基于Linux开发安全操作系统的研究*)

Research of the Design for a Secure Operating System Based on Linux

刘文清　刘海峰　卿斯汉

(中国科学院信息安全技术工程研究中心　北京100080)

Abstract　The operating system security is the necessary condition of the software security. Designing a secure operating system is very important and necessary. Linux is a free operating system and the computer circles commonly know that it will have more and more application. So that, designing a secure operating system based on linux is imperative. This paper discusses its feasibility and analyzes the method and the process of designing and something that we have need to pay more attionation in the course of designing.

Keywords　Secure operating system, Linux, Design

1　引言

当前信息安全的问题已经引起人们的广泛关注，随着防火墙、网络保密机、网络安全服务器、安全管理中心等网络安全产品的研制和使用，人们不禁提出这样的问题：它们的"底座"(操作系统)可靠坚固吗？"

操作系统是计算机资源的直接管理者，所有应用软件都是基于操作系统来运行的，没有操作系统的安全，是不可能真正解决数据库安全、网络安全和其它应用软件安全问题的。操作系统的安全是计算机系统安全的基础，开发安全的操作系统，成了提高计算机信息系统安全性的重要手段，所以我们应对操作系统本身的安全性予以高度的重视。

现在应用最广泛的Windows系列操作系统在安全性方面漏洞很多，已发现在Win95和Win98中都存在着"后门"，由于Windows操作系统不提供源码，象一个"黑盒子"，对它的安全性难以估量和增强，我们国家的政府、经济、军队等重要部门迫切需要自主开发的安全操作系统做平台。近几年来，Linux蓬勃发展，其开放源代码和遵守GPL协议给我们基于其自主开发安全操作系统提供了历史的机遇：

1)克服了以往国内基于其它操作系统开发安全操作系统缺少核心源程序的困难，使得我们可以对Linux内核进行安全性增强和开发所需的各种安全机制，并且能够有序地进行和说明这些安全机制的完备性，从而使得基于Linux资源自主开发高安全级别的操作系统成为现实和可行。

2)克服了以往国内自主开发安全操作系统存在的版权问题。

2　Linux操作系统支持安全性开发

操作系统安全的目标主要是保证其自身的系统安全性和完整性；按安全策略对用户在系统中的操作进行存取控制，防止用户对计算机资源中信息的非法存取(窃取、篡改和破坏)；监督系统运行的安全性。操作系统的安全功能主要包括：

·用户标识和身份鉴别：如用户登录时的口令机构等；

·存取控制：对用户对系统中信息的访问请求进行面向安全策略的存取控制；

·审计：监视、记录和处理系统中有关安全性事件的活动。

显然，我们基于Linux开发安全操作系统也必须达到这些目标和实现这些安全功能。

2.1　Linux的现有安全性

Linux的现有版本无需任何修改，就基本符合美国国防部橘皮书《可信任计算机系统评价准则(TCSEC)》的C1级条款。它主要有以下安全特性：

·系统中的每个文件和目录都具有不同于其它文件和目录的唯一标识符，系统中的每个用户也都有一个可相互区分的标识符。

·用户必须通过注册名和口令经系统识别无误后，才可登录系统。没有合法用户的口令，非法用户将无法

*)本文受中国科学院重大科研项目基金资助。刘文清　博士生，研究领域为操作系统安全、网络安全。刘海峰　博士生，研究领域为操作系统安全。卿斯汉　研究员、博士导师，研究领域为信息系统安全。

进入系统。

·系统具有一定的自主型存取控制(DAC)安全机制，即"owner/group/other"存取控制机制。用户对系统中的文件和目录拥有相应的许可权限，系统能够控制其访问哪些程序或信息以及如何访问。

·Linux 系统内核在一个物理上的安全域中运行，这个域受到硬件的保护。安全域保护着在它内部的核心和安全机制，安全机制本身是无法绕过的。

2.2 Linux 支持存取控制机制开发

在安全系统中，只有授权用户才可以操作相应的信息资源，也就是说，系统要实现完备的信息存取控制机制。即：

1)必须有一个明确的、定义良好的安全策略，并且该安全策略要求实现于系统中。它表现为一组存取控制规则，用来确定主客体之间的存取关系。存取控制体现在两方面：自主存取控制和强制存取控制。

