# 基于安全域隔离的嵌入式系统的访问控制机制研究

牛文生[1] 李亚晖[1,2] 张亚棣[1]

(中国航空工业计算技术研究所 西安 710068)[1] (西安电子科技大学计算机学院 西安 710071)[2]

**摘 要** 针对嵌入式领域安全关键系统的信息安全问题,提出了基于安全域隔离的访问控制模型,采用分区间信息流隔离控制机制,结合分区间消息路由和消息权限鉴别机制,实现了分区操作系统中安全关键类应用任务的多级安全访问控制,并依据该模型设计了多级安全操作系统的访问控制机制。通过安全性分析证明,该机制使基于微内核的嵌入式操作系统能够防止非法的资源访问、身份伪装、信息泄露和隐秘通道等安全威胁;经过系统的性能测试表明,安全访问控制机制的引入使嵌入式操作系统的综合性能消耗约为10%左右。

**关键词** 多级安全,强制访问控制,时空隔离,安全监控器

**中图法分类号** TP309 **文献标识码** A

## Research on Secure Access Control Mechanism Based on Secure Domain Separation for Embedded Systems

NIU Wen-sheng[1] LI Ya-hui[1,2] ZHANG Ya-di[1]

(Aeronautical Computing Technique Research Institute, Xi'an 710068, China)[1]

(School of Computer and Science, Xidian University, Xi'an 710071, China)[2]

**Abstract** Based on secure domain separation model, the research in secure architectures of embedded systems proposed a method of the secure access control, which supports multi-level secure separation of information stream with the message router between partions and messages authority based on the secure partition kernels. In order to implement the multi-level security embedded operating system, the structure of the secure access control mechanism was presented according to the secure domain separation model. The security analysis results prove that the proposed method can keep from security threats includeing illegal resource accessing, identity personation, information revealing and cover channel etc. The perfangmance analysis results show that the synthetical comsuming is about 10% with importing the security access control mechannism.

**Keywords** Multi-level security, Mandatory access control, Space separation, Security monitor

## 1 引言

随着在工业、医疗和武器装备战争中的信息化程度越来越高,安全关键类嵌入式系统越来越受到重视。此类系统必须提供高度灵活的控制数据和媒体数据的通信能力,同时需要保证不同安全等级的控制信息和数据信息相互间不受影响。这些能力的提升与功能的增强建立在大量软件共享硬件资源的基础上,必然要求把不同安全级别的应用集成到一个综合化的信息处理平台上,因而系统安全成为当前急需解决的重要问题。

## 2 多级安全的嵌入式操作系统

在综合化电子系统的开放环境下,安全关键类嵌入式操作系统除了保证不同安全关键级别的软件互不影响外,还要避免系统遭受来自网络连接的恶意攻击。面对这种情况,国外开始研究多重独立等级安全(MILS, Multiple Independent Levels of Security)体系架构[1],如图1所示。MILS安全性的核心设计思想是将操作系统进行层次划分,内核层仅仅包含非常小的、提供时间和空间隔离机制的软件,并且其经过了形式化验证,而大多数传统的操作系统功能(如设备驱动和分区化通信软件)则作为中间件服务提供给用户,应用程序仅仅负责实施应用层的安全策略。如果操作系统按照MILS架构设计,那么运行在每一个分区中的不同安全级别的应用就可以被独立地评估,这种"分而治之"的方法可极大地降低系统的安全隐患。

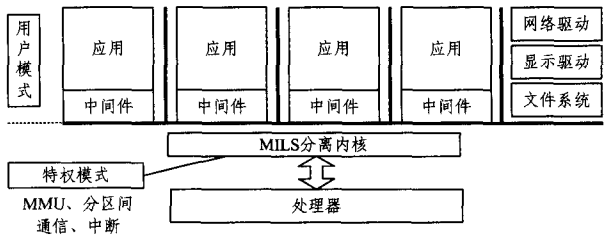


图1 MILS体系架构

### 2.1 嵌入式操作系统的安全需求

在嵌入式系统中,为了获得高安全,软件系统需要设计为分层的系统架构,在该架构中多个层提供各自明确的、定义良

本文受航空科学基金项目(2010ZC31002)资助。

牛文生(1967-),男,博士,研究员,主要研究方向为嵌入式系统和系统安全,E-mail:nwsheng@yahoo.com.cn;李亚晖(1976-),男,博士,高级工程师,主要研究方向为嵌入式系统和信息安全。

