第 33 卷 第 6 期 计 算 机 工 程 2007 年 3 月
Vol.33 No.6 Computer Engineering March 2007
·博士论文· 文章编号：1000—3428(2007)06—0012—03 文献标识码：A 中图分类号：TP316

操作系统可信增强框架研究与实现

陈幼雷[1]，黄 强[2]，沈昌祥[2]
(1. 武汉大学计算机学院，武汉 430072；2. 海军计算技术研究所，北京 100036)

摘 要：操作系统安全增强技术是解决系统安全问题的有效手段，但无法保证系统基础可信。文章从分析可信和安全关系入手，提出可信增强概念。设计了操作系统可信增强框架，将可信机制和安全功能有机结合进安全体系结构设计中，并对实施和应用进行了研究。
关键词：安全增强；可信增强框架；可信机制；安全功能；可信计算体系结构

Design and Implementation of Trusted Enhanced Framework of Operating System

CHEN Youlei [1], HUANG Qiang [2], SHEN Changxiang [2]
(1. School of Computer, Wuhan University, Wuhan 430072; 2. Computing Technology Institute of China Navy, Beijing 100036)

【Abstract】 The traditional security enhanced technology based on operating system is usually the general solution to resolve the security problem, but can not guarantee base trust of the system. Starting with analysis of the relation between trust and security, this paper presents the concept of trusted enhancement and a trusted enhanced framework. It integrates the trusted mechanism and security capability into the design of security architecture. Then the enforcement and application of the framework is researched.
【Key words】 Security enhanced; Trusted enhanced framework; Trusted mechanism; Security capability; Trusted computing architecture

TCSEC[1]发布后，人们围绕操作系统安全进行了大量研究，而通常对现有系统进行安全增强的方式具有成本低，易于实现，可用性强等优点。操作系统安全增强是针对具体的安全目标，在内核中增加安全功能及策略实施部件，来提高系统安全性。比较有代表性的有LSM框架和SeLinux项目[2]。但传统安全增强手段往往忽视对系统自身安全性的保护，无法确保策略实施的正确性，比如安全功能可能被绕开或篡改。导致这种问题的原因在于构成系统基础的硬件平台和操作系统不可信。TCG提出的可信计算思想[3]认为，如果计算平台从一个初始“可信根”出发，在平台计算环境的每一次转换时，可信状态都可以通过传递的方式保持下去不被破坏，则平台才是可信的。构建可信根的核心部件是TPM[3]，它嵌入在平台上，为上层可信机制和安全功能提供硬件保障。可信计算从平台基础可信角度理解信息系统安全，和通常的安全含义是有区别的。本文从可信和安全的关系入手，分析其中联系，提出了操作系统可信增强概念，将安全增强技术纳入到可信增强框架中，在确保系统自身功能正确实施的同时为上层应用提供安全支撑，能够有效解决传统安全增强技术自身脆弱性的问题。可信增强框架还能满足TCB[1]的不可旁路和防篡改要求。

1 可信与安全的关系模型

TCG将可信定义为：一个实体能够按照期望的方式达到预定目标[3]。系统行为的可信可以从两个层次来理解：(1)系统的运行是正确的，运行正确性体现系统功能的正常合理；(2)运行结果合法，体现在系统各种操作流程没有违反整体安全策略。将前一层含义称为狭义可信，而包含两层含义的可信称为广义可信。安全则通常以一组安全目标来衡量，分为5个方面[4]：保密性，完整性，可用性，可记账性(Accountability)，保障性(Assurance)。保密性指系统信息或数据不能泄漏给非授权用户；完整性指防止非授权修改系统信息或数据；可用性确保系统正确工作和提供服务；可记账性保证系统行为能够被正确的跟踪和记录；保障性衡量系统安全机制能否正确实施。其中可用性和保障性可对应狭义可信概念。图1表述了两者间的联系。

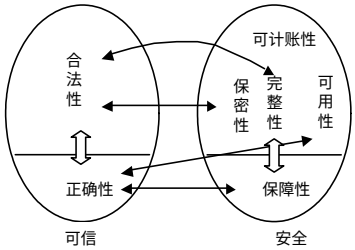

图 1 可信与安全定义间的联系

可见广义可信和安全是相通的。安全关注目标和结果，满足某种安全需求即是安全，是外部表现；而可信强调系统基础的正确性，是内在因素。但安全并不绝对，在实际系统中安全目标往往非常具体，是对系统应用环境安全需求的反映。广义可信中的合法性和系统总体安全策略相联系，它既包含系统自身需要遵循的基本安全原则，同时也包含系统所处应用环境所要满足的安全目标。因此广义可信中合法性随应用环境而变化，与系统自身可信无关。因此我们将基于狭义可信，对其内涵进行扩展，将可信和安全合理区别开，以此为基础建立可信与安全关系模型。

