文章编号:1671 - 6833(2012)05 - 0130 - 03

一种 XPE 安全加固技术的研究与实现

郭育艳

(河南财经政法大学 图书馆 450002)

摘 要:操作系统安全一直是人们关注的焦点,如何构建一个安全操作系统是当前信息安全研究的热点课题之一.依据可信计算和主动防御的思想,将 Windows XPE 系统和 USBKEY 一体化,研究 Windows 安全加固技术,设计并实现了一个安全防护系统 SR-XPE,系统工作在内核模式,实现了可信引导、进程启动控制和网络访问控制,实现了关键资源强制访问控制.

关键词:安全加固;XPE;USBKEY;可信计算;访问控制

中图分类号:TP309 **文献标志码**:A doi:10.3969/j.issn.1671 - 6833.2012.05.029

0 引言

计算机技术发展至今,信息安全问题一直备受关注.目前针对信息安全问题,相继出现了不少新技术,如侦测与反侦测技术、动态度量技术、主动防御技术等,这些技术都在系统应用层和操作系统内核层等不同层次上实现.Windows 系统是目前最流行的 PC 操作系统之一,同时也是信息安全研究最关注的操作系统之一[1].在广泛流行杀毒软件技术、防火墙技术的情况下,安全操作系统的研究也日益受到关注,这也是我们的研究重点.作者选择 USBKEY 嵌入式 Windows XPE 研究、设计并实现了一个安全操作系统原型 - Security Reinforced XPE,简称 SR-XPE.首先简要介绍 SR-XPE 系统设计,主要有基于 GRUB 的可信引导,基于过滤驱动和内核 Hook 的进程、网络及外接设备访问控制,基于 GINA 技术的身份认证,安全通讯协议等,然后侧重介绍强制访问控制技术和文件访问控制的实现.

1 SR-XPE 系统设计

1.1 基于 GRUB 的可信引导

基于可信计算信任链传递的思想,可以采用层层验证的方法来保障系统整体的安全性.可信引导作为可信系统的基础,是系统实现可信计算非常重要的部分.SR-XPE 采用基于 USBKEY 的 Grub 引导启动,在 Grub2 内核加入了引导控制程序.

在裁剪 Grub2 时,不使用 Grub2 默认包含的/boot/grub 目录及 grub 目录下的文件,把所有使用到的模块都要静态加载到 Grub2 内核镜像中.为实现 USB 启动,引导程序必须使用的模块有硬盘设备模块 biosdisk、分区类型 part_msdos、分区格式 fat、驱动器号映射模块 drivemap、引导主程序模块 normal 和命令模块 boot,在 Linux 环境下创建内核文件的命令为:

./grub - mkimage -d . -o coreloadxpe.img biosdisk part_ msdos fat drivemap normal boot

Grub 引导过程的一个重要工作是关键资源(操作系统启动核心文件和安全组件自身等)保护.关键资源保护通过文件完整性校验实现,目的是防止重要文件遭恶意篡改.

1.2 系统强身份认证

SR-XPE 系统使用定制的用户身份认证模块,以增强系统登录安全.Windows XP/2003/XPE 系统默认使用 GINA 机制进行登录用户身份认证[1].GINA(Graphical Identification and Authentication)是 Windows 操作系统的核心文件之一.Winlogon.exe 在系统启动时加载 GINA.GINA 的主要功能包括:用户身份认证、系统锁屏登录、启动 Explorer 等.

微软提供了使用定制 GINA 替换系统 GINA(msgina.dll)的方法,因此我们可以在验证用户名密码的同时加入我们关心的其他验证模块,如人

收稿日期:2012 - 04 - 15;**修订日期**:2012 - 07 - 01

作者简介:郭育艳(1977 -),女,河南郑州人,馆员,硕士.主要从事文献信息开发与利用.

