计算机应用 2009, 29(09) 2369-2374 DOI: ISSN: 1001-9081 CN: 51-1307/TP

信息安全

基于Linux驱动级内核访问监控技术研究与实现

马博[1],袁丁[2]

1. 四川师范大学
2. 四川师范大学计算机学院

摘要： 针对POSIX.1e标准的权能模块的缺陷进行了改进，在Linux内核安全模块（LSM）框架基础上，加载改进的模块，对操作系统内核层进行监听和控制处理,完成进程信任状特权仲裁、安全i节点(i-node)操作、信息队列反馈等一系列操作,最后调用字符设备反馈监控信息到应用层进行安全控制处理。实验表明，改进方案与加载原有权能模块Linux内核的方法相比，不仅在系统的运行效率、监控的正确率和系统扫描覆盖率上有所提高，而且在系统资源占用率等多项指标中都显示其具有良好的监控性能。

关键词： 访问控制 内核驱动 系统调用 Linux安全模块 权能模块 access control kernel driver system call Linux Security Model (LSM) capability module

Research and implementation of layer access control technology based on Linux kernel driver

Abstract: A method was proposed to improve POSIX.1e standard capability module. In addition, monitoring and controlling were performed on the operation system kernel layer after loading improved module at the kernel of Linux Security Module (LSM) framework. Furthermore, a series of operations were carried out, which included the process trust-like privileges arbitration, security i-node operation, information feedback, queue operation, etc. At last, the character devices were used to feedback the monitor information to application layer and performed security control. Compared with original capability module, the proposed scheme not only improves efficiency of system operation, correct monitoring rate, and coverage of system scanning, but also keeps better monitoring performance in system resources occupancy rate and several parameters.

Keywords:

收稿日期 2009-04-16 修回日期 2009-06-09 网络版发布日期 2009-09-01

DOI:

基金项目:

通讯作者: 马博

作者简介:

作者Email:

