恶意 USB 设备原理及防护措施研究

康云川[1],代 彦[2]
(1. 重庆三峡学院 计算机科学与工程学院,重庆 404000;
2. 重庆市文化信息中心,重庆 401121)

摘 要:在网络与信息安全领域中,计算机 USB 接口安全一直以来都面临着严峻的风险挑战,也是用户最容易忽略的问题,而恶意 USB 设备是计算机 USB 接口安全的主要威胁之一,它严重威胁着企业的信息安全与公民隐私信息安全。针对当前 USB 安全问题现状进行了分析,介绍了常见的恶意 USB 设备 Keylogger 与 BadUSB 的危害、攻击特性,对 Keylogger,BadUSB 硬件电路原理,硬件程序实现,攻击方法进行了详细剖析。通过 AVR 微控芯片构建出 Keylogger,BadUSB 设备,然后用其设备对计算机进行攻击实验,最终实现对目标主机的监听与控制,并研究拦截 Keylogger 记录监听与抵御 BadUSB 攻击的安全防护措施,为用户提供有效的安全保护解决方案。这些防护措施与解决方案能有效地保护公共信息安全与个人信息安全,能遏制 USB 接口层面信息安全事件的发生。

关键词:USB 安全;USB HID 攻击;信息安全;BadUSB;Keylogger
中图分类号:TP309.1 **文献标识码**:A **文章编号**:1673-629X(2020)01-0112-06
doi:10.3969/j.issn.1673-629X.2020.01.020

Research on Principles and Protection Measures of Malicious USB Devices

KANG Yun-chuan[1],DAI Yan[2]
(1. School of Computer Science and Engineering,Chongqing Three Gorges University,Chongqing 404000,China;
2. Chongqing Cultural Information Center,Chongqing 401121,China)

Abstract:In the field of network and information security,computer USB interface security has been facing serious risks and challenges,but also the most easily ignored by users,while malicious USB device is one of the main threats to computer USB interface security,which seriously threatens the enterprise information security and citizen privacy information security. We analyze the present situation of USB security problems,introduce the harm and attack characteristics of common malicious USB devices Keylogger and BadUSB,and analyze Keylogger,BadUSB hardware circuit principle,hardware program implementation,and attack methods in detail. The Keylogger,BadUSB devices are constructed by AVR microchip,by which the attack experiments are carried out on the computer. Finally,the recording and control of the target host are realized,and the security protection measures of intercepting Keylogger record listening and resisting BadUSB attack are studied to provide users with effective security protection solutions. These protection measures and solutions can effectively protect public information security and personal information security,and can curb the occurrence of information security events in the USB interface field.

Key words:USB security;USB HID attack;information security;BadUSB;Keylogger

0 引 言

计算机现有的 USB 接口给广大用户提供了相应的便利,例如移动存储设备数据的存取、移动设备的充电、输入设备的连接等。由于人们对信息安全意识的不足,即使有相应的了解或认知,关注点也仅限于计算机操作系统或应用软件安全,很少关注 USB 层面的安全问题。而 USB 接口提供了多条入侵路径[1],当外置设备插入 USB 接口时,操作系统会自动识别、配置并为接口加载独立的驱动程序,这也使得 USB 接口成为了不法分子入侵、窃取数据的途径之一,给用户带来了严重的安全威胁[2]。

据统计,全球数十亿台 USB 设备遭受过 USB

收稿日期:2019-03-07 **修回日期**:2019-07-10 **网络出版时间**:2019-09-25
基金项目:重庆市智慧文化云—文化大数据平台建设专项(P-NN-20180514150627210)
作者简介:康云川(1987-),男,高级工程师,硕士,研究方向为物联网技术、Web 技术、网络与信息安全。
网络出版地址:http://kns.cnki.net/kcms/detail/61.1450.TP.20190925.1525.064.html

Bomb、BadUSB 等攻击,例如 Stuxnet 蠕虫利用 USB 操纵伊朗核电站的离心机,最终破坏了伊朗核计划的关键部分[3]。国外有一款名为 USB Kill Stick 的设备,当用户将该设备插入任何一部计算机或者含有 USB 接口的电子产品,该设备会马上破坏整部计算机或电子设备,USB Kill Stick 没有病毒,破坏的原理是当用户插入 USB Kill Stick 后 USB 会通过信号线发送一道 220 V 的高压冲击波并摧毁设备。还有 2013 年的"棱镜门"事件,斯诺登通过 U 盘把机密带从安全局带了出来[4],可见 USB 安全问题防不胜防。

