基于 uC/OS-II 的嵌入式安全操作系统的框架设计

赵跃华， 黄卫菊， 蔡贵贤， 蒋 军
(江苏大学 计算机科学与通信工程学院，江苏 镇江 212013)

摘 要：针对电力应用中嵌入式系统的安全问题，设计了一个嵌入式安全操作系统的框架。该操作系统框架以 uC/OS-II 为内核蓝本，采用模块化设计方法，并将安全特性有机地融合于每一模块，并加入联网通信功能，不仅从整体上保证了嵌入式操作系统的安全性，而且也保证了其网络安全。该嵌入式操作系统保持了嵌入式操作系统实时、可靠的特性，同时也具有安全特性，其安全级别达到了 C2 级。

关键词：嵌入式操作系统；uC/OS-II；安全性设计；审计；入侵检测；IPSec
中图法分类号：TP316.2 **文献标识码**：A **文章编号**：1000-7024 (2006) 15-2818-03

Framework design of uC/OS-II-based embedded secure operating system

ZHAO Yue-hua, HUANG Wei-ju, CAI Gui-xian, JIANG Jun
(College of Computer Science and Telecommunication Engineering, Jiangsu University, Zhenjiang 212013, China)

Abstract: According to the security of embedded system in electronic system, an embedded secure operating system is designed, Which reduces, perfects uC/OS-II and applies security into each module. This system can visit the internet and ensure not only the security of the whole system, but also the internet security. This embedded operating system keeps the characteristic of real time and credibility of embedded operating systems, it also has security, and its security reaches C2.

Key words: embedded operating system; uC/OS-II; design of security; audit; intrusion detection; IP security

0 引 言

嵌入式系统在电力系统中的应用有着悠久的历史，在发电厂自动化、变电站自动化、调度自动化等控制中用于数据采集和监控。而且随着信息化技术高速发展，电力企业将连上电力广域网，并最终连接 Internet。它们提高了电力信息化水平，提高了企业生产效率，但由于 Internet 是一个不确定的网络，随之也带来了安全性的问题。一个安全的嵌入式系统是其发展的重要基础。

1 电力应用背景下嵌入式操作系统的需求分析

在调度控制中心和变电站，运行人员看到的数据都是从远方的 RTU 传送过来的，这些 RTU 就是典型的嵌入式系统，他们不仅将现场的数据数字化并分析出很多难以直接测量的数据，并通过特定的 RTU 通讯规约传到集中计算机上。

在这些场合必须要保证系统的实时性和可靠性，这是关系电力企业安全运行的基础。嵌入式系统本身具有实时性强、可靠性高和可扩展性好等特点，而且随着信息化技术的发展，嵌入式系统除了保持它原有的特点外，还必须提供下面功能：

(1) 网络通讯功能

随着信息化技术的发展，电力企业连上电力广域网，并最终连接 Internet。这样才能实现整个电网的供电、配电和用电的整体调度和控制的功能，提高电力信息化水平。

(2) 安全的功能

首先操作系统要为它的应用软件提供一个可靠的应用平台，其次当电网的各个工作站之间的联网、整个电网的整体控制成为一种发展趋势时，网络安全问题就是一个不得不面对的问题。这里的安全包括对一些重要和敏感数据的安全保护以及对整个电网控制的安全保护。安全功能能够防止非授权用户对电网数据的窃取和对电网控制的破坏。

2 嵌入式安全操作系统的整体框架设计

根据上述要求，本文所设计的嵌入式操作系统是一个具有联网功能的、安全的嵌入式操作系统 (embedded secure operating system，ESOS)，其安全级别达到 C2 级。

ESOS 的安全性首先是为应用软件提供一个可靠、稳定的应用平台，其次是能够抵御网络威胁，保证网络通信的安全。

考虑到操作人员对嵌入式系统的访问不是经常的，所以设计成单用户的操作系统，以减少系统的开销和复杂度。将用户分为 3 个等级：超级用户，拥有对所有文件的操作权力 (创