好的安全机制，该安全机制能够被更高层所使用，因而涉及到以下 4 方面的安全需求。

多级安全的嵌入式系统需要在分区操作系统中支持多种安全级别的任务同时运行在一个分区或多个分区内，这样分区就因为应用的安全级别而具有了相应的安全级别。当一个分区中存在多个安全级别的应用时，分区内的应用也需要相互间进行安全级别的隔离和保护[2]。

多级安全的嵌入式系统中需要能够支持对分区内的应用功能的安全监控，当分区内存在多个安全级别的应用任务时，能够通过安全监控代理对应用间的消息通信进行访问控制和信息隔离；

多级安全的嵌入式系统中的安全机制需要操作系统的微内核的安全机制支撑，这种具有安全功能的微内核其代码量必须小，且能够通过形式化验证的方式保证其理论证明的安全性[3]；

多级安全的嵌入式系统的授权和验证机制需要采用模块化设计，能够分布在不同分区中进行访问控制，能够达到安全功能与操作系统系统服务功能的松耦合，同时能够进行增量式的组件化安全验证；

在支持多级安全的嵌入式软件系统中，不同安全级别的应用任务之间的信息流需要进行安全隔离，以防止不同级别信息流之间相互泄露敏感信息，包括基于时间和空间的隐蔽通道的防护[4]。

### 2.2 相关研究情况

当前安全操作系统的构建主要集中在传统操作系统的改进方面，这种方法的设计思想是通过对传统操作系统的内核进行改进，在系统内核的多个系统调用接口增加安全访问机制，使系统能够达到一定的安全级别，例如黄玉琪等提出的基于三权分立原则的安全操作系统结构设计，利用虚拟机对传统操作系统的功能进行分割与重组，实现安全隔离的目的[5]；韩立毛等采用在开源嵌入式操作系统 uC/OS-Ⅱ中增加安全内核，同时改造系统的调用接口，实现安全访问控制功能的嵌入方式[6]。但是，这种改进方法却存在着先天的不足之处，首先是操作系统内核无法对安全访问控制功能提供安全支撑，内核自身的安全性无法保证；其次是增加的安全功能分散在系统的多处，无法完整地验证安全功能自身的安全性；最后，由于和系统服务功能紧密耦合，安全功能对系统的影响无法验证。

本文采用基于 MILS 架构的嵌入式软件体系架构，针对微内核进行安全增强，保证安全微内核在能够进行形式化验证的基础上，为用户态的安全功能提供支撑。安全访问控制功能以组件的方式运行于用户态的分区中，基于安全微内核提供的信息流隔离机制实现对分区中应用任务的多级安全保护，因而能够从底层实现安全防护支撑，并能够单独对用户态的安全访问控制功能组件进行安全性验证，更加高效和安全地实现全系统的安全防护。

## 3 多级安全的保护机制

### 3.1 安全域隔离机制

采用多级安全架构的微内核操作系统，将各类任务进行多种级别的安全域划分。多级安全的域划分规则是可以根据用户的安全需求进行配置和修改，用户可以根据任务的密级划分为非密、秘密、机密和绝密，也可以根据安全关键类任务的安全性等级进行细粒度划分，进而扩展安全访问控制策略来实现安全域的隔离机制。本文采用任务密级原则进行任务的安全域划分，如图 2 所示。系统共有 12 个任务分别运行在 A、B、C、D 4 个分区中，其中任务 1、4、7、10 是秘密级任务，任务 2、3、5、9、11 是机密级任务，任务 6、8、12 是绝密级任务。当系统按照安全等级将任务划分成多个安全域后，安全域之间的访问通信必须通过系统的安全访问策略进行仲裁，而在安全域内的任务之间，则可以通过消息路由后进行相互通信。采用安全域隔离机制，可以将任务的安全性约束在一定的范围内，当其出现故障或恶意行为时，只能在安全域内产生影响。安全域可以应用于任务的冗余容错机制，当多个备份的任务运行在不同的分区中时，其安全级别相同，当一个任务实例发生故障时，还可以在安全域内进行动态迁移实现系统功能的动态重构。

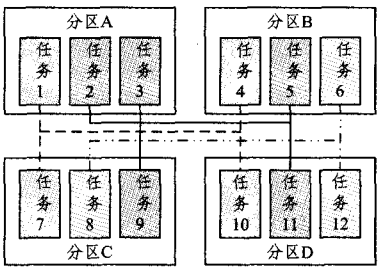


图 2 安全域隔离机制

### 3.2 多级安全访问控制

在多级安全的嵌入式操作系统体系架构中，利用安全中间件层的透明性在分区中引入 MILS 消息路由(MMR：MILS Message Router)和 GUARD 两个安全中间件，构建安全访问控制模型。MMR 的基本功能是为分区间通信提供路由，同时支持数据隔离、信息流控制等功能。GUARD 中植入 BLP 授权模型，包含系统的强制访问控制策略。结合本文设计的安全域隔离机制，任务 1、2 运行在分区 A 中，任务 3、4 运行在分区 B 中，其中任务 1、4 属于同一安全域，而任务 2、3 属于另一安全域。