USB 攻击是一种新兴的技术,相比传统的攻击更为隐蔽,产生的安全威胁更大。由于其技术实现相比传统攻击更具有复杂性和危害性,文中对目前 USB 设备常见入侵攻击方式,Keylogger 与 BadUSB 设备软硬件原理进行深度剖析,并利用可编程 USB 设备进行恶意代码的烧录,实现对计算机键盘记录的监听,操作系统的远程控制及用户权限的获取,对攻击的防护提出相应的解决方案。这对于保障用户信息安全具有一定的重要意义。

1　常见恶意设备类型

常见的恶意 USB 设备有 Keylogger,BadUSB,其特点具有高度的隐蔽性、伪装性、跨平台特性并且能逃避安全软件的探测。攻击方法主要是通过可编程 USB 接口设备,对 USB 设备中的单片机逆向工程编程,烧录恶意程序,编程后的 USB 设备不受操作系统限制,具备窃取键盘记录、攻击计算机操作系统的功能。Keylogger 与计算机主机,键盘连接,监听用户键盘按键行为记录,实现计算机终端数据自动窃取,而 BadUSB 设备直接连接计算机主机 USB 接口,向终端发起攻击,实现创建操作系统超级管理员账号,开启远程访问端口,自动进行脚本程序远程下载并执行,自动创建免杀木马后门等,实现对计算机终端的远程控制[5]。

1.1　Keylogger

Keylogger 硬件采用可编程的 USB 接口硬件进行逆向编程,烧录窃听程序,Keylogger 用于监听用户在使用计算机过程中的键盘按键记录,安装监听设备或监听软件后的计算机。用户在操作系统界面输入管理员的权限信息,在线购物网站输入银行卡凭证,聊天工具产生的交流记录,登录社交系统的社交账号密码等,都将会被监听工具所窃取记录[6]。键盘按键监听也是计算机取证、信息收集最为流行的手段之一。该技术虽然给计算机取证信息收集带来了方便,但也常被不法分子所利用,常见的监听工具有监听软件与监听硬件,软件有 Keystroke、键盘记录者等[7]。由于软件监听不是文章所研究的对象,故不再赘述。

(1)隐蔽性强。

监听设备体积较小,可以藏匿于 USB 延长线、键盘中,整个监听过程并未对计算机操作系统带来任何影响,设备中并无恶意程序,只记录用户的按键信息,防病毒软件也很难探测与阻止该恶意行为,从而逃避防病毒软件的监控与评估。且监听过程不影响用户对计算机的任何操作,整个监听过程非常隐蔽,用户很难察觉,如图 1 和图 2 所示。

图 1　Keylogger 连接示意

图 2　Keylogger

(2)跨平台性。

这种设备具有良好的跨平台性,不受计算机操作系统的影响,对于 Linux、Unix、Windows、MacOS 等操作系统,只要终端具有外置键盘都无法摆脱 Keylogger 的监听。

(3)免驱动。

设备连接后运行于计算机底层,且计算机不需要安装额外的驱动,即插即用,实时性运行,只要计算机通电后设备就开始监听键盘的记录信息。

1.1.1　硬件原理

硬件部分是 Keylogger 的基础载体,是数据窃取的物理实现,其电路原理如图 3 所示。硬件主要由微控芯片(MCU)与存储芯片(EEPROM)等构成,MCU 完成计算机键盘记录的窃取,存储芯片则保存 MCU 窃取的记录数据,更高级的 Keylogger 还具有无线网络传输单元,监听者可以对目标主机的键盘记录通过网络进行实时监听。

从图 3 可知,整个窃取单元的设计并未改变 USB 原始的供电及数据传输模式,只是在接口的中间增加了单片机系统,与主机键盘形成旁路。VCC、GND 分别为 USB 电源与地线,D+与 D-为 USB 数据线。USB 接口连接了单片机控制系统,并对 MCU 8 位 RISC 单片机与 EEPROM 存储芯片的针脚 VCC 与 GND 供电,MCU 的 RA0 针脚与 RA2 针脚开始窃取从 USB 接口的 D+与 D-数据线上传输的数据,数据通过 MCU 整理后保存至 EEPROM 实现数据的窃取,而 PS/2 转

