Hotmobile 2012 Demo: L4Android Security Framework on the Samsung Galaxy S2

Matthias Lange[a] **Steffen Liebergeld**[a]
Adam Lackorzynski[b] **Alexander Warg**[b]
Janis Danisevskis[a] **Jan C. Nordholz**[a]
[a]Security in Telecommunications, TU Berlin, Germany
[b]Chair of Operating Systems, TU Dresden, Germany

There is a recent trend to use privately owned mobile devices in corporate environments. This poses serious threats on the security of corporate data. In this demo we show how we applied an efficient sandboxing mechanism to the Android software stack. This allows us to run multiple instances of Android securely isolated side-by-side on one device. We implemented a prototype on the Samsung Galaxy S2.

I. Introduction

Virtualization, a technology well known from server and desktop computers, gained interest in the mobile handset market to employ multiple personalities on one device. As described by [1, 2] virtualization also allows for high-assurance isolation between secure and insecure components which is required by emerging applications such as micro payment via NFC or mobile banking.

As smartphones are heavily used in today's businesses they are usually provisioned by the corporate's IT department to prevent unsolicited data revelation. This often makes these devices cumbersome to use and consequently many carry an additional private phone with them. Running both tasks on one device is highly desirable.

In this demo we show how we leveraged the features of the L^{4}Android [3] security framework on the Samsung Galaxy S2 to implement two virtual machines running on the device.

II. System Architecture

Our system architecture is depicted in Figure 1. The system is based on a modern third-generation microkernel. The system does not require hardware-assisted virtualization capabilities. Instead the Android kernel has been modified to run as an userspace application on the microkernel. We run two instances of L^{4}Android where one is for private and the other for business purposes. Access to the graphics hardware and input devices is multiplexed by a secure GUI.

The board support package provides a generic interface to device drivers. Android implements this generic interface in its hardware abstraction layer.

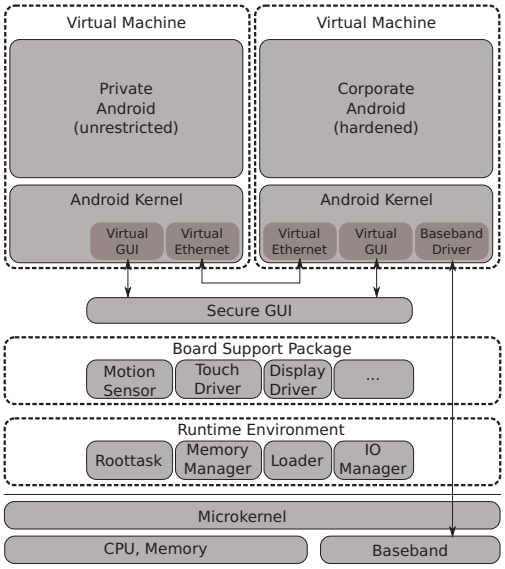

Figure 1: Two instances of Android running in parallel on one device.

While still providing the same interface the board support package can be changed without the need to adapt Android.

III. Demo Setup

We implemented our demo on the Samsung Galaxy S2 smartphone. It features a dual core ARM Cortex-A9 CPU with 1GB of RAM. We ported the microkernel to the Exynos4 SoC of the Galaxy S2 and implemented the board support package (BSP). The BSP contains various drivers for devices such as display, input devices, real time clock and accelerometer. Our prototype is capable of connecting to the mobile network

for sending and receiving SMS as well as data connectivity.

We run two instances of Android concurrently. The Android version is the latest Gingerbread release from the Android open source project. The L^4Android kernel version is Linux 3.1.

References

[1] GUDETH, K., PIRRETTI, M., HOEPER, K., AND BUSKEY, R. Delivering secure applications on commercial mobile devices: the case for bare metal hypervisors. In *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices* (2011), SPSM '11, ACM.

[2] LANGE, M., LIEBERGELD, S., LACKORZYNSKI, A., WARG, A., AND PETER, M. L4Android: A Generic Operating System Framework for Secure Smartphones. In *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices* (2011), SPSM '11, ACM.

[3] LANGE, M., LIEBERGELD, S. L4Android: Android on top of L4. `http://www.l4android.org`, January 2012.