

JOURNAL

ISSN 1001-9146

CN33-1339/TN

OF HANGZHOU DIANZI UNIVERSITY

杭州电子科技大学 学报



ISSN 1001-9146



2011 5

Vol. 31 No.5 Oct. 2011

目 次

基于五维混沌系统的数字图像加密算法	王晓飞	王光义	(1)
基于广义 Henon 映射和 DWT-SVD 的数字水印算法	刘 瑜	王光义	(5)
一种新的 Rossler 混沌序列图像加密算法	邓 玥	袁 方	(9)
基于 Pro/E 和 ANSYS 的 LED 灯热设计	程筱军	李菊华	(13)
一种用于光通信的高速 LVDS 发送器设计	洪 慧 朱忠英	孙玲玲	(17)
LED 照明产品的性能参数及测试研究		时 佳	(21)
基于多级缓存的内存管理方案	丁 锐	陈 维	(25)
通用型引导装载程序中闪存驱动的设计	叶汉能	赵武锋	(29)
矩形 MQAM STFBC-OFDM 的性能分析	余 晨	李光球	(33)
相关衰落信道上 LDPC 码的性能分析	方锋华	李光球	(37)
二元周期序列的 k -错线性复杂度研究	周建钦	刺 锋	(41)
量子密钥诱骗态的经典仿真研究	汤颖轲	陈小余	(45)
颗粒群在平面湍射流中输运弥散的大涡模拟		吴迪冲	(49)
基于拉丁方阵的准循环 LDPC 码构造	陈集炜	包建荣	(54)
TD-SCDMA 下行预同步量化及截断研究	高 正 邓彰超	孟利民	(58)
嵌入式心音身份识别系统研究	王 佳	赵治栋	(63)
基于声与图像融合的车辆识别硬件系统设计	黄 亮	郭宝峰	(67)
3G 网络 H.264 视频监控系统的设计和实现	蒋 维	孟利民	(71)
Web 应用中的 ReDoS 检测方法研究	梁兴开	黄 亮	(75)
动态精密单点定位联合卫星测高求解潮位研究	罗孝文 高金耀 金翔龙	吴招才	(79)
一种基于逆序编码性质的 Apriori 算法改进	李家彪	王 盛	(83)
一种 Linux 平台下的可执行文件防篡改方法	张华飞	董黎刚	(87)
便携式冠状动脉狭窄无损诊断仪的研制	姜 斌	张 君	(87)
基于联合降低 PAPR 和干扰的小波包结构优选	田县庭	赵治栋	(91)
基于光正交码构造的准循环 LDPC 码	马丹丹 唐向宏	栗昆昆	(95)
多天线超宽带信道建模及相关性对其影响	董庭亮	赵泽茂	(99)
基于超正交码的最优预编码设计	黄 河	曹 估	(103)
基于数字预失真技术的功放性能改善研究	刘顺兰	刘艳艳	(107)
单载波频域均衡中独特字类型选择性能分析	张福洪	吴铭宇	(111)
基于中值滤波与边缘插值的视频去隔行算法	成佩茂	包建荣	(115)
基于 Mini2440 的低带宽语音通信系统	刘顺兰	刘顺兰	(119)
高速 LVDS 收发器的设计及硬件实现	赵娜娜	章坚武	(123)
MRC 分集接收 CE-OFDM 系统性能分析	沈 磊	章坚武	(127)
基于脆弱水印的彩色视频认证方案	陈 权	李光球	(131)
一种基于区域搜索的快速图像修复算法	锁光辉	陈宏炳	(135)
一种基于人眼视觉特征的图像内容认证算法	侯志宇	任 澍	(139)
一种基于多音字的中文文本篡改检测水印算法	张巧焕	陈宏炳	(143)
跨平台手机移动中间件	曹守斌	王丽娜	(147)
DVB-C 数字电视接收系统的设计与实现	唐向宏	林 远	(151)
一种基于两测度的无线链路重要性评价方法	费文斌	郭淑琴	(155)
关于 B/S 模式下对串口实时监测的研究	王志德	陈 磊	(159)
一种适合硬件实现的低复杂度 MAD 预测算法	董志远	董黎刚	(163)
基于 Codec Engine 下车牌定位方法研究	王 佳	周冰倩	(167)
SIFT 算法图像自适应优化	王 佳	张 桦	(171)
基于 FPGA 的多模式实时立体显示系统设计	李克腾	王泽梁	(175)
基于小波能量的轮廓抖动性烟雾检测算法	汪丽华	郑 宁	(179)
	刘来成 周文晖	楼 斌	(183)
	李庆奇	马 莉	(183)