USB 的对应接线方式为 VCC->VCC,GND->GND, D+->CLK,D-->DAT[8]。

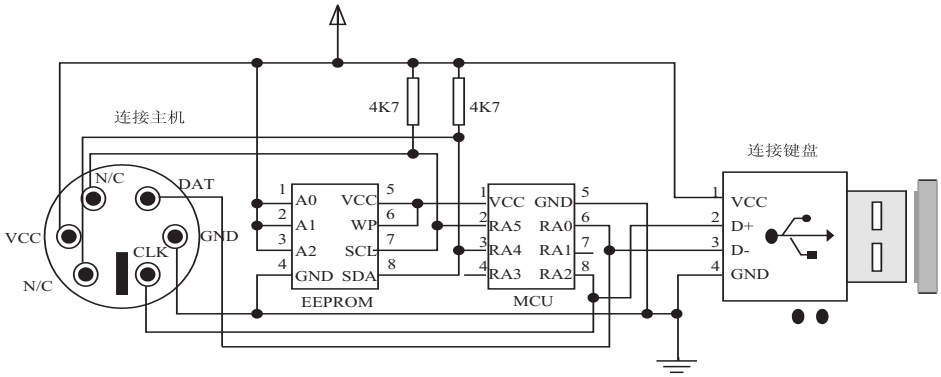

图 3 Keylogger 硬件电路

1.1.2 硬件程序

程序部分是 Keylogger 的系统核心,也是数据窃取与数据重放过程的逻辑实现。Keylogger 可以采用 C#语言或 Arduino 语言开发。以 Arduino 语言开发的代码为例,单片机采用 AVR ATMega32u4-AU 芯片为主控芯片,采用 PS2Keyboard、SD 等内置函数库[9],PS2Keyboard 库主要用于与键盘外围设备的通信,SD 库为 SD 内存卡提供读写操作,用于键盘监听记录的存储。整个键盘记录监听与存取程序代码如图 4 所示。

```
#include <PS2Keyboard.h>
#include <SD.h>
const int data_pin = 2;//为键盘的数据线DATA
const int IRQpin =  3;//键盘的CLK线
const int chipSelect = 10;//设定CS接口为10
File file;
PS2Keyboard keyboard;
void setup(){
  Serial.begin(9600);//初始化波特率
  pinMode(10, OUTPUT);  //设置CS接口为输出状态
  while(!SD.begin(chipSelect)); //CS口与SD卡通信
  keyboard.begin(data_pin, IRQpin);//键盘初始化
}
void loop(){
  if(keyboard.available()){//检查是否可用
     char c = keyboard.read();//读取键盘记录
     while(!(file = SD.open("new.txt", FILE_WRITE)));//打开SD卡，模式为可写模式
     file.print(c);//将键盘记录保存至SD卡
     file.close();//关闭文件操作句柄
  }
}
```

图 4 键盘记录存取程序代码

当用户敲击键盘后,Keylogger 收到数据,keyboard.begin()函数初始化键盘,SD.begin 函数初始化 SD 卡,keyboard.read()函数为读取用户的键盘行为操作,函数 SD.open()以可写的模式打开 SD 卡,函数 file.print()将数据保存至 SD 卡,最终实现键盘记录的监听与保存。

1.2 BadUSB

BadUSB 也采用可编程的 USB 接口硬件进行逆向编程,烧录攻击载荷程序,当攻击者向计算机或带有 USB 接口的终端插入 BadUSB,BadUSB 就会在用户不知情的情况下,模拟键盘输入行为,向终端数据接口发送恶意指令,几秒就可完成木马执行,完成操作系统漏洞提权、0Day 漏洞攻击等恶意行为操作;且整个攻击设备本身不带任何病毒或木马,攻击过程是通过模拟用户对计算机的正常操作,防病毒软件也很难探测与阻止该恶意行为,从而逃避防病毒软件的监控与评估。这种攻击行为给计算机信息安全带来了巨大的安全隐患[10]。

