https://doi.org/10.1051/jnwpu/20203851063

星载操作系统可信计算与度量认证技术研究

高建军[1,2], 闫文[1,2], 石郡儒[1,2], 刘明明[3], 姚红静[3,4], 郭阳明[3,4]

(1.航天恒星科技有限公司, 北京 100086; 2.北京市天地一体化信息安全工程技术研究中心, 北京 100020;
3.西北工业大学, 陕西 西安 710072; 4.西北工业大学 深圳研究院, 广东 深圳 518057)

摘 要:针对空间环境复杂和星载资源受限的特点,基于可信芯片支持,提出了一种适应于星载操作系统的动态度量认证方法,给出可配置的关键度量对象标识方案和验证策略。该方法根据星载应用关键等级设置关键度量对象和度量策略,对运行中关键应用进程进行周期性的度量验证,形成了一套星载软件的系统安全防护验证机制。实验结果表明,动态度量方法提升了系统可信度,性能满足星上应用要求,具有很好的实用价值。

关 键 词:星载操作系统;高可信;动态度量
中图分类号:TG316 **文献标志码**:A **文章编号**:1000-2758(2020)05-1063-05

未来异构星地网络的融合应用会引入一系列信息安全隐患,作为天基互联航天器的信息处理基础设施——星载操作系统,其开放性、网络支持性、不易维护等特点,使得操作系统被攻击后造成的损失更为巨大。现有星载系统的功能升级主要通过将新代码直接注入内存,并修改跳转地址的方式实现。这种方式在操作者易于实现的同时,也为攻击者提供了通过类似方式向星载系统注入恶意代码的通路。因此,该方式为星载系统带来了巨大的安全风险。现有星载系统常采用纠错码校验机制来保证代码可靠性,然而攻击者对恶意代码同样可以生成正确的校验码,因此该机制无法防止恶意代码的注入。

可信计算可通过建立可信根和信任链来保证系统的完整性和安全性,将可信计算技术引入星载操作系统的安全防护领域,是解其安全问题一个行之有效的方法,但目前尚未有关于星载操作系统可信技术的相关研究。为此,本文旨在设计一个高可信的星载操作系统,通过引入硬件可信模块,基于可信基引导建立信任链,在星载操作系统内核、星载应用程序等装载运行之前进行静态度量与验证,利用周期性快照的思路对运行中的应用进程、内核中的关键元素进行动态度量与验证,保证星载系统整个运行周期的可信性。

1 高可信星载操作系统安全设计框架

星载操作系统可信启动与完整性度量的构建设计包括加入可信平台模块作为可信根,通过可信启动建立信任链完成静态验证,在启动之后进行动态完整性度量验证[1-2]。当地面系统向星载系统发送任务或对应用功能进行在轨维护时,地面系统可主动向星载系统发起验证请求,通过可信“远程验证”机制实现对星载系统的身份和平台状态配置信息的可信保证。星载操作系统的高可信设计框架如图 1 所示。

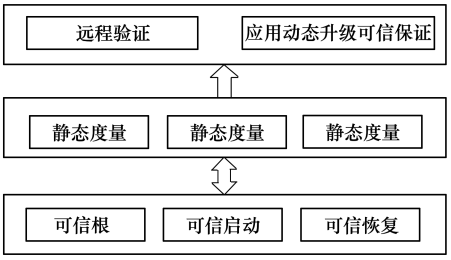

图 1 星载系统可信启动与完整性度量验证设计框架

可信模块作为系统的信任根,是星载系统建立

收稿日期:2020-01-14 **基金项目**:陕西省创新能力支撑计划项目(2019PT-03)资助
作者简介:高建军(1980—),西北工业大学硕士研究生,主要从事信息系统安全研究。

高安全可信体系的基础保证。可信模块是一个包括密码运算部件、存储个部件,专用运算处理器、基于独立总线的 I/O 系统、独立内存空间、永久性存储空间和随机数产生器的小型片上系统。运用用符合可信规范的密码算法对外提供各类加解密相关的运算。可信模块无法占用星载计算机的内、外存,需要在模块内部执行一定的安全算法,以实现和其他部件的接口标准化并提供内部的密码运算。高可信星载操作系统的信任根主要有:

