支持MLS的多层次嵌入式高可信软件架构

杨 霞，雷 剑，熊光泽

(电子科技大学计算机科学与工程学院 成都 610054)

【摘要】为增强安全关键系统的高可信能力，在分析高可信保障机制现状的基础上，提出了一种多层次的高可信软件架构。该架构采用“时空分离”思想、虚拟机技术，为基于MLS的嵌入式安全关键系统提供了一种整体解决方案。基于该架构，研究了多层次的安全和防危策略管理方法、信息流控制机制、可信软件的评估和认证方法，为安全关键嵌入式系统提供可认证的安全服务。

关 键 词 BLP安全模型； 信息流控制； 多级安全； 安全关键系统； 安全分离内核

中图分类号 TP302.8 **文献标识码** A doi:10.3969/j.issn.1001-0548.2009.06.023

Multi-Layered Trusted Architecture Supporting MLS for Embedded Systems

YANG Xia, LEI Jian, and XIONG Guang-ze

(School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 610054)

Abstract To improve the dependability of security/safety-critical systems, after analyzing status quo of high dependable safeguard mechanism, a multi-layered architecture based on the concept of separation and the VM is proposed, which supports applications with multi-level security. This paper researches multi-layered security/safety policy, the information flow control mechanism and the evaluation and certification for trusted software. This architecture can provide trustworthy services for the embedded security/safety-critical systems.

Key words BLP security model; information flow control; multi-level security; security/safety-critical systems; security separation kernel

嵌入式安全关键系统(embedded security/safety-critical systems，ESCS)是指系统功能一旦失效将危及人的生命和财产的嵌入式系统，这类系统广泛存在于航空航天、国防、交通运输、核电能源和医疗卫生等诸多领域[1]。随着美国亚丽安娜V型火箭发射失败、俄罗斯核潜艇事故的相继出现，ESCS的高可信性问题日益受到全球的普遍关注。高可信是指系统需要满足的关键性质，一旦违背这些关键性质会造成不可容忍的损失，称这些关键性质为高可信性质。高可信性质包括：可靠性(reliability)、防危性(safety)、安全性(security)、生存性(survivability)、容错性(fault tolerance)、实时性(real time)[2]。统计资料表明，随着软件技术在ESCS中的大量使用，软件的故障、失效以及安全泄漏逐渐成为引发ESCS灾难性事故的主要根源，因而ESCS高可信问题的重点在于其所使用的安全关键软件的安全性、防危性。另外，在一些非常尖端的航空、军事信息等安全关键系统中，存在多个安全级别(milti-level security，MLS)的应用，并且这些系统要求达到CC(common criteria) EAL4及以上的较高安全认证[3]。

提高 ESCS 高可信能力的传统技术有安全核技术(security kernel)、防危核技术(safety kernel)，它们通常采用对 RTOS 打补丁的方式分别增强 ESCS 的安全性和防危性。该方式一方面增加了实时内核的复杂度和大小，以至于 RTOS 无法通过较高安全级别的安全认证；另一方面无法同时解决安全性、防危性问题；此外，还不能满足 MLS 应用的需要。

本文提出一种支持 MLS 的面向 ESCS 的高可信软件架构，从嵌入式软件整体结构考虑，从根本上同时解决多级安全关键嵌入式系统的安全性、防危性问题。

1 安全关键系统高可信保障机制的现状

1.1 安全核、防危核技术

经过多年的研究与发展，目前在高可信保障技术方面已取得了大量的研究成果，其中包括安全核

收稿日期：2008－06－23；修回日期：2008－12－15
基金项目：国家863计划(2007AA01Z131)
作者简介：杨 霞(1978－)，女，在职博士生，主要从事嵌入式系统可信计算方面的研究.

