USB HID 攻击检测技术研究

姜建国[1),2)] 常子敬[1),2)] 吕志强[1),2)] 张 宁[1)]

[1)](中国科学院信息工程研究所 北京 100093)

[2)](中国科学院大学网络空间安全学院 北京 100049)

摘 要 该文提出了一种基于多元击键特征的 USB HID 攻击检测算法.该算法根据人类用户自然击键习惯将数据流切分为特征稳定的短击键序列,通过融合隐藏在噪声中的多组短序列数据提取出稳定的多元特征,并利用这些特征汇聚成为特征知识,为 SVM 分类器提供决策依据.基于这种算法的安全策略实现了实时认证实时授权的检测机制并从数据组表征的自然击键事件中得到了丰富稳定的击键特征.这些特征不单是击键间隔,还包括错误率、速度、节奏波动等多元特征.该文提出的 HID 攻击检测算法在真实环境中的测试显示且分类准确率达到了 99.9127%.相比现有的检测技术,该算法具有自动识别、高准确率、高鲁棒性等优点,可以部署在个人电脑上保护用户隐私,可以抵御包括 BadUSB 在内的多种恶意工具的攻击.

关键词 恶意 USB 设备;USB HID 协议;攻击检测;击键动力学特征;SVM 分类器

中图法分类号 TP334 **DOI 号** 10.11897/SP.J.1016.2019.01018

Research on USB HID Attack Detection Technology

JIANG Jian-Guo[1),2)] CHANG Zi-Jing[1),2)] LV Zhi-Qiang[1),2)] ZHANG Ning[1)]

[1)](*Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093)

[2)](*School of Cyber Security, University of Chinese Academy of Sciences, Beijing* 100049)

Abstract As a powerful computer interface, the USB interface has become an essential hardware device for general-purpose computers, and a large amount of data is exchanged through this interface. However, the security problems that the USB interface has faced are also increasingly prominent. Attacks by hackers using this interface are also becoming increasingly sophisticated, not just for spreading viruses. In the USB attack, the USB HID attack technology plays a key role, which is used to quickly enhance permissions. This also leads to new challenges for privacy and data security. At the same time, the rapid development of programmable embedded hardware provides the foundation for attack miniaturization and integration. Not only that, the attack began to try some more sophisticated attacks, such as the combination of USB HID attacks and other attack techniques. This also revealed an important problem, the lack of computer hardware security protection. USB HID attack is a new type of technology that uses the USB interface for malicious hardware attacks. This technology manipulates the computer to execute malicious programs by using the HID protocol vulnerability to forge user keyboard input. The defense technology against USB HID attacks can be divided into USB protocol extensions and enhancements, USB enumeration authentication, and key-based dynamic feature detection technologies. At present, the existing protection measures against this attack technology are still imperfect, with low automation, poor robustness, and incomplete protection. This paper starts with the USB

收稿日期:2017-06-17;在线出版日期:2018-07-11.本课题得到国家自然科学基金(61501458)资助.**姜建国**,博士,研究员,博士生导师,主要研究领域为信息安全与保密技术.E-mail:jiangjianguo@iie.ac.cn.**常子敬**,硕士,主要研究方向为嵌入式设备安全.**吕志强**(通信作者),博士,副研究员,硕士生导师,主要研究领域为信号收发与分析、射频系统集成.E-mail:lvzhiqiang@iie.ac.cn.**张 宁**,硕士,助理工程师,主要研究方向为电磁物理安全.

protocol, and analyzes the two loopholes of the device permission management and device reliability in the process of USB protocol enumeration and HID protocol operation using the state machine model. A USB HID attack detection algorithm based on multiple keystroke characteristics is proposed in this paper. The algorithm continues the idea of keystroke feature analysis and establishes a new detection protection model with the idea of active authentication. It divides the data flow into short keystroke sequences with stable characteristics according to the natural keystroke habits of human users, extracts stable multiple features (such as keystroke interval, error rate, speed, and rhythm fluctuations, etc.) by merging multiple sets of short sequence data hidden in noise and provides decision basis for SVM classifier. The security strategy based on this algorithm realizes the real-time authentication and real-time authorization detection mechanism, obtains rich and stable keystroke characteristics from the natural keystroke events characterized by data groups. These features are not only the keystroke intervals but also the error rate, the speed, Rhythm fluctuations and other characteristics. The proposed HID attack detection algorithm shows that the classification accuracy rate is up to 99.9127% in real environment tests. Compared with the existing detection technology, this algorithm has the advantages of automatic identification, higher accuracy and higher robustness. In addition, this paper adopts a larger data set and a richer test scenario, which does not require the input and length of the attacker, and is more in line with the actual application scenario. It has greatly improved the accuracy and universality of detection. It can be deployed on personal computers in the protection of users' privacy, and can defend against various malicious tools including BadUSB.

Keywords　malicious USB device; USB HID protocol; attack detection; keystroke feature; SVM classifier

1　引　言

USB 接口作为一个功能强大的计算机接口已经成为了通用计算机必不可少的硬件设备，大量的数据通过这种接口交换. 但是 USB 接口所面临的安全问题也日益凸显. 黑客利用这种接口实现的攻击也日趋复杂，不仅仅局限于传播病毒.

一种被称为 USB HID 攻击的新型 USB 攻击技术正在兴起. 这是一种利用 HID 协议漏洞的攻击技术，通过伪造用户键盘输入内容，操纵计算机执行恶意程序. 最早，一些黑客使用一种称为“Teensy”的小型 USB 开发板，制作了利用这种漏洞的攻击工具[1]. 随后出现了伪装成 USB 插头的多功能 HID 攻击工具“COTTONMOUTH-1”和“TURNIPSCHOOL”，还有利用普通 U 盘作为攻击工具的“BadUSB”[2-3]. 得益于成本的降低，如今，USB HID 攻击技术正在快速普及. 不仅如此，攻击开始尝试一些更为复杂的攻击手段，这种手段是将 USB HID 攻击和其他攻击技术相结合的手段. 例如，使用 HID 攻击技术帮助虚拟机逃逸[4-5]等. HID 攻击技术扮演了关键角色，它被用于快速提升权限. 随之而来的个人隐私和数据安全又面临新的挑战.

目前，针对这种攻击技术已有的防护手段依然不完善，存在自动化程度不高、鲁棒性差、防护不全面等问题. 因此本文针对以上问题做了以下 3 个方面的贡献：

(1) 从 USB 协议入手，利用状态机模型，分析了 USB 协议枚举过程和 HID 协议运行过程中存在的设备权限管理和设备可靠性校验两个漏洞.

(2) 设计了时域聚合的数据预处理算法. 算法根据人类用户自然击键习惯将数据流切分为特征稳定的短击键序列，原有掩藏在噪声中的数据通过数据融合后汇聚成为有用的特征知识，为 SVM 分类器提供决策依据. 基于这种算法的安全策略实现了实时认证实时授权的防护机制.

(3) 设计了多元击键特征提取算法，从数据组表征的自然击键事件中得到了丰富稳定的击键特征. 这些特征不单是击键间隔还包括错误率、速度、节奏波动等多元特征. 本文还应用了 SVM 分类器

实现小样本下的自动学习分类.

本文在第 2 节介绍近年来 USB HID 攻击防护技术发展情况;第 3 节介绍本文所使用的 USB HID 协议和 SVM 分类器的技术背景;第 4 节重点介绍设计流量识别算法的具体细节;第 5 节是实验部分,通过 3 个实验进一步说明了识别算法的设计方法和识别效果;最后一节是结论.

2 相关工作

目前,USB HID 攻击防护工作已经有一些学者做了研究,但是效果均不理想,没有实用化的成果出现. 攻击防护工作大致分为 3 个方向:

(1) 扩展和加固 USB 协议

在原有 USB 协议基础上扩展了认证、签名算法[6]. 所使用的 USB 设备必须支持这种扩展的 USB 安全协议,经过主机的签名认证才能建立通信. 这种方式保证了主机所连接的设备都是经过认证的安全设备,但是这种技术不兼容大多数未经改造的 USB 设备. 因此这种技术存在很大的局限性.

