安全技术

DOI:10.19695/j.cnki.cn12-1369.2018.02.95

# 安全可信的嵌入式系统架构

游夏 马云 胡明星
(中国电子科技集团公司第三十二研究所,上海 201808)

**摘要**:为解决安全关键嵌入式系统的信息安全问题,针对多级安全架构特点,本文提出了安全可信的嵌入式系统架构技术。通过实现嵌入式操作系统的隔离内核,在资源分配、信息流和故障等方面的完全隔离,实施严格的数据访问与通信限制。通过构建系统可信度量链,提供用户身份授权和应用完整性验证,使安全关键嵌入式系统具有多级安全策略、故障隔离、安全通信、可信度量、身份认证等能力。

**关键词**:多重独立安全等级;隔离内核;可信驱动;安全服务
**中图分类号**:TP316 **文献标识码**:A **文章编号**:1007-9416(2018)02-0186-03

## 1 概述

我国信息安全问题越来越需要得到重视,特别是航空航天、核电能源、交通运输、武器装备等安全关键嵌入式系统面临由系统安全漏洞带来的安全威胁。信息化系统往往存在着不同安全等级的多类应用,需要采用嵌入式软件多重独立安全等级(Multiple Independent Levels of Security,MILS)[1]模型,将应用部署于物理上隔离的多台设备中,以实现对系统资源、通信过程、系统故障等隔离处理与隔离控制,从系统底层构建可信度量链,打造多级安全系统内核,根据安全级别来分离数据,实施严格数据访问限制,确保特定授权得用户访问指定数据。

因此,针对国内安全关键领域嵌入式系统的迫切需求,本文将多级安全服务和可信服务相结合,基于国产嵌入式处理器芯片、国产可信芯片和国产嵌入式虚拟分区操作系统,以嵌入式操作系统隔离内核为核心,开展嵌入式系统多级安全防护技术研究,为不同安全等级的嵌入式应用建立隔离的运行环境,将故障和不可信分区与可信区域隔离,为安全关键应用分区提供可信度量与完整性校验,防止嵌入式系统的故障和不安全信息的扩散,形成安全可信的嵌入式系统架构,如图1所示。

## 2 操作系统隔离内核

内核是嵌入式操作系统管理嵌入式计算机硬件资源的核心管理软件。本文基于虚拟化技术设计了嵌入式操作系统的隔离内核[2],采用最小特权管理机制,根据安全等级把系统资源通过系统配置划分为独立分区,每个分区块具有自己的安全等级,分区间通过配置受隔离内核信任的安全策略组件实现安全通信。操作系统隔离内核通过对计算机资源进行抽象模拟完成了系统资源的虚拟化[3],包括CPU资源、内存资源、中断资源、时钟资源、设备资源等,确保各分区的空间、时间资源不会互相影响,并提供标准的操作系统接口管理设备、文件系统和网络协议栈等共享资源。操作系统隔离内核实现了嵌入式应用的时间隔离、空间隔离[4],并将应用故障和不可信分区与其他区域隔离,以防止故障和不安全信息的扩散。

