第35卷 第19期 计 算 机 工 程 2009年10月
Vol.35 No.19 Computer Engineering October 2009
·安全技术· 文章编号：1000—3428(2009)19—0135—03 文献标识码：A 中图分类号：TP393

移动存储介质信息安全系统的研究与实现

俞卫华[1]，路松峰[2]
(1. 河南科技大学电子信息工程学院，洛阳 471003；2. 华中科技大学计算机科学与技术学院，武汉 430074)

摘 要：针对当前移动存储介质使用和管理过程中存在的典型安全问题，设计并实现一个内网移动介质信息安全系统。该系统采用C/S模式，建立起以防外联服务器、部门服务器和客户端组成的三级体系构架，根据内外兼防和多级安全控制思想，分别从互联网和内部网络对接入移动存储介质的计算机以及移动存储介质本身进行监控，有效保障移动存储介质中数据的保密性、完整性和可用性。
关键词：移动存储介质；多级安全控制；网络隔离

Research and Implementation of Removable Storage Medium Information Security System

YU Wei-hua[1], LU Song-feng[2]
(1. Electronic Information Engineering College, Henan University of Science and Technology, Luoyang 471003;
2. School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074)

【Abstract】Aiming at the current security problems in using the removable storage medium, an information security system in local area network is designed and implemented. It adopts C/S pattern and consists of anti-connecting-Internet server, department server and client. Based on multi-level security control idea and inside-and-outside defend idea, it protects client computer and removable medium from threaten not only in the LAN, but also on the Internet. The system safeguards the secrecy, integrality, usability of the information saved in the removable storage medium.
【Key words】removable storage medium; multi-level security control; network isolation

1 概述

移动存储介质因其使用灵活、快捷、方便的特点迅速得到普及。但同时也带来了诸如数据拷贝不受限、数据传输不受限、内外网交叉使用等问题，对数据安全产生了严重威胁。当前使用移动存储介质过程中所面临的安全威胁主要有：

(1)单位内部任意个人的移动存储介质都可以在内网计算机上随意使用，造成病毒感染和泛滥。

(2)内部人员可以将重要信息复制出去，易造成泄密。据IDC权威机构调查，80%的泄密事件来自内部人员。

(3)移动存储介质中的数据一般以明文形式存放，内部人员可将涉密终端上的数据通过移动介质转移到连接互联网的计算机中，通过互联网泄露涉密信息。

(4)移动存储介质一旦丢失，其中存储的大量敏感数据可能失控。

信息安全领域专家一直呼吁构建内外兼防的安全信息系统，强调内部防范的重要性和外部监控的必要性[1]。针对频繁使用移动存储介质的工作环境，内部防范的重点在于对移动存储介质的使用负责到具体人员，对内部人员使用移动存储介质的行为进行实时监控。外部防范的重点在于及时检测和判断移动存储介质的使用状态，当其使用者把移动存储介质违规接入互联网时，及时进行网络阻断，并把事件记录备案同时通报相关负责人。当前主流的杀毒、入侵检测和漏洞扫描技术无法有效解决来自内部的威胁，外部监控和阻断也不尽人意。

基于以上分析，本文以计算机系统的整体安全为切入点[2-3]，设计并实现了针对内网工作环境的移动存储介质信息安全系统，该系统在技术上对移动介质中的数据进行加密，对网络进行逻辑隔离；在管理上对移动介质实行责任制并注册在案，当用户对介质操作时需要身份认证；在审计上，对用户的所有操作进行全程监控并记录在案，方便发现隐患以及日后的审计追踪。在对移动存储介质进行安全管理的同时，对其信息传输的渠道也进行必要的保护，全方位保证涉密信息和设备的安全。

2 系统的总体设计

系统设计的总体目标是保证工作环境内部的涉密信息不能通过移动存储介质的渠道泄露到外部环境中。当前，计算机系统之间的信息交换普遍采用移动存储介质和网络传输这2种渠道进行。因此，制定出合理的安全策略，以安全策略为指导，设计并部署相应的安全系统，对信息传输的2种主要渠道进行控制，能达到信息防泄露的目的。本系统的实施所依赖的安全策略如下：

