高安全性移动存储设备（微盾）研发与应用

一、 产品研发背景

随着企事业信息化建设速度和水平的不断提高，以及电子政务和新型战略产业大数据、物联网技术的广泛应用，所产生的数字信息量呈指数增长，已经成为企、事业单位赖以生存的核心资产。如何有效地保证组织机构内部重要或涉密电子文档在整个生命期内的受控、安全和保密，特别是重要、涉密数据在交换、共享过程中不被截获、不被篡改、不被扩散和伪造（存储安全性），且安全受控，已成为企事业单位最为关注的信息安全问题。与此同时，“病毒”、网络攻击等对企事业内部重要信息系统安全稳定运行的威胁日益严重，特别是移动存储设备已成为单位内部信息泄露和攻击企业内网的主要途径之一，迫切需要按照各类企事业单位内网信息系统的应用和安全需求，研发信息安全防护能力强，又易用便捷的移动安全存储系列专用设备，并实现产业化。为此，西安建筑科技大学和中国电子科技集团公司第 15 研究所下属的北京华兴太极信息科技有限责任公司合作研发了高安全性移动存储专业设备（产品名称“微盾”），防范企事业单位在内部重要或涉密信息交换、共享过程中引发的信息安全威胁。

二、 产品研发必要性

由于移动存储设备以其体积小、容量大、使用方便和传输速度快等优点，已经成为信息存储、传播和交流的一个主要手段。但是移动存储设备引发的信息安全问题随之而来，包括：

（1）木马病毒感染或恶意软件入侵对 U 盘或/和主机系统中信息的破坏。当 U 盘插入计算机系统时，无论是发生 U 盘被感染木马或病毒，还是 U 盘中的木马或病毒传播给计算机，都可能造成对移动存储设备或主机中的信息破坏；

（2）木马病毒引发的信息窃取和泄露。木马病毒或恶意程序通过 U 盘感染上计算机系统，隐蔽地下载计算机中的敏感信息，并伺机自动发送到木马指定的

互联网计算机中，造成涉密或敏感信息泄露，给个人、企业甚至国家的损失；

（3）因移动存储设备丢失或被盗造成的信息泄露。存有敏感、涉密信息的U盘一旦丢失，会带来存储信息泄露的严重后果。

（4）在通过移动存储设备进行数据交换的过程中，用户未经允许，可任意拷贝U盘、光盘中的敏感信息。这种授权用户无意或有意地主动扩散或泄密行为造成的信息泄露和信息偷盗，已成为目前企业信息安全系统的管理死角，难于防范。

上述信息安全威胁已成为企业或个人使用移动存储设备急需解决的信息安全问题，因而高安全性移动存储设备的研发十分必要，可实现U盘设备的防木马，防病毒和防信息拷贝造成的信息泄露；并采用无线射频定位和移动通信技术，实现U盘设备的智能定位与追踪管理，防范设备丢失等信息安全事故，以满足涉密、敏感单位或个人对移动存储高安全、高保密的需求。

三、 产品功能

移动安全存储系列专用设备包括第一代产品“绿盘”和正在研制的升级换代产品——“微盾”。

(一) 第一代产品“绿盘”功能

“绿盘”是具有拒绝病毒感染、加密存储、安全可管和可控的U盘设备，主要功能包括：

（1）身份安全认证。通过口令认证后才能使用“绿盘”内嵌的资源管理器，访问“绿盘”数据存储区。口令认证错误次数超限，设备自动锁死；

（2）拒绝病毒感染，防木马。“绿盘”拥有专门设计的、不对外公开的安全文件系统和专用读写接口。只有在这个特殊的安全文件系统的管理下，由通过身份认证的用户调用“绿盘”的专用读写接口（类似于一个特殊浏览器），才能访问“绿盘”的存储空间；