2)对系统中的文件或目录要给予敏感级标识，对系统中的用户也要给予敏感级标识。

3)对与系统安全有关的事件要进行审计，并且事后能找到当事人。

4)要有一套机制(软件或硬件)来实现上述功能，这些机制嵌入在操作系统中。机制的实现要有清晰的文档，可以用来评价或说明这些机制的完备性和与安全策略一致性。

可见，存取控制机制是实现操作系统安全性的关键，要基于 Linux 开发安全操作系统，则其体系结构必须适合存取控制机制的开发。

Linux 同 UNIX 一样，系统运行态分用户态和核心态两种，运行内核中程序的进程处于核心态，运行核外程序的进程处于用户态，系统保证用户态下的进程只能存取它自己的指令和数据，而不能存取内核和其它进程的指令和数据，并且保证特权指令只能在核心态执行，象所有的 I/O 指令等在用户态下不能使用。用户程序只能通过系统调陷入核心才能存取系统资源，运行完系统调用，又返回用户态。系统调用是用户在编写程序时可以使用的界面，是用户程序进入 Linux 内核的唯一入口。一旦用户程序通过系统调用进入内核，便完全与用户隔离，从而使内核中的程序可对用户的存取请求进行不受用户干扰的访问控制。因此，Linux 支持存取控制机制的开发，从而支持安全性的开发。

系统的安全性不依赖于系统设计的保密，而是通过系统中的安全机制来实现的，所以 Linux 开放源码不影响其安全性开发。

3 基于 Linux 资源开发安全操作系统的方法

如图1所示，在一个现有的非安全操作系统(ISOS)基础上开发安全性，一般有以下三种方法：

(1)虚拟机法：在现有操作系统与硬件之间增加一个新的分层，作为安全内核，操作系统几乎不变地作为虚拟机。安全内核的接口几乎与原有硬件等价，操作系统本身并未意识到已被安全内核控制，仍象在裸机上一样执行它自己的多进程和内存管理功能，因此，它可以不变地支持现有的应用程序，且能很好地兼容 ISOS 的将来版本。但是，采用虚拟机法开发操作系统的安全性时，硬件特性对虚拟机的实现非常关键，它要求原系统的硬件和结构都要支持虚拟机。因此，用这种方法开发安全操作系统的局限性很大。

(2)改进/增强法：在现有操作系统的基础上，对其内核和应用程序进行面向安全策略的分析，然后加入安全机制，经改造、开发后的安全系统基本上保持了原 ISOS 的用户接口界面。

由于改进/增强法是在现有系统的基础上开发增强安全性的，受其体系结构和现有应用程序的限制，所以很难达到很高(如 TCSEC 的 B3级以上)的安全级别。但这种方法不破坏原系统的体系结构，开发代价小，且能很好地保持原 ISOS 的用户接口界面和系统效率。

(3)仿真法：对现有操作系统的内核做面向安全策略的修改，然后在安全内核与原 ISOS 用户接口界面中间，再编写一层仿真程序。这样，在建立安全内核时，可以不必受现有应用程序的限制，且可以完全自由地定义 ISOS 仿真程序与安全内核之间的接口。但采用这种方法要同时设计仿真程序和安全内核，还要受顶层 ISOS 接口的限制。另外，根据安全策略，有些 ISOS 的接口功能不安全，从而不能仿真，有些接口功能尽管安全，但仿真实现特别困难。

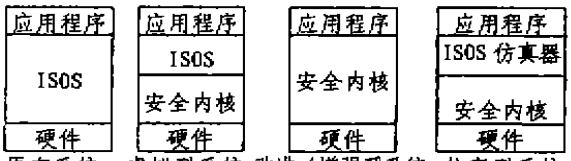

图1 安全操作系统开发方法

由前面分析可知，Linux 同 UNIX 一样，系统运行态分用户态和核心态两种，用户程序只能通过系统调陷入核心才能存取系统资源(文件、目录、设备等)。因此，对 Linux 的安全性开发可以采用改进/增强法，即以系统调用为基元，引入可信任计算基(TCB)机制，分别在系统调用中实施安全强制存取控制机制(MAC)和自主存取控制机制(DAC)，另外开发审计机制、最小特权管理机制、可信通路机制并进行隐通道分析处

