



综述

人机交互安全攻防综述

葛凯强^{1,2}, 陈铁明^{2,3}

- (1. 浙江工业大学教育科学与技术学院, 浙江 杭州 310023;
2. 浙江省网络空间安全创新研究中心, 浙江 杭州 310023;
3. 浙江工业大学计算机科学与技术学院, 浙江 杭州 310023)

摘要: 随着物联网和人工智能等技术的发展, 人机交互应用也在不断推陈出新。然而, 人机交互技术的发展也伴生新的安全问题, 人机交互安全攻击事件频发。综述分析了 4 种人机交互技术——HID-USB、指纹识别、语音识别和人脸识别的安全攻防现状及攻防效益, 并探讨未来人机交互安全的研究方向, 同时给出了一些建议。

关键词: 人机交互; HID-USB; 指纹识别; 语音识别; 人脸识别; 安全攻防

中图分类号: TP391

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2019196

A survey of attack and defense on human-computer interaction security

GE Kaiqiang^{1,2}, CHEN Tieming^{2,3}

1. College of Education, Zhejiang University of Technology, Hangzhou 310023, China
2. Zhejiang Innovative Research Center on Cyberspace Security, Hangzhou 310023, China
3. College of Computer Science and Technology, Zhejiang University of Technology, Hangzhou 310023, China

Abstract: With the development of technologies such as the internet of things and artificial intelligence, human-computer interaction applications are constantly being introduced. However, the development of human-computer interaction technology is also accompanied by new security issues, and human-computer interaction security attacks frequently occur. The status of four kinds of human-computer interaction technologies: HID-USB, fingerprint recognition, speech recognition and face recognition, as well as the offensive and defensive benefits were reviewed and analyzed, and the research direction of human-computer interaction security in the future was discussed. At the same time, some suggestions were given.

Key words: human-computer interaction, HID-USB, fingerprint recognition, speech recognition, face recognition, safety attack and defense

收稿日期: 2019-04-10; 修回日期: 2019-07-29

基金项目: 国家自然科学基金资助项目 (No.61202282, No.61772026); 国家自然科学基金与浙江省政府联合项目 (No.U1509214)

Foundation Items: The National Natural Science Foundation of China (No.61202282, No.61772026), The Joint Project of National Natural Science Foundation and Zhejiang Provincial Government (No.U1509214)

1 引言

人机交互 (human-computer interaction, HCI) 是计算机、人体工程学、工程心理学、认知学等多学科交叉的领域^[1]。人机交互于 1975 年首次提出,专业的称呼则出现于 1980 年。1983 年,卡德、莫兰和内韦尔^[2]出版《人机交互心理学》一书,自此人机交互的概念迅速普及。随着信息技术的迅速发展,人机交互经历了从最初的按键交互到键鼠交互,再到 20 世纪 90 年代兴起的基于人体生物特征的身份验证等交互,特别是在移动设备兴起之后,指纹识别、人脸识别等技术在移动支付的身份验证方面开始广泛应用。随着人工智能技术的发展,语音识别助手如微软的 Cortana、苹果的 Siri、亚马逊的 Alexa 和国内科大讯飞的灵犀语音助手等,均能与人进行简单的语音交流,通过语音人机交互实现自动搜索天气等智能服务。

人机交互技术的发展在方便人们生活的同时,也引发了骇客、黑产等不法行为。他们利用人机交互系统的漏洞进行攻击,达到破坏或者控制主机的目的,例如键鼠 HID-USB 交互等已被研究发现了数十种攻击方式,而语音识别等先进生物技术也被逐一破解。因此,本文首次聚集人机交互的安全攻防,研究分析了人机交互安全攻防技术现状及发展趋势。

2 人机交互安全威胁

人机交互技术种类众多,包括 HID-USB、指纹识别、语音识别及人脸识别等,这些技术应用面临被破解、被入侵等安全风险。鉴此,本文聚焦人机交互安全,综述了人机交互安全威胁的分类及其攻击方式,重点研究分析了 HID-USB、指纹识别、语音识别、人脸识别等技术。人机交互安全威胁分类如图 1 所示。

2.1 HID-USB 安全攻防

2.1.1 HID-USB 介绍

(1) USB 设备特点

USB 是 1 个总线型数据通路,通过定义不同的接口来制定数据在总线上的传输类型,接口之中又定义了端点,用于数据交换^[3]。操作系统根据不同的接口,将数据传送给对应的程序。数据根据指定的端点进行交换、传输。其中 0 端点是保留的控制端点,所有接口不可使用。每次通信过程由主机发起,通过握手和设备建立通信。通过枚举将接口、端点、USB 设备的识别码等信息通过描述符的形式告诉主机。成功枚举后 USB 设备就可以和主机正常交换数据了。常用的 USB 接口类包括 HID (human interface device) 接口类、CDC 接口类、MSC 接口类等。HID 接口类是一种用于人机交互设备的通信接口,不限于键盘、