1) 可信度量根(root of trust for measurement, RTM)[3],在星载系统未启动之前完成对星载系统初始启动代码的完整性度量和验证;

2) 可信存储根(root of trust for storage, RTS),通过一个存储根密钥加密保护子密钥等对象、完成解密和签名操作,以此记录星载系统各部件完整性度量摘要值[3],并保证度量值顺序计算以及度量日志的完整性;

3) 可信报告根(Root of Trust for Reporting, RTR),基于背书密钥生成星载系统可信身份密钥,保证星载系统身份的真实性和报告的完整性。RTR 是进行"远程验证"的基础,确保 RTS 可靠的计算引擎[4]。

星载系统建立基于可信启动的信任链,延伸系统的可信范围,确保星载系统启动全过程的安全可信任[5]。信任传递机制是指在信任当前某一环节的前提下,由该环节去评估下一个环节的安全性,确定下一环节可信之后再将控制权转交给下一环节,然后依次向后推进[4]。星载系统的启动序列都遵循当前阶段的代码负责度量下一阶段即将要执行的代码,然后再将度量值扩展到星载系统可信模块的寄存器中,由此形成信任链[6]。

静态度量之后的完整性存储,则是将包括完整性度量对象和度量过程的日志信息存储到相应数据存储区,将完整性度量结果,即摘要值存储在平台的配置寄存器[7]。为扩展每一个平台配置寄存器的存储能力,这里将同一个部件不同时间的度量值采用哈希链接[8]的方式扩展到同一个寄存器中,如图 2 所示,哈希链计算如公式(1)所示。

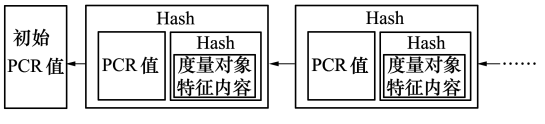

图 2 基于哈希链的星载系统度量值扩展

$$PCR_i^N = Hash(PCR_i^O \mathrm{P} Hash(\mathrm{C})) \quad (1)$$

式中:PCR_i^O 表示扩展之前旧的配置寄存器值;PCR_i^N 表示扩展之后新的配置寄存器值;;P 表示连接;C 表示度量对象的特征内容。

星载操作系统在进行可信度量时,将每一个度量对象的所有度量值扩展到可信模块的配置寄存器(platform configuration register, PCR)中,为该度量对象记录相应的链式度量日志,同时将所有度量对象扩展后的 PCR 值利用生成树算法构造树形度量日志。度量日志用于星载本地验证和地面远程验证,如图 3 所示。

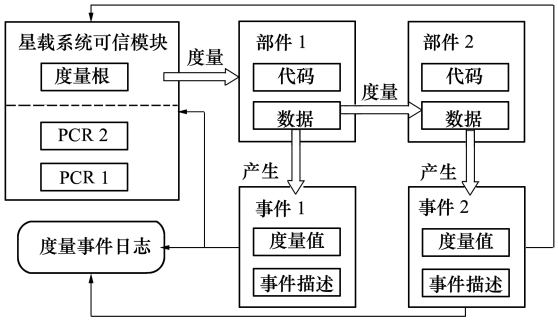

图 3 星载系统完整性度量示意图

将所有度量对象扩展后的 PCR 值,利用生成树算法构造不平衡的树形度量日志,其数据结构如图 4 所示。

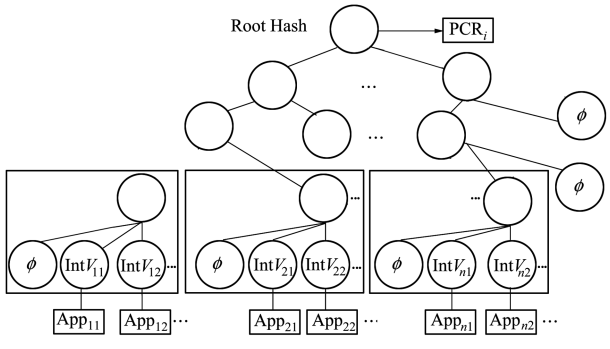

图 4 度量日志数据结构

2 星载应用进程的动态度量

操作系统可信启动之后,在星载应用程序启动、装载时,进行一次性的静态度量、验证,确保其在装载运行之前是可信的。星载应用通常需要在轨维护功能支持,地面上注的更新应用一般维护在内存中,为确保应用程序在整个运行生命周期中没有被恶意

