一个安全嵌入式操作系统内核设计与实现

赵跃华 马祥顺

(江苏大学计算机科学与通信工程学院 江苏镇江 212013)

摘要： 针对电力领域中的嵌入式操作系统安全问题，在分析 uC/OS-II 源码的基础上，修改和精简 BLP 模型，对系统内核的 API（应用程序接口）访问控制进行了设计与实现，以达到内核的安全访问。具体包括访问监视器，仲裁服务器以及策略缓存的设计，最后对系统进行部分安全测试和性能测试。实验结果表明设计能有效地控制不同等级主体对内核资源的访问。

关键字: 嵌入式系统; 安全; 强制访问控制; 内核; 访问监视器。

Design And Implement Of A Secure Embedded Operating System Kernel

ZHAO yue-hua , MA xiang-shun

Dep. of computer Science and Telecommunication engineering, Jiangsu University, Zhenjiang Jiangsu, 212013 China

Abstract: Aim at the secure problems of the embedded operating system in power filed, analyzing source code of uC/OS-II, modify and simply the BLP(Bell-La-Padula) model, design and implement the function of API(application program interface)access to kernel, to achieve secure access. The design includes the access monitor, the arbitrator, and the buffer of policy. Finally, test partial function of security and the performance of system. The experiment indicates that design can effectively control access to kernel by various grades subjects.

Keywords: embedded system; security; MAC (mandatory access control); kernel; access monitor.

中图分类号 TP309.2 **文献标识码：A**

1 前言

嵌入式操作系统具有面向应用、专业性强、可以裁剪、效率和资源利用率高等优点，在电力行业有着悠久和广泛的使用。但是由于嵌入式系统本身条件的限制，嵌入式操作系统的安全防护能力相对有限，系统比较脆弱，易受攻击，安全性能比较差，特别是随着电力设备的开放性和网络化发展，更加容易受到攻击，系统的信息安全面临更大的挑战。电力领域的嵌入式操作系统的系统安全主要包括下面几个方面：标识与鉴别，访问与控制，入侵检测，安全审计等。安全机制的核心内容之一就是访问控制控制，特别是对系统底层资源的访问控制。本设计将结合电力系统的分析，采用开源操作系统内核 uC/OS-II 为原型，构建微内核的安全访问控制，以达到系统内核的可信访问。

2 电力系统安全威胁分析

当电网之间各子站之间的以及与主站之间进行网络传输，信息交互时，访问控制就成为一种安全需求，包括一些重要数据的保护以及整个子站系统资源的访问保护。嵌入式系统接入网络以后所面临的安全问题主要可分为两个方面，即系统安全和信息安全，具体而言主要包括以下几类：(1) 中断：对系统的可用性进行攻击，使变电站和其他系统的通信发生中断，如调度端或数据中心无法获知现场信息，厂站端也无法接收来自调度端的命令。(2) 窃听：对系统的保密性进行攻击，在变电站和其他系统进行通信时，非法窃取敏感信息。(3) 篡改：对系统的完整性进行攻击，更改变电站与其他系统之间传输的信息，使调度主站得到错误的运行工作情况，威胁电网的安全运行。如果篡改的是来自调度端的遥控命令、修改定值

命令等，更有可能造成严重的后果。(4) 伪造：对系统的真实性进行攻击，在网络中插入伪造“合法”信息发往变电站或主站，可能造成与篡改信息类似的后果。

因为内核处于系统的底层资源，所以实现嵌入式操作系统内核的访问控制将能有效的保证内核资源的保密性以及内核运行的可靠性。

3 系统整体方案设计

内核访问控制就是要在外层访问和内核之间介入一个安全机制，验证访问者是否有权限访问受保护的目标资源。当外部访问者提出对内核的访问请求，被访问监视器执行单元截获，执行单元将请求信息和目标信息以决策请求的方式提交给决策仲裁服务器，仲裁单元根据决策算法返回决策结果，访问监视器根据决策仲裁是否执行访问。针对 uC/OS-II 内核中已定义了一系列调用函数，我们可以根据其系统调用设计安全钩子函数，当调用产生时即触发访问监视器的安全检查，检查访问主体是否有权限访问内核。本文以系统调用为基元，控制对客体的访问。系统结构图 2 如下：