理等。

设计和开发安全操作系统的主要目的是安全性，但安全性的建立必须与系统其它方面的需求求得平衡，在达到安全目标的前提下、不应过份地影响其它特性。采用改进/增强法开发 Linux 的安全性时，由于原有的系统调用的用户接口界面保持不变，所以，安全性的开发一般不影响 Linux 系统的兼容性。另外、在保证系统安全性的前提下，系统效率也要充分考虑、比如，审计机制要可以灵活地设置审计事件标准、可以随时开启和关闭审计操作、DAC 和 MAC 等都充分使用了内存缓冲区，尽可能地减少其与磁盘打交道的次数、等等，使得安全性开发对 Linux 效率的影响降到最低。

4 基于 Linux 资源开发安全操作系统的过程

基于 Linux 资源开发安全操作系统，要经过三个阶段，如图2所示。

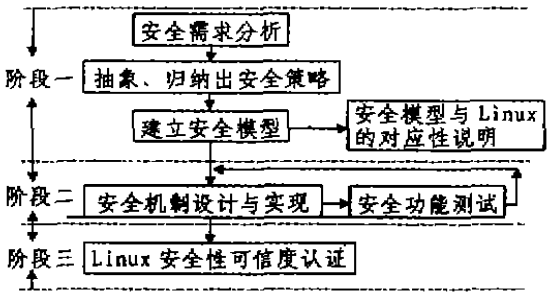

图2 Linux 安全性的开发步骤

(1)建立一个安全模型 在一个现有 Linux 资源上开发安全性之前，必须进行安全需求分析，根据面临的风险、需要的安全性和其它可行性因素，如经济的承担能力等，及基于的 Linux 操作系统版本，给出哪些安全功能是原系统已具有的，哪些安全功能是要开发的。明确了安全需求，才能给出相应的安全策略。计算机安全模型是实现策略的机制，建立安全模型有利于正确地评价模型与实际系统间的对应关系，帮助我们尽可能精确描述系统功能，以堵住所有的安全漏洞。非形式化安全模型仅需模拟系统的安全功能；形式化安全模型要使用数学语言，精确地描述安全性及其在系统中的情况。

建立安全模型后，就要进行模型与 Linux 系统的对应性分析，然后考虑如何将模型用于 Linux 系统安全性开发之中，并且说明所建模型与安全策略二者是一致的。

(2)安全机制的设计与实现 有了安全模型、就要选择一种实现该模型的方法，结合 Linux 的特点和将来的发展，可以采取改进/增强法、使得开发成的安全 Linux 系统具有最佳安全/开发代价之比。

逐步建立安全模型所要求的安全存取机制、同时在设计了一部分安全功能之后，便检查它所提供的安全性尺度。

在开发安全机制时，要注意在安全机制的完备性、与原系统的兼容性及系统的效率等方面需要做出平衡，

(3)安全操作系统的可信度认证 要证明一个系统的安全性是与设计密切相关的，必须保证从设计者到用户都相信设计准确地表达了模型，而代码准确地表达了设计。一般说来，表征操作系统安全性的方法有三种：形式化验证、非形式化确认和入侵分析。这些方法可以独立使用，也可以将它们综合起来评估所开发的 Linux 安全机制的可信性。

结束语 操作系统的发展趋势表明，未来的操作系统将是 Windows 和 Linux 之争。据 IDC 预测、在五年后 Linux 将跃居操作系统的第二位。今天，我们重新提出了发展我国自主操作系统的口号就是因为出现了 Linux，它源代码公开，且已被实践证明是高性能、稳定可靠的操作系统，特别是1998年以来，它已得到世界上许多大软件公司的支持，从而拥有了大量应用软件的支持，确实具备了挑战 Windows 的条件。因此，基于 Linux 的安全操作系统将会具有巨大的市场潜力和很广阔的应用需求。

参 考 文 献

1 Trusted Computer System Evaluation Criteria Department of Defance U. S. A. 1985. DoD 5200. 28-STD
2 Mayer F L. An Interpretation of a Refined Bell-La-Padula Model For the Mach Kernel. 1988
3 Bach M J. The Design of the UNIX Operating System. Prentice-Hall, Inc. 1986
4 Managing Security on the Trusted DG/UX™ System. AVLLON PRODUCT LINE. 1994
5 莫瑞·加瑟著，吴亚非，等译. 计算机安全的技术与方法. 电子工业出版社、1992