TRSF:一种移动存储设备主动防护框架

马 俊,王志英,任江春,刘 聪,伍江江,程 勇,梅松竹
(国防科技大学计算机学院,湖南长沙 410073)

摘 要: 移动存储设备属于被动设备,其安全防护往往依赖于终端系统的安全机制,在提供安全性的同时会降低系统可用性.本文提出了一种基于可信虚拟域的移动存储设备结构框架 TRSF(Trusted Removable Storage Framework)实现存储设备的主动防护.TRSF 将智能卡芯片和动态隔离机制绑定到存储设备中,并由片上操作系统构建从底层可信平台模块到隔离运行环境的可信数据通道,从而为移动存储设备在非可信终端系统中被非可信进程访问和使用提供一个可信虚拟环境.最后基于 TRSF 实现了一款主动安全 U 盘 UTrustDisk.与没有增加主动防护机制相比,增加该机制导致平均读写性能开销分别增加了 7.5%和 11.5%.

关键词: 可信虚拟域; 主动防护; 可信存储; 信任链; 隔离; 片上操作系统
中图分类号: TP309.2 **文献标识码:** A **文章编号:** 0372-2112 (2012) 02-0376-08
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2012.02.027

TRSF: Implementing Active Removable Storage Protection via Trusted Virtual Domains

MA Jun, WANG Zhi-ying, REN Jiang-chun, LIU Cong, WU Jiang-jiang, CHENG Yong, MEI Song-zhu
(*School of Computer, National University of Defense Technology, Changsha, Hunan* 410073, *China*)

Abstract: As removable storage medias are passive devices, their security policies depend on mechanisms in connected terminal systems, which will reduce the availability while providing security. This paper presents TRSF, a framework of removable storage based on trust virtual domain to implement active protection. TRSF solidifies a smart card and an isolation mechanism into the storage device and builds trust data channels from the device to the isolated usage environment in terminal system. So TRSF is able to provide trust virtual environment for data access and usage of removable storage even in untrust terminal systems by untrust processes. We implement an intelligent USB disk based on TRSF called UTrustDisk to evaluate the framework. The average overhead on read and write caused by trust chain mechanism is 7.5% and 11.5%.

Key words: trusted virtual domains (TVDs); active protection; trusted storage; trust chain; isolation; chip operation system (COS)

1 引言

目前移动存储介质不仅面临木马病毒窃取等外部威胁,还要应对内部授权人员主动泄漏和误操作等内部威胁.很多企业为防止数据泄漏采取了各种保护策略,如磁盘加解密[1,2]、USB 端口控制[3,4]以及设备认证管理[5,6]等.国家和军队也针对移动存储介质保密防护的管理和使用做出了明确规定.这些策略和规定在一定程度上保证了移动存储介质的使用安全,但通常会因为限制过于严格而导致可用性和灵活性的降低.这是由于移动存储介质属于被动设备,其安全性需要终端系统中安全机制的支持.因此,如何在保证灵活性的前提下,提高移动存储介质的安全性,是当前急需解决的关键问题.

为此,研究者将一部分数据处理和安全控制功能集成到存储设备中以增强存储设备的主动性,提出了主动存储[7]、智能存储[8]和自安全磁盘[9]等概念.国内靳超[10]和谢雨来[11]等重点基于面向对象方法实现主动存储,赵跃龙[12]则研究了以虚拟存储映射方式实现的网络智能磁盘.这些研究主要侧重提高存储设备在数据计算和管理的主动性,而较少考虑计算机终端的应用环境和进程对数据的使用是否可信.TCG 组织发布的可信存储(Trusted Storage, TS)规范[13],以可信计算平台模块 TPM 为信任根,确保数据只能被可信主体访问和使用.徐明迪[14]和汪丹[15]分别提出了基于可信计算的存储

收稿日期:2010-12-21;修回日期:2011-04-25
基金项目:国家自然科学基金青年基金(No.60903240);核高基重大专项(No.2010ZX01045-001-002-5)

和数据封装方案.但可信存储基于可信主体不会主动泄漏数据的假设,难以防止可信主体泄密.

近年来,针对可信主体主动泄密和非可信软件的安全控制问题,研究者将可信计算与虚拟化技术结合提出了可信虚拟域(Trusted Virtual Domains,TVDs)[16]的概念.TVDs 是借助于虚拟机(Virtual Machine,VM)构造程序的隔离运行环境,并通过交互式可信计算基(Mutually-Trusted Computing Base,MTCB)[17]建立不同隔离环境之间的可信连接,从而为敏感数据提供透明可信的访问环境.这种基于硬件层虚拟机的实现,侧重提供的是一种服务式的执行接口(Execution Entities,EEs),比较适合于分布式服务应用中的数据保护,而对于终端及移动存储中的数据保护,这种方式开销较大[18].Catuogno[18]将 TVDs 应用于移动存储设备的安全保护,通过集中管理为不同存储设备构建可信虚拟域.但存储设备不能脱离当前管理环境,主动性有限.艾丽华[19]从网格虚拟机视角提出了针对数据网格环境的动态存储体系的层次结构.Yang Yu[20]在其博士论文中设计实现了一种轻量级的虚拟机 FVM,通过系统调用的监控和重定向,为进程提供一个隔离的运行环境.FVM 在保持良好隔离性的同时,具有更小的时间和性能开销,因此适合用于构建针对终端和移动存储应用的 TVDs.

