



红旗 Asianux Server 3

安全技术白皮书

北京中科红旗软件技术有限公司
2007 年 10 月

目 录

文档说明3

引 言4

红旗Asianux Server 3 安全技术综述4

技术原理和实现.....5

技术特性6

 1. 遵照国家标准，参照国际标准进行开发 7

 2. 特权分离 7

 3. 保密性和完整性强制访问控制 7

 4. 角色访问控制(RBAC) 8

 5. 基于ACL的自主访问控制 8

 6. 网络访问控制..... 8

 7. 集中化安全管理 9

 8. 内核级审计跟踪和报表生成..... 9

 9. 预制安全策略.....10

 10. 模块化架构和自主防护10

 11. 良好的软硬件兼容性.....10

总结10

文档说明

本文档描述了红旗 Asianux Server 3 产品系列所涉及到的安全技术基础和实现。通过这些安全功能的部署使用，可以对服务器主机进行完备有效的系统保护。

本文档的主要内容：

- 引言

- 安全技术综述

- 技术原理和实现

- 技术特征

 - 遵循国家标准，参照国际标准开发

 - 特权分离

 - 保密性和完整性强制访问控制

 - 角色访问控制（RBAC）

 - 基于 ACL 的自主访问控制

 - 网络访问控制

 - 集中化安全管理

 - 内核级审计及报表生成

 - 预制安全策略

 - 模块化架构和自主保护

 - 良好的产品兼容性和高效性

引言

信息技术尤其是计算机网络已成为二十一世纪社会经济运行的必要条件,日益广泛的信息共享与互连使得信息安全成为迫切需要解决的问题。信息安全已经直接关系到一个国家的政治、军事和经济安全。

信息安全的主要要求是保护信息的保密性、完整性、可用性及抗抵赖性。对信息安全的威胁不仅仅来源于外部网络的攻击,也来自于内部有意无意的破坏或自然灾害等。建立信息安全体系是一个系统工程,需要从制度、人员、技术三方面入手。此外,一个好的安全体系不能只依靠单一的安全机制,而需要建立起一套纵深防御体系,多种安全机制共同作用,互相提供必要的冗余与备份,提供网络安全、主机安全和人员安全。

从计算机系统体系结构来看,一个完整的安全计算机系统需要解决物理层、操作系统层、网络协议层、数据库、中间件和应用层各个层次的安全问题。由于操作系统是整个软件系统的基础,操作系统安全就成为了整个软件安全体系的基础。缺乏操作系统的安全保护,网络到应用的安全将成为“沙滩上的堡垒”,失去了根基。

秉承多年来对系统安全的研发成果,2001年以来红旗软件陆续推出了安全 Linux 服务器产品 Red Flag Secure OS、RedFlag Advanced Server 4.1 SE 以及 RFGuard 安全套件。2007年红旗软件将系统安全技术直接集成到最新发布的服务器产品红旗 Asianux Server 3 上,使得 Asianux 系列服务器产品的安全性得到了很大的提升。

全新的红旗 Asianux Server 3 服务器面向企业的网络服务器的安全需求,严格遵循中国国家标准 GB17859-1999 第三级(等同于 TCSEC B1 级)的要求,并参照国际权威安全评估标准 CC 开发。集成的安全特性不仅能够防范来自外部网络的入侵攻击,更能够建立内部主机安全管理的策略和机制。通过在 Linux 内核层实现了经典的安全策略和访问控制,包括最小化特权、自主访问控制、强制访问控制、角色访问控制、内核级审计跟踪,以及对各种不同应用服务的良好支持和保护,能够满足政府、军队、电力、银行、证券、涉密机关,以及企业电子商务对操作系统安全的需要。

红旗Asianux Server 3 安全技术综述

红旗 Asianux Server 3 产品遵照国家标准 GB17859-1999 和行业标准 GA/T 390-2002,参照国家推荐标准 GB/T18336-2001 和国际权威标准 ISO/IEC 15408(CC)标准要求,基于 Linux 最新 2.6 内核开发的商品化安全操作系统。新产品结合国内信息安全市场需求,在实现 GB17859 全部三级和部分四级功能,增加了若干实用的安全功能,并在安全操作系统实现方法上有重要创新。除提供了基于 BLP 模型的保密性和完整性强制访问控制外,还提供了业内先进的角色访问控制,以及基于 ACL(访问控制列表)的丰富多样的自主保护机制,如细粒度的客体保护、命令执行和 Setuid 受限、限制 Kill 进程等等。此外,还提供诸如细粒度的网络访问控制和审计信息检索和分析手段,是国内目前提供访问控制手段最多、部署易用性和管理集中化上最为实用的商用安全操作系统。

