文章编号：1672-2892(2010)03-0341-04

USB外设网络集中监控装置的研制

高 杨[1]，李俊艳[2a]，王 强[2b]，陈营端[2a]

(1.中国工程物理研究院 电子工程研究所，四川 绵阳 621900；
2.西南科技大学 a.信息工程学院；b.制造科学与工程学院，四川 绵阳 621010)

摘 要：根据涉密USB外设信息安全管理的要求，基于网络客户端/服务器模型，研制了一种USB外设网络集中监控装置。根据构建的USB外设的唯一性标识，采用集线器收发装置扩展USB接口插槽，用嵌入式USB接口设备存放装置获取和识别每一个USB插槽上的USB外设的唯一性标识和状态信息，并通过Ethernet传输到远程的监控中心。采用Winsock编程技术在监控中心上实现网络服务器功能。通过远程监控中心使USB外设的借出和归还状态处于实时有效的监控之下，并能根据报警规则触发报警。该装置具有体积小、安装方便、可靠等优点，可通过涉密内网实现本单位涉密USB外设的集中管理。

关键词：信息安全；USB接口设备；监控；唯一性标识；客户端/服务器

中图分类号：TN918 **文献标识码：**A

Development of the networked surveillance device for USB peripherals

GAO Yang[1], LI Jun-yan[2a], WANG Qiang[2b], CHEN Ying-duan[2a]

(1.Institute of Electronic Engineering, China Academy of Engineering Physics, Mianyang Sichuan 621900, China;
2a.School of Information Engineering; 2b.School of Manufacturing Science and Engineering, Southwest University of Science and Technology, Mianyang Sichuan 621010, China)

Abstract: According to the information security management requirements to the USB peripherals, basing on the network client/server model, this study developed a network centralized surveillance device for USB peripherals. Basing on the unique ID of USB peripherals, adopting hub dispatch device to expand USB insert slot, it could obtain and identify every unique mark and status message for each USB peripheral in USB slots by using the inbuilt USB interface store system, then transfer them to remote supervising center by the Ethernet. It built web service functions by using Winsock technology in the controller center. It could supervise the USB interfaces status including lending and returning through the remote monitoring center effectively and in real-time. Moreover, it would give an alarm according to alarm device regulation. This device is of small size, high credibility, easy to be installed. And the centralized supervising of the USB interfaces can be realized through the confidentiality network.

Key words: information security; USB peripherals; surveillance; unique ID; client/server

按照保密管理规定，涉密单位职工使用完U盘等移动存储介质必须当天按时归还保密员，并存储在密码文件柜中(如部队的枪支入架)。保密文件柜由保密员人工管理，涉及借出、归还、监督、提醒等事项，难免疏漏。个别人员违规(未经审批许可)携带涉密U盘外出，可能导致涉密U盘丢失或涉密数据失窃，泄漏国家或商业秘密，造成巨大的损失。推而广之，涉密单位需要依靠创新的技术手段，加强USB外设，尤其是具有存储/摄录/网络通信功能的USB接口设备的管控力度，确保保密管理规章制度贯彻落实。

目前国内外主要采取以下措施保障USB接口设备的信息安全：采取物理去除USB接口芯片、软件禁用USB接口等措施，控制USB外设的使用；通过USB外设与主机绑定、审计日志等手段，避免USB外设交叉使用；通过信息加密等手段，避免USB外设中的敏感信息外泄[1-3]。

上述措施都有其固有的缺陷，必须综合使用且需配合内部USB外设的监管措施。这一方面，未见公开文献

收稿日期：2009-09-01；**修回日期：**2010-02-28
基金项目：中国工程物理研究院科学技术发展基金重点资助项目(2007A05001)；西南科技大学研究生教改资助项目(2007XJJG33)

报道。本文报道的 USB 外设网络集中监控装置，基于本单位的涉密信息网络，由服务器端和客户端两部分组成，可以实现 USB 外设的集中统一保管，在线实时查阅其保管状态，发现违规现象及时触发报警，为涉密单位完善 USB 外设的保密管理提供了一种新的可供选择的技术手段。

1 总体结构

图 1 为 USB 外设网络集中监控装置的原理图[4−5]。该装置基于本单位的涉密信息网络(通常为以太网(Ethernet))，由服务器端和客户端两部分组成。

服务器即远程的监控中心，它根据不同的用户、不同的要求，灵活地设计相应的人机界面。通过此人机界面，能够实时浏览、监测或控制所监控的 USB 接口设备的状态。同时，对于监控对象所发生的违规现象及时报警。