(2) USB 枚举属性检查

这种技术主要用于设计硬件沙箱或者局域网内检测服务器来检测未知 USB 设备的枚举内容并通知用户,用户核验枚举内容和设备用途后确定未知设备是否具有威胁[7-8]. 目前大部分的防护技术研究都集中在这一领域,这种检测技术依靠用户的判断而且仅仅检查设备枚举内容,存在自动化水平不高,检测内容单一、防护能力不强的问题.

(3) 基于击键特征的检测技术

这种技术将正常用户的输入作为模板,通过击键动力学身份认证算法分析未知输入和模板的差别,判断输入者的身份[9]. 这种方法优点在于能够持续地监控未知 HID 设备的输入特征,不仅关注枚举环节的验证,重点监控后续的行为特征. 但是这种技术只能识别模板库中已有的内容,而实际的攻击内容千变万化很难保证完全匹配. 但是这种技术还是为本文提供了很好的思路.

在下一节内容中,将介绍建立流量识别模型的基础理论.

3 USB HID 协议漏洞分析

3.1 USB HID 协议

USB HID(Human Interface Device)是众多 USB 设备中的一种,也是最常见的一种,它被广泛用于人机交互和少量实时数据传输,例如键盘、鼠标等设备①②. HID 设备不仅限于人机交互设备,任何符合 HID 接口协议规范的设备都可以称为 HID 设备. Windows 操作系统最早开始支持 HID 设备,原生系统提供了默认的驱动程序,至今所有的主流操作系统都已经内置有 HID 设备的驱动程序,应用程序可以直接使用这些驱动程序来与 HID 设备通信.

HID 设备同其他 USB 设备一样需要经过握手(handshake)、枚举(enumeration)的过程才能和主机建立通信. 枚举就是主机向设备询问配置需求,并根据需求准备好通信条件的过程. 一台主机上可以同时定义多个 HID 接口和其他不同类型的接口,这些接口组成一个复合设备. 定义的接口种类和数量由设备申请而自由决定.

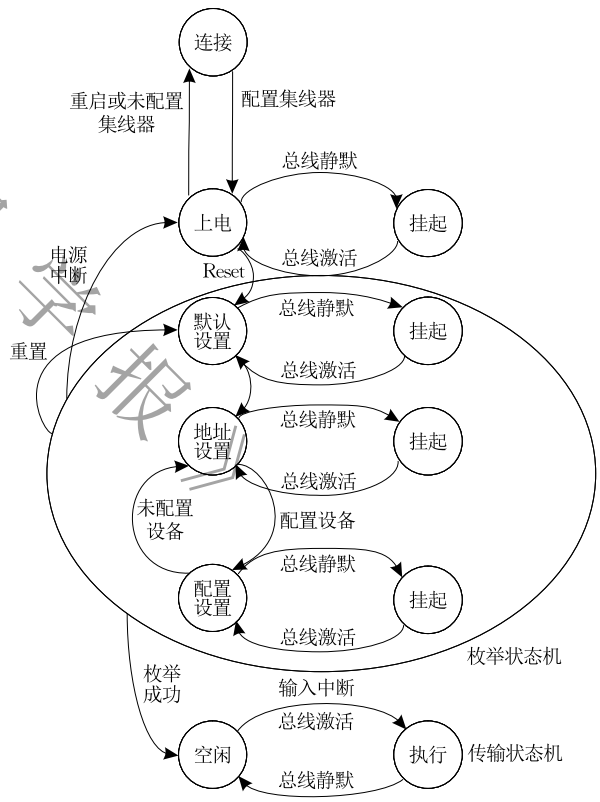


图 1 以 USB HID 为例分析 USB 枚举状态机

USB 的枚举过程可以总结为一个状态机的状态转移过程,不同的接口传输状态机不尽相同,HID 协议是一种事件驱动型状态机,图 1 是以 HID 为例

① Universal Serial Bus HID Usage Tables. http://www.usb.org, 2015.12.20

② USB Class Codes. http://www.usb.org/developers/defined_class/#BaseClass0Fh, 2015.12.20

分析了协议运行状态转移过程. 设备完成枚举后，由枚举状态机跳出，进入到了传输状态机①. HID 协议在进入传输状态后，是以事件为中心驱动协议工作. 以键盘为例，用户的按键中断事件驱动 HID 协议发送数据，协议状态机由空闲态转为执行态，执行命令响应用户操作. 由于采用中断传输模式，HID 协议可以在空闲态保持长时间等待，直到事件触发状态机.

3.2　数据特征分析

HID 接口传输的数据称为报表(report)，设备的固件必须能够处理 HID 报表的格式. 报表的格式非常有弹性，可以处理任何类型的数据. 传送的数据可以是鼠标的位移、键盘的键值、滚轮的滚动值甚至可以是文本数据②.

传感器捕获到 USB 总线上传送的 HID 报表，这些被捕获的报表经过解析并加盖时间戳后可以得到表 1 中展示的数据. 这是用户用键盘输入的“Win＋R cmd”，“Win＋R”即为 Windows 组合快捷键.

每条数据包含设备号、数据长度、相位、8 字节按键内容、数据间隔和时间戳. 为了便于理解，在表最后一列备注了按键内容. 这里需要说明的是，设备 ID 不是 USB 设备的 PID 和 VID 值，是传感器为每个 USB 设备分配的 ID 编号.

表 1　传感器收集并解析后的 HID 数据

设备	长度	相位	数据	间隔	时间	内容
28.1	8	IN	08 00 00 00 00 00 00 00	6.4 s	14:42:02.304	Win
28.1	8	IN	08 00 15 00 00 00 00 00	327 ms	14:42:02.632	Win＋r
28.1	8	IN	08 00 00 00 00 00 00 00	135 ms	14:42:02.768	Win
28.1	8	IN	00 00 00 00 00 00 00 00	15 ms	14:42:02.784	Blank
28.1	8	IN	00 00 06 00 00 00 00 00	1.0 s	14:42:03.791	c
28.1	8	IN	00 00 00 00 00 00 00 00	112 ms	14:42:03.904	Blank
28.1	8	IN	00 00 10 00 00 00 00 00	39 ms	14:42:03.944	m
28.1	8	IN	00 00 00 00 00 00 00 00	135 ms	14:42:04.080	Blank
28.1	8	IN	00 00 07 00 00 00 00 00	79 ms	14:42:04.160	d
28.1	8	IN	00 00 00 00 00 00 00 00	71 ms	14:42:04.232	Blank

3.3　协议脆弱性分析

所有的 USB 物理攻击技术不论是 COTTONMOUTH-1 还是 BadUSB，都使用了 USB HID 协议的漏洞提升权限执行恶意行为. 分析这一问题的根源需要从 USB 协议本身入手，了解漏洞形成原因、运行原理才能有针对性的利用和防范.

以美国国家安全局研制的一款 USB 攻击工具——COTTONMOUTH-1 为例展示 USB HID 攻击的过程并分析其中原理. 如图 2 所展示，COTTONMOUTH-1 是一种典型的 HID 攻击工具，它是植入在 USB 接口的微型间谍设备，具有窃取数据、远程控制、无线回传数据等功能，利用 HID 攻击技术实现对目标计算机的入侵和控制.