由于Windows操作系统的文件系统以及其它进程都无法识别和直接访问

“绿盘”的数据存储区，固化在“绿盘”内的工具软件在 Windows 操作系统下只作为一个只读设备出现，因此木马等病毒程序找不到“绿盘”中的存储空间，也就无法感染“绿盘”，更谈不上窃取或破坏存储在“绿盘”中数据信息了。即使用户主动将一个含有木马、病毒程序的文件存放到“绿盘”上，由于“绿盘”的存贮空间是由其自带的文件系统自行管理，木马等病毒程序不能识别此特殊的保密文件系统，因此恶意代码只能作为数据驻留在“绿盘”的数据存储区内，失去了执行能力，不可能感染存放在“绿盘”上的其它文件；也不会主动去感染当前插放“绿盘”的计算机系统。除非用户把这个文件拷贝到当前计算机上，并激活这个病毒。这就使隐蔽木马以 U 盘为“跳板”的数据摆渡窃取机制失效。

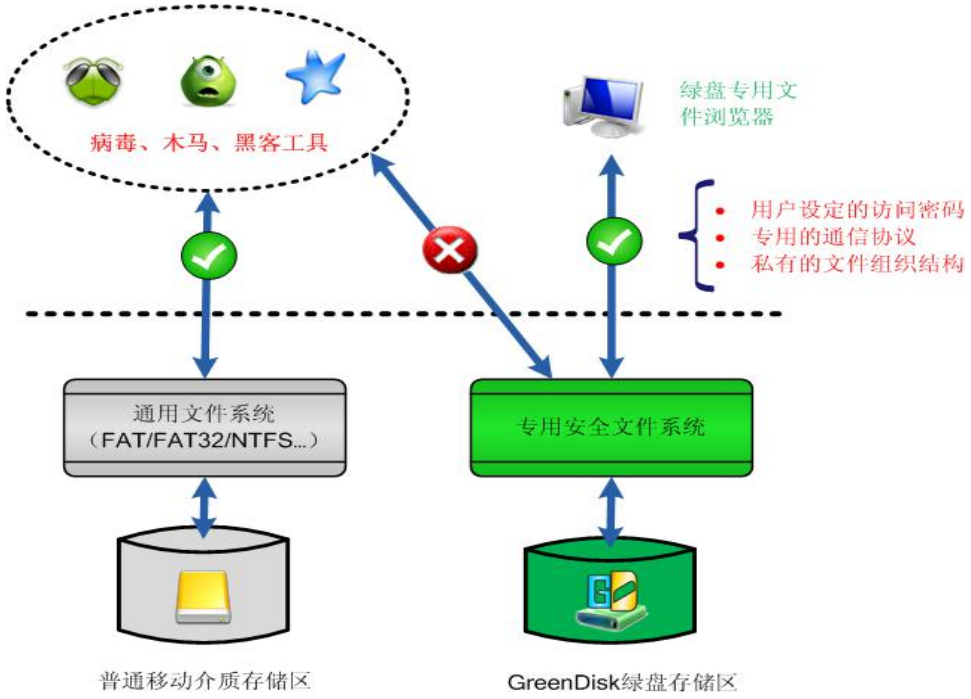

图 1“绿盘”防木马工作原理以及和普通 U 盘的比较

（3）文件分块加密保护，实现安全存储。“绿盘”支持普通文件夹和安全文件夹，安全文件夹也可以设定访问密码。由“绿盘”内置的国内专用高速安全芯片对存入安全文件夹的文件和目录进行加密存储。用户在访问安全文件夹时，除了“绿盘”的身份认证口令外，还需要验证文件夹访问口令后才能解密读取文件；

（4）权限分级管理。将用户权限划分为普通用户和管理者，分别拥有不同

的使用和管理权限。管理员可以设定 U 盘的安全属性。如：授权普通用户仅能够向“绿盘”中拷贝文件，无权限删除已拷贝文件；文件存满“绿盘”以后，只有管理员权限才能查看“绿盘”日志信息，并格式化“绿盘”，清空存储区，以便重复使用；