收稿日期：2005-06-01。
作者简介：赵跃华 (1958－)，男，江苏镇江人，博士，教授，研究方向为嵌入式操作系统、信息安全； 黄卫菊，女，硕士研究生，研究方向为嵌入式操作系统、信息安全； 蔡贵贤，男，硕士研究生，研究方向为嵌入式操作系统、信息安全； 蒋军，男，硕士研究生，研究方向为嵌入式操作系统、信息安全。

建、修改、删除等）；操作用户，拥有对与应用进程操作控制有关文件的操作权力；一般用户，拥有对部分数据的只读权力。

在电力系统中，必须记录所有操作命令，因此设计一审计系统，并具有初步的入侵检测功能。对于一些重要的文件则设计加密存储。

2.1 ESOS 的框架设计

ESOS 根据软件工程的思想，为适应嵌入式系统的可裁剪性，采用模块化的设计方法，将系统划分为以下几个功能模块（如图 1 所示）：内核模块、内存管理模块、文件系统模块、网络模块等。ESOS 屏蔽了底层和任务调度的复杂性，实现了底层系统的稳定性，也减少了用户程序设计的复杂度，从而能够提高整个嵌入式系统的稳定性。在每个模块的具体设计中，将有机地融合安全功能，从而保证整体 ESOS 的安全性。

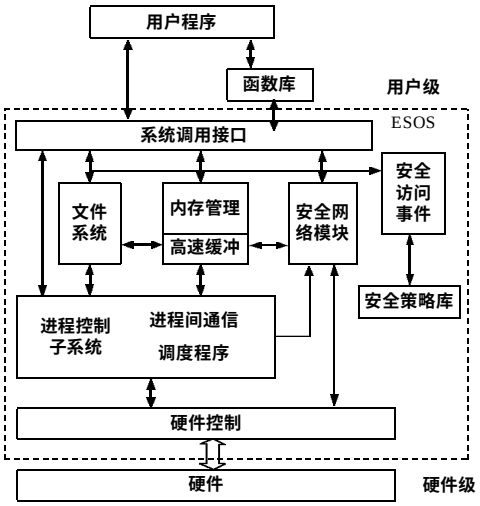

图 1　ESOS 的整体结构

2.2 各模块的设计思路

2.2.1 安全实时内核模块

为了加快开发的步伐，实时内核模块以 uC/OS-II 为蓝本，因为 uC/OS 短小精悍、稳定可靠，自从 1992 年它问世以来，在嵌入式领域，特别是工业控制系统中得到了越来越多的应用。经过十几年的研究和应用，它不断地得到完善和增强，其稳定性和实时性经受了时间的考验，现在已经发展到了 uC/OS-II。而且它的源代码是免费开放的，这对越来越重要的安全性要求来说无疑是一个福音。因为嵌入式操作系统的安全性是整个系统安全性的基础，开源代码可以不必顾忌它在系统中放置“安全后门”和设置一些人为的漏洞，而且可以修改原有的内核，并添加一些功能模块，使这些功能模块很好地与内核相结合，使系统更加安全、稳定、可靠。

uC/OS-II 只是一个简单的微内核，没有提供安全性保证。要使系统达到 C2 级安全级别，必须修改其内核，为安全性打下基础。一个 C2 级的系统必须具备两个基本功能：自主访问控制（自主安全保护的能力）和审计跟踪（有对主体责任及其动作审计的能力）。根据前面对电力系统应用的需求分析，对内核作适当的裁减和修改，加入保证安全性的内核属性和方法。

（1）强制访问权限控制

本系统采用强制访问权限控制，而没有采用前面提到的自主访问控制，主要是因为强制访问控制是比自主访问控制更严格的控制方法，这个级别的控制手段是 B 类安全标准的基础，采用强制访问控制可以为以后系统安全性的进一步加强打下基础。而且一切的系统资源调用都是要通过内核提供的函数实现，采用强制访问控制对所有的主客体资源进行安全标识，才能保证系统的安全性。

