文章编号:1671-4598(2020)09-0202-04 DOI:10.16526/j.cnki.11—4762/tp.2020.09.040 中图分类号:TP309.1 文献标识码:A

税控 USB 终端设备安全过滤器的设计与实现

王 磊[1],宋 军[1],彭 铭[2],张晓航[3]
(1. 河南理工大学 计算机科学与技术学院,河南 焦作 454000;2. 启明星辰公司,郑州 450000;
3. 河南工业和信息化职业学院,河南 焦作 454000)

摘要:为了防止不法分子在 USB 设备与电脑连接时植入非法程序,从而窃取电脑中的敏感信息或控制电脑向外设发出非法指令,文章针对 USB—key 的接入安全问题,提出了建立黑、白名单的方案;传统的 USB—key 安全防范措施都是基于加密认证,未考虑税控机接入的 USB 设备安全性;因此,文章提出对接入的 USB 设备进行分类,并对不同类别的 USB 设备执行相应的处理方案;通过设计开发针对税控系统的硬件检测设备和软件控制程序,从物理层面对接入税控机的 USB 设备进行安全检测;文中给出了 USB 设备过滤器的硬件设计图和软件控制程序的流程图,并对几种有代表性的设备进行了测试;测试结果表明,该设备能够对 USB 设备合法性进行有效的检测,并对违规的 USB 设备做出相应的处理,提高了税控系统 USB—key 接入 USB 设备的安全性。

关键词:安全检测;设备过滤;USB—key

Design and Implementation of Tax Control USB Terminal Device Security Filter

Wang Lei[1], Song Jun[1], Peng Ming[2], Zhang Xiaohang[3]
(1. School of Computer Science and Technology, Henan Polytechnic University, Jiaozuo 454000, China;
2. Venus tech Company, Zhengzhou 450000, China; 3. Henan College of Industry & Information Technology, Jiaozuo 454000, China)

Abstract: In order to prevent lawless persons from planting illegal programs when USB devices are connected with computers, and stealing sensitive information in the computer or controlling the computer to issue illegal instructions to peripherals, this paper proposes a plan to create black and white lists for USB—key access security. Traditional USB—key security precautions are based on encryption authentication, without considering the security of USB devices connected to the tax control machine. Therefore, this paper proposes to classify the connected USB devices and implement corresponding processing schemes for different types of USB devices. Through the design and development of the hardware detection equipment and software control program for the tax control system, the security detection is carried out from the physical layer to the USB device connected to the tax control machine. The hardware design drawing and software control program flow chart of USB device filter are given, and several representative devices are tested. The test results show that the device can effectively detect the legitimacy of USB devices and deal with the illegal USB devices, which improves the security of USB—key access to USB devices in the tax control system.

Keywords: security detection; device filter; USB—key

0 引言

随着计算机通信技术的快速发展,USB 设备的使用日益广泛。在终端系统中,通常设有可外接设备的 USB 端口,这些端口根据不同的应用需求可插入不同的 USB 设备,例如税务部门[1-2]的自助税务终端可接入 USB—key,自助打印终端可接入 U 盘,以及银行系统自助终端可接入 U 盾。但是,传统的 USB 设备接入方式由于没有相应的安全保护技术,经常导致税务系统信息被盗取,外接设备携带病毒攻击系统[3],导致系统做出错误响应,如非法打印发票等问题。因此,对于 USB 设备的安全防护与检测成为了个人用户以及企业重点关注的问题。

关于企业内网被“USB 设备”侵入给出的解决方案有软件防护和硬件防护。软件防护是在 PC 上安装 USB 驱动过滤程序,能够过滤掉一些非法设备;硬件防护采取封存 USB 接口,即禁止 PC 机接入所有 USB 设备。税务系统为保障个人和企业的信息安全,采用 USB—key[4-7] 作为个人或企业身份认证设备,通过税务自助服务终端可验证 USB—key 用户身份,认证通过才可办理相关的业务。

收稿日期:2020-02-17; **修回日期**:2020-03-27。
基金项目:河南省重点科技攻关项目(192102210123,182102110333)。
作者简介:王 磊(1977-),男,博士后,副教授,主要从事嵌入式系统、物联网应用技术、网络控制方向的研究。
通讯作者:宋 军(1996-),男,甘肃人,本科,主要从事嵌入式系统、物联网应用技术方向的研究。

