

STM32 微控制器的 badUSB 防护设备

胡金亮, 陈家刚

(上海中兴软件有限责任公司 无线产品经营部, 上海 201203)

摘要: Bad Universal Serial Bus(badUSB)是一种利用 Universal Serial Bus(USB)接口来攻击计算机的设备,由于其伪装成正常的计算机 USB 外设,杀毒软件的防护对其没有任何作用,因此是一种极难防御的攻击手段。本文设计了一种利用微控制器 USB 主机来探测防御 badUSB 的设备,此设备成本低、体积小、安全性高,而且不影响 USB 通信速度。

关键词: badUSB;STM32F405RG;信息安全;TS3USB221

中图分类号: TN918.91

文献标识码: A

Protecting Device for badUSB Based on STM32 Microcontroller

Hu Jinliang, Chen Jiagang

(Wireless Product Operation Division, Shanghai ZTE Corporation, Shanghai 201203, China)

Abstract: Bad Universal Serial Bus (badUSB) is a kind of device to attack computers by Universal Serial Bus (USB) port. It can camouflage as a normal USB device. The computer protective measure by anti-virus software is invalid. The attack from badUSB is very difficult to block. This paper introduces and verifies a device to block the badUSB by micro-controller USB host. The device is low-cost, small volume and highly safe, and the communication bandwidth of USB port is normal.

Keywords: badUSB;STM32F405RG;information security;TS3USB221

0 引言

通用串行总线(Universal Serial Bus, USB)自 1996 年发布 1.0 标准以来经过近 30 年的发展,其通信速度已经由 1.0 标准的 1.5 Mb/s 提高到 USB4.0 的 40 Gb/s。随着 USB type-C 接口标准的发布,USB 接口不仅支持数据通信和正反插入,还支持高达 100 W 的供电功能。目前,计算机外设没有统一使用 USB type-C 接口的趋势,因此 USB 接口的信息安全变得越来越重要。

早期关于 USB 信息安全的问题主要集中于防护 U 盘病毒,利用 Windows 操作系统的自启动漏洞,将 U 盘内存在的计算机病毒自动执行,从而威胁信息安全,较为典型的是伊朗核设施受到通过 USB 设备传播病毒的攻击^[1],造成了巨大的损失,但这种在软件层面的病毒使用杀毒软件就可以很好地防护。因此,在免费杀毒软件普及之后,此类病毒在一般环境中几乎消失。

Bad Universal Serial Bus(badUSB)是在 2014 年美国拉斯维加斯举行的黑帽大会上由 Nohl 等人^[2]最先展示的一种攻击计算机的手段。badUSB 的攻击原理是利用特别制作的嵌入式设备模拟 USB 设备类型下的人机接口(Human Interface Device, HID)类或网络类设备,直接模

拟鼠标键盘或者网卡对目标计算机进行操作攻击,由于发动攻击的设备在计算机软件层面认为是正常的外设,因此防计算机病毒软件对 badUSB 的防护没有任何效果。造成这样情况的原因是 USB 枚举过程中计算机的 USB 主机对 USB 设备的完全信任,通信没有认证机制,USB 主机对 USB 设备的操作完全不做任何判断就执行,所以留下了这个巨大的漏洞。2016 年陈威等人^[3]讨论过 badUSB 对电力系统的巨大威胁,对于 badUSB 的防护已经到了刻不容缓的地步,但很长一段时间对于 badUSB 设备主流的防护方案都停留在禁止将未知的 USB 设备插在重要的计算机上,直到 2016 赵松银等人^[4]提出并设计了一种双向加密的 USB 通信方法,利用 USB 驱动对数据和控制信令进行加密和过滤,从而实现安全的 USB 通信。2020 年由张乃珩^[7]提出了一种监控驱动层面数据包的防护方案,这种方案对 USB 信令数据包进行监控,发现异常时切断 USB 通信,但上述这类利用软件加密过滤方法会影响 USB 通信速度,同时防护软件容易受到攻击,且开发难度极大,成本高。2016 年 Loe^[5]等人和 2017 年 Kang^[6]等人利用高级的微处理器作为 USB 主机,探测 USB 设备同时配合软件来检测 badUSB 设备,但这些方案有以下缺点:①使用微处理器实现成本较高,机制复杂;②使用了运行



