一种基于 TrustZone 架构的引导时可信度量机制设计

尹 超，黄凡帆，周 霆
（航空工业计算所，陕西 西安 710119）

摘要：ARM TrustZone 架构具有通过硬件能力将运行在安全世界和非安全世界的软件从物理上进行隔离的能力，天然的保护了安全世界中的实体不受非安全世界的干扰，其安全性高于使用传统架构硬件的软件。但在操作系统启动时，各安全功能还未初始化完成，若此时加载的代码或配置数据被篡改，攻击者可能会得到系统控制权，后续安全手段形同虚设。因此，为了保证运行在 TrustZone 架构双世界中操作系统引导时的完整性，结合 TrustZone 架构的特点，提出一种引导时可信度量机制，确保了引导时操作系统功能和数据的完整性，给安全关键操作系统后续的安全运行创造了条件，从根本上保证了整个系统的安全性。

关键词：信息安全；可信度量；引导时度量；TrustZone 架构
中图分类号：TP309 **文献标识码：**B **文章编号：**1673-1131（2020）11-0020-03

Design Of An Active Measurement Mechanism Based On The TrustZone Architecture

Yin Chao, Huang Fanfan
（Xi'an Aeronautics Computing Technique Research Institute，AVIC，Xi'an 710119，China）

Abstract:The ARM TrustZone Architecture has the ability to physically separate software running in The TEE and REE,which naturally protects the entity in the TEE from interference by REE,and its 'security is higher than that of software using traditional architecture hardware.However,when the operating system boot,security function has not been initialized.If the code or configraion data loaded at this time been tampered,the attacker may gain control of the system,and the subsequent security means become useless.Therefore,in order to protect the integrity of the operating systems 'boot time operation which run in double world based on the TrustZonearchitechture,according to the characteristics of the Trustzonearchitecture,proposes a trusted measurement mechanism, ensure that when in the booting time,functions and data of the operating system is integrated,created the condition of consequence security operation,guarantee the safety of the whole system fundamentally.

Key words:security;TrustZone;trustedmeasurement;measurement strategy

0 引言

经过信息安全领域长期的研究与探索，人们逐渐认识到传统的以堵漏洞、筑高墙、防攻击为特征的信息安全防御技术并未能阻止病毒的肆意泛滥，计算机威胁的根源来自于终端。根源在于终端原有体系结构过于简单，资源权限可以被随意占用，病毒可以很容易地嵌到软件的可执行代码中，并获取系统的控制权，而系统缺乏监测、阻止这种行为发生的相应手段、机制。因此，必须从终端平台的源头采取措施，改进相应的体系结构，增加对病毒或恶意代码的监测、防范手段，才能确保委托的重要数据、计算任务的安全性，构建可信计算环境，提升安全关键嵌入式系统的安全性水平。只有作为嵌入式系统核心软件的嵌入式操作系统是可信赖的，才能够保证它为系统所提供的安全保护、错误恢复、故障隔离等多项可信功能是值得信赖的，从而才能为应用系统提供可信赖的底层支撑和服务，没有可信的操作系统，信息的可信如同建立在沙滩上的城堡。

操作系统启动时，在硬件平台初始化完成后，各阶段的运行代码按启动顺序依次从外部存储空间加载到内存中运行。对于存储和处理关键信息安全关键操作系统来说，在代码加载到内存的过程中面临被非法攻击的风险，可能造成系统启动代码或在配置阶段生成的配置文件面临被篡改的情况，此时加载到内存的运行代码和配置数据的完整性无法保证。在嵌入式操作系统中 Boot 和 MSL（Module Support Layer，模块支持层）完成的功能包括硬件资源的配置和初始化，中断向量、MMU 等资源初始化，之后引导操作系统内核启动。上电启动期间 MSL 引导加载操作系统内核的位置如果被更改，在操作系统运行之前运行了攻击者注入的恶意代码，攻击者可能会得到系统控制权，后续的系统安全策略就形同虚设。此外，安全关键系统的安全功能依赖安全策略的配置来执行，如果配置文件被篡改，那么操作系统对系统资源的控制、对安全功能的控制等都难以保证。

此外，ARM 公司提出的 TrustZone 技术，通过硬件手段，构建了可信执行环境（TEE）和普通执行环境（REE）完全隔离的双世界架构，基于硬件隔离的双系统各自拥有不同的权限，可从硬件上对实现可信度量功能进行支撑。综上，基于 TrustZone 架构的硬件平台，提出一种引导时的可信度量机制，与传统安全技术相比能够更加有效地保证系统引导时代码和配置数据的完整性，给安全关键操作系统后续的安全运行创造了条件，从根本上保证了整个系统的安全性。

