基于国产安全操作系统的集中存储管控系统①

王 涛[1], 党翠芳[1], 任 启[2], 高洪鹤[2]

[1](北京跟踪与通信技术研究所, 北京 100094)
[2](湖南麒麟信息工程技术有限公司 北京 100089)

摘 要: 主要介绍以国产安全操作系统为运行环境的集中存储管控系统的研究与设计, 系统通过运用"沙箱"、多因素增强身份认证、数据集中加密存储、负载均衡等核心技术, 实现对用户文档的安全加密、数据集中存储、终端安全管理、外设封控管理及日志全面审计功能, 以达到针对特殊目标用户数据灵活、安全、高效的集中存储管控策略控制.

关键词: 国产安全操作系统; 沙箱技术; 数据安全

Centralized Storage Management and Control System Based on Domestic Secure Operating System

WANG Tao[1], DANG Cui-Fang[1], REN Qi[2], GAO Hong-He[2]

[1](Beijing Institute of Tracking and Telecommunications Technology, Beijing 100094, China)
[2](Hunan Kylin Information Engineering Technology Co.,LTD, Beijing 100089, China)

Abstract: This essay focuses on introducing the study of centralized storage management and control system based on domestic secure operating system, by employing core technologies of sandbox, multi-factors intensifying ID authentication, data storage with centralized encrytion, load balancing, etc. It can realize the functions of secure encryption of users' files, centralized storage of data, Terminal Security Management, peripheral Traffic control management and log comprehensive audit function, through a flexible, secure and efficient centralized storage and management strategy control aiming at special targeted users will be achieved.

Key words: domestic secure operating system; sandbox technology; data security

人们在享受信息化建设带来便利的同时, 因计算机/网络而引发的信息安全和数据安全问题也受到了越来越广泛的关注.

2013 年"斯诺登事件"的爆发, 披露的很多鲜为人知的敏感数据让人不寒而栗, 人们不得不重新审视安全问题. 信息化和大数据环境下的安全防护仅仅依靠防止黑客攻击、网络窃听、病毒感染、漏洞后门入侵等常规手段并不足以遏制安全问题的发生, 无法有效阻断敏感数据的泄露. 从"被动防御"到"主动预防"的安全角色转换势在必行, 必须从源头建立起数据加密防护的关键防线.

在基础操作系统方面, 根据市场研究公司 Net Applications 在 2015 年 6 月的最新数据, 微软的 Windows 系列操作系统作为主流占有大量的市场份额, 如图 1.

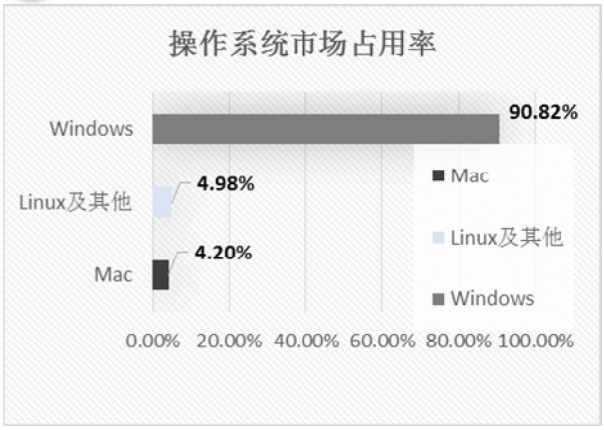

图 1 全球操作系统市场份额

① 收稿时间:2016-02-19;收到修改稿时间:2016-03-31 [doi: 10.15888/j.cnki.csa.005405]

但由于该系统为微软独立开发设计，整套系统具有极大的封闭性，而且完全受控于美国微软公司，在系统维护和升级方面存在安全隐患.

① 2009 年 4 月 8 日，微软在全球停止对 Windows XP 系统的主流支持服务[1];

② 2014 年 4 月 8 日，微软在中国终止对 Windows XP SP3 系统的主流支持服务;

③ 2015 年 1 月 13 日，微软将不再对 Windows 7 提供主流支持服务.