(1)内部移动存储介质脱离其工作环境后，其中的数据不能被使用；外部移动存储介质不能在内部工作环境使用。

(2)用户只能在系统授予的权限范围内使用终端和移动存储介质，权限到期时必须被系统回收。

(3)移动存储介质的管理需要在技术上和政策上双重入手，以技术为主导，以行政管理为辅助。

(4)移动存储介质的管理软件具备自我保护功能。

基于以上安全策略的指导，本文设计和实现了针对内网

基金项目：国家自然科学与中国工程物理研究院联合基金资助项目(10876012)
作者简介：俞卫华(1979－)，女，助教、硕士研究生，主研方向：计算机网络及其应用；路松峰，副教授、博士
收稿日期：2009-04-20 **E-mail：**hustywh@163.com

环境的移动存储介质信息安全系统。

2.1 系统体系结构和网络拓扑

系统选用层次化、模块化的设计思路。在体系结构上分为 3 层：(1)用户界面，用于处理用户发出的相关命令并将结果显示给用户；(2)数据逻辑处理层，负责对存储在移动介质上的数据进行加解密以及对通过网络的数据包进行访问控制和加解密，并处理来自网络或发往网络的数据；(3)数据访问层，负责对数据库和网络上的数据进行访问。

系统在单位内部网络环境设置部门服务器，对所有客户端使用移动介质的状况进行实时监控；在互联网出口搭建防外联服务器，对客户端非法连接互联网的操作进行记录和阻断，并通过手机短信发送装置以短信息的方式告知单位负责人，对违规人员和违规操作进行处理。三级结构的建立从各个方面均对用户在客户端上的操作提供了安全防护，从而将泄密风险降到最低。图 1 显示了系统的网络拓扑结构。

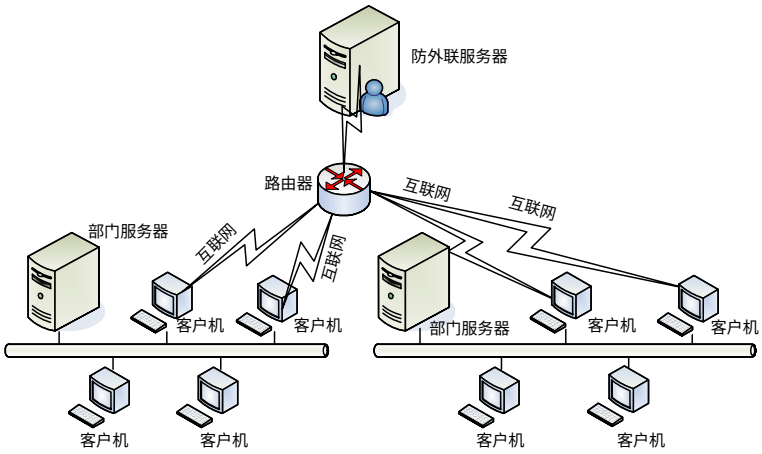


图 1　系统网络拓扑结构

其中，客户机是执行整个系统安全策略和实施监控行为的主体；部门服务器在单位内部实施监控，并负责保存用户、移动存储介质和客户端计算机的注册信息以及分发安全策略，使客户端脱离部门服务器后不能正常工作，从而防止了涉密信息通过移动介质泄露；防外联服务器则独立于各个单位，通过路由器与互联网连接，负责在外联出口对非法连接互联网的客户端实施监控，防止信息从互联网上泄露。

2.2 系统功能结构

图 2 给出了内网移动存储介质信息安全系统的功能结构。防外联服务器、部门服务器分别通过互联网和内部网络与客户端相连。

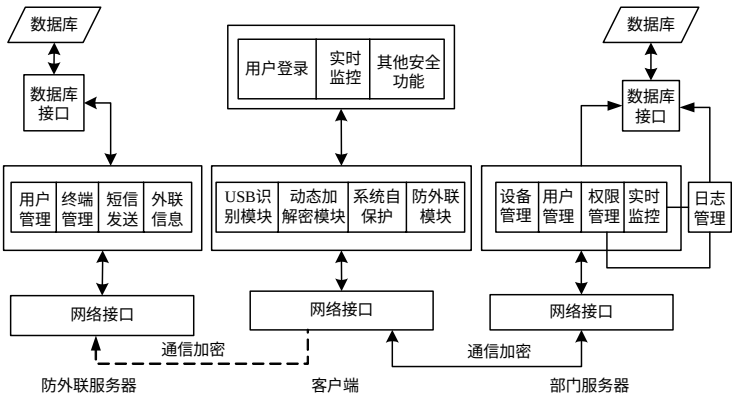


图 2　系统功能结构

客户端是整个系统安全策略和防护机制的执行单元。安装客户端的终端一经启动，即向部门服务器开机注册，此后便处于部门服务器的监控状态中。终端接入移动存储介质时，USB 识别模块即可检测到设备的接入，然后获取该设备的标记号，以此标记号作为向部门服务器的注册信息。