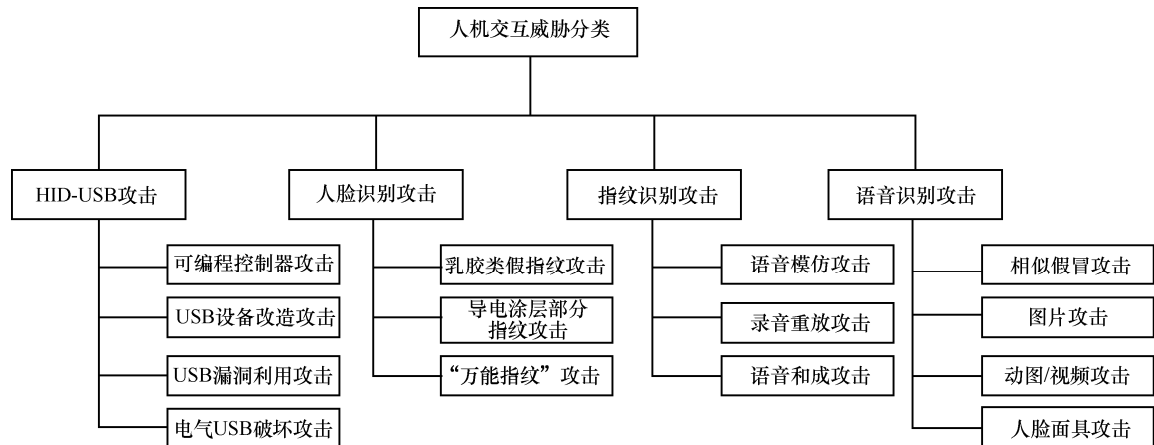


图1 人机交互安全威胁分类



鼠标等设备,任何符合 HID 协议规范的接口都称为 HID 接口。USB 协议规定,同一个 USB 物理接口可以定义多个接口类,此类设备称为复合类 USB 设备,即 HID 接口也可同时定义为 MSC 接口。

(2) HID 接口分析

HID 接口是 USB 设备中运用最广泛的一种接口,如键盘、鼠标等。HID 接口采用报表 (report) 的数据交换方式,可处理任何类别的数据,且通过报表的格式送达对方,设备的固件必须支持 HID 报表的格式。因此,传送的数据可以是键盘的键值、鼠标的位移、滚轮的滚动值,也可以是普通的数据。HID 设备和其他 USB 设备一样需要枚举后才能和主机建立通信。在 USB1.1 协议中定义了设备描述符 (device descriptor)、配置描述符 (configuration descriptor)、接口描述符 (interface descriptor)、端点描述符 (end descriptor) 以及字符串描述符 (string descriptor)。HID 描述符结构关系如图 2 所示。

与 HID 接口相关的描述定义在接口描述符中,接口描述符主要记录了接口的编号、端点数、所使用的类、子类和协议等。通过不同的协议编号区别 HID 接口的不同用途。目前,HID 接口规定在协议字段中有 3 个选项:0 是数据通道 (none),1 是键盘 (keyboard),2 是鼠标 (mouse),并预留了供用户自行定义的 3~55 选项。已定义的 3 个选项都对应操作系统中不同的驱动程序,且在 Windows XP 之后的系统和大多数 Linux 系统下均是免驱动的,由操作系统自行加载驱动,在不同

品牌的硬件中均可正常工作,开发者也只需调用自带的 API 即可和 HID 设备通信。HID 接口也广泛用于低速数据传输、信号控制。

(3) HID 权限问题

USB 设备便捷的背后隐藏着安全隐患,键盘和鼠标 (以下简称键鼠) 在操作系统的设置有问题。操作系统中的 HID 设备最初设计的目的是作为人机交互的接口,键鼠就代表人类。它的每个操作、每组数据都是在用户的允许和操作下发出的,收到数据后,操作系统直接调用驱动程序响应操作。这个过程中缺少校验环节,无条件信任本身就违反了安全设计准则。不做校验就使用这些数据给操作系统带来了很大的安全隐患,相关的安全策略更是直接放行这部分操作,缺少相关限制。虽然 Windows 7 系统引入了权限控制机制,但是来自键鼠的操作依然代表着用户的最高权限。USB 协议并未对这部分设备做出有效的管控,任何 1 个 USB 设备都可以通过枚举成为 HID 设备,并将获得很大的权限自由。比如模拟用户的操作、运行应用程序,这样 1 个普通的 USB 端口就可以完成很多用户操作。目前已知的几种恶意 USB 设备都是通过这种 HID 接口提升权限,模拟计算机管理员的操作,绕过安全策略,获取操作系统权限,运行恶意程序。

2.1.2 HID-USB 类攻击

HID-USB 类攻击经历了从最初的 USB 病毒攻击到当前的 BadUSB、USB 小偷等攻击。根据 Nissim 等人^[4]的研究,将 USB 类攻击分为 4 类:可编程控制器攻击、常见 USB 设备改造的攻击、

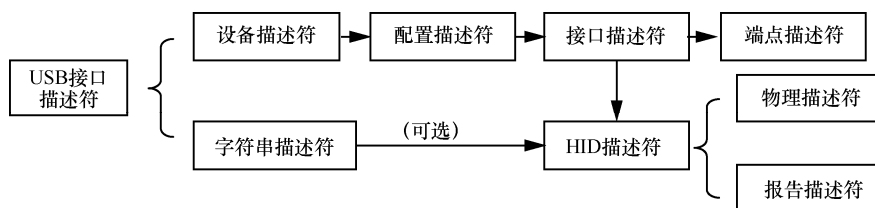


图 2 HID 描述符结构关系

USB 安全漏洞攻击、电气 USB 攻击。

2.1.2.1 可编程控制器攻击

(1) Rubber Ducky (橡皮鸭)

Rubber Ducky 是 2010 年发布的商业击键注入攻击平台。它的硬件包括一个 Atmel 60 MHz 的 32 位处理器、用于加载有效载荷的 micro SD 读卡器、可轻松重新执行有效负载的按钮、LED 指示灯和用于 I/O 的 JTAG 接口。Rubber Ducky 支持一种称为 Ducky Script 的脚本语言,一旦连接到主机,就模拟成一个键盘自动注入一个预加载的按键序列,从而改变系统设置、打开后门、检索数据。