作为商业化公司，微软对非主力版本操作系统的停止服务意味着因使用 Windows 操作系统带来的安全风险随之攀升，引起了社会和广大用户的广泛关注和对信息安全的担忧. 一旦操作系统后门被激活，那么所有使用 Windows 操作系统的用户都将可能受到不可估量的影响.

近年来，在国家科技攻关计划、863 计划、信息产业部电子发展基金及军队科研等支持下，我国在核心操作系统领域取得了巨大的突破：服务器操作系统已突破垄断进入市场；桌面操作系统基本可用. 国产化操作系统的成熟度和取得的巨大成果为我国操作系统逐步替代 Windows 的自主解决方案提供了前提.

其中，由国防科学技术大学自主研发的银河麒麟操作系统采用安全内核与密码机制[2]深度融合技术、增强身份鉴别技术、细粒度自主访问控制技术构建了具有了一体化安全防护体系；同时采用加密文件系统、角色定权等特色安全机制令整体运行环境的安全性得到进一步巩固.

若要真正实现终端计算机环境安全，除了把国产操作系统作为基础运行环境之外，还需借助一套完整的桌面防护体系.

本次研究的目标核心就是综合运用“沙箱”、数据集中加密存储、负载均衡、系统监控等多种技术，达到数据从用户到桌面再到服务器的三层端到端安全集中存储管控的最终效果. 如此才能彻底摆脱前述安全性风险、避免对 Windows 操作系统的依赖，形成具有完全自主可控的集中存储管理系统解决方案. [3]

1 研究目标

在数据存储一般不脱离计算机主体的情况下，运行环境的安全才能有效保障其数据的安全，集中存储管控所涉及的计算机运行环境必须解决以下问题:

1) 安全操作系统. 操作系统是运行各类服务和应用的平台，要求操作系统在一定程度上具有访问控制、安全内核和系统设计等安全功能.

2) 信息加密技术. 信息加密技术是保障数据安全的最重要和最基本的技术措施，敏感信息的有效加密对于意外丢失或人为盗窃后造成的损失能以最少代价获得最大程度的安全防护.

3) 身份认证技术. 数据的使用要求通过严格确认信息的来源和去向，以及其所有者和接收者的权限范围. 对用户的身份认证除了使用常规的数字身份认证方法外还要保证以数字身份进行操作的操作者必须有相对应的合法物理身份.

4) 网络封控技术. 数据的安全传输、文件的使用必须得到可授信的认证过程，避免数据被篡改和盗窃.

5) 审计技术. 数据的使用，系统应该具备完善的记录用户访问记录、系统运行日志、系统运行状态等各类信息，并能经过规范化、过滤、归并和告警分析等处理后，以某种统一格式的日志形式进行集中存储和管理.

2 系统设计

集中存储管控系统的设计采用完全模块化的设计理念，在以麒麟国产安全操作系统为基础框架的基础上为用户提供安全身份认证、数据集中加固管理、终端安全管理的功能.

2.1 系统框架设计

系统总体设计框架如图 2 所示.

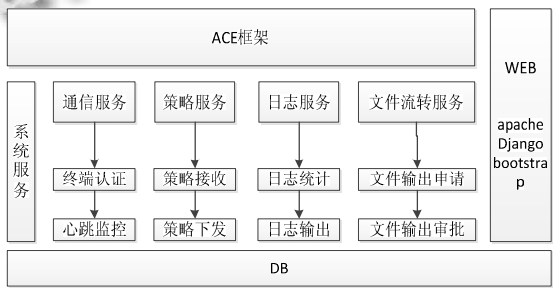

图 2 系统设计框架

系统采用 ACE 设计框架(Adaptive Communication Environment 自适配通信环境)，在国产操作系统运行环境之上构建通信服务、策略服务、文件流转服务以及日志服务，通过一系列关键技术的支撑实现了数据从用户到桌面再到服务器的三层安全管控的最终效

果.