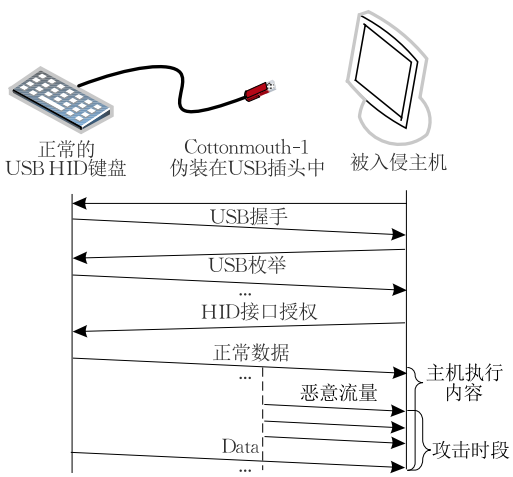


图 2　以 Cottonmouth-1 为例说明 USB HID 协议的漏洞

在图 2 中所示一个正常的 USB 键盘通过握手和枚举顺利地在主机上申请了一个 HID 接口，用于向主机发送用户的击键数据. COTTONMOUTH-1 利用正常键盘刚刚申请好的 HID 接口向主机发送伪造的击键数据. 主机在未判明数据可靠性的情况下接受并执行了伪造数据，攻击者利用这些伪造数据就成功地控制了目标计算机. 在这个攻击过程中存在两个重要的安全漏洞.

(1) USB 主机特权许可漏洞. USB 协议中规定设备可以自定义各种接口，而 HID 接口具有直接操作主机的特权. 这个特权是 HID 接口固有特性，USB 协议缺少对这类高权限接口的管理机制，在枚举时完全依照设备需求配置相应的接口、授予权限，授权后也缺少取消授权机制，这样的设计让攻击者可以毫无限制的申请和使用高权限的接口.

① Universal Serial Bus Specification Revision 2.0. http://www.usb.org, 2015.12.20

② Universal Serial Bus Device Class Definition for Human Interface Devices (HID). http://www.usb.org, 2015.12.20

(2) HID 数据源可靠性漏洞. HID 协议默认传输的是用户产生的人机交互数据,但是协议并没有对数据源进行校验,所有数据不加甄别即执行,使得攻击者可以随意伪造数据欺骗主机执行恶意操作.

攻击者利用上述两个漏洞可以快速地获取目标主机管理员权限,执行恶意操作,进而窃取用户隐私数据等. 无论是主机的特权漏洞还是数据源可靠性漏洞,其根本原因是操作系统和 USB 协议认为 USB 外设是安全可信的,因此没有设置任何防范措施. 所以,在 USB 设备出现了恶意行为后操作系统完全没有防御能力.

4 USB HID 流量识别算法

完整的流量识别算法主要分为 5 个步骤,采集数据、数据预处理、提取特征、SVM 分类和攻击响应. 本文创新的提出了时域聚合的数据预处理算法、击键动力学提取特征算法并在流量识别中引入 SVM 分类器实现自动化检测,具体工作流程如图 3 所示. 采集的离散数据通过比较数据间隔时间 τ 和聚合阈值 T_{gap} 将满足条件的数据截断,聚合为特征稳定的数据组后提取数据组特征,SVM 分类决策输出告警.

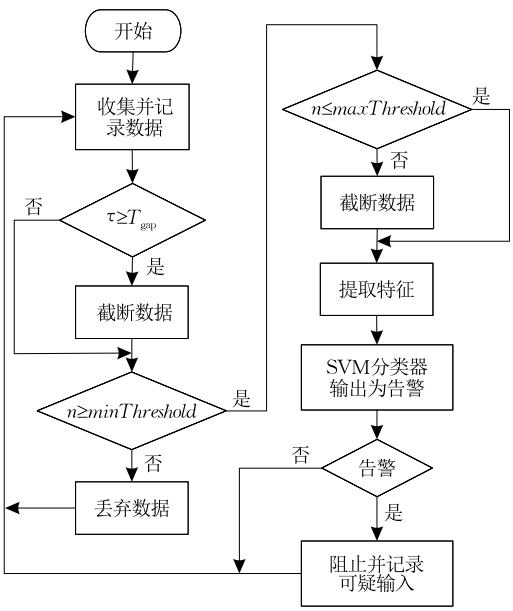


图 3 攻击检测算法流程图

4.1 主动认证

主动认证(active authentication)策略最早公开出现于2013年美国国防部高级研究计划局(DARPA)的一篇报告中. 报告指出现有的使用密码认证的信息安全系统已经无法应对日益严峻的安全挑战,提出了一种主动认证的思想[10]. 这是一种全新的认证机制,目的在于避免传统静态密码易伪造、易猜测、易截获的弱点. 报告认为,账户密码组合只是真实用户的身份代理,这种代理只在一定条件下能真正代表真实的用户,但并不能保证任何时候都是安全有效的. 而且基于这种代理账户的认证还存在着很多问题,如一次认证持续授权. 用户可能使用弱密码、有规律的密码以及攻击者计算能力的增强. 所以,DARPA 提出了实时的认证用户生物特征,直接对真正用户的物理、生物特征实时认证实时授权的安全认证策略,并已经开发完成了一套完善的基于软件的生物信息认证系统.

总的来说,主动认证思想的核心包含两部分:

(1) 主动认证用户生物特征代替传统口令密码的代理认证策略;

(2) 实时认证,动态授权.

本文的检测算法全面继承了主动认证核心思想,击键动力学为核心认证机制,实时认证用户的击键行为,一旦发现违规行为立刻撤销授权. 不仅如此,本文采用的安全策略还结合了外围设备持续不可信假设. 外部 HID 设备将视为持续不可信的数据源,接口的数据需要接受和外部访问者一样的验证后才能授权. 这种授权是主动认证,通过直接判断数据源的生物信息,持续认证使用者的合法性. 区别于传统的认证-授权机制,系统对设备一直保持不信任,持续分析实时授权,一旦判断的结果不满足安全条件将撤销其授权. 这种不信任假设保证了系统对每一个接入设备的每一时刻都采取了有效的主动识别策略,避免了浑水摸鱼的设备骗取主机一时的授权后为所欲为.

4.2 数据聚合预处理算法

这一节阐述本文提出的基于数据聚合思想设计的数据预处理算法. 同一 HID 在时域上的数据流如图 4 所示,一条数据认为是一次击键行为,横轴为时间. 一段连续的击键行为会产生一组密度较大的数据流,在大时间尺度下,它们看起来是一个整体,称为一个数据组 G. 图中深灰色代表了 7 组连续击键行为产生的数据流. 缩小时间尺度,观察第 4 组数

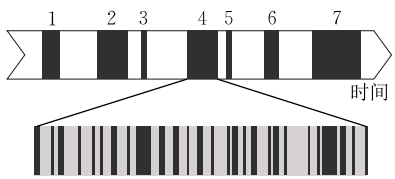


图 4 键盘输入数据流在时域上的分布

据，会发现完整的数据组是由很多离散地击键行为所组成的，深灰色的时间段代表有按键按下，每个按键被按下的时间和间隔都不是一致的.

基于上述事实，本文提出了形式化定义和两条基本假设.

定义 1.　针对同一 HID，存在时域内离散的击键行为 K 构成原始 HID 数据流 S，每次击键行为具有相应的安全属性 P_i. 对击键行为的安全属性分析操作定义为 $\triangleright$.

$$P=\{P_{\text{authorized}},P_{\text{unauthorized}}\},$$
$$S=\{K_1,K_2,K_3,\cdots,K_{N-1},K_N\},$$
$$K_i\triangleright P_i\in P.$$

假设 1.　时域上连续的击键行为具有同一属性 P_j.

根据假设 1，可以得到如下推论.

推论 1.　一段连续行为来自同一个输入者，它们具有相同的安全属性.