Linux 系统的微处理器作为探测设备,本身也有可能受到 badUSB 的攻击;③用软件路由的方式连接 USB 设备和主机,通信速度慢。因此这些方案并不是最佳的防护方案。

因为 USB 通信是以主机为主导的通信过程,所以 USB 设备的信息无法隐藏,鉴于这个特点,利用无法被攻击的微控制器 USB 主机来对未知设备进行检查,以发现 badUSB 设备,检查完成后利用 USB 双路复用芯片将正常设备与计算机相连,badUSB 设备将会被断开,以保护计算机不被攻击。根据以上思路,本文实现并验证了一种 badUSB 防护设备,其成本低、体积小、安全性高,而且不影响 USB 通信速度。

1 实验装置

防护设备电路结构框图如图 1 所示,防护设备使用 USB 的公口从计算机上的 USB 接口取得 5 V 供电,由电源芯片(AMS1117-3.3V)将 5 V 电压转换为 3.3 V,供微控制器(STM32F405RGT6)和 USB 双路复用芯片(TS3USB221)使用;数据从 USB 的母口进入防护设备,经过 USB 双路复用芯片,一路进入 MCU 的 USB 主机控制器,另一路直接连通到防护设备的 USB 公口接口;同时利用 MCU 的端口来控制 USB 双路复用芯片,从而控制 USB 母口的信号是与 MCU 连接还是与防护设备另一侧的 USB 公口连接。

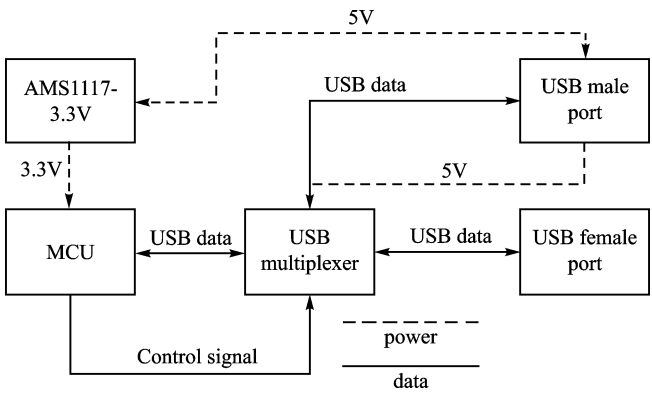
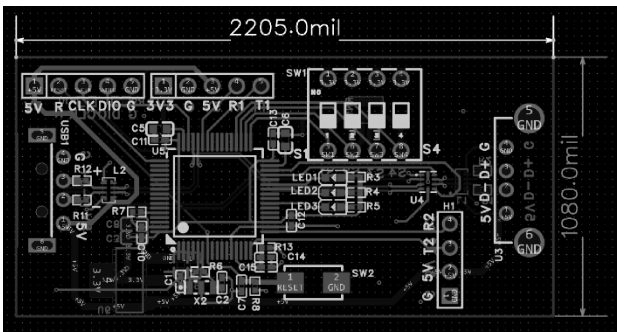


图 1 电路结构框图

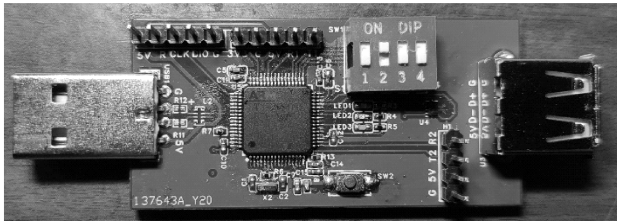
电路的 PCB 设计图及实物图如图 2 所示,其长为 2 205 mil(5.6 cm),宽为 1 080 mil(2.74 cm),非常小巧。