本文基于 FVM 构建系统级的 TVDs,并将其应用于移动存储设备的实现结构中,提出了一种具有主动防护能力的可信移动存储框架(Trusted Removable Storage Framework,TRSF).TRSF 将 TVDs 和可信平台模块一起固化到移动存储设备中,由存储设备中的嵌入式系统实现对 TVDs 的管理和可信认证.在存储设备接入终端系统时,TRSF 通过可信启动机制在终端系统中构建相应的 TVDs,并通过可信互连过程建立 TVDs 与存储设备之间的可信数据通道.授权访问移动存储设备的进程必须在 TVDs 内使用获取的数据.因此不论是具有固定授权的可信进程还是获取临时授权的非可信进程,都不能将存储设备中的数据泄漏出去.最后基于 TRSF 实现了一款可信的主动安全 U 盘 UTrustDisk.

2　TRSF 框架

TRSF 通过可信机制在终端系统中建立与存储设备对应的 TVDs,为访问存储设备的进程提供可信的执行环境.图 1 给出了 TRSF 的框架示意图.

在 TRSF 框架下,可信移动存储设备(Trusted Removable Storage,TRS)中集成了 TPM 模块、TVDs 管理器和数据访问接口.其中 TPM 模块既是数据可信存储的信任根,也是构建从物理存储到 TVDs 信任链的可信度量根;TVDs 管理器对 TVD 的创建、运行以及权限进行管理,并完成信任链的构建;数据访问接口对数据访问进行控制,包括身份认证、权限验证以及数据封装和解封装等功能.

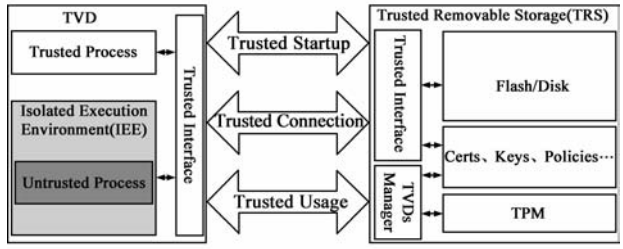

图1　可信移动存储框架

TVD 是从硬件中启动并在终端系统上构造的可信虚拟环境,主要包括可信进程、可信通信接口和隔离运行环境(Isolated Execution Environment,IEE).其中可信进程在本文中专指运行在终端系统中并负责 TVD 管理维护和用户身份认证的代理程序.除可信进程之外的所有访问 TRS 的进程都认为是非可信进程.可信通信接口负责 TVD 与 TRS 的可信通信,包括管理控制接口和数据传输接口.非可信进程获取 TRS 中数据后,只能在 IEE 的控制下使用,所有企图泄漏数据到 TVD 之外的操作都被严格控制:如果是向网络或者 TVD 之外的进程发送数据,操作被禁止;如果是向 TRS 以外的磁盘中的文件写数据,操作将被重定向到 TRS 中.

在此基础上,TRSF 着重解决了以下关键问题:(1)TVD 的可信启动(Trusted Startup);(2)TVD 与 TRS 之间的可信互连(Trusted Connection);(3)TVD 的管理及数据使用策略的实施,即数据的可信使用(Trusted Usage).

2.1　可信启动

TVD 的可信启动包含三个主要过程:

(1)TRS 中固化有可以在终端系统中执行可信启动的代理程序.该代理程序的存储区域对终端系统是只读的,从而保证代理程序的完整性.通常该区域以只读光盘分区的形式存在.TRS 接入终端计算机之后,该程序由用户手动启动或者通过系统自动运行方式启动.

(2)可信进程启动之后,需要验证用户身份和环境信息,包括操作系统平台信息和硬件平台信息等.验证通过才能启用存储设备中的数据访问接口.

(3)可信进程与 TVDs 管理器通信,获取相应的策略权限,并在终端系统中构建对应的 IEE.该过程中,TVDs 管理器通过 TPM 模块验证 IEE 对应镜像文件的完整性,并为 IEE 构建提供可信验证,确保 IEE 的可信.TVD 权限管理和 IEE 完整性度量值的存储策略将在 2.3 节详细介绍.

2.2　可信互连

可信互连是要保证 TRS 只能与对应的 TVD 之间建立连接.虽然可信进程对应的代理程序和 IEE 镜像是物

理固化在 TRS 中,但是在终端系统中运行之后 TRS 无法判断连接请求的来源.徐明迪[14]的可信存储结构通过出厂证书和平台证书进行双向验证,建立主机与存储设备之间的可信互连.这种可信互连主要是验证授权,由于证书的可复制性,主机与存储设备并不是绑定在一起的.而 TRSF 则需要实现 TVD 与 TRS 的绑定.

TRSF 的可信互连机制基于 RSA 的非对称加解密体系实现:代理程序的 RSA 密钥对记为公钥 $PubKey_{tvd}$ 和私钥 $PrvKey_{tvd}$,TRS 的 RSA 密钥对分别为公钥 $PubKey_{trs}$ 和私钥 $PrvKey_{trs}$.$PubKey_{tvd}$、$PrvKey_{tvd}$ 和 $PubKey_{trs}$ 直接以缓冲数组的形式保存于代理程序的源代码中,编译后即固化到程序中.而 $PubKey_{tvd}$、$PubKey_{trs}$ 和 $PrvKey_{trs}$ 存储在 TPM 芯片中的可信区域.基于非对称密钥对的双向认证过程如图 2 所示.