（2）审计跟踪和入侵检测

根据电力系统的需求分析，必须记录下所有的操作命令，为以后的查询服务。所以加入审计跟踪的功能。同时加入入侵检测功能，可以对系统起到一定的保护作用。本系统采用基于内核的审计跟踪，这是按照数据来源划分的检测技术。对于入侵检测采用的是滥用检测技术。滥用检测是运用已知攻击方法，根据已定义好的入侵模式，通过这些入侵模式是否出现来判断。整个入侵检测系统划分为 4 个独立的功能模块：事件产生器、事件分析器、事件数据库及响应单元。在系统的文件系统模块、网络模块和内存模块中安插一个事件产生器，用于记录各模块的日志文件，并且保存在事件数据库中，由事件分析器对其数据进行分析，产生警告，然后调用响应单元进行相应的保护。采用这种技术可以很大地减少系统的开销。

2.2.2 安全内存模块

结合上面所述电力应用的具体安全要求，内存模块的设计应该尽量精悍高效，而且能方便、实时地为 ESOS 的各个任务分配合适的 RAM 空间，并且整个系统要安全而且可靠。基于实时性考虑，内存模块主要采取固定分区策略。系统把内存空间划分为系统程序区、堆栈区、缓冲区这 3 个区。其中系统程序区主要存放一些可执行代码的映象，由于这部分改动较少，所以不再进行小分区的划分。其余的两个区要进行小分区划分，每个小分区中划分出整数个相等的块，以块作为分配和回收的单位。

内存管理模块中提供了对内存空间的安全存储控制，以便于对整个嵌入式操作系统的安全性设计提供必要的支持。首先，在该模块的一些重要的数据结构中，增加了安全性字段，为算法设计时实现安全存取控制提供保证。其次，在算法设计时，加入了基于安全性的存取判断，从而实现安全存取控制。

考虑到内存管理经常出现的内存泄漏、越界等问题，本系统也采取了一些措施。对于内存泄漏的问题采用的方法是内存管理模块扫描每个块的块控制结构，找出占用任务的任务号，再查看系统的任务表，若此任务不存在，就释放该内存。对于越界保护采用带有内存管理单元的芯片加以解决，这样在速度上可以得到保证。

2.2.3 文件系统模块

在电力应用场合中，嵌入式操作系统需要处理的数据的种类不多，而且考虑到嵌入式系统的资源较少，所以本文件系统不具备目录管理的功能，这样有利于减少系统设计的复杂度，也能够减少存储目录文件信息的空间开销。

文件系统的设计主要参照了 JFFS 文件系统的特点，并结合 ESOS 的具体情况来进行设计。首先把 Flash 分为两个大的区：一个是系统区，用来存放整个操作系统和应用软件的可执

行代码映象；另一个是数据区，用来存放一些重要的数据。这样可以防止两部分数据相互干扰。为了提高速度和灵活性，文件系统采用可变分区存储分配策略，每个文件按顺序存放在 Flash 中。安全性的实现是通过对分区中的控制块登记安全级别进行判断而实现的。对于一些重要数据采用三重冗余，从而实现简单的差错恢复和一致性的功能。

2.2.4 安全网络模块

系统连接 Internet，必须要有联网通信协议 TCP/IP，此模块中的联网通信协议采用的是 lwip（轻量级 TCP/IP 协议栈），因为 lwip 占用的资源较少，适合在嵌入式系统中使用。

当系统连接 Internet 后，网络安全是一个必须要考虑的问题，否则一些黑客就有机可乘，对电网进行破坏。本文设计是把网络层和应用层安全相结合的方法来实现网络安全。网络层实现安全可有效地降低密钥协商的开销，并可提供较全面的网络层安全服务，可为 IP 及运行于 IP 之上的任何一种协议（TCP、UDP 等）进行保护。应用层实现安全的优点是可以根据应用的活动来定义特殊的安全服务，这样做比较有针对性，可以减少不必要的开销。

网络层安全性设计主要采用了 IPSec 中的 AH 头。AH 头可验证数据起源地、保障数据完整性及防止数据报重播。具体的方法是修改 lwip 的 IP 处理程序，使 IPSec 与 IP 处理程序捆绑在一起，形成新的具有 IPSec 处理功能的 IP 层处理程序，这样可以抵御一部分网络威胁，进行安全通信。应用层的安全性设计主要是对一些重要数据和命令采用加密传输，这样即使数据报被截取也无法知道其中的内容。网络层和应用层安全相结合，它们各司其职，增强了抵抗网络威胁的能力，保证安全通信。