(1)隐蔽性强。

BadUSB 设备体积较小,可以藏匿于任何具有 USB 接口的设备中,整个攻击过程非常隐蔽,因恶意软件是固化在硬件芯片内,防病毒软件无法清除恶意代码,攻击速度非常快,用户很难察觉,外观如图 5 所示。

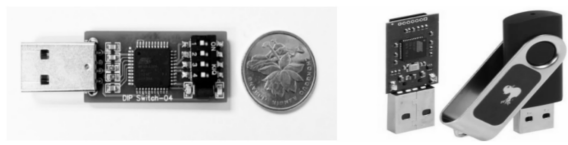

图 5 BadUSB

(2)跨平台性。

BadUSB 具有良好的跨平台性,不受计算机操作系统的影响,对于 Linux、Unix、Windows、MacOS 等操作系统,只要终端具备 USB 接口都无法逃脱 BadUSB 的攻击。

(3)免驱动。

设备连接后计算机操作系统会自动识别,不需要安装额外的驱动,即插即用,实时性运行,只要计算机通电后设备就可以对计算机实施攻击。

(4)传播性。

把病毒植入在 USB 设备的固件里,当用户插入 BadUSB 后,病毒可以在计算机磁盘里传播或复制,而传统的防病毒软件发现后无法清理病毒,即使用户对设备进行整体格式化清理,但仍不能清除它。

1.2.1 硬件原理

BadUSB 可采用 ATMega32u4-AU 为单片机主控芯片,该芯片是一款基于 AVR 的低功耗 8 位 CMOS 微控制器,并且支持 USB-HID,可用于模拟用户键盘,

鼠标操作行为。BadUSB 硬件部分主要分为单片机控制单元(MCU)与存储(SD 卡)两部分,MCU 主要用于计算机 USB 接口的通信与终端指令的发送[11],SD 卡用于保存对计算机恶意攻击的脚本命令,其硬件电路如图 6 所示。其中 D_1 和 D_2 二极管限制数据线上的电平,电阻 R_1 与 R_2 阻值均为 68 Ω,防止电流过载保护计算机终端 USB 接口与单片机电路,上拉电阻 R_3 阻值为 2.2 kΩ,用于分辨总线状态。