(2) PHUKD/URFUKED

Crenshaw^[5]创建了基于 Teensy 微控制器的结合键鼠仿真的可编程 HID-USB 键盘/鼠标加密狗 (PHUKD)。Mentae^[6]开发的射频版本则称为通用射频 USB 键盘仿真设备 (URFUKED)。攻击者通过连接到主机的 URFUKED,可选择最佳的攻击时间和方法进行远程按键攻击。

(3) USB driveby

由白帽安全研究员 Kamakar^[7]基于 Teensy 开发的 USB 硬件木马。USB driveby 通过 USB 模拟键鼠键入受控命令并控制鼠标操作,实现后门隐蔽安装和覆盖 DNS 设置,以此更改网络设置。

(4) Evilduino

由 Feroz^[8]基于 Arduino 微控制器开发的 USB 硬件木马,与基于 Teensy 的 USB 硬件功能相同。

(5) Unintended USB channel

Clark 等人^[9]在 2010 年开发了一种概念验证 (POC) USB 硬件特洛伊木马程序。他们将一个非预期 USB 通道定义为使用 USB 协议,并以协议未预期的方式进行通信,从而泄露数据。他们基于 USB 标准指定的 4 种传输类型中的两种创建了两个非预期的 USB 通道:控制和同步。Trjan 通过键盘仿真在按下相应的修改键时切换键盘 LED 的控制传输来泄露数据。且还模拟了一个 USB 扬声器,用于音频从主机到扬声器的等时传输,为

数据泄露提供了更高的吞吐量。

(6) TURNIPSCHOOL (COTTONMOUTH-1)

由美国国家安全局 (NSA) 无线安全研究人员 Ossman M、Spill D 和 Busse K^[10]开发的一种隐藏在 USB 线缆内的硬件植入物,作为 NSA Playset 计划的一部分,旨在接入目标电脑后植入恶意程序,通过无线芯片向外发送信息。

(7) 通过 USB 大容量存储进行 RIT 攻击

RIT (read it twice),即进行二次读取。此攻击由 Mulliner 和 Michèle^[11]在 2016 年提出,它基于在大容量存储设备连接到攻击目标时存在一个可检查的使用时间 (TOCTTOU),允许用户提供的大容量存储设备安装应用程序和固件升级,软件的安装不受文件完整性检查的约束,且文件的检查和安装处于不同时间,从而改变文件内容,达到攻击目的。

(8) 攻击无线 USB 加密狗

无线 USB 加密狗也即常用的无线键鼠,是 2015 年由安全研究员 Kamkar^[12]发布的一个名为 KeySweeper (Samy) 的基于北欧射频芯片 (NRF) 的攻击平台。此设备配合软件可以嗅探 2.4 GHz 的无线键鼠发送的数据分组,也可以模仿无线键鼠发送数据分组给无线 USB 加密狗,模拟无线键鼠的击键功能,从而操控计算机。

(9) 覆盖默认网关

2014 年 Nohl 和 Lell^[13]在 SRLabs 实验室通过欺骗 USB 以太网适配器实现了对计算机默认网关的 DHCP 覆盖,该适配器通过 root 之后的 Android 智能手机模拟。由于 Android 带有以太网 USB 仿真功能,通过使用 root 权限就能将手机重新编程为一个 USB 上的以太网适配器 (用于 Internet 共享连接)。手机通过 USB 连接为主机提供默认网关,从而拦截主机的所有流量,计算机因此会遭受 MITM 攻击。也可使用如 badusb 等微控制器重新编程,伪装成 USB 以太网适配器,覆盖主机的 DHCP 设置来劫持本地流量。



2.1.2.2 常见 USB 设备改造的攻击

(1) 基于智能手机的 HID 攻击

2010 年 Wang 和 Stavrou^[14]通过使用恶意 Android 智能手机来模拟键鼠。他们自主开发了一款 USB 驱动小工具,将此 API 添加到 Android Linux 内核中的 USB 接口中,使手机能够模拟 USB 键鼠的功能,最后达到控制主机的效果。也可使用 kali NetHunter, NetHunter 中包含了 USB HID 模式,将 Android 手机的 USB-OTG 线转换为预编程键盘,通过此方式键入用户想让主机执行的命令。

(2) 通过修改 USB 固件覆盖 DNS

根据 Nohl 和 Lel 的实验,恶意 DHCP 服务器通过修改 U 盘的固件并利用其模拟 USB 以太网适配器对主机重新分配 DNS,然后利用其劫持本地流量。

(3) 通过修改 USB 固件模拟键盘

根据 Nohl 和 Lel 的实验修改 U 盘固件,模拟键盘并注入预先定义好的击键序列。

(4) 隐藏分区补丁

Caudill 和 Wilson^[15]将 USB 闪存驱动器重新编程为像普通驱动器一样,将部分设定为隐藏分区。快速格式化驱动器不会删除隐藏分区的数据,使此分区能有效地从主机过滤数据。

(5) 密码保护旁路补丁

Caudill 和 Wilson 通过对 USB 闪存驱动器固件的特定区域的小修改,覆盖闪存指定密码保护分区的用户输入密码,从而将任何输入的密码视为合法密码。

(6) 虚拟机突破攻击

Nohl 和 Lel 研究云实例 VM 的情况,其备份存储通过 USB 连接。机器默认情况下通过对存储设备进行重新编程(假设可以从 VM 访问)以生成连接到主机的第二个设备。Brockner 和 Checkoway 通过重新编程某些版本的 MacBook 和 iMac 内置的 USB 网络摄像头 iSight 的固件,使之