这个推论很容易理解，在日常使用键盘设备的情况下间隔相对集中的输入都是同一使用者的输入，而间隔时间较长的输入则有可能是其他用户所为. 因此，安全属性可能发生改变. 判断击键行为是否连续，本文引入聚合阈值 T_{gap} 判断击键行为是否连续，数据 K_i，K_{i-1} 间隔时间记为 τ_i，比较 T_{gap} 和 τ_i 将原始 HID 数据流 S 被截断为多个数据集合 G_i. 对于上述问题的形式化表达如下：

$$\tau_i=\begin{cases}T(K_i)-T(K_{i-1}), & i=2,3,\cdots,N\\ 0, & i=1\end{cases}$$
$$G_j=\{K_i\in S\mid K_i,K_{i+1},K_{i+2},\cdots,K_{i+n}\}$$
$$\text{s.t. }\tau_i>T_{\text{gap}}\ \&\ \tau_{i+n+1}>T_{\text{gap}},\ i,j=1,2,3,\cdots,N$$
$$G_j\Delta P_j=\{K_i\in S\mid K_i\Delta P_i,K_{i+1}\Delta P_{i+1},K_{i+2}\Delta P_{i+2},\cdots,K_{i+n}\Delta P_{i+n}\}$$
$$P_j=\{P_i\cap P_{i+1}\cap P_{i+2}\cap\cdots\cap P_{i+n}\}\in P$$

假设 2.　相邻数据组之间相互独立.

根据假设 2，G_i 和 G_{i-1} 之间相互独立，可以得到推论.

推论 2.　相邻两个时间片内的击键行为相互独立，安全属性相互独立.

这些数据组 G_i 构成了本文安全属性的最小分析单元，也是击键特征的最小分析单元.

如图 4 中，G_6 是一组攻击工具产生的数据. 根据假设 1 可知，每个数据组由同一安全属性的按键数据组成；根据假设 2 可知，G_6 和 G_5 以及 G_7 是相互独立的数据组，安全属性也没有联系.

上述过程将原有在时域上离散的数据，通过融合、关联分析后聚合为了一些同一属性的数据组 G. 数据组可以集中、稳定、可靠表征这些行为特征，进而分析其安全属性. 实际意义体现在：HID 在一段时间没有操作后（超过 T_{gap} 时间），原有安全属性消失，再有新的操作时系统需要重新分析其安全属性是否为授权用户行为.

为了保证聚合后的数据 G 能够稳定的体现击键行为的特征，需要设置约束条件对聚合长度 n 加以限制，不满足条件的数据将舍弃. G_i 的特征是通过数据的统计学分析得到，样本过短过长都会导致统计学特征出现偏差，过短的样本会使平稳特征值引入过量噪声，过长样本会使动态特征不敏感. 因此本文设置了 $minThreshold$ 和 $maxThreshold$ 限制聚合长度 n. 根据实验统计和分析，攻击者要想实现一次成功的 USB HID 攻击，需要不少于 20 次的输入，因此 $minThreshold\leq 20$ 则满足安全规则，可认为丢弃数据为安全行为. 由此可以得到以下结论：

$$(D_1\Delta P_1)\cap(D_2\Delta P_2)\cap\cdots\cap(D_j\Delta P_j)=P_{\text{authorized}},$$

其中 D_i 为丢弃数据组.

4.3　多元击键特征

击键动力学这种技术已经被广泛用于生物特征认证技术中[11-12]. 在 2011 年美国国防部高级研究计划局（DARPA）就开始研究使用击键动力学特征增强安全系统的访问控制. USB HID 攻击是通过伪造键盘的数据控制目标主机，因此分析击键行为的差异能够识别攻击者，本文近似的认为两条数据间隔即为击键间隔（keystroke latency）. 攻击者为了防止被发现，会快速的向计算机发送按键数据. 据采集的 HID 数据绘制成击键曲线如图 5 所示，“用户”曲线是正常用户的输入，“攻击工具”曲线是攻击者的输入. 因此，本文提出的特征提取算法将围绕击键速度、击键节奏、错误率等特征开展.

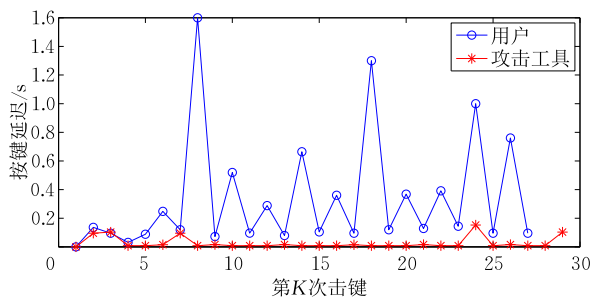


图 5　正常用户和攻击工具的击键间隔对比

定义特征向量 $\boldsymbol{F}=[\mu,\sigma,\eta,n,e,s]$. 提取特征工作是将数据组内在属性显式化的过程：

$$E(G_1,G_2,\cdots,G_i)=\{F_1,F_2,\cdots,F_i\}^{\mathrm{T}}(i=1,2,\cdots,N),$$

式中，E 表示特征提取函数，输出为对应数据组的特征矩阵，n 为击键序列长度.

(1)平均击键速度 μ. 反映了输入者的这段输入的平均击键速度，即单位时间内的击键次数.

$$\mu = n \Big/ \sum_{i=1}^{n} \tau_i .$$

(2)击键间隔方差 σ. 反映击键行为在频域上的波动情况.

$$\sigma = \sum_{i=1}^{n} (\tau_i - \bar{\tau})^2 / n .$$

(3)平均击键个数 η. 反映了每次击键动作的完整性.

$$\eta = \sum_{i=1}^{n} k_i / n .$$

该特征通过统计每条数据中按键的个数 k，计算一段击键行为的平均击键个数. 它反映每次击键行为的连贯性和完整性. 如果按键一次后马上抬起，传感器会收到一条含有击键内容的数据和按键抬起后的空数据，此时 $\eta = 0.5$. 如果击键过程很快，存在大量连击或者使用组合按键的行为，这个值将上升. 以表 1 中的 10 条数据为例，$\eta = 0.7$. 对于攻击工具而言，这个特征值将会增大. 这个值过大或者低于 0.5 都将视为异常.

(4)击键错误率 e. 反映了击键行为的错误情况，通过统计使用 Backspace 和 Delete 键次数占全部输入内容的比率得到. 人在正常的输入过程中难免会有输入错误的情况，但是对于攻击工具来说不会出现任何错误. 错误率这个特征是一个辅助的参考，还应该结合 η, n, μ 联合做出判断.

(5)可疑输入次数 s. 分析输入内容，如果输入中存在“Win+R”之类的输入，则认为是一种值得重点关注的行为，出现的次数记为 s.

(6)规范化. 各个特征值需要缩放在一个合理的范围内，避免某个特征参数因为幅值过大导致在分类决策中在占比过大影响分类准确率. 我们选取样本集中正常用户输入各项特征的最大值的倒数，并将这个值固化为分析时的固有参数，保证各个样本缩放在统一尺度内.

4.4 SVM 分类器

支持向量机(Support Vector Machine，SVM)基于统计学习理论，是一种通用的机器学习方法. 20 世纪 60 年代 Vapnik 等人[13-14]开始研究有限样本情况下的机器学习问题. 该算法采用结构风险最小化原则(Structural Risk Minimization，SRM)，综合考虑了经验风险和置信范围，使分类器不仅有较好的分类性能而且有较好的推广性. SVM 实质上是求解一个凸二次规划问题，从理论上获得该问题的全局最优解，同时，解决了神经网络方法中无法避免的局部极值问题. 此外，SVM 是专门针对有限样本问题的解决方案，其目标是得到现有信息下的最优解而不仅仅是样本数趋于无穷大时的最优值. SVM 算法还利用核函数解决了维数灾难的问题，其算法复杂度与样本维数无关[15-16].

本文研究的问题是一种小样本下的统计学习问题. SVM 分类器可以非常好的解决这类问题，实现全自动化的流量识别，提高防护水平[13].