2 实验原理

当防护设备通过 USB 公口插入计算机时,整个防护设备从计算机取电,使 MCU 和 USB 双路复用芯片开始工作,此时 MCU 中的程序命令 USB 双路复用芯片将 USB 母口与 MCU 的 USB 主机控制器相连,等待未知 USB 设备通过防护设备上 USB 母口与防护设备连接。当检测到有 USB 设备接入时,MCU 的 USB 主机接口配合



(a) 无覆铜PCB设计图



(b) 实物图

图 2 PCB 设计图及实物图

内部的 USB 主机协议程序对连接的 USB 设备进行枚举,完整查看 USB 设备的信息,通过读取 USB 设备中的接口描述符判断设备的种类,目前在 USB 协议协会的官网^[8]上可以查询到如表 1 所列的接口类信息,经过 MCU 的

表 1 USB 接口描述符类^[8]

Base Class	Descriptor Usage	Description
01h	Interface	Audio
02h	Both	Communications and CDC Control
03h	Interface	HID (Human Interface Device)
05h	Interface	Physical
06h	Interface	Image
07h	Interface	Printer
08h	Interface	Mass Storage
0Ah	Interface	CDC - Data
0Bh	Interface	Smart Card
0Dh	Interface	Content Security
0Eh	Interface	Video
0Fh	Interface	Personal Healthcare
10h	Interface	Audio/Video Devices
12h	Interface	USB Type - C Bridge Class
13h	Interface	USB Bulk Display Protocol Device Class
3Ch	Interface	I3C Device Class
DCh	Both	Diagnostic Device
E0h	Interface	Wireless Controller
EFh	Both	Miscellaneous
FEh	Interface	Application Specific
FFh	Both	Vendor Specific

USB 主机查询后,若设备信息中出现危险 HID 类和网络类信息,则 MCU 就会点亮“警告 LED 指示灯”并终止后续操作;若未检测到上述可能存在的危险类,则 MCU 命令 USB 双路复用芯片将 USB 的母口与公口直接相连,并点亮“通过的 LED 指示灯”,这样 USB 设备就直接与计算机相连。整个设备程序的工作流程如图 3 所示。

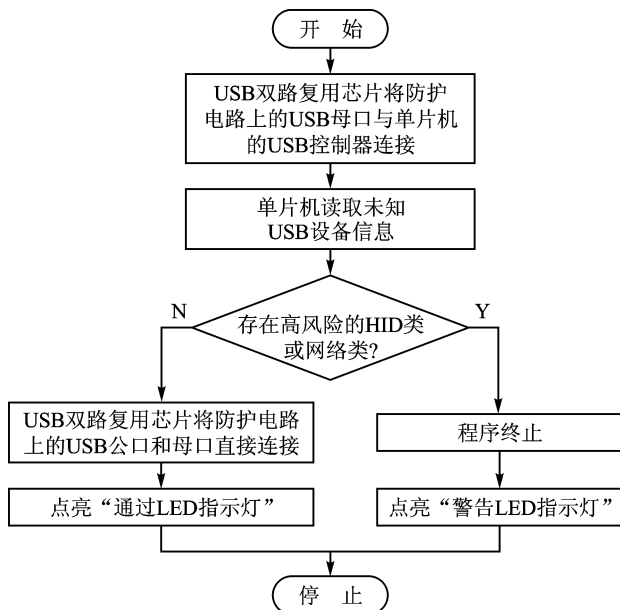


图3 防护设备工作流程

防护设备在未知 USB 设备与计算机建立数据连接前,先通过 MCU 中的 USB 主机协议检查未知 USB 设备。若确认没有危险的类,则令设备直接与计算机相连;反之,则终止流程,给出警告指示。