上述的 USB 设备安全防护检测方案存在以下几个方面的不足之处：

1）封存 USB 端口固然能减少 USB 设备的威胁，但使用的范围具有局限性，同时也会在个人使用 PC 时带来不便。

2）USB 驱动过滤程序[8]只能对系统带有的 USB 驱动程序进行操作，对未知的 USB 设备无法起到安全防护作用。

3）USB－key 适于在税务、银行等部门使用，在其他方面使用成本代价过高；其次，USB－key 只能保证 USB 设备中信息的安全性，对自动服务终端未起到安全防护作用。

综合以上几种 USB 设备安全防护检测方案，本文提出一种基于 STM32－USB 设备过滤装置的解决方案[9-11]。通过对接入的 USB 设备进行识别，将识别的类型与数据库中的黑名单和白名单进行对比，在白名单内便可与主机或服务终端进行交互，在黑名单内便拒绝其接入终端。数据库中记录终端或主机接入 USB 设备的历史信息，根据应用需求可动态地更改黑名单、白名单中的内容。

1　USB 设备过滤系统总体设计和功能模块

基于嵌入式系统 STM32 的 USB 设备过滤系统的设计由微控制器（STM32F105RCT6）[14]、USB 设备插拔检测模块、日志信息存储模块（SPI _ Flash）、RTC 时间模块、USB 信号切换模块和数据实时显示模块等部分组成。USB 设备插拔检测模块是通过检测 USB 端口 D＋、D－之间的电压变化，实现对 USB 设备插拔的检测。

USB 设备插拔检测模块检测到设备插入，由软件部分实现对 USB 设备进行枚举，与日志信息存储模块中的黑白名单（用户自定义）进行比对。USB 信号切换模块得到比对信息结果为白名单设备，将 USB 设备接入用户主机；若对比结果为黑名单设备，将其接入微控制器。最终将 USB 的设备信息记录在日志存储模块当中，并通过上位机软件进行 USB 设备信息和接入情况的显示。该检测系统如图 1 所示。

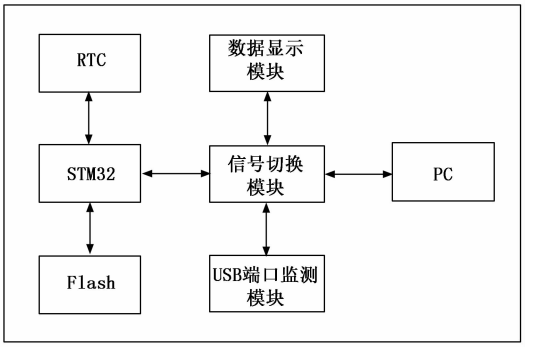

图 1　系统架构图

2　USB 设备过滤系统的硬件设计

2.1　STM32 最小系统电路设计

采用 ST 公司生产的 STM32F105 系列芯片。USB 设备过滤系统的 STM32 最小系统电路主要包括晶振电路、JTAG 下载电路、按键（K1）复位电路、USB－HOST 主机电路[12]、指示灯电路以及 I/O 口接排线座等 5 大模块电路组成。

2.2　信号指示灯电路

基于嵌入式系统 STM32 的 USB 设备过滤系统的信号指示模块电路的主要作用是实现显示设备的运行状况。该模块主要由单色发光二极管（LED0）和 RGB 发光二极管（LED1）构成，LED0 用于指示设备电源接入情况，LED1 用于指示设备的运行状态，蓝色表示正在检测接入的 USB 设备，红色表示拒绝该 USB 设备接入客户机，绿色表示放行该 USB 设备接入客户机。

