

# WHID Defense: USB HID 攻击检测防护技术

吕志强<sup>1,2</sup>, 薛亚楠<sup>1,2</sup>, 张 宁<sup>1,2</sup>, 冯朝雯<sup>1,2</sup>, 金忠峰<sup>1,2</sup>

<sup>1</sup>中国科学院信息工程研究所 北京 中国 100093

<sup>2</sup>中国科学院大学网络空间安全学院 北京 中国 100049

**摘要** USB(universal serial bus)接口的出现为用户带来了便利,但也正由于它的便利性、使用广泛性使得其成为攻击者的攻击目标之一。常见的USB攻击主要有USB摆渡攻击和USB HID攻击,本文通过对USB协议漏洞以及恶意USB HID攻击工具的攻击特点的分析,提出了USB HID(human interface device)攻击模型并生成了相应的攻击数据流。基于以上研究构建了一个集按键注入攻击预警、捕获恶意USB HID攻击设备数据、干扰恶意USB HID攻击设备通信、风险等级分类与显示、用户身份管理与访问控制等功能于一体的恶意USB HID攻击检测防护平台——WHID Defense。经实验验证,WHID Defense按键注入攻击的拦截率为99.98%,目标数据捕获率为100%,干扰目标设备正常通信成功率为97.7%,功能完善,性能突出。相比现有检测技术,WHID Defense平台形成了多级防护体系,可以部署在个人电脑上进行实时防御,抵御了包括BadUSB等多种恶意USB HID工具的攻击。

**关键词** 恶意USB设备; HID攻击; USB组合设备; 攻击检测; 特征分析; 身份管理与访问控制; 风险分类  
**中图分类号** TP334 **DOI号** 10.19363/J.cnki.cn10-1380/tn.2021.03.08

## WHID Defense: Detection and Protection Technology for USB HID Attack

LV Zhiqiang<sup>1,2</sup>, XUE Yanan<sup>1,2</sup>, ZHANG Ning<sup>1,2</sup>, FENG Zhaowen<sup>1,2</sup>, JIN Zhongfeng<sup>1,2</sup>

<sup>1</sup> Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

<sup>2</sup> School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

**Abstract** The emergence of the USB (universal serial bus) interface has brought convenience to users, but it is also one of the targets of attackers due to its convenience and wide use. Common USB attacks mainly include USB ferry attacks and USB HID (human interface device) attacks. In this paper, we analyze the vulnerability of USB protocol and the attack characteristics of malicious USB HID attack tools, meanwhile, present a USB HID attack model generates the attack data stream. Based on above research, this paper constructs a detection and protection platform – WHID Defense, which includes key injection attack warning model, malicious data capturing model, communication interferes attack model, risk level classification and display model, user identity management and access control model, etc. The experimental results show that the interception rate of WHID Defense keystroke injection attack is 99.98%, the target data capture rate is 100%, and the normal communication success rate of jamming target equipment is 97.7%. Compared with the existing detection technology, the WHID Defense platform has formed a multi-level protection system, which can be deployed on a personal computer for real-time defense against attacks of various malicious USB HID tools such as BadUSB.

**Key words** malicious USB device; HID attack; USB composite device; attack detection; characteristic analysis; identity management and access control; risk classification

## 1 引言

硬件(hardware),指单片机、计算机硬件、软件程序的载体及交互的接口,手机、计算机、键盘等一切具备电子电路的设备,都可以称为“硬件”<sup>[1]</sup>。USB接口是一种被广泛使用的硬件接口之一,如图1所示

为USB接口标识。1996年1月,USB(universal serial bus) 1.0版本的正式发布正式拉开了USB接口的序幕,其定义了1.5Mbps低速和12Mbps全速两种数据速率<sup>[2]</sup>。

随着1998年USB 1.1版本的发布,USB接口开始被广泛使用。如今,USB已经发展到USB 3.2版本,

**通讯作者:** 薛亚楠, 硕士, Email: xueyanan@iie.ac.cn。

本课题得到国家自然科学基金资助项目(No. 61601460)资助。

收稿日期: 2019-04-02; 修改日期: 2019-04-26; 定稿日期: 2020-12-21

其最高传输速率也高达 20Gbps<sup>[3]</sup>。



图 1 USB  
Figure 1 USB

USB 接口简化和改进了个人计算机与外围设备之间的接口,以多种方式提高了易用性,由于该接口是自配置模式,用户无需对设备和接口进行任何干预即可使用。USB 接口实现了数据的高速率传输,具备多种供电模式,使用灵活,而且可以连接键盘、鼠标、U 盘、摄像头等多种外设。USB 作为一种输入输出接口的技术规范,被广泛应用于个人电脑及手机等移动通信设备中,而且在摄影器材、数字电视、游戏机、工控系统等领域中也广泛使用。USB 闪存盘是一种使用 USB 接口的数据存储设备,能够通过 USB 接口与任意符合 USB 传输协议的设备进行数据交互<sup>[4]</sup>。

随着移动互联网向物联网转移,智能硬件作为承载物联网的关键实体,也逐渐成为攻击者关注的焦点。如今,恶意攻击形式趋于多样化,过去基于软件环境所存在的安全隐患也在逐渐向硬件环境转移。此外,硬件安全不仅仅局限于整个硬件实体本身,其硬件接口中所存在的隐患也愈发明显,利用硬件接口发起恶意攻击也越来越成为攻击者的重要目标之一,USB 接口就是硬件接口攻防中的典型代表。2016 年 6 月,首次被检测出的震网(stuxnet)病毒是一种专门定向攻击核电站、水坝、国家电网等基础设施的“蠕虫”病毒。“震网”病毒经 U 盘传播,通过修改可编程逻辑控制器(PLC)的控制软件代码使 PLC 向用于分离浓缩轴的离心机发出错码命令完成攻击,其感染了全球超过 20 万台电脑,摧毁了伊朗浓缩轴工厂五分之一的离心机,破坏力之大显而易见<sup>[5-7]</sup>。2014 年甚至出现了通过修改 U 盘固件加入 HID 攻击技术的 BadUSB 技术,其中, HID 攻击技术是指通过将 USB 设备枚举为 HID 设备(如键盘、鼠标等)完成一系列系统级的破坏操作<sup>[8]</sup>。若攻击者将设备枚举为 HID 键盘,那么攻击者便获得了键盘权限,攻击者利用计算机系统本身对 HID 键盘高度可信的特点便可以通过模拟键盘操作完成一些恶意操作,破坏目标设备。同样,攻击者也可以将设备枚举为鼠标等进行相应恶意操作。

然而,目前针对 USB 攻击的防护大都集中于对 U 盘等可移动存储设备的文件扫描层面,旨在对

USB 可移动存储设备进行安全监控与访问控制,以保证此类设备存储内容安全,是一种软件层面的恶意文件型检测技术。但是对于 HID 设备则以硬件沙箱为主,需要对设备进行二次识别以及预定义授权等操作,过程繁琐,也大大削弱了 HID 设备的便利性。因此,针对 HID 攻击的桌面级防护手段成为检测 HID 攻击的最佳解决方案之一。

基于以上问题本文做了以下 2 个方面贡献:

(1) 分析了 USB 协议存在的漏洞以及 USB HID 攻击特点,提出了 USB HID 攻击模型,生成了 USB HID 攻击数据流,为研究人员从事相关研究提供理论基础及攻击数据。

(2) 提出了新型的针对 USB HID 攻击的检测防护思想及安全防护框架,设计了基于 Windows 平台的恶意 USB HID 攻击检测防护平台,并通过实验验证了该平台的功能和性能指标。同时,为研究人员研究 USB HID 攻击检测防护方案提供了实验验证平台和依据。

本文后续章节安排如下:第 2 部分介绍了近来 USB 攻击技术及恶意 USB 攻击检测防护技术的发展情况及特点;第 3 部分对 USB HID 脆弱性进行了分析,提出了 USB HID 脆弱性模型;第 4 部分重点介绍了恶意 USB HID 攻击检测防护平台的设计思想及各模块的具体细节;第 5 部分是本文的实验部分,通过利用 3 种攻击工具/平台产生的攻击数据流对第 4 部分的检测防护平台进行了实验验证,进一步说明平台在功能和性能方面的优势;第 6 部分为结论,对本文取得的进展和未来工作进行总结。

## 2 相关工作

本节对近年来出现的 USB 攻击技术和恶意 USB 攻击检测防护技术的主要思路和研究进展进行简要总结。

### 2.1 USB 攻击技术

自 USB 接口广泛使用以来,针对 USB 接口或 USB 设备的攻击从未停止。相比以恶意软件为主的攻击技术,USB 攻击充分利用了社会工程学和硬件隐患难检测、易忽略的特点,破坏性更强。

文献[9]对典型的 USB 攻击进行了全面的综述,介绍和分析了 29 种 USB 攻击技术。本文结合该分类方法对近年来出现的 USB 攻击技术进行整理如下:

(1) 对 USB 设备内部主控芯片重新编程的 USB 攻击技术:攻击者通过重新改写 USB 设备内部主控芯片中的程序,使其具备恶意功能,然后通过 USB 枚举等方式使恶意 USB 设备具备与其外形不符的功

能或者通过 USB 设备植入目标设备时自动执行某些特定的恶意操作, 典型的攻击技术有 USB Rubber Ducky<sup>[10-11]</sup>、USBdriverby<sup>[12]</sup>等。其中, USB Rubber Ducky 诞生于 2010 年, 是最早的按键注入攻击工具, 后发展成为一个商业化的按键注入攻击平台。其外形类似于 U 盘, 具备代码注入、运行程序和窃取数据等强大功能, 支持通过 Micro SD 进行内存扩展, 并且板载有效载荷重放按钮, 攻击力强, 破坏性大, 如图 2 所示为 USB Rubber Ducky。



图 2 USB Rubber Ducky  
Figure 2 USB Rubber Ducky

(2) 恶意修改 USB 设备固件的 USB 攻击技术: 攻击者对 USB 设备固件进行重新编程, 写入恶意程序, 从而使其执行如下载恶意软件、泄露数据等恶意操作。典型的攻击技术有 Virtual machine break-out<sup>[13]</sup>、Hidden Partition Patch<sup>[14]</sup>等。其中, Hidden Partition Patch 技术是通过使用 Windows 系统中“安全移除硬件”选项对 USB 闪存驱动重新编程, 在其中创建一个无法被格式化的隐藏分区, 实现数据渗漏等恶意操作。

(3) 利用 USB 固有漏洞的 USB 攻击技术: 攻击者利用操作系统与 USB 协议交互时的漏洞对目标计算机发起攻击, 典型的攻击技术有 USB Backdoor into Air-Gapped Hosts<sup>[15]</sup>、AutoRun Exploits<sup>[16]</sup>、USBee<sup>[17]</sup>等。其中, Air-Gapped Hosts 通常搭配 Fanny 恶意软件一起完成攻击操作。其通过 USB 隐藏存储区存储预置命令, 将计算机映射至 Air-Gapped 网络中, 该网络上的信息将会被存储到 U 盘的隐藏存储区中。

