

核安智华终端安全登录与文件保护系统

标准版介绍 V1. 11



文档名称	核安智华终端安全登录与文件保护系统		版本号：V1.11
拟 制	智华产品部	审 核：李中华	批准：郭子扬
日期	2011 年 3 月 2 日	制作部门	产品部
修改类型	MODIFIED	修改部门	市场部
发送组织	市场部/商务部/合作伙伴/智华用户	有效期：V1.12 版本发布前有效	

*修改类型分为 A - ADDED M - MODIFIED D - DELETE

一、 系统介绍

近年来，虽然各党政机关、企事业单位、金融、军队等系统在计算机网络及信息安全方面的投入越来越大，但在安全技术防范和管理上，依然存在着明显的隐患和漏洞，使国家信息安全受到严重威胁，失窃密事件时有发生。产生这种局面的根源在于：目前各党政机关单位对计算机信息系统的关键泄密部位缺乏专业性技术防控手段，系统建设方案缺乏完整性设计，而传统的“打补丁、补漏洞”式的管理方案，无法从根本上杜绝失窃密事件的发生。由此可见，传统安全防护手段已暴露出其局限性，不能适应当前信息系统的安全需求。

为此，北京智华天成科技有限公司与核工业计算机应用研究所，对我国计算机信息系统现状充分调查分析研究后，融合国家保密局《涉及国家秘密的信息系统终端安全与文件保护产品技术要求》、BMB-15《涉及国家秘密的信息系统安全审计产品技术要求》、BMB-22《涉及国家秘密的信息系统分级保护测评指南》的要求，研发了《核安智华终端安全登录与文件保护系统》，来解决当前计算机信息系统存在的安全问题。

该系统以“综合安全防护”为理念，采用保密技术手段，从根本上杜绝了内网计算机信息系统的安全隐患，提高了计算机信息系统的安全防范能力，变被动整改为主动防护。

二、 系统防护目标

- 禁止移动存储介质的交叉混用
- 防止摆渡木马窃取内网信息
- 杜绝计算机违规联接互联网
- 监控记录U盘操作和违规外联日志
- 实现外部数据向内网计算机的单向导入
- 实现文件保险箱透明加密和隐藏加密
- 实现系统登录的双因子身份认证和锁屏保护
- 实现对内网计算机和移动存储介质的信息登记备案
- 实现内网计算机违规外联后向国家级、省级、地市级等报警平台报警

三、 系统防护原则

（一） 对计算机及网络“分类管理、分级保护”

采集计算机硬件信息并与终端计算机的单位、部门、使用人、物理位置等信息匹配，达到国家保密局要求的“分级保护、分类管理”目标。

（二） 对计算机信息系统主动防御

对计算机信息系统及关键泄密部位进行主动技术防御，消除安全隐患。并且对计算机的违规行为主动监控，一旦发现立即告警和阻断。该系统的主动防御策略涵盖了身份认证、电子登记、U盘注册发行、移动存储介质管控、防止间谍木马和摆渡木马攻击、非法外联检测阻断与报警、日志审计等安全策略。

(三) 从系统内核底层进行有效综合防护

本系统所构筑的防御体系始终运用底层内核技术。从底层驱动到文件安全管理器，从专用通讯协议中所用的校验到专用文件系统的实现，从认证应用程序到文件完整性认证，这些底层技术都有效的保障了系统综合安全防护目标的实现，使得该系统具备了相当高的防护强度，来保障计算机信息系统的安全。

(四) 防控间谍木马、摆渡木马窃密

本系统以USB底层过滤驱动、保护驱动、专用文件系统、专用API、专用文件系统以及底层过滤驱动共同构建一个防范摆渡木马的整体安全体系，构筑在这一技术体系上的移动存储介质管控模块，具备了防范间谍木马、摆渡木马攻击窃密的功能。目前，该技术已经运用在外交部及全球220个驻外使领馆、国家密码管理局、国家机要局等国家重要部门作为专业防控间谍木马的防护系统。