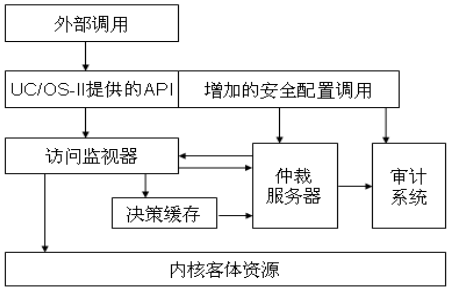

图 2：系统框架结构图

系统中增加的安全配置调用模块主要用于可信主体对安全策略的配置和对审计系统的数据访问。考虑到应用到电力系统中要求的实时性要求很高，为了减少安全检查对系统实时性能的影响，在设计中，本文增加了决策缓存模块，以缓解仲裁服务器因决策的计算和传递每个决策通信而造成的实时性能的降低。本文在仲裁策略的设计上采用基于修改的 BLP 模型的 MAC 对内核资源进行受控访问设计。

4 系统详细设计与实现

本文采用模块化设计方式，减少了各模块之间的耦合度，这样可以更方便一些模块的更新，添加和卸载，灵活性更强，更容易移植。

4.1 uC/OS-II 分析

uC/OS-II 操作系统内核的客体资源包括任务信号量，事件标志组，邮箱，消息队列，内存块以及进程等 IPC 进程间通信资源。

根据对 uC/OS-II 内核分析，客体的访问操作类型有:(1)创建 OSTaskCreate OSMemCreate 等(2) 只读 OSSemAccept OSSemQuery 等 (3)只写 OSQFlush OSTimeSet 等(4)可读写 OSTimeDly OSTimeDlyHMSM 等(5)删除 OSSemDel OSFlagDel 等(6) 为了实现安全配置，新增加的操作有授予、改变、撤销安全级别操作 OSSetAtt、OSChangeAtt、OSDelAtt，分别为设置客体安全属性、改变安全属性和撤销客体安全属性。

当外部主体进行上述 API 内核调用时，将触发其安全钩子函数检查，交予策略缓存或者仲裁服务器决策。

4.2 BLP 模型的修改

通过对 BLP 模型的分析，为了使该模型能更适用于本文开发的嵌入式安全操作系统内核，将对 BLP 模型做必要的修改和简化，以更好的适应嵌入式系统的环境和需求。

（1）考虑到嵌入式操作系统资源的有限，以及电力系统中的实时性，简化对访问请求的复杂度，本文采用单独策略支持，支持 MAC 访问控制。

（2）在强制访问控制策略中，为了保证客体内容的完整性，修改 MAC 策略中的写操作，规定当主体以 w、a 属性访问客体时，主体安全级别必须等于客体安全级别，或者主体为可信主体。

（3）关于激活型策略的修改，当主体创建一个新客体时，客体的安全级别继承等于主体的安全级别，当主体删除一个客体时，主体的安全级别必须大于等于客体，删除客体必须先删除其敏感信息，然后删除客体本身。

（4）在本文中，由于 uC/OS-II 内核简单，不存在层次关系，故 BLP 模型中的兼容性策略可以忽略。

由此对应修改的 BLP 模型对安全钩子函数进行仲裁算法的可设计如下：

read 操作，其规则特征函数：

Op (p, f, r)=true iff $f(O) \leq f(S)$

write 操作，规则特征函数：

Op (p, f, w)=true iff $f(O)=f(S)$

append 操作，规则特征函数：

Op (p, f, a)=true iff $f(S)=f(O)$

execute 操作，规则特征函数：

Op (p, f, e)=true iff $f(O) \leq f(S)$

delete 规则特征函数：

Op (p, f, d)=true iff $f(O) \leq f(S)$

说明：其中 f 函数用于获取主体或客体的安全级别。

为了实施多等级安全访问控制，本文根据主体、客体的类型分别在其结构体中加入相应的安全标识结构。

主体安全标识结构如下：

```
strcut sec_subinfo{
struct os_tcb  *task;  //指向任务控制块
SECURITY ssid;          //对象的安全级别
SECURITY csid;         //主体当前安全级别
struct sectasklist *list;// 安全任务队列
struct avc_node *poavc;    //指向上次决策缓存中该主体其客体访问权限节点
  }
```

与主体的安全标识类似，同样可以在客体的结构体中加入指针，指向安全信息结构体。

将系统设计分成访问监视器，安全服务器，以及决策缓存的设计。以下为各个模块的详细设计。

4.3 访问监视器

访问监视器是安全核中核心部件，根据 UC/OS-II 客体的类型，每种客体有一系列调用，故本文的访问监视器以钩子函数形式分别嵌入到系统的各个客体调用中，仍然以信号量操作为例，定义安全调用截获函数：

OSSECSemDel ，OSSemPend，OSSECSemPost，OSSECSemAccept，OSSECSemQuery

分别截获信号量的删除，挂起，发送，接受，查询是否符合制定的安全策略。这些安全截获函数将客体类型和安全级别，主体安全级别以及访问属性进一步提交决策缓存或者

仲裁服务器决策，并执行返回结果。

4.4 仲裁服务器

仲裁服务器的主要功能是对访问监视器提交请求进行仲裁，给新建的主客体分配安全标识，管理可重用策略缓存等。其中核心功能是访问仲裁。在仲裁服务器中实现的访问权限判定算法根据上述 BLP 模型的访问模式制定，只有经过访问策略服务器仲裁的允许，才会返回访问许可结果，交予访问监视器执行。