部门服务器是系统内各种信息的管理中心，包括用户注册信息、设备注册信息、终端注册信息、部门信息、权限信息以及日志信息。用户注册需记录用户 ID 和密码；移动存储介质的注册就是在其中的非用户存储区域写入唯一标识符来标识其注册和认证信息；计算机终端则使用硬盘序列号来唯一标识。部门服务器利用保存在数据库中的这些信息，与客户端进行一系列的信息交换，从而能够在方便用户使用计算机和移动存储介质的前提下，保证用户计算机和移动介质中信息的安全。

部门服务器根据客户端的注册信息对客户端的合法性进行验证，保证非注册计算机无法在内部网络中使用；当客户端接入移动介质时，部门服务器通过对比数据库中保存的标记号以及认证信息判断移动介质的合法性，从而可以拒绝外来移动介质的接入；认证成功后，部门服务器对比用户 ID 和密码，返回给用户相应的操作权限。在移动介质使用过程中，部门服务器会将从客户端发来的日志信息保存在数据库中以便日后查看，对安全事故进行追踪。

防外联服务器作为外联信息的管理中心，同样在数据库中保存了用户信息、部门信息和计算机终端信息。它在互联网出口对客户端实施远程监控，当各单位内部的计算机非法连接互联网时，防外联服务器可以实时检测到联网状况，并将联网计算机的外联信息保存在外联信息表中，与此同时，防外联服务器端开辟独立的线程定时扫描数据库中外联记录，根据外联记录获取联网计算机的标记号以及当前接入的移动介质信息，从而确定联网用户信息，并通过短信息的形式向该用户所在的单位负责人通报非法外联情况，以便单位内部进一步处理。

另外，在部门服务器、防外联服务器和客户端上安装 NDIS(Network Driver Interface Specification)中间层驱动程序，对内外网进行逻辑隔离，只允许注册终端与部门服务器、防外联服务器进行通信。终端所有网络数据包在发送到内网之前被系统拦截，对其中的数据载荷进行加密和完整性校验，在接收端对所有从网络上接收的数据包进行解密并检查完整性，使得整个系统内部的数据传输都处于密文状态，防止中间人攻击。

3　系统的实现

系统提供的防泄露能力主要体现在以下 5 方面：

(1)对移动存储介质进行认证注册和身份识别；

(2)对移动存储介质中的文件进行加密存储；

(3)对网络数据包进行加密传输；

(4)对客户端联网监控；

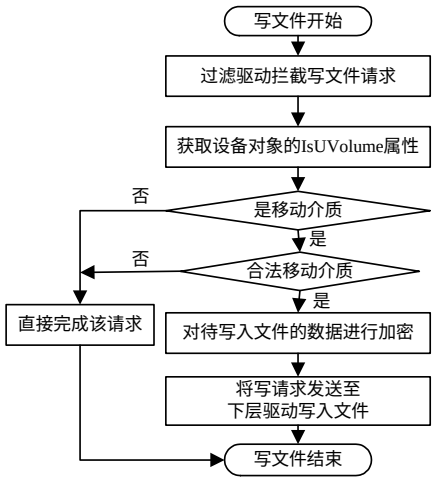
(5)系统自身的保护措施。

其中，移动存储介质的注册和识别以及文件的加解密在文件过滤驱动中完成；加密传输在 NDIS 中间层驱动中完成；对客户端联网监控使用 TDI Client 驱动程序完成；而系统的自我保护机制则采取

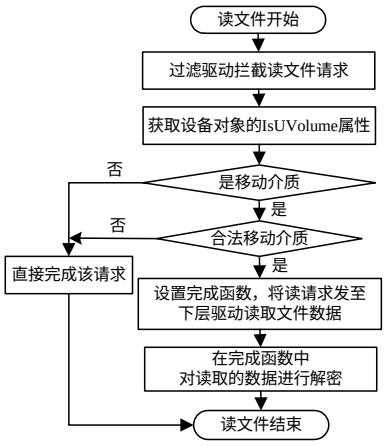
一些内核技术来实现。本文就系统主要模块进行如下阐述。

3.1 文件存储加解密和移动介质识别模块

文件加密存储和移动介质识别在文件过滤驱动程序[4]中完成。当拦截到 IRP_MN_MOUNT 请求后，在过滤驱动中创建一个新的设备对象，并绑定到文件系统刚刚接入的卷设备对象上，新创建的设备对象可以拦截到所有对该卷内文件的新建、打开、读写等操作，从而实现对移动介质中文件的动态加密与解密[5]。加密操作在 IRP_MJ_WRITE 的派遣例程中完成，解密操作在 IRP_MJ_READ 的派遣例程中完成，文件加解密的一般流程如图 3 所示。