(五) 保证用户或黑客不能篡改访问控制

系统具有多层次的防篡改保护特性，使得终端用户及黑客无法越权访问及入侵或篡改权限。

(六) 确保系统对所有设备使用进行管控

随着通信和存储协议数量的日益增多，保证终端所有外部设备的安全是至关重要的，本系统最大程度地对各种可能会使用到的设备进行授权和保护。

(七) 快速简便地对终端安全策略进行授权管理

管理员在授权状态下可以管理安全策略，权限的设置是基于“积极防护”的原则下进行。

(八) 终端事件日志记录与严重异常警告

对计算机的违规行为主动监控，一旦发现立即告警和阻断，并有日志进行详细记录。

(九) 避免造成网络或个人主机负担过重

避免对网络或个人终端节点的运行、存储资源产生过大负担。

(十) 对用户的最小干扰

所有策略机制在正常运行的条件下，达到了对用户的最小干扰。只有在出现异常时，才弹出监控程序，用户日常使用感觉不到防护系统的存在。

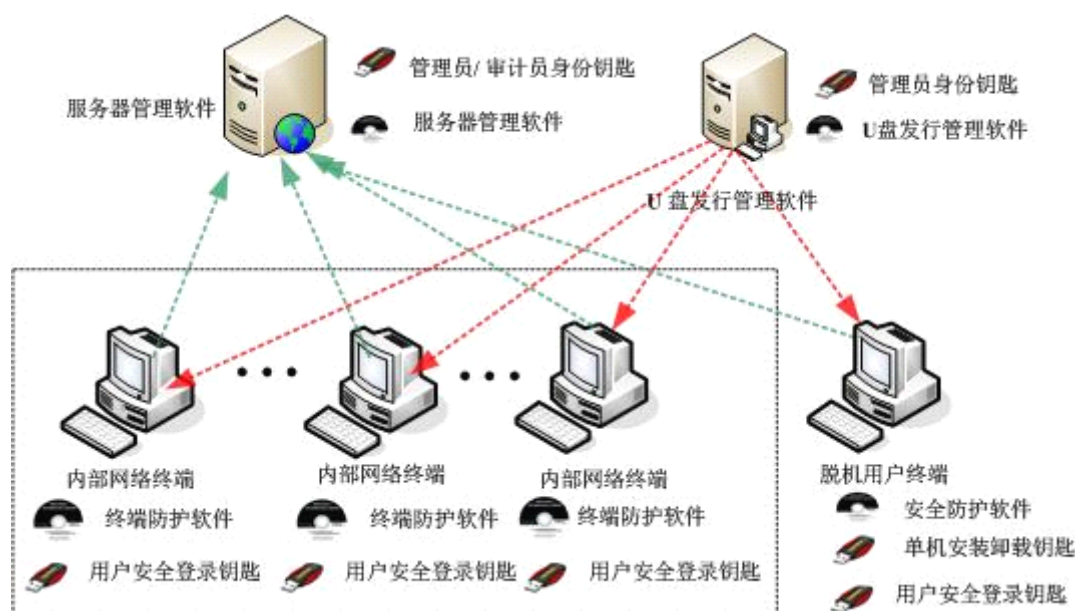
四、 系统组成和部署结构

(一) 系统组成

核安智华终端安全登录与文件保护系统由服务器管理软件、U盘发行管理软件和终端防护软件组成。系统硬件由管理员身份钥匙/审计员身份钥匙和安装卸载钥匙组成。

系统部署环境由管理中心服务器、U盘发行管理计算机和终端计算机组成。管理中心服务器用于部署服务器管理软件，U盘发行管理计算机用于安装U盘发行管理软件，终端计算机用于安装终端防护软件。

(二) 系统部署



五、 系统主要功能介绍

(一) 对计算机及网络的“分类管理”

1. 终端计算机电子登记和信息备案

通过全面对计算机分级分类，登记备案计算机的单位、部门、使用人、物理位置等信息，采集计算机硬件信息自动匹配到责任人，达到国家保密局要求的分级保护、分类管理的目标。

2. 移动存储介质电子登记和信息备案

对移动存储介质分级分类、登记备案。备案信息包括U盘的流水号、单位、部门、使用人、U盘状态、U盘类型等。

(二) 终端计算机安全登录认证与保护

采用全球领先的双因子认证机制，对用户登录计算机系统的身份进行认证。

用户登录系统需要验证合法的USB钥匙和用户口令，此双因子认证体系有效地避免了非法用户登录计算机。同时在用户离开计算机时，可以拔除USB钥匙锁定计算机，防止非法用户偷窥、拷贝和删除文件。本系统可以通过禁用安全模式来防止非法用户对计算机进行操作。

