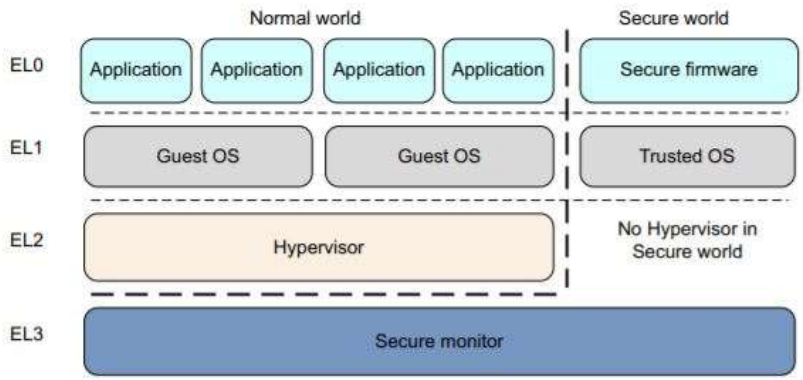
Ethan.Zhang · 2019年08月08日

Cortex-M和Cortex-A的TrustZone差异

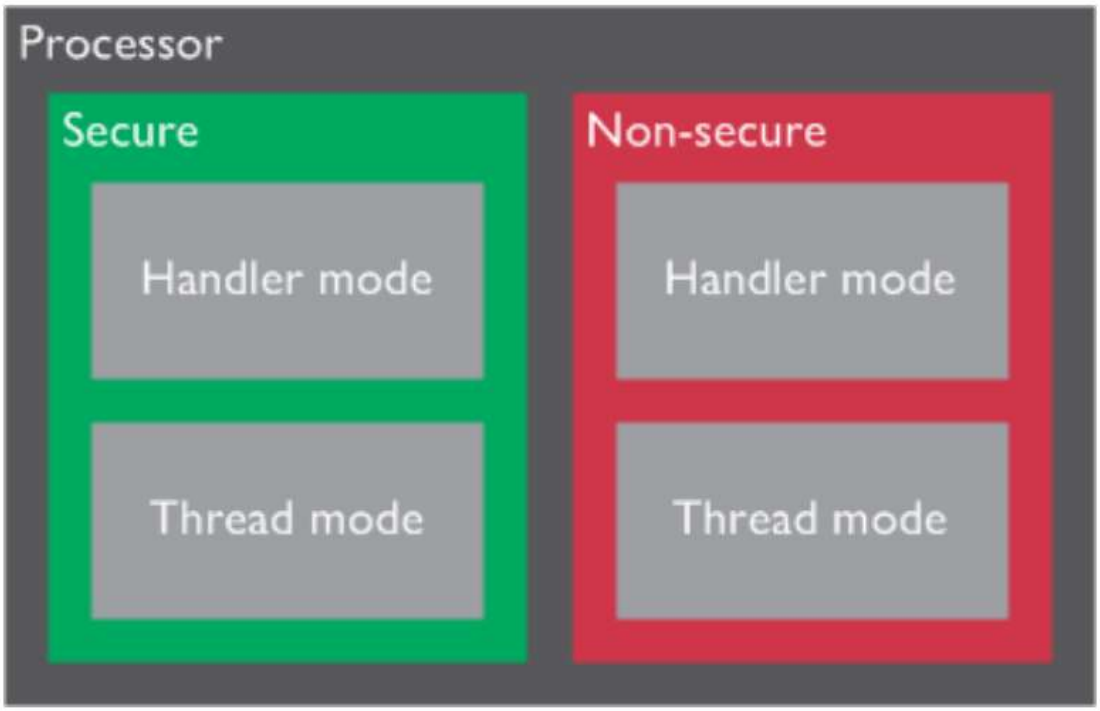
PSA Cortex-M TrustZone IoT

相信关注安全和嵌入式的开发者对TrustZone都不陌生，最近看到有网友在问Cortex-A和Cortex-M的TrustZone之间的差异，我们来简单介绍下。

Arm在2003年的Armv6开始就开始引入TrustZone，到Armv7-A和Armv8-A把trustzone作为架构的可选的安全扩展。虽然TrustZone做架构的可选扩展，但是所有的Cortex-A的CPU都实现这个扩展，例如Cortex-A7，Cortex-A53，Cortex-A55，和最新的Cortex-A77等都支持TrustZone，并且得到非常广泛的应用，比较典型的场景如指纹识别，人脸识别，移动支付，企业应用，数字版权保护等等，都是基于TrustZone来实现保护的。其实对于底层安全技术来说，无论是哪个场景的安全要求归结到硬件上面可以分为两点，一个对数据的访问，一个是对外设的控制。TrustZone天生就具备这样的优势，因为CPU分为安全状态和普通状态，结合地址空间控制器可以实现对不同的访问数据权限，结合总线和系统IP可以非常灵活控制外设的访问权限，网上有非常多的Cortex-A的TrustZone资料。



Arm从2015年把TrustZone引入到M系列，也是作为Armv8-M的可选的安全扩展，同样虽然是可选的安全扩展，但是Cortex-M23、Cortex-M33等CPU都实现TrustZone，为什么把TrustZone引入到M系列呢？因为越来越多的设备具备联网能力，只要能够联网都存在安全威胁，云服务商要确保只有可信的设备才能接入到他们的云服务，另外是设备端一般要把数据上传到云端，如果设备端不安全，数据的源头都不安全，那么上传到云端也没有价值，或者有负价值，所以说设备端是IOT安全的源头，确保设备的安全性是IOT安全的基础。



Cortex-A 和Cortex-M的TrustZone在设计思想上是一样的，CPU都有两个安全状态，并且系统上的资源划分为安全资源和非安全资源，在非安全状态下只能访问非安全资源，在安全状态下能否访问所有的资源。但是M系列和A系列架构本身就存在差异，那么TrustZone从具体实现角度来看也存在差异，并且M系列资源比较有限和需要实时响应，在安全的具体设计时也不一样。例如在A系列两个状态的切换只能通过monitor来切换，M系列的切换入口就比较多；M系列可以直接响应非安全中断，也可以直接调用非安全的代码；M系列的banked寄存器也会更多，在软件的差异上也比较大，A系列需要软件来保存上下文，M系列很多是通过硬件的方式自动保存，Arm在网站介绍了Cortex-A和Cortex-M之间的差异，同时也提供了Armv8-M的TrustZone白皮书。