(4) USB 电力攻击: 攻击者通过 USB 设备触发电力超载, 从而永久性地破坏目标设备, 典型的攻击技术有 USB Killer<sup>[18]</sup>等。USB Killer 攻击造成的危害是毁灭性的, 该技术以毁坏目标设备为目的, 如图 3 所示为 USB Killer。其插入目标设备后会积蓄电容, 然后快速释放大电流能损伤目标设备主板。该攻击只能从物理层面进行防护。

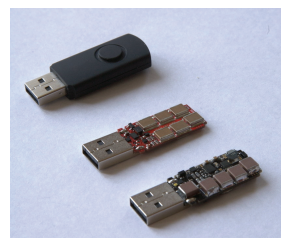


图 3 USB Killer  
Figure 3 USB Killer

此外, 2018 年还出现了一种新型的 BadUSB 攻击——USBHarpoon<sup>[19]</sup>。该技术将恶意芯片植入到 USB 数据线中, 当数据线连入目标计算机后, 被枚举为人体工程学设备(HID)进行按键注入攻击等操作。

这些利用 USB 设备或接口发起的攻击具有极大危害, 其经由 HID 接口完成恶意程序注入或恶意按键操作, 并通过 HID 接口或 USB 大容量存储设备本身完成数据窃取等操作, 形成了将 USB 硬件与恶意软件相结合的新型攻击模式。由于 USB 接口的快速发展以及使用广泛性, 通过 USB 协议防范 USB 攻击已变得不现实, 深入分析 USB 协议漏洞, 掌握 USB HID 攻击特点, 并以此制定完整的防护策略成为研究恶意 USB HID 攻击的主要方向。

## 2.2 恶意 USB 攻击检测防护技术

恶意 USB 攻击检测防护技术主要有三个方面, 一是针对 USB 接口枚举、USB 数据流等进行监控以达到识别恶意操作的目的; 二是通过软件或硬件沙箱对 USB 设备进行验证和数据过滤, 从而保证目标设备来源的可靠性; 三是利用 USB HID 攻击中存在的按键注入间隔短的特点, 利用按键间隔识别是否为恶意自动化操作。

(1) USB 数据监控: 该技术体现在两方面, 一是监控 USB 设备本身, 通过设定一定的安全规则实现设备监管, 如果设备不符合安全规则则被拒绝使用; 二是通过捕获 USB 设备数据, 再将其上传至服务器或后台直接进行分析。如李锦山等人<sup>[20]</sup>提出的基于驱动层的 USB 存储设备安全监控技术, 实现了对 USB 数据包的截获功能; 卢志刚等人<sup>[21]</sup>提出的基于 HID 的 USB 监控技术则是对局域网内的 USB 数据流进行监控并上传至服务器进行分析。以上两种典型技术主要集中在数据包的截获与分析方面, 对数据包的分析力度以及对恶意 USB 攻击技术的检测力度有限, 且难以防范 USB HID 攻击。

(2) 软件或硬件沙箱: 所谓软件沙箱是指通过软件层面实现 USB 设备认证。如美国乔治梅森大学 Wang 等人<sup>[22]</sup>提出的 USBSec 协议增加了主机与外设



间的身份认证机制,只有认证通过才进行设备枚举。当设备插入主机时,双方会完成一次双向认证,当验证通过时才可以正常使用 USB 设备。但该协议修改了通用的 USB 协议,需要定制,推广难度大、局限性大。而硬件沙箱是通过外置硬件设备引入安全审计机制,只有符合该规则的设备才可以通过审计并启用。如美国堪萨斯大学 Kang 等人<sup>[23]</sup>提出的 USBProxy 硬件防火墙以及 Federico 等人<sup>[24]</sup>提出的 USBCheckIn 工具(如图 4 所示)。这两种工具对于外观与功能相符的恶意 USB 设备则无能为力,且其大大降低了 USB 设备的便利性和开放性。综合分析软件和硬件沙箱机制,这两种机制在防护性与易用性方面均未做到良好的均衡。



图 4 USBCheckIn  
Figure 4 USBCheckIn

(3) 按键间隔识别: USB HID 攻击中利用键盘发起按键注入操作,由于按键注入速度快,该方法通过识别相邻按键的间隔区分人机操作。如实验室已有的研究成果中,姜建国等人<sup>[25]</sup>利用 SVM 分类器对按键间隔进行识别,用以区分用户和机器的按键行为。但是该方法对于按键注入间隔与正常用户间隔近似的高级别按键注入攻击不适用,且无法防范 USB HID 攻击中如信息密取等恶意操作。

因此,还缺少一个高效的通用的针对 USB HID 攻击的检测防护方案,本文将在第 4 节重点介绍桌面级的恶意 USB HID 攻击检测防护平台。

### 3 USB HID 脆弱性模型

USB HID 攻击技术是恶意 USB 攻击技术的典型代表,其通过 HID 进行按键注入操作,实现提权,进而完成信息密取、控制传输、指令下达甚至系统攻击等恶意操作。本节对 USB 协议进行了详细分析,总结了 HID 存在的脆弱性,并提出了 USB HID 脆弱性模型。

#### 3.1 USB HID 脆弱性分析

通用串行总线(Universal Serial Bus, USB)是连接

计算机系统与外部设备的一种串口总线标准,也是一种输入输出接口的技术规范,广泛应用于个人计算机和移动设备等信息通讯产品<sup>[26]</sup>。当 USB 设备插入主机时,主机会枚举该 USB 设备,然后主动加载设备所需的驱动程序。目前,多数 USB 设备,尤其是键盘、鼠标等通用 USB 设备仍以 USB 2.0 为主。在 USB 2.0 版本中,共支持高速(Hi-Speed: 480Mbps)、全速(Full Speed: 12Mbps)、低速(Low Speed: 1.5Mbps)三种速率。其中,低速速率主要用于低速率的人机接口设备,如键盘、鼠标、游戏杆等。本文主要研究 USB 2.0 版本下的 USB HID 攻击技术及相应的检测防护技术。

USB 设备插入主机后的初始化过程称为 USB 枚举,如图 5 所示。枚举过程主要有以下四步:

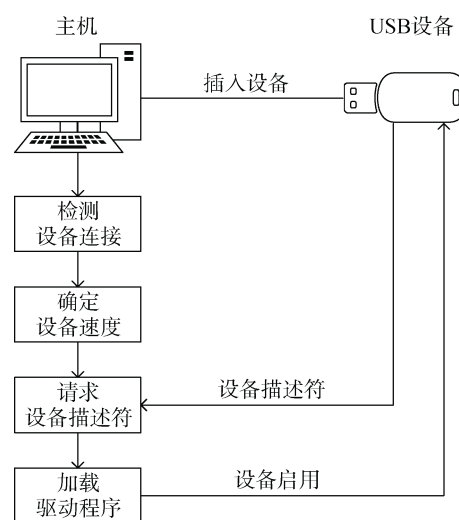


图 5 USB 枚举过程  
Figure 5 USB enumeration process

(1) 主机检测 USB 设备是否连接: 主机通过检测 USB 数据线信号的变化判断 USB 设备是否连接,若检测到有一根数据线是高电平,则认为有 USB 设备插入。

(2) 主机确定 USB 设备速度: 主机通过检测 USB 数据线信号的变化判断 USB 设备所支持的速度模式,主机根据是 D+ 还是 D- 被拉高来判断目标设备是全速还是低速设备。此处仅对枚举步骤作简要论述,不对如何区分全速和高速设备作详细解释,具体请参见 USB 2.0 协议。

(3) 主机请求 USB 设备描述符: 当主机确定 USB 设备已连接以及 USB 设备所支持的速度模式后,主机会向 USB 设备发起设备描述符请求,完成设备识别操作。首先,主机向设备发起请求读取设备的各种描述符,从而获得设备类型、端点等信息。然后,

主机向设备发起设置地址请求操作, 请求设备使用指定地址, 以便主机区分每个不同的 USB 设备。最后, 主机向设备发起设置配置请求操作, 确定相应配置。

(4) 主机加载相应 USB 设备驱动程序: 主机完成设备识别操作后, 需要加载相应的驱动程序以便与 USB 设备进行交互。通常, USB 设备使用 Windows 系统中自带的标准驱动, 如设备为定制化设备或有特殊功能需求时, 主机需要下载相应的驱动以实现对于 USB 设备的控制。

通过对 USB 协议分析, 本文整理了恶意 USB 设备所利用的漏洞(适用于 USB 3.2 及以下版本):

**USB 组合接口漏洞:** 在一个 USB 设备上可以实现多个设备并具有多种功能, 这种设备又称为具有两种及两种以上功能的 USB 设备。其实现方法有两种, 一种是几个具有不同功能的设备通过一个 USB HUB 形成单一设备, 称为 USB 复合设备, 一种是一个配置多个接口实现不同功能的 USB 设备, 称为 USB 组合设备<sup>[27]</sup>。在 USB 组合设备模式下, 每个功能接口共用根 USB 设备的生产厂商 ID(Vendor ID, VID)和产品 ID(Product ID, PID), 因此通过将 USB 设备组合成具备多种功能的设备在一定程度上可以提高恶意设备的隐蔽性。

**USB 设备验证漏洞:** 根据 USB 规范, 所有的 USB 设备都有 VID 和 PID, 主机通过不同的 VID 和 PID 来区别不同的设备, 其中, VID 由供应商向 USB 执行论坛(USB IF)申请, 每个供应商的 VID 是唯一的, PID 由供应商自行决定, 理论上来说, 不同的产品、相同产品的不同型号、相同型号的不同设计的产品最好采用不同的 PID, 以便区别相同厂家的不同设备<sup>[28]</sup>。但是 VID 和 PID 的存在只是为了给设备打标签, 便于迅速定位产品的生产商、型号等信息, 并不作为设备运行的依据, 因此很多山寨厂商会直接使用所采购 USB 芯片本身的 ID 信息或者根据自身情况任意赋值。此外, 即便是生产 USB 设备的大厂, 虽然他们的 VID 信息由 USB IF 分配, 但有时为了自身需要也会向同一批次的设备中写入相同的 PID 信息。VID 和 PID 虽然在理论上可以实现对 USB 设备的唯一标识, 但通过分析以上两种情况可以看出, 实际生产中存在冒用和误用 VID、PID 信息的情况, 这也就导致攻击者在开发恶意 USB 设备时可以采用与正规厂家相同的 VID 和 PID, 从而避免一些安全软件的定向查杀。

**USB 权限许可漏洞:** HID 设备是计算机直接与人类交互的设备, 所有现代主流操作系统都可以识别

标准 USB HID 设备(例如键盘和鼠标), 而无需专门的驱动程序。此外, HID 接口设备, 如键盘、鼠标等具有直接操控计算机的能力, 计算机在识别键盘、鼠标等高权限 HID 设备时, 缺少专门的许可检查机制, 默认此类设备高度可信。基于以上两个特性, 一旦攻击者伪装成该类设备即可完成系统级的操作, 危害性大。

