Integrating the Tocreo Crypto Module and Redwall Hypervisor

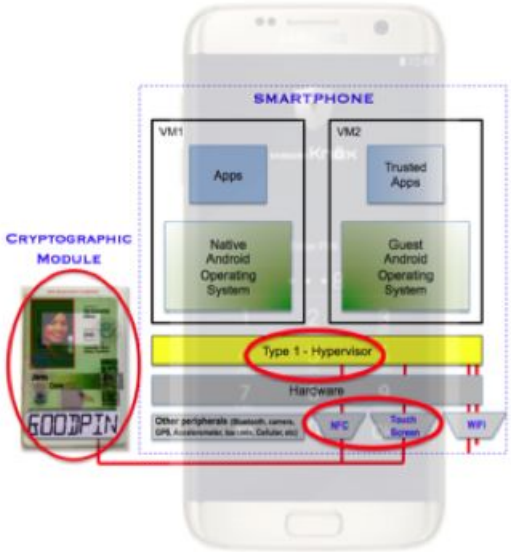
Using the latest LG 5X & V20 smartphones we've demonstrated a new architecture of securing a commercial smartphones. We will introduce two new novel security components, an NFC crypto module and hybrid Type 1 hypervisor. Together, they achieve a level of security robustness on a true commercial smartphone never before realized. The solution provides the same familiar apps and features of the commercial smartphones yet is underpinned with the military grade standards, encryption, and data storage / processing protection.

The short description provided focus on the security details of how the Tocreo Crypto Module and Redwall hypervisor are integral to each other. Highlighting the security functions and features of how these components interface to the smartphone, we will demonstrate a new approach to very challenging problem. The critical differentiator of this approach is the ease the Crypto Module and hypervisor can be overlaid and scale to most Android / ARM processor based mobile devices.

The Crypto Module

The Tocreo Crypto Module evolved after 7 generations hardware development to to fully achieve the high security requirements of the USG and military applications. It was designed in the form factor of an ID card with the capability to provide an entire isolated and secure hardware execution environment to ARM smartphone processor.

to



The Crypto Module (CM) interfaces the smartphone below the Operating System through the standard Near Field Communication (NFC) port. Integrating a programmable crypto processor, trusted memory & data bus, and display the CM is now capable of STORING, PROCESSING, and DISPLAYING trusted operations.

The value added of an entire separate, isolated, and trusted processing environment of the CM provides tremendous advantages such as:

- Simplifying the hardware security / firmware previously required to be integrated into the smartphone
- Simplifying the network security components previously required
- Augmenting the ability to enforce policy, protect data and applications, and operate in multiple security domains or personas.
- Providing a single security solution across multiple vendors' devices in a cost efficient timely way.

The TCM is a hardware-based device designed specifically to executed several specific cryptographic functions like device and user authentication, key generation, multiple X.507 certificates & keys /policy / sensitive data storage, continuous security monitoring of smartphone configuration, and verification of policy / boot-up / resource access to apps. We have developed and demonstrated all of these security functions with over a half dozen Android smartphones.

However, it was soon realized that a Cryptographic Module is not the standalone component needed to fully protect a commercial smartphone. For example, executing 2-factor user authentication with a PIN inputted on the keypad of the phone has a class of malware attacks (i.e. APT II) that could feasibly skim this data while being sent from the touch screen to the Crypto Module.

A security layer is needed to protect critical data while it is being transmitted or temporarily stored, from unwanted access by other apps. While there were multiple technologies to isolate and protect this data *WHILE-IN-USE*, none were sufficiently secure.

It became clear after integrating the Crypto Module with the Redwall hypervisor that these two novel security components had significant intrinsic advantages for isolating and protecting data while-in-use and while-at-rest that no other mobility architecture has achieved.

The Redwall Hypervisor

The roots of the hybrid hypervisor design began while working with the Government to determine vulnerabilities from commercially evolving TrustZones, Secure Elements (SE), virtualization solutions, Trusted Execution Environment (TEE), SE Linux, containerization / sandboxing, custom hybrids like Samsung KNOX$_{TM}$ / GD Protected$_{TM}$, and Type I / 2 hypervisors. None of these approaches proved effective and could not resist even basic attacks. More importantly these solutions are vendor specific requiring changes to the driver code or other proprietary source code if moved to another mobile platform. Engineering overhead can be many man-years to be operational on a single device.

The Redwall hypervisor resides below the smartphone OS at the kernel level. The hypervisor firmware is a custom Android-based ROM (sometimes referred to as an image) designed to preserve the smartphone vendors proprietary code – only small source modifications are required. The custom hypervisor is ported to a new device and easily modified with new versions of Android.

The core security of the Redwall hypervisor is a trusted security monitor that runs alongside the Linux kernel. This security monitor runs within the hardware of Crypto Module processor while connected. The monitor performs checks on every system call, as well as in the scheduler. Other security functions which are split between the Crypto Module & Redwall hypervisor include:

- To isolate different personas, privileges, the Redwall hypervisor utilizes the Crypto Module hardware Suite B cryptographic processor to provide hardware-based encryption for temporal isolation.
- To isolate data and apps at different levels of sensitivity, the hypervisor retrieves either the decryption key or decrypted data from the Crypto Module and never presents the data in the smartphone registers or memory and never presented on the device at the same time. It is simply not possible to leak data from one persona to another.
- To reconfigure or move between security levels, Redwall hypervisor firmware resides on top of this secure base. This is called the **rCore** and is simply an extension of the Linux kernel that enforces policies. The hypervisor utilizes behavioral analysis to define what is, and is not allowed. Attributes fields for policies are stored in separate memory containers within the Crypto Module. Policies for each access level or application drive low level system calls, network locations, and file system locations. These policies can also define and restrict high-level mobile phone resources like Bluetooth, GPS, WiFi, microphone, speaker, and camera.
- By continually and constantly monitoring any changes to the kernel or rogue apps (using the cryptographic Module hardware), the Redwall hypervisor easily detects their presence. Attempts to circumvent the OS built-in protections, escalate user privileges, or execute system calls are also trivially detected. More recent, one-click rooting APK developed in China for SE Android phones with strict custom policies, as with other zero day exploits, are detected and did not require modifications or patches to the hypervisor.

The red lines and circles in the figure above show illustrate how small of security footprint the hypervisor requires. Only a few smartphone peripherals require robust trusted paths. These include the NFC to the CM, the touchscreen to the CM (for user authentication of PIN), the Wifi to the CM (for Over-the-air Rekeying and trusted app store), and other I/O port enabling / disabling for each trusted application.

In short, the Redwall hypervisor provides security to the smartphone *While-In-Use* and connected to the Crypto Module. When not connected to the Crypto Module, ***Data-at-Rest*** is achieved since no root keys or critical user data is stored within the smartphone. The Redwall hypervisor not only a trusted data path below the OS for sensitive data but a flexible control to securely route this data depending upon the enforced security policy.