1 TrustZone 双世界架构

对保存和处理关键信息的安全关键嵌入式操作系统来说，上电之后进行系统引导时，各个阶段运行代码将按序从外部

收稿日期：2020-07-28
基金项目：装备预研联合基金项目资助（6141B05060401）。
作者简介：尹超（1988-），女，陕西咸阳人，工程师，硕士研究生，主要研究方向：操作系统信息安全。

存储装载到内存，在代码装载过程中存在被篡改的风险，一旦系统中的运行代码被篡改，系统将无法建立初始可信安全状态，更无法进行信任传递构造信任链。因此对于运行在 TEE 中的安全功能来说，首要的就是要保障系统在引导过程中的安全。

在双世界架构操作系统中分别在 TEE 和 REE 中运行着两个系统 运行在 TEE 中的安全操作系统和运行在 REE 中的普通嵌入式操作系统。其中 TEE 安全操作系统不仅为存储和处理关键信息提供保障，还为运行在 REE 中的普通嵌入式操作系统提供信息安全支撑功能，即 REE 中运行的操作系统需要通过接口可调用 TEE 中安全操作系统提供的安全功能。

本文基于图 1 所示的双内核的高可信架构提供的可信执行环境进行引导时可信度量机制的设计。该架构由互相隔离的三大功能部分组成，包括：①TEE 中的安全操作系统；②REE 中的普通操作系统；③独立的安全固件，为运行其上的软件提供硬件安全支持。三者相互隔离，但是共享计算资源。TEE 对 REE 中的可执行实体进行度量和监控，REE 中的实体只能通过服务接口 TEE API 访问 TEE 中的服务，无法对 TEE 中的安全支持功能造成干扰和影响，TEE 和 REE 之间的交互则在监视器的参与下完成。

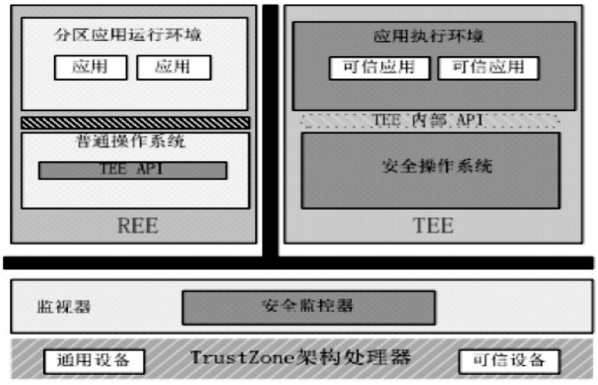

图 1　TrustZone 双世界架构

2　引导时度量流程

双系统安全引导的安全原点是在 CPU 中的只读内存（ROM）中固化的一段可信代码段。这段代码所占空间不大，在启动过程中被加载至 CPU 的可信静态随机存取存储器（SRAM）中运行。以此为基础，对双系统其余组件进行可信引导，实现系统安全引导。

双系统启动时，安全引导的第一步就是利用片上可信代码对运行时引导程序（Boot）进行完整性校验。然后将信任传递给 Boot，接着 Boot 对关键组件安全初始化，并对监控器 Monitor 进行校验，同时传递系统信任，之后由 Monitor 对 TEE 中安全操作系统内核进行校验，同时传递信任并完成安全操作系统内核的初始化，之后由内核对 TEE 的应用进行校验，并传递信任完成 TEE 中软件的安全引导 之后由 TEE 中的应用对 REE 中的引导程序进行校验，将信任传递给 REE 引导程序，在 REE 中逐级度量同时逐级传递信任完成 TEE 操作系统的引导。在以上叙述的引导过程中每次进行完整性校验，都通过在平台配置寄存器中将其中一位更新为新的校验值来进行保存 还在每一次进行完整性校验时产生度量日志，并将度量日志保存于 TEE 的内存中供后续验证使用，如图 2 所示。