在实际系统中，所有实施安全策略的功能集合称为

基金项目：国家“863”计划基金资助项目(2002AA1Z2101)
作者简介：陈幼雷(1977－)，男，博士生，主研方向：信息安全；黄 强，博士生；沈昌祥，教授、博导、中国工程院院士
收稿日期：2006-03-21 **E-mail：**cylbaggio@263.net

TCB[1]。狭义可信则是保障TCB运行的正确性，它是安全功能正确实施的基础。可见可信是安全的充分条件，只有在可信前提下，才可能通向最终的安全目标。将可信机制定义为保障系统可信的软硬件功能集合。同安全功能一样，系统可信的基础也需要不同的可信机制来保证，它和安全功能相结合，才能达到系统整体安全目标。

图 2 给出了可信与安全关系的框架模型。可信处于安全下方，作为保障安全功能正确实施的基础。图中引入可信根概念，它是可信机制自身可信基础。可信机制和安全功能相辅相成，为处于顶层的安全目标服务。以可信根为基础，所有可信机制和安全功能共同构成 TCB。关系模型将可信机制纳入到系统安全基础架构中，相比 TCSEC 有所扩展。由此可将安全增强定义为针对具体安全目标，实施安全策略的功能集合，可信增强则是对安全功能实施正确性提供保障机制的集合。可信与安全关系模型是可信增强框架设计的基本思路。

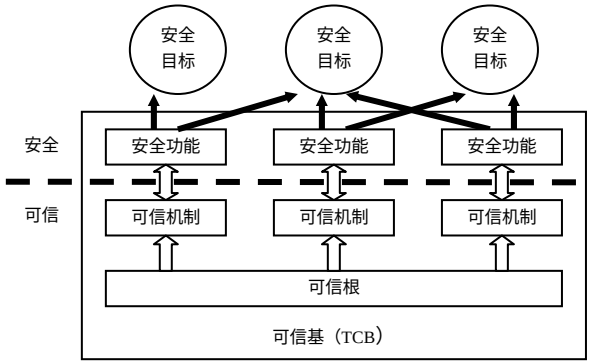

图 2 可信与安全关系模型

2 可信增强框架的设计

可信增强框架设计着重于从体系结构上将安全功能和可信机制结合起来，有效保障安全策略正确实施，确保系统基础可信和总体安全目标的实现。在操作系统内核安全增强基础上，我们将安全功能和可信机制分离开，并采用层次化方法构建可信增强框架。整个框架不仅包含操作系统部分，引入的可信根和可信引导机制作为框架的基础支撑部件而成为框架的重要组成部分。

2.1 体系结构

框架由 3 个主要部分构成：可信根作为硬件支撑基础，上层是可信机制，最上层是安全功能。图 3 采用层次化方法描述框架体系结构。

(1)可信根：为了确保平台基础硬件的可信，同时为上层提供支撑功能，框架中引入符合 TCG 定义的安全模块作为框架的可信基础部件。这种设计使框架能够充分兼容符合 TCG 规范的可信计算平台。

(2)可信机制：包括两个层次，底层是保障系统框架建立过程可信的可信引导机制，上层保障安全功能及安全策略正确实施的可信机制，在可信增强内核中实现。可将其分为可信验证、可信存储和可信报告。

1)可信引导：确保系统按照经过严格验证的路径进行引导。它对主引导记录、操作系统装载器、操作系统内核，系统配置信息进行验证，确保引导过程中各部件的完整性。其中，作为内核部分的可信机制和安全功能以及安全策略库均将被验证，保证可信增强框架被正确建立，没有被旁路或篡改。

2)可信验证：结合可信根中保存的预期值(预期值生成见应用模式一节)，对调用的可执行体或数据进行一致性验证。可信引导将控制权转移给可信增强内核后，内核模块或用户进程在调用可执行程序时都将利用可信验证机制对其进行验证，通过后才能调用。例如内核对启动的系统初始化进程进行验证，初始化进程再利用可信验证机制对重要的系统进程、服务脚本和可加载内核模块进行验证，所有验证通过后才能最终建立用户操作环境。

3)可信存储和可信报告：参考 TCG 规范设计，能够为内核安全功能和上层应用提供敏感信息的存储和获取系统当前环境状态等服务。其具体应用可结合安全功能和应用环境安全需求定义。