(三) 终端计算机重要文件加密保护和隐藏加密保护

用户可以通过USB钥匙对终端计算机的重要文件进行加密保存。单纯的软件加密很容易被别人破解造成信息外泄，核安智华终端安全登录与文件保护系统采用硬件加密，大幅度提高了数据的安全性。

用户还可以对一些重要的、不愿意让其他人看到的文件，通过文件保险箱加密保护。文件保险箱对存放的文件进行了透明加密，当用户拔出USB钥匙后，文件保险箱及文件会自动隐藏，即使有人查看计算机，也无法看到文件保险箱和被隐藏加密的文件。

(四) 文件粉碎擦除保护

本系统集成文件粉碎擦除功能。被粉碎擦除的文件，用专用恢复软件也不能恢复，有效保证了文件删除后被恢复的风险。

(五) 违规外联行为监控审计和主动防御

1. 终端计算机违规外联行为检测、阻断

能够完全、准确的探测出终端计算机通过任何方式（拨号、有线网卡、无线网卡、蓝牙、红外等）试图连接互联网的违规外联行为，发现违规外联行为后立即实施阻断、告警，并生成违规外联日志。

2. 终端计算机违规外联后向国家级、省级、地市级等报警平台报警

发现违规外联行为时，自动向服务器管理软件发送报警信息。同时向所有预先设置好的违规外联报警平台（国家级、省级、地市级、区县级）发送报警信息（是否向违规外联报警平台报警根据各地保密局要求和各单位实际情况确定）。

(六) 移动存储介质使用管控和主动防御

1. 内部专用U盘的发行和回收

U盘发行管理软件可以通过专有技术将通用U盘发行为专用U盘，同时可以为发行的专用U盘设置登录口令和自动透明加密。

发行后的专用U盘可以限定在本单位或本部门范围内使用，在限定范围外的计算机上禁止使用，也不能格式化。如果内部专用U盘设置了密码验证，需要输入正确的密码才能使用；如果设置了自动透明加密，写入U盘的所有文件将被自动透明加密，即使U盘丢失后被物理破解，也无法读取存储的数据。

2. 摆渡U盘的发行和回收

为了方便内部数据向外部安全摆渡，同时能够防控摆渡木马窃取内网信息，U盘发行管理软件可以通过专有技术将通用U盘发行为安全摆渡U盘。安全摆渡U盘在安装终端安全防护软件的计算机和未安装终端安全防护软件的计算机上均可使用，保证内部数据向外部交换的过程中防控摆渡木马窃取内部资料。

3. 终端计算机移动存储介质的底层驱动防护

任何模式下（包括正常模式、安全模式），终端安全防护系统能根据移动存储介质的类型，控制其授权接入。

移动存储介质插入终端计算机时，过滤驱动完成对移动存储介质的配置，底层驱动获取移动存储介质的控制权，Windows不知该设备的存在，计算机托盘和磁盘管理器中看不到盘符，任何程序或个人无法通过Windows读写移动存储介质，只有通过U盘文件管理器才能读写移动存储介质。

4. 实现数据的单向导入及U盘病毒过滤

安装有终端安全防护软件的计算机，只能使用本单位发行的U盘，未经发行的普通U盘只能单向导入，但不影响USB鼠标、键盘、打印机等其他设备的正常使用。同时，“U盘文件管理器”具有对U盘内自动感染型病毒的阻止和过滤功能。

5. 防控间谍木马、摆渡木马攻击窃密

核安智华终端安全登录与文件保护系统以USB底层驱动技术为依托，通过文件认证、读写安全策略、专用API、专用文件系统以及底层过滤驱动共同构建一个防范摆渡木马的整体安全体系。构筑在这一技术体系上的移动存储介质管控模块，具备了防范间谍木马、摆渡木马攻击窃密的功能。

(七) 终端计算机设备及端口审计和管理

通过对终端计算机设备及端口审计管理功能，能够充分保护网络中终端计算机的安全性，保护数据不被恶意盗窃，防止外接设备随意连接到计算机。

控制的端口包括：蓝牙设备、红外设备、IEEE 1394设备、IEEE 1394总线控制器、调制解调器（包括手机、PDA等），存储驱动器（包括FLASH存储卡等存储设备）、磁带机、Windows CE USB 同步设备（Windows CE平台手机、PDA等）、多功能设备（包括PCMCIA接口的调制解调器、网卡等）、软驱控制器、软盘驱动器。PCMCIA接口卡、SCSI及RAID控制器、CDROM驱动器、图像设备（包括摄像头、数码相机、扫描仪）、网卡、串口、并口、打印机、智能卡读卡器、网卡等。