脸识别、声控、自定义口令等. 当然,自定义 GINA 需要实现系统 GINA 的全部接口函数,也可以仅实现自己关心的部分接口,其余直接调用系统 GINA 的接口实现. 图 1 是 GINA 修改后的系统登录界面截图:

图 1　SR-XPE 系统登录界面

Fig. 1　Landing interface for SR-XPE

在这个自定义 GINA 中系统重新实现了标准接口函数 WlxLoggedOutSAS,增加了 USBKEY 硬件口令验证(即 PIN 码),同时去掉了密码输入框. 自定义 GINA 需要实现的供 Winlogon. exe 调用的一系列 WinWlx 接口函数,如 WlxInitialize, WlxLoggedOutSAS, WlxLoggedOnSAS, WlxActivateUserShell, WlxShutdown, WlxCreateUserDesktop, WlxWkstaLockedSAS 等.

1.3　进程启动控制

SR-XPE 系统提供对应用程序真实性和完整性度量和校验的功能. 可执行程序的真实性度量,是为了确保运行的可执行程序都是合法的. 可执行程序完整性度量,是为了保证系统启动的可执行程序都是可信的,禁止不符合预期的程序的启动. SR-XPE 核心模块会在可执行程序启动前,度量该程序的真实性和完整性,只有在度量结果和预存值匹配的情况下,才允许程序启动,否则禁止启动. 如果 SR-XPE 中的某个程序被恶意代码感染,将无法通过度量,进而无法启动,这就能够有效阻止病毒或木马继续传播和破坏,实现对恶意代码的免疫,保障系统完整性不被破坏.

SR-XPE 系统的进程启动控制是通过内核钩子和文件过滤驱动实现的. Windows 内核 Hook 技术已趋于成熟[2],我们可以通过修改系统服务描述符表(SSDT)来实现控制系统的内核操作(详见 2.2 节). 系统应用程序的一些操作,比如用户层执行 CreateFile 函数创建文件,内核层钩到该 IRP 请求并进行拦截控制. 成功拦截之后,判读文件摘要与预设值是否匹配,如果匹配则允许启动;否则拒绝执行,如图 2 所示.

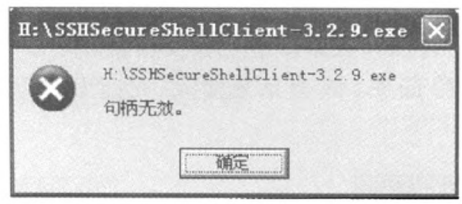

图 2　进程阻止运行提示

Fig. 2　Indication of halt of proceeding course

1.4　网络访问控制

SR-XPE 系统网络访问控制实现类似于防火墙的功能. 当截获网络数据包时,系统核心模块会检查数据包头中的源 IP、源端口、目的 IP、目的端口和协议类型,看与访问控制策略库(白名单列表)是否匹配. 系统会放行允许的数据包,阻止非法的数据包,如试图 telnet 不在白名单中的 IP,如图 3 所示.

图 3　网络策略配置库

Fig. 3　Network strategy configuration database

系统通过在 NDIS 层挂接内核钩子实现对所有网络数据包进行拦截控制[2]. 拦截的 IRP 请求包括创建(IRP_MJ_CREATE)、关联请求(TDI_ASSOCIATE_ADDRESS, TDI_DISASSOCIATE_ADDRESS)、关闭(IRP_MJ_CLOSE)以及 Socket 操作. 通过解析 address_entry 可以获取当前操作的目的是 IP 或者本地进程,目前实现了基于 IP 的控制.

1.5　安全通讯协议

以上主要描述了系统终端设计,为了对 SR-XPE 系统进行统一管理,需要构建一个管理平台,SR-XPE 系统终端与管理平台间的安全通讯变得尤为重要.

下面简要介绍安全通讯序列中的会话密钥协商过程:终端发送包含终端身份信息的协商请求(client_hello);服务端产生一个会话 ID,并和服务端证书一起发给终端(sercer_cert);终端使用服务端 CA 验证服务端证书,验证通过后,发送随机数和客户端证书(client_cert),同时存储会话 ID;服务端验证终端证书,验证通过后,产生一个会话密钥,再加上服务端随机数和终端随机数,用服务端私钥和终端公钥进行签名和加密后发给终端(secret_info);终端使用自身私钥和服务端公钥解密和验签,然后验证随机数,得到会话密钥,接下来发送一个协商完成消息(client_finish);服务端

应答消息(server_finish)使用会话密钥加密.之后的会话过程和数据传输过程使用新的会话密钥加密.实验证明,该会话密钥协商过程是安全可靠的.