4)可信硬件驱动：处于可信机制底层，是访问可信根的唯一合法入口，确保可信根不能被非授权使用。

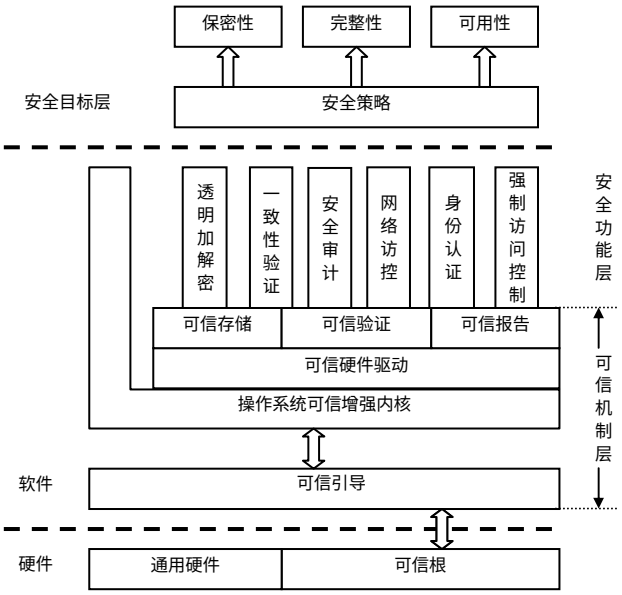

图 3 框架体系结构

(3)安全功能：安全功能实施安全策略，安全策略又为安全目标服务。具体应用环境对应不同的安全目标，但总体上可归纳为保密性、完整性和可用性，其中可用性也可部分由完整性和保密性体现，因此在框架中将重点针对前 2 个目标设计 6 种安全功能：透明加解密，一致性验证，安全审计，网络访控，强制访问控制，身份认证等。透明加解密可以满足自主保密性和离线保密性需求，确保用户实施自定义保密策略和数据的密文存储；一致性验证实现应用数据的完整性保护；而安全性要求高的应用可利用强制访问控制功能实现严格的访问控制策略。身份认证确保用户身份的合法性，是其它安全功能实施的基础和依据。安全审计功能确保操作的可追踪性，为安全监管和策略维护提供依据。网络访控是为满足互联网环境下的安全需求而定义的，确保用户合法地访问网络资源和限制恶意网站对终端的攻击行为。

2.2 框架实施

框架的实施采用传统安全增强技术，对现有操作系统内核进行改进。以通用硬件平台和 Linux-2.6.2 内核为基础实现了一个可信增强框架的原型。由于利用通用平台，不具备 TCG 定义的可信根，因此原型中采用在其它项目中开发的具备密码功能和保护存储机制的可信支撑模块作为可信根。限于篇幅，本节只重点阐述可信增强框架在内核的实施流程。

图 4 显示了实施流程，其中黑边框部件表示已通过可信引导机制和系统初始化过程的验证。在内核中，主要的安全功能流程插入到每一个和安全相关的系统调用中构成策略实施部件。它与安全策略无关，负责实时地截获系统核心事件并进行相应的处理，再分发给策略判定部件，从而在内核中

形成不可旁路的细粒度安全控制。可信机制则体现在具体安全功能实施过程中。

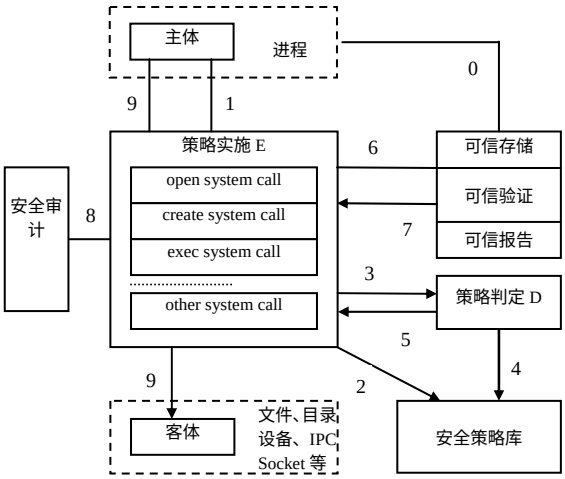

图 4 可信增强框架内核实施流程

下面以典型的主客体访问流程为例描述可信增强框架的实施流程。

(1)进程(主体)运行过程中发起系统调用，由此进入策略实施部件。

(2)策略实施部件 E 根据系统调用的类型从安全策略库中获取必要的系统参数，包括请求类型、调用进程的标识、访问对象标识等。

(3)将判定请求和参数传递给策略判定部件 D。

(4)根据参数从安全策略库中获取主客体安全属性和相应的安全规则。

(5)根据安全规则返回本次操作请求的判定结果。

(6)如果判定结果为允许访问，则根据具体访问的对象，激活可信机制，进入相应处理流程。在可信机制实施中涉及 3 种流程：

1)利用可信验证机制验证对象一致性，对于数据对象和可执行对象，均要检查其是否被篡改或破坏，并返回验证结果；

2)根据具体应用需求，利用可信存储机制保存敏感数据对象的完整性值或当前访问时刻系统环境状态值，可作为下次访问该对象的依据；

3)利用可信报告机制检查当前系统环境状态是否符合访问该对象的状态条件，如应用环境要求指定的程序或数据必须在当前系统软硬件环境处于某种状态下才允许执行和访问。除可信验证流程必须实施外，后两种处理流程可依据应用要求进行配置，属可选流程。

