<<信息安全技术解析与开发实践>>

图书基本信息

书名：<<信息安全技术解析与开发实践>>

13位ISBN编号：9787302255680

10位ISBN编号：7302255687

出版时间：2011-7

出版时间：清华大学

作者：訾小超//薛质//姚立红//蒋兴浩//潘理

页数：292

<<信息安全技术解析与开发实践>>

内容概要

《信息安全技术解析与开发实践》以信息安全技术开发实践为目标导向，围绕如何开发相应的信息安全原型系统编写，书中详细阐述了linux内核级安全、网络防火墙、安全脆弱性检测，以及攻击检测这四类典型信息安全技术的实现解析和开发过程。
本书分为上下两篇，上篇为技术解析篇，重点介绍这四类信息安全技术的基本概念和原理，并对进行相关信息安全技术开发实践所需要的关键方法和技术措施做了详细的探讨；下篇为开发实践篇，以实例方式阐述如何实现信息安全技术和原型系统的开发实践，本篇共十章，每章阐述一个信息安全相关原型系统的具体开发过程。

《信息安全技术解析与开发实践》可作为高等院校信息安全、计算机科学与应用等专业的高年级本科生或研究生信息安全技术开发实践或课程设计的教材，也可作为相关信息安全技术原理类课程的参考书。
本书以实例的形式展示了十几种操作系统和网络相关的常用开发技术，本书也适合从事相关软件开发的工程师和技术人员参阅。

<<信息安全技术解析与开发实践>>

书籍目录

章节摘录

版权页：插图：本扩展开发实践的开发目标与A3“基于LSM的网络连接控制系统”基本相同，即对各种网络连接和通信操作进行控制，实现类似于windows系统中个人防火墙的大致功能。
与A3中扩展开发实践不同的是，本扩展开发实践在实现网络连接控制时采用的是系统调用重载方式，而不是设置LSM钩子函数。
本扩展开发实践的具体目标和内容详见9.5.2节。
本扩展开发实践的关键在于实现系统调用处理函数的重载，本书第9章的基于系统调用重载的文件操作日志原型系统展示了重载系统调用处理函数的详细过程。
可参照该原型系统完成本扩展开发实践。
相关原理、技术及实现请参见本书第1、2、9章。
A10基于系统调用重载的基本型文件保险箱本扩展开发实践的开发目标与A4“基于LSM的基本型文件保险箱”基本相同，即设置一个文件夹（即保险箱文件夹）用作文件保险箱的数据存储。
同时开发一个保险箱数据管理程序，实现保险箱文件的管理。
保险箱文件夹对其他任何程序都不可见，从而为用户的重要数据提供更为严格的安全保障。
与A4中扩展开发实践不同的是，本扩展开发实践在实现文件保险箱时采用的是系统调用重载方式。
本扩展开发实践的具体目标和内容详见9.5.2节。
本书第9章实现了一个基于系统调用重载的文件操作日志原型系统。
在重载的系统调用处理函数中可以实现相关的操作日志，也可以进行资源访问控制，可借此完成本开发实践中的文件保险箱功能。
本扩展开发实践可参照该原型系统的实现技术来完成。
相关原理、技术及实现请参见本书第1、2、9章。
A11基于系统调用重载的加密型文件保险箱基本型文件保险箱从操作系统层面上保证了个人重要数据的安全性，但存储保险箱数据文件的磁盘一旦离开系统，将会造成数据泄密。
本扩展开发实践要实现一个加密型文件保险箱，该保险箱除实现基本型文件保险箱的所有安全功能外，还实现对保险箱数据文件的加密和解密，即将文件放入到文件保险箱时对文件内容进行加密，当从文件保险箱中取出文件时，对文件进行解密以恢复文件的原始内容。
在本扩展开发实践中，完成加解密的方案有两种，即系统级的加解密和应用级的加解密。
本扩展开发实践的具体目标和内容详见9.5.3节。
本书第9章实现了一个基于系统调用重载的文件操作日志原型系统。
在重载的系统调‘用处理函数中，除了可以实现相关的操作日志、资源访问控制外，还可对访问所涉及到的数据进行变换，据此可以实现系统级的数据加密和解密。
在进行本扩展开发实践时，如采用系统级的加解密方案，可参照该原型系统的实现技术来完成。

编辑推荐

《信息安全技术解析与开发实践》是上海市重点课程配套教材,重点大学信息安全专业规划系列教材之一。
教学目标明确，注重理论与实践的结合教学方法灵活，培养学生自主学习的能力教学内容先进，反映了信息安全技术的最新发展教学模式完善，提供了配套的教学资源解决方案。

<<信息安全技术解析与开发实践>>

版权说明