技术[4]、防危核技术[5]，分别用于提高嵌入式操作系统的安全性和防危性。安全核通过对操作系统进行重构，将可信组件隔离在安全核内，其他大部分操作系统组件及应用软件放在安全核外，防止外来不可信事件对系统的非法入侵；防危核对安全关键应用软件和ESCS实施故障隔离，防止软件故障及误操作影响安全关键设备的正确运行。这两种技术存在的问题是：

(1) 在实现方法上均通过打补丁的方式增强系统的可信性能力。但随着应用越来越复杂，操作系统内核将变得更加庞大，以至于可能无法对内核进行安全评估和认证。

(2) 针对相对简单的单级安全嵌入式系统具有一定的实用性，但无法满足复杂的多级安全(MLS)应用系统的需要。

(3) 体系结构比较简单，但面临越来越复杂的安全需求时无法方便地扩充、更新安全策略。

(4) 无法同时解决安全、防危问题。

(5) 无法达到CC EAL4以上的安全认证要求。

总之，安全核、防危核技术未从根本上解决嵌入式系统的可信性问题，其主要原因在于没有把可信问题纳入到嵌入式软件体系结构中。

1.2 其他可信体系结构

从体系结构方面综合考虑可信问题的有sHype安全结构[6]、Xen VMM安全保障机制[7]、MILS安全结构[8]。它们的共同缺陷在于结构复杂，需要向嵌入式实时操作系统中添加过多的代码以至于无法通过较高安全级别的认证。另外，MILS通过安全中间件来完成分区间的信息流控制，增加了系统开销；Xen VMM没有为不同安全级别分区提供信息交互控制，自身的安全性无法得到保障，不能满足MLS应用需要；sHype借鉴FLASK安全机制的方法进行分区间信息流的控制，但其安全钩子的方法缺乏灵活性、可扩展性和可移植性。

本文提出的Hades高可信软件架构，采用分层思想分级解决系统的高可信问题，使用简单的BLP安全模型为不同安全等级分区间的信息流提供最基本的安全控制。通过尽可能简单的方法提高嵌入式安全关键系统的高可信能力，从而使系统关键部分能够通过较高安全级别的认证。

2 支持MLS的多层次高可信软件架构

Hades是一个基于MLS的多层次高可信软件架构，可从根本上提高基于MLS的嵌入式安全关键系统的安全性、防危性，下面首先介绍MLS的要求及其采用的BLP安全模型。

2.1 MLS及BLP安全模型

在一些非常尖端的航空、军事信息等安全控制系统中，存在多个安全级别(MLS)的应用，这些应用程序分别运行于多个安全模式[9]。MLS的基本要求是严格限制用户的访问请求，使用户只能访问所处安全级别中的资源，不能随意访问所有系统资源，为达到此目的通常采用BLP安全模型进行访问控制。Hades为每个子系统定义不同的安全级别，根据BLP的要求应用程序不能读比自己安全级别高的信息，也不能向比自己安全级别低的文件中写入信息，以此防止由恶意程序对系统特权信息的获取和篡改而引起的系统安全问题。例如，OS_1的安全级别为L_1，OS_2的安全级别为L_2，假设$L_1<L_2$，按照BLP模型的要求，OS_1与OS_2之间的读写关系如图1所示。本文提出的Hades高可信架构以BLP安全模型作为多级安全应用程序之间的信息交互控制策略。

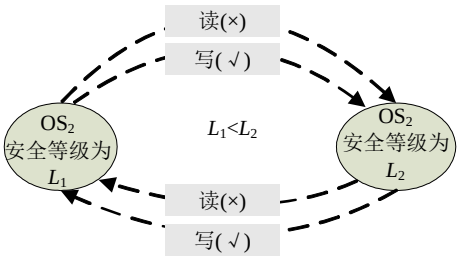

图1 BLP安全模型

2.2 Hades架构设计

Hades采用分层思想将系统分为安全分离内核、虚拟机、客户OS、嵌入式中间件、嵌入式应用软件共五层，每一层为其上层提供服务和支持。除了安全分离内核运行于特权模式外，其余各层均运行于用户模式，如图2所示。