CONTENTS

An Image Encryption Algorithm Based on Five-dimension Chaotic System	WANG Xiao-fei WANG Guang-yi	(1)
A Digital Image Watermarking Algorithm Based on the Generalized Henon Maps and SVD-DWT	LIU Yu WANG Guang-yi	(5)
A New Image Encryption Algorithm Based on Improved Rossler Chaotic Sequence	DENG-Yue WANG Guang-yi YUAN-Fang	(9)
Thermal Analysis of LED Lamps Based on Pro/E and ANSYS	CHENG Xiao-jun Li Ju-hua	(13)
Design of a High Speed LVDS Transmitter for Optical Communication	HONG Hui ZHU Zhong-ying CHEN Ke-ming SUN Ling-ling	(17)
Research on the Performance Parameters and Test of LED Lighting Product	SHI Jia	(21)
One Memory Allocating Method Based on Multilevel Cache	DING Rui ZHANG Ya-jun CHEN Wei	(25)
Design of Flash Driver for Universal Bootloader	YE Han-neng YAO Mao-qun ZHAO Wu-feng	(29)
Performance Analysis of Rectangular MQAM STFBC-OFDM	YU Chen LI Guang-qiu	(33)
Performance Analysis of LDPC Codes in Correlated Fading Channels	FANG Feng-hua LI Guang-qiu	(37)
Research on k-error Linear Complexity of Periodic Binary Sequences	ZHOU Jian-qin LA Feng	(41)
Classical Simulation Study for Decoy-state of Quantum Cryptography	TANG Ying-kai CHEN Xiao-yu	(45)
Large Eddy Simulation of Particles Transport and Diffusion with Different Mass Flow Rate in Turbulent Planar Jet Flow	WU Di-chong	(49)
Construction of QC-LDPC Codes Based on Latin Squares	CHEN Ji-wei ZHAO Ze-mao BAO Jian-rong	(54)
Research on Quantification Word Length Threshold and Truncation of TD-SCDMA Pre-synchronous	GAO Zheng DENG Zhang-chao HUA Jing-yu MENG Li-min	(58)
Research on Embedded Heart Sound Identification System	WANG Jia ZHAO Zhi-dong	(63)
The Hardware System Design of Vehicle Identification Based on the Fusion of Acoustical Signal and Image	HUANG Liang PENG Dong-liang GUO Bao-feng	(67)
Design of H. 264 Video Monitoring System Based on 3G Network Transmission	JIANG Wei MENG Li-min	(71)
A Research on Detection of ReDoS Attack in Web Application	LIANG Xing-kai ZHAO Ze-mao HUANG Liang	(75)
A Primary Research and Practice to Determine Tide Height Using PPP and Satellite Altimeter	LUO Xiao-wen GAO Jin-yao JIN Xiang-long LI Jia-biao CHU Feng-you WU Zhao-cai	(79)
An Improvement for Apriori Based on the Property of Reverse Coding	ZHANG Hua-fei DONG Li-gang WANG Sheng	(83)
An Approach for Protecting Linux Platform-runable from Being Tampered	JIANG Bin ZHANG Jun	(87)
Research on Portable Non-destructive Diagnostic Instrument for Coronary Artery Stenosis	TIAN Xian-ting ZHAO Zhi-dong	(91)