(7)可信机制返回处理结果。E 将根据结果作进一步处理，对于可信验证，如果一致性被破坏，则可查询并启用备份文件，否则将拒绝访问。对于可信报告，如果当前状态不符合访问要求，则拒绝访问。

(8)不论访问是否允许，均进行审计。

(9)主体获得访问授权，并实施对客体的访问。

内核实施流程的客体可以是文件、目录、设备、IPC 和 Socket 等对象，因此实施流程能够覆盖包括网络访控在内的所有安全功能。

3 应用模式

框架的应用必须和安全管理手段相结合。因此在框架实际应用中，引入管理中心概念，围绕目标系统安全策略，设计了包括策略的分析制定，配置发行，预处理和实施 4 个环节的应用模式。其简要流程如图 5 所示。

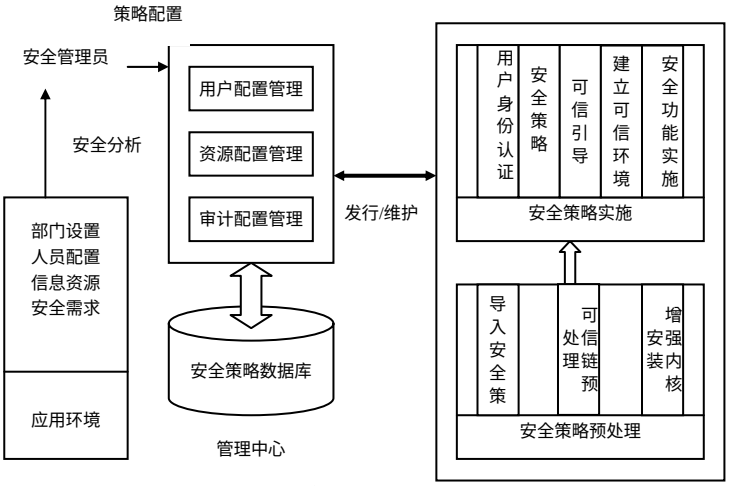

图 5 应用模式简化流程

(1)策略分析制定：由安全管理员利用专业知识，根据应用环境的部门划分、人员配置、角色职能、信息资源等各方面信息，进行综合分析，形成安全策略初步描述。在原型中，安全策略被划分为用户授权策略、资源访问策略(本地和网络资源)、审计管理策略、密码策略。其中密码策略是框架正确实施的技术保障。

(2)发行维护：利用管理工具将安全策略初步描述转化为策略实施机制能识别的数据结构，并最终形成安全策略数据库，由管理中心进行集中管理。管理中心是安全管理和密钥管理的集中体现[5]。在原型中，管理中心软件对安全策略进行配置及维护，并将安全策略网络化分发到各个应用处理终端。安全策略在实施过程中能够根据实际效果进行调整，并由管理中心对各应用终端进行安全策略的维护。

(3)预处理阶段：是可信增强框架在目标终端上建立和安全策略的导入过程。原型中，策略以密文导入目标终端，根据密钥策略对可信根设备进行密钥初始化。可信链预处理对系统各引导部件、系统内核、系统配置、服务脚本和可加载模块等生成完整性值(预期值，作为衡量可信性的一种方式，实体的可信度量通常采用评估标准和证书相结合的手段，但在实际环境中这种方式不易实现)。最后安装可信增强内核。

(4)安全策略实施：包括框架初始化和内核实施两个阶段。前一过程是策略实施的基础，包括用户身份认证，确保用户身份信息正确映射到安全策略中；可信引导，确保系统加电直到可信增强内核装载完毕各个环节的可信；策略初始化包括安全策略解密和导入内核空间；建立可信环境，确保系统初始化进程、系统服务、内核可加载模块及用户交互环境的可信。最后，内核态下的可信机制和安全功能将监控用户的操作，并根据策略库实施安全策略。整个实施过程中前一环节为下一环节服务，系统 TCB 逐层建立，并扩展到直接为应用服务的安全功能层。

4 结论

操作系统可信增强框架借鉴可信计算思想提出，明确分析并提出可信与安全的关系模型，作为框架设计的基础。它将安全功能和可信机制严格划分，提出了保障系统可信的基本可信机制，以及如何保障安全功能正确实施的运行原理，并将两者有机地结合到系统结构设计中。框架在实现上采用

(下转第 18 页)