破坏,进一步增强可信度,提出动态完整性度量验证方案,保证应用程序等在运行过程中的完整性和可信性,如图 5 所示。

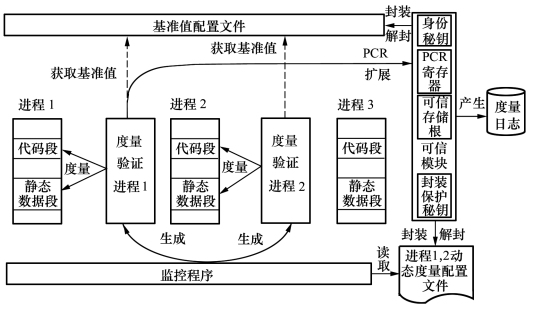

图 5　星载应用进程动态度量示意图

系统启动后,内核创建常驻内存、运行于内核层的监控进程。监控程序模块作为进程动态度量架构的出入口,其主要功能有:①实时读取动态度量配置文件,根据配置文件获取度量进程相关信息;②循环进程列表,获取进程的相关信息,为正在运行的进程创建伴随度量进程;③通知伴随度量进程对正在运行的进程进行挂起、结束和重启等操作;④周期性地挂起该进程,通知伴随度量进程发送度量对象进程信息,对度量对象进行可信性判定,并根据返回值进行相应处理[8]。

度量进程调用度量基准库获得度量基准值,将其与度量值综合比较,若结果为 True,伴随进程返回信息给监控程序,证明当前进程运行状态可信;反之,伴随进程将 False 反馈到监控程序,证明当前进程运行状态不可信,然后对该进程进行恢复[9]。其中,动态度量配置文件是提供给外部的接口,由可信模块封装储存保护,在其读取、修改或更新之前,需先判断当前平台配置是否处于可信状态。监控进程每次读取改动态度量配置文件之前,都会先判断当前配置平台是否可信,若处于可信状态,可信模块对配置文件进行解封操作再发送给监控进程,确保其安全性。

3　系统验证机制

3.1　本地验证

本地验证是在星载系统启动时进行的一种可信验证机制,是指可信部件基准值与度量值比较的过程,星载系统在完成度量之后即可进行星载本地验证。在安全环境下对原始星载系统可信部件进行哈希计算,生成验证基准值,为了保证基准值在星载系统上不被篡改,使用可信模块的一个密钥作为消息认证码(message authentication code,MAC)密钥,生成基准值的(Hash-based MAC,HMAC)。

基本步骤是,首先使用可信模块的一个密钥,计算度量对象标准值文件内容的 HMAC 值,将其存储在文件的安全扩展属性中;当需要使用该文件之前,进行同样的 HMAC 计算,再进行比较验证,利用 HMAC 的单向性和 MAC 密钥的安全性,防止对标准值的恶意篡改,确保基准值的安全性。

3.2　远程验证

卫星在轨服役过程中,地面系统往往根据任务需要对其星上应用进程进行在轨维护或动态重构。远程验证是地面系统向星载系统发送任务前,确认星载系统的身份和平台状态配置信息是否可信的一种技术手段,过程示意如图 6 所示。