**USB 数据认证漏洞:** HID 设备采用报表(report)结构与主机进行数据交互, 其要求设备固件必须支持 HID 报表的格式, HID 报表格式灵活, 可以处理任何类型的数据(如温度、湿度、地理坐标、键盘键值、鼠标坐标、普通数据……), 而且在 HID 数据交互过程中, 缺乏数据认证机制, 只要符合 HID 报表格式的数据均会被主机接收, 攻击者可以利用这个漏洞伪造符合 HID 报表格式的数据达到欺骗甚至攻击主机的目的。

### 3.2 模型设计思想

在 Windows 环境中, 从 Windows98 操作系统开始, 便提供了 HID 类设备的通用驱动程序。对于 HID 类设备, Windows 系统可以自动识别, 在开发相应通信软件时, 也省去了复杂的驱动程序的编写过程, 具备即插即用等优点。在进行 HID 开发时, 只需要调用自带的 API 即可与 HID 设备进行通信, 降低了开发难度。

在 HID 事务传输中, 不同速率的 USB 设备其传输能力不同, 每笔 HID 事务所支持的字节数也不同。对于 USB 低速设备, 每一笔 HID 事务最大是 8 字节, 但每 10ms 内不会超过一笔事务, 即低速设备最大速度为 800B/s; 全速设备最大为 64 字节, 每 1ms 一笔事务, 即最大速度为 64KB/s; 高速设备最大为 1024 字节, 每 125 $\mu$ s 一笔事务, 即最大速度为 24.576MB/s<sup>[29]</sup>。本文采用 USB 2.0 High Speed 模式, 该模式下通过 HID 进行数据传输可以获得可观的传输速率。因此, 本文充分利用 HID 设备的特点开展研究, 具体设计目标如下:

- (1) 以计算机认可的设备形式存在, 且符合计算机常用设备设计;
- (2) 能够实现多种按键注入攻击, 有可编辑的攻击载荷库;
- (3) 支持 USB 2.0 高速模式, 实现 USB 数据的高速传输;
- (4) 具备无线通信功能, 能够与远程客户端联动, 实现远程控制;
- (5) 设备小型化, 能以键盘、鼠标等多种形态存在。

根据以上功能,本文提出了 USB HID 攻击模型——WHID,结合 3.1 节中所述漏洞做以下设计:

(1) 利用 USB 复合接口漏洞和 USB 权限许可漏洞将 USB 设备枚举为一个组合设备,即“HID 键盘+HID 数据口+MSC 大容量存储设备”的形式,使其具备多种功能。

(2) 利用 USB 设备验证漏洞将 USB 组合设备的 VID 和 PID 设置为市面上已知的合法设备的值,以便躲避某些安全软件对设备 VID 和 PID 的相关检测。

(3) 利用 USB 数据认证漏洞伪造符合 HID 报表格式的合法数据,并设计符合 HID 报表格式的载荷攻击库及数据传输协议。

(4) 引入设备认证机制,即被植入恶意软件的目标主机发送认证指令读取存储在 WHID Flash 中的序列号,然后与已知序列号库进行比对,完成认证,继而才实行后续攻击操作。该机制是为了避免设备被检测(通过模拟利用检测设备异常等方式),这也大大增强了 WHID 的健壮性。

如图 6 所示为 WHID 模型系统结构图。

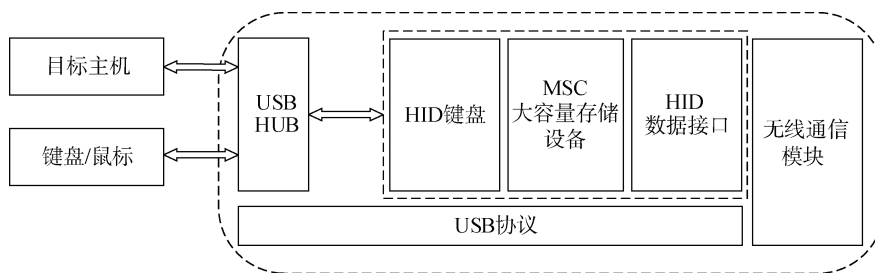


图 6 WHID 模型系统结构图

Figure 6 WHID model system structure diagram

### 3.3 基本架构

USB 设备中,由于 HID 设备具有高用户权限,HID 键盘具备命令等信息输入功能,HID 数据口可用于数据传输, MSC 大容量存储设备可用于数据存储等。因此,针对 WHID 的存在形式,结合 HID 高权限、数据报表格式灵活、免驱等特点,本文将设备枚举为“HID 键盘+HID 数据口+MSC 大容量存储设备”的组合形式,如图 7 所示。

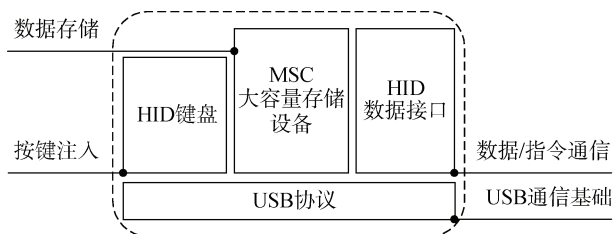


图 7 WHID 模型设备形态

Figure 7 The device configuration of WHID model

**HID 键盘:** HID 键盘是计算机高度可信的设备,通过键盘可以操作设备运行的指令,也可以进行数据输入等操作。键盘是最常用也是最主要的输入设备,通过键盘可以将英文字母、数字、标点符号等输入到计算机中,从而向计算机发出命令、输入数据等<sup>[30]</sup>。利用键盘的这一特点,本文通过 USB 枚举使得 WHID 具备 HID 键盘的功能和特征,从而实现将由

英文字母、数字、标点符号等组成的攻击载荷注入到目标计算机中,控制目标计算机,实现攻击。

**HID 数据口:** 本文所提及的 WHID 模型设计了 HID 数据接口。由于 HID 设备在主流操作系统中具有免驱等特点,因此通过 HID 数据接口进行数据传输更加便捷,同时,免驱也可以使 WHID 在进行相关指令或数据操作时更加便捷,不易被目标用户发现。本模型利用 USB 2.0 Hi-Speed 协议的 HID 数据口功能实现 WHID 与主机之间的高速率数据交互等功能。

**MSC 大容量存储设备:** USB 大容量存储设备类(The USB mass storage device class)是一种计算机和移动设备之间的传输协议,它允许一个通用串行总线(USB)设备来访问主机的计算设备,使两者之间进行文件传输<sup>[31]</sup>。WHID 模型通过将设备枚举为 MSC 大容量存储设备实现数据存储等功能。

在 Bushound 数据监控软件中,可以查看计算机中 USB 设备的相关信息,包括单一 USB 设备和组合 USB 设备。如图 8 所示为单一 USB 设备,图 9 所示为“HID 键盘+HID 数据口+MSC 大容量存储设备”组合设备。



图 8 单一 USB 设备

Figure 8 A single USB device



图9 USB组合设备

Figure 9 A USB composite device

## 4 恶意 USB HID 攻击检测防护平台

基于 USB HID 脆弱性模型所总结的主流 USB HID 攻击技术利用的漏洞和攻击特点, 本文提出了一种新型的检测防护思想, 并设计了一个恶意 USB HID 攻击检测防护平台——WHID Defense。本节将从设计思想、按键注入特征分析及防御、数据捕获与反向干扰、用户身份管理与访问控制、风险事件分类与统计、功能分析等六个方面进行详细阐述。

### 4.1 平台设计思想

以往关于检测防护技术的研究一般以检测与查杀为主, 本文根据 USB HID 攻击的特点, 在检测与查杀的基础上引入了反向干扰的思想, 形成了新型的检测防护思想: “监+查+反+审”。

(1) 监: 能够实时监测恶意工具行为、数据流等信息, 确保恶意工具的操作均在监测范围内。

(2) 查: 能够对恶意设备的恶意数据流进行鉴别、查杀。

(3) 反: 能够反向干扰或反向攻击恶意设备, 干扰其正常通信。

(4) 审: 设备的行为、数据要可审计。

“监+查+反+审”思想可以形成一个多层级的检测防护体系, 平台可以对目标设备实时监测, 一旦有异常发生即可发出报警, 同时对于恶意数据流可以进行查杀, 该思想中的“审”要求平台对目标设备所有数据和行为进行记录, 为后续审计人员进行审计提供了便利。此外, 该思想中创新性地引入了反向干扰思想, 对恶意设备实施反向干扰, 扰乱其正常通信。

由于 USB HID 攻击一般以硬件的形式存在, 如果仅仅对可疑设备进行监测可能会存在误报等情况, 本文所提出的“监+查+反+审”思想更加全面地实现对 USB HID 攻击的检测与防护, 保证个人计算机安全。

### 4.2 基本架构

基于“监+查+反+审”思想, 并结合 USB HID 脆弱性模型的特点, 恶意 USB HID 攻击检测防护平台

具体设计目标如下:

(1) 基于 WHID 模拟键盘进行按键注入攻击的特征, 通过对键盘数据信息的监控, 实现对按键注入攻击的预警;

(2) 基于 WHID 利用 HID 数据口进行数据通信的特征, 通过对 HID 设备进行数据信息的监控, 实现对 WHID 设备数据的捕获, 并统计、分析数据流量大小实现可疑信息初步预警; 此外, 通过分析捕获数据包的构成特点, 模拟构建数据包并发送给 WHID, 实现对 WHID 通信的干扰;

(3) 基于恶意 USB HID 攻击工具的特点, 对 USB HID 设备进行分类, 划定设备风险等级, 实现风险信息实时显示; 同时, 根据平台监控结果, 实时动态调整目标设备分类, 使设备风险等级显示更科学;

(4) 根据 WHID Defense 可能使用的场景和对象, 构建不同的角色访问机制, 并制定不同级别的安全风险预警系统;

(5) 为了便于后续对设备通信数据的审计, 构建通信数据库, 将 HID 设备的通信数据包以及 HID 键盘的按键数据保存在数据库中。

如图 10 所示为 WHID Defense 系统结构图。

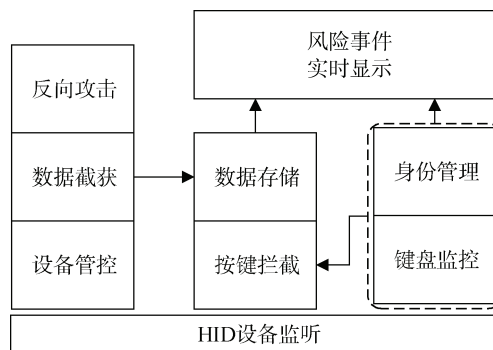


图10 WHID Defense 系统结构

Figure 10 The system structure of WHID Defense

通过监测 USB HID 设备可以掌握 USB HID 设备的行为, 如插入、拔出、发送数据、接收数据等, 通过可视化界面可以将此类行为一一列出, 便于观察, 必要时可对可疑行为进行预警。为防止按键注入攻击, WHID Defense 平台引入了按键注入攻击预警机制, 可以记录所有按键事件并对可疑按键流进行弹窗提醒。而对 USB HID 数据流的捕获一来可以监控数据流量和速度, 通过统计发现异常; 二来可以用于后续数据包分析及审计工作。反向干扰则是本文检测防护思想的亮点之一, 可以实现对恶意设备的通信干扰。