## 3 操作系统安全策略

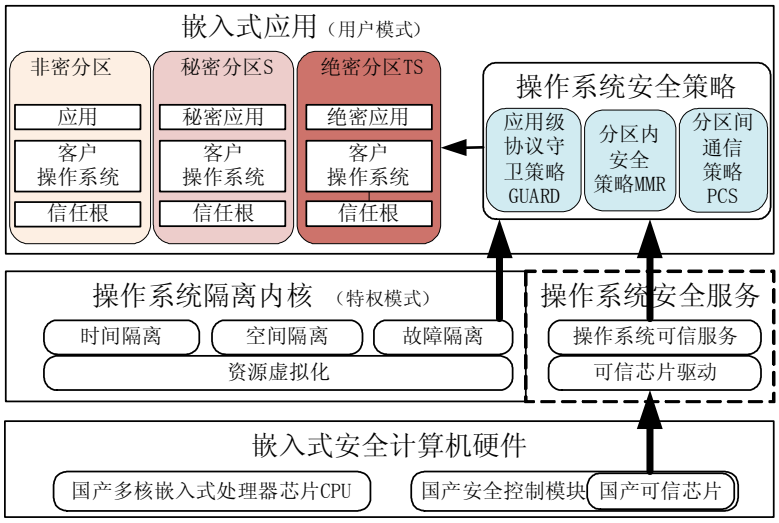


图1 安全可信的嵌入式系统架构

收稿日期:2018-01-22
作者简介:游夏(1981—),男,江苏泰州人,本科,工程师,研究方向:嵌入式操作系统安全访问与防护技术。

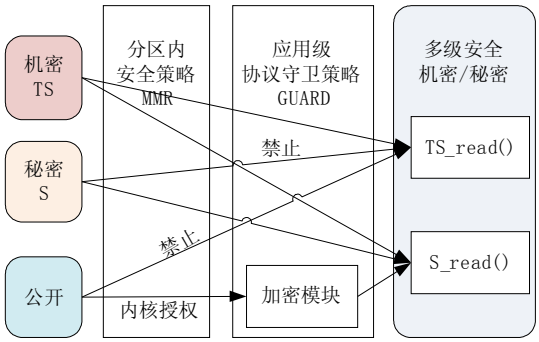


图2 分区内安全策略MMR的信息流图

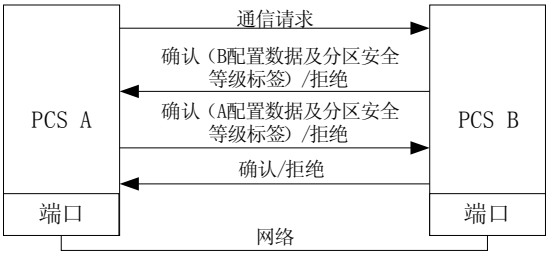


图3 分区间通信策略PCS握手流程图

本文中嵌入式操作系统设计了安全策略组件，规定了不同安全等级的实体必须要经过安全策略组件的可信实体的仲裁进行安全通信，具体包括分区内安全策略MMR[5]、分区间通信策略PCS[6]、应用级协议守卫策略GUARD[7]，不同分区间的通信要经过分区内安全策略MMR，不同处理器核之间的通信要经过分区间通信策略PCS，扩展的降级安全策略由应用级协议守卫策略GUARD实现。

3.1 分区内安全策略MMR

分区内安全策略MMR是执行信息流安全策略的可信组件。如果一个实体想发送消息给另一个实体，则首先检查该消息是否合法，并将消息发送至可信分区共享缓冲区中，通过交换可信分区共享缓冲区的所有权进行传输，如果消息不合法，则MMR返回错误。当分区发起文件读写请求时，MMR基于安全策略根据发起方的安全等级判定是否允许该信息流，通过守卫检查消息内容。在发起方的安全等级较低的情况下，安全策略本身不允许该信息流，但如果隔离内核配置数据的信息流控制表中允许该信息流，则其不会被MMR所禁止。信息流控制机制如图2所示。

3.2 应用级协议守卫策略GUARD

应用级协议守卫策略GUARD创建分区间授权通信来实现应用级的安全策略，作为具体通信协议相关的应用级消息过滤器。每个GUARD处理一种类型的消息。GUARD从MMR处接收消息，解析消息体的内容，查看其格式是否与要求的格式一致，并对分区间传送的消息执行详细的、基于协议的信息流控制。GUARD对消息的处理有三种结果：通过消息，将其发送给MMR；修改消息(加密、降级等)；拒绝消息，通知 MMR 发送错误响应给源端。

3.3 分区间通信策略PCS

分区间通信策略[8]提供了嵌入式系统不同节点之间的信息流控制。PCS使用升级和降级策略加密并降级信息，输出公开级别的信息，发送到网络。当消息被传送到接收节点后，由接收方PCS进行解密和安全等级提升。PCS维护信息流的端到端安全性，提供身份认证，防止未经授权的信息流，通过加密传输信息确保数据保密，通过检查所有用户数据和确保数据的安全完整性，通过实现信道带宽管理以防止拒绝服务攻击。