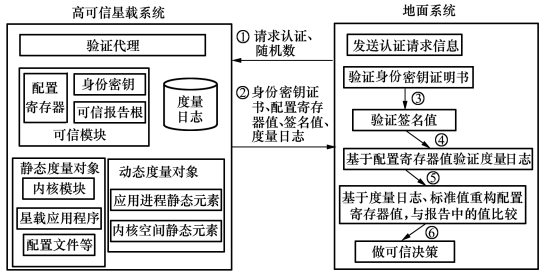

图 6　地面系统对星载系统的远程可信验证及可信恢复

远程验证时,远程交互实体向星载系统发送含有随机数的请求消息。星载系统可信模块拥有唯一的背书密钥及相应的数字证书。为保护隐私需要,星载系统基于背书密钥生成对应的身份密钥,并申请相应的数字证书。星载系统可信模块可生成多个身份密钥和证书,在不同的场合使用不同的身份密钥,以达到保护隐私的目的。

星载系统收到请求消息后,相关配置寄存器值通过身份密钥签名后和相应的度量日志与身份密钥证书同时发送给远程交互实体。星载系统收到认证请求消息后,采用公式(2)对配置寄存器值签名[10]

$$\sigma = \mathrm{Sign}(\mathrm{PCR\ P\ Nonce}, \mathrm{IKey}) \qquad (2)$$

然后,星载系统需将树形度量日志中的相应叶子结点到根节点的认证路径上的散列序列、TPM 签名的可信根节点值以及叶子结点的链式度量日志发送给地面系统。地面系统收到报告消息后,先验证身份密钥证书的正确性;通过后验证配置寄存器值签名

的正确性。根据认证路径序列重构根节点,与 TPM 中存储的根节点比对,验证发来的叶子结点的链式度量日志是否被篡改,是否是可信的。认证通过后则表明所报告的链式度量日志是正确的,否则就是不可信的;接着根据链式度量日志和度量目标部件的认证标准值,重构配置寄存器值,与报告消息中的配置寄存器值进行比较,若匹配则判断星载系统中度量目标部件的可信;反之,则表明星载系统上配置寄存器对应的相关部件被篡改过,处于不可信状态,可以通过动态恢复等方式对其进行可信恢复。

4 实验结果分析

研制开发板验证信任链在可信操作系统启动过程中的建立过程,以及可信操作系统进程级的动态度量认证功能,并做性能分析。

启动开发板,通过信任链从可信度量根开始启动操作系统,boot 度量结果与由可信存储根保护的校验基准值匹配,内核度量结果与由可信存储根保护的校验基准值匹配。当系统出现异常启动,可信操作系统会自动重新烧录由可信模块保护的可信内核镜像,恢复完成后系统自动重启,实现可信启动。

通过设置配置文件得到操作系统对应用进程动态度量,将度量结果与可信模块基准值进行认证比对。设计实验对 3 个 64 kB 大小的应用进行动态度量与认知,选取 10 次实验结果进行均值分析,实验结果如图 7 所示,单次认证过程 2.2 ms,小于 10 ms;度量时间 1.6 s/MB,小于 3 s/MB。指标符合设计要求,满足星上应用性能需求。

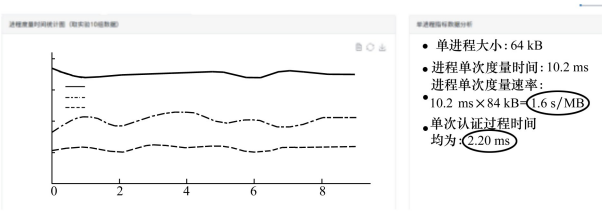

图 7 进程动态度量对标图

5 结 论

未来构建天地一体化互联的应用场景中,星载操作系统是影响网络安全性的重要环节。现有星载操作系统注重可靠性与实时性,但缺乏系统安全防护机制。论文提出一种可信计算与认证度量方法,通过引入可信硬件,基于可信基与可信引导,完成了系统与关键应用全运行周期的静态和动态度量与验证。实验结果表明,该方法能够安全且高效的实现系统的可信计算,是对传统的星载系统防护技术的一次革新。

致谢 感谢国防基础科研计划(2018 年、2019 年)、民机科研项目(2018 年、2019 年)和深圳市新兴产业大数据智能应用开发实验室对项目研究的支持。

参考文献:

[1] ZHAO S J, LI X, ZHANG Q Y, et al. Security Analysis of SM2 Key Exchange Protocol in TPM2.0[J]. Security & Communication Networks, 2015, 8:383-395

