祺安移动存储介质安全管理系统

技术白皮书

北京弘信安科技有限公司

2009 年 **5** 月

目录

1 产品简介

1．1 概述

《祺安移动存储介质安全管理系统》是一套针对于移动存储介质控制与审计的产品。

根据不同企业的各自需求，我们将移动存储介质管理分为：普通移动存储介质管理和标识移动存储介质管理两种；根据使用范围的不同，标识移动存储介质管理又分为：内部标识盘管理和外带盘管理。实现对不同种类移动存储介质管理的前提是基于《内安全网监控系统》平台之下，通过监控端对不同种类移动存储介质的识别来加以控制与审计。

1．2 基础架构

《祺安移动存储介质安全管理系统》整体采用业界主流的 C/S 和 B/S 结合的开发模式。内网安全体系由如下部件组成：服务器与监控端。

服务器

服务器是一个集成的 Web 和数据库管理环境。负责接收各客户端的监控信息。通过普通浏览器的访问，进行对移动存储介质的数据综合查询、统计分析、移动存储介质管理与权限分配等操作。后台数据库采用稳定性强、安全性强、易操作、空间占用小的 mysql 数据库，数据库安装随服务器安装的时候一同进行，无须进行二次安装。

监控端

客户端是一个服务程序，开机后根据服务器配置的安全监控策略自动加载，收集监视信息，控制被监控机的 USB 出口。客户端收集的监视信息包括：移动存储介质的读写删改等操作。

1．3 安全性分析

随着现代科技的迅猛发展，日常办公中的数据交互成为不可缺少的一部分，使得便捷、灵活的移动存储介质迅速普及开来，但是对于对交互数据较敏感的军工企业、政府、涉密单位来说，如何防止数据泄露成为一个不可避免的严峻问题。

每个企业对各自企业内移动存储介质管理的制度各不相同，而且都有各自的独到之处，例如像禁止驱动运行、固体胶封 U 口等方法，但都无法从根本上解决对移动存储介质滥用而造成的内部信息泄露问题，私人移动存储设备、带存储功能的 MP3、数码相机都是造成内部信息泄露的重要源头。与此同时由于正常工作的需求还是需要使用移动存储设备进行资料交互。既要满足日常工作的数据交互需求，又要防止重要信息被随意拷贝查看、防止移动介质丢失后重要资料的泄露，这样就急需一款能够解决这一对不可调和矛盾的产品来加以控制。

《祺安移动存储介质安全管理系统》是通过对移动介质不同使用范围的划分来加以区分控制与审计的。通过对移动介质的标识实现涉密局域网与外界的区分，这样可以有效的控制移动介质的使用范围，

避免私人的移动介质与涉密局域网内计算机的信息交互，同时防止由于移动介质的丢失而造成重要数据的泄露；其次，为移动介质赋予使用权限，可以严格的控制移动介质在涉密局域网内的使用范围，避免了涉密局域网内不同部门间的重要数据资料的不必要交互，同时通过数据密级流向控制有效的限制了不同密级计算机之间由于信息交互而造成的信息泄露问题。再次，由于涉密局域网需要与外界进行必要的数据交换，提供外带盘这种加密形式以解决特殊的工作需求。

潜在泄密途径与潜在威胁：

- 内部人员恶意或无意使用移动存储介质将涉密信息带出；
- 外来人员恶意或无意使用移动存储介质将涉密信息带出；
- 接触非涉密信息人员恶意或无意查看涉密移动存储介质内涉密信息；
- 存有涉密信息的移动存储介质在非涉密计算机上使用；
- 使用移动存储介质从涉密计算机中拷贝处涉密信息；
- 由于病毒和木马造成的涉密移动存储介质的损坏；
- 存有涉密信息的移动存储介质遗失或被盗造成的涉密信息泄露；
- 发生涉密信息泄露安全事故时无法进行追踪查询；
- 恶意或无意格式化涉密移动存储介质造成的涉密信息丢失等。