参考文献：

本刊中的类似文章

1．蒋世忠; 杨进; 张英.基于免疫原理与粗糙集理论的入侵检测方法[J]. 计算机应用, 2006,26(5): 1077-1080

2．夏鹏万 陈荣国 孙剑.增强的基于角色的数据库访问控制模型[J]. 计算机应用, 2007,27(3): 597-600

3. 张智广 郭忠文 .无线传感器网络中基于分簇的自适应MAC协议[J]. 计算机应用, 2006,26(11): 2528-2530
4. 王维林 张来顺 张远洋 .基于角色的Web Services动态访问控制模型[J]. 计算机应用, 2006,26(11): 2607-2609
5. 沈海波 洪帆 .基于属性的授权和访问控制研究[J]. 计算机应用, 2007,27(1): 114-117
6. 陈志祥 陆音 陆桑璐 陈道蓄.基于协议转换的安全网关原型系统设计与实现[J]. 计算机应用, 2007,27(2): 299-302
7. 谭良 周明天 .带时间特性的自主访问控制政策及其在Linux上的设计与实现[J]. 计算机应用, 2006,26(12): 2906-2909
8. 瞿进 李清宝 白燕 魏珉.文件过滤驱动在网络安全终端中的应用[J]. 计算机应用, 2007,27(3): 624-626
9. 张艳霞 王劲林.一种P2P网络鲁棒访问控制协议[J]. 计算机应用, 2007,27(3): 538-540
10. 杨涛;刘锦德;谭浩.Web服务安全基础设施的研究[J]. 计算机应用, 2006,26(6): 1248-1250
11. 王娜; 陈越; 汪斌强.适用于多源IP组播的安全访问控制协议[J]. 计算机应用, 2006,26(4): 818-819
12. 孟健; 曹立明; 王小平; 姚亮.XML文档的加密访问控制与传输[J]. 计算机应用, 2006,26(5): 1061-1063
13. 钱丽萍;汪立东.一种评测应用程序实际性能开销的方法[J]. 计算机应用, 2006,26(5): 1180-1182
14. 陈岳阳 马学森 韩江洪 魏振春.RBAC模型中用户代理机制的研究[J]. 计算机应用, 2007,27(9): 2200-2201
15. 彭智勇 杨鏖丞 任毅.可信数据库—概念、发展和挑战[J]. 计算机应用, 2008,28(11): 2741-2744
16. 王雷 庄毅 潘龙平 .基于强制访问控制的文件安全监控系统的设计与实现[J]. 计算机应用, 2006,26(12): 2941-2944
17. 李志英 黄强 楼新远 冉鸣 .RBAC模型研究、改进与实现[J]. 计算机应用, 2006,26(12): 2945-2947
18. 张军 苏璞睿 冯登国 .基于系统调用的入侵检测系统设计与实现[J]. 计算机应用, 2006,26(9): 2137-2139
19. 刘孝保; 杜平安.J2EE模式下基于角色访问控制的应用[J]. 计算机应用, 2006,26(6): 1331-1333
20. 王婷 陈性元 张斌 包义保 夏春涛.基于GAA-API的Web网页细粒度访问控制方法研究[J]. 计算机应用, 2007,27(5): 1274-1276
21. 王志强 黄皓 夏磊.进程内细粒度保护域模型及其实现[J]. 计算机应用, 2007,27(6): 1356-1359
22. 陈敏 刘晓强 .扩展RBAC的CRM动态用户访问控制模型与实现[J]. 计算机应用, 2007,27(10): 2508-2511
23. 晏立 朱宏伟.访问权限实时更新的模型与实现[J]. 计算机应用, 2007,27(11): 2712-2714
24. 李焕洲 刘益和 李华.基于信任和安全等级的P2P信息流模型[J]. 计算机应用, 2008,28(12): 3168-3170
25. 晏樱 李仁发.P2P网络中一种可信访问控制模型[J]. 计算机应用, 2008,28(12): 3194-3196
26. 丁怡 方勇 周安民 曾蕉 樊宇.网格环境下的G-R_TRBAC访问控制模型[J]. 计算机应用, 2008,28(12): 3214-3216
27. 吴俊军 朱建新 白喆.一种改进的轻量级嵌入式安全文件系统模型[J]. 计算机应用, 2008,28(1): 242-244
28. 王宇新 王政 郭禾 刘天阳 田佳.基于XML图的RBAC模型研究[J]. 计算机应用, 2009,29(1): 185-188
29. 刘志远 杨秋伟 崔国华 洪帆.一种基于标识的隐私资源保护方案[J]. 计算机应用, 2008,28(2): 418-421
30. 张德银 刘连忠.多安全域下访问控制模型研究[J]. 计算机应用, 2008,28(3): 633-636
31. 欧晓鸥 王志立 魏建香.基于RBAC与GFAC架构的访问控制模型[J]. 计算机应用, 2008,28(3): 612-614
32. 陈娟娟 程西军.支持动态角色切换的RBAC模型[J]. 计算机应用, 2008,28(4): 924-926
33. 姚慧 高承实 戴青 张徐.一种基于动态规划的自动信任协商策略[J]. 计算机应用, 2008,28(4): 892-895
34. 赵文刚 钟乐海 张娅 杨金 邹海洋.模糊窗口Markov链在IDS中的应用[J]. 计算机应用, 2008,28(6): 1398-1400
35. 张润莲 武小年 董小社.基于委托的分布式动态授权策略[J]. 计算机应用, 2008,28(6): 1365-1368
36. 张立臣 王小明.普适计算环境下的动态访问控制模型[J]. 计算机应用, 2008,28(8): 1931-1935
37. 何志 范明钰.基于HSC的进程隐藏检测技术[J]. 计算机应用, 2008,28(7): 1772-1775
38. 林丛 向勇.支持功率和速率控制的自组网MAC协议研究[J]. 计算机应用, 2008,28(8): 1946-1950
39. 陈钦 原焕 冯建华.企业检索中访问权限控制方法的实现与比较[J]. 计算机应用, 2009,29(07): 2000-2002
40. 沈海波.面向语义Web的基于语义和上下文的访问控制模型 [J]. 计算机应用, 2009,29(05): 1289-1292
41. 王睿 刘占军 李云 陈前斌 赵为粮.针对非对称链路的MAC协议改进策略[J]. 计算机应用, 2009,29(07): 1868-1870
42. 刘玉梅 郭黎利 申丽然.联合空时需求预留和功率控制的MAC协议[J]. 计算机应用, 2009,29(08): 2171-2174
43. 高迎 战疆.P2P环境下基于信任度的可控委托信任管理模型 [J]. 计算机应用, 2009,29(09): 2332-2335

44. 李时文 卢建朱.快速有效的XML访问控制新方案 [J]. 计算机应用, 2009,29(09): 2336-2338

文章评论

反馈人		邮箱地址	
反馈标题		验证码	2529