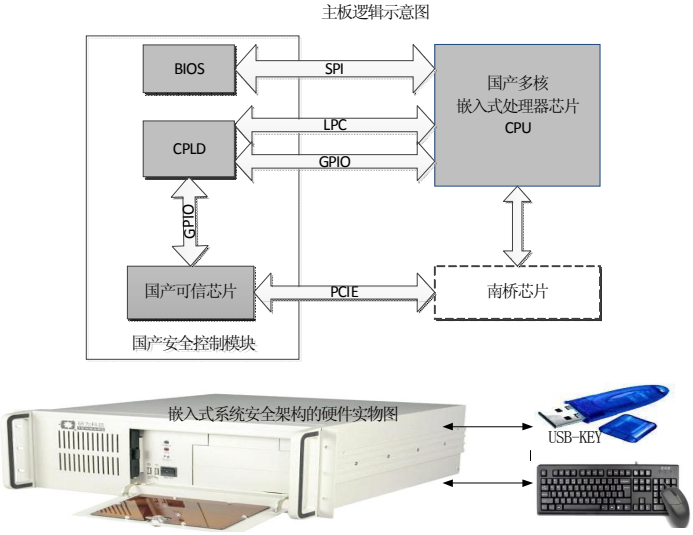


图4 嵌入式系统安全架构硬件示意图

在分区间通信之前，PCS建立连接以认证通信双方身份并授权。源PCS首先获得目标PCS配置数据确保两个PCS具有相同的配置数据，如图3所示，PCS A首先向PCS B发出请求消息，包括源节点和目的节点。B收到请求后如果返回确认消息，则同时B将发送其配置数据和分区安全标签配置到A。A接收到响应消息后修改自身配置数据使其与B一致，并发送分区安全等级标签和修改后的PCS配置数据到B，最后B确认配置数据一致，两个PCS完成建立分区间安全通信连接。

## 4 嵌入式安全计算机硬件

嵌入式系统安全架构的硬件平台采用国产高性能多核嵌入式处理器芯片作为操作系统隔离内核的运行载体，同时设计了基于国产可信芯片的国产安全控制模块，提供操作系统可信服务，形成嵌入式安全计算机硬件，其实物图和主板逻辑示意图如图4所示。

嵌入式系统安全架构硬件主要包括芯片部分和通道部分。BIOS芯片存放与主板相关的基本输入输出例如安全输入模块，PCIE插槽用于外接安全可信芯片与桥片相连，CPLD芯片用于控制国产安全控制模块的上电时序，先给安全可信芯片供电以进行对BIOS的主动度量，并通过GPIO通道与CPU和安全可信芯片相连，安全可信芯片通过片上可信固件程序对外部提供可信命令处理服务接口和高速密码服务接口，通过资源注入通道与安全可信芯片相连，实现芯片内的密码资源注入，通过主动度量通道，能够实现对固件的主动度量。

## 5 操作系统安全服务

5.1 可信芯片驱动

嵌入式操作系统实现了嵌入式系统安全架构的可信芯片驱

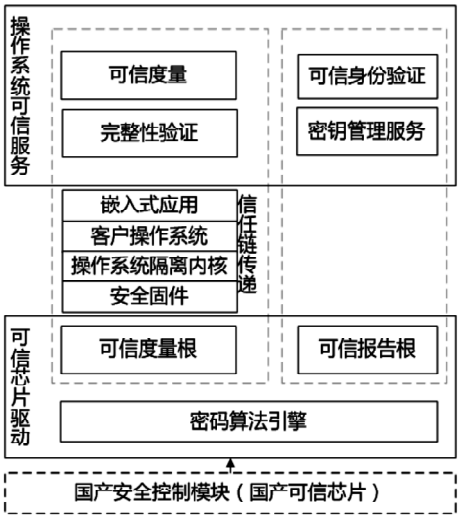


图5 操作系统可信服务的软件结构图

动[9]，完成对嵌入式安全计算机的安全控制模块的初始化，完成对固件、嵌入式操作系统的可信验证和引导，并支撑操作系统可信服务的运行。可信芯片驱动完成可信芯片上电初始化，提供对芯片硬件的识别接口，系统枚举芯片硬件后即加载安全可信芯片驱动进行配置。可信芯片驱动实现了获取状态、自检、用户认证、度量值读写、加解密算法、签名等接口，用于支撑操作系统可信服务功能的调用。