2.2 系统模块设计

2.2.1 多重文件安全保护

考虑到数据对于用户的重要性, 系统设计的核心围绕可信身份鉴别以及文件密钥、保险箱公私钥、用户公私钥三级密钥管理机制[4]对文件进行多重安全保护展开. 其中身份鉴别用于对用户的可信身份予以确认、文件密钥用于加解密文件、保险箱公私钥用于加解密文件密钥、用户公私钥则用于加解密保险箱私钥.

用户认证参考国际上通用的方法处理, 采用专用加密安全通道来对通信内容进行加密. 加密协议位于TCP/IP 协议与各种应用层协议之间, 为数据通信提供安全支持. 加密协议在应用层通信之前就已经完成加密算法、通信密钥的协商以及服务器认证工作. 在此之后应用层协议所传送的数据都会被加密, 从而保证通信的保密性.

身份认证支持智能卡方式的双因子认证和口令认证. 智能卡的编程遵循标准接口规范实现, 可移植性高; 用户的私钥不出智能卡. 简要认证流程如下:

1) 和服务器建立 TCP 连接.

2) 验证服务器发过来的公钥证书.

3) 加密握手协议负责建立当前会话的参数.

服务器管理软件启动并通过认证后, 首先从服务器获取用户信息、共享组信息、主机信息, 然后解析并验证其完整性和正确性, 若验证通过, 则将相应信息以可读、友好的方式清晰的呈现在管理员操作界面上, 否则报告错误信息.

针对用户的每一个文件, 系统通过 Hash 产生一个随机值作为文件密钥. 由于随机值的不同, 可以保证实现一文一密, 而系统就使用该文件密钥作为加密该文件的对称密钥. 同时, 系统会生成一对保险箱公私钥和一对用户公私钥, 其中保险箱公钥用来加密文件密钥, 而保险箱私钥则使用用户公钥来加密.

2.2.2 终端安全管理[5]

在银河麒麟安全操作系统中, 对所有设备的操作都会对应到一个文件, 如 read、write、ioctl 等操作首先要打开该文件, 然后再调用相关系统调用. 因此, 对外设的封控可以通过截获对设备的这类系统调用来实现. 如禁止刻录光驱的使用, 可通过截获刻录光驱的 open 操作, 对该调用进行阻断, 来实现禁止刻录光驱使用的目的.

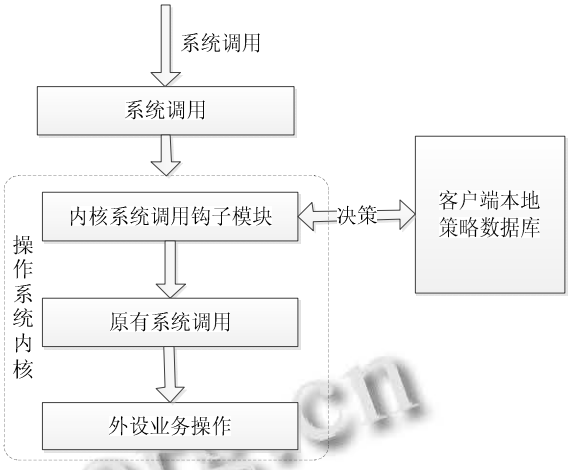

图 3 终端安全管理原理图

此次研究过程中, 有效利用银河麒麟操作系统的处理机制, 通过操作系统的公共接口对终端用户的设备等进行有效管理. 当请求外设进行操作时, 首次触发相关系统调用, 而内核系统调用钩子模块会截获此类调用, 并通过查询客户端本地策略数据库进行决策, 如果本地策略数据库中指定该设备不可执行该操作, 则阻断该调用, 否则予以放行, 继续执行后续业务.