一个监控中心可以控制多套嵌入式 USB 接口设备存放装置。客户端即嵌入式 USB 接口设备存放装置中的网络控制器起到了桥梁的作用，实现与服务器端的网络通信。

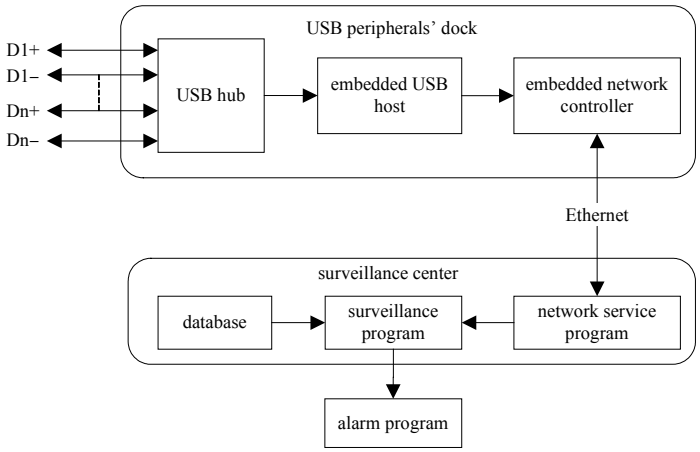

Fig.1 Schematic of the networked surveillance device for USB peripherals
图 1 USB 外设网络集中监控装置原理图

由于要实时地同时监控多个 USB 外部设备，采用了 USB 集线器来对 USB 接口插槽进行扩展。其中嵌入式 USB 主机与 USB 集线器收发装置相连，通过 USB 总线枚举识别插在集线器上的 USB 外设的唯一性标识[6]。

嵌入式网络控制器与嵌入式 USB 主机相连，将 USB 外设唯一性标识和状态信息传给远程的监控中心。

数据库查询与比较模块一端与网络服务器模块相连，另一端与数据库模块相连，通过网络服务器接收到的数据与数据库预存的数据进行比较，根据保密管理规定确定是否发出报警信号[4−7]。

2 嵌入式 USB 接口设备存放装置

嵌入式 USB 接口设备存放装置由 USB 集线器收发装置、嵌入式 USB 主机、嵌入式网络控制器组成。其结构原理图如图 2 所示。

图 2 中，嵌入式 USB 主机和嵌入式网络控制器采用 CYPRESS 公司的 CY7C67300 作为核心处理器，控制芯片内部的 USB 串行接口引擎(Serial Interface Engine，SIE)完成 USB 主机的功能，控制 MAX232 芯片进行电平转换，完成通用异步串行收发器(Universal Asynchronous Receiver/Transmitter，UART)内部参数设置，以供调试。

控制网络接口以完成嵌入式网络控制器实现网络客户端功能，通过外部存储器接口控制外部存储器以扩展代码和数据存储空间。

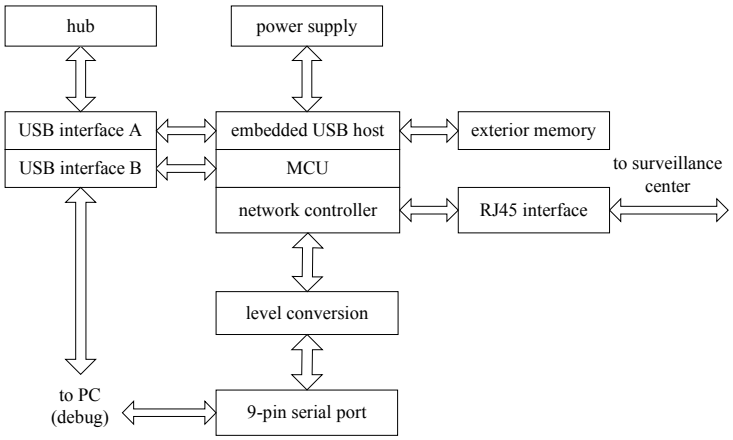

Fig.2 Diagram of the hardware structure of the embedded USB peripherals
图 2 嵌入式 USB 接口设备存放装置的硬件结构框图