4.2.1 按键注入特征与分析

恶意 USB HID 攻击工具是恶意软件与恶意硬件相结合的攻击技术的典型代表, 具有极强的隐蔽性和破坏性。对于一款恶意软硬件相结合的攻击工具, 恶意硬件的植入是攻击实施的前提, 而恶意软件的感染则是攻击实施的必要路径。此类攻击工具利用 USB HID 协议脆弱性, 将恶意 USB HID 攻击工具枚举为计算机高度可信的 HID 键盘设备, 通过键盘路

径可以实现对目标计算机“命令提示符”的开启, 以便于将木马程序植入到目标计算机或者实施更高级别的有针对性的攻击, 如文件查找、关闭计算机等。

利用键盘高权限、操作设备运行指令、数据输入等特点, 结合主流 USB HID 攻击工具功能, 本文对标准 HID 键盘的 HID 报表格式进行分析, 掌握攻击载荷的特点, 从而实现对按键注入攻击精准化识别。

HID 键盘输入报表的数据格式如图 11 所示。

BYTE	7	6	5	4	3	2	1	0
值	键值6	键值5	键值4	键值3	键值2	键值1	保留	修饰键

图 11 HID 输入报表数据格式

Figure 11 HID input report data format

由图可知, 输入报表共 8 个字节, 各字节具体信息如下:

BYTE0: 特殊按键, 其中:

(1) bit0 表示 Left Control 是否按下, 按下为 1, 抬起为 0;

(2) bit1 表示 Left Shift 是否按下, 按下为 1, 抬起为 0;

(3) bit2 表示 Left Alt 是否按下, 按下为 1, 抬起为 0;

(4) bit3 表示 Left GUI(Windows 键)是否按下, 按下为 1, 抬起为 0;

(5) bit4 表示 Right Control 是否按下, 按下为 1, 抬起为 0;

(6) bit5 表示 Right Shift 是否按下, 按下为 1, 抬起为 0;

(7) bit6 表示 Right Alt 是否按下, 按下为 1, 抬起为 0;

(8) bit7 表示 Right GUI(Windows 键)是否按下, 按下为 1, 抬起为 0。

BYTE1: 保留位。

BYTE2——BYTE7: 普通按键。

由于攻击载荷由按键构成, 因此载荷特征体现在按键特征上。通过 HID 键盘报表格式可知, 每一个字节规定了按键类型, 常用的按键组合一般体现在 BYTE0 和 BYTE2 中, 二者赋以特定的值即可完成一次按键操作。为了达到按键注入攻击“隐蔽性”的目的, 实施快速的按键注入操作成为此类攻击的最大特点, 这种特点表现为相邻按键之间的间隔很短(具体间隔可根据需要自定义)。在设计攻击载荷时, 可以将要实现的恶意操作转换为一条条按键输入指令, 然后对每一个按键指令进行 HID 报表的还原。

基于以上标准 HID 键盘报表格式, 并根据实际攻击场景, 本文列出了两个攻击载荷, 如表 1 所示。

表 1 攻击载荷  
Table 1 Attack payload

序号	功能	键值	攻击载荷
1	打开“命令提示符”	WIN+R	08 00 15 00 00 00 00 00
		C	00 00 06 00 00 00 00 00
		M	00 00 10 00 00 00 00 00
		D	00 00 07 00 00 00 00 00
		ENTER	00 00 28 00 00 00 00 00
		F	00 00 09 00 00 00 00 00
		O	00 00 12 00 00 00 00 00
		R	00 00 15 00 00 00 00 00
		M	00 00 10 00 00 00 00 00
		A	00 00 04 00 00 00 00 00
2	格式化 D 盘	T	00 00 17 00 00 00 00 00
		SPACE	00 00 2C 00 00 00 00 00
		D	00 00 07 00 00 00 00 00
		:	02 00 33 00 00 00 00 00
		/	00 00 38 00 00 00 00 00
		Q	00 00 14 00 00 00 00 00
		ENTER	00 00 28 00 00 00 00 00

综合分析此类攻击工具的按键注入攻击特点发现其均是依托于 HID 键盘模拟用户进行命令注入。因此, 调用“命令提示符”成为此类攻击的一个必然选择, 在 Windows 操作系统中, 通过按键形式打开“命令提示符”有以下三种方法:

(1) 通过搜索框直接打开“命令提示符”:

- ① 按下“Windows”键;
- ② 输入“cmd”打开“命令提示符”。

(2) 通过搜索框打开“运行”窗口, 进而打开“命令提示符”:

- ① 按下“Windows”键;
- ② 输入“运行”或“yunxing”, 打开“运行”窗口;



③ 输入“cmd”打开“命令提示符”。

(3) 通过“Windows+R”组合键打开“运行”窗口, 进而打开“命令提示符”:

① 按下“Windows+R”组合按键, 打开“运行”窗口;

② 输入“cmd”打开“命令提示符”窗口。

通过以上三种方法可以看出, 进行按键注入攻击时均有按下“Windows”键的过程, 为了使拦截准确, 本文对以下三种操作进行按键注入标记, 如表 2 所示。

表 2 按键注入标记

Table 2 Key-press injection mark

序号	按键识别	功能
1	“Windows”+“c”	打开“命令提示符”窗口
2	“Windows”+“y”	打开“运行”窗口
3	“Windows+R”组合键	打开“运行”窗口

当键盘数据监听模块监听到以上按键组合时, 则发出警告, 提醒用户当前设备可能存在风险。整个过程算法实现如表 3 所示。

表 3 按键注入标记特征算法

Table 3 Key-press injection marking feature algorithm

算法 1 按键注入特征标记

输入: flag: “Windows” flag; Keyboard_Monitor(): key value. 输出: alert_flag: Warning flag.	
1.	function Key_Flag()
2.	key ← Keyboard_Monitor();
3.	if key == “Windows” then
4.	flag ← 1;
5.	end if
6.	if flag == 1 then
7.	if key == ‘c’ then
8.	alert_flag ← 1;
9.	else if key == ‘y’ then
10.	alert_flag ← 2;
11.	else if key == ‘y’ then
12.	alert_flag ← 3;
13.	else
14.	flag ← 0;
15.	alert_flag ← 0;
16.	end if
17.	end if
18.	end function

4.2.2 数据捕获与反向干扰

恶意 USB HID 攻击工具利用 HID 数据口完成与

目标计算机的指令传递与数据交互操作。WHID 依托 HID 数据接口可实现数据密取功能。开发者可以自定义 HID 接口, 该接口除了用于实现键盘、鼠标等功能外, 其接口数据可以是温度、湿度、控制指令, 甚至是数据格式符合 HID 报表格式的任意数据。实现 HID 接口数据传输需要对 HID 接口描述符进行自定义, HID 标准接口描述符结构如表 4 所示。

表 4 HID 标准接口描述符

Table 4 HID standard interface descriptor

字节	域	字节数	说明
0	bLength	1	接口描述的长度
1	bDescriptorType	1	接口描述符的类型
2	bInterfaceNumber	1	接口编号
3	bAlternateSetting	1	接口备用编号
4	bNumEndpoints	1	接口所使用的端点数
5	bInterfaceClass	1	接口所使用的类
6	bInterfaceSubClass	1	接口所使用的子类
7	bInterfaceProtocol	1	接口所使用的协议
8	iInterface	1	描述该接口的字符串的索引值

WHID 模型通过数据密取单元处理远程通信单元所接收的控制指令和有效数据, 同时, 也接收目标机所发送的敏感数据以及指令反馈等。

此外, WHID 模型远程通信单元, 为 WHID 系统提供了远程指令控制与数据透传功能。远程通信单元可以是 WIFI 模块、4G/5G 移动通信模块、无线射频模块等形式, 此类模块使 WHID 系统与远程控制端实现互联。远程控制端可以通过远程通信单元将控制指令、校验数据等信息下发至 WHID 系统, 同时, WHID 系统也可以将收集到的目标系统中的敏感数据回传至远程控制端, 实现目标敏感数据远程密取功能。但整个过程均需依托 HID 数据口实现目标机数据获取后才可进行无线透传。

具备 HID 数据口的恶意 USB HID 攻击工具可以通过 HID 报表完成上述操作, 通过监听 USB HID 设备, 可以获取通过该设备的数据流, 将其数据流捕获并保存到数据库中, 便于后续对设备数据流的分析与还原。此外, 标准 HID 键盘的 HID 报表为 8 字节/包, 标准鼠标的 HID 报表为 4 字节/包, 而对于全速 USB 设备, 其 HID 报表为 64 字节/包, 对于高速 USB 设备, 其 HID 报表为 1024 字节/包。由此可以看出, HID 数据接口的流量远大于标准 HID 键盘和鼠标, 通过监控 HID 数据接口的流量并分析, 可以对可疑数据交互操作进行预警, 形成 WHID Defense 第二层防护屏障。本文在 WHID Defense “数据捕获”

功能中加入了实时显示设计, 可以将捕获的 HID 数据包实时滚动显示在主界面上, 便于用户查看。

如表 5 所示为 WHID Defense 数据捕获算法。

表 5 数据捕获算法  
Table 5 Data capture algorithm

算法 2 数据捕获算法	
输入: <i>open_flag</i> : open device or no; <i>milliseconds</i> : timeout; <i>WaitForSingleObject(milliseconds)</i> : waiting event trigger; <i>res</i> : the number of bytes; <i>GetOverlappedResult()</i> : get the number of bytes; <i>memcpy()</i> : data copy. 输出: <i>data</i> : HID data; <i>read_buf</i> : USB data; <i>copy_len</i> : data length.	
1.	<b>function</b> <i>Intercept_Data()</i>
2.	<b>if</b> <i>open_flag</i> <b>then</b>
3.	<b>if</b> <i>milliseconds</i> $\geq 0$ <b>then</b>
4.	<i>WaitForSingleObject(milliseconds)</i> ;
5.	<b>end if</b>
6.	<i>res</i> $\leftarrow$ <i>GetOverlappedResult()</i> ;
7.	<b>if</b> <i>res</i> && <i>read_bytes</i> $> 0$ <b>then</b>
8.	<i>memcpy(data, read_buf, copy_len)</i> ;
9.	<b>end if</b>
10.	<b>end if</b>
11.	<b>end function</b>

