Project Report

1.1. Project: OKL4 Hypervisor and Secure Mobility

1.2. Duration: 2011.6 ~ 2013.3

1.3. Brief Description

OKL4 Microvisor is a light-weight, high performance embedded hypervisor developed based on Microkernel design principles. The primary aim of the Microkernel design philosophy is to minimize the trusted computing base (TCB) of the system. A service or feature is only included in the Microkernel if it is impossible to provide the service outside of the kernel without sacrificing functionality or if including the feature in the kernel provides significant benefits and does not increase the complexity of the Microkernel. Certain security critical components which are unavoidably part of the TCB do not have to reside in the Microkernel, that is these components can be provided as secure user-level services. The OKL4 Microvisor adheres to the Microkernel principles by minimizing the features and functionality in kernel mode required for a high performance, secure virtualization environment. The Microvisor does not distinguish between "system services", virtual machines and standalone "applications". These are all treated as unprivileged user-mode subsystems. The OKL4 Microvisor provides a proven framework and foundation to break down complex software into smaller and more manageable components.

Each of these components or subsystems is partitioned into its own secure isolated world, called a Secure HyperCell or simply secure cell. A secure cell is lightweight virtual machine which can be used to run anything from a standalone 'C' application to a device driver, to a complex multi-processor capable operating system. The OKL4 Microvisor controls all resources such as addressable memory, interrupts and execution time in the system and securely partitions these resources between secure cells using a capability security model which is fully under the developer's control. Finally, the OKL4 Microvisor provides secure communication between cells to enable integrating the components into a high performance system. An example system with five secure cells running on the OKL4 Microvisor is illustrated in Figure 1. The arrows connecting two secure cells indicate that these secure cells are permitted to communicate, cells with no connecting arrows cannot communicate with each other.

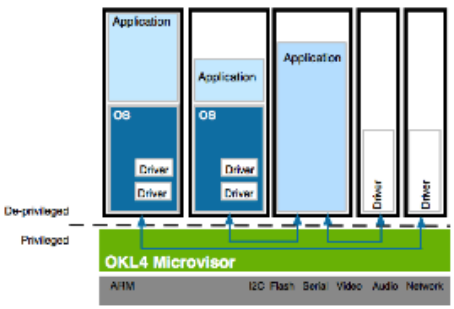

Figure 1: Levels of abstraction in libokl4 library.

1.4. Role

■ As a senior software engineer, I was involved in implementation and porting of the OKL4 hypervisor. Tasks are:

- Hybrid Linux system for OMAP3 (Beagle board) and OMAP4 (Panda board): hybrid Linux is a virtualized Linux kernel which can access native device driver. Hybrid Linux is used as a driver server for the device. Kernel version 2.6.35/2.6.38/3.0.21
- Bringup Android (ICS) on hybridized Panda board
- SMP support: supported SMP in the virtualized Linux with fake local timer.
- Virtualized driver: Virtualized client Linux can access drivers exported from Hybrid Linux. GPIO and Framebuffer
- Porting dual Android system on LG smart phone: LG Optmus 3D Max and Optimus L9. LG OEM Android is used for personal domain, and OK:Android is used for business domain. Proof of concept product. 3D Max used Linux kernel 2.6.35/Ginger Bread, L9 used Linux kernel 3.0.21/ICS.
- Secure mobility: OMAP firewall programming and split driver cell. 3D Max. split driver cell.

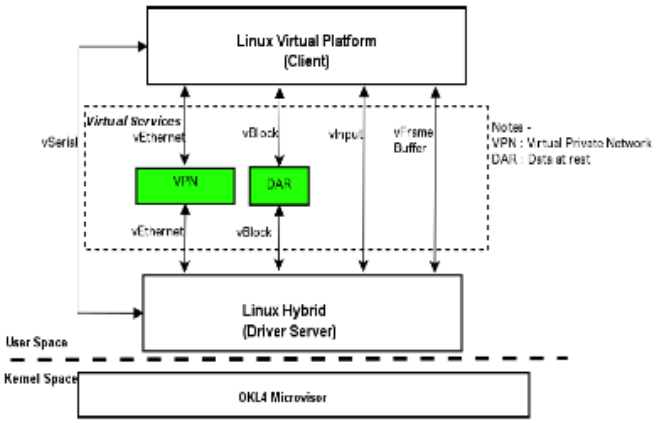

Figure 2: Dual persona System

Appendix

■ Definition & Acronyms

■ References

1. http://www.ok-labs.com