运行后模拟成 USB 键盘,实现虚拟机突破,即可在虚拟机中敲写代码,在主机中运行。

(7) 引导扇区病毒

当前计算机的安全防御几乎在启动操作系统之后,这就给了病毒感染引导扇区的机会。Nohl 和 Lel 研究通过 BadUSB 来部署所谓的引导扇区病毒。通过不同的枚举区分不同的操作系统,并模拟另一个隐藏驱动,里面包含一个主机引导的 rootkit。

(8) iSeeYou

Brockner 和 Checkoway 开发了一款名为 iSeeYou 的 POC 程序,通过 USB 微控制器对 iSight 网络摄像头的固件重新编程,使得摄像头工作时 LED 指示灯不点亮,从而能偷录用户隐私。

2.1.2.3 USB 安全漏洞攻击

(1) .LNK 中 stuxnet / fanny 等 USB 闪存驱动器漏洞

2010 年 6 月,白俄罗斯反病毒公司 VirusBlokAda 发现了来自 USB 闪存驱动器的 Stuxnet 蠕虫病毒^[16]。通过 Windows.LNK 文件的 shell 图标处理程序中的漏洞感染 PC,也即 CVE-2010-2568 漏洞。2014 年卡巴斯基实验室表示,早在 2008 年,Fanny 计算机蠕虫利用此漏洞,通过闪存驱动器上的初始攻击媒介,能不依赖主机上的自动运行功能而执行位于闪存驱动器上的任意 DLL 文件。恶意.LNK 文件可利用自定义图标处理代码中的漏洞执行位于闪存上的恶意代码。

(2) 通过 USB 后门隔空入侵主机

USB 闪存驱动器被攻击者用来建立主机后门,并配合一些漏洞使用。比如 Fanny 使用 FAT16/FAT32 文件系统驱动程序在 USB 记忆棒上创建一个隐藏的存储区域从而感染它。然后此隐藏存储区域包含一个在空气网络上控制 C&C 服务器的命令。它先在未连接 Internet 的计算机上收集信息,保存到隐藏区域,并在计算机连上 Internet

时将信息发送至 C&C 服务器。Fanny 恶意软件能在空气网络中执行命令（利用受感染的 USB 棒），并感染此网络的其他基础设施。

（3）将数据隐藏在 USB 大容量设备中

更改文件属性，通过将其更改为操作系统文件、将文件夹图标和名称设置为透明并隐藏在不可见的文件夹中、伪装成位图或 DLL 文件、设置为备用数据流隐藏到 NTFS 分区等技巧将 U 盘中的文件隐藏。将数据存储在主引导记录、卷引导记录、保留扇区、标记为“坏”或者“使用中”的扇区中，操纵文件系统（如 FAT 文件系统等）元数据，使操作系统不再访问此数据。

（4）自动运行漏洞利用

恶意分子利用 Windows 7 之前的操作系统没有禁用 autorun 自动播放存储设备的漏洞感染计算机。Pod slurping attack 就是基于 autorun 攻击的第一个例子，它由 Abe Usher 创造，将大量敏感文件从主机复制到 USB 存储设备上。但 Windows 7 已经开始禁用此功能，使计算机更加安全。另一个流行的是 hacksaw/switchblade 系列工具，这些工具基于可配置的闪存驱动器（光盘也可），通过只读存储器（CD-ROM）分区进行定制。当连接到主机时，这些闪存驱动器监视主机在连接新的外部驱动器时默认安装恶意程序，并在检测时，压缩、拆分并将存储的所有数据发送到攻击者的电子邮件账户。

（5）冷启动攻击

也称为 RAM 转储攻击，由于大多数 PC 可以从外部 USB 设备启动，Halderman 等人^[17]就为 SYSLINUX 写了一个 10 KB 引导程序插件。通过此插件，将系统 RAM 内容保存到 USB 设备的指定分区中，4 min 就转储了 1 GB 的数据到 USB 存储设备中，并获得了已安装的安全硬盘的完全访问权限。而此攻击也可以恢复出 MAC OS X 用户的登录密码并从 Apache Web 服务器提取 RSA 私钥。

（6）基于缓冲区溢出攻击

计算机驱动程序会自动加载插入的 USB 设备的信息，如 USB 规范、VID、PID 等，而当安装好后无法正确检查到 USB 设备的输入边界时，就很有可能导致缓冲区溢出。当攻击者恶意改变设备的回响给驱动，则可能溢出，并能插入任意代码到计算机中。攻击者在 USB 设备插入计算机时，在枚举期不断发送不同的 VID 和 UID，其中就包含易受攻击的驱动程序，可开启后门。

（7）驱动更新攻击

此攻击需要在 Microsoft 网站提交恶意驱动，并通过审核从而能被合法更新。由于 Microsoft 接受已签名的二进制驱动程序，因此给了驱动者使用某些混淆的恶意代码的机会。USB 设备描述符中唯一的 VID 和 PID 需要注册在恶意程序中，当启用自动驱动程序安装并匹配了该 ID 之后，恶意驱动程序就能被加载。

（8）设备固件升级攻击

设备固件升级（DFU）是 USB 标准支持的一个合法过程，攻击者利用此方式将本地合法固件升级到恶意固件，将其变成一个 BadUSB 设备，进而感染更多计算机设备。