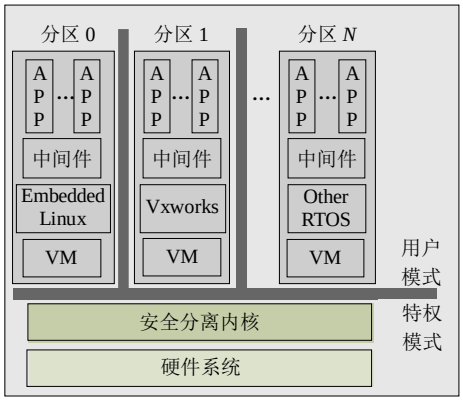

图2 基于MLS的多层次高可信软件Hades架构

文献[10]提出了Hades架构所采用的分离思想，将CPU和内存资源根据不同的安全级别分离成多个

独立区域，这一思想被称为“时空隔离”。通过这种分离可将故障和不安全信息与其他安全区域隔离，以确保对数据的隔离和信息流的控制，并能限制恶意破坏，从而提高整个系统的可信性。采用虚拟机技术使每个分离区域可以独立安装不同类型的嵌入式操作系统，将这些操作系统称为“客户”OS。根据各分区的安全关键度为每个分区指定安全级别，应用程序运行于相对独立的不同安全级别的“客户”OS中，从而将不同安全级别的应用分离，即使某个“客户”OS出现安全状况或运行失效，也不会影响其他子系统的安全和正确运行，不同安全级别应用之间的信息交互遵守BLP安全模型。下面分别介绍Hades架构主要安全层的功能及其实现方法。

2.2.1　安全分离内核

该架构最重要的模块是安全分离内核(security separation kernel，SSK)，其基本功能是分离CPU和内存资源。它将内存资源分成多个分区，并严格控制分区间的数据隔离及信息交互。通过虚拟技术为每个分区创建虚拟的硬件资源，每个“客户”OS的硬件抽象层(HAL)将分离内核看作硬件环境，“客户”OS和应用程序能够相对独立地运行于这些分区中。所有分区的时间分离由SSK的分区调度器完成，分区调度器将时间分成多个时间片，并采用相应的调度算法使每个分区只能在自己的时间片内使用CPU及其他系统资源。另外，通过在SSK中定义最基本的安全策略和安全控制模型，以控制各分区之间所有信息和数据的安全交互，以达到对数据和信息流的绝对控制，实现故障隔离，即使某个客户OS出现安全状况或运行失效，都不会影响其他分区的安全和正确运行。SSK基本功能如下：(1) 时间、空间分离。(2) 分区调度；(3) 数据隔离。(4) 分区间信息流控制。(5) 分区间同步机制。(6) 共享资源空间清理。(7) 最小中断服务。(8) 时钟。

SSK仅提供最基本的安全机制，根据文献[11]的建议，SSK的安全机制应尽可能地简单，以此保障SSK的大小严格控制在5K以内，从而有可能通过较高的安全认证。

2.2.2　虚拟机技术

虚拟机技术使得一个OS可以运行于其他内核环境中，多个不同的OS共享单个硬件资源。虚拟机技术目前分为全虚拟机、半虚拟机两种类型。Hades架构在每个分离的区间中实现半虚拟机，运行于其中的客户操作系统需要做一定修改，而其应用程序则无需任何改动。Hades的隔离模式，可以方便地实现多个虚拟机，支持多个不同安全级别客户操作系统的运行。

2.2.3　“客户”OS

该架构允许任意多个嵌入式OS作为“客户”OS运行于SSK之上，并且每个“客户”OS运行在由虚拟机技术实现的分离的安全空间中。“客户”OS可以是任何嵌入式操作系统(如嵌入式Linux，Win CE等)，以此满足某些相对复杂的、异构的嵌入式应用需要。每个“客户”OS的硬件抽象层(HAL)将分离内核看作硬件环境，运行于“客户”OS之上的中间件和应用程序并不知下层基础软件情况。“客户”OS可以设立独立的安全策略和安全机制来保护该分区的安全，各分区应用程序之间的信息流控制由SSK和“客户”OS共同完成。