新产品通过将安全核心进行模块化架构,在保持安全核心与标准 Linux 核心相互独立的同时,也继承和保持了原有 Linux 内核良好的性能和软硬件兼容性。在安全核心的实现上,通过采用通用访问控制框架设计,将安全决策和决策实施进行分离,从而可以灵活的支持多

种访问控制机制，保证了安全核心对于访问控制的良好扩展性。

此外，新产品在性能、分布式管理、易用性、应用环境适应性方面进行了大量优化和改进，使之符合企业级大规模应用的要求。同时，针对网络环境中的各种威胁，将安全操作系统与应用层安全方案相结合，提供从操作系统层到应用层的完整安全解决方案。

技术原理和实现

红旗 Asianux Server 3 的安全技术架构可以用图 1 来表示。可以看到，红旗 Asianux Server 3 上运行的安全组件由四部分组成。最底层是以内核模块形式存在的安全核心，提供各种访问控制模型的决策实现以决策信息流控制。再向上是同样运行在核心态的额外提供的安全系统调用，以及作为访问控制决策后信息流执行的决策实施模块，该模块实际是通过修改标准 Linux 系统调用形式存在的。此外，运行在核心态的模块还有实现网络访问控制必须调用的主机防火墙的核心实现。在上述核心态组件之上是运行在应用层的两大模块，分别是完成本地安全节点必需的系统管理、身份认证、审计管理及系统监控用代理程序管理的安全管理接口，以及完成分布式多节点的集中化安全管理的全局管理控制台。