应对策略：

- 普通移动存储介质可以通过条件申请策略对带出文件加以审批，保证数据带出时有人审批并且有两人以上知晓，或者通过涉密企业内应用的中间机进行交互；

- 外部的移动存储介质在涉密局域网内被禁止使用；
- 经由移动盘格式化工具格式化后的内部移动存储介质在涉密网以外禁止使用；
- 被格式化的内部移动存储介质在涉密网内部没有被授权的计算机上禁止使用；
- 外带格式盘在外部和内部被授权计算机上必须通过密码识别后才能正常使用；
- 内部盘和外带盘对文件进行透明加解密过程，即不会在用户拷入和拷出文件时造成影响和多余的处理工作；
- 对经由移动盘格式化工具格式化后的内部盘和外部盘进行格式化保护，禁止在非使用状态下的格式化操作，允许在使用状态下的格式化操作；
- 支持密级流向，即高密级计算机只读低密级移动介质，低密级计算机禁止使用高密级移动介质；
- 用一般的文件恢复程序是无法恢复内部盘和外部盘的内部加密数据；
- 无论是普通移动介质、内部盘、外部盘或外部移动介质，在使用的过程中都会对具体操作进行审计，即允许使用时做数据交换日志，不允许使用是做违规操作日志等。

1．4 应用范围

根据用户的网络部属情况，《移动存储介质管理》不仅仅适用于

涉密局域网内的所有计算机，同时也适用于不在网内的独立计算机，从应用范围上来说，《移动存储介质管理》可以分为网络版和单机版。

2 产品功能

2．1 普通移动存储介质管理

此功能主要针对于普通移动存储介质的管理，提供方便管理方式，并审计移动存储介质的操作行为。

2．1．1 普通移动存储介质的控制

普通移动存储介质带出文件行为控制：对普通移动存储介质的使用从行为上分为允许使用、禁止使用。

【允许使用】，可随意使用移动存储介质读写文件，操作动作可选择审计或不审计；

【禁止使用】，移动存储介质在受控计算机上不允许使用，不能做任何的读写动作；

可监控的设备包括：

软盘 FD；

ZIP 盘；

USB 存储设备；

移动硬盘等。

2．1．2 普通移动存储介质的审计

审计对普通移动存储介质的加密文档读、写、改名、删除动作，审计的文件信息为：计算机名、用户名、进程、动作、结果等。

2．2 标识移动存储介质管理

通过移动盘格式化工具，对移动存储介质进行重新的加密格式化，来实现对移动存储介质的标识，可标识成两种形式：【内部标识盘】和【外带盘】。该部分的核心功能是采用了底层驱动技术，可将一个普通的移动磁盘通过专用的磁盘格式化工具，将其格式化成为一个企业内部专用标识盘。

在使用标识移动存储介质时，必须先进行认证处理，在未认证的状态下是无法写入和读取任何文件的，所以防止了一些木马和病毒的写入（例如像 Autorun 类型病毒的写入），从而极大程度的提高了移动存储介质内部数据的安全性。

2．2．1 内部标识盘管理

内部移动存储介质增加唯一标识并授权指定的计算机能使用。标签功能启用后普通移动存储介质将被彻底禁止使用，避免了外来移动存储介质在内部随意使用。同时，标识盘在内部网络中能正常使用，离开安全域不能正常打开，避免了因丢失等原因造成的信息泄露。

在认证状态下（即内部盘可以正常使用的情况下），用户可以对内部盘进行普通格式化操作，格式化后不会影响内部盘格式，可以继

续进行正常使用；在未认证状态下（即内部盘在涉密网以外或未授权计算机上使用），禁止用户对内部盘进行普通格式化操作。

内部标识盘的控制

对内部表示盘的使用从行为上分为和读写使用和禁止使用两种形式：

【读写使用】，可随意使用内部盘读写文件，操作动作可选择审计或不审计。

【禁止使用】，内部盘在受控计算机上不允许使用，不能做任何的读写动作；

内部标识盘的审计

审计对内部标识盘的加密文档读、写、改名、删除动作，审计的文件信息为：计算机名、用户名、进程、动作、结果等；

数据密级流向控制

内部移动存储介质支持密级定义，分为四个级别，即普通、秘密、机密、绝密。高密级移动存储介质在低密级计算机上无法使用。低密级移动存储介质在高密级计算机上无法使用（指移动存储介质）。同等密级能正常使用。