3　分区间信息流控制机制

在实现方式上，有些采用分离思想的系统要求分区间绝对分离，如IBM公司的PR/SM[12]系统。该方式只需简单地将机器划分成多个分区，并且绝对禁止分区间的信息共享，称为“纯数据分离”。其优势在于非常简单，易于实现，但在实际应用中无法满足复杂应用的需要。文献[13]中提出的分区间“安全共享”思想可解决分区间资源的共享问题，允许分区间可以共享和通信某些重要资源。

3.1　信息流控制框架

Hades安全架构采用的信息流控制机制(information flow control，IFC)只允许授权信息在分区间流通，并且分区间所有信息的通信都必须经过IFC的强制控制，使用BLP安全模型控制不同安全等级分区间的数据交互。IFC一方面可以防止由于低安全等级分区恶意篡改和读取高安全等级分区的信息而导致的高级安全数据的泄密和毁坏，另一方面可以防止未受权的“脏”数据对其他分区的污染。

IFC机制覆盖了Hades安全架构的所有层包括：

(1) 用户模式下的安全服务分区。

(2) “客户”OS中的安全代理模块。

(3) 特权模式中的访问控制模块(access control module，ACM)和BLP安全模型。如图3所示。通过IFC机制可以达到对分区间信息流的绝对控制和管理，以此实现重要信息在分区间的安全流通。

(1) 安全服务分区。

安全服务分区作为用户模式下最重要的安全保障模块，包含安全/防危(security/safety)验证器、分区安全信息表，安全/防危策略库等功能模块。当客

户OS要向其它分区发送/接收数据时，必须首先从分区安全信息表中获取源分区和目的分区的安全等级、可信度等信息。安全/防危验证器验证每个分区的可信度，并写入分区安全信息表中。安全/防危策略库存放用户层的安全策略，如强制访问控制、防火墙、加密等安全策略，可以根据实际需要扩充、裁剪该策略库。这种将策略与应用分离，并使用安全服务分区统一存放安全策略的方法便于策略的管理和维护。

(2) 安全代理。

在客户OS中设立安全代理控制、管理分区间所有信息流，该模块必须是一个可信赖的模块。例如，分区A向分区B中读取/发送数据，该操作请求首先由A中的安全代理接管，然后请求安全服务分区和SSK做出是否允许该请求的仲裁。一方面防止不可信信息发送到其它分区；另一方面禁止分区读取比自己安全级别更高的信息，以及向低级分区中写入信息。

(3) ACM和BLP。

为保障SSK能够通过较高安全级别的认证，在SSK中仅提供最基本的安全机制即访问控制模块ACM和BLP安全策略。当分区A向B发送消息时，A中的安全代理调用ACM做出是否允许该请求的决策。ACM仅使用最简单的BLP安全策略实施强制访问控制授权。

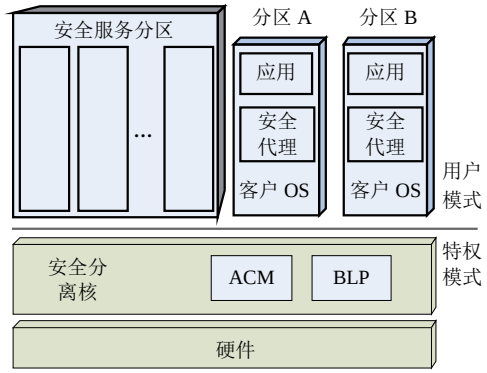

图3 分区间信息流控制机制

分区间所有信息的通信均被应用层的安全服务分区和安全代理所监控，其访问权限最终由SSK控制和授权。为使Hades架构能够获得较高安全级别的认证，安全机制应尽可能的简单、高效。