The Research on Structures of Wavelet Packet Modulation Based on PAPR and Interference Reduction	MA Dan-dan TANG Xiang-hong DONG Ting-liang LI Kun-kun	(95)
Construction of Quasi-cyclic LDPC Codes Based on Optical Orthogonal Codes	HUANG He ZHAO Ze-mao	(99)
MIMO&UWB Channel Modeling and Impact on Channel Performance from Correlation	LIU Shun-lan CAO Ji	(103)
Optimal Pre-coding Design Based on Super Orthogonal Codes	LIU Shun-lan LIU Yan-yan	(107)
Improving Power Amplifier Performance Based on Digital Per-distortion Technology	ZHANG Fu-hong HUANG-Yong WU Ming-yu	(111)
Performance Analysis of Unique Words Selection in Single Carrier Frequency Domain Equalization	CHENG Pei-mao LIU Shun-lan BAO Jian-rong	(115)
Video De-interlacing Algorithm Based on Median Filtering and Edge-dependent Interpolation Algorithm	ZHAO Na-na WANG Xiang-wen LIU Shun-lan	(119)
Low-bandwidth Voice Communication System Based on Mini2440	SHEN Lei ZHANG Jian-wu	(123)
High-speed LVDS Transceiver Design and Hardware Implementation	CHEN Quan ZHANG Jian-wu	(127)
Performance Analysis of CE-OFDM System with MRC Diversity Reception	SUO Guang-hui LI Guang-qiu	(131)
Integrity Authentication Scheme of Color Video Based on the Fragile Watermarking	HOU Zhi-yu TANG Xiang-hong CHEN Hong-bing	(135)
A Fast Image Inpainting Algorithm Based on Local Search	ZHANG Qiao-huan TANG Xiang-hong REN Shu	(139)
Image Content Authentication Algorithm Based on Human Visual System	CAO Shou-bin TANG Xiang-hong LIN Jun-hai CHEN Hong-bing	(143)
A Chinese Text Watermarking Algorithm for Tamper Detection Based on Polyphone	FEI Wen-bin TANG Xiang-hong ZHANG Ning WANG Li-na	(147)
Cross-platform Cell Phone Mobile Middleware	LIN Yuan	(151)
Design of DVB-C Digital TV Receiving System Based on USB	WANG Zhi-de WANG Jing-hui GUO Shu-qin	(155)
A Method for Estimating the Importance of Based on both Sides of the Wireless Networks Link	DONG Zhi-juan ZHANG Pin CHEN Lei	(159)
The Research about Real-time Monitoring of the Serial Port in B/S Mode	ZHU Xiao-jun DONG Li-gang	(163)
A Low-cost MAD Prediction Algorithm Facilitating Hardware Implementation	WANG Jia YIN Hai-bing ZHOU Bing-qian	(167)
The Research of License Plate Location Algorithm Base on DM6446	LI Ke-teng WU Er-yong ZHANG Hua	(171)
Research Based on Distance Ratio Thresh Adaptive Parameter of Scale-invariant Feature Transform Algorithm	WANG Li-hua WANG Dao-jin WANG Ze-liang	(175)
FPGA-based Multi-mode to Achieve Real-time Stereoscopic Display System	LIU Lai-cheng ZHOU Wen-hui LOU Bin ZHENG Ning	(179)
A Smoke Detection Algorithm Based on the Contour Jitter of Wavelet Energy	LI Qing-qi MA Li	(183)