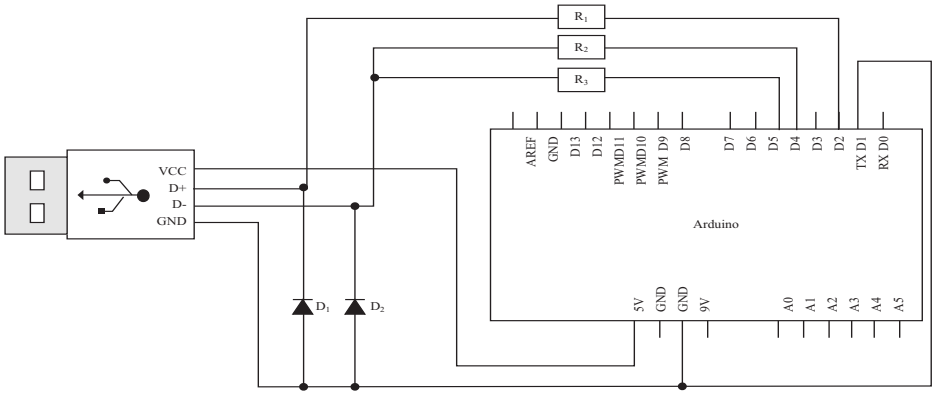

图 6　硬件电路

1.2.2　硬件程序

基于 ATMega32u4－AU 芯片构建的 BadUSB 设备,可使用 Arduino IDE 环境开发,Arduino IDE 封装了 ATMega32u4－AU 芯片常用的 USB 通信库、模拟键盘行为的 Keyboard 库、SD 卡库等[12]。模拟键盘输入主要采用 Keyboard. press( )、Keyboard. releaseAll( )、Keyboard. println( )等函数,Keyboard. press( )函数为模拟键盘按键操作,按下后并未释放操作,Keyboard. releaseAll( )函数为释放按键,Keyboard. println( )函数为模拟键盘敲出字符并换行,其中硬件恶意攻击程序示例代码如图 7 所示。

```
1  #include "Keyboard.h"
2  void typeKey(uint8_t key)
3  {
4    Keyboard.press(key);
5    delay(50);
6    Keyboard.release(key);
7  }
8  void setup()
9  {
10   Keyboard.begin();
11   delay(500);//延时
12   delay(3000);
13   Keyboard.press(KEY_LEFT_GUI);//按住win键
14   Keyboard.press('r');//按住r键
15   Keyboard.releaseAll();//win+r组合后 松开按键
16   delay(500);
17   Keyboard.print("CMD");//执行cmd命令
18   typeKey(KEY_RETURN);//回车
19   typeKey(KEY_RETURN);
20   delay(500);
21   Keyboard.println("net user test 1234 /add ");//创建管账号
22   Keyboard.println("net localgroup administrators test /add ");//将test账号设为管理员
23   Keyboard.println("netsh firewall set portopening tcp 3389 enable");//开启3389端口
24   typeKey(KEY_RETURN);
25   Keyboard.end();
26 }
```

图 7　BadUSB 攻击程序示例代码

图 7 中的第 13 行、14 行、15 行代码,模拟了同时按下键盘上的 win+r 键组合,弹出 Windows 操作系统的程序运行窗口;第 17 行代码自动在运行窗口输入 cmd 命令,弹出 Windows 操作系统命令行窗口;第 21 行与第 22 行代码,为 Windows 系统下创建用户权限的命令;第 23 行代码为添加防 Windows 防火墙规则,开启远程访问端口 3389;第 24 行代码为添加注册表允许计算机被远程访问规则。当把编写有以上的程序 BadUSB 设备插入至 Windows 计算机的 USB 接口后,该设备就会在数秒内完成权限的创建,完成远程访问端口的开启,实现对计算机的远程控制,实验结果,如图 8 所示。

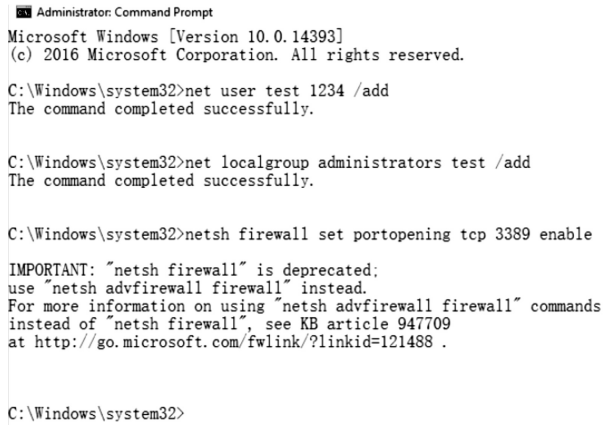

图 8　BadUSB 攻击实验

在攻击 Windows 7 及以上版本的操作系统时，BadUSB 还可以执行超级终端 powershell（new - objectSystem. Net. WebClient）. DownloadFile（）、Start - Process 命令，攻击设备自动进行恶意程序的远程下载与执行，实现对计算机操作系统进行的非法操作。

2 防护措施研究

2.1 Keylogger 防护措施

由于 Keylogger 设备体积较小、隐蔽性强，可藏匿于键盘，键盘延长线中，插在计算机主机上也不需要安装额外的驱动程序，插上后甚至计算机操作系统也无相应的提示信息，即插即用，这些特点使得用户很难防护 Keylogger 的监听。但只要用户意识到 Keylogger 的危害性，提高相应的安全意识，经常检查主机与键盘之间的连接是否安全可靠，中间是否存在可疑的设备，不使用不明来源的键盘，主机与键盘禁止任意插拔，在输入用户名、密码等敏感信息时，可采用软键盘输入信息，也可使用蓝牙键盘替代有线键盘，还可对键盘键值进行加密处理等，这些都可避免 Keylogger 设备对键盘记录的监听[13]。