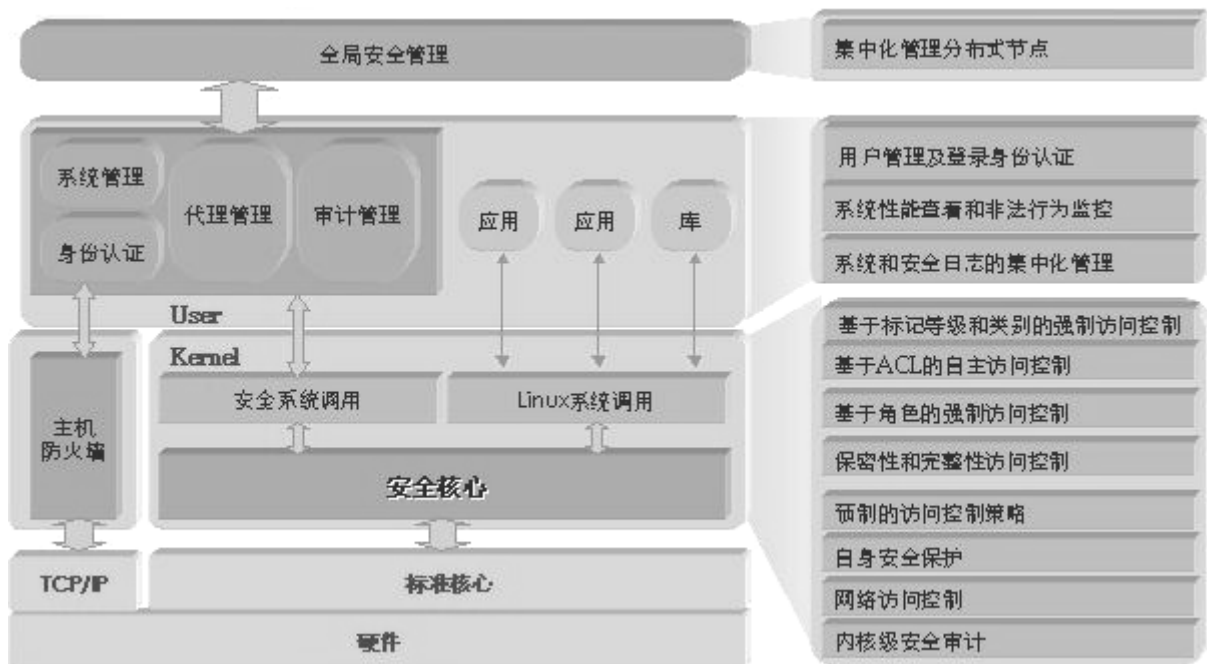


图 1 安全技术架构图

具体到安全核心实现上，红旗 Asianux Server 3 把安全内核分为安全决策和决策实施两个部分，安全决策是多种访问控制模型的综合实现，负责判断一个安全相关行为是否可以执行，安全决策内部设立平行独立的安全政策支持机制，每个安全政策对应一种访问控制模型，这样做的目的是希望在访问控制模型的支持方面获得一定的灵活性。决策实施与安全政策无关，负责执行一个已经得到许可的行为所要执行的任务。系统通过修改核心中与安全相关的系统调用，在具体操作执行前请求安全决策，根据决策结果决定是否允许实施操作。这样，安全决策模块与决策实施模块结合，构成了一个强大的安全内核。

图 2 是红旗 Asianux Server 3 所采用的访问控制体系结构图。从图中可以看出访问控制决策与实施的流程。

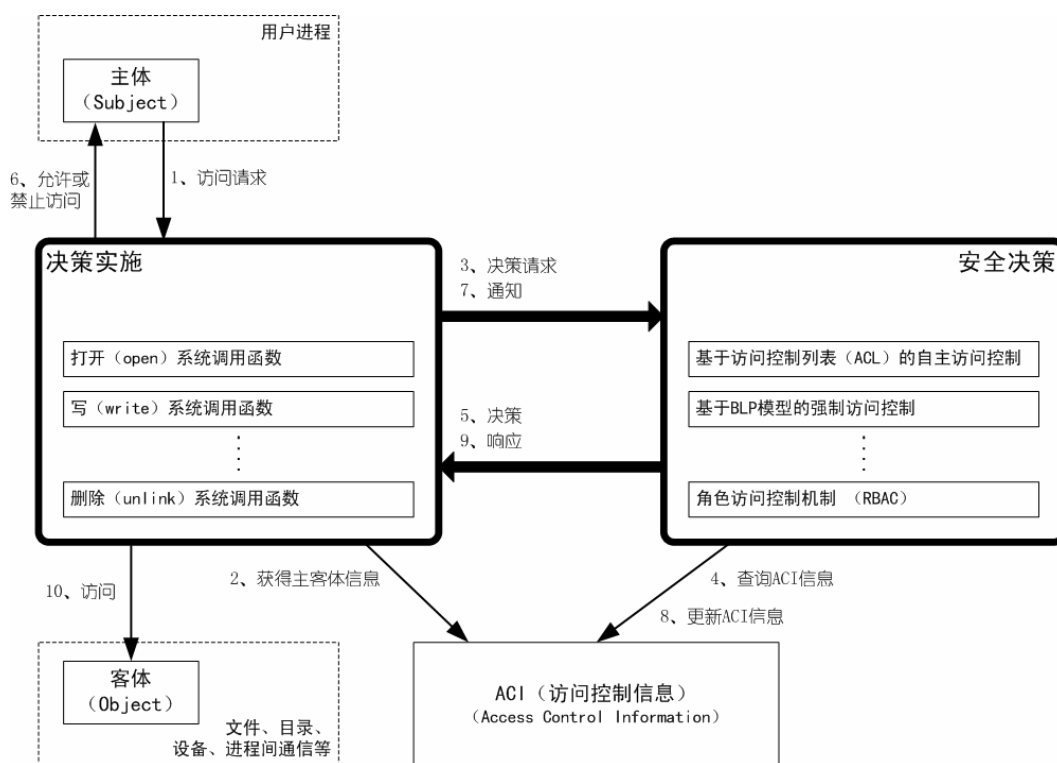


图2 访问控制体系结构图

当一个主体访问客体时，相关系统调用会触发安全决策机制。安全决策机制首先根据安全请求的类型确定应采用的安全政策，再把决策任务转交给对应的政策支持机制，最后将决策结果返回给决策实施机制去执行。从内核的角度看，安全相关行为是由系统调用触发的。以 `open` 系统调用打开文件为例，这是个安全相关行为，首先决策实施模块把打开文件的请求提交给安全决策子系统，决策系统受理这个请求，并由相应的政策支持机制作出判断。决策结果返回给决策实施部分，决策实施部分根据决策结果实施相应动作，并将结果信息返回给 `open` 系统调用。 `open` 系统调用根据这个安全决策结果确定下一步的行为。