(1)安全域内任务间通信访问控制模型。当属于同一安全域的分区 B 中的任务 4 向分区 A 中任务 1 请求通信时，消息进行分区间转发，其中 MMR 提取消息的路由信息，当判别出属于同一安全域时就直接将消息转发给分区 A 中的任务 1，如图 3 所示。

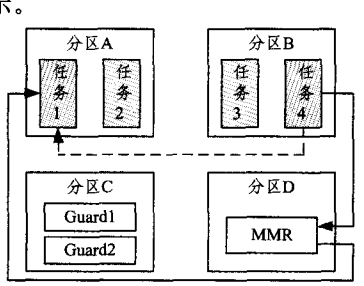


图 3 安全域内访问控制模型

(2)安全域间任务通信的访问控制模型。当属于不同安全域的分区 B 中的任务 3 向分区 A 中任务 1 请求通信时，消息进行分区间转发，其中 MMR 提取消息的路由信息，当判别出属于不同安全域时，将消息传给相应的 Guard1，Guard1 依照访问控制策略进行判断分析，禁止或允许该通信的进行，同

时将结果反馈给 MMR。如果允许，MMR 将把消息传输至目的地，否则将丢弃消息，如图 4 所示。

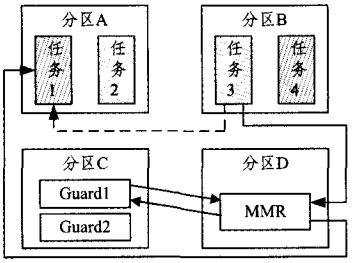


图 4　安全域间访问控制模型

(3)分区内安全域内通信。如果属于同一安全域的两个任务运行在同一分区内，则可以采用分区内任务通信机制实现消息交互，如消息队列、白板等，但仍然需要分区内安全监控机制进行访问控制。

(4)分区内安全域间通信。如果属于不同安全域的两个任务运行在同一分区内，则仍然需要按照步骤(2)中的机制进行安全访问控制。

## 4　多级安全的系统安全核架构设计

本文提出一种安全核体系结构，其基本思想是：通过基于 MILS 架构的嵌入式操作系统安全相关应用程序接口，实现分区内应用程序安全监控；然后在决策缓存中查询，如果请求的操作被允许则允许操作执行；如果没有找到则把请求转交到策略服务器进行判定；策略服务器用策略数据库中的策略数据元素和所请求的调用，通过 BLP 和 DTE 安全策略进行判定[7]；如果判定请求允许则返回正确，同时将判断的结果存入策略缓存中，以便下一次直接判定；如果判定请求不允许则对该应用程序的调用请求被拒绝；每次判定完后将结果交给审计子系统，用于以后查询。

### 4.1　系统安全核体系结构

该结构中实现安全核功能的访问控制机制主要包含以下组件，如图 5 所示。

(1)策略服务器：策略服务器主要负责多级安全策略和完整性策略的加载和更新，依据安全策略对应用的访问行为进行鉴权仲裁，对分区策略缓存和内核策略缓存进行管理，并对系统中主客体的安全标识和安全属性进行维护管理。

(2)策略缓存：系统中策略缓存分为两部分，一部分是分区策略缓存，主要用于分区内应用之间的相互访问行为的快速鉴权，对应在策略服务器中关于安全策略的组织结构中将分区内关于主客体访问的安全策略集中管理；另一部分是内核安全策略缓存，主要用于分离内核中分区间信息流隔离机制快速鉴权，对应在策略服务器中将内核信息流隔离的多级安全策略和完整性策略集中管理。缓存策略的更新机制采用最近最多使用原则。

(3)访问监控器：访问监控器监控所有与安全相关的访问。当拦截到访问请求时，转到安全判定部分。访问监控器分为两个部分，一部分是分区中分区内应用之间的行为监控，另一部分是分离内核中分区间通信的行为监控。

(4)安全策略配置接口：安全策略是安全嵌入式系统的核心策略，是支持全系统进行安全访问控制的依据规则，系统中的安全策略主要通过配置接口为用户提供配置信息导入，通过该接口能够将系统安全策略配置信息加载到策略服务器，并将系统安全审计信息进行卸载维护。