（9）USB 小偷

USB Thief 是 2016 年由 ESET 发现的一种基于 USB 闪存驱动器的数据窃取软件。它以插件或 DLL 的形式通过应用广泛的 Firefox、NotePad++ 等程序进行传播，并在执行应用程序时在后台运行，它专注自我保护及隐身，使计算机很难识别出数据是否被盗。

（10）通过 USB 端口攻击智能手机

攻击者利用电源和数据通过手机的同一个 USB 端口，在充电时利用 USB 数据线非法访问手机数据或者注入恶意代码，造成 Juice Jacking 攻击^[18]。Wang 和 Stavrotu 通过 USB 连接接口发送触摸输入事件来解锁手机。完成之后，更换手机系统映像，从而控制手机里包括内核、应用程序等所有软件。



(11) USBee 攻击

2016 年 Guri 等人^[19]提出 USBee 攻击, 此攻击不修改任何硬件设备及固件代码, 利用 USB 连接器中的数据总线产生的特定频率的电磁波来传输数据。通过计算机上的恶意代码调制 USB 连接器, 从而发射特定频率且可被附近接收器接收的隐蔽通信通道。实验表明, 此攻击的带宽可达 80 byte/s。

2.1.2.4 电气 USB 攻击

USB 杀手是由俄罗斯安全研究人员 Purple^[20]在 2015 年发明的一个 USB 棒, 它能够通过电涌损坏计算机的敏感组件。之后的 USB killer v2.0 设备主要由电容器和转换开关组成。当插到 USB 口上时, 它会自动通过电压转换器将电容充电至 220 V, 然后关闭转换器, 电容放电给 USB 口, 造成计算机硬件损坏。

2.1.3 HID-USB 类攻击防御技术

针对 HID-USB 类攻击方式, 现有以下几种防御措施。

- 对于需要安装驱动的 BadUSB 来说, 可通过监视驱动安装的完整性、合法性及驱动数据的完整性来判别设备的性质。
- 对于重新编程微控制器的 USB 设备, 由于它利用系统赋予 USB 设备中 HID 协议的最高权限, 可在操作系统给 HID 授权时加以强制验证, 使用人机身份校验技术, 如验证码、验证语音等。不但在设备插入时需要验证, 而且在设备运行时还要反复确认, 确保主机安全。
- 对于一些模拟键盘、鼠标、网卡等的攻击设备, 当其插入计算机时, 将它们定义为第二键盘、鼠标和网卡, 在操作人员没有主动使用这些设备时, 计算机应该不允许其自动启用, 这时应该是被禁止的, 只有当第一设备不能正常使用时才询问操作者, 是否需要启用第二设备, 从而避免一

开始就被 USB 设备攻击。

- 对于重新编程控制的 USB 即 BadUSB 和设备模拟攻击, Tian 等人^[21]在 2015 年基于 Linux USB 堆栈提出了 GoodUSB 防御框架, 基于用户对设备功能的预期来强制执行权限。此框架包括一个简易图像界面和用于观察可疑 USB 活动的蜜罐机制, 允许用户对设备功能和设备声明进行比较, 从而鉴别恶意设备。但此框架无法跨平台防护 Windows 系统, 且恶意固件可以利用主机 USB 驱动程序的缓冲区溢出漏洞绕过 GoodUSB。
- 对于特定的模拟键盘的 HID 攻击, 可以使用基于击键动力学的监测方法^[22]。此方法首先在用户机上建立用户的击键习惯文档, 由击键持续时间及按键保持的时间等数据组成, 配置此文件用于过滤需要检测的行为和捕获击键。通过与配置文件的对比检测出是否是用户本人操作。
- 对于 USB 存储设备攻击, 通过更新补丁、更新驱动及固件能大幅降低此类入侵事件的发生概率。对于不明设备需要禁用, 在不得已的情况下, 配合人工验证, 加强防范意识。
- 针对电气 USB 攻击, 可在 USB 接口处安装 USB 集线器/数据电缆。最安全的方法是使用带电涌保护的 USB 接口。

2.1.4 HID-USB 类人机交互攻防效益分析

HID-USB 类人机交互攻防效益分析见表 1。

可编程控制器攻击与常见 USB 设备改造的攻击两种攻击方法的攻防效益相同, 都可通过人机身份校验或击键动力学检测来防御, 但前者防御成本高于后者, 这两种攻击成本较低、成功率高且影响范围大, 将给大众带来一定威胁。USB 安全漏洞攻击主要通过计算机漏洞进行攻击, 可使用较低成本的 U 盘杀毒专家等软件进行防御, 但也需

警惕未知漏洞的攻击。电气 USB 攻击的攻击成本高、影响范围小,但成功率高,可使用 USB 集线器或 USB 数据电缆防止损坏计算机,最有效的方式是使用带电涌保护的 USB 接口,但此防御成本高于前者。

2.2 指纹识别安全攻防

指纹识别技术是众多生物特征识别技术中的一种,随着信息技术的飞速发展,指纹识别技术也取得了进步,并广泛应用于刑侦、考勤、手机身份识别和支付等领域,但指纹识别应用也面临着安全威胁。

2.2.1 指纹识别介绍

2.2.1.1 指纹识别发展历史

人类很早就对指纹产生了兴趣,而具有现代意义的指纹学研究则起源于 Purkinje、Herschel、Faulds、Galton 等人对指纹分类的研究,这些研究逐渐发现指纹适用于个人的身份鉴别^[23]。

1892 年, Galton^[24]出版的《Fingerprints》确定了指纹的两个重要特点:独特性和稳定性。独特性是指,几乎没有两枚指纹的特征是完全相同的;稳定性是指每个人的指纹形态是终身不变的,除非受到严重的伤害或疾病的影响。