（5）设备运行限制。通过将“绿盘”和计算机系统绑定，管理员可以限定在某些机器中只能使用“绿盘”，不能使用其它的移动存储介质，包括 U 盘、移动硬盘等等；

（6）详细的日志记录。在设备内部详细记录 U 盘的使用、退出和各种文件操作等日志信息，包括本次操作的用户名、文件名、操作条件、计算机名和时间等信息，为管理者提供细粒度的事后审计依据；

（7）安全数据摆渡。传统的数据摆渡威胁来自于移动存储介质在内外网之间的交叉使用。近几年，病毒（木马）通过移动存储介质摆渡来窃取用户文件，逐渐成为信息安全的焦点问题，如何有效的鉴别用户和病毒（木马）行为，通过有效的手段来保证移动存储介质在内外部网络之间进行数据摆渡的安全，成为移动存储设备保密管理越来越重要的需求。

第一代产品在银行、油田、研究所、军工、税务工商等单位得以推广应用，用户响应良好。但在移动存储设备丢失或被盗、恶意代码入侵、文件跟踪等方面需要进一步增强信息安全特性，为此，**在第一代产品“绿盘”功能基础上，我们联合研制了第二代移动安全存储专用产品“微盾”。**

(二)　第二代产品“微盾”功能的提升

“微盾”在“绿盘”防病毒感染、信息安全可管可控的基础上，进一步增加了文件全生命周期内管理和设备安全功能，主要包括：

（1）嫌疑文件安全隔离。检查文件内容里含有不同特征的代码，根据相关嫌疑特征码检测出存入移动安全存储设备的嫌疑文件，并报告相关嫌疑内容，用于检测、隔离存入到设备中的嫌疑文件；

（2）文件跟踪。对指定来源、指定类型、指定位置的文件，加入文件数字

水印信息，用于文件流转追踪；文件在流转过程中，保持文件水印不被篡改，同时将流转过程中的信息写入文件水印；同时检测查看文件水印，追踪文件流转过程，确认流转文件出处；

（3）外发文件安全管控。为了保障外发文件的安全，对一些安全性要求比较高的重要文件，可以把它们制作成受控外发文件，受控条件包括：打开次数、生存周期、修改限制、打印限制、拷贝范围等，超出限制将无法打开文件，防止外发文档二次扩散，确保信息安全；

（4）数据智能自毁。内置时钟芯片与电池，独立计时，不依赖于计算机的时间系统。可为安全存储文件设置生命周期。一旦到达安全文件有效期限或者访问次数超出限制后，无论“绿盘”是否接入主机，都将在“绿盘”设备内自动销毁文件数据。

（5）无线定位与跟踪

安全存储设备支持安全空间内的区域定位；并可和智能终端 App 结合，支持室外 GPS、北斗定位模式，以满足室内和室外的不同应用需求；结合服务端的路径配置和管理功能，实现轨迹监控，丢失寻找等多种应用场合的需求。