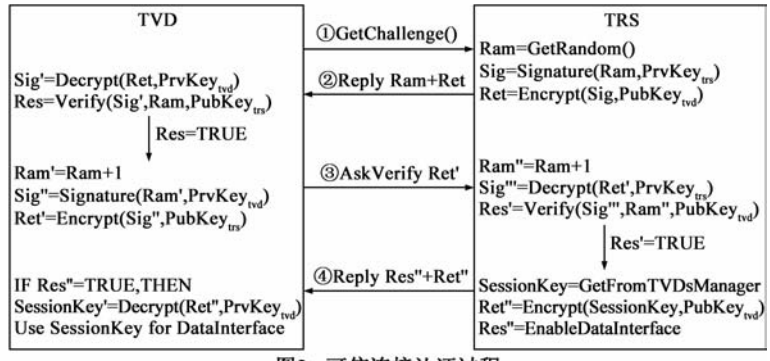

图2 可信连接认证过程

(1)TVD 对 TRS 的认证过程

TVD 中的可信进程向 TRS 发送挑战请求 GetChallenge,TRS 产生一个随机数 Ram,并使用 TRS 的私钥对 Ram 签名,然后使用 TVD 的公钥对签名数据进行加密得到 Ret,最后将 Ret 与 Ram 一起返回给可信进程.可信进程首先使用 TVD 的私钥对 Ret 进行解密得到 Sig′,然后使用 TRS 的公钥验证 Sig′是否是 Ram 的签名.如果验证通过,则完成 TVD 对 TRS 的认证.

(2)TRS 对 TVD 的认证过程

在完成 TVD 对 TRS 的认证之后,可信进程将 Ram 加 1 得到 Ram′,然后使用 TVD 的私钥对 Ram′进行签名,得到 Sig″,再用 TRS 的公钥对 Sig″进行加密得到 Ret′.可信进程将 Ret′发送给 TRS 进行验证.TRS 将原来产生的随机数 Ram 加 1 得到 Ram″,并用自己的私钥对 Ret′解密,得到 Sig‴,然后使用 TVD 的公钥验证 Sig‴是否是 Ram″的签名.如果验证通过,则完成 TRS 对 TVD 的认证.

完成 TRS 对 TVD 的认证之后,TRS 通过 TVDs 管理器获取 TVD 与 TRS 之间进行数据传输时使用的加解密密钥 SessionKey,并使用 TVD 的公钥加密得到 Ret″,然后启用存储访问的接口,并将启用结果与 Ret″一起返回给 TVD.如果 TRS 已经启用存储访问接口,TVD 在收到结果之后,使用 TVD 私钥解密 Ret″得到 SessionKey′,然后将 SessionKey′配置到数据通信接口中.其中加解密密钥的管理策略将在 2.3 节中详细介绍.

在 TRS 对 TVD 进行认证的过程中,可信进程将收到的随机数加 1 后进行签名,而 TRS 验证时使用之前传送给 TVD 的数值,这样可以防止恶意进程劫持中间数据进行重放攻击.

2.3 可信使用

TVD 与 TRS 建立可信连接之后,还需要灵活策略支持 TVD 中进程对文件的使用权限.汪丹[15]基于可信虚拟平台的数据封装方案中,使用虚拟平台配置寄存器 vPCR 存储每个虚拟机实例的完整性度量值,并由 Dom0 维护 vPCR 与密钥槽的关联.在 TRSF 中,每个 TVD 需要同时考虑完整性度量值、权限和数据加解密密钥的管理.因此,本文在汪丹提出方案的基础上,将每个虚拟机实例抽象为 TVD,并由 TVDs 管理器替代 Dom0 完成相应的管理维护功能.扩展后的关键资源分布如图 3 所示.

每个 TVD 对应的权限策略文件保存在只读存储区域,并由 TVDs 管理器进行统一管理.可信进程在启动 TVD 时与 TVDs 管理器通信,根据对应 vPCR 的完整性度量值对 IEE 镜像和安全属性进行验证,通过验证后则从对应的权限文件中获取控制权限,在 TVD 运行时进行配置.在完成 TVD 与 TRS 的双向认证之后,根据对应关系获取数据加解密的密钥,并配置到存储访问接口中.