2．2．2 外带盘管理

外带盘形式是针对于涉密局域网与外界进行必要数据交换的一种解决方案，通过密码识别方式，实现对外带盘中加密部分的解密，解决内外网数据交换和出差时信息保密的需求。

外带盘同样也进行了格式化保护，即在认证状态下（即解密后外部盘可以正常使用的情况下），用户可以对解密后外部盘进行普通格式化操作，格式化后不会影响外部盘格式，可以继续进行正常使用；在未认证状态下（即解密后外部盘在授权计算机上使用），禁止用户对解密后外部盘进行普通格式化操作。

外带盘的控制

对外带盘的使用从行为上分为读写使用和禁止使用三种形式：

【读写使用】，可随意使用外带盘读写文件，操作动作可选择审计或不审计。

【禁止使用】，外带盘在受控计算机上不允许使用，不能做任何的读写动作；

外带盘的审计

审计对外带盘的加密文档的读、写、改名、删除动作并记录违规事件，审计的文件信息为：计算机名、用户名、进程、动作、结果等。

数据密级流向控制

由于外带盘形式特殊，所以外带盘只允许在已授权计算机上同密级进行使用。

2．2．3 标识盘管理

在管理控制台中的移动介质管理里，经由移动盘格式化工具格式化的移动存储介质会生成一条记录，其中包括标签号、容量、使用人、秘级、类型、部门、状态、注册时间、注销时间、注销去向及原因等

信息。我们不但可以按照部门对标识盘进行管理、对使用计算机进行授权，同时还可以将记录导出（以 EXCEL 格式导出）留作备份或进行统计，提高了我们对移动存储介质管理的透明度。

3. 系统特点

系统特点

1. 管理策略多样，适应各种移动介质管理的不同需求

对于移动存储介质细分为普通移动存储介质、内部标识盘、外带盘。企业实际使用时可禁止所有普通移动存储介质的使用，单位内部使用内部标识盘，出差人员外出使用外带盘。

2. 认证盘数据加密，不在受信环境中无法打开

认证盘采用磁盘加密的方法，需要授权指定的客户端才能使用，即使采用二进制编辑工具也无法查看实际内容，安全性高。

3. 外带盘控制安全可靠

外发盘的使用需要口令授权才能打开隐藏分区，即使丢失也能保证移动存储介质里的文档内容不被泄露。

4. 操作简便易用的管理平台

基于 B/S 的管理平台，管理员在任何一个计算机上都能通过 IE 浏览器登录管理控制台进行管理，不用单独安装管理控制台端。

标识盘制作、使用简单快捷。

4. 产品运行环境

配置表：

- 系统安装软件光盘
- 系统监控端安装、使用手册
- 系统服务端安装手册
- 系统管理员用户使用手册

系统软硬件环境要求如下：

<table>
<tr><td colspan="4">服务器</td></tr>
<tr><td>基本监控端数量</td><td colspan="2">0</td><td>允许监控端最大数量 2000</td></tr>
<tr><td rowspan="3">硬件基本配置(2000 点推荐)</td><td>CPU</td><td colspan="2">Intel®Pentium 4 2.4G，双 CPU</td></tr>
<tr><td>硬盘</td><td colspan="2">200GB</td></tr>
<tr><td>内存</td><td colspan="2">4GB</td></tr>
<tr><td>操作系统</td><td colspan="3">WindowsXP/2003/2008</td></tr>
<tr><td>数据库系统</td><td colspan="3">MYSQL、SQLSERVER、ORACLE</td></tr>
<tr><td colspan="4">监控端及外发环境</td></tr>
<tr><td rowspan="3">硬件配置(推荐)</td><td>CPU</td><td colspan="2">Intel®Pentium II 或更高</td></tr>
<tr><td>内存</td><td colspan="2">1GB 以上</td></tr>
<tr><td>硬盘</td><td colspan="2">监控程序所在磁盘有 600MB 以上可用空间</td></tr>
<tr><td>操作系统</td><td colspan="3">WindowsXP/2003/2008/VISTA/WIN7。并能运行于以上操作系统的 32 及 64 位软硬件平台</td></tr>
<tr><td colspan="4">管理控制台</td></tr>
<tr><td>浏览器</td><td colspan="3">IE6 及以上版本,推荐 IE7 及以上或 Google Chrome</td></tr>
</table>