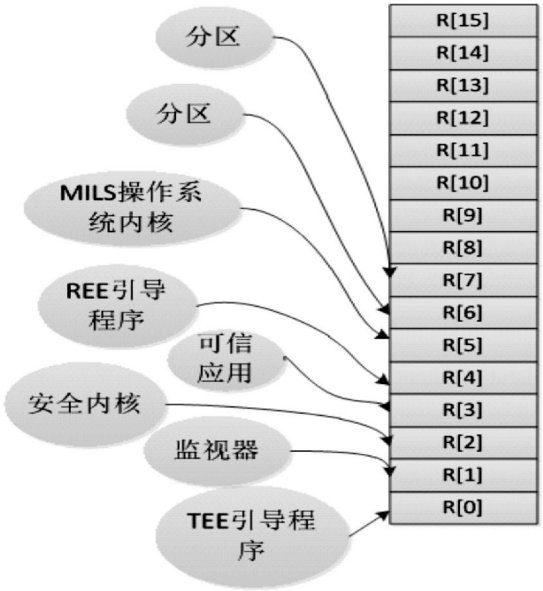

图 2　杂凑值存储示意

总体来说，安全引导从安全原点开始，对 Boot 验证引导，然后对安全环境相关部分验证引导，接着对通用环境相关部分验证引导，完成双系统的安全引导，如图 3 所示。

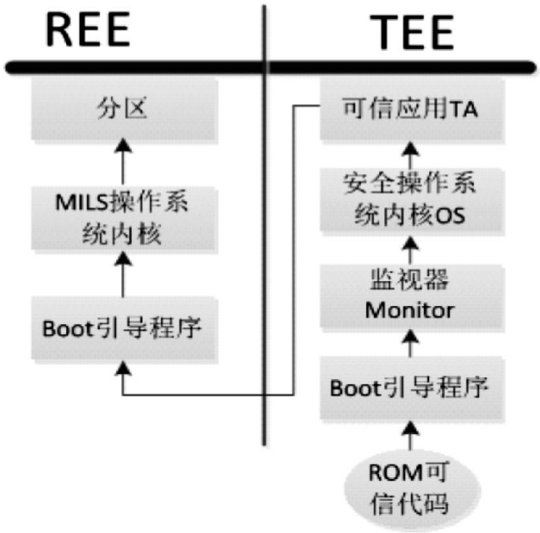

图 3　引导时度量流程图

在整个引导时度量流程中，核心关键就是信任链的传递。只有被引导部分的安全性与完整性通过验证，信任才会传递，否则信任链构建失败，系统无法完成安全引导。

3　引导时完整性度量

系统完整性是指：如果一个系统能够的行为遵循良好定义的行为准则，那么就认为它具有完整性属性。本系统在进行引导时完整性度量时，需要对按照上述的引导时度量流程，针对 TEE 中 Boot 镜像文件、监视器镜像文件、TSD 可信操作系统内核镜像文件、TSD 可信应用镜像文件、MSD 中 MSL 镜像文件、MSD 操作系统内核镜像文件、MSD 操作系统分区镜像文件以及 MSD 操作系统应用镜像文件进行完整性校验。

数据完整性的保护算法有很多种，例如可以基于对称认证技术，使用密钥生成并验证消息认证码（MAC），MAC 就是

一个用来验证消息完整性的加密校验和，使用加密杂凑函数或对称加密算法来生成。然而为了生成并验证 MAC 的值需要知道一个共同的秘钥值，所有验证的节点组件两两都要配备相同的密钥。这可能带来密钥分发问题：因为每一对组件需要协商一个自己的密钥，要求通过秘密信道来分发的密钥数量会随着网络上组件的数量指数级增长。另一种可以使用非对称加密如数字签名来保护数据的完整性和真实性，避免了分发密钥的问题，这种方法中只需将每个组件的公钥分发给所有组件。

由于嵌入式系统具有资源受限的特性，因此选择数字签名机制来进行完整性度量。在非对称加密算法中，每个实体都有自己密钥对包括公钥和私钥。私钥只有设备自身可读取，而公钥被随着度量的进行分发给每一级度量主体，如图 4 所示：