本文将数据 $(x_1, y_1), (x_2, y_2), \cdots, (x_n, y_n)$ 分为两类，其中 $\boldsymbol{x}_i \in \Re^N$ 是特征向量，$y_i \in \{-1, +1\}$ 是分类标签. 我们假设在希尔伯特空间 H 内两类样本可被一个超平面 $\boldsymbol{\omega} \cdot x + b = 0$ 准确分开，由于缺乏对数据的先验知识，最优超平面应是分类间隔最大的平面. $\boldsymbol{\omega}$ 是超平面的法向量，b 是超平面的常数项[14-15]. 对于线性不可分的情况，可以通过在约束条件中加入松弛变量 $\xi_i \geq 0$，在目标函数中加入惩罚参数 C 来解决这一问题，相应的优化问题变为

$$\min J(\boldsymbol{\omega}, \xi) = \frac{1}{2}\boldsymbol{\omega}^{\mathrm{T}}\boldsymbol{\omega} + C\sum_{i=1}^{n}\xi_i$$

$$\text{s.t. } y_i(\boldsymbol{\omega}^{\mathrm{T}}\boldsymbol{x}_i + b) \geq 1 - \xi_i,\ \xi \geq 0,\ i = 1, 2, \cdots, n$$

在这个函数中我们得到了一个重要的参数 C，它决定了函数对错分样本的惩罚程度，是平衡分类能力和泛化能力的重要参数. SVM 通过核函数将特征映射到希尔伯特空间求解最优分类平面. 由此得到分类函数：

$$f(x) = \mathrm{sgn}\Big(\sum_{i=1}^{n} a_i^* y_i K(\boldsymbol{x}_i, x) + b^*\Big),$$

其中 b^* 为分类阈值，$a_i^*\ (i = 1, 2, \cdots, n)$ 是拉格朗日乘子. $K(\boldsymbol{x}_i, x)$ 是核函数. 对比分析文献，本文采用 RBF(Radial Basis Function)核函数[17].

$$K(\boldsymbol{x}_i, x_j) = \exp(-\gamma \| \boldsymbol{x}_i - x_j \|^2),\ \gamma > 0.$$

此时，得到了第二个重要的参数 γ，其决定了样本特征子空间分布的复杂程度，也决定了模型的泛化能力和分类能力[18]. 因此，本文在优化 SVM 分类器时需要寻找一组最优的 (C, γ) 参数来确保分类模型的性能.

5 实验分析

根据上一节理论分析可知，算法的一些关键参

数决定了模型的性能，具体参数包括预处理数据时的数据组划分间隔（T_{gap}）、数据聚合长度门限值和 SVM 分类器参数组(C,γ). 本文将通过实验方式分别确定以上 3 个参数.

本实验选取了 6 位受试者，采集他们 3 天内的所有的键盘输入行为作为正常的用户的输入行为参考，他们的输入包括写代码、写文章、聊天、浏览网页等常见的输入内容. 还会刻意的要求受试者使用 Win＋R 热键调用 PowerShell 模拟攻击者的行为，在电脑上运行 BUSHound 记录使用者的所有 HID 数据. 考虑到 BadUSB、COTTONMOUTH-1、TURNIPSCHOOL 都是采用相同的攻击技术，HID 流量具有相似的特征，本文使用 Teensy 开发板模拟了其它几种工具的攻击流量. 包含了关机、生成并运行恶意脚本、下载恶意软件、修改注册表等多种攻击载荷，这些载荷在攻击时均未被反病毒软件发现和阻止. 实验总共收集到了 204 233 条数据，其中正常用户数据 98 643 条，攻击工具产生 105 590 条.

检测算法运行硬件环境为：联想 K41 笔记本运行 Windows 10 操作系统、2.4 GHz Intel Core i7-5500U CPU、8 GB 内存.

5.1　预处理关键参数寻优

5.1.1　寻找最优 T_{gap} 值

为了将连续的数据流分割聚合成为数据组，首先需要确定如何分割这些数据. 分割这些数据的第一个关键参数就是 T_{gap}，大于 T_{gap} 时间长度的击键间隔将被认为是新的独立击键行为. 因此，本实验旨在寻找最优 T_{gap} 值. 原始数据是一片长长的击键流量记录表，记录了每次击键间隔. 这些间隔的差别很大，最短的能达到 1 ms，最长的可以达到数小时. 为了寻找一个合适的分割参数，实验统计了这段时间内所有人类输入的击键间隔，将实验数据绘制成了图 6 的饼状图，大多数击键间隔集中在 0～1.0 s 之间，这说明大部分击键活动还是快速连续的. 击键行为的速度和使用键盘的熟练程度、个人习惯、所在场景有很大关系，为了保证算法的有效性，需要保证 98％以上的行为能够被模型覆盖. 0～6.0 s 内集中了 98.06％的击键行为，对于剩余的不足 2％的间隔时间过长而且占比非常少的间隔，认为这种间隔即为连续数据组间隔. 用户超过了 6 s 没有输入，认为之前的输入行为中止，$T_{gap}=6.0$ s.

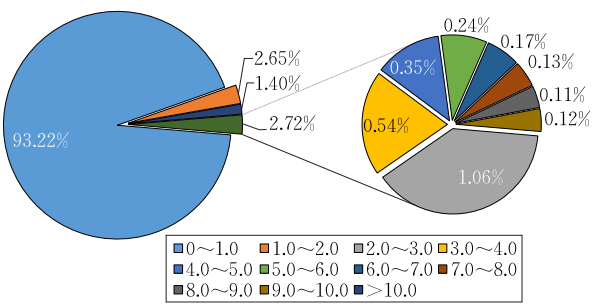


图 6　人类用户按键延迟统计频数分析

5.1.2　寻找最优数据长度门限

通过上一实验连续的数据流已经分割成了相互独立的数据组，每个数据组内数据长度不一致. 数据组过短会影响特征的稳定性，过长会影响特征敏感性. 本实验目的是确定最优数据聚合长度门限. 门限值 *maxThreshold* 和 *minThreshold* 分别限定了数据组长度的上下限. 长度低于 *minThreshold* 的数据组将会被舍弃，所以它的选取决定了数据丢弃量. 本实验原则是在尽可能少丢弃数据的情况下去除干扰噪声，因此定义数据丢弃率 β 作为参数评价指标.

$$\beta=\frac{\text{丢弃数据条数}}{\text{总数据条数}}\times 100\%.$$

实验使用正常用户数据输入，为了充分研究数据丢弃率的影响因素，本实验分别从最小聚合长度值和数据组间隔时间两个维度统计了对数据丢弃率(β)的影响，并绘制了图 7. 由实验结果可知，β 整体上随 T_{gap} 增加和最小聚合长度值减小而减小. β 和 T_{gap} 成线性的关系，随着 T_{gap} 的增大 β 下降；但是实验数据反映出 β 随 *minThreshold* 呈阶梯下降的趋势.

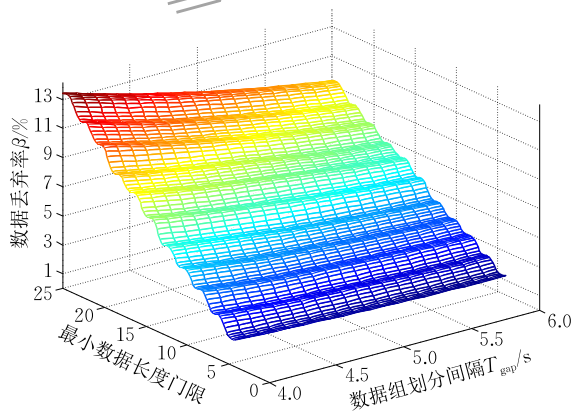
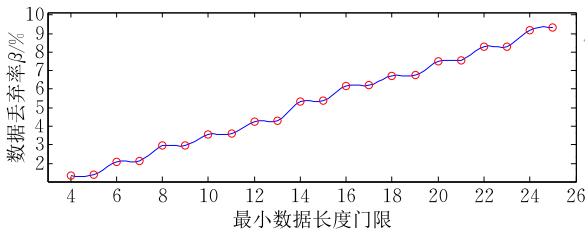