技术特性

红旗 Asianux Server 3 具有如下技术特性：

- ☐ 遵循国家标准，参照国际标准开发
- ☐ 特权分离
- ☐ 保密性和完整性强制访问控制
- ☐ 角色访问控制（RBAC）
- ☐ 基于 ACL 的自主访问控制
- ☐ 网络访问控制
- ☐ 集中化安全管理
- ☐ 内核级审计及报表生成
- ☐ 预制安全策略
- ☐ 模块化架构和自主保护
- ☐ 良好硬软件兼容性

下面，逐条介绍这些技术特性：

1. 遵照国家标准，参照国际标准进行开发

秉承红旗安全操作系统产品研发成果和认证优势，红旗 Asianux Server 3 遵照国家标准 GB17859-1999《计算机信息系统安全保护等级划分准则》所规定的内容，通过引入安全等级、安全分组等安全标记，以 BLP 模型作为强制访问控制框架，实现了全部安全标记保护级(第 3 级)和部分结构化保护级(第 4 级)所要求的等级保护功能。其次，鉴于 CC 标准(Information Technology Security Evaluation Common Criteria)已于 1999 年 7 月通过国际标准化组织认可，确立为国际标准 ISO/IEC 15408，并在 2001 年采纳为我国国家推荐标准 GB/T18336-2001。红旗在安全产品研发阶段就注意参照 CC 标准 EAL4 级要求进行了满足性实现。CC 标准对安全的内容和级别给予了更完整的规范，为用户对安全需求的选取和表达提供了更灵活和规范的手段，更有利于应对层出不穷的新的安全问题，已经得到了越来越多的技术先进国家的支持。

秉承红旗软件在安全认证方面的技术积累，和 Asianux 的联盟优势，红旗 Asianux Server 3 已于 08 年 4 月顺利通过 CC EAL4 认证，成为目前亚洲首个通过国际 CC 标准 EAL4 认证的安全 Linux 系统。

2. 特权分离

普通 Linux/Unix 的用户特权划分只有两级，超级用户和普通用户。超级用户具有所有的特权，普通用户没有特权。这种做法不符合安全系统的“最小特权”原则。攻击者只要获得超级用户身份，便得到了对整个系统的完全控制，其后果是不言而喻的。

红旗 Asianux Server 3 根据“最小特权”原则对超级用户的特权进行了化分，在日常系统管理员角色之外单设了安全管理员角色。系统管理员负责系统的安装、管理和日常维护，如安装软件、增添用户帐号、数据备份等。安全管理员负责安全策略的制定和执行，安全属性的设定、安全审计等职责。传统的超级用户(Root)与其它标准用户一样，操作行为将受到安全管理员部署的所有安全策略的制约。即使由于人为管理疏忽使得非法用户获得 Root 权限，其操作行为仍受限于安全策略限制并被实时审计。

3. 保密性和完整性强制访问控制

强制访问控制是指对客体访问的安全政策是由系统强制实施的，客体属主无权控制客体的访问权限。红旗 Asianux Server 3 通过改进的 BLP 模型实现了保密性访问控制和完整性访问控制，以阻止信息的非法访问，和防止涉密信息被非法篡改。

BLP (Bell—LaPadula) 模型是公认的信息安全模型，自产生以来在很多安全操作系统的开发中得到了应用。

红旗 Asianux Server 3 开发了易用的配置管理工具和配置模板，增加强制访问控制的易管理性，并简化了实现，提高了部署的实用性。

4. 角色访问控制(RBAC)

RBAC 是红旗 Asianux Server 3 的重要新增功能，角色访问控制由于更为贴近现实世界的权限分配机制易于完成安全策略部署而成为目前国际安全领域的热点之一。红旗 Asianux Server 3 实现了基于角色的访问控制并提供了集成化的配置管理工具，管理员可以通过配置管理工具设置合适的角色及权限，按‘最小特权’原则分配和限制用户权限，从而灵活有效的控制主体对客体的访问。