5.2 操作系统可信服务

操作系统可信服务[10]对操作系统安全策略提供可信度量、完整性校验、密钥管理服务、可信身份验证等服务能力，其结构如图5所示。

(1)密钥管理服务。密钥管理服务完成密钥生成加载和密钥存储。密钥管理服务包括机密性、完整性保护和身份认证、加解密等需求。用户通过调用可信创建密钥接口，产生对称加密密钥，并用上一级密钥加密存储。创建密钥时设置使用密码，用于加密和解密操作的使用授权。当用户需要使用该密钥时，它载入到一个空闲的区域，调用可信密钥加载命令，用父密钥解密并将返回密钥供用户使用。密码模块密钥直接存放在可信密码模块内部，通过可信密码模块的物理安全措施保护。实体加密密钥、实体认证密钥、实体权限数据等信息构成实体身份数据块，由存储根密钥加密保护，存放在可信外部。

(2)可信度量与完整性校验。完整性度量服务实现了嵌入式安全计算机可信性，将可信芯片作为信任根[11]，对固件、操作系统隔离内核、分区客户操作系统镜像等进行逐级加载，逐级验证其完整性。可信度量评估与完整性校验服务主要包括完整性计算、完整性验证、完整性存储三个步骤。嵌入式安全计算机上电启动后，加载被度量软件对象，度量单元对被调用组件的相关信息进行Hash运算得到组件完整性度量值；从预期度量值列表中获取其完整性预期值；将计算得的度量值与预期值比较，若相同则运行该组件，并准备下一个组件的加载，将度量值存储在安全存储区域的配置寄存器和存储度量日志中。

(3)可信身份验证。标识用于系统对用户惟一身份的标识，将用户标识符与用户联系的过程称为鉴别[12]。身份标识与鉴别机制的实现基于可插入认证模块和强化的口令管理，以USB KEY方式进行硬件身份认证、登录方式限制、多重身份鉴别等。嵌入式系统安全架构的可信身份认证过程通过国产安全控制模块创建身份认证密钥，签署运行在嵌入式安全计算机各个分区上的应用程序的公钥来保证可信性，通过存储根密钥保护密钥的私有部分，通过可信第三方认证机构负责密钥公有部分的认证。

## 6 结语

本文研究的安全可信的嵌入式系统架构通过在资源分配、信息流和故障等方面的完全隔离，使嵌入式系统能够完全遵循由开发人员或系统定义的各种安全规则，具有多级安全策略、故障隔离、系统安全可信度量、用户身份认证、安全通信等能力。安全可信的嵌入式系统架构目前已成功应用在SCA软件无线电中，作为电台通信的安全模块，实现了软件无线电系统的信息安全与可信，下一步将在军事国防、航空航天、汽车船舶、工业控制等国内安全关键领域推广应用。

## 参考文献

[1]Harrison W S,Hanebutte N,Oman P,et al.The MILS Architecture for a Secure Information Grid[J].Journal of Defense Software Engineering,2005,18(10):20-24.

[2]闫路平,龚乐中.基于MILS架构的高可信嵌入式操作系统研究[J].通信技术,2016,(12).

[3]石鹏.基于MILS架构的操作系统安全技术研究与实现[D].成都:电子科技大学,2016.

[4]邢薇薇.面向航空电子的分区内核关键技术研究[D].西安:西安电子科技大学,2011.

[5]Kaiqiang Li,Hao Feng. Information flow control model and method in distribute MILS[C]//Proceedings of the Tenth International Conference on Computational Intelligence and Security, 2014.

[6]张灯.面向多重独立安全等级架构的安全通信机制研究[D].西安:西安电子科技大学,2011.

[7]崔西宁,王聪琳.基于MILS CORBA的多级安全分区通信机制[J].计算机科学,2013,40 (5):38-41.

[8]Carolyn Boettcher,Raytheon.The MILS Component Integration Approach To Secure Information Sharing[C]//Proceedings of the 27th Digital Avionics Systems Conference, October 26-30,2008.

[9]关巍.可信软件栈中TSP的研究与应用[D].沈阳:东北大学,2010.

[10]朱强.一种可信计算软件栈的设计与实现[D].北京:北京邮电大学,2009.

[11]闫建红.可信计算的动态远程证明研究[D].太原:太原理工大学,2012.

[12]刘英.专用可信计算网络的研究与设计[D].成都:电子科技大学,2011.