3.2 多层次的安全策略

Hades制定多层次的安全策略，特权模式中的SSK仅定义最基本的安全策略，用户模式的安全策略由专门的“安全服务”分区统一管理，并保留各“客户”OS原有的安全策略。Hades支持多级安全策略(MLS)，根据每个分区的安全特性为其指定相应的安全等级，各分区间的通信必须遵循相应的安全策略。首先定义SSK必须满足的4个基本安全策略。

1) 数据分离。一个分区中的信息不能被其他分区随意访问，保持私有数据的私密性，对于分区间重要信息的交互必须采用相应地措施进行严格的控制，防止各分区信息被破坏和窃取。

2) 信息流控制。信息在分区间的流动是受控的，没有任何的秘密通道，对于点到点的通信要求具有认证，并且要保证信息的完整性。信息流控制遵循以下3个策略：

(1) 只有授权信息才可以流动；

(2) 信息只能传送到指定的接受者；

(3) 信息源必须能够鉴别信息接受者的身份。

3) 共享资源清理。在分区上下文切换时必须对系统的共享资源进行空间清理，如在将A分区中使用过的共享资源(如共享内存、寄存器等)交于B分区使用前，出于安全考虑必须将这些共享资源清零。

4) 故障隔离。一个分区的故障不能够影响其他分区的运行，并且故障应能够被检测、记录、处理。

另外，用户模式中的安全策略形式多样，可以使用强制访问控制策略、防火墙、信息加密等多种安全策略。为便于安全策略的管理和扩展，所有应用程序公用的安全策略均存放于专门的安全服务分区中。为保障信息的安全流通，分区间的信息流控制非常重要。分区可信度的验证也至关重要，下面将阐述分区安全评估和认证方法。

4 可信评估和认证

可信计算的定义中明确指出[14]：从用户角度看，可信计算就是计算机系统所提供的服务是可信赖的，而且这种可信赖是可论证的。我国已将可信计算的验证和评估作为2008年可信重大研究计划的重点，由此可见可信评估和认证至关重要。为使Hades架构所提供的安全服务是可认证的，其核心模块SSK的行为以及应用层提供的安全服务都必须经过验证。

当前，有很多关于可信评估和认证的模型，它们解决了可信方面的若干具体问题。比较流行的模型有：

(1) 混合型模型[15]：包括可靠性块图，容错树、攻击树，用于可靠性评估和测量。

(2) 模型检测[16-17]方法：在可靠性和安全性的分析和建模方面经常使用。

(3) 基于状态的随机模型[15,18]：在硬件系统、实

时系统中使用马尔可夫模型、MRM模型(markov reward model)、随机Petri网进行可靠性分析和评估。在可信性其他属性评估方法方面，文献[19]提出使用随机技术评价安全、防危等可信属性。但这些方法均只解决了单个具体问题，未从整个系统的角度考虑可信的评估和认证。因此，文献[19]建议当前比较重要的工作是建立一个好的基于模型的框架量化系统的可信属性。

嵌入式安全关键系统的可信性验证和评估是一个重要问题，也是一个难题，我国当前还没有非常成熟的评估标准和完善的评价体系。Hades高可信架构支持分层认证，即不同安全关键层分开认证。安全关键层SSK必须通过较高等级认证，而其他非安全关键层通过较低安全等级认证即可，以此减少认证难度。Hades中设立安全、防危认证器专门验证和评估应用程序和分区的安全和防危能力。如何用形式化的方法建立可信性评价模型，并且如何量化和验证整个Hades架构的高可信能力，是以后要重点研究的问题。

5　结　论

本文提出了一种多层次的基于安全关键系统的高可信软件架构Hades，它支持多个独立安全级别的应用。该架构与传统安全核、防危核的不同之处在于其为基于MLS的嵌入式安全关键系统提供了一种整体解决方案，并同时提高了系统的安全、防危能力。采用“分离”思想、虚拟机技术、多层次的安全策略以及信息流控制机制为安全关键系统提供可信赖的安全服务。通过不同安全关键层分开认证的方法减少认证开销，使系统可以通过较高安全级别的认证。以后的工作将重点解决该架构的分区调度、可信性质的量化、可信的形式化验证和评估、应用层安全策略的设计。希望通过这些工作能够为国家研制具有出自主知识产权的嵌入式安全关键系统高可信软件架构，以解决目前非常紧迫的安全关键系统的高可信问题。