5. 基于ACL的自主访问控制

红旗 Asianux Server 3 通过访问控制列表（ACL）机制细化了对系统资源的访问控制粒度，可以实现系统中任一用户（组、角色）对各种系统资源（目录，文件，特殊文件等）的控制访问。

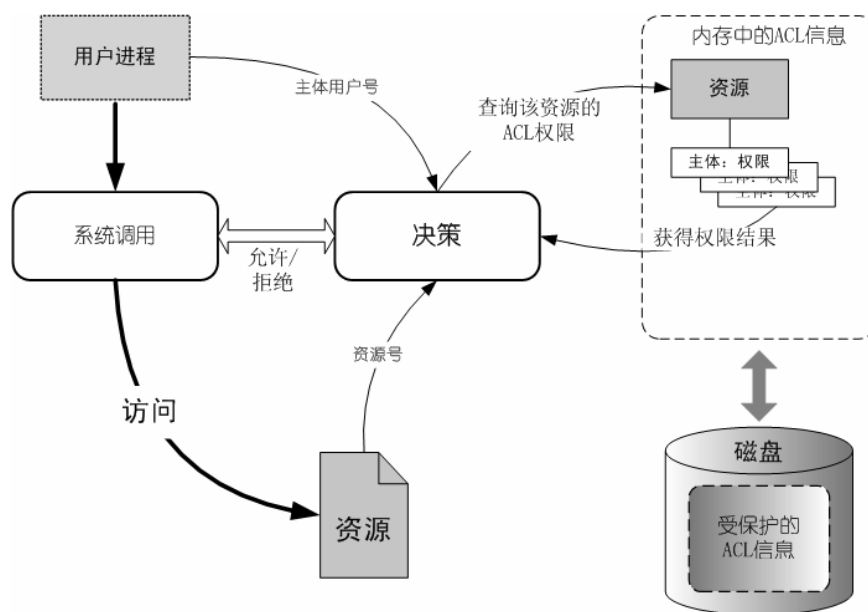


图3 自主访问控制结构和流程

除了提供上述标准客体的 ACL 保护外，红旗 Asianux Server 3 中的自主访问控制还提供了对于 Linux 安全敏感资源的 ACL 控制，如限制命令和 Setuid 程序的执行，以及阻止进程被 Kill 等等。

6. 网络访问控制

网络访问控制是新产品的一大增强性特色。红旗 Asianux Server 3 不仅提供了基于 IP、端口的主机包过滤型防火墙，还在传统安全访问控制规则中引入 IP 域，可以实现仅通过授权 IP 登录安全系统并拥有指定安全属性的用户方能访问授权涉密文件的更细粒度的访问控制规则。此外，红旗 Asianux Server 3 通过提供增强性 PAM 认证手段，可以限制在授权 IP 和端口范围，以及限制时间段内，通过指定的限制接入服务程序，以指定安全属性的用户身份登录安全系统，从而使得身份验证控制得到了细粒度强化。

7. 集中化安全管理

集中化安全管理也是红旗 Asianux Server 3 新增的一大管理新特性。新产品不仅提供了直观易用的管理控制台，而且将该管理控制台从管理单个主机安全节点拓展到全网管理，可以管理 200 个以上的分布式安全节点。这样，安全管理员不必象以前一样，需要分别在各个主机控制台上完成安全属性设置、安全策略部署和关注审计信息，而只需通过一个全网唯一的管理控制台集中管理所有分布式节点，进而有助于从整体上把握全网安全状况。

8. 内核级审计跟踪和报表生成

红旗 Asianux Server 3 进一步增强了审计功能，优化审计性能，重新设计和实现审计管理工具，增强对审计数据的保护，提供灵活的审计记录检索和查看功能。为事故发生前的预测、报警以及事故发生后事故原因的查询、定位、追踪提供详细、可靠的依据和支持。

发生可审计事件的代码段称为审计点。审计点很多，但都可以划分到核心层和用户层两个层次中。因为用户的应用程序都是通过系统调用获得操作系统服务的，所以可以在系统调用中截获大部分审计事件。对于发生在用户层的涉及系统安全的事件，则需要修改相应的应用程序才能截获。