(a)文件加密流程



(b)文件解密流程

图 3 文件加解密流程

3.2 网络通信加密模块

该模块位于 NDIS 中间层，用于对网络数据传输进行访问控制，并对所有经过内部网络的数据包进行加解密。系统在 Microsoft DDK 中附带的 PassThru 的基础上实现了一个数据包加解密和访问控制的驱动程序。对发送出去的数据包加密，只要在 PassThru 中的 MPSendPackets 中加入必要的操作代码即可实现；对接收到的数据包解密，则需要在 PtReceive 和 ProtocolReceviePackets 中加入必要的操作代码。下面给出发送加密的关键代码，接收解密的过程本文不再赘述。

```
BOOLEAN FltFilterSendPacket( IN PADAPT pAdapt, IN
  PNDIS_PACKET pReceivedPacket)
{
BOOLEAN bPass = TRUE;
PADAPT_FILTER_RSVD pFilterContext = (PADAPT_FILTER_
RSVD)&pAdapt->FilterReserved;
    UCHAR buffer[MAX_PACKET_HEADER_LEN];
    ULONG nReadBytes;
    …
    // 读取封包中的数据，这里仅读取封包头
    FltReadPacketData(pReceivedPacket, buffer, MAX_PACKET_
HEADER_LEN, &nReadBytes);
    // 检查过滤规则，看看是否允许这个封包通过
    return
FltCheckFilterRules(pAdapt,pFilterContext->pFilterList,buffer,
nReadBytes, TRUE, FALSE);
    }
```

3.3 防外联模块

防外联模块是一个通过调用 TDI 接口(Transport Driver Interface)进行数据发送和接收的 TDI 客户驱动，程序的主体通过定时等待互斥量的方法，以固定的时间间隔向防外联服务器发起 UDP 连接来将终端非法外联信息发往防外联服务器。基于 SPI, WinpCap 和 Tdi Filter 的网络嗅探器无法嗅探出以此方式发送的数据包，只有基于 IMD(Intermediate Driver)的嗅探器可以实现嗅探，而 IMD 是被本系统自身所控制的，因此可以保证传输的网络数据包不会被中间人攻击。防外联模块的工作流程如图 4 所示。

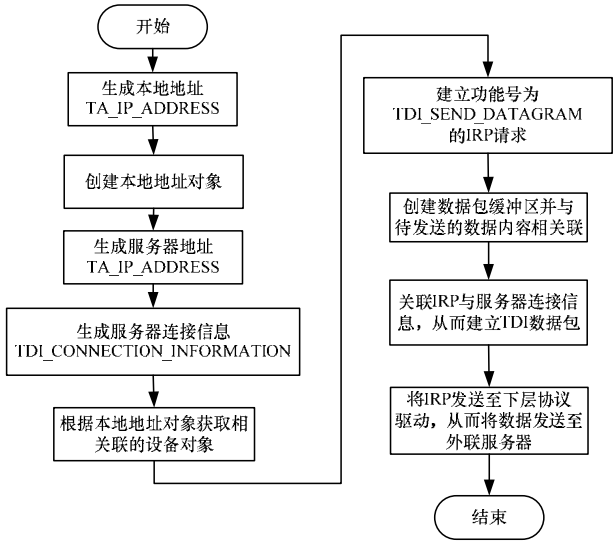


图 4 防外联模块工作流程

4 功能和性能测试

为了检测系统各功能部件的工作情况，验证系统的可靠性、健壮性、容错性和稳定性，对系统进行了不间断性能测试。同时对服务器所能承受的负荷进行压力测试，以检测系统的最大客户端承载量。

4.1 功能测试

利用 20 台内网 PC 机，其中的 2 台分别作为部门服务器和防外联服务器，以及 100 台连接互联网的 PC 机搭建起系统运行的模拟网络环境，对系统功能进行了全面的测试，包括移动存储介质识别、动态加解密、权限分配和实时回收、通信加密传输等功能的测试，主要内容如下：

(1)动态加解密测试。保证移动介质中的数据文件都以密文方式存储，只有在安装客户端软件的计算机终端上才能够恢复明文。

(2)用户各项权限分配及其测试。需要测试的权限包括文

（下转第 140 页）