在反向干扰设计方面, 本文结合了重放攻击和 DoS 攻击的思想。

(1) 重放攻击: 又称重播攻击、回放攻击, 是指攻击者发送一个目的主机已接收过的包, 来达到欺骗系统的目的, 主要用于身份认证过程, 破坏认证的正确性<sup>[32]</sup>。很多时候, 设备之间在进行双向通信时都有一套内部的通信协议或者传输经过加密的数据, 而攻击者对拦截数据进行解析需要耗费大量精力, 通过重放攻击, 攻击者只需要了解拦截数据的作用即可在一定程度上干扰目标设备正

常通信。具体到本文的研究中, 由于可疑设备可能存在通信协议复杂、破解难度大的问题, 因此, WHID Defense 平台在对可疑设备进行反向干扰时, 结合数据捕获的结果将捕获的数据包直接打包下发至可疑设备, 达到欺骗可疑设备并干扰其正常通信的目的。

该设计的作用如下:

- ① 无需了解、分析可疑 USB 设备的通信协议即可对可疑设备进行信息注入操作;
- ② 通过增加额外的数据流干扰可疑 USB 设备正常通信, 在一定程度上增加了其正常传输的恶意数据流的时延, 耗用通信链路的带宽;
- ③ 可能引起恶意程序进行数据重传等操作, 从而干扰正常通信。

(2) DoS 攻击: DoS 攻击, 又称拒绝服务攻击, 通过利用网络协议中存在的脆弱性或系统漏洞使目标设备无法提供正常服务<sup>[33]</sup>。USB HID 低速设备的最高数据包轮询时间为 10ms, 全速设备的最高数据包轮询时间为 1ms, 而高速设备的最高数据包轮询时间为 125 $\mu$ s<sup>[28]</sup>。因此, 结合 USB HID 设备的轮询时间, 设置三档反向注入模式, 即低速模式: 以 1 包数据/10ms 的速率将捕获的数据包下发至目标设备; 全速模式: 以 1 包数据/1ms 的速率将捕获的数据包下发至目标设备; 高速模式: 以 1 包数据/125 $\mu$ s 的速率将捕获的数据包下发至目标设备。通过长达半小时的不间断信息注入, 扰乱目标设备的正常通信, 当然, 也可以自定义注入时间。

该设计的作用如下:

- ① 利用 USB HID 设备的最高数据包轮询时间, 循环不间断注入干扰信息, 可以干扰可疑设备正常通信, 使其无法正常接收数据;
- ② 可能引起可疑 USB 设备宕机等操作, 从而干扰其正常通信。

反向干扰流程如图 12 所示。

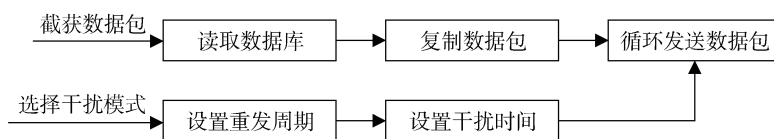


图 12 反向干扰流程

Figure 12 Reverse interference process

#### 4.2.3 用户身份管理与访问控制

WHID Defense 平台具备用户身份管理与访问控制功能, 用户可以根据实际需要选择对应的角色, 从而确定相应的防护策略, 这种思想增强了 WHID

Defense 平台的多场景适应性。

访问控制(Access Control)指系统对用户身份及其所属的预先定义的策略组限制其使用数据资源能力的手段, 是系统保密性、完整性、可用性和合法使

用性的重要基础,也是主体依据某些控制策略或权限对客体本身或其资源进行的不同授权访问<sup>[34]</sup>。为了使 WHID Defense 平台更具有普遍适用性,本文结合实际使用人员和场景对平台防护性能进行了划分。

本课题共设计三种用户角色,分别为开发者、管理员和普通用户,其中,开发者对应开发模式,管理员对应增强模式,普通用户对应办公模式。具体设计如下:

开发模式:开发模式主要针对开发人员。由于开发者在进行软硬件开发时,经常会用到键盘的许多快捷按键或功能,而且为了便于调试,也会启用计算机中的很多功能和接口,并设置为较高权限。基于这一特点,平台在设计时对 HID 键盘接口只进行监控和记录,将其产生的数据保存到数据库中,便于后续审计时使用。同时,为了在一定程度上保护计算机免受恶意 USB HID 攻击工具攻击,保留了对 USB HID 设备的数据捕获与存储功能,开发人员也可以根据实际需要自行设定干扰周期和时长对可疑设备进行通信干扰。此外,防护平台也会针对设备信息为用户提供可行性建议,如提示开发人员查看当前计算机设备信息等。

增强模式:增强模式主要针对管理员。实际环境中,一些对防护级别要求较高的计算机需要通过专网甚至是物理隔离等手段使计算机处于一个相对安全的状态,但是面对像恶意 USB HID 攻击工具这种类型的恶意软硬件相结合的攻击则有些力不从心。为了保证键盘的基本功能、确保计算机的正常使用场景,同时,过滤和监控可疑按键操作,在该模式下,平台对 HID 键盘接口进行了监视和记录,并将其产生的数据保存到数据库中,便于后续审计时使用。同时,对 4.2.1 节中提到的可疑按键操作均进行了直接过滤,牺牲了一些快捷按键操作,在一定程度上减小计算机受到按键注入攻击的风险。此外,保留了对 USB HID 设备的数据捕获与存储功能,用户也可以根据实际需要自行设定干扰周期和时长对可疑设备进行通信干扰。

办公模式:办公模式主要针对普通用户。在实际办公环境中,用户对系统快捷按键等有一定需求,如果完全禁用会大大降低用户体验,降低工作效率。因此,在该模式设计中,充分结合实际办公场景,当监控到可疑指令时,WHID Defense 平台会向用户发出警告,并询问用户是否是可信行为,若是,则放行该指令,否则,过滤该指令并禁用当前计算机所有键盘设备,同时,向用户发出预警。若用户更换目标

设备为可信设备或经排除风险认为目标设备可信,则可通过键盘恢复功能使平台自动进入办公模式并开启按键监控。整个过程依然保留了对 HID 键盘接口的监视和记录功能,并将其产生的数据保存到数据库中,便于后续审计时使用。此外,还保留了对 USB HID 设备的数据捕获与存储功能,用户也可以根据实际需要自行设定干扰周期和时长对可疑设备进行通信干扰。

4.2.4 风险事件分类与统计

WHID Defense 平台具备对恶意 USB HID 攻击工具的风险事件分类与统计功能,引入了风险定级思想,能够根据事件类型和可疑操作对设备进行动态定级,使评判更科学、直观。

风险事件分类与统计的设计思想基于外围设备持续不可信原则。首先,依据设备类型及特点设定初始化风险事件等级分类;在平台监测过程中,风险等级会随设备状态、事件等信息重新设置,实时动态变化。这样设计更有利于动态识别本地计算机 USB HID 设备可能存在的风险,实现设备从插入、使用到拔出这一全生命周期的预警。

HID 类设备中,HID 键盘或鼠标等设备为系统独占设备,是现今用户正常使用计算机所必备的工具之一,因此,将其定义为最低风险等级——四级;而常规的有标识的 HID 设备(如游戏杆等能识别出的有具体厂商号的 HID 设备或者具有双向数据传输功能的 HID 设备),将其风险等级定义为三级;其他未知的没有标识的 HID 设备,由于不确定具体来源,将其风险等级定义为二级;如果在监测过程中被系统判定为可疑设备,将其风险等级定义为一。具体设备风险分类如表 6 所示。

表 6 设备风险等级分类  
Table 6 Device risk classification

风险等级	所属设备	说明
四级	HID 键盘、HID 鼠标	系统独占设备
三级	有标识的 HID 设备	来源可靠但有数据通信功能的设备
二级	未标识的 HID 设备	来源未知或有数据通信功能的设备
一级	经平台识别后判定为可疑类型的 HID 设备	有可疑操作的设备

4.2.5 功能分析

恶意 USB HID 攻击检测防护平台——WHID Defense 充分利用了 USB HID 协议的脆弱点及主流 USB HID 攻击技术的攻击特点,实现了对恶意 USB HID 攻击工具的监控与预警,具备兼容性高、智能化

高、交互性强、功能完善等特点, 具体功能指标如下:

- (1) 可以获取本地计算机中的所有 USB HID 设备, 并显示各设备 VID、PID 等详细信息;
- (2) 实时监测 USB HID 设备流量, 获取 HID 设备数据报表, 捕获数据包并存入数据库中;
- (3) 针对可疑恶意 USB HID 设备, 结合重放攻击和 DoS 攻击开启反向干扰模式, 干扰设备正常通信;
- (4) 实时监控本机计算机所有 HID 键盘, 对所有

产生的按键信息进行监控并存入数据库中;

- (5) 平台具备三种使用场景, 每种场景所提供的防护等级不同, 用户可根据实际需要进行选择;
- (6) 划定了设备风险等级, 实现风险信息的实时显示。

如图 13 所示为 WHID Defense 平台运行图。如表 7 所示为 WHID Defense 平台与 Curtain<sup>[35]</sup>及 USB HID 攻击检测算法<sup>[25]</sup>的功能指标对比。

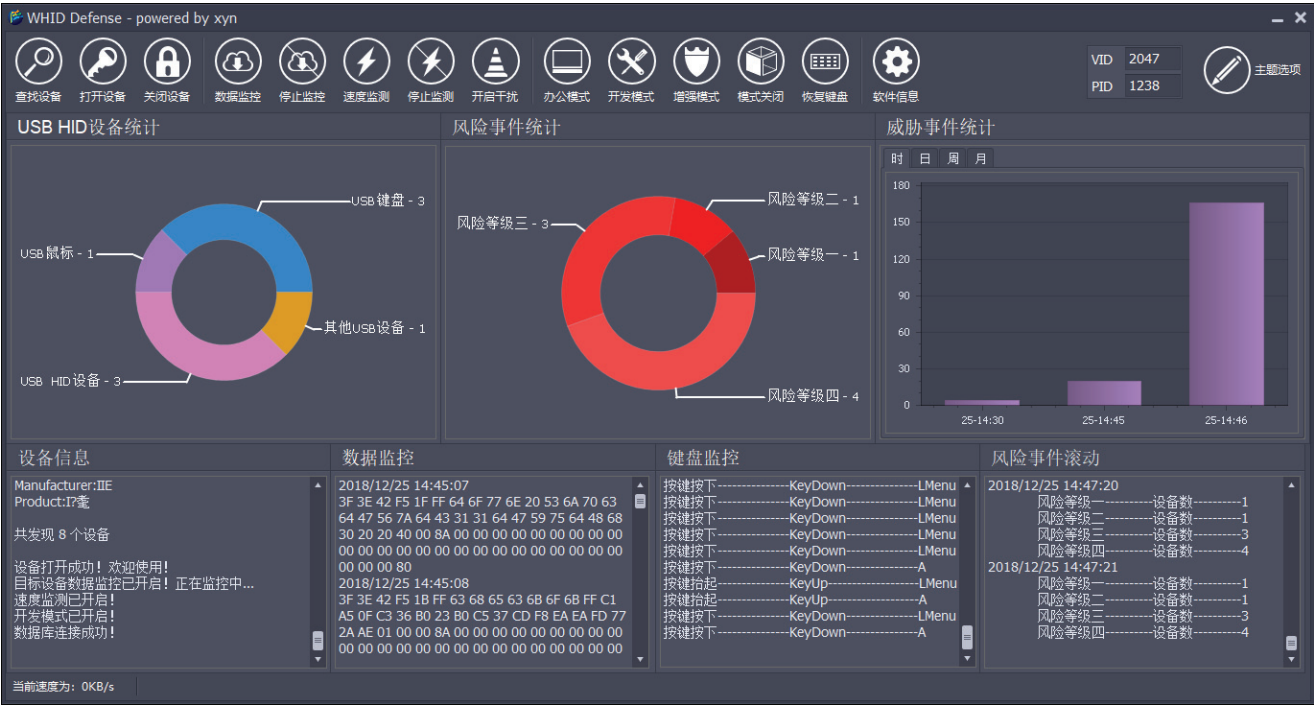


图 13 WHID Defense  
Figure 13 WHID Defense

表 7 WHID Defense、Curtain、USB HID 攻击检测算法功能指标对比

Table 7 Comparison of functional indicators of WHID Defense, Curtain, and USB HID attack detection algorithms			
风险等级	WHID Defense	Curtain	USB HID 攻击检测算法
按键注入报警	√	×	√
按键监控与审计	√	×	×
USB HID 设备监听	√	√	×
HID 数据捕获与审计	√	√	×
反向干扰通信	√	×	×
用户身份管理	√	×	×
风险事件分类与统计	√	×	×
可视化操作界面	√	√	×