一种 Linux 平台下的可执行文件防篡改方法

姜 斌¹, 张 君²

(1. 杭州电子科技大学通信工程学院, 浙江 杭州 310018; 2. 浙江省电子信息产品检验所, 浙江 杭州 310007)

摘要: 保证可执行文件的完整性对于整个系统的安全性是非常重要的。该文提出了一种可执行文件防篡改方法, 该方法的基本思想是: 通过安全钩子捕获可执行文件的执行请求; 在捕获执行请求之后, 计算该文件当前的哈希值, 并与预期哈希相比较。如果两者一致, 则说明可执行文件是可信的, 允许运行; 否则是不可信的, 拒绝运行。以 Linux 平台为基础实现了原型系统, 实验验证, 该方案能够有效保证可执行文件的完整性。

关键词: 完整性; 安全模块; 信息安全

中图分类号: TP309

文献标识码: A

文章编号: 1001-9146(2011)05-0087-04

0 引言

随着信息技术的飞速发展, 信息安全事件已经深入到人们生活的方方面面^[1]。调查表明, 在各类信息安全事件当中, 恶意代码是最重要的安全威胁之一^[2]。恶意代码要传播, 必须要进行几个特定的操作, 以最典型的病毒和木马为例, 其在传播的过程中, 必然要改写其它可执行文件, 以达到感染的目的。因此, 如果能有效检测到病毒木马对其它可执行文件的篡改, 则可以遏止病毒木马的传播过程。基于这种思想, 本文提出了一种可执行文件防篡改方法。这种方法的基本思想是: 在任何一个可执行文件运行之前, 先检查其是否被篡改。如果被篡改了, 则说明该文件不可信, 拒绝其执行; 如果没有被篡改, 则允许其执行。由此达到防止被篡改的(恶意)软件运行的目的。Linux 平台下的实验结果表明达到了预期效果。

1 Linux 平台下可执行文件防篡改架构

要实现可执行文件防篡改架构, 有两个关键步骤: 第一步, 在任何一个可执行文件运行之前, 先捕获其运行请求; 第二步, 在捕获到运行请求之后, 判定该文件是否被篡改。要实现第一步, 可以采用钩子机制。在 Windows 平台下采用相应的 Hook 函数即可, Linux 平台下, 则可以通过 Linux 安全模块(Linux Security Module, LSM)实现; 要实现第二步, 只要计算可执行文件的哈希值即可。如果可执行文件的当前哈希值与该文件的预期哈希值是一致的, 则说明文件没有被篡改, 是可信的; 否则说明被篡改, 是不可信的。

1.1 Linux 内核安全模块

LSM 是一个轻量级通用的访问控制框架。它通过在内核当中的特点位置增加检测点, 并在检测点插入钩子函数。这样, 当用户需要施加额外的访问控制的时候, 可以改写这些钩子函数, 从而获得安全增强^[3]。一个访问文件节点 inode 的访问过程如图 1 所示。在经过了错误检查、访问控制 DAC 检查之后, 就在 Linux 内核试图对内核对象进行访问之前, LSM 钩子调用一个 LSM 模块所提供的函数。该函数根据策略引擎进行判断, 要么允许此次访问, 要么拒绝访问并强制返回一个错误。在 LSM 当中, 对如

收稿日期: 2011-07-20

基金项目: 浙江省教育厅基金资助项目(Y200803422)

作者简介: 姜斌, (1980-), 男, 浙江衢州人, 助理研究员, 网络优化。

下一些内核对象插入了安全钩子:任务钩子、程序钩子、文件系统钩子、管道/文件/socket 相关钩子;文件操作钩子;网络数据包相关钩子;网络设备相关钩子;信号量/共享内存/消息队列钩子;单个消息钩子等。可见,LSM 的功能还是比较强大的。