1897 年 6 月,英属印度总督签署的一项决议宣布指纹鉴定成为英属印度政府官方鉴定犯罪的手段标准。指纹技术在印度的成功使用激起了其他国家和地区使用指纹系统的兴趣。

1901 年,英国政府决定在 Scotland Yard (苏

格兰场)建立指纹系统。从此,指纹系统在全世界得到了推广,成为一种被广泛接受的身份鉴定手段,并普遍应用于刑事案件的侦查与犯罪鉴定。

1946 年, FBI (美国联邦调查局)手工维护的指纹档案达到 1 亿份;到了 1971 年,达到 2 亿份。1999 年, FBI 决定对非犯罪人员捺印,并保存在计算机系统的自动指纹识别系统中。

在 20 世纪以后,随着指纹档案的急剧增加,对其自动化处理的需求就变得十分强烈。20 世纪 60 年代,美英法等国都开始了指纹自动识别系统 (automatic fingerprint identification system, AFIS) 的研制。到 20 世纪 70 年代,逐渐出现了一些商业化的系统,如著名的 FBI 系统、NEC 系统、De La Rue Printrac 系统等。

我国的指纹自动识别系统研究大约在 20 世纪 80 年代初开始研制,主要用于刑事犯罪调查,如北京大学的 Delta-S 系统、清华大学的 CAFIS 系统等。

“9·11 事件”之后,指纹识别又被广泛用于反恐。我国政府在二代身份证、电子护照等个人身份证件的制作和验证上都采用了指纹识别技术。

2012 年 7 月, FIDO (fast identity online, 快速身份识别在线) 联盟成立,制定有关标准,用生物特征识别技术替代传统密码安全技术。

2013 年,苹果公司推出带有指纹识别技术的 iPhone 5S,通过指纹识别解锁手机和进行移动支

表 1 HID-USB 类人机交互攻防效益分析

HID-USB 类攻击方法	攻击成本	攻击成功率	影响范围	防御方式/防御成本
可编程控制器攻击	较低	高	大	人机身份校验/高击键动力学检测/较低
常见 USB 设备改造的攻击	较低	高	大	人机身份校验/高击键动力学检测/较低
USB 安全漏洞攻击	较低	较低	大	U 盘杀毒专家/较低
电气 USB 攻击	高	高	小	USB 集线器或 USB 数据电缆/低电涌保护的 USB 接口/高



付, 获得了商业上的成功。但 iPhone 5S 的指纹识别 Touch ID 在当年 9 月即被 SRL 项目主管 Ben Schlabs 破解。2014 年 4 月 11 日三星发布了配备指纹识别技术及可支持 PayPal 支付的智能手机 Galaxy S5, 不到一周的时间, 指纹传感器即遭破解。但不管指纹识别是否遭到破解, 在接下来的几年中, 国产手机华为、魅族、小米等都配置了指纹识别传感器。到 2018 年, 指纹识别技术已在移动电子设备上大面积应用。

2.2.1.2 指纹识别技术

依据使用特征的不同, 可以将指纹识别方法分为图像统计法、纹线匹配法、细节特征法、汗孔特征法, 其中主流的方法为细节特征法。

(1) 指纹识别技术分类

由于不同的指纹识别技术的收集方式相异, 可分为光学式指纹模块、电容式指纹模块、射频式指纹模块。

• 光学式指纹模块

利用光线反射成像识别用户指纹。该类型指纹模块对使用环境的温/湿度都有一定要求, 但在识别准确度上效果并不理想, 且占用空间大。

• 电容式指纹模块

利用硅晶元与导电的皮下电解液形成电场。当按压手指时, 指纹的高低起伏将导致二者之间出现不同的压差, 从而测得准确的指纹。该方式适应能力强, 对使用环境无特殊要求。目前, 电容式指纹模块分为划擦式与按压式两种, 前者虽然占用体积较小, 但在识别率及便捷性方面不如后者。

• 射频式指纹模块^[25]

现阶段有无线电波探测与超声波探测两种方式, 原理与声纳类似, 根据特定频率的信号反射来探知指纹的具体形态。具体通过传感器本身发射出的微量射频信号, 穿透手指的表皮层来测量里层的纹路, 获得最佳的指纹图像。这类指纹模块最大的优点是手指无需与指纹模块接触。

(2) 指纹识别流程

指纹识别的工作流程大致分为“指纹采集→指纹评估→特征提取→指纹存储→再次按压指纹→指纹比对→完成验证”这 7 个步骤, 在“特征提取”中又有“图像预处理→指纹图像增强→二值化→细化→提取特征点”这 5 个步骤。

步骤 1 指纹采集: 以智能手机按压式为例, 通过手指按压在指纹识别模块上实现数据采集, 由于按压式指纹采集面积较小, 需要通过多次采集, 拼凑出一块完整的指纹图案, 并通过软件算法来保障识别的精度。

步骤 2 指纹评估: 通过对采集的指纹质量进行评估, 若不合格则需要重新采集, 若合格就进入步骤 3。

步骤 3 特征提取: 经过处理后会依次得到预处理图、增强图、二值图、细化图, 最后进行特征点提取。

步骤 4 指纹存储: 在提取特征点之后, 将指纹数据存储到指纹存储芯片中。

步骤 5 再次输入指纹: 使用指纹应用时需要再次按压指纹识别模块。

步骤 6 指纹比对: 录入指纹后, 将采集到的指纹与指纹存储芯片中的数据进行比对, 若在阈值之下则通过, 否则需要重新输入正确的指纹。

步骤 7 完成验证: 指纹验证通过。

2.2.2 指纹识别攻击

指纹识别技术已在生产生活中特别是智能手机解锁和移动支付上大规模应用。当前指纹识别系统也已被研究员和黑客成功攻击, 安全人员需要做好指纹识别安全防御研究。现有以下 3 种攻击方式。