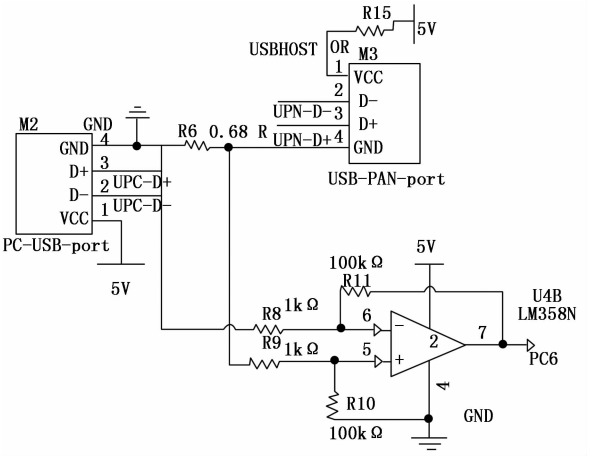

图 2　USB 设备插拔检测

2.3　USB 设备插拔检测模块

该模块是整个系统功能实现的关键，整个模块设计采用运算放大电路对 USB 端口的电压进行检测，当无设备插入时，CPU 循环检测 PC6 引脚的电平变化，当检测到该引脚电平为高电平时，程序进入任务处理函数中执行相关的函数指令。

2.4　RTC 实时时钟模块

RTC 实时时钟为系统提供一个可靠的时间，并且，在断电的情况下，RTC 实时时钟也可以通过电池供电，一直运行下去。RTC 通过 STRB/LDRB 这两个 ARM 指令向 CPU 传送 8 位数据（BCD 码）。数据包括秒，分，小时，日期，天，月和年。RTC 实时时钟依靠一个外部的 32.768 kHz 的石英晶体产生周期性的脉冲信号，每一个信号到来时，计数器就加 1，通过这种方式，完成计时功能。

在系统设计的日志信息存储模块中，日志处理程序需要将 USB 设备插入的具体时间信息记录下来，以便日后的历史信息查询。同时，在创建日志文件时，通过判断系统时间，以天为单位创建日志文件，方便用户对日志文件的管理和查阅。

2.5　USB 信号切换模块电路设计

USB 信号切换模块采用的主控芯片是“沁恒 CH440E”模拟开关。模拟开关是利用模拟器件（JFET 或 MOS）的

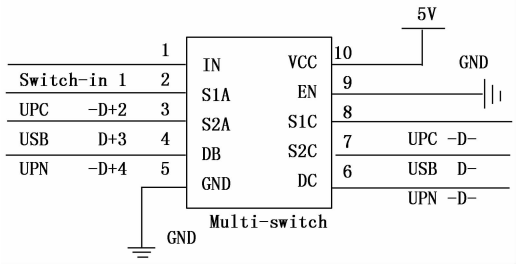

图 3 USB 信号切换

特性实现控制信号通路的开关，主要用来完成信号链路连接或断开的切换功能，具有功耗低、速度快、无机械触点、体积小和使用寿命长等特点。CH440E 芯片的工作电压 3.3～5 V，导通电阻约为 5 Ω，实现快速切换，切换时间小于 5 ns，支持 500 MHz 带宽，可应用于 VGA 信号、USB 信号等高速信号切换。多通道开关统一使能，统一切换，节省 IO 口。

通过多路开关芯片 CH440E，可将输入端接到 STM32 主机的 usb＋/usb－端口上，而将输出端分为 2 路信号，通过多路开关的 CS、IN 引脚的电平组成的二进制数，依此选择不同的信号线路。

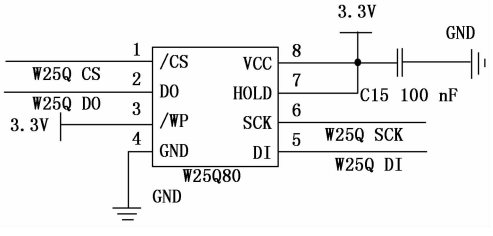

图 4 外部存储模块

2.6 日志信息存储模块

外部存储模块采用的是“华邦 W25Q80”，实际的容量为 8M－Bit，将 W25Q－CS 引脚、W25Q－SCK 引脚、W25Q－DO 引脚、W25Q－DI 引脚分别接到主控芯片的 PB12－PB15 引脚。W25Q80 芯片通过 SPI 总线与主控芯片进行通信。通过软件设计，在 W25Q80 芯片中开辟 6 M 的存储空间建立 FATFS 文件系统，加载文件系统便于对日志文件的管理以及存储空间的分配。在进行日志信息拷贝时可直接将日志文件拷贝到特定 U 盘中。