••••••下转第190页

分析,逐级缩小报表的颗粒度,更快速、准确定位事件数据项。

2.5 数据的存储和检索

大量的数据积累对空间要求比较大,但这些数据又要保留下来以便日后的查询,所以数据的压缩存储显得尤为重要。系统支持自动按照规定一定的压缩方法,用95%以上的高压缩比例来存储数据。可以自定义重新检索的数据范围,进行回档操作,并对回档出来的数据重新检索。

2.6 对数据库疑似攻击防范

数据库中的潜在威胁可以被审计记录发现,如相关的密码输入错误和一些在操作过程中的命令语句等都可能存在被恶意攻击的风险。本系统内置专门用来检测的规则库,可将有可能对数据库造成威胁的风险及时阻止,让数据库安全平稳的运行。

2.7 审计预警机制

系统具备独立的告警配置功能模块,支持用户自定义预警策略,对所关注的敏感信息操作进行告警;用户可以自定义报警的机制,将不同的级别信息用对应的警告方法,可以设置短信提醒和电话提醒等,可以及时挽回或降低损失。

2.8 系统自身安全性机制

系统具备完善的权限管理体系,严格区分不同角色。在授权和审计方面实行分离的原则,具有更好的安全性;在日志上做到尽量完善,将用户和设备的操作过程完整的记录下来;系统可支持加密处理,用户自己设置加密措施,出现相关异常处理时,系统发出邮件告警、消息等告警方式提醒用户;关键部件设置自检装置,可用于自动修复异常情况。

## 3 系统应用部署

3.1 单独对应模式

对于用户业务应用相对较单一的数据库系统,可采取业务客户端单独对应数据库的客户端,用户可对其服务器进行访问,同时审计引擎将所有的访问都进行记录,审计服务器负责对这些记录集中管理。

3.2 多监听多路部署模式

对于数据库规模和版本不统一,有多个不同业务系统的运行条件的情况下,可以用引擎多口形式,采集不同口的数据再通过审计中心服务器集中处理。

3.3 分布式环境部署模式

如果数据库所需规模较大且分布很广,审计引擎的需求量较大,采取地区分布布置引擎,再由一台审计中心服务器集中管理。

## 4 结语

本文从企业的数据库安全方面出发,制定了安全审计系统的实现方法,设计出较为全面的安全审计功能。可追踪用户的操作过程,支持异常行为警告,还可以进行数据查询和展现报表结果,适用于电力企业数据库的安全要求,而且其部署方式较灵活,具有很高的应用价值和前景。

## 参考文献

[1]彭友,王延章.信息系统内部安全审计机制[J].北京交通大学学报,2009,33(2):112-116.

[2]黄晨,胡红云,蒋安东,等.分布式安全审计系统设计与实现[J].计算机工程与设计,2007, 28(4):811-813.

[3]杨磊,毕红军. 基于旁路监听的数据库安全审计系统[J]. 计算机工程与应用,2015,51(8):138-142.

# Design and Application of Database Security Audit System for Electric Power Enterprises

ZHANG Hao,SUN Chang-chun,ZHU Xiang-li,GUO Zhong-ying

(State Grid Huangshan Power Supply Company,Huangshan Anhui 245000)

**Abstract:**For electric power enterprises, the database in its business application system is charged with providing real-time, efficient and reliable services for all levels of users and electric power production and operation. Its safety problem is particularly important. From the perspective of information security, this paper explores the analysis and supervision of system database operation, and provides effective technical means, so as to ensure the safety control and risk prevention of all kinds of businesses.

**Key words:**electric power enterprise;data base;security;audit

••••••上接第188页

# Safe And Reliable Embedded System Architecture

YOU Xia,MA Yun,HU Ming-xing

(The 32nd Research Institute of China Electronics Technology Corporation,Shanghai 201808)

**Abstract:**To resolve the information security of the security-critical embedded systems, aiming at the features of multi-level security architecture, this paper proposes a safe and reliable embedded system architecture. By implementing the separable kernel of the embedded operation system, strict data access and communication are achieved in the aspects of resource allocation, information flow and failure separation. By building a system reliability chain, user identity authorization and application integrity verification are provided. The security key embedded system has the ability of multilevel security strategy, fault isolation, secure communication, trusted measurement, identity authentication and so on.

**Key words:**Multiple Independent Levels of Security(MILS);separable kernel;trustiness driver;security service