3 TRSF 实现

近年来将智能卡与移动存储设备结合进行安全性

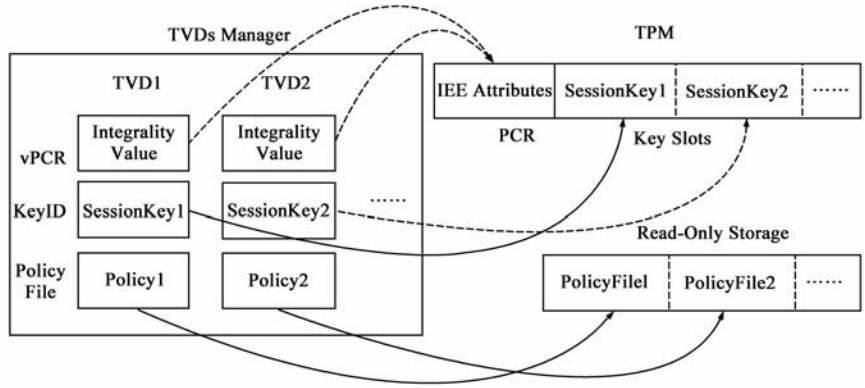

图3 关键资源分布图

增强成为一种趋势.如吴世忠[21]将智能卡与 U 盘结合构造的复合设备、SanDisk[22]推出的 U3 智能盘、以及国民技术针对移动存储安全推出了安全 KEY 盘 Armordisk[23].这些解决方案利用智能卡及运行在智能卡上的片上操作系统(Chip Operation System,COS)提供硬件层的加解密,并通过集成口令验证软件实现用户口令验证.但是,用户一旦通过口令验证,磁盘中的数据访问将不再受保护,可能被木马访问窃取.本文则是在 TRSF 框架基础上,通过在移动存储设备中集成主动防护模块,由主动防护模块在终端系统中动态构建用于限制访问磁盘数据的虚拟隔离环境,并基于安全芯片提供的签名验证机制实现从存储设备到隔离环境的信任链.最后实现了一个具有主动防护能力的安全 U 盘 UTrustDisk.

3.1　体系结构

UTrustDisk 的体系结构如图 4 所示.

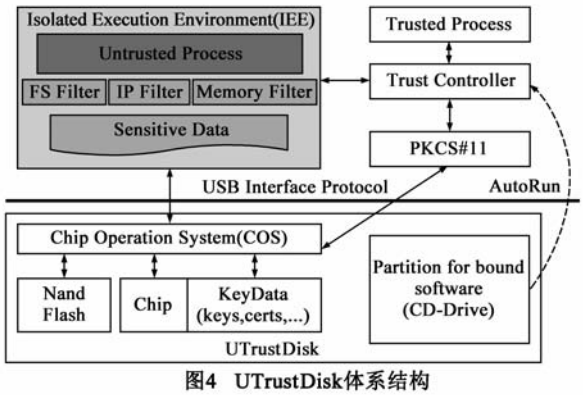

图4　UTrustDisk体系结构

UTrustDisk 硬件结构中,固化了一个只读的光盘分区,用于保存可信进程对应的代理程序和构建 TVD 的程序镜像文件.光盘分区结构及其存储的内容在设备出厂设置时进行初始化,并通过增加 AutoRun.inf 在 UTrustDisk 接入终端系统时自动运行代理程序.智能卡提供加解密和签名验证等安全功能,并将片内的永久存储空间以文件形式组织,用于保存 TVD 的完整性度量值、密钥和安全策略等.智能卡中运行的嵌入式操作系统负责实现 TVDs 的管理以及与终端系统层的安全通信接口.

代理程序通过自动或者用户手动运行后,通过 PKCS#11[24]通信库与 COS 进行通信,完成用户身份验证和对应 TVD 的完整性验证.其中 PKCS#11 是 RSA 实验室针对智能卡等加密设备的安全通信而推出的密码令牌接口标准,它基于会话和对象模型提供密钥访问的安全性[25].可信控制器模块(TrustController)是在 PKCS#11 的 API 接口基础上进行封装,为 IEE 提供安全的权限访问接口.

UTrustDisk 基于 TRSF 框架构建从底层硬件到上层应用的可信数据通道.其状态变迁过程如图 5.

图 5 中的五个状态代表了其使用过程中的关键节点.状态切换过程也对应信任链的构建.

(1)State0 到 State1 的状态切换对应 UTrustDisk 插入终端系统中,加电启动的过程.此时 COS 启动并进行自检,自检通过后加载只读的光盘分区;

(2)State1 到 State2 的状态切换对应光盘分区中固化的代理程序启动进行用户身份验证;

(3)State2 切换到 State3 时,代理程序在终端系统中构建对应的 TVD,并加载 UTrustDisk 对应的保护分区;

(4)State3 到 State4 的切换过程中,代理程序通过 PKCS#11 构建 TVD 与保护分区之间的加密数据通道,并获取智能卡存储中对应的 TVD 权限策略.

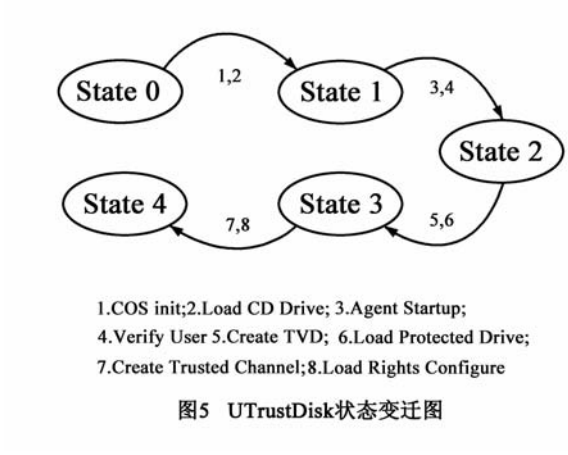

图5　UTrustDisk状态变迁图

3.2　TVD 及 TVD 管理器实现

现有 TVD 的研究主要基于硬件层的虚拟机系统实现[16~18],但这种虚拟机对于移动存储来说空间和速度开销都相对较大.国内的经略公司推出的口袋操作系统 PrayayaV3[26],将应用程序安装在移动存储设备中,并实现应用与系统盘的隔离.但是这种硬件层的虚拟机将数据和进程一起进行隔离,不能防止进程的主动泄密.谢均[27]通过操作系统内核层隔离实现了多保护域进程隔离机制.Weiqing Sun[28]实现的隔离文件系统通过重定向实现敏感文件与系统资源的单向隔离.Yang Yu[20]则在此基础上增加注册表和进程同步对象等系统资源的重定向,在操作系统层构造了一个轻量级虚拟机 FVM.