通过 USB 接口 A 连接集线器实现 USB 接口的扩展。USB 接口 B 接主机进行调试。

3 监控中心

监控中心包括网络服务器模块、数据库模块、数据库查询与比较模块和报警模块。网络服务器记录网络传输过来的信息，与预存在数据库中的信息比较，确定当前 USB 接口设备所处状态，发现有违规操作的情况及时通

知使用者或发出警告信号。通过 VC 编程构建的操作界面完成 USB 接口设备信息的接收、显示、监管设置以及报警等功能。

通过 winsock 编程构建了监控中心中的网络服务器[8]。如图 3 所示，首先服务器端和客户端分别通过 Creat()创建各自的 Socket 对象；然后服务器调用 Listen 监听用户服务请求，客户端通过 Connect()建立与服务器的连接。服务器一旦接收到请求后，会调用 OnAccept()函数接收连接，客户端调用 Send()函数发出消息给服务器，服务器调用 Receive()函数接收，服务器也可以发送消息给客户端，客户端进行接收。最后，通信结束时，再调用 Close 关闭套接字的连接[4]。

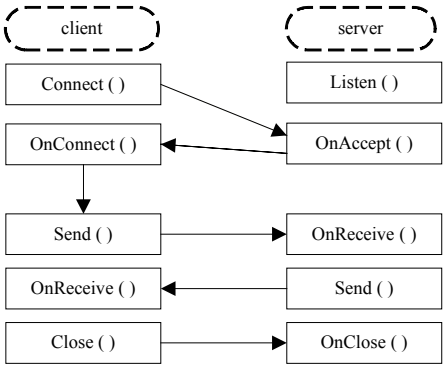

Fig.3 Schematic of the network controller and network server
图 3 网络控制器和网络服务器的工作原理图

监控中心的工作流程如图 4 所示，服务器端首先处于监听状态，判断是否有连接请求，如果有，则接受该连接，发送控制命令到远程的嵌入式 USB 接口设备存放装置，嵌入式 USB 接口设备存放装置响应命令发送 USB 接口设备的唯一性标识和状态信息。参考文献[5]对如何构建 USB 接口设备的唯一性标识和状态信息给出了仔细解释。监控中心接收该标识和状态信息，通过数据库进行存储、显示，通过与预存在数据库中的信息比较产生相应的报警信号。

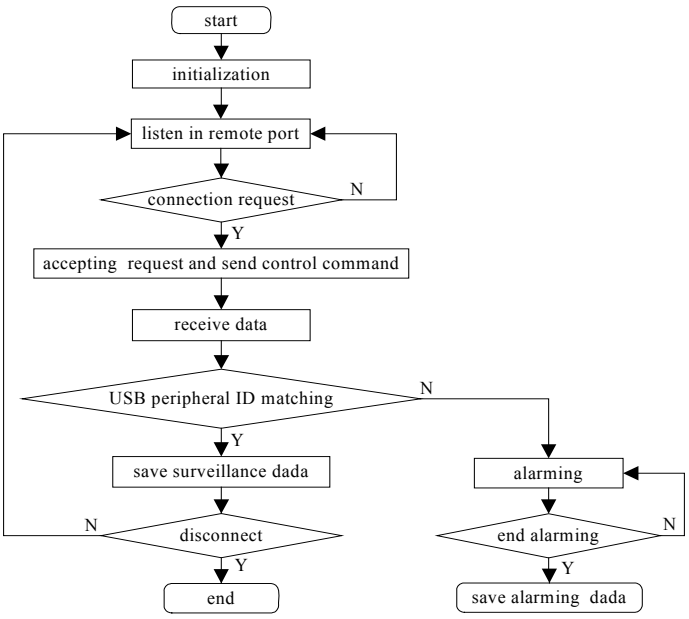

Fig.4 Work flow chart of the monitoring center
图 4 监控中心工作流程图

监控中心端的管理员程序窗口界面如图 5 所示。在管理员程序窗口，可以设置监控中心上的网络服务器端的 IP 地址和端口号。当客户端发起连接，服务器接收客户端传输过来的USB接口设备的唯一性标识和状态信息，管理员程序将接收到的唯一性标识和状态信息与USB接口设备使用者的信息绑定并存储在 ACCESS 数据库中以进行显示，以 U 盘为例，建立了已注册 U 盘、已插入 U 盘和未插入 U 盘的表格，通过软件编写的界面来显示。