用户的按键信息经过加密处理，计算机操作系统根据解密算法对键值进行解密获得真实的键值，键值加密原理如图 9 所示。以键盘上的字母“E”为例，“E”的键盘编码为 00_00_08_00_00_00_00_00，【引文】，如果对字母“E”的键盘编码加密，加密后的密文为##_127_##_##_##_##_##_##，用户在敲打按键“E”时，键值始终以密文的方式传送至计算机主机，在计算机主机接收端，通过系统底层过滤驱动对密文的键值信息进行解密操作，还原“E”的正常键盘编码。这样一来监听工具所监听的按键信息是加密后的密文，攻击者无法获得用户真实的记录，有效地避免了键盘按键被监听的风险，也避免了数据被窃取。

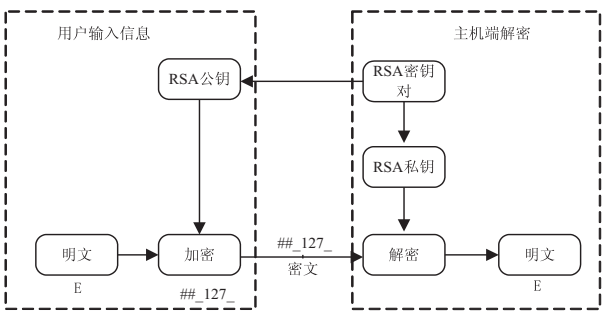

图 9 键值加密与解密过程

键值加密算法可采用 RSA 公钥加密方式。假设 C 为密文，M 为明文，发送端和接收端都必须知道 n 和 e 的值，d 为私钥由接收端保存不对外公开，公钥 KU = $\{e, n\}$，私钥 KR = $\{d, n\}$，加密解密中的模数 $n = pq$，p，q 为任意选择的两个素数，分别为 23 和 7[14]，$n = pq$ = 161。使用欧拉函数计算出整数数量 $\varphi(n) = (p - 1)(q - 1) = 132$。选择 $\varphi(n)$ 互素的数，并且小于 $\varphi(n)$ 的数 7 为 e 的值，$e = 7$。根据 $de \bmod 132 = 1$，$d < \varphi(n)$，求出 $d = 19$。求出公钥 KU = $\{7, 161\}$，私钥 KR = $\{19, 161\}$。

键盘键值采用 RSA 公钥加密算法，公式如下：

$$C = M^e \bmod n$$

键值密文解密算法的公式如下：

$$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$$

发送端对键盘按键“E”明文编码 8 进行加密处理，如下：

$$C = M^e \bmod n = 8^7 \bmod 161 = 127$$

其中 127 为按键“E”的密文。

接收端对发送端的密文进行解密处理，如下：

$$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n \cdot 127^{19} \bmod 161 = 8$$

2.2 BadUSB 防护措施

BadUSB 设备可隐藏于任何 USB 接口类型的设备中，其伪装性极强，使得用户很难防范来源 BadUSB 的攻击，而主要防护措施有以下六点：

（1）通过限制计算机 USB 接口的使用，不使用陌生的 USB 设备。

（2）开发相应的 USB 防护软件防止 BadUSB 设备对主机的直接操作，当 USB 设备插入计算机 USB 接口时，操作系统底层预先阻止 USB 设备对接口的任何行为，防护软件提示用户设备是否受信任，用户需输入相应的口令接受 USB 设备，避免 BadUSB 直接模拟键盘、鼠标行为，有效降低被攻击的几率。

（3）可采用 USB 硬件防火墙，计算机所有的 USB 接口不直接向用户开放，与 USB 硬件防火墙连接，防火墙向用户开放接口供用户使用，防火墙的内部具备 USB 设备枚举、内容检测等，USB 设备必须通过防火墙安全检测后才能接入使用[15]。防火墙原理如图 10 所示。

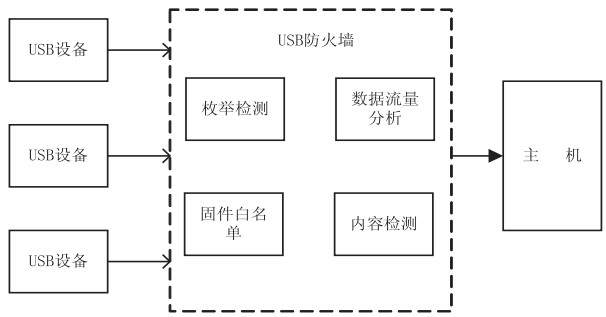

图 10 USB 硬件防火墙原理

（4）计算机 USB 外围设备采用固件签名算法、区块链等技术以确保固件不被篡改，防止对 USB 接口外围设备逆向编程，植入 BadUSB 恶意程序。

(5)建立 USB 设备白名单机制,操作系统底层判断 USB 设备固件 ID 是否已在白名单内,以防止非法 USB 设备的插入,从而保护计算机免受到底层的攻击。

(6)调整操作系统设备安装策略,例如在 Windows 操作系统中设置计算机本地策略组,建立基于 GUID 的可信 HID 设备的组策略,对 USB 设备加载进行严格限制,禁止操作系统 CMD 命令。