UTrustDisk 中的 TVD 即为在 FVM 基础构建的隔离执行环境 IEE,它将重定向路径定位在移动存储器中,同时增加权限控制.主要权限包括文件权限,网络权限,剪贴板权限和同步对象权限等.IEE 从网络、文件系统和内存相关 API 函数三个方面对进程运行环境进行隔离监控.对文件系统的监控主要通过文件过滤驱动(File System Filter Driver,FSFD)实现.FSFD 监控磁盘的

挂载和进程对磁盘文件的访问,如果有进程访问了UTrustDisk 对应磁盘分区中的文件,则建立该进程到UTrustDisk 的关联关系.此后进程对其他非 UTrustDisk 磁盘的写操作以及通过网络发送数据的操作都将被禁止.API HOOK 监控进程对剪贴板和其他内存的读写操作,并通过信息流关联模块查询进程是否关联到UTrustDisk.如果关联到 UTrustDisk 的进程对某块内存区域进行了写操作,没有关联到 UTrustDisk 的进程将不能对此区域执行读操作.

UTrustDisk 对 TVD 的管理主要借助于片上操作系统 COS 实现.COS 是 UTrustDisk 硬件中的核心部件,负责完成数据加解密管理、密钥对及证书管理、通信控制和安全运算等功能.所有与 UTrustDisk 通信的数据首先经过 COS 处理.根据 USB 数据包中结构判断数据请求的类型,并进行相应处理:(1) 对 KEY 的访问请求,则需要根据命令类型由命令处理过程进行执行;(2)对磁盘访问请求,首先要判断是否已经启用存储访问功能.如果没有启用,说明用户还未通过身份验证,不允许访问;如果已经启用,则提交给硬件加解密部件对数据进行加解密,然后再提交给底层磁盘.

4 系统测试与分析

本文借鉴国民技术的 Armordisk 的硬件体系结构,设计并实现了一个容量为 2GB 的 UTrustDisk,实现效果如图 6 所示.其中存储接口使用 USB2.0 协议,与 KEY 的通信基于 Mass Storage 协议.

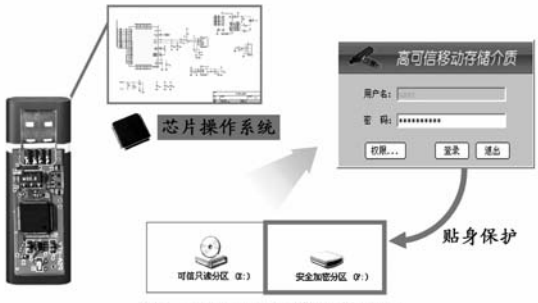

图6 UTrustDisk实现效果图

4.1 性能测试与比较

为测试性能影响,我们分别测试了启用 IEE 和禁用 IEE 时的读写速度,并与使用国民技术提供的原始 COS 时的速度做比较.

测试的硬件平台为:Intel(R) Pentium(R) 4 CPU 2.8GHz,RAM 1.0GB,硬盘 149GB.

测试的软件环境为:Windows XP SP3 及相关硬件驱动.测试工具为目前常用的可以进行 U 盘扩充检测和存储卡检测的工具 MyDiskTest V2.93[29].

MyDiskTest 的速度测试过程包括 9 个测试项目.由于 UTrustDisk 的泄漏防护,4KB 和 32MB 的文件复制测试不能进行.因此,本节对其他 7 项测试结果进行比较和分析.

表 1 是物理性能测试的结果.对表 1 中原始 COS 和禁用 IEE 的数据进行比较可以看出,单独增加可信认证会导致前段读写速度明显降低,而中段和后段的影响较小,这是由于可信认证时在挂载 U 盘和最开始访问 U 盘时进行.其中,读性能平均开销增加了 1.9%,写性能平均开销增加了 7.8%.

对表 1 中原始 COS 和启用 IEE 的数据进行比较可以看出,启用 IEE 对于前段的读写影响不大,而对后段的影响较大,这主要是由于 IEE 中访问文件历史链表增长会导致权限判断时间的增加.其中,读性能平均开销增加了 7.5%,写性能平均开销增加了 11.5%.

表 1 UTrustDisk 物理性能测试比较

位置		原始 COS	启用 IEE	禁用 IEE
前段(MB/s)	R	18.12	17.76	17.83
	W	4.87	3.98	4.27
中段(MB/s)	R	17.98	16.17	17.78
	W	7.05	6.39	6.58
后段(MB/s)	R	17.74	15.89	17.21
	W	6.82	6.22	6.42
平均(MB/s)	R	17.95	16.61	17.61
	W	6.25	5.53	5.76

为进一步分析 UTrustDisk 的读写性能,图 7 给出了 MyDiskTest 每次读取不同磁盘块数进行速度测试的结果比较.从图中数据可以看出,每次读取不同磁盘块数时增加可信认证和启用 IEE 对读写造成的性能损失基本与物理性能测试的规律一致,且读写的损失比例也都低于物理测试的结果.