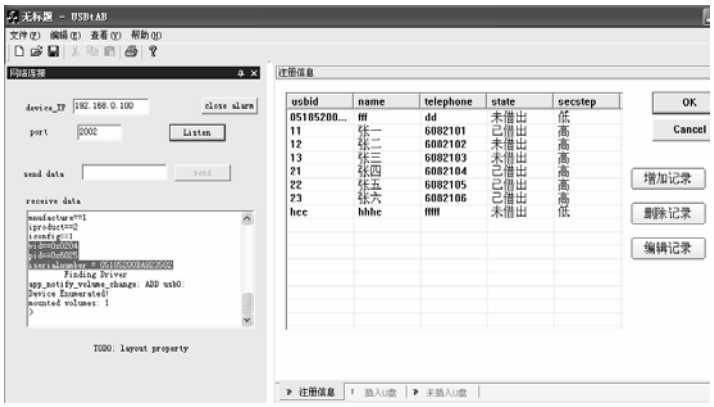

Fig.5 Screenshot of the administrator program window
图 5 管理员程序窗口截图

4　结论

研制了一种 USB 外设网络集中监控装置。通过对嵌入式 USB 接口设备存放装置和监控中心的构建，远程监控中心对比采集到的 USB 外设的唯一性标识和数据库里预存的信息是否一致，使 USB 外设的借出和归还状态处于实时有效的监控之下，并能根据报警规则触发报警，达到了涉密 USB 外设网络化集中监管的目的。

参考文献：

[1] 王黎,蔡皖东. 移动存储介质安全管理系统设计与实现[J]. 信息安全与通信保密, 2007(2):119-121. (WANG L,CAI W D. Design and implementation of the mobile storage medium safety management system[J]. Information Security and Communication Confidentiality, 2007(2):119-121.)

[2] 牛玲,李骞. 信息安全防护与USB安全控制技术[J]. 周口师范学院学报, 2006,23(2):109-110,118. (NIU L,LI Q. The safety protection of information and the technology of USB security control[J]. Proceedings of the Zhoukou normal college, 2006, 23(2):109-110,118.)

[3] 周明贵,姬学民. 移动存储介质管理在保密工作中的问题与对策[J]. 河北省社会主义学报, 2008(2):84-85. (ZHOU M G,JI X M. The problems and countermeasures of mobile storage media management in secrecy work[J]. Proceedings of Hebei province socialism, 2008(2):84-85.)

[4] 高杨,李俊艳,刘婷婷. 涉密U盘远程监管系统与方法:中国,200810147784.5[P]. 2008-12-05. (GAO Y,LI J Y,LIU T T. Remote surveillance method and device for classified flash disk:CN,200810147784.5[P]. 2008-12-05.)

[5] 高杨,李俊艳,白竹川,等. USB接口设备网络化的集中监管装置及监管方法:中国,200910306025.3[P]. 2009-8-25. (GAO Y, LI J Y,BAI Z C,et al. Network centralized surveillance method and device for USB peripherals:CN,200910306025.3[P]. 2009-8-25.)

[6] 李俊艳,高杨,刘婷婷,等. U盘唯一性标识信息的构建与识别方法[J]. 电子技术应用, 2009,35(3):130-134,117. (LI J Y, GAO Y,LIU T T,et al. The construction and recognition method of U dish unique identification information[J]. Applications of Electronic Technology, 2009,35(3):130-134,117.)

[7] 李俊艳. 涉密U盘远程监管系统的研制[D]. 绵阳:西南科技大学, 2009. (Li J Y. Develop of the Networked Surveillance system for Classified USB Flash Drives[D]. Mianyang:Southwest University of Science and Technology, 2009.)

[8] 毕传林,倪志莲. Winsock控件在网络通信软件中的应用[J]. 九江职业技术学院学报, 2004(1):27-28. (Bi C L,NI Z P. The application of Winsock control in the network communication software[J]. Proceedings of Jiujiang occupational college, 2004(1):27-28.)

作者简介：

高　杨(1972-)，男，四川省绵阳市人，博士，副研究员，主要研究方向为传感器与检测技术.email:gaoyang@caep.ac.cn.

李俊艳(1984-)，女，河南省许昌市人，硕士，主要研究方向为电子信息工程.

王　强(1983-)，男，四川省内江市人，在读硕士研究生,主要研究方向为微电子机械系统(MEMS).

陈营端(1983-)，男，山东省枣庄市人，在读硕士研究生,主要研究方向为微电子机械系统(MEMS).