(1) 由硬件生成非对称加密算法私钥/公钥对；

(2) 调用硬件杂凑运算机制计算镜像文件的杂凑值；

(3) 用私钥对 (2) 中生成的杂凑值做加密操作，形成数字签名；

(4) 验证时使用公钥解密得到杂凑值，只有匹配的公钥才能解密得到正确的杂凑值，保证了来源合法；

(5) 计算需验证的文件杂凑值，与 (4) 中杂凑值比对，结果一致则该未被恶意修改可正常运行，否则执行违背安全策略。

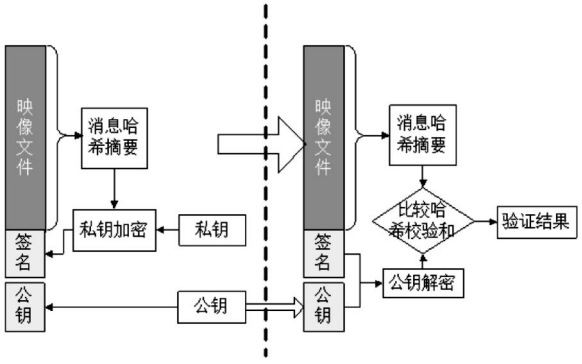

图 4　数字签名原理图

从以上的数字签名过程可以看出，密钥的使用是通过数字签名技术验证数据完整性过程中很重要的一部分，密钥的合理使用决定了验证完整性的可信性。因此，需要确保私钥的机密性，否则攻击者非法获取到该私钥，可对自己的恶意代码进行签名，安全启动机制进行签名验证时无法检测到恶意代码。因此通过平台内生的随机数发生器来产生密钥对，并使用平台提供的硬件寄存器加密存储私钥，从根本上杜绝了通过软件攻击修改私钥的可能性。此外，还应确保公钥的合法性、可信性，公钥的分发一般依赖 PKI (Public Key Infrastructure) 技术，完整的 PKI 系统包括：认证机构、证书库，密钥备份及恢复系统、证书撤销处理系统以及 PKI 应用接口系统，数字证书中包含公钥信息以及认证机构对该数字证书的签名信息，可保证证书的可信性。但嵌入式系统对实时性要求高，同时通信资源有限，所以 PKI 技术不适用，因此公钥的分发拟采用预共享的方式，但这会带来一个问题，签名步骤 (4) 中使用预共享的公钥验证数字签名的可信性之前需要保证公钥的合法性，如果公钥和私钥同时被替换，那安全性无从谈起。为了解决此问题，采用硬件平台提供的一次性可编程器件来保存公钥的杂凑值。一次性可编程器件作为硬件安全存储器具有防篡改、防攻击的特性，并能永久存储，但它有限的空间只能存储少量的数据，因此计算公钥的杂凑值存储在一次性可编程器件中以节省空间，在读取公钥值验证数字签名之前，先计算它的杂凑值，与存储在安全熔丝的杂凑值对比，如果一致的话按照上述步骤继续映像文件的完整性验证。综上，设计出引导时可信度量的验证流程如图 5 所示。

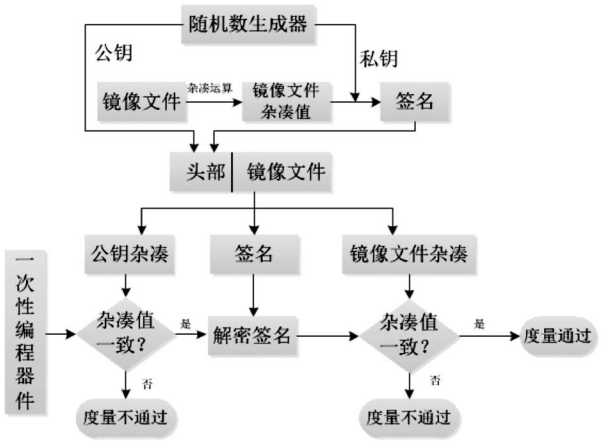

图 5　引导时可信度量验证流程

在对被加载镜像进行验证之前，需要确保镜像文件已经形成了签名。其形成过程为：对要加载的镜像文件进行杂凑运算，然后利用要加载部分的私钥对杂凑运算结果进行签名，将签名添加在镜像头部。而被加载部分的公钥的杂凑值被直接写入硬件平台提供的一次性可编程器件中，以防验证公钥遭到篡改或者替换。在验证过程中，首先取出镜像文件头部的签名进行解析，分别对公钥和镜像文件进行杂凑运算，将公钥杂凑运算结果与存储于一次性可编程器件中的值进行比对，验证公钥合法性；再用经过验证的公钥解密签名得到镜像文件的杂凑值，对比该杂凑值与计算得到的杂凑值，如果比对成功，证明该部分镜像文件完整性未遭到破坏，可信度量通过，可以加载并值得信任，可获得执行权，否则可信度量不通过，引导失败。

4　结语

本文基于 TrustZone 双世界架构，设计了一种面向双世界的引导时可信度量机制。在系统各安全功能还未初始化时，结合 TrustZone 硬件特点，为系统启动时代码以及配置数据的完整性提供了保障，确保运行在 TEE 和 REE 两个世界中的系统的安全功能和安全策略均可正确初始化而未被篡改，是系统按照安全策略正确执行的前提条件，从根本上保证了整个系统运行的安全性。

参考文献：

[1] 郑显义,李文,孟丹.TrustZone 技术的分析与研究[J].计算机学报,2016,39(9):1912-1928.

[2] 夏常钧.基于 TrustZone 的内核完整性保护[D].西安:西安电子科技大学,2017.

[3] 孙海泳,杨霞,雷航,等.基于 TrustZone 的 TEE 设计与信息流形式化验证[J].电子科技大学学报,2019,48(2):259-263.

[4] 冯登国,秦宇,汪丹,初晓博.可信计算技术研究[J].计算机研究与发展,2011,48(8):1332-1349.