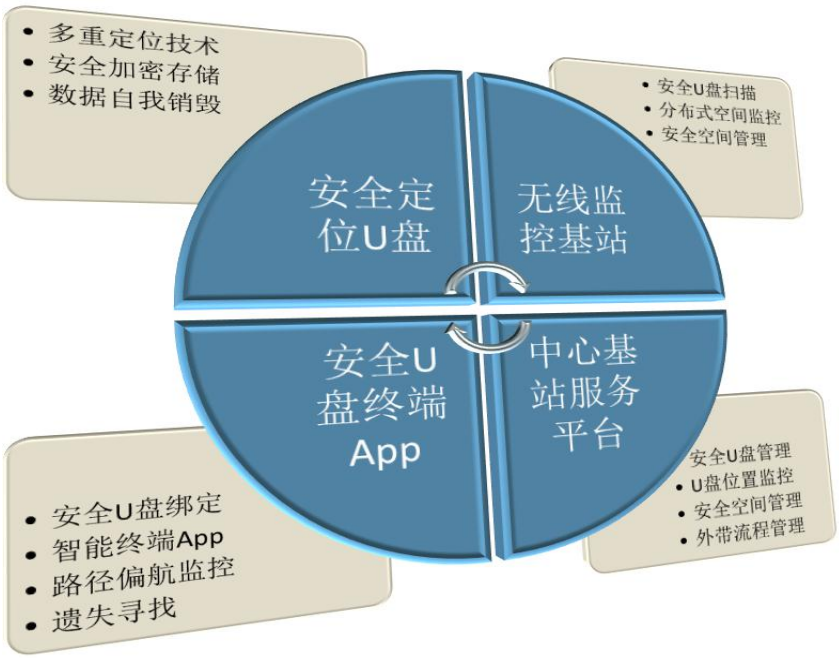

图 2 第二代产品“微盾”功能

表 1 “微盾”与其它 U 盘的功能对比

功能	普通U盘	杀毒U盘	防木马U盘	微盾
读写速度	USB2.0	USB2.0	USB2.0	USB2.0
安全功能	无	查杀病毒	安全存储	防病毒/安全存储/多权限管理
读写接口	开放式接口	开放式接口	专用接口	专用接口 + 专用文件格式
防病毒	不能	需升级病毒库	防病毒	主动检查嫌疑文件，百分之百防病毒
数据自销毁	无	无	多次输错PIN码后销毁整盘数据	更细的控制粒度，可按时间销毁单个文件夹
权限管理	无	无	一级权限	二级权限管理，并能对单个文件夹进行权限控制
审计日志	无	无	无	有
主机绑定	无	无	无	管理员可以根据主机设定微盾的用户使用权限，例如在某些机器上只允许拷入数据，不允许拷出数据
设备使用限定	无	无	无	管理员可设定只允许在某台机器上使用微盾，别的U盘都无法使用
支持私有文件夹	无	无	无	可以设定私有文件夹，防止微盾外借时发生私有文件非授权传播
易用性	非常方便	方便	方便	非常方便，完全兼容Windows操作
支持数据加密	无	无	无	有，基于国产算法专用加密芯片
支持设备定位	无	无	无	有
支持数字水印	无	无	无	有，可追踪文件流转过程

四、 产品主要特点

（1）解决数据的被动泄密。存储介质非法使用(木马病毒)或在流转过程中丢失造成重要数据被动的泄密；数据的外部合法使用者不经意间把数据扩散出去；

（2）解决数据的主动泄密。内部人员主动将自己权限范围内的重要信息通过各种方式传播出去；非授权人员通过各种渠道获取自己权限之外的数据并将其扩散泄密(内网用户攻击文件服务器窃取涉密数据)；

（3）实施用户单点登录身份验证，并可用于制作或验证防扩散文档，内置时钟芯片，有效防止篡改文档安全控制信息；

（4）采用内外环境隔离技术，保证外部的病毒木马无法进入内部感染文档和数据，摆脱传统防病毒软件的被动升级模式。

五、 产品主要性能指标

（1）读写速度快。产品支持 USB2.0/USB3.0 接口（目前采用的安全主控芯片只支持 USB2.0）。采用独有优化主控方案、顶级高速芯片，确保信息高速存取，其数据读写速度可达 15MB/秒；

（2）存储容量可扩展。可根据用户需求，生产各类规格容量 4G/8G/16G/32G/64G/128G 等的产品。通过存储芯片的串行或并行，扩展存储设备容量；

（3）高可靠性。 重复插拔使用>10000 次无故障；

（4）高保密性。文件数据加解密钥长度可达 128 位（SM1）；

（5）定位精度。室内＜2 米，室外＜8 米。

西安建筑科技大学

二〇一六年一月十日