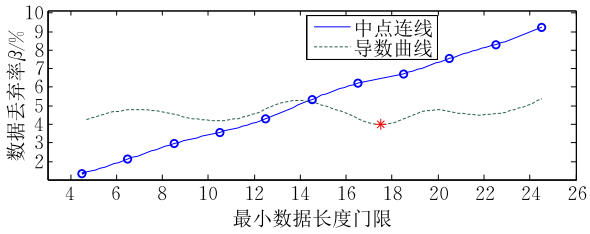
图 7　数据丢弃率受最小长度门限值和数据组划分间隔影响分析

结合上一实验的结论，选取 $T_{gap}=6.0$ s 单独分析最小聚合长度的影响，如图 8 所示，图 8(a)是真实测量数据绘制的曲线，β 呈阶梯上升的趋势. 按照之前的预想，理想的曲线应该呈线性增加的趋势. 但

实际上,这种线性增加的趋势是间隔出现的,奇数长度和偶数长度的数据丢弃率各自呈线性增加,而相邻的长度的数据丢弃率,如 4 和 5,8 和 9 之间是非常相近的,造成这种情况的原因是由于短数据代表了用户偶发的击键行为,这种行为一般击键速度较慢,击键行为完整,即($\eta=0.5$),数据都是一个按键内容对应按键释放的空白数据包,丢弃时成对丢弃.因此,我们求一对数据平均值后,进行插值并绘制了图 8(b),对生成的曲线求导,在理想情况下,数据丢弃率应该随着门限值的提升线性增加,导数为一条水平直线,但是观察导数曲线我们发现导数曲线在 11.5 和 17.5 处出现了低点次低点和最低点,说明用户产生的击键数据在这两个长度下较少.选取这两个值作为最小门限值可以减少丢弃率同时保证符合人类用户的击键习惯,合理的切分数据流.结合 4.1 节的结论:长度低于 20 的数据组是满足安全要求的.综合考虑特征提取的要求,为了最大程度的保证特征稳定,我们选择 18 这个长度值作为最低门限.此时 $minThreshold=18$,长度低于 18 的数据组将会被丢弃,丢弃率 6.20%.



(a) 当$T_{gap}=6.0$s时数据丢弃率受最小数据长度门限值影响曲线



(b) 每对临近点的中点连线及其导数曲线

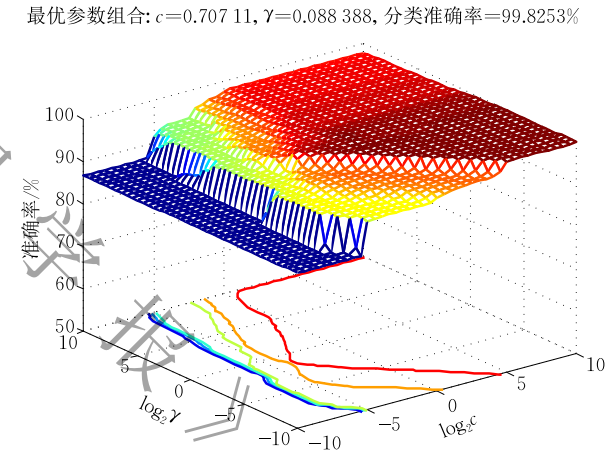
图 8 最小聚合长度影响分析

最大长度门限目的是限制数据组过长,防止反映动态变化水平的特征量失效,影响特征的敏感性.这个参数不会丢弃数据,选择时考虑保证数据的完整性和分析的实时性即可.因此我们设置了 500,800,1000 三个档位,根据实验情况看,分类结果对这三个档位不敏感,分类器都可以很好的适应这一设置,在选择不同最大长度门限时,归一化因子也要随之变化.在满足实时性的要求下,本文在后续实验中,$maxThreshold=1000$.按照上述实验得到的参数,204 233 条数据经过预处理分为了 1145 个数据组,其中正常用户数据 992 组作为正样本标记 1,恶意攻击数据 153 组作为负样本标记为−1.

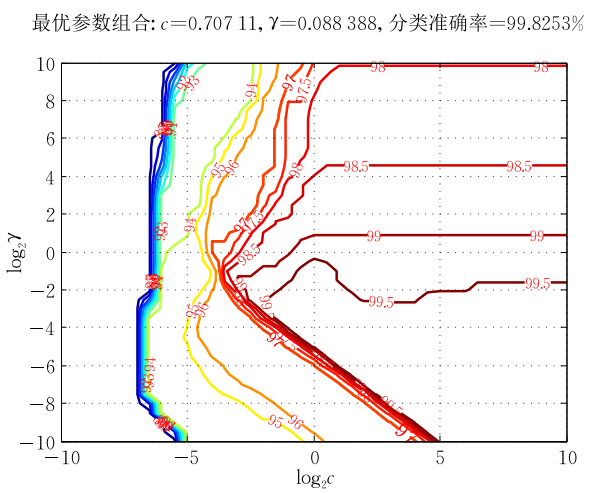
5.2 SVM 分类器优化

根据 SVM 分类器的理论分析,(C,γ)参数组合决定了分类器性能.综合考量数据规模和计算复杂度后本文采用网格搜索法寻找全局最优解,并通过使用指数函数作为步长提高搜索效率,即 $C=2^a$,$\gamma=2^b$[19].在验证模型效果时,采用 K-fold 交叉验证方法,充分利用现有数据集训练模型并进行验证,提高模型的泛化能力和学习准确性.

本实验采用 $K=5$ 的 K-fold 交叉验证算法,经过网格搜索法寻优后的结果如图 9 所示,得到最优参数组合($C=0.70711$,$\gamma=0.088388$),分类准确率达到 99.8253%,攻击识别率 $TNR=98.6928\%$,存在两例漏警,漏警率为 0.1747%,误警率为 0.



(a) SVC参数搜索结果(3D视图)

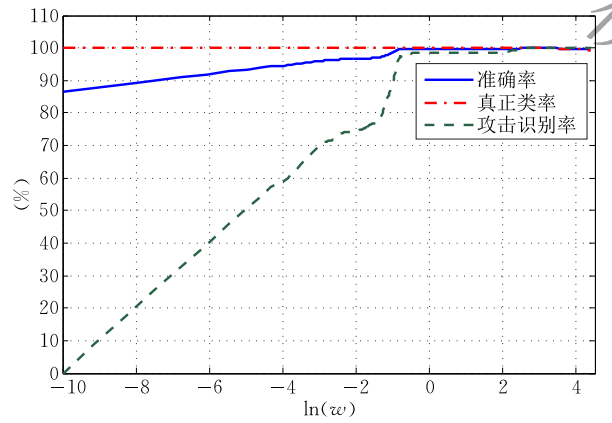


(b) SVC参数搜索结果(等高线图)

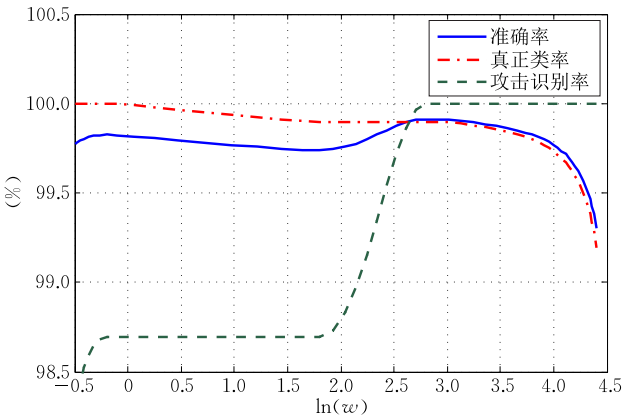
图 9 SVM 参数组全局寻优结果

安全系统在实际应用中，人们更希望能够准确的识别攻击，宁可接受一定的虚警(FP)以确保系统安全. 因此本实验通过改进模型来降低漏报率. 分析可知，正负样本数量不均衡，分类器对负样本学习能力不足是出现漏报的主要原因. 调整惩罚系数 C 可以改进分类器对样本的学习能力. 单独提高分类器对负样本的惩罚系数，可以提高对负样本的学习能力. 因此在负样本惩罚系数上增加权重值 w，此时对于负样本惩罚系数为 $C\times w$，正样本的惩罚系数为 $C\times 1$.