采用本方案的 badUSB 防护设备有以下优点:①采用微控制器,成本低且体积小;②相比于微处理器,微控制器 USB 主机协议栈软件更加简单,不可能被 badUSB 攻击,安全性高;③确认安全后,利用双路复用芯片连接被保护的 USB 主机和 USB 设备,由于没有 USB 数据路由过程,通信速率更高。

3 实验结果

分别使用 U 盘、鼠标和 USB 转串口模块来测试防护设备,上述 3 种 USB 设备分别代表了 MSC 类、HID 类和 CDC 类,根据表 1,上述 3 类设备的接口描述符编号为 08h、03h 和 02h。

首先将 U 盘插入防护设备的 USB 母口,再将防护设备的公口插到计算机上,同时将防护模块的串口连接到 USB 转串口模块上,最后将串口模块通过 USB 接口连接到计算机上。在串口助手软件上可以得到如图 4 所示的输出信息。

```

USB Device Connected
USB Device Reset Completed
PID: 1666h
VID: 951h
Address (#1) assigned.
Manufacturer : Kingston
Product : DataTraveler 3.0
Serial Number : E0D55EA574D71730C87506AF
Enumeration done.
This device has only 1 configuration.
Default configuration set.
No registered class for this device.
access
USB Device disconnected
class:0x8
  
```

图4 U 盘连接时串口输出信息

可以发现,MCU 上的 USB 主机接口准确识别了 U 盘的接口描述符类编号为 08h,对比表 1 可知是 MSC 类,因此防护模块放行,将 U 盘直连到计算机上正常工作。

之后将键盘与防护设备相连接进行实验,实验步骤与 U 盘的实验步骤相同,此时在串口助手上的输出如图 5 所示。

```

USB Device Connected
USB Device Reset Completed
PID: 2107h
VID: 413ch
Address (#1) assigned.
Manufacturer : Dell
Product : Dell USB Entry Keyboard
Serial Number : N/A
Enumeration done.
This device has only 1 configuration.
Default configuration set.
Device remote wakeup enabled
Switching to Interface (#0)
Class : 3h
SubClass : 1h
Protocol : 1h
Keyboard device found!
HID class started.
deny
USB Device disconnected
class:0x3
  
```

图5 键盘连接时串口输出信息

可以发现,此时识别的接口描述符类型编号为 03h,对比表 1 可知,USB 为 HID 类,这个类为高危类型,因此防护设备将键盘与 MCU 主机接口断开,且不与计算机的 USB 接口相连,有效阻止了潜在的 badUSB 设备攻击。

最后将一个利用 STM32 MCU 制作的飞控与防护设备相连进行实验。根据内部的固件程序,飞控的 USB 接口会虚拟成一个 USB 串口(CDC 类),用于与计算机上的上位机配置软件进行通信。实验步骤与上边两次的实验过程相同,此时在串口软件上的输出如图 6 所示。

可以发现,此时识别的接口描述符类型编号为 02h,对比表 1 可知是 CDC 类,因此防护设备放行,将飞控直连到计算机上正常工作。

```
USB Device Connected
USB Device Reset Completed
PID: 5740h
VID: 483h
Address (#1) assigned.
Manufacturer : EmuFlight
Product : CrazyBee F4 FR
Serial Number : 0x8000000
Enumeration done.
This device has only 1 configuration.
Default configuration set.
No registered class for this device.
access
USB Device disconnected
class:0x2
```

图6 飞控板连接时串口输出信息

由 MCU 调试串口输出的信息可以发现,STM32 的 USB 主机协议准确识别了上述 3 个 USB 设备的信息,得到上述 3 个设备的类型,根据程序禁止 HID 类的 USB 设备连接计算机,放行 MSC 类和 CDC 类的设备与计算机连接,有效防护了可能存在 badUSB 设备的 HID 类 USB 设备。判断成功后,USB 设备直接通过 PCB 线路与计算机直接相连,由于没有经过 USB 协议解析,所以通信的速率没有降低,不影响设备的正常使用。

