 19–22, 2015, Florence, Italy.
ACM 978-1-4503-3494-5/15/05.
http://dx.doi.org/10.1145/2742647.2745915.