在($C=0.70711$，$\gamma=0.088388$)基础上，寻找最优 w 值，也采用对数步长提高搜索效率，得到图 10，图中横轴为 w 对数轴，图 10(a)是 $\ln(w)$从−10 到 4 得到的搜索结果，为了关注攻击识别率 TNR 在 98%以上的变化趋势，在图 10(b)中放大了这一部分的曲线，$\ln(w)\in[2.8,3.4]$这个范围内攻击识别率 TNR 上升为 100%，整体分类准确率达到了最大值 99.9127%，漏报率为 0，出现一例误报，误报率 0.0873%. 此时模型达到最优，训练结果：$T_{gap}=6.0$ s，$18\leq n\leq 1000$，$C=0.70711$，$\gamma=0.088388$，$w=e^{2.8}$.



(a) 0～100%全视图



(b) 98%～100%局部放大图

图 10　SVM 分类器参数 w 寻优结果

5.3　算法评估

通过上述方法得到了最优分类模型，SVM 分类器选取支持向量 78 个，占整体样本的 6.8122%. 占比很低，表明运算复杂度低，单个样本分类识别速度小于 10 ms. 最终设计好的分类器 ROC 曲线如图 11 所示，特征曲线为本分类器曲线，灰色斜线为随机选择曲线，$AUC\approx 1$，准确率很高，在后续的实际测试中，识别算法也表现出了良好的性能. 采用上述模型，准确判断了 5 位测试者连续 3 天的测试数据和全部的 30 次攻击行为并提供告警，测试分类准确率达到了 100%，算法实时性得到验证，如图 12 所示. 从攻击开始算起，响应速度小于 3.5 s，均在攻击结束前实现告警. 攻击响应时间主要由收集到的数据长度所决定，如果攻击者使用较慢的速度输入，检测时间则会变得较长，但是根据测试算法均可以在攻击完成前判断出输入者的安全属性给出准确告警.

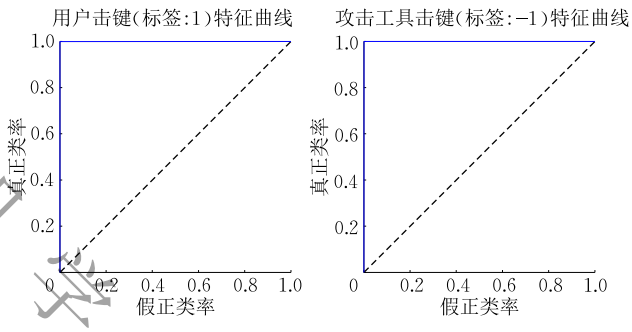


图 11　SVM 分类器 ROC 曲线($AUC\approx 1$)

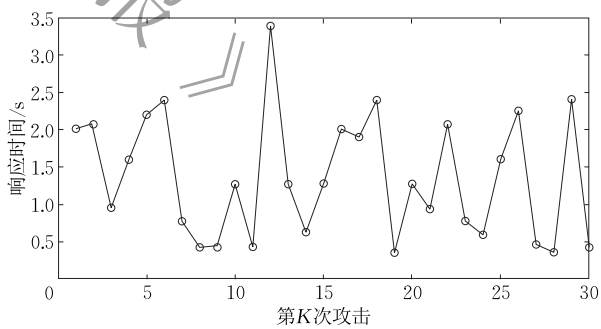


图 12　本算法对 30 次攻击的处理响应时间统计

5.4　与国内外相关研究工作对比

为了说明本算法的优势，横向对比国内外相关研究成果. 在表 2 中，简要罗列对比了近些年来针对恶意 USB 设备防护工作的研究成果. 通过和这些技术对比，评估本算法的性能.

以枚举内容验证技术为代表的 Kang 等人[7]和 Tian 等人[8]的工作使用了嵌入式硬件沙箱和部署蜜罐服务器等手段增强验证效果. 但是他们的核心技术基本一致，都是通过设定一些已知且明显的规

则提示用户可能存在的风险或者干脆交给用户判断设备是否存在风险，如设备枚举时同时申请了 HID 接口和 MSC 接口.但是这种工作还是不能完全防范不断更新的 HID 攻击.首先，这种技术无法准确的判断设备是否存在风险，而是通过向用户发布提示信息，依赖用户决策.用户个人的经验和水平决定了防护的效果，对于伪装程度较好的攻击工具，或者缺乏安全意识的用户都不能达到理想的防护效果.该技术的自动化程度不高，不能实现自主防护；其次，它没有采用主动认证的思想，对设备是一次认证长期授权.恶意设备可以先拿隐藏恶意行为蒙混过关，获取授权后发动攻击；最后，这种技术依赖复杂的外围硬件设备做为沙箱或者分析主机，成本高，不适合个人用户部署.这种技术根本目的在于对 USB 设备功能的分析，并不针对行为.因此，不能够有效的防护现有的恶意 USB 攻击.

Wang 等人[6]使用了 USB 协议加固的技术.这种技术修改了 USB 协议，在协议中添加了签名验证环节，只有获得签名的安全设备才能接入主机.通过排除不安全的接入设备获得相对安全的环境，具有明显的排他性.协议不兼容现有的 USB 设备，因此适用范围很小.对于安全防护等级要求较高的组织内部可以采用这样的方式，不适合全面推广，成本较高.

Barbhuiya 等人[9]提出的击键分析模型相对更具有潜力.通过对输入者击键行为的分析，判断是否具有威胁.但是他们提取的击键行为特点单一，只通过比对固定字母间击键间隔来判别是否相似.这种算法需要事先建立一套模板库保存攻击内容，能够分析匹配的攻击必须和模板库一致才行.虽然他们的研究成果声称识别准确率达到了 100%，但是实际情况并非如此理想.攻击者的输入内容不可能完全按照模板库一样，各种类型的攻击层出不穷，即使是同一种攻击，输入的内容也可能千差万别.所以，该算法在通用性上存在非常大的缺陷.

相比之下，本算法延续了击键特征分析的思路，以主动认证的思想建立了新的检测防护模型.模型提取了更丰富的击键特征，多元特征和新的数据预处理算法大大提高了特征的鲁棒性和准确性，并且使用了 SVM 自动分类器实现了全自动的分析和告警.通过多项优化技术，训练的模型分类准确率达到了 99.9127%.本文采用了更大的数据集和更丰富的测试场景，对攻击者的输入内容和长度没有要求，更符合实际应用场景.通过上述实验也证明了算法的有效性.

表 2 几种检测算法性能对比

	本算法	Tian 等人[8]	Kang 等人[7]	Barbhuiya 等人[9]	Wang 等人[6]
关键技术	击键动力学多元特征；SVM 分类；主动认证	枚举内容验证；蜜罐技术	枚举内容验证	击键动力学特征	加固 USB 协议，增加签名认证
自动化程度	全自动	需要用户决策	需要用户决策	全自动	全自动
实时性	实时授权	静态授权	静态授权	实时授权	实时授权
系统复杂度	低	高	中	低	低
成本	低	高	高	低	很高
通用性	适用所有的 HID 攻击	适用大多数 HID 攻击	适用大多数 HID 攻击	适用特定内容的 HID 攻击	适用与特定设备

6 总 结

USB HID 攻击技术的出现是恶意硬件技术发展的必然结果.在反病毒技术日益成熟的今天，攻击者希望从其他角度突破安全系统的防护，防护相对薄弱的底层硬件成为了攻击者的首选目标.与此同时，可编程的嵌入硬件的快速发展为攻击小型化、集成化提供了基础.由此也暴露出了一个重要的问题，计算机底层硬件缺乏安全防护.一直以来信息安全工作以系统软件为主，长期忽视硬件在此过程中的重要性，导致了现在这种恶意硬件攻击事件爆发式的出现，以至于一时间各种电子设备对这种攻击毫无抵抗能力.