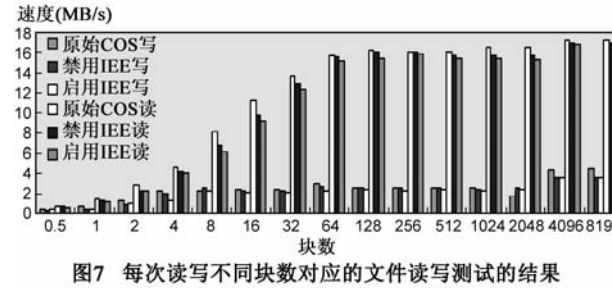

图7 每次读写不同块数对应的文件读写测试的结果

表 2 其余 5 项测试比较

测试项目		原始 COS	启用 IEE	禁用 IEE
空白文件创建(ms/file)		4.56	3.28	4.05
文件删除(ms/file)		5.03	4.06	4.58
32MB 文件创建(MB/s)		6.14	6.01	5.95
4.0K 随机读写(MB/s)	R	4.6	4.1	4.4
	W	2.8	2.4	2.3
512K 随机读写(MB/s)	R	17.1	16.3	16.5
	W	2.3	1.9	2.0

其他各项的测试如表 2 所示.从表 2 中数据可以看出,增加可信认证和启用 IEE 对小文件的创建和读写影响要比对大文件的影响要大,这主要是由于可信认证和 IEE 的访问控制主要在文件的初次访问时执行,而对后续的读写操作几乎没有影响.

4.2　安全性分析

UTrustDisk 的主要安全特性就是可以防止磁盘中的数据在存储、访问和使用过程中发生泄漏.为说明这一特性,本节基于 Denning[30] 的信息流模型对 TRSF 框架下的信息流进行描述和分析,将安全控制规则转换为信息流规则,最后给出 TRSF 的数据泄漏防护安全定理.

DS 和 DU 分别表示移动存储设备中文件集合和其他存储设备或网络中的文件集合;$f_1, f_2, \cdots, f_n \in (DS \cup DU)$, $n \in N$ 表示系统中的文件; PS 和 PU 分别表示 FVM 内和 FVM 外的进程集合; $p_1, p_2, \cdots, p_m \in (PS \cup PU)$, $m \in N$ 表示系统中的进程;: $\rightarrow_t$ 表示 t 时刻的信息流请求;$\rightarrow_t$ 表示 t 时刻的实际信息流动.根据 FVM 的进程控制机制,给出如下信息流规则:

规则 1　如果 FVM 外的进程请求访问移动磁盘中文件,在规则允许的情况下,需要将该进程切换到 FVM 的保护域中运行,即

$$\forall f \in_{t_0} DS, p \in_{t_0} PU, f: \rightarrow_{t_0} p \Rightarrow f \rightarrow_{t_0} p \wedge \forall t > t_0, p \in_t PS.$$

规则 2　如果 FVM 中的进程请求对移动磁盘外的文件进行写操作,则在移动磁盘中创建该文件的副本,并将写操作请求重定向到对副本文件的操作,即

$$\forall f \in_{t_0} DU, p \in_{t_0} PS, p: \rightarrow_{t_0} f \Rightarrow CreateAndCopy(f', f) \wedge (p \rightarrow_{t_0} f' \wedge \forall t > t_0, f' \in_t DS).$$

规则 3　如果 FVM 中的进程与 FVM 外的进程进行通信,在规则允许的情况下,需要将 FVM 外的进程切换到 FVM 的保护域中运行,即

$$\forall p \in_{t_0} PS, p' \in_{t_0} PU, p: \rightarrow_{t_0} p' \Rightarrow p \rightarrow_{t_0} p' \wedge \forall t > t_0, p' \in_t PS.$$

基于以上规则,可以得到 TRSF 泄漏防护的安全定理:

定理 1　基于 TRSF 构建的安全系统中,安全域中的文件内容不会泄漏到安全域之外*.

证明　采用反证法证明.假设安全域中的文件内容可以泄漏到安全域之外,即存在如下信息流:

$$\forall f \in_{t_0} DS, f' \in_{t_0} DU, \exists t > t_0, f \rightarrow_t f'$$

由于信息流具有传递性[31],而且信息流动主要由进程对文件的读、写以及进程间通信三种操作触发.因此 $\exists p \in_{t'} (PS \cup PU), t_0 < t' < t'' < t, f \rightarrow_{t'} p, p \rightarrow_{t''} f'$.

由规则 2 可知,$p \in_{t'} PU$,否则不存在 $p \rightarrow_{t''} f'$.

对于 $f \rightarrow_{t'} p$,分以下两种情况考虑.

(1) p 在 t' 时刻直接请求读取 f,由规则 1 可知,$p \in_{t'} PS$,这与 $p \in_{t'} PU$ 矛盾.

(2) $\exists p' \in_{t'} (PS \cup PU), t_0 < t''' < t', f \rightarrow_{t'''} p' \wedge p': \rightarrow_{t'} p$.由规则 3 可知,$p' \in_{t'} PU$.TVD 的实现机制中,FVM 内的进程不会切换到 FVM 之外,即进程不可能从 PS 切换到 PU 中.因此 $p' \in_{t'''} PU$.与 $f \rightarrow_{t'} p$ 类似递归分析 $f \rightarrow_{t'''} p'$.必然存在 p'' 在 t_0' 时刻直接读取 f 并且 $p'' \in_{t_0'} PU$.由(1)知,存在矛盾.