[2] 冯伟, 冯登. 基于串空间的可信计算协议分析[J]. 计算机学报,2015,38(4):3-18
FENG Wei, FENG Deng. Analyzing Trusted Computing Protocol Based on the Strand Spaces Model[J]. Chinese Journal of Computers, 2015,38(4): 3-18 (in Chinese)

[3] 潘汪洋. 基于 vTPM 的 Xen 虚拟机动态完整性度量模型研究[D]. 保定:河北大学,2017
PAN Wangyang. Research on Dynamic Integrity Measurement Model of Xen Virtual Machine Based on vTPM[D]. Baoding: Hebei University, 2017 (in Chinese)

[4] 王勇. 基于可信计算 PLC 的身份认证与终端度量技术的研究[D]. 沈阳:沈阳理工大学,2018
WANG Yong. Research on the Authentication and Terminal Measurement Technology of PLC Based on Trusted Computing[D]. Shenyang: Shenyang Ligong University, 2018 (in Chinese)

[5] 马卓. 智能电网环境下基于可信计算的移动终端安全接入技术研究[D]. 北京:国网电力科学研究院,2012
MA Zhuo. The Security Access Technology Research of Mobile Terminals Based on Trusted Computing in Smart Grid[D]. Beijing: State Grid Electric Power Research Institute, 2012 (in Chinese)

[6] 张磊. 可信网络功能虚拟化关键技术研究[D]. 南京:东南大学,2017

ZHANG Lei. Research on Key Technology of Trusted Network Function Virtualization[D]. Nanjing: Southeast University,2017 (in Chinese)

[7] 徐日. 可信计算平台完整性度量机制的研究与应用[D]. 西安:西安电子科技大学,2009
XU Ri. Research and Application of the Integrity Measurement Mechanism on Trusted Computing Platform[D]. Xi'an: Xidian Universtity, 2009 (in Chinese)

[8] MEGUMI A, JOSHUA D. GUTTMAN, et al. Hash-Based TPM Signatures for the Quantum World[C]//Proceedings of the 16th International Conference on Applied Cryptography and Network Security ACNS, Guildford, UK, 2016: 77-94

[9] 张建标. 面向 Windouws 环境进程主动动态度量方法[J]. 山东大学学报,2018, 53(7): 46-50
ZHANG Jianbiao. Process Active Dynamic Measurement Method for Windows Environment[J]. Journal of Shandong University, 2018, 53(7): 46-50 (in Chinese)

[10] 蒋逸尘, 韩臻, 张大伟. 基于 PTM 的可信虚拟平台方案[J]. 北京交通大学学报,2013,37(5):67-74
JIANG Yichen, HAN Zhen, ZHANF Dawei. A Scheme of Trusted Virtualization Platform Based on PTM[J]. Journal of Beijing Jiaotong University, 2013,37(5):67-74 (in Chinese)

Study on Trusted Computing and Measurement Certification Technology of On-Board Operating System

GAO Jianjun[1,2], YAN Wen[1,2], SHI Junru[1,2], LIU Mingming[3], YAO Hongjing[3,4], GUO Yangming[3,4]

(1.Space Star Technology Co., Ltd, Beijing 100086, China;
2.Beijing Engineering Research Center of Space-Ground Integrated Information Security, Beijng 100020, China;
3.Northwestern Polytechnical University, Xi'an 710072, China;
4.Research and Development Institute of Northwestern Polytechnical University in Shenzhen, Shenzhen 518057, China)

Abstract: Based on the complexity of space environment and the limitation of space resources, a dynamic metric authentication method for spaceborne operating system with the trusted chip support is proposed, and the configurable key metric object identification scheme and verification strategy are given. In this method, Key measurement objects and measurement strategies can be set according to the key level of on-board application. The critical application processes in operation can be measured and verified periodically, then a system security protection verification mechanism for on-board software is obtained. The experimental results show that the dynamic measurement method improves the reliability of the system, and the performance meets the requirements of on-board applications, which has great practical value.

Keywords: on-board operating system; high assurance; dynamic measurement