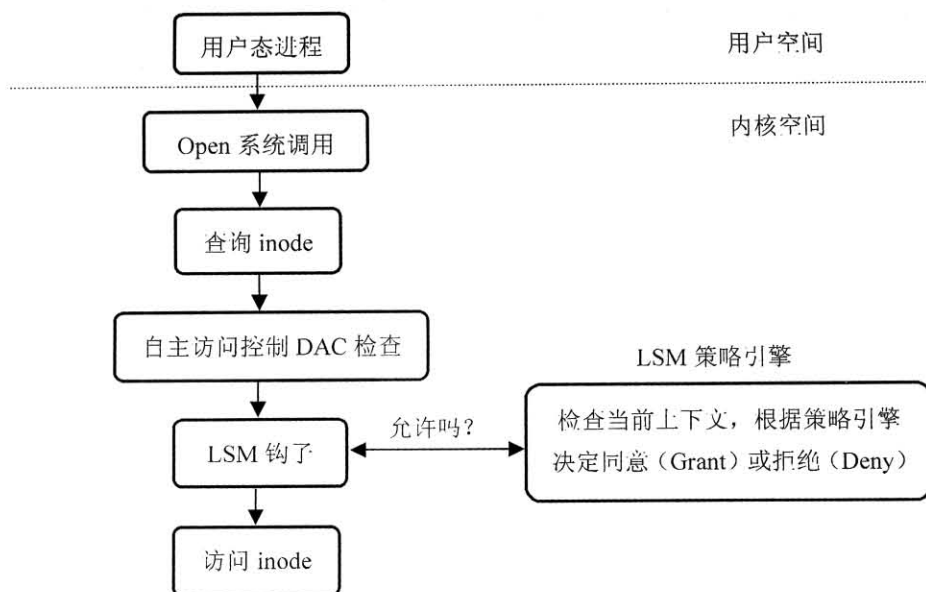


图1 LSM 的挂钩结构 (以文件访问为例)

1.2 系统架构

在 LSM 的基础上, Linux 平台下可执行文件防篡改架构如图2所示。

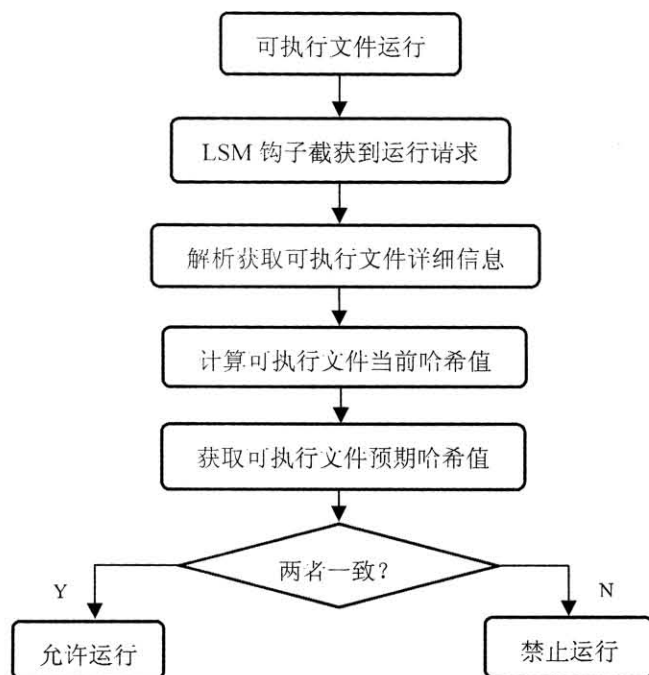


图2 Linux 平台下可执行文件防篡改架构

整个架构的工作流程是这样的: (1) 首先, 某个可执行文件被用户运行; (2) LSM 钩子截获到该文件的运行请求; (3) 相应的 LSM 钩子函数被执行。该函数将解析请求运行文件的详细信息——包括绝对

路径文件名、参数等等;(4)根据步骤(3)当中获取的可执行文件绝对路径文件名,计算该文件的当前哈希值;(5)获取该文件的预期哈希值(通常保存在外部的U盘当中);(6)将文件的当前哈希值与预期哈希值相比较,如果两者一致,则允许该可执行文件的运行,否则拒绝其运行。

2 系统实现

2.1 LSM 钩子设置

在图2的架构当中,为了截获可执行文件的运行请求,需要进行LSM钩子设置,这是通过设置 `bprm_check_security` 函数钩子实现的。`bprm_check_security` 钩子函数原型是:

`int (* bprm_check_security) (struct linux_binprm * bprm)`。其中,参数 `bprm` 包含了基本的 `linux_binprm` 结构体信息,例如:要执行的应用程序的真实名称、命令行参数信息等等。通过在LSM内核模块文件当中添加如下代码,可以设置 `bprm_check_security` 钩子:

```
static struct security_operations jetway_security_ops = {
    .bprm_check_security = appprotec_check_security,
};
```