2.2.3 网络安全管理

网络管理利用 netfilter 框架实现[6]. netfilter 框架在内核 TCP/IP 协议栈上选择了 5 个卡哨(pre_routing、forward、post_routing、local_in 和 localout), 这 5 个卡哨是报文必将流经的位置, 对应提供了 5 个 hook 函数; 当有报文经过时, 对应卡哨的钩子函数会被执行, 以达到对流入、流出和流经本机的报文进行过滤和处理的目的.

系统增加一个网络管理组件, 在内核构建一个策略“数据库”, “数据库”的内容在用户登录时根据服务器指定策略设置, 通过检测策略数据库规则, 达到 IP 控制、网络端口控制的目标.

2.2.4 集群负载均衡[7]

针对大范围用户的使用场景, 必须对系统服务器实现高效的集群负载均衡机制, 一方面提升系统可靠性, 一方面提高系统的可用性.

集群负载均衡技术有多种实现模式, 如 VS/NAT(Virtual Server via NAT)、VS/TUN(Virtual Server via IP Tunneling)、VS/DR(Virtual Server via Direct Routing)等, 结合各种模式的特点及应用场景, 最后采用 VS/DR(直接路由)工作模式. 在直接路由模

式中, 负载均衡服务将用户的请求调度到集中存储管控软件, 集中存储管控软件直接将响应返回给用户, 而不需经过负载均衡系统. 集中存储管控软件的网络连接一般都是长连接, 在调度算法上选用最少链接(Least Connections)算法: 调度器动态地将网络请求调度到已建立的链接数最少的服务器上.

在正常情况下, 由负载均衡服务 1 作为主节点提供负载均衡服务. 而负载均衡服务器 2 作为备用节点通过心跳服务来实时检测主节点是否出现故障. 当主节点出现故障, 负载均衡服务无法正常运转时, 这一状态将被备用节点实时监控到. 备用节点将立刻启用本机的负载均衡服务来替代主节点. 此时所有的集中管控应用请求将由备用节点来实现负载均衡调度, 用户终端并不会感知调度服务的转移.

2.2.5 日志管理[8]

日志子模块提供系统运行状态的记录、用户行为的审计日志记录、审计日志检索等功能, 这些功能强化了整个系统的安全性和可调试性. 日志模块包括运行日志子模块和审计日志子模块.

1) 运行日志

运行日志子模块对管控系统本身的运行情况进行记录, 这些日志以特定格式存储到文件系统中; 以时间为顺序进行记录, 供给系统开发和维护人员进行产品改进和排除故障; 系统还支持对这些日志进行定时转储, 避免日志文件过大.

运行日志子系统遵循日志框架标准, 分别定义日志 ID、配置文件、日志必要项等, 日志 ID 定义日志基础要素, 配置文件定义日志开关及输出日志类型, 日志必要项定义日志详细内容. 系统开发及维护人员通过查看运行日志来对系统进行分析和改进.

2) 审计日志

审计日志子模块对用户使用管控系统的各种事件进行记录, 并将日志以特定格式存储到数据库. 审计日志检索引擎响应管理员发出的检索日志请求, 从数据库中检索符合指定条件的日志并返回给调用者.

审计日志要素应该包括记录 ID、事件主体、事件客体、事件内容、事件结果、发生时间、事件种类等要素; 管理员可在 WEB 管理界面指定根据“时间、用户名、事件类型”等类检索条件对日志进行检索来进行审计查询.

审计日志要素	字段	别名	描述
	Log	审计日志	从此处开始为审计日志信息(XML 节点名)
记录 ID	LogID	日志 ID	填写审计日志的 ID
事件主体	Node	主体 IP 地址	填写 IP 地址
	NodeID	主体 ID	填写主体 ID, 采用主板号附件硬盘号的方式命名
	UserName	用户名	1)如果是管理员操作日志, 应填写管理员的账号; 2)如果是用户操作日志, 经过身份鉴别后应填写用户名, 否则为空或缺省值, 或者是某种责任人
事件客体	Object	事件客体	事件客体一般是指文件、目录、设备、网络等资源, 当事件主体在一次审计事件中完成对多个客体的操作行为时, 应在审计日志中记录所有事件客体的唯一身份信息.
事件种类	Type	事件种类	1)管理员操作日志为‘m’(manage); 2)用户操作日志为‘a’(audit); 3)其他日志为‘s’