4 结 语

本文利用 STM32 MCU 和 USB 双路复用芯片设计并实现了一种 badUSB 防护设备,实验结果表明,该防护设备能够有效防护可能存在 badUSB 的 HID 类的 USB 设备。本方案成本低、体积小、安全性高、通信速率高,但目前这个防护设备仅支持 USB2.0 及以下设备。后续可以改进设计,从而设备支持 USB3.2 和 USB4.0 协议,使应用更

69 测量结果如表 2 所列。通过传统 JTAG 方式完成一次图像跟踪器的 FPGA 升级需要两个小时,而利用本文的升级方式只需要 0.2 个小时,在效率上整整提升了 10 倍左右;另外,本文方案只需系统电缆连接正常即可,而不需要使用专用的仿真器,升级距离和稳定性都得到了较大提升。

表 2 测试比较结果

升级方式	电缆	距离/m	时间/h
传统方式	USB-JTAG 线缆	3	2
本文方式	RS422 串口线	1200	0.2

4 结 语

本文提出的基于 Stratix 系列 FPGA 可远程实现软件升级的方法,缩短了产品升级过程中消耗的时间,提升了

加广泛;此外,意法半导体提供了 AI 代码库,可以利用代码库进行训练,在 MCU 中部署一个神经网络模型,进一步识别 HID 类设备是否正常设备还是 badUSB 设备,以便于对 HID 类设备做更加详细的判断。

参考文献

- [1] Shin S, Gu G. Conficker and beyond: a large-scale empirical study[C]//Proceedings of the 26th Annual Computer Security Applications Conference, 2010: 151-160.
- [2] Nohl K, Lell J. Bad USB - On accessories that turn evil[C]//Black Hat USA, 2014: 1-22.
- [3] 陈威, 陈乐然, 徐小天, 等. USB 设备对电力工控系统的威胁[J]. 华北电力技术, 2016(7): 5.
- [4] 赵松银, 郁滨. USB 安全连接方案设计与实现[J]. 系统仿真学报, 2016, 28(6): 6.
- [5] Loe E L, Hsiao H C, Kim T H J, et al. Sand USB: An installation-free sandbox for USB peripherals[C]//2016 IEEE 3rd World Forum on Internet of Things (WF-IoT). IEEE, 2016: 621-626.
- [6] Kang M, Saiedian H. USB Wall: A novel security mechanism to protect against maliciously reprogrammed USB devices[J]. Information Security Journal: A Global Perspective, 2017, 26(4): 166-185.
- [7] 张乃珩. 一种基于 Hypervisor 的 BadUSB 攻击防御方法[J]. 河南科学, 2020, 38(9): 1400-1408.
- [8] usb.org. Defined Class Codes[EB/OL]. [2023-06]. <https://www.usb.org/defined-class-codes>.

胡金亮(工程师), 主要研究方向为嵌入式系统、软件无线电、移动通信。通信作者: 胡金亮, predator_hjl@foxmail.com。

(责任编辑: 薛士然 收稿日期: 2023-06-16)

维修效率, 并将产品升级过程中造成的风险降到最低, 同时节约了系统的维护成本。

参考文献

- [1] 周琼, 周鹏. 单核 FPGA 系统的可靠性远程升级设计[J]. 中国新通信, 2018, 20(2): 47-49.
- [2] 刘永恩, 王俊芳. FPGA 远程升级技术的分析与实现[J]. 无线电工程, 2012, 42(9): 48-50, 60.
- [3] 吴冬冬, 杨晓君, 张佩珩. 一种 FPGA 的远程系统升级方法[J]. 计算机工程与应用, 2006, 18(1): 86-89.

王晓辉(硕士研究生), 主要从事图像信息处理及嵌入式系统设计与开发。通信作者: 王晓辉, xmwangxiaohui@163.com。

(责任编辑: 薛士然 收稿日期: 2023-05-17)