这样,任何时候当某个应用程序开始运行之后,在Linux内核调用实际的加载器加载其运行之前,会自动转到定义的 `appprotec_check_security` 函数。`appprotec_check_security` 首先根据参数“`struct linux_binprm * bprm`”获取文件的相关信息,特别是其绝对路径文件名、参数信息等,其中 `bprm->interp` 就给出了绝对路径文件名;然后,内核根据获取的绝对路径文件名打开相应的文件,计算其哈希(MD5);最后,内核从U盘读取该文件的预期哈希:如果两者不一致,则返回-1拒绝文件的运行;否则返回0允许其运行。

2.2 USB 驱动

在图2的架构当中,进行哈希值比较的时候,需要从U盘读取文件的预期哈希值。这就需要编写特定的USB驱动。为什么不直接使用Linux自带的USB驱动呢?这是因为:需要对U盘进行判定,只有是特定的U盘,才相信其存储的预期哈希值,否则如果读取任意U盘的话,那攻击者完全可以伪造假的预期哈希值从而使得架构失去作用。从U盘读取预期哈希值的过程是:首先从内核判定插入的U盘是不是允许的U盘(这可以通过id号,以及特殊扇区的特殊信息来保证),如果是允许的U盘,则读取U盘内部名为 `expectedhash` 的文件,并解析该文件获取预期哈希值。

USB本身有4种传输方式:等时传输、中断传输、控制传输和猝发传输。USB使用1ms的时间帧来传输数据。在每次传输之前,HC产生一个帧头 `Start Of Frame`。每次传输的时候,如果有等时数据存在,则等时数据最先被传输。HCD需要确保:有足够的时间用来完成所有的等时传输和中断传输数据,然后使用剩下的时间来完成控制传输和猝发传输数据^[4]。根据上述USB驱动特点,就可以对USB驱动框架进行填写,开发实际的USB驱动了。描述USB驱动程序的结构体是系统定义的标准结构 `struct usb_driver`,在 `struct usb_driver` 中, `name` 用来告诉内核模块的名字; `probe` 和 `disconnect` 是函数指针,当设备与在 `id_table` 中的变量信息匹配时,函数被调用; `id_table` 用来告诉内核模块支持的设备。更详细的USB开发可以参见文献4、5。

3 实验和讨论

3.1 实验结果

Linux Redhat 内核2.4上实现了一个原型系统,构造了一个名为 `appproect.ko` 的LSM驱动,在其中实现了 `int (* bprm_check_security) (struct linux_binprm * bprm)` 钩子。在root权限下,使用“`insmod appproect.ko`”加载的内核,然后插入具有预期哈希信息的U盘。启动 `/bin/ls`,可以发现,正常列出了文件和目录信息;之后,使用编辑器更改 `/bin/ls` 当中任意位置的任意个字节,再次运行,系统显示“`operation not permitted`”。实验达到了预期结果。

经过多次实验统计,系统引起约1%的额外负载,这主要是计算哈希值所引起的。不过,1%的负载对系统性能影响不大,可以接受,用户几乎感受不到时间的延迟。

3.2 讨论

首先需要指出的是,虽然本文在 Linux 平台实现的原型系统,但该架构仍然可以应用到 Windows 平台上面。当应用到 Windows 平台时,其基本流程类似于 Linux 平台(如图 2 所示),唯一不同的是, Linux 平台采用 LSM 捕获可执行文件运行请求,而在 Windows 平台下,可以通过设置 Windows 钩子的方法来达到相同目的。要设置 Windows 钩子,可以调用 SetWindowsHookEx() 函数。其次需要指出的是,本文提出的方法是在可执行文件运行之前,先判定该文件是否已经被篡改。也就是说,本文的方法并不能“阻止篡改”,而只能“发现篡改”,并在“发现篡改”之后,调用备份文件进行主动恢复,从而达到保护的目的。之所以不采用“阻止篡改”的方法,是由于采用“阻止篡改”的方法,就需要判定当执行写入操作时,执行写入的进程究竟是一个正常进程,还是一个病毒或者木马进程,而这种判定从理论上是不可行的:因为不存在一个算法,能够判定任意一个文件是否是病毒或者木马。基于这种原因,才采用了“发现篡改”的方法。注意到在架构当中,任何一个可执行文件在刚刚发出执行请求,而并没有创建进程实体之前,其完整性就被检查了,因而这种方案不仅能够发现对文件的篡改,而且能够有效避免系统感染病毒或者木马,保证了系统的安全性。