2.3 系统指标

实验室环境说明:

序号	设备类型	参数
1	集中存储管控系统服务器*2	CPU: 1*Intel Xeon 2.4GHz 内存: 1*8GB 硬盘: 1*2TB 网络: 2*RJ45 千兆网口
2	集中存储管控系统客户端计算机*10	CPU: 1*Intel i5 2.5GHz 内存: 1*4GB 硬盘: 1*1TB 网络: 1*RJ45 千兆网口
3	集中存储管控系统服务器平台软件*1	1) 支持安全身份认证模块; 2) 实现文档集中加密存储; 3) 提供可靠的终端封控技术, 强制加载终端安全使用环境;

		4) 能对终端入网、端口、进程、网络行为等均具备细粒度管理措施; 5) 具备全面终端和文档操作安全审计机制;
4	操作系统*12	麒麟国产安全操作系统 V3
5	交换机	24 口全千兆网络交换机

在实验室环境下搭建 10 用户并发的实验模拟环境, 在实验室环境中展现效果如下:

(1) 可信用户进入到集中存储管控环境下, 原有本地磁盘通过沙箱技术被屏蔽不可见, 同时针对每个用户发布一个网络磁盘, 用户所有文件都只能存储在网络磁盘中;

(2) 用户在集中存储管控环境下插入普通U盘提示“未注册, 禁止使用”; 访问白名单以外的网站提示“未被授权许可访问, 连接终止”; 刻录文件时提示“该光驱为只读, 请选择可读写光驱”;

(2) 管理员登录后台存储查看用户数据, 借助于三级密钥管理机制, 因为是非授权用户, 显示为乱码;

(3) 管理员直接将文件拷贝到其他终端, 借助于三级密钥管理机制, 因为是非授权用户, 显示为乱码;

(4) 同时启动 10 用户, 每台服务器负载 5 用户; 关闭任意一台服务器, 有 5 用户显示离线状态, 重启用户终端设备后, 10 用户全部负载到正常运行的服务器上;

(5) 下发 IP 与端口控制的网络行为策略, 限制用户的网络访问行为, 功能生效;

3 结语

通过研究设计与实验室原型软件测试, 利用基于麒麟安全操作系统集中存储管理方式可以有效保障信息安全、数据安全; 全面对用户数据操作行为进行安全保护, 这相对于在非受控的 Windows 系统下对敏感数据防护的产品设计有了质的提高.

由于缺少复杂的实验室环境, 该系统设计模型中只是基本阐述了技术可实现方式, 并未涉及不同业务场景的应用模式, 为了满足不同用户的不同需要, 可以此模型作为基础继续扩展, 从而满足更广泛的市场需求.

参考文献

1 赵宪华,崔传文,李成龙.操作系统的国产化探讨.计算机科学,2014,(24):200.
2 吴庆波,戴华东,吴泉源.麒麟操作系统层次式内核设计技术.国防科技大学学报,2009,(2):80–84.
3 王凯,王晖.一种基于国产基础软件平台的软件部署方案.计算机与现代化,2014,(1):5–9.
4 孙萍萍.应用三级密钥管理体系实现 Client/Server 安全通讯.研究与开发,2004,(6):72–74.
5 饶炜,卢桂强.基于终端安全管理的企业内网设计与应用.软件导刊,2014,(11):111–112.
6 黄晓辉,周定康,许东海.Linux 网络安全架构 Netfilter 的分析和探讨.计算机与现代化,2008,(3):55–58.
7 吴书华.基于麒麟操作系统的双机热备系统的设计与实现[硕士学位论文].长沙:国防科学技术大学,2006.
8 李锦川,钱秀槟,方星,等.基于国产操作系统的网络日志管理系统构建.计算机安全,2010,(10):59–60.