2.7 数据实时显示模块

数据实时显示模块是将微控制器的 USART1 模块的 RX、TX 引脚分别接至 CH340 芯片的 S1C、S2C 引脚。当微控制器未与 PC 机或终端进行通信时，将信号切换至 USART1，利用上位机软件通过串口通信的方式将微控制器发送的数据显示到 PC 端或显示到特定的终端上。当微控制器与 PC 机或终端进行通信时[13]，将 USART1 的数据通路切断。当微控制器与 PC 机结束通信后，将信号切换至 USART1。

3 系统软件设计部分

系统流程如图 6 所示。系统的主要执行流程如下。

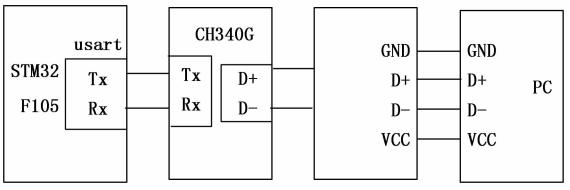

图 5 数据实时显示模块

1）程序进入到主函数 main（）当中，对系统的各个功能模块进行相应的初始化，包括时钟初始化、RTC 模块初始化、USB _ HOST 初始化、串口初始化、SPI _ FLASH 初始化等。

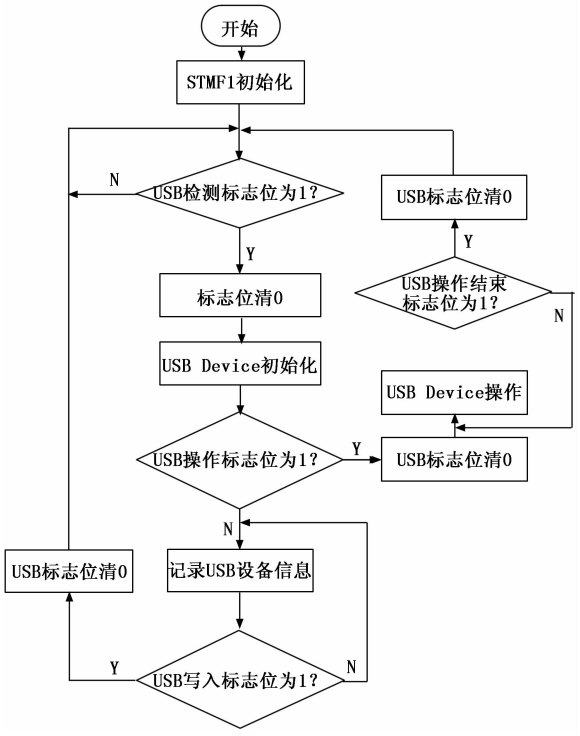

图 6 软件执行流程图

2）对 USB 端口的电压变化进行监测，当有设备插入时，USB 端口会产生一个电压变化，由运放电路模块捕获电平跳变。此时，判断 USB 检测标志位是否为 1。当标志位 1 时，说明检测到插入设备，程序继续向下执行，并将 USB 检测标志位清 0；否则，说明未检测到有设备插入，程序将会继续监测 USB 端口的电平变化。

3）USB 设备的初始化。提取 USB 设备的基本信息并加载相应的 USB 设备驱动程序，由 USB _ HOST 对 USB 设备进行枚举，判断出设备类型（包括设备的 PID、VID、生产商、制造商、序列号等信息）。

4）判断 USB 操作标志位是否为 1。当 USB 操作标志位 1 时，将 USB 操作标志位清 0，并根据不同的 USB 设备做出不同的决策，同时可在不同的应用场景也可以设置不同的操作指令。当 USB 操作标志位为 0 时，表明当前插入的 USB 设备没有操作权限，需要记录 USB 设备的基本信息，设备的基本信息以“设备插入时间—设备类型—生产商—序列号—

系统主机标号”的格式存储到外部的 flash 当中，并且使能拒绝信号灯，提示用户该 USB 设备无法接入主机。

5）判断 USB 操作结束标志位是否为 1。当 USB 操作结束标志位为 1 时，将 USB 操作结束标志位清 0，程序继续监测 USB 端口的电平变化。当 USB 操作结束标志位为 0 时，程序将延迟等待用户操作结束。