(八) 终端计算机事件监控和日志审计

1. 终端计算机违规外联事件和U盘操作日志监控

自动记录终端计算机上的U盘操作和计算机违规外联日志，待服务器检测终端与内网服务器的联通状态，如果处于联通状态，自动将本地操作记录上传至服务器。如果处于脱机状态，将U盘操作和违规外联日志保存在本地“黑匣子”，管理员可以用专用工具导入到内网服务器数据库。

2. 终端计算机违规外联日志的管理和审计

终端计算机外联管理包括设置报警方式、查看新报警信息，查询、导出历史报警记录、生成报警日志报表等，并对计算机进行跟踪定位。

3. 终端计算机U盘操作日志及违规外联的管理和审计

U盘操作日志管理包括U盘文件拷入、拷出记录，查询、导出U盘操作记录、生成日志报表等，及对专用U外联报警及跟踪定位。

4. 终端安全防护软件安装卸载日志管理和审计

管理员登录管理中心后，可以审计终端安全防护软件的安装卸载记录。包括查询、导出安装卸载日志、生成日志报表等（单机用户终端安装卸载日志由管理员用专用工具从单机黑匣子里读取后，导入到管理中心）。

5. 日志支持本地黑匣子存储和网络实时上传

自动记录U盘操作和违规外联日志，待服务器检测终端与内网服务器的联通状态，如果处于联通，自动将U盘操作和违规外联日志上传至内网服务器。如果处于脱机状态，将U盘操作和违规外联日志保存到本地“黑匣子”，管理员可以用专用工具导出后，导入到内网服务器数据库。

6. 管理员操作日志审计

审计员登录管理中心后，可以对管理员的所有操作日志进行管理、审计。包括查询、导出日志、生成日志报表等。

7. 软件安全控制和安全域控制

（一）客户端防护软件保护机制

为了避免软件的随意安装和卸载，造成发行权的滥用和U盘使用范围的扩大，该系统设计全面周到的安全策略。对网内的客户端通过网络直接认证安装和卸载，对不在网内的单机，可以通过安装卸载钥匙来安装和卸载。

（二）审计员、管理员权限分离

为了保证系统中审计信息的正确性、权威性，防止同时掌握任意两种权利的内部人员进行非法操作，造成审计信息的丢失和错误，将管理员、审计员权限分离，并分别由不同人员掌握，有效的防止此类情况的发生。

（三）安全域控制

核安智华终端安全登录与文件保护系统对不同安全域之间的数据交换进行了控制，防止拥有同等权限的不同单位之间的数据泄露。

六、 系统优势及特点

- (一) **便利性**——无需改变现有系统结构，部署防控系统后可以轻松实现防范摆渡木马窃取内部机密信息的安全防护功能。
- (二) **安全性**——具有完善的安全设计体系，技术实现完全趋于底层设计，自主研发，安全强度高。
- (三) **可控性**——拥有完备的日志信息查询和审计功能。
- (四) **方便性**——支持普通U盘和安全U盘，这是防控系统最大的特点之一。它解决了采购专用U盘投入费用高的难题，可有效利用现有的普通U盘。

七、 典型用户

- 中华人民共和国外交部及全球 220 个驻外使领馆
- 中华人民共和国财政部 中华人民共和国民政部
- 中华人民共和国核工业部（集团） 中华人民共和国国务院
- 中华人民共和国机要局 中华人民共和国密码管理局
- 北京市通信管理局
- 唐山市保密局 唐山市委/市政府
- 昆明市委 昆明市委/市政府
- 玉溪市委 玉溪市委/市政府
- 楚雄市委 楚雄市委/市政府
- 秦皇岛保密局 保定保密局
-

在网络安全的世界里，如果不想亡羊补牢，就要做到料敌之先！

北京智华天成科技有限公司

北京市海淀区紫竹院路 1 号人济山庄 C 栋 1905

电话：+86-10-51651800