4 结束语

本文提出了一种可执行文件防篡改框架,该框架在任何可执行文件实际运行之前,先通过计算哈希值判定其是否被非法篡改。如果被篡改,则禁止其运行;否则允许其运行。本文以 Linux 平台为基础,实现了一个原型系统,达到了预期效果。下一步,该架构可以进一步扩展,即:在可执行文件进行完整性哈希比较时,针对指定的配置文件进行完整性比较。

参考文献

- [1] 国际计算机网络应急技术处理协调中心. CNCERT 互联网安全威胁报告 [EB/OL]. <http://www.cert.org.cn/UserFiles/File/201101monthly.pdf> 2011-02-01.
- [2] 国际计算机网络应急技术处理协调中心. CNCERT 互联网安全威胁报告 [EB/OL]. <http://www.cert.org.cn/UserFiles/File/201102monthly.pdf> 2011-03-01.
- [3] Wright C, Cowan C, Smalley S, et al. Linux Security Modules: General Security Support for the Linux Kernel [C]. San Francisco: Proceedings of the 11th USENIX Security Symposium, 2002: 1-14.
- [4] Intel. Universal Host Controller Interface (UHCI) Design Guide [EB/OL]. <http://download.intel.com/technology/usb/UHCI1D.pdf> 2011-05-31.
- [5] Corbet J, Rubini A, Kroah-Hartman G. Linux Device Drivers (Third Edition) [M]. O'Reilly Media Press: Cambridge Massachusetts, 2005: 10-14, 50-64.

An Approach for Protecting Linux Platform-runable from Being Tampered

JIANG Bin¹, ZHANG Jun²

(1. School of Communication Engineering, Hangzhou Dianzi University, Hangzhou Zhejiang 310018, China;

2. Zhejiang Provincial Testing Institute of Electronic Information Products, Hangzhou Zhejiang 310007, China)

Abstract: Protecting the integrity of applications is important to the security of an information system. This paper introduces a framework for keeping the applications from being tampered. The basic idea of the framework is as the following: firstly, capturing the running request of an application according to security hooks; then, calculating the current hash the application and compare it with the expected hash. If they match, it means the application is trusted and the running request is granted; otherwise untrusted and the running request is denied. We implement a prototype in the Linux platform, and experimental results show that our approach can efficiently protect the integrity of applications.

Key words: integrity; security module; information security

杭州电子科技大学学报

2011年10月 第31卷 第5期 双月刊

JOURNAL OF HANGZHOU

DIANZI UNIVERSITY

Vol. 31 No. 5 Oct., 2011 Bimonthly

Started in 1981

HANGZHOU DIANZI KEJI DAXUE XUEBAO

Sum No.133

主办单位: 杭州电子科技大学

编辑出版: 杭州电子科技大学学报编辑部

浙江省杭州市下沙高教园区

电话: 0571-86915100 电传: 0571-86919103

邮政编码: 310018

E-mail: hdxh@hdu.edu.cn

国内发行: 杭州电子科技大学学报编辑部

天津市大寺泉集北里别墅17号

邮政编码: 300385

印刷: 杭州地质印刷有限公司

Sponsor: Hangzhou Dianzi University

Editor and Publisher: Editorial Department of
Journal of HDU

Address: Shiasa Higher Education Zone
Hangzhou, Zhejiang, 310018,
China

Distributed: Editorial Department of Journal of
HDU

Printed: Printing House of Huaxing
(Hangzhou, China)

国内统一刊号: **ISSN1001-9146** (公开发行业)
CN33-1339/TN

定价: 6.00 元