## 5 实验分析

为了验证 WHID Defense 检测防护平台的功能及性能, 本文开展了实验验证工作。本文基于 BadUSB、HID 漏洞测试平台及 WHID 平台共三种攻击工具完成 WHID Defense 检测防护测试, 着重测试了平台按键注入识别、数据捕获与干扰通信三个方面(由于三种身份模式下按键注入识别实现原理类似, 本节仅测试办公模式下的按键注入识别用于功能验证)。

结合第 2 部分相关工作所述恶意 USB 检测技术国内外研究现状, 尚未有研究人员将恶意 USB HID 攻击过程中产生的恶意操作进行完整识别, 目前, 大多数检测方案处于研究阶段且多为硬件沙箱模式, 无市售产品用于对比。为了使测试结果更科学,



具有对比性, 本节通过在 PC-0、PC-1 和 PC-2 中分别安装 USB HID 攻击检测算法软件、360 安全套件和 WHID Defense 对识别恶意按键注入攻击、捕获目标设备数据流、干扰目标设备正常通信三方面进行了实验验证对比和结果分析。(注: PC-0、PC-1、PC-2 均只安装需要测试的软件, 未安装其他安全软件)。

### 5.1 评价指标

WHID Defense 平台评价指标主要包括识别恶意按键注入攻击、捕获目标设备数据流、干扰目标设备正常通信三个方面。

#### (1) 识别恶意按键注入攻击

若检测防护工具可以嗅探恶意按键注入操作或及时提醒用户, 则认为该工具具备识别恶意按键注入攻击的能力。对于 WHID Defense 平台, 在办公模式下, 若发生按键注入攻击, WHID Defense 平台会弹窗提醒并询问用户是否为用户行为, 如图 14 所示。基于该特点, 在评价 WHID Defense 平台按键注入识别时可以通过记录按键注入攻击数以及按键注入提醒数作为识别结果的衡量依据。

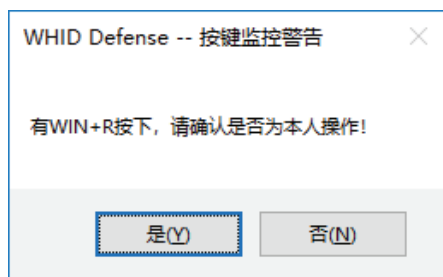


图 14 办公模式按键注入攻击预警

Figure 14 Office mode key-press injection attack warning

假设攻击平台共发起  $N$  次攻击, 检测防护工具成功拦截并实现预警  $M$  次攻击, 拦截率为, 漏报率为, 则:

$$\eta = \frac{M}{N} \times 100\% \quad (1)$$

$$\theta = \frac{N-M}{N} \times 100\% \quad (2)$$

#### (2) 捕获目标设备数据流

目标设备通过 HID 数据接口进行指令下达或数据交互操作, 若检测防护工具可以将流经目标设备的数据流进行本地存储或云端存储, 则认为该工具具备捕获目标设备数据流的能力。对于 WHID Defense 平台, 可以通过查看 WHID Defense 平台数据监控接口以及数据库数据可以作为平台是否成功捕获目标设备数据流的衡量依据, 如图 15 所示为 WHID Defense 捕获的数据。

假设攻击平台共产生  $P$  条通信数据, 数据库(或本地存储/云端存储)中存储  $Q$  条通信数据, 捕获率为, 丢失率为, 则:

$$\alpha = \frac{Q}{P} \times 100\% \quad (3)$$

$$\beta = \frac{P-Q}{P} \times 100\% \quad (4)$$

#### (3) 干扰目标设备正常通信

通过 BUSHOUND 数据监控软件可以观察流经设备的数据包, 若开启通信干扰功能后, 目标设备开始不断地流入数据而没有发生新数据发送或新数据接收操作, 则认为平台通信干扰功能正常。如图 16 所示为 BUSHOUND 监控的设备数据流, 图中可以看出设备在 Cmd.Phase 为 1.1 处发送一包数据后, 在 2.1 处接收一包数据, 然后于 3.1 处发送一包数据, 此后, 平台干扰开启, 设备在 4.1 处接收 223 包干扰数据且无任何其他新数据发送或接收操作。本实验规定, 平台只需完成 100 包重复数据发送即认为成功完成一次通信干扰操作。对于 WHID Defense 平台, 其通过重放捕获数据包进行 DoS 攻击实现干扰目标设备正常通信的功能。

对象		threatdata @test (test) - 表	
开始事务	十六进制	筛选	排序 导入 导出
ID	Date	ThreatData	
21	2018-12-25 14:45:45	(BLOB) 64 bytes	
22	2018-12-25 14:45:45	(BLOB) 64 bytes	
23	2018-12-25 14:45:45	(BLOB) 64 bytes	
24	2018-12-25 14:45:48	(BLOB) 64 bytes	
0x00		BF3E 42F5 28FF 6368 6563 6B6F 68FF F8CD ?>B?( checkkok ??	
0x10		39AC C3D6 353A 971C 7598 BA80 4AF9 3CB1 9???5:?.u??€J?<?	
0x20		CA1C 29C5 EC33 7884 694F 7367 7913 0000 ?.)??3x?i Os gy...	
0x30		0000 0000 0000 0000 0000 0000 0000 0093 .....	

图 15 WHID Defense 捕获数据(MySQL 数据库)

Figure 15 WHID Defense capture data (MySQL database)

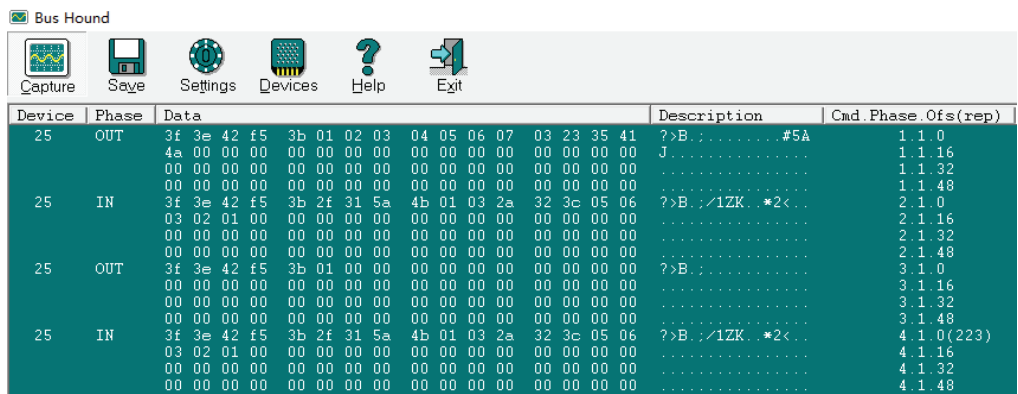


图 16 BUSHOUND 监控干扰数据  
Figure 16 BUSHOUND monitors interference data

5.2 实验数据

本文通过 BadUSB、HID 漏洞测试平台及 WHID 平台共生成 27000 条数据验证了 USB HID 攻击检测算法、360 安全套件和 WHID Defense 的防护效果, 其中, 按键注入攻击数据 9000 条, 通信数据 18000 条, 具体分布如图 17 所示。

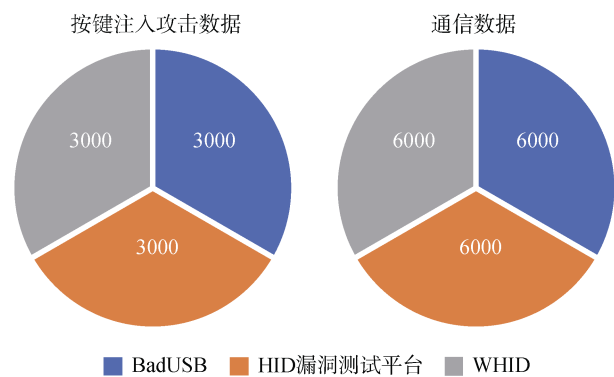


图 17 攻击数据分布  
Figure 17 Attack data distribution

按键注入攻击数据依据按键注入特征进行构建, 分别通过 BadUSB、HID 漏洞测试平台及 WHID 平台发起 25 种各 120 次、120 次、120 次按键注入攻击, 以此作为平台按键注入识别功能的检测数据。

通信数据由算法 3(如表 8 所示)生成 6000 个不同的数据包, 然后将各数据包下发至目标设备, 并将设备设置为数据回传机制模拟双向通信, 即设备收到某一数据包后会将数据包最后一个字节加 1, 然后进行回传, 将以上数据作为平台捕获数据功能的检测数据。

5.3 实验验证及结果分析

实验验证环节中所有计算机(PC-0、PC-1、PC-2) 都符合以下环境:

表 8 通信数据生成算法

Table 8 Communication data generation algorithm

算法 3 通信数据生成算法

输入:  $data\_len$ : data length.