综上,假设 $\forall f \in_{t_0} DS, f' \in_{t_0} DU, \exists t > t_0, f \rightarrow_t f'$,则存在矛盾.说明假设错误.从而结论得证. ■

由于 UTrustDisk 是基于 TRSF 进行的实现,而且基于可信计算建立的信任链可以确保信息流严格遵守上述规则,所以 TRSF 的泄漏防护安全性可以有力保证 UTrustDisk 的安全性.

4.3　与相关实现比较与分析

UTrustDisk 是借鉴 Armordisk 的硬件结构实现的,除了具有原有结构的安全特性[24],还具有如下新的灵活特性:

(1) 使用控制的连续性.传统的安全 U 盘主要侧重于用户身份的认证,而对于通过认证的进程没有限制;UTrustDisk 通过扩展到终端系统中的 TVD 对进程使用磁盘中数据的过程进行控制,从而保证数据的使用也符合安全预期.

(2) 控制策略的灵活性.除了提供读、写、修改和重命名等常用的控制权限,还可以对可能造成数据泄漏的复制/粘贴、拖放、进程间通信、网络发送等权限进行控制.

(3) 数据泄漏防护的主动性.现有安全 U 盘虽然可以集成木马检测和杀毒等安全软件,对使用环境进行检测,但对进程的控制依赖于终端系统的安全机制,因此对于临时文件导致的数据泄漏,特洛伊木马窃取数据等无能为力.PrayayaV3 等口袋操作系统虽然通过虚拟操作系统实现应用环境的便携性,但操作系统内部同样面临数据泄漏的风险.UTrustDisk 通过构建硬件存储到应用环境的信任链保证对数据的访问和使用都符合安全预期,因此具有好的主动性,保证移动存储设备即使在非可信环境中使用也是安全可信的.

5　结束语

本文针对移动存储介质在非安全环境使用或者被非可信进程访问时面临的数据泄漏威胁,提出了一种

---

* 该定理不考虑内部人员通过超出计算机外的手段主动泄漏的情况

基于可信虚拟域的移动存储框架 TRSF.TRSF 基于硬件层的 TPM 模块构建从存储硬件到进程隔离环境的信任关系链,从而实现移动存储设备的主动防护.由于终端系统的隔离环境是由移动存储设备主动构建的,因此 TRSF 对终端系统自身的安全机制没有严格要求,从而在保证安全性的前提下,提高了移动存储设备的可用性和灵活性.最后基于 TRSF 框架,并借鉴国民技术的 Armordisk 磁盘硬件体系结构,实现了一款具有主动防护能力的安全 U 盘 UTrusttDisk.实际测试说明引入信任链安全验证和可信执行环境 IEE 导致平均读写性能开销分别增加 7.5%和 11.5%.

参考文献

[1] TRUECRYPT. TrueCrypt volume [EB/OL]. http://www.truecrypt.org/docs,2010-07-09.

[2] MICROSOFT. BitLocker drive encryption [EB/OL]. http://windows.microsoft.com/en-us/windows7/products/features/bitlocker,2010-07-09.

[3] McAfee. Data loss prevention [EB/OL]. www.mcafee.com/us/enterprise/products/data_protection/data_loss_prevention/index.html,2010-07-09.

[4] VERDASYS. Mobile data protection & remote media encryption [EB/OL]. www.verdasys.com/Mobile_Data_Protection_Encryption.php,2010-07-09.

[5] 曾文英,赵跃龙,宋玮,等.个人存储管理策略研究[J].计算机研究与发展,2009,46(Suppl):96 – 101.
Zeng Wenying, Zhao Yuelong, Song Wei, et al. Research on personal storage management strategies[J]. Journal of Computer Research and Development, 2009, 46(Suppl.): 96 – 101. (in Chinese)

[6] Michael Fabian. Endpoint security: Managing USB-based removable devices with the advent of portable applications[A]. In InfoSecCD'07: Proceedings Security Curriculum Development[C]. New York: ACM, 2007. 1 – 5.

[7] Hyeran Lim, Vikram Kapoor, Chirag Wighe. Active disk file system: A distributed, scalable file system[A]. Proceedings of the Eighteenth IEEE Symposium[C]. Washington, DC: IEEE Computer Society, 2001. 101 – 114.

[8] KimberlyKeeton, David A. Patterson , Joseph M. Hellerstein. A case for intelligent disk[A]. ACM SIGMOD Record[C]. New York: ACM, 1998.

[9] John D Strunk, Garth R Goodson, Michael L Scheinholtz, et al. Self-securing storage: Protecting data in compromised systems [A]. Proc of the 4th Symposium on Operating Systems Design and Implementation[C]. Berkeley, CA: USENIX Association, 2000. 12 – 26.

