Secure World

From Vita Development Wiki

Secure World, also known as TrustZone (http://www.arm.com/products/processors/technologies/trustzone/index.php), Trusted Execution Environment, and (by Apple) Secure Enclave, is a sandboxed execution environment that has higher privileges that the normal Kernel. On the Vita, it seems that secure world has only a few tasks, which is facilitating communication with the F00D Processor, as well as SceGrab and SceSonyRegbus HW devices. This provides an additional layer of buffer between the application processor and the security processor. In addition, after firmware 2.10, kernel process exceptions invoke a TrustZone call to initiate a kernel memory snapshot and encrypt it for use in a coredump.

Security

The main security of secure world is the same security that prevents kernel access which is that the secure kernel code is completely proprietary and cannot be seen in normal world. Without access to the code, it is hard to develop a targeted attack on secure world. However, once a secure world memory dump is achieved through a memory leak exploit, one can see that the secure kernel lacks most of the security features found in the non-secure kernel. This is likely because the secure kernel is only to provide an extra layer of protection to prevent unauthorized access to F00D Processor and does not function as it does on other TrustZone enabled devices (the iPhone for example uses it to store fingerprint data). Most of the above-kernel security will be found in that processor.

Secure Devices

See Physical Memory for a list of known devices that can only be accessed in the secure world. The DRAM region `0x40000000` for 2MB (3MB prior to 3.52) can only be accessed in secure world. This is where the secure bootloader and kernel are loaded to. The F00D Processor can only be accessed in secure world and only secure world can handle interrupts from that processor.

SCR

After the boot initialization, the SCR is set to 0x00000004 which means FIQs are handled in secure world.

Category: Kernel