4.5 决策缓存的设计

采用决策缓存可以加快决策速度，减少性能开销。访问控制服务器将成功访问请求以<SUB_SEC_ID,OBJ_SEC_ID,PERMISSION>存储在缓存中，当访问监视获得访问请求时，转为 AVC 模块寻求匹配，如果没有合法的匹配项存在，则 AVC 模块发送访问请求给仲裁服务器，服务器咨询策略逻辑中的访问规则，并同时将访问规则写回至 AVC 模块。

策略缓存的设计是按客体的类型以单链表的形式存在的，初始化时为空，当访问请求时，根据客体类型分别快速映射到各个客体类型的链表表中。其节点数据结构如下：

```
typedef struct avc_node{
    SECURITY SUB_SID;     //主体安全级别
    SECURITY OBJ_SID;     //客体安全级别
    ENTITY_TYPE OBJ;      //客体类型
    UNSIGHED32 PERM;      //被允许的权限
    UNSIGHED32 LASTPERM; //上次被授权的权限
    BOOLEAN AUDITED;     //是否进行审计
    BOOLEAN USED;        //该节点是否已被使用
    }
```

5 系统测试分析

功能测试：

测试方案设计：以系统 IPC 中的简单邮箱测试为例，系统初始化及安全模块初始化时，创建任务 1 和任务 2。任务 1 的优先级为 2，安全级别为 1，任务 2 的优先级为 5，安全级别为 2，由任务 2 创建一个邮箱，继承任务 2 的安全级别。然后设置一个信息的投递和接受过程，测试是否按照所制定的安全策略进行 IPC 通讯。测试表明，对邮箱的安全访问控制完全符合设计的要求，同样可以测试其他 IPC 客体，因篇幅关系，不一一详述。

性能测试：在增加强制访问控制功能后，系统的整体性能和请求的响应速度必然会受到影响有所下降，这是由用户请求的进一步处理，也即监控器模型导致的请求时间消耗。从实用性考虑，系统性能的下降应该控制在实时系统所能容忍的范围之内。具体地说，由于新增安全功能而造成的系统性能的下降，应控制在电力领域的规范的范围以内。整个测试主要采用黑盒测试法，测试目标为进程的切换时间，测试结果表明，增加安全访问控制功能之后，整个系统的实时性有所增加，但是控制在 10%之内。

本文作者创新点：

访问控制技术作为操作系统最为基本的安全技术被广泛的使用。为了实现 uC/OS-II 的安全化，使之达到可信内核，在本文采用监视器模型的结构思想，以 BLP 模型为基础，对 uC/OS-II 的进行了以系统调用为基元的强制访问控制的实施，以保证对系统内核部件的访问。

参考文献：

【1】Jean J.Labrosse[USA] MicroC/OS-II The Real-Time Kernel Second Edition[M] 2002

【2】Bell D. E ,La Padula L.J . Security Computer Systems :Mathematical Foundations and Model. M74～244. Bedford ,Mass. Mitre Corpl ,1973.

【3】Philip Koopman, Carnegie Mellon University,Embedded system security ,EM BEDDED COMPUTING.

【4】CAI Yi，ZHENG Zhi-rong，SHEN Chang-xiang,Prcoceding of IEEE TENCON'02 :Design and Implementation MAC in Security Operating System [J]

【5】钟城，赵跃华主编 《信息安全概论》[M] 武汉理工大学出版社 2005

【6】卿斯汉,刘文清等编著 操作系统安全[M] 清华大学出版社 2004

【7】郭玮,茅兵,谢立 计算机应用与软件:强制访问控制 MAC 的设计及实现 [J] 第21卷第3 期 2004 年3月

【8】许宪成，杨存祥 组件技术及其在嵌入式系统设计中的应用[J] 微计算机信息 2007，02-016

作者简介：

赵跃华（1960- ），男，汉族，教授，主研方向：计算机网络与通信技术，信息安全，计算机控制等；

马祥顺（1981-）男，硕士研究生，主研方向：安全操作系统，嵌入式控制。

Biography: Zhao yue-hua (1960-), male , doctor , the Han nationality, Jiangsu University , Professor , Research area: security of information，computer control.

Ma xiang-shun (1981-), male, master , the Han nationality，Jiangsu University, Research area: secure OS，embedded control.

作者的通信地址：江苏镇江江苏大学 计算机科学与通信工程学院 信息安全系 赵跃华

邮编：212013