[10] 靳超,郑纬民,张悠慧.主动存储系统结构[J].计算机学报,2005,28(6):1013 – 1020.
Jin Chao, Zhen Wei-Min, Zhang You-Hui. Active storage architecture[J]. Chinese Journal of Computers, 2005, 28(6): 1013 – 1020. (in Chinese)

[11] 谢雨来 冯丹 王芳,主动存储技术及其在对象存储中的实现[J].中国计算机学会通讯,2008,4(11):27 – 32.
Xie Yulai, Feng Dan, Wang Fang. Active storage technology and its implementation for object storage[J]. Commuications of CCF, 2008, 4(11): 27 – 32. (in Chinese)

[12] 赵跃龙,蒋骞.基于智能网络磁盘的虚拟存储技术的研究与设计[J].计算机研究与发展,2009,46(Suppl):44 – 49.
Zhao Yuelong, Jiang Qian. Research and design of the virtualization storage technology based on Intelligent Network disk [J]. Journal of Computer Research and Development. 2009, 46 (Suppl): 44 – 49. (in Chinese)

[13] Trusted Computing Group. TCG storage architecture core specification [EB/OL]. http://www.trustedcomputinggroup.org/files/static_page_files/B6811067-1D09-3519-ADDAFC18E3A87CB2/Storage_Architecture_Core_Spec_v2_r1-Final.pdf,2010-07-09.

[14] 徐明迪,张焕国.基于可信计算平台的可信存储研究[J].通信学报,2007,28(11A):117 – 120.
Xu Mingdi and Zhang Huanguo. Research on trusted storage based on trusted computing platform[J]. Journal on Communications. 2007, 28(11A): 117 – 120. (in Chinese)

[15] 汪丹,冯登国,徐震.基于可信虚拟平台的数据封装方案[J].计算机研究与发展,2009,46(8):1325 – 1333.
Wang Dan, Feng Dengguo, Xu Zhen. An approach to data sealing based on trusted virtualization platform[J]. Journal of Computer Research and Development, 2009, 46(8): 1325 – 1333. (in Chinese)

[16] J L Griffin, T Jaeger, R Perez, et al. Trusted virtual domains: Toward secure distributed services[A]. Proceedings of the 1st IEEE Workshop on Hot Topics in System Dependability[C]. Los Alamitos: IEEE Computer Society. 2005.

[17] Burdonov I, Kosachev, A, Iakovenko. Virtualization-based separation of privilege: working with sensitive data in untrusted environment[A]. Proceedings of the 1st Eurosys Workshop on Virtualization Technology For Dependable Systems (VTDS'09)[C]. New York: ACM. 2009. 1 – 6.

[18] Catuogno L, Löhr, Manulis M, et al. Transparent mobile storage protection in trusted virtual domains[A]. 23rd Large Installation System Administration Conference (LISA'09)[C]. Berkeley, CA: USENIX Association, 2009.

[19] 艾丽华,罗四维.数据网格虚拟机动态存储层次的研究[J].电子学报,2010,38(11):2680 – 2685.
Ai Lihua, Luo Siwei. Research on dynamic storage hierarchy of data grid virtual machine[J]. Acta Electronica Sinica, 2010, 38(11): 2680 – 2685. (in Chinese)

[20] Yang Yu. OS-level virtualization and its applications[D]. New York: Stony Brook University, 2007.
[21] 吴世忠,石超英.一种智能卡和 U 盘复合设备及其与计算机通信的方法[P].中国专利: CN200710000328.3, 2007-01-08.
[22] SanDisk. Introduction to U3 smart drive[EB/OL]. http://u3.sandisk.com/, 2010-07-09.
[23] 国民技术. Armordisk(安全 KEY 盘)加密存储[EB/OL]. http://www.nationz.com.cn/Solutions2.aspx? id = 18, 2010-07-09.
[24] RSA Laboratories. PKCSJHJ11: Cryptographic token interface standard[EB/OL]. http://www.rsa.com/rsalabs/node.asp? id = 2133, 2010-07-10.
[25] St′ephanie Delaune, Steve Kremer, Graham Steel. Formal analysis of PKCSJHJ11[A]. Proceedings of 21st IEEE Computer Security Foundations Symposium[C]. Pittsburgh: IEEE Computer Society, 2008.331 – 344.
[26] 广州市经略电子有限公司. PrayayaV3 虚拟操作系统的特点[EB/OL]. http://www.prayaya.com/prayayav3/product.php, 2010-07-09.
[27] 谢均,黄皓,张佳.多保护域进程模型及其实现[J].电子学报, 2005, 33(1): 38 – 42.
Xie Jun, Huang Hao, Zhang Jia. A multi-protection domains process model and its implementation[J]. Acta Electronica Sinica, 2005, 33(1): 38 – 42. (in Chinese)
[28] Weiqing Sun, Zhenkai Liang, R. Sekar, etc. One-way Isolation: an effective approach for realizing safe execution environments[A]. Proceedings of the Network and Distributed System Security Symposium(NDSS'05)[C]. California: The Internet Society, 2005.265 – 278.
[29] 数码之家. U 盘扩容检测工具[EB/OL]. http://www.mydigit.cn/mydisktest.htm, 2010-09-07.
[30] Denning D E. A lattice model of secure information flow[J]. Communications of the ACM, 1976, 19(5): 236 – 243.

作者简介

马　俊　男,1982 年生,博士研究生,中国计算机学会学生会员,主要研究方向为数据安全和系统安全. E-Mail: majun_nudt@sohu.com

王志英　男,1956 年生,教授,博士生导师,中国计算机学会高级会员,主要研究方向为先进计算机体系结构、微处理器设计技术研究、信息安全及异步电路设计等.