根据不同应用场景的需求，将黑名单内设备的相关信息打印到相应的终端，用户可实时监测自己主机接入 USB 设备的情况，并在同一时间内做出应对措施。

4　系统测试结果与分析

根据最初的系统设计要求，对系统进行了性能测试。该 USB 过滤设备板载两个 LED 灯，LED1 为电源指示灯，LED2 为信号灯。其中信号灯显分为 3 种情况：蓝灯（表示正在检测设备），红灯（表示拒绝设备），绿灯（表示放行设备）。

选择不同的设备，包括 USB－HUB、智能手机、税控盘、大容量存储设备和外设（鼠标）作为测试对象，每组设备进行 20 次的插拔操作，最终以拒绝率和放行率来验证系统功能，具体数据如表 1 所示。

表 1　设备测试表

测试设备	测试次数	预期结果	放行率	拒绝率
HUB	20	拒绝，红灯亮	0%	100%
手机	20	拒绝，红灯亮	2%	98%
税控盘	20	接入，绿灯亮	98.7%	1.3%
Mass storage	20	接入，绿灯亮	95%	5%
HID	20	拒绝，红灯亮	0%	100%

系统在 Flash 中保存了黑/白名单，USB 设备过滤器开机后可对接入的 USB 设备进行准确的识别，并能够根据预存的黑白名单进行设备的分类，黑白名单设置的内容如图 7 所示。以下是系统对黑/白名单以及日志存储模块的测试结果。

```
int Brand_Matching(char *STR)
{
  //char *str = STR;
  char str_tmp0[16]={0};
  //char str_tmp0L5[8]={0};
  //手机名称数组
  char smartDev_Name[16][10] ={ {"HUAWEI"},{"XIAOMI"},{"HTC"},{"QUALCOMM"},
                {"MEIZU"},{"OPPO"},{"APPLE"},{"ANDROID"},
                {"SAMSUNG"},{"OnePlus"},{"COOLPAD"},{"VIVO"}
              };
  //char str2[2][10] = {{"Aisino"},{"NISEC"}};
  char TAX_Dev_Str[2][10] = {{"AISINO"},{"NISEC"}};
  char white_list_str3[2][10]={{"FS"}};
```

图 7　黑白名单列表

1）大容量存储设备测试：

将 U 盘接入到 USB 设备过滤器上，USB 设备过滤器准确识别出接入设备的类型，下一步执行软件设置的“扫描危险文件”指令；扫描结果显示未发现危险文件，USB 设备过滤器上的绿灯亮起，U 盘便可以接入个人 PC，与其进行数据通信。实际操作图结果如图 8 所示。

2）USB－HUB 设备测试：

将 USB－HUB 接入到 USB 设备过滤器上，USB 设备过滤器准确识别出接入的类型，并在黑白名单中筛选当前接入的设备类型，USB－HUB 属于黑名单中的设备，USB 设备过滤器上的红色指示灯被点亮，USB－HUB 将被拒绝接入个人 PC。上位机软件将接入的 USB 设备信息打印出来并存入到日志存储模块当中。实际操作以及结果显示如图 9 所示。

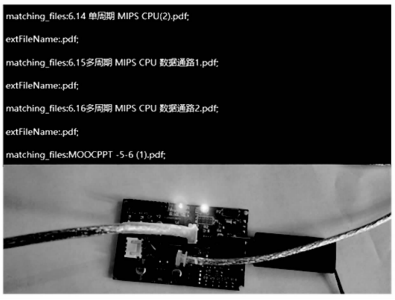

图 8　大容量存储设备测试图

图 9　USB－HUB 设备测试图

3）智能手机测试：

将智能手机接入到 USB 设备过滤器上，USB 设备过滤器准确识别出接入的设备属于智能手机设备，智能手机在黑名单内，USB 设备过滤器的红色指示灯被点亮，提示该设备无法接入到个人 PC。实际操作图以及测试效果图如图 10 所示。

图 10　智能手机测试图

（下转第 211 页）