在这样的背景下，有研究者明确指明硬件设备不可信是问题的本质.反思现有的防护机制，主动认证的思想正是解决这个问题的合适的思路.通过直接认证使用者唯一的多维生物特征，包括击键特征、鼠标操作习惯、语言文字特征以及各类行为模式等，为每一位使用者建立唯一的身份特征，利用这些特征实时甄别合法用户和攻击者，解决不可信硬件这样的安全盲点，为安全系统提供了一种可靠实时的认证机制.

本文在这样的思想指导下，对 USB HID 防护

技术进行了深入的研究，分析了 HID 漏洞的原理和成因，设计了一种基于流量监控的实时 HID 攻击检测模型. 相比已有的 HID 攻击检测成果，本算法使用了新颖的设计思想，在复杂的实际场景中可以自动、实时地检测 HID 攻击，在检测的准确率和通用程度上都有了很大的提升. 通过在实际使用中测试，检测算法取得了较好的防护效果，算法识别准确率达到 99.9127%，有效阻止了 BadUSB、Teensy 等 HID 攻击. 而且检测系统可以部署在单机，为个人用户提供有效的隐私防护.

本文的工作还有一些可以提高和改进的地方. 黑客可以通过模拟人类的输入方式，有节奏的敲击键盘，甚至也可以录制人的输入，进行攻击，但是要实现最简单的一次 HID 攻击，至少要输入 20～30 个字符内容，如果要实现复杂的操作，至少需要上百个字符，这样的输入量对于人类的打字速度来说，攻击过程需要很久，也增大了攻击被发现的可能. 毕竟每一次攻击都需要调用输入框，输入攻击脚本，一个黑框弹出，有条不紊地开始输入，用户看到了自然明白发生了什么. 目前本算法对每条新加入的 HID 数据都会计算相应的特征，并且进行识别，这样做的优势在于能够最大限度提高算法的响应时间，但是会带来一定程度的计算资源浪费，很多数据被重复计算，接下来希望通过改进分析窗口，在满足响应时间的前提下实现更高效计算分析. 而且我们希望在未来能够完成检测系统级的开发工作，能够快速的部署在需要防护的设备上提供具有实用价值的防护，或者整合在目前现有的安全平台中，提供 HID 攻击的定向防护.

参　考　文　献

[1] Crenshaw A. Programmable HID USB Keyboard/Mouse Dongle for Pen-Testing. Las Vegas, USA: DEF CON 18, 2010

[2] Nohl K, Lell J. BadUSB—On Accessories That Turn Evil. Las Vegas, USA: Black Hat USA, 2014

[3] Schumilo S, Spenneberg R, Schwartke H. Don't Trust Your USB! How to Find Bugs in USB Device Drivers. Amsterdam, Nederland: BlackHat Europe, 2014: 1-6

[4] Brocker M, Checkoway S. iSeeYou: Disabling the MacBook webcam indicator LED//Proceedings of the Usenix Conference on Security Symposium. Berkeley: USA, 2013: 337-352

[5] Tzokatziou G, Maglaras L, Janicke H, et al. Exploiting SCADA vulnerabilities using a human interface device. International Journal of Advanced Computer Science & Applications, 2015, 6(7): 234-241

[6] Wang Z, Johnson R, Stavrou A. Attestation & Authentication for USB communications//Proceedings of the 6th IEEE International Conference on Software Security and Reliability Companion. Washington, USA, 2012: 43-44

[7] Kang M, Saiedian H. USBWall: A novel security mechanism to protect against maliciously reprogrammed USB devices. Information Security Journal A Global Perspective, 2015, 26(365): 1-20

[8] Tian J, Bates A, Butler K. Defending against malicious USB firmware with GoodUSB//Proceedings of the Computer Security Applications Conference. New York, USA, 2015: 261-270

[9] Barbhuiya F A, Saikia T, Nandi S. An anomaly based approach for HID attack detection using keystroke dynamics. Cyberspace Safety and Security. Berlin, Germany: Springer, 2012: 139-152

[10] Li F, Clarke N, Papadaki M, et al. Active authentication for mobile devices utilising behaviour profiling. International Journal of Information Security, 2014, 13(3): 229-244

[11] Monrose F, Rubin A. Authentication via keystroke dynamics //Proceedings of the ACM Conference on Computer & Communications Security. New York, USA, 1997: 48-56

[12] Ali M L, Monaco J V, Tappert C C, et al. Keystroke biometric systems for user authentication. Journal of Signal Processing Systems, 2017, 86(2-3): 175-190

[13] Vapnik V, Levin E, Cun Y L. Measuring the VC-dimension of a learning machine. Neural Computation, 1994, 6(5): 851-876

[14] Vapnik V. The nature of statistical learning theory// Proceedings of the Conference on Artificial Intelligence. Orlando, USA, 1995: 988-999

[15] Cortes C, Vapnik V. Support-vector networks. Machine Learning, 1995, 20(3): 273-297

[16] Joachims T. Making large-scale SVM learning practical. Technical Reports, 1998, 8(3): 499-526

[17] Andrew A M. An Introduction to Support Vector Machines and Other Kernel-Based Learning Methods by Nello Christianini and Shawe-Taylor. Cambridge, UK: Cambridge University Press, 2000

[18] Platt J C. Fast training of support vector machines using sequential minimal optimization//B. Scholkopf, C. J. C. Burges, A. J. Smola (Eds.) Advances in Kernel Methods. Cambridge, UK: MIT Press, 1998: 185-208

[19] Liu S, Jiang N. SVM parameters optimization algorithm and its application//Proceedings of the IEEE International Conference on Mechatronics and Automation. New York, USA, 2009: 509-513

JIANG Jian-Guo, Ph.D., professor. His research interests include information security and privacy technology.

CHANG Zi-Jing, M. S. His research interests focus on embedded device security.

LV Zhi-Qiang, Ph.D., associate professor. His research interests include signal transceiver and analysis, RF system integration.

ZHANG Ning, M. S. His research interests focus on electromagnetic security.

Background

USB HID attack technology, which this paper mainly researches on, is a novel malicious hardware attack technology. This technology mainly uses HID protocol vulnerabilities to launch attacks, which can simulate the user's key operations. The USB HID attack detection technology has become a new spot of malicious behavior detection. Defense technology against with USB HID attack can be classified into three categories: (1) Expansion and Reinforcement of the USB Protocol. This is extension to the current USB protocol that authenticates the device identity. The USB device used must support this extended USB security protocol, and communication can be established only after the host's signature authentication. (2) USB Enumeration Verification. Some researchers designed dedicated hardware such as hardware sandbox and LAN server to detect unknown USB device enumeration content and notify user. This detection technology relies on the user's judgment and only checks the enumerated content of the device. There is a problem that the automation level is not high, the detection content is single, and the protection capability is not strong. (3) Detection Technology Based on Keystroke Dynamic Feature. This technique uses keystroke dynamics identification algorithm to analyze the difference between the unknown input and the users' input to decide whether to authorize. However, this technology can only recognize what is already in the template library, and it is difficult to ensure exact matches for the ever-changing actual attack content. Currently, the effect of the existing studies are not ideal. So these methods are rare in practical.

We propose detection algorithm based on keystroke dynamics features in this paper. By directly authenticating the user's unique multi-dimensional biological features, including keystroke characteristics, mouse operating habits, language features, and various types of behavior patterns, unique identification features are created for each user, and real-time screening of these features is utilized. The improvement includes a novel data preprocessing method, feature extraction algorithm and applying SVM classification algorithm. Compared to existing technology, it is an entirely protective method which can alarm automatically in real-time with high robustness and high accuracy. It can be deployed on the personal computer at low cost to defend against various HID attacks and protect user's privacy. Although this algorithm individual mechanisms have precedent in the literature, the principle and the synthesis are novel to the best of our knowledge. As the experiment results make clear, the algorithm is pragmatic and surprisingly powerful. It can work well to protect personal privacy in real scenario.

This work is supported by the National Natural Science Foundation of China (Grant No. 61501458).