(5)安全域配置接口：系统安全域的划分需要依据应用任务的安全等级和功能关系，在安全嵌入式系统中安全域的定义在系统加载前通过配置文件来确定。系统安全域中应用的配置信息需要通过安全域配置接口加载到分区消息路由。

(6)分区间消息路由：分区间消息路由是实现分区间通信的核心机制。为了能够支持基于信息流的多级安全性，分区间的消息通信都必须通过分区路由机制进行鉴权和转发。鉴权过程依据安全域配置信息，采用多级安全策略授权分区间的通信。

(7)分区间通信接口：分区间通信需要安全嵌入式操作系统的微内核支持，该机制的接口位于微内核中，负责分区间通信管理、信道资源分配和信道隔离，检测隐蔽信道的存在，对信道进行安全保护。

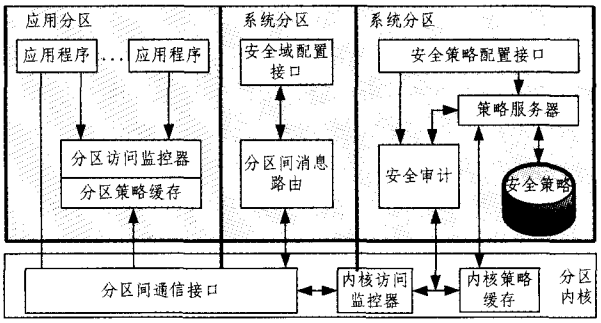


图 5　支持多级安全的访问控制架构

### 4.2　安全访问控制流程

(1)应用请求调用。当应用任务访问分区内资源时，应用任务首先发起资源访问请求，该请求将被发转发给分区访问监控器；当应用任务访问分区外系统资源时，首先通过系统调用向操作系统内核发起请求，系统调用将该请求转入内核的分区通信接口，该接口将调用内核访问监控器进行访问控制。

(2)安全监控器响应请求。安全监控器接收到应用任务的资源访问请求时，将依据请求消息中携带的应用任务标识、分区标识和资源标识在策略缓存中进行策略查找，当找到相应的策略记录后，依据策略规则进行鉴权，并将鉴权结果发送访问监控器。

(3)安全策略匹配。系统设计的安全策略采用两级缓存机制，在靠近安全监控器的位置采用最近策略缓存机制，以加快安全策略的匹配过程。当策略缓存中没有对应的策略记录时，策略缓存机制会通过分区间通信将查找请求转发给系统的安全策略服务器，以获取该请求的策略记录，当取得记录后即进行鉴权；如果没有对应的策略记录，则默认为禁止访问。

(4)安全审计记录。在安全监控器对每个应用任务的请求做出鉴权后，都要将鉴权结果发送给安全审计，安全审计将以请求消息中携带的应用任务标识、分区标识和资源标识作为记录索引，在安全审计数据库中添加鉴权结果记录，用于后期系统安全管理员的审计维护。

## 5　性能分析

### 5.1　安全性分析

本文采用多级安全模型和基于域和型的访问控制模型来设计安全策略，实现对系统中的不同安全等级的进程进行基

(下转第 326 页)

系统的分析评估体系和应用系统。相关研究成果已经成功应用到国内某大型科研研究机构，并通过了安全保密测评。实践证明，该系统具有了操作简便、运维方便、多模式下视频业务应用灵活及高安全防护等级等特点，对涉密等级和安全要求高的单位在建设高清视频会议系统及解决相关安全防护方面具有一定的借鉴意义。

## 参 考 文 献


[1] ITU-T Recommendation H. 323-1998, Packet-based multimedia communication systems[S]

[2] SNL. Sandia Lab Accomplishments 2001－2007 [EB/OL]. http://www.sandia.gov/LabNews/labs-accomplish/archive.html

[3] Masullo C. BNL. "Can you See me Now?"[R]. NLIT. 2010

[4] 王颖. H.264 在视频会议系统中的应用[J]. 硅谷，2010(08)

[5] 刘浩，胡栋. 基于 RTP/RTCP 协议的 IP 视频系统设计与实现[J]. 计算机应用研究，2002，19(10)

[6] 王枫博，贾世杰，郭宇明，等. 基于 H.323 网络视频会议系统的关键技术研究[J]. 科技情报开发与经济，2009(05)

[7] 丁久荣. 浅议网络安全与信息安全[J]. 新课程：教育学术，2010，(03)

[8] 陈丽英. 网络视频会议业务的现状与未来[J]. 电信技术，2009(12)