整个安全协议实现框架中设计了两个任务（协议主任务和 TCP 相关的时钟任务）和一个中断响应函数。主任务主要是通过 uC/OS-II 提供的信号量，获取驱动程序提交的数据，进行分析，对于需要进行安全处理的数据包交给 AH 协议进行处理，处理完后再交给上层协议进行处理，不需要安全处理的数据包，就绕过安全协议交给上层模块处理（图 2 画出了主任务的接收处理过程）。TCP 相关的时钟任务是一个定时任务。而且协议栈还设计一个类似 Windows Socket 的接口，以方便用户编写自己的网络应用程序。

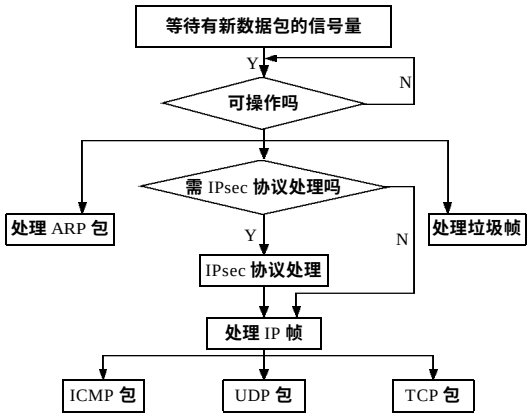

图 2 主任务的接收处理流程

3 结束语

本文所设计的嵌入式安全操作系统安全级别达到 C2 级，其整体的安全性是由各个模块的安全性来保证的。内核为内存管理、文件系统及网络模块的安全性提供支持，保障它们对资源访问的合法性。并且网络层安全协议和应用层安全协议相结合，保障了网络安全。本设计是能满足电力应用中对嵌入式系统的安全性的需求，这对于电力企业的信息安全将是一个突破。

参考文献：

[1] Jean J Labrosse.MicroC/OS-II the real-time kernel[M]. Second Edition.北京:北京航空航天大学出版社, 2003.

[2] 刘克龙,冯登国,石文昌.安全操作系统原理与技术[M].北京:科学出版社, 2004.

[3] 牛少彰.信息安全概论[M].北京:北京邮电大学出版社, 2004.

[4] 赵辉,刘志勤,胡宝成.基于嵌入式实时操作系统的文件系统的研究与设计[J].航空计算技术, 2004,(3):73-75.

[5] 王保进,王志刚.uC/OS-II 实时操作系统内存管理的改进[J].电子技术应用, 2002,(5):19-21.

[6] Nagamand Dorasany.IPSec 新一代因特网安全标准[M].北京:机械工业出版社, 2000.

(上接第 2714 页)

参考文献：

[1] 杨芙清.软件复用及相关技术[J].计算机科学, 1999,26(5):1-4.

[2] Giancarlo Succi,Luigi Benedicenti,Paolo Predonzani,et al.Standardizing the reuse of software processes [J]. *StandardView*, 1997,5(2):74-83.

[3] 徐伟华,周之英,钱岭.P－F 模型的过程复用机制及工具[J].计算机工程与应用, 2001,37(3):88-91.

[4] 周之英.基于 P－F 方法的软件过程建模的复用性[J].软件学报, 2001,12(8):1258-1264.

[5] 潘秋菱,刘宗田,张立群,等.PETRI 网在软件过程建模及过程实施中的应用[J].小型微型计算机系统, 2002,23(5):569-573.

[6] 庞岩梅,晏海华.基于工作流技术的软件过程定义和追踪机制[J].计算机工程与应用, 2003,39(26):69-72.

[7] WFMC-TC-1011.Workflow management coalition terminology and glossary[S].

[8] 李怀璋,王青.基于 ISO9000 和 CMM 的软件质量管理系统的研究[J].计算机应用与软件, 2002,19(2):25-27.