Arm TrustZone Technology for the Armv8-M Architecture

Introducing Arm TrustZone

TrustZone for Armv8-A vs. TrustZone for Armv8-M

Feature/Architecture	TrustZone for Armv8-A	TrustZone for Armv8-M
Additional security states	SEL0 - Trusted Apps SEL1 - Trusted OS EL3 - Trusted Boot and Firmware (Armv8-A)	Secure thread - Trusted code/data Secure handler - Trusted device drivers, RTOS, Library managers...
Secure interrupts	Yes	Yes (Fast)
State transition (Boundary crossing)	Software transition	Hardware transition (Fast)
Memory management	Virtual memory MMU with secure attributes	Secure Attribution Unit (SAU) and MPU memory partitions
System interconnect security	Yes	Yes
Secure code, data and memory	Yes	Yes
Trusted boot	Yes	Yes
Software	Arm trusted firmware (and third-party TEEs)	Keil CMSIS, Arm mbed OS, mbed uVisor and third-party software

推荐阅读

Arm平台安全架构(PSA)详解（视频+PPT)

TrustZone和PSA之间是什么关系？ 8

11月1日-一起来听PSA专家给你介绍Arm平台安全架构 2

IOT安全方案有了SE，为什么还要用TrustZone？ 5

极术干货|张晓楠-Arm 平台安全架构(PSA)（PPT下载+视频回放）

Arm与FreeRTOS如何保障IoT的安全性

0 条评论

PSA 平台安全架构(PSA)

关注数 2021　内容数 48

Arm发布的PSA旨在为物联网安全提供一套全面的安全指导方针，使从芯片制造商到设备开发商等价值链中的每位成员都能成功实