本文得到电子科技大学青年基金项目(L08010601JX05030、L08010601JX0752)的支持，在此表示感谢。

参　考　文　献

[1] KNIGHT J C. Safety critical systems: challenges and directions[C]//Proceeding of the 24th International Conference on Software Engineering. Florida: [s.n.], 2002.

[2] 陈火旺, 王　戟, 董　威. 高可信软件工程技术[J]. 电子学报, 2003, 31(12A): 1933-1938.
CHEN Huo-wang, WANG Ji, DONG Wei. High confidence software engineering technologies[J]. Chinese Journal of Electronics, 2003, 31(12A): 1933-1938.

[3] KARGER P A. THOMAS J. Multi-level security requirements for hypervisors[C]//Proceeding of IEEE ACSAC. Tucson, AZ, USA: IEEE Computer Society Press, 2005.

[4] AMES S R, GASSER M, SCHELL R R. Security kernel design and implementation: an introduction[J]. IEEE Computer, 16-7: 14-22.

[5] RUSHBY J. Kernels for safety?[C]//Safe and Secure Computing Systems Symposium. London: Blackwell Scientific Publications, 1989.

[6] SAILER R, JAEGER T, VALDEZ E, et al. Building a MAC-based security architecture for the xen open-source hypervisor[C]//Proceedings of the 21st Annual Computer Security Applications Conference. Washington D C, USA: [s.n.], 2005: 276-285.

[7] BARHAM P, DRAGOVIC B, FRASER K, et al. Neugebauer, I. Pratt, and A. War_eld. Xen and the Art of Virtualization[C]//Proceedings of the 19th ACM Symposium on Operating Systems Principles. New York: ACM Press, 2003: 164-177.

[8] ALVES F J, HARRISON W S, OMAN P, et al. The MILS architecture for high assurance embedded systems[J]. Journal of Embedded Systems, 2006, 2(3): 35-41.

[9] DoD Computer Security Center. Computer security requirements-guidance for applying the department of defense trusted computer system evaluation criteria in specific environments[EB/OL]. [1985-07-25]. http://www.radium. ncsc.mil/tpep/library/rainbow/index.html.

[10] RUSHBY J. Design and verification of secure systems [C]//Proceeding of the 8th ACM Symposium on Operating System Principles. [S.l.]: ACM Press, 1981: 12-21.

[11] SALTZER J, SCHROEDER M. The protection of information in computer systems[C]//Proceeding of the IEEE. Washington D C, USA: IEEE Press, 1975: 80-87.

[12] IBM Coporation. Certification report for processor resource/system manager (pr/sm) for the IBM eserver zseries 900[R]. 2003.

[13] MADNICK S E, DONOVAN J J. Application and analysis of the virtual machine approach to information system security[C]//Proceedings of the ACM SIGARCHSIGOPS Workshop on Virtual Computer Systems. Cambridge, MA: Association for Computing Machinery, 1973: 210-224.

[14] AVIZIENIS A , LAPRIE J C , RANDELL B , et al . Basic concepts and taxonomy of dependable and secure computing[J]. IEEE Transaction on Dependable and Secure Computing , 2004, 1(1): 11-33.

[15] TRIVEDI K S. Probability and statistics with reliability queuing, and computer science applications[M]. 2nd ed. New York: John Wiley and Sons, 2001: 105-110.

[16] BESSON F, JENSEN J, METAYER D L, et al. Model checking security properties of control flow graphs[J]. Journal of Computer Security, 2001, 9(3): 217-250.

(下转第1046页)