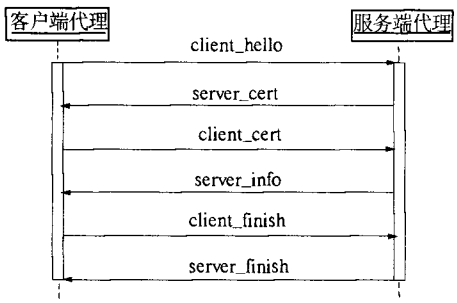

图4 通讯协议-密钥协商

Fig.4 Communicating agreement-code consulting

2 强制访问控制

2.1 访问控制

访问控制,是指按用户身份及其所归属的分组来限制用户对特定资源的访问权限,一般分为自主访问控制和强制访问控制两大类.

强制访问控制基本思想是每个主体和每个客体都有既定的安全属性,主体对客体的访问权限,取决于二者安全属性之间的关系[3].主体对客体的访问主要有4种方式:向下读(rd),向上读(ru),向下写(wd),向上写(wu).可见,MAC通过分级的安全标签实现了信息的单向流通,比较著名的有BLP模型和BIBA模型.

在设计实现的强制访问控制中,所有的主体(如用户或进程)和客体(如资源或文件)都划分安全级别,如1-6级.主体对客体的访问权限是在安全策略中规定的.SR-XPE将安全级别按照从高到底排序,规定安全级别高的进程可以单向读写安全级别低的文件,而安全级别低的进程禁止访问安全级别高的文件.

2.2 文件访问控制实现

作者按照访问控制以安全级别制定控制策略的原理和内核过滤驱动技术,实现了一个强制访问控制模型.控制策略规定重要资源(包括文件和注册表项)拥有较高安全级别,只有特定进程才能访问.

操作系统中文件是最重要的信息载体,操作系统安全最重要的工作之一就是保障重要文件的安全.使用文件过滤驱动技术和Hook技术,可以覆盖了文件的整个生命周期,包括文件的创建(ZwCreateFile),打开(ZwOpenFile),删除(ZwDeleteFile),读(ZwReadFile),写(ZwWriteFile)等操作.目前SR-XPE系统实现了我们关心的核心文件禁止普通进程访问的功能(打开、重命名、删除等).当用户进程notepad.exe试图打开一个安全级别较高的文件时,SR-XP系统会阻断访问,弹出提示如图5所示.

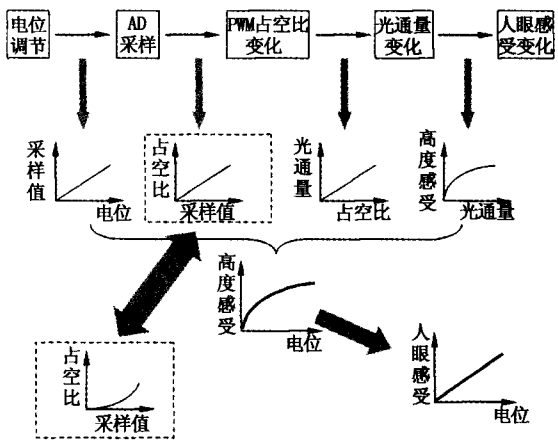

图5 文件拒绝打开

Fig.5 Default of opening files

3 结语

作者介绍了一种Window安全加固技术并设计了SR-XPE系统,实现了基于GRUB的可信引导、基于GINA的强身份认证、基于内核HOOK的进程启动控制和网络连接控制、改进的安全通讯协议以及基于过滤驱动关键资源访问控制等功能,可以有效保护操作系统安全.

参考文献:

[1] LI L, WU J, GUO X W, et al. Framework for Windows Password Function Security Enhancement[J]. Journal of Southeast Univesity, 2007,37:26-28.