输出:  $data$ : generated communication data.

```
1.      function Generate_Data()
2.      for  $i \leftarrow 0$  to  $data\_len$  do
3.           $data[i] \leftarrow i$ ;
4.      end for
5.      end function
```

(1) 计算机型号: DELL OptiPlex 7050

(2) 操作系统版本: Windows 10 企业版(版本号 1803)

(3) 系统类型: 64 位操作系统, 基于 x64 处理器

(4) 处理器: Intel Core i7-6700 CPU 3.40GHz

(5) 运行内存: 16.0 GB

实验验证操作步骤如下:

(1) 分别在 PC-0、PC-1、PC-2 运行 USB HID 攻击检测算法软件、360 安全套件和 WHID Defense;

(2) 通过 BadUSB、HID 漏洞测试平台及 WHID 平台分别向 PC-0、PC-1、PC-2 发起 25 种各 120 次、120 次、120 次按键注入攻击, 并记录各检测防护软件预警情况;

(3) 通过 BadUSB、HID 漏洞测试平台及 WHID 平台分别向 PC-0、PC-1、PC-2 各产生 6000 次数据通信(基于表 4.8 算法 3), 并记录各检测防护软件捕获数据情况;

(4) 通过 BadUSB、HID 漏洞测试平台及 WHID 平台分别向 PC-0、PC-1、PC-2 各产生 100 次数据通信, 查看并记录 BUSHOUND 数据监控软件中各设备的数据接收情况。

### (5) 实验数据整理与结果分析。

具体实验过程及结果如下所示:

#### (1) 识别按键注入攻击实验过程及结果分析

##### ① USB HID 攻击检测算法验证(基于 PC-0)

首先, 开启 USB HID 攻击检测算法, 进入按键监控状态, 然后通过 BadUSB、HID 漏洞测试平台及 WHID 平台发起 25 种各 120 次、120 次、120 次按键注入攻击。统计各个工具发起攻击时 USB HID 攻击检测算法的预警次数。

实验过程中, BadUSB 发起 3000 次按键注入攻击, 该检测算法实现预警 1997 次, 漏报 1003 次, 即 USB HID 攻击检测算法对 BadUSB 发起的按键注入攻击拦截率约为 66.57%, 漏报率约为 33.43%。HID 漏洞测试平台发起 3000 次按键注入攻击, 该检测算法实现预警 2798 次, 漏报 202 次, 即 USB HID 攻击检测算法对 HID 漏洞测试平台发起的按键注入攻击拦截率约为 93.27%, 漏报率约为 6.73%。WHID 平台发起 3000 次按键注入攻击, 该检测算法实现预警 1883 次, 漏报 1117 次, 即 USB HID 攻击检测算法对 WHID 平台发起的按键注入攻击拦截率约为 62.77%, 漏报率约为 37.23%。如图 18 所示为 USB HID 攻击检测算法按键注入拦截结果。

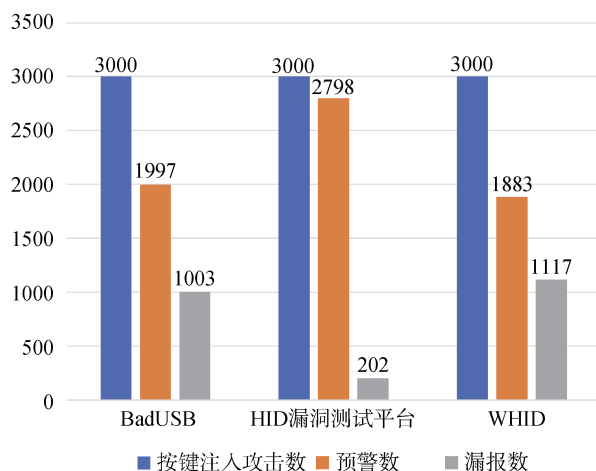


图 18 USB HID 攻击检测算法按键注入拦截结果  
Figure 18 USB HID attack detection algorithm key-press injection interception results

##### ② 360 安全套件验证(基于 PC-1)

首先, 在 PC-1 开启 360 安全套件, 然后通过 BadUSB、HID 漏洞测试平台及 WHID 平台发起 25 种各 120 次、120 次、120 次按键注入攻击。统计 360 安全套件预警次数。经实验验证, 360 安全套件无法对 3 个平台的按键注入攻击进行预警。

##### ③ WHID Defense 平台验证(基于 PC-2)

首先, WHID Defense 平台开启办公模式, 进入按键监控状态。然后通过 BadUSB、HID 漏洞测试平台及 WHID 平台发起 25 种各 120 次、120 次、120 次按键注入攻击。统计各个工具发起攻击时平台弹窗警告的次数。

实验过程中, BadUSB 发起 3000 次按键注入攻击, 平台完成了所有按键注入数据的监测, 成功拦截攻击并实现弹窗警告 2998 次, 漏报 2 次, 即 WHID Defense 对 BadUSB 发起的按键注入攻击拦截率为 99.93%, 漏报率为 0.07%。HID 漏洞测试平台发起 3000 次按键注入攻击, 平台完成了所有按键注入数据的监测, 成功拦截攻击并实现弹窗警告 3000 次, 漏报 0 次, 即 WHID Defense 对 BadUSB 发起的按键注入攻击拦截率为 100%, 漏报率为 0。WHID 平台发起 3000 次按键注入攻击, 平台完成了所有按键注入数据的监测, 成功拦截攻击并实现弹窗警告 3000 次, 漏报 0 次, 即 WHID Defense 对 BadUSB 发起的按键注入攻击拦截率为 100%, 漏报率为 0。如图 19 所示为 WHID Defense 按键注入拦截结果。

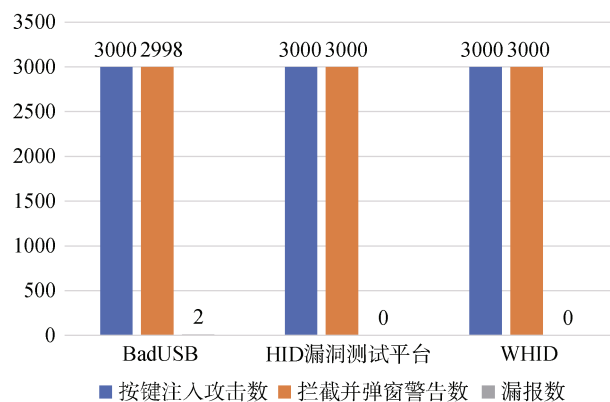


图 19 WHID Defense 按键注入拦截结果  
Figure 19 WHID Defense key-press injects the interception result

综上, 三个 USB HID 攻击平台共发起 9000 次按键注入攻击, USB HID 攻击检测算法实现攻击预警 6678 次, 漏报 2332 次, 拦截率为 74.2%, 漏报率为 25.8%; 360 安全套件无法拦截按键注入攻击; WHID Defense 平台成功监测了所有按键注入数据, 成功拦截攻击并实现弹窗警告 8998 次, 漏报 2 次, 拦截率约为 99.98%, 漏报率约为 0.02%。

#### (2) 捕获目标设备数据流实验过程及结果分析

##### ① USB HID 攻击检测算法验证(基于 PC-0)

首先, 在 PC-0 运行 USB HID 攻击检测算法, 然后通过 BadUSB、HID 漏洞测试平台及 WHID 平台各产生 6000 次数据通信, USB HID 攻击检测算法无

法捕获 3 个平台的数据流。

② 360 安全套件验证(基于 PC-1)

首先, 在 PC-1 开启 360 安全套件, 然后通过 BadUSB、HID 漏洞测试平台及 WHID 平台各产生 6000 次数据通信, 360 安全套件无法捕获 3 个平台的数据流。

③ WHID Defense 平台验证(基于 PC-2)

首先, WHID Defense 平台开启数据监控, 然后通过 BadUSB、HID 漏洞测试平台及 WHID 平台各产生 6000 次数据通信。统计数据库中存储的各攻击平台的通信数据量。

实验过程中, 数据库分别存储 BadUSB、HID 漏洞测试平台及 WHID 平台通信数据量为 6000、6000、6000, 实现了通信数据全监控, 捕获率为 100%, 丢失率为 0。

(3) 干扰目标设备正常通信实验过程及结果分析

① USB HID 攻击检测算法验证(基于 PC-0)

首先, 在 PC-1 运行 USB HID 攻击检测算法, 然后通过 BadUSB、HID 漏洞测试平台及 WHID 平台各产生 100 次数据通信, BUSHOUND 监控软件中各平台数据流向正常, USB HID 攻击检测算法无法干扰目标设备正常通信。

② 360 安全套件验证(基于 PC-1)

首先, 在 PC-1 开启 360 安全套件, 然后通过

BadUSB、HID 漏洞测试平台及 WHID 平台各产生 100 次数据通信, BUSHOUND 监控软件中各平台数据流向正常, 360 安全套件无法干扰目标设备正常通信。

③ WHID Defense 平台验证(基于 PC-2)

首先, WHID Defense 平台开启干扰模式, 然后通过 BadUSB、HID 漏洞测试平台及 WHID 平台各产生 100 次数据通信, 查看 BUSHOUND 数据监控软件中各设备的数据接收结果。

实验过程中, BadUSB、HID 漏洞测试平台及 WHID 平台各产生 100 次数据通信。其中, WHID Defense 成功干扰 BadUSB 数据通信 97 次, HID 漏洞测试平台 98 次, WHID 平台 98 次, 共成功干扰目标设备 293 次, 成功率为 97.7%。

综合以上三个实验结果表明, WHID Defense 平台在识别恶意按键注入攻击、捕获目标设备数据流、干扰目标设备正常通信三方面有着较强的检测防护能力, 防护手段完善、防护面广。如表 9 所示为 USB HID 攻击检测算法、360 安全套件、WHID Defense 功能评价对比结果。此外, 结合用户身份管理与访问控制、风险事件分类与统计等功能构建了一个全面的通用 USB HID 攻击检测防护平台, 为解决 USB HID 攻击提供了技术思路和系统原型。

表 9 USB HID 攻击检测算法、360 安全套件、WHID Defense 功能评价对比结果表

实验	攻击工具	目标机器	测试系统	结论
识别按键注入攻击		PC-0	USB HID 攻击检测算法	拦截率: 74.2% 漏报率: 25.8%
		PC-1	360 安全套件	拦截率: 0 漏报率: 100%
		PC-2	WHID Defense	拦截率: 99.98% 漏报率: 0.02%
捕获目标设备数据	BadUSB; HID 漏洞测试平台; WHID Defense	PC-0	USB HID 攻击检测算法	捕获率: 0 丢失率: 100%
		PC-1	360 安全套件	捕获率: 0 丢失率: 100%
		PC-2	WHID Defense	捕获率: 100% 丢失率: 0
干扰目标设备通信		PC-0	USB HID 攻击检测算法	成功率: 0
		PC-1	360 安全套件	成功率: 0
		PC-2	WHID Defense	成功率: 97.7%

6 结论

以往人们认为恶意攻击总会通过软件或网络发起或传播, 只要保证硬件处于物理隔离环境便可保

护硬件设备免受攻击从而确保数据安全, 但是随着“震网”病毒、COTTONMOUTH-I、BadUSB、USB Rubber Ducky 等攻击事件或攻击工具的曝光, 研究人员开始思考硬件层次的安全。随着 USB 接口的提



出和广泛使用,越来越多的数据存储在 USB 设备中或通过 USB 设备完成数据的迁移和交互,针对 USB 接口的 USB HID 攻击技术也逐渐兴起,保护个人计算机免受 USB HID 攻击正面临着严峻挑战。