(1) 使用乳胶等材料制作假指纹攻击

首先, 通过如胶带提取、烟雾显影法、摄影术等获取指纹信息; 然后, 分析指纹信息并数字化; 最后, 使用日常的材料如凝胶、乳胶漆、黏土等制作成指纹膜或者假指纹。通过此方法制作

的假指纹可以直接骗过光学传感器,如在此基础上再加上导电特性,就能骗过电容传感器。假指纹制作经过不断改进,从最初的普通硅胶、凝胶到现在的导电硅胶、带导电涂料的凝胶等。

(2) 使用透明胶带加导电涂层更新指纹信息

由于指纹识别每次输入的指纹和保存着的指纹信息有部分是不同的,当在一个阈值内相同时,指纹识别就通过,并会“记住”这个新验证的指纹。基于此原理,将携带导电涂料的透明胶带贴在指纹识别模块上,当多次使用指纹识别功能后,指纹识别模块就会“记住”这一半真实一半假冒的指纹。当使用其他手指解锁手机时,由于导电涂料形成的一半指纹比对通过,所以在此阈值下,也通过了指纹识别模块的验证。使用其他手指甚至橘子皮时也能通过验证^[26]。

(3) 基于相同特征制作的“万能指纹”

由于移动智能设备上的指纹识别系统模块较小,一次不能完全覆盖整个手指的指纹,就需要通过多次拼接存储这些部分指纹。这些碎片化的指纹出现匹配错误的几率将会大大提高。纽约大学和密歇根大学的研究员研究出一种“万能指纹”,解锁率可达到65%。这个“万能指纹”通过在不同指纹中找出相同特征点来制作,一般手机有5次开锁机会,可使用5个不同的指纹进行解锁,成功率就会上升。

2.2.3 指纹识别安全防御

指纹识别攻击技术的出现和不断升级,使得指纹识别安全防御变得愈发重要,可通过指纹识别安全软硬件来防御指纹识别攻击。

(1) 超声波指纹识别技术^[27]

超声波识别可通过3D扫描技术扫描指纹,穿过手指表皮,分析出手指汗水、凝露和食物油脂等信息,使第一、二种假指纹不能验证成功。

(2) 安全芯片

为设备提供可信的硬件平台和安全载体,能有效解决目前指纹识别中主要存在的指纹信息导

出、明文传输、能否提供安全的软件系统运行环境、没有身份认证/识别等安全风险。大唐微电子技术有限公司结合自身优势,自主完成了高性能指纹算法处理芯片^[28]DMT-FAC-CG4Q的研发,该芯片支持国密加解密协处理器,为指纹识别的安全可控提供了硬件基础。

(3) “活体检测技术”^[29]

活体指纹识别与非活体指纹识别的最大不同在于,活体指纹识别针对手指的真皮层,能有效杜绝“假指纹”。

(4) 指静脉技术^[30]

指静脉是通过对手指发射近红外线,静脉产生反射,形成静脉纹路图像,从而提取特征的一种方法。由于是识别真实手指的静脉特征,所以安全性高。

2.2.4 指纹识别类人机交互攻防效益分析

指纹识别类人机交互攻防效益分析见表2,假指纹的攻击方法的成本高,需要获取受害者的高精度指纹来制作,且还需获得受害者的手机,但攻击成功率高,影响范围很小,局限性大;透明胶带加导电涂层的破解成本最低,但使用难度大,攻击成功率低,影响范围小;“万能指纹”的破解成本中等,且无需受害者配合,通过提取大众指纹并制作5个不同特征的“万能指纹”即可破解,此方法破解成功率高,影响范围大。以上3种攻击方式都可通过超声波识别、活体检测或者安全芯片等进行防御,但成本高。

2.3 语音识别安全攻防

语音是人类最自然的交互方式。在计算机发明之后,让机器能够“听懂”人类的语言,理解其中的意义,并作出正确的回应成了人们追求的目标,并发展为一门综合人类智能等各项研究的独立学科。

近几年,随着深度神经网络^[31]、大数据和云计算的使用,语音识别技术取得了突飞猛进的发展,语音识别产品进入了人们的日常生活,主要



表2 指纹识别类人机交互攻防效益分析

指纹识别攻击方法	攻击成本	攻击成功率	影响范围	防御方式/防御成本
假指纹	高	高	小	超声波识别/高活体检测/较高安全芯片/高
透明胶带加导电涂层	低	低	小	超声波识别/高活体检测/较高安全芯片/高
“万能指纹”	中	高	大	超声波识别/高活体检测/较高安全芯片/高

包括苹果的 Siri、亚马逊的 Alexa、科大讯飞语音输入法等。语音技术在方便人们生产生活的同时，也面临着严峻的威胁。

2.3.1 语音识别介绍

(1) 语音识别的发展历史

语音识别技术始于 20 世纪 50 年代的 Bell 实验室，他们实现了第一个可以识别 10 个英文数字的语音识别系统——Audry 系统。

20 世纪 60 年代，语音识别研究取得了实质性的进展，出现了动态规划（DP）和线性预测分析技术（LP），较好地解决了语音信号的产生和不等长的问题。

20 世纪 70 年代，提出了动态时间规正技术（DTW），对特定人孤立词语音识别特别有效。期间又出现了矢量量化（VQ）和隐马尔可夫模型（HMM）理论。

20 世纪 80 年代，研究的重点逐渐转向大词汇量、非特定人连续语音识别。随着对语音识别研究的进一步深入，基于 HMM/VQ、HMM/高斯混合模型、HMM/人工神经网络等技术的语音建模方法开始广泛应用于大词汇量连续语音识别（LVCSR）系统，语音识别技术取得了新的突破。