3　结束语

分析了常见的 Keylogger,BadUSB 设备软硬件原理,提出了应对安全风险的措施,可有效解决键盘记录监听,BadUSB 攻击等 USB 层面的安全问题,但这些措施在实际运用中还需对相关算法不断优化,安全策略进行调整。只有当外围设备被视为主机不可信的数据源时,USB 安全协议才会被创新,被访问设备的主动认证才能得到补充,才能从根本上消除恶意 USB 攻击。USB 层面的安全问题也是用户自身的问题,与用户的安全意识紧密相连,对信息系统安全性要求较高的用户应该提高使用 USB 设备的安全性意识,应该谨慎使用来自未知来源的 USB 设备,定期检查设备管理器,检查 USB 设备访问记录,以及制定合理的 USB 设备访问策略,才能将安全风险降到最低。

参考文献:

[1] 董晶晶,霍珊珊,袁　泉,等. 移动办公终端信息安全技术研究[J]. 计算机技术与发展,2018,28(1):155-158.

[2] 刘意先,慕德俊. 基于 CIA 属性的网络安全评估方法研究[J]. 计算机技术与发展,2018,28(4):141-143.

[3] 刘亚丽. 电网工控系统安全防护中流量异常检测的研究与应用[D]. 沈阳:中国科学院大学(中国科学院沈阳计算技术研究所),2018.

[4] 周　健,孙丽艳. 电子虚拟空间的信息犯罪分层研究[J]. 计算机技术与发展,2017,27(8):125-129.

[5] SAMTANI S,CHINN R,CHEN H,et al. Exploring emerging hacker assets and key hackers for proactive cyber threat intelligence[J]. Journal of Management Information Systems,2017,34(4):1023-1053.

[6] YAO L,FAN Z,DENG J,et al. Detection and defense of cache pollution attacks using clustering in named data networks[J]. IEEE Transactions on Dependable and Secure Computing,2018,99:1-11.

[7] HENDERSON A,PRAKASH A,YAN L K,et al. Make it work,make it right,make it fast:building a platform-neutral whole-system dynamic binary analysis platform[J]. IEEE Transactions on Software Engineering,2017,43(2):164-184.

[8] 姜小云,李昭春,吴　俞. 基于 STM32 的新一代天气雷达远程监控系统设计[J]. 计算机技术与发展,2017,27(5):196-200.

[9] SHANMUGAM M,SINGH M. Arduino based IOT platform for remote monitoring of heart attacks and patients falls[J]. Journal of Computer Science,2018,14(4):574-584.

[10] YOUNG N,DREES R. Cyber security for automatic test equipment[J]. IEEE Instrumentation & Measurement Magazine,2018,21(4):4-8.

[11] 闫　萌,邹俊伟,刘亚辉,等. 闪付卡重放攻击研究与 PBOC3.0 协议漏洞分析[J]. 计算机技术与发展,2018,28(4):148-151.

[12] CANNOLS B,GHAFARIAN A. Hacking experiment by using USB rubber ducky scripting[J]. Systemics,Cybernetics and Informatics,2017,15(2):66-71.

[13] CREUTZBURG R. The strange world of keyloggers - an overview,Part I[J]. Electronic Imaging,2017(6):139-148.

[14] 刘彦辰,王　箭,屈琪锋. 混合加密的宋词载体文本信息隐藏技术[J]. 计算机技术与发展,2018,28(1):138-143.

[15] KANG M,SAIEDIAN H. USBWall:a novel security mechanism to protect against maliciously reprogrammed USB devices[J]. Information Security Journal:A Global Perspective,2017,26(365):1-20.