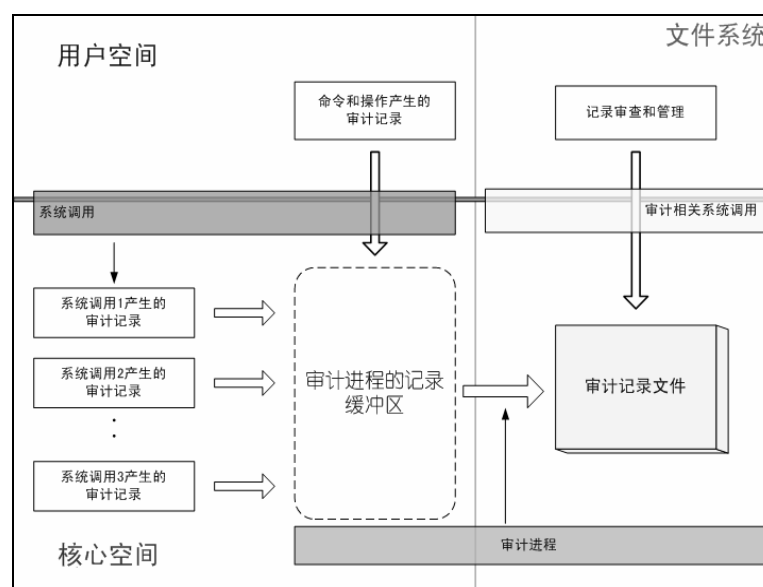


图4 审计跟踪技术结构图

审计数据在系统中应得到严格的保护，防止非授权查看，更要防止数据的篡改和删除。红旗 Asianux Server 3 中由核心对审计配置文件、审计数据文件实施相应的角色访问控制，以保证只有安全管理员才能访问它们。

鉴于审计数据的重要性，为了最大限度地挖掘审计信息的价值，把握系统的安全状况，红旗 Asianux Server 3 从统计分析的角度提供了详尽的安全分析报表，从而增强了审计信息的可用性。

9. 预制安全策略

为了保证系统的基础安全，以及为用户提过简单明了的安全策略配置模板，红旗 Asianux Server 3 提供了预制的的安全策略配置模板，对系统命令、配置文件和核心目录进行了完整性保护，并阻止了/tmp 目录下文件的可执行权限。

此外，Asianux Server 3 还提供了简单直观的策略编辑器，安全管理员可以通过向导式方式完成策略规则的直观定义和部署。

10. 模块化架构和自主防护

为了保证安全核心与 Linux 核心的相对独立，增强系统的可维护性和稳定性，保留通用 Linux 内核的稳定性和兼容性，红旗 Asianux Server 3 中的安全核心采用 Linux 内核模块方式实现，只有安全管理员可以控制安全核心的加载和配置，系统管理员无法对安全核心进行操作。

11. 良好的硬软件兼容性

红旗 Asianux Server 3 依托多年来红旗软件与国内外各硬件厂商的良好合作关系，对主流的服务器硬件平台和配件都进行严格的兼容性和高负荷压力测试，以保证产品的硬件兼容性。

同时，红旗 Linux 在软件兼容性上处于国内外 Linux 操作系统前列，对各种大型商业软件都能良好地支持，红旗与 Intel、Oracle、HP、IBM、Sybase、CA 等国际知名企业保持长期的合作关系，对相互的新产品都会进行测试和认证，以确保双方的产品在到达用户现场之前就能够良好地运行在一起。

总结

从上述红旗 Asianux Server 3 所提供的安全特性来看，产品不但完全达到了 GB17859-1999 第三级和 CC 标准相应等级所要求的功能，而且实现了目前国际前沿的安全操作系统技术，提供了丰富实用的安全特性和简单易用的配置工具。通过合理的应用这些安全特性，可以形成对企业各种网络服务器完整强大的主机安全保护方案。红旗 Asianux Server 3 保持并强化了在国内商业化安全操作系统产品的市场领先地位，从操作系统底层对用户的应用与敏感数据实施强大的保护。另外，它与网络防火墙，入侵监测，病毒网关等网络安全产品互为补充，可以形成多层次，纵深防御的安全体系架构。

北京中科红旗软件技术有限公司

电话：8610-82656655

传真：8610-82658096

网址：<http://www.redflag-linux.com>

地址：中国北京海淀区万泉河路 68 号紫金大厦 6 层

邮编：100086

本材料最终解释权归北京中科红旗软件技术有限公司所有