USB 接口简化和改进了个人计算机与外围设备之间的接口,为数据传输等交互工作提供了便利性,也提高了人们的工作效率,可以说 USB 接口就是为了便利性而生。USB 接口在提供便利性的同时,也存在很多脆弱点,USB HID 攻击正是利用这些脆弱点展开了通过硬件接口进行恶意操作和数据窃取等一系列破坏性操作。因此,研究 USB HID 攻击的攻击特性,并研究相应的检测防护技术迫在眉睫。

本文通过对 USB 协议进行研究,提出了 USB 协议中存在的 4 个脆弱点。通过研究国内外主流 USB HID 攻击工具提出了 USB HID 攻击模型,并以此为原型提出了新型的检测防护思想,设计了恶意 USB HID 攻击检测防护平台,为研究人员研究基于 HID 的 USB 设备安全技术提供了理论模型和实验验证平台。

随着 USB HID 攻击技术正朝着高隐蔽性、高速度、高集成方向发展,研究更完善的 USB 设备安全技术还有很长的路要走。以下是针对本文研究内容存在的不足以及未来研究构想提出的几点展望,主要概括如下:

### (1) 按键间隔识别

由于按键注入攻击具有快速注入的特点,与正常用户按键间隔差异明显,因此,可以通过构建“按键键值间隔索引库”,引入机器学习的方法构建一个智能检测比对模型用以区分按键注入攻击和正常按键,同时,随着用户按键录入数据的增多,该模型可以自主学习用户按键习惯,从而使识别结果更科学。开展本部分工作的前提是收集具有代表性、广泛性的大量按键数据。

### (2) 多设备监控

目前 WHID Defense 平台只能实现单设备实时监控,随着计算机功能的增强,越来越多的 USB 外设成为日常工作的必要组成设备,因此,可以研究对多设备的实时监控,保证个人计算机安全。

根据以上分析,基于 HID 的 USB 设备安全技术按键间隔识别和多设备监控方面还有很大的研究空间,也有很多问题亟待解决。这需要研究人员不断深入分析和研究 USB HID 技术,借助新兴技术,不对完善 USB HID 攻击检测防护技术,保护个人隐私、商业秘密、政府机密不受侵害。

## 参考文献

- [1] Jian Y D, Yang Q, Yuan J. Hardware security attack and defense revealed[M]. Beijing: Publishing House of Electronics industry, 2017. (简云定, 杨卿, 袁舰. 硬件安全攻防大揭秘[M]. 北京: 电子工业出版社, 2017.)
- [2] Lü Z Q, Xue Y N, Zhang N, et al. Review of USB Device Security Technology[J]. *Journal of Information Security Research*, 2018, 4(7): 639-645.  
(吕志强, 薛亚楠, 张宁, 等. USB 设备安全技术研究综述[J]. *信息安全研究*, 2018, 4(7): 639-645.)
- [3] Universal Serial Bus Revision 3.2 Specification. USB Implementers Forum. <https://usb.org/document-library/usb-32-specification-released-september-22-2017-and-ecns>. Sept. 2017.
- [4] Sun G. Design and Implementation of Flash Disk Firmware[D]. University of Chinese Academy of Sciences(Institute of Software Chinese Academy of Sciences), 2003.  
(孙庚. 闪存盘固件的设计与实现[D]. 中国科学院研究生院(软件研究所), 2003.)
- [5] To kill a centrifuge: A technical analysis of what stuxnet's creators tried to achieve. Technical report. The Langner Group, <https://www.langner.com/2013/11/langners-final-stuxnet-analysis-comes-with-surprises/>. Nov. 2013.
- [6] Falliere N, Murchu L O, Chien E. W32. stuxnet dossier[J]. *White paper, Symantec Corp, Security Response*, 2011, 5(6): 29.
- [7] Masood R, Anwar Z. Swam: Stuxnet worm analysis in metasploit[C]. *2011 Frontiers of Information Technology. IEEE*, 2011: 142-147.
- [8] K. Nohl, J. Leil. BadUSB-On accessories that turn evil[J]. *Black-Hat USA*. 2014, 1(9): 1-22.
- [9] Nissim N, Yahalom R, Elovici Y. USB-based Attacks[J]. *Computers & Security*, 2017, 70: 675-688.
- [10] Episode 709: USB Rubber Ducky Part 1. HAK5. <https://hak5.org/episodes/episode-709>. Apr. 2010.
- [11] USB Rubber Ducky Payloads. HAK5. <https://github.com/hak5darren/USB-Rubber-Ducky/wiki/Payloads>. Dec. 2018.
- [12] USBdriveby. S. Kamkar. <http://samyp.pl/usbdriveby/>. Oct. 2014.
- [13] Broucker M, Checkoway S. iSeeYou: Disabling the MacBook Webcam Indicator LED[C]. *23rd {USENIX} Security Symposium ({USENIX} Security 14)*, 2014: 337-352.
- [14] Making BadUSB work for you - Derbycon. Adam Caudill. <https://adamcaudill.com/2014/10/02/making-badusb-work-for-you-derbycon/>. Oct. 2014.
- [15] A Fanny Equation: "I am your father, Stuxnet". Kaspersky Lab. <http://securelist.com/blog/research/68787/a-fanny-equation-i-am-your-father-stuxnet/>. Feb. 2015.
- [16] Anderson B, Anderson B. USB Hacksaw[M]. Seven Deadliest

- USB Attacks. Amsterdam: Elsevier, 2010: 1-26.
- [17] Guri M, Monitz M, Elovici Y. USBee: Air-Gap Covert-Channel via Electromagnetic Emission from USB[EB/OL]. 2016: arXiv:1608.08397[cs.CR]. <https://arxiv.org/abs/1608.08397>
- [18] USB killer v2.0. D. Purple. <https://habr.com/en/post/268421/>. Oct. 2015.
- [19] USBHarpoon is a BadUSB Attack with a Twist. Ionut Iascu. <https://www.bleepingcomputer.com/news/security/usbharpoon-is-a-badusb-attack-with-a-twist/>. Aug. 2018.
- [20] Li J S, Shu H, Dong W Y, et al. Security Monitoring Technology of USB Storage Device Based on Driver Layer[J]. *Computer Engineering*, 2008, 34(8): 255-257.  
(李锦山, 舒辉, 董卫宇, 等. 基于驱动层的 USB 存储设备安全监控技术[J]. *计算机工程*, 2008, 34(8): 255-257.)
- [21] Lu Z G, Liu J H, Liu B X, et al. Design and Implementation of USB Monitoring Technique Based on HID[J]. *Computer Engineering*, 2010, 36(4): 1-3.  
(卢志刚, 刘建华, 刘宝旭, 等. 基于 HID 的 USB 监控技术的设计与实现[J]. *计算机工程*, 2010, 36(4): 1-3.)
- [22] Wang Z, Stavrou A. Attestation & Authentication for USB Communications[C]. *SERE-C '12: The 2012 IEEE Sixth International Conference on Software Security and Reliability Companion*. 2012: 43-44.
- [23] 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(4): 166-185.
- [24] Grisioli F, Pizzonia M, Sacchetti M. USBCheckIn: Preventing BadUSB attacks by forcing human-device interaction[C]. *2016 14th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 2016: 493-496.
- [25] Jiang J G, Chang Z J, Lü Z Q, et al. Research on USB HID Attack Detection Technology[J]. *Chinese Journal of Computers*, 2019, 42(5): 1018-1030.  
(姜建国, 常子敬, 吕志强, 等. USB HID 攻击检测技术研究[J]. *计算机学报*, 2019, 42(5): 1018-1030.)
- [26] Huang W Z, Xu J. Universe Serial Bus (USB)[J]. *Application Research of Computers*, 2001, 18(2): 46-48.  
(黄维柱, 许军. 通用串行总线 USB[J]. *计算机应用研究*, 2001, 18(2): 46-48.)
- [27] Universal Serial Bus Revision 2.0 Specification. USB Implementers Forum. [http://www.usb.org/developers/docs/usb20\\_docs/](http://www.usb.org/developers/docs/usb20_docs/). Apr. 2000.
- [28] Liu R. Quanquan Teaches You How to Play USB [M]. Beijing: Beijing University of Aeronautics & Astronautics Press, 2009.  
(刘荣. 圈圈教你玩 USB[M]. 北京: 北京航空航天大学出版社, 2009.)
- [29] Device Class Definition for Human Interface Devices (HID). USB Implementers Forum. <https://usb.org/document-library/device-class-definition-hid-111>. June. 2001.
- [30] Yang M L, Yuan T. Keyboard Design Based on Ergonomics[J]. *Packaging Engineering*, 2005, 26(5): 168-170.  
(杨明朗, 袁桃. 基于人机工程学的键盘设计[J]. *包装工程*, 2005, 26(5): 168-170.)
- [31] Universal Series Bus Mass Storage Control/Bulk/Interrupt (CBI) Transport. USB Implementers Forum. <https://usb.org/document-library/mass-storage-controlbulkinterrupt-cbi-specification-11>. June. 2003.
- [32] Mo Y, Sinopoli B. Secure control against replay attacks[C]. *2009 47th annual Allerton conference on communication, control, and computing (Allerton)*. IEEE, 2009: 911-918.
- [33] Lemon J. Resisting SYN Flood DoS Attacks with a SYN Cache[C]. *BSDCon*. 2002: 89-97.
- [34] Sandhu R S, Samarati P. Access Control: Principle and Practice[J]. *IEEE Communications Magazine*, 1994, 32(9): 40-48.
- [35] Fu J M, Huang J W, Zhang L X. Curtain: Keep your Hosts Away from USB Attacks[M]. *Lecture Notes in Computer Science*. Cham: Springer International Publishing, 2017: 455-471.



吕志强 副研究员, 硕士生导师。于 2007 年在哈尔滨工业大学微电子学与固体电子学专业获得博士学位。现任中国科学院信息工程研究所副研究员。研究领域为信号收发与分析、射频系统集成。Email: lvzhiqiang@iie.ac.cn



薛亚楠 于 2016 年在中国地质大学(北京)电子信息工程专业获得学士学位。现在中国科学院信息工程研究所攻读硕士学位。研究领域为嵌入式硬件安全。Email: xueyanan@iie.ac.cn



**张宁** 于 2013 年在哥伦比亚大学电气工程专业获得硕士学位。现在中国科学院信息工程研究所攻读博士学位, 任中国科学院信息工程研究所工程师。研究领域为信息安全。Email: zhangning@iie.ac.cn



**冯朝雯** 于 2016 年在武汉理工大学通信工程专业获得学士学位。现在中国科学院信息工程研究所攻读博士学位。研究领域为信息与信号处理。Email: fengchaowen@iie.ac.cn



**金忠峰** 于 2017 年在辽宁工程技术大学获机械电子工程专业硕士学位。现于中国科学院信息工程研究所攻读博士学位。研究领域为工业控制系统安全。Email: jinzhongfeng@iie.ac.cn