[2] 刘邦明,邬浙艳,孙黉杰. SSDT挂钩:基于Windows内核的RootKit技术样本[J]. 网络安全技术与应用,2009(3):62-64.

[3] 谭文,杨潇,邵坚磊. 寒江独钓:Windows内核安全编程[M]. 北京:电子工业出版社. 2009:90-99.

[4] LACOSTE M, JARBOUI T, HE R. A component-based policy-neutral architecture forkernel-level access control [J]. Annales Des Telecommunications - Annals of Telecommunications, 2009, 64:121-146.

(下转第137页)

浅显易懂的方式讲授,循序渐进地让学生接受这些难以理解的概念及思想方法.

参考文献:

[1] 左孝凌,李为监,刘永才. 离散数学[M]. 上海:上海科技文献出版社,2001.

[2] 耿素云, 屈婉玲, 张立昂. 离散数学[M]. 北京:高等教育出版社, 2008.

[3] 傅彦. 离散数学基础及应用[M]. 成都:电子科技大学出版社. 2000.

[4] 孙吉贵,杨风杰, 欧阳丹彤,等. 离散数学[M]. 北京: 高等教育出版社. 2002.

[5] KENNETH A R, CHARLES R B. Discrete Mathematics (Fifth Edition) [M]. 北京:清华大学出版社, 2003.

[6] 吴明芬, 汪立民. 代数系统中的数学思想及同构(同态)的初等诠释[J]. 计算机科学,2010, 37(7), 15 - 19.

[7] 许蔓苓. 离散数学的方法与挑战[J]. 计算机研究与发展. 2002, 39(12):1771 - 1772.

[8] 李梅霞. 离散数学中关系性质的判定方法[J]. 大学数学, 2010, 26(5) 203 - 206.

[9] 李小梅. "离散数学"中代数理论教学的处置[J]. 赣南师范学院学报. 2000(3):75 - 76.

[10] 崔艳荣, 陈勇, 黄艳娟. 离散数学教学方法与手段探[J]. 长江大学学报, 2009, 6(2):373 - 374.

[11] 薛占熬, 肖运花, 杜浩翠,等. 论 " 双主"在离散数学教学过程中的作用[J]. 计算机教育, 2011, 18: 37 - 40.

[12] 刘卫锋,刘 林,王东晓,等. 数学文化融入离散数学的教学研究[J]. 计算机教育, 2011(6):52 - 55.

[13] 吴明芬,张先勇. 应用驱动激发离散数学课程的学习兴趣和动力[C]. 大学计算机课程报告论坛论文集. 北京:高等教育出版社, 2009:281 - 285.

[14] 朱家义, 苗国义,梁云娟. 基于知识关系的离散数学教学内容设计[J]. 计算机教育, 2010(18):98 - 100.

Closure Concepts and Applications in Discrete Mathematics

WU Ming-fen, QU Yun-yun

(School of Computer Science, Wuyi University, Jiangmen 529020, China)

Abstract: We make a thorough inquiry about the concepts in discrete mathematics based on the amplification and minimum features of the closure. We collected some explicit concepts and implicit concepts of closure from discrete mathematics such as closures of binary relation、strong part graph、subspace、sum subspace、generating subgroup and so on. Trying to format the teaching of these concepts and procedure standardization in the framework of the closure. At the same time, we introduce our teaching programs and techniques. Finally, the thinking of relationship transitive closure is applied to the algorithm design of the shortest path and Euler roads.

Key words: closure; binary relation; subspace; undirected graph; connected graph; generating subgroup; shortest path

(上接第 132 页)

Research and Implementation of Security Reinforced XPE

GUO Yu-yan

(Library, Henan University of Economics and Law, Zhengzhou 450002, China)

Abstract: Operating system security has attracted the attention of researchers since the very beginning. How to build a secure operating system has become a hot topic of current research. Based on trusted computing and active host protect, we designed and realized the system with kernel mode protection that provides functions such as Trusted boot, Process starts protect, and Network access protect. Besides, it provides mandatory access control of critical resources.

Key words: security reinforcement; XPE; USBKEY; TPM; MAC