[9] 梅云红. 计算机网络安全隐患与防范策略的探讨[J]. 计算机与信息技术，2007(09)

[10] 国家保密局. BMB20-2007《涉及国家秘密的信息系统分级保护管理规范》[S]. 2007

[11] 国家保密局. BMB22-2007《涉及国家秘密的信息系统分级保护测评指南》[S]. 2007


(上接第 322 页)

于策略模型的安全访问控制。下面给出本文涉及到的安全模型的安全性分析。

本文通过运用基于安全域隔离模型，设计在 MILS 架构下的访问控制机制实现方法，有效解决了几方面的安全问题：

(1)非法的资源访问。每个分区内应用任务的访问请求都要被监控，判断主体请求的操作是否合法，以确保在符合安全策略规则的条件下能够访问被请求的资源，从而保护系统的安全。

(2)身份伪装。访问鉴权的过程中，首先要对请求的主体的身份标识进行验证，验证的方法可以采用密码学中公钥证书的签名验证或者基于对称密钥的 HMAC 验证码，从而保证请求主体身份的合法性，有效防止非法应用任务获取资源导致敏感信息泄漏。

(3)信息泄露。系统通过安全监控器对请求消息的拦截与鉴权，并依据多级安全的强制访问控制策略对不同级别的消息进行隔离，能够有效防止不同安全级别间的消息出现敏感信息的泄露[8]。

(4)隐秘通道。系统通过采用 BLP 模型进行多级安全的强制访问控制，并采用通常禁止不同密级的应用任务之间进行访问请求，从而能够有效避免基于时间和空间的信息流隐蔽通道的存在。而当个别不同安全级别的应用任务间需要跨级访问时，需要通过安全审计中心进行特别记录，并在记录中增加访问操作的发生时间和敏感信息摘要，用于安全管理员的后期审计维护。

### 5.2 系统性能分析

本文设计的安全操作系统的性能测试环境为：目标机 CPU 是 PPC7447，主频 1GHz，宿主机操作系统为 WinXP，目标机操作系统是安全嵌入式操作系统。采用相同的测试用例，在本方案规定的测试环境中，测试代码优化/非优化、CACHE 打开情况下的操作系统基本性能。完成操作系统下主频 1GHz 的 PPC7447 目标机运行性能测试。方法：将用于测试的计算应用程序移植到操作系统中，在代码优化/非优化情况下进行该项测试。其中包括：常规运算型用例，其赋值语句占 55%，控制语句占 32%，过程/函数调用占 15%；双精度浮点运算的用例；大计算量的控制率计算用例。经过在测试环境中运行，增加安全访问控制机制的安全操作系统的性能下降约 10%左右。

**结束语** 在安全嵌入式系统中，操作系统不仅作为整个系统的功能性平台，还作为系统的安全平台对整个系统的安全性产生影响。本文对基于微内核的安全嵌入式系统模型进行研究，不仅能够保证各分区的隔离安全性、信息流的可控性，还能基于微内核的特点构建多重独立安全体系，进一步增强系统的安全性。基于微内核系统由于结构简单，在具体实现时能够保证嵌入式系统的实时性能，因此能较好地解决安全嵌入式系统设计中安全与性能之间的平衡问题。

## 参 考 文 献


[1] Alves-Foss J, Taylor C, Oman P. A Multi-layered Approach to Security in High Assurance Systems[C]// Proceedings of the Hawaii International Conference on System Sciences. January 2004

[2] Rushby J M. The Design and Verification of Secure Systems[J]. ACM Operating Systems Review, 1981, 15(5): 12-21

[3] Rushby J M. Proof of Separability: A Verification Technique for a Class of Security Kernels[J]. Computer Science, 1982, 137: 352-367

[4] Boettcher C, Rushby J. The MILS component integration approach to secure information sharing[C]// the 27th Digital Avionics Systems Conference. October 2008: 26-30

[5] 黄玉琪，张建平，马利. 基于三权分立原则的安全操作系统结构设计[J]. 计算机应用与软件，2010，27(8)：159-162

[6] 韩立毛，赵跃华，马祥顺. 嵌入式操作系统的内核安全研究与设计[J]. 计算机工程与设计，2010，31(14)：3233-3236

[7] Bell D, LaPadula L. Secure Computer Systems: a Mathematical Model[R]. Technical Report MTR-2547 (Vol. II). MITRE Corp., Bedford, MA, May 1973

[8] Brien R O, Rogers C. Developing application on LOCK[C]// Proceedings of Symposium Research in Security and Privacy. Oct 1991: 206-214