20 世纪 90 年代后，人们进一步研究语音识别与自然语言处理技术的结合，HMM-ANN 的语音识别算法取得了显著进展，进一步提高了语音识别的稳健性和准确性。

国内的语音识别研究起始于 20 世纪 50 年代，

但直到 20 世纪 80 年代后，随着计算机技术在国内的逐渐普及和应用，国内的许多单位才具备了研究语音技术的基本条件。在“863”计划的支持下，中国的语音识别技术进入了一个前所未有的发展阶段。

(2) 语音识别原理

语音识别系统是模式识别的一种，主要包括特征提取、模式匹配、参考模式库 3 个基本单元，系统原理如图 3 所示。

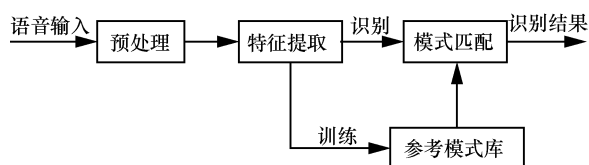


图3 语音识别系统原理

首先麦克风接收到语音信号，并转换为电信号，作为语音识别系统的输入端。然后进行预处理，再根据个人语音特点建立声学模型和语言模型，并从电信号中提取出所需特征，建立语音识别所需模板，并在此基础上形成参考模式库，里面存储语音特征模型。之后再输入一段语音，将提取的语音特征在参考模式库中进行模式匹配，得出识别结果。这种特征提取、语音模型和参考模式库的好坏与能否较好识别出语音有很大关系。

2.3.2 语音识别攻击

语音识别技术在不断发展的同时，作为一种安全身份认证手段，由于语音识别算法目前技术

水平有限,所以面临着诸多风险。下面将由简到难列出语音识别的攻击方法。

(1) 语音模仿攻击

在语音识别的初级阶段,由于识别算法简单,可通过两个相似声音的人,让其中一个人攻击另一个人的语音识别设备。

(2) 录音重放攻击

攻击者通过记录受害者的语音并在登录受害者设备时候播录音,通过验证。

(3) 特定人语音合成或声音转换攻击^[32]

攻击者使用深度学习等算法,将受害人的语音进行建模,提取出受害人的语音特征,将特定文字与受害人语音的特征相结合,合成受害人的语音,再进行播放攻击。在深度学习流行之前,传统的机器学习在语音合成上的真实度还较低,但近几年 Google 的 WavNet、Adobe Project VoCo 等技术的发展,极大地提升了语音合成的真实度,对语音识别系统造成了严重威胁。

2.3.3 语音识别安全防护

下面是对以上攻击方法的一些防御措施。

(1) 语音模仿攻击

提高语音识别算法提取特征的细粒度,从细微差别上分辨出不同人的语音特征;使用声纹识别系统区分声纹特征。

(2) 录音重放攻击

活体检测能有效检测出是否受到录音重放攻击;随机语音验证在语音识别时,提示用户朗读一段随机显示的内容,确保是合法用户;国内基于 MFCC 的重录语音检测算法可判别录

音重放^[33];基于信道噪声的录音回放攻击检测技术^[34]通过提取原始语音系统、偷录设备及回放设备的信道模式噪声来检测,从而确定是否被录音重放攻击。

(3) 语音合成攻击

提高特征提取的细粒度,并配上活体检测和随机语音验证等组合手段来防范语音合成攻击;可使用 PAL^[35]在研究中发现的 GMM-SVM SV 系统。

2.3.4 语音识别类人机交互攻防效益分析

语音识别类人机交互效益分析见表3,语音模仿的攻击成本低且相应的攻击成功率也不高,影响范围小,只能在语音相似的人之间使用,提高语音识别算法精度就能抵御此种攻击;录音重放攻击成功率比语音模仿稍高,使用录音设备重放受害者语音对其语音设备进行攻击,不过此方法影响范围小,可通过增加活体检测手段或者随意语音验证来抵御此种攻击,但防御成本较高;语音合成攻击成本最高,需要有较强的专业技能,攻击成功率高,此种攻击的影响范围小,可采用更高级的算法、随机语音验证和活体检测等组合防御,也可采用 GMM-SVM SV 系统,但两者防御成本较高。

2.4 人脸识别安全攻防

2.4.1 人脸识别介绍

人脸识别是图像处理技术的重要应用之一,是人类在开发自身生物特征过程中的又一次伟大尝试。人脸识别主要利用计算机提取个人特征信息,并比对数据库中是否存在此特征,从而识别出人脸

表3 语音识别类人机交互效益分析

语音识别攻击方法	攻击成本	攻击成功率	影响范围	防御方式/防御成本
语音模仿	低	低	小	提高算法细粒度/低
录音重放	低	较高	小	活体检测或随机语音验证/较高 基于 MFCC 的重录语音检测算法/较高
语音合成	高	高	小	算法、活体检测和随机语音验证/较高 GMM-SVM SV 系统/较高



对象的身份。目前,该技术已经融入了人们的日常生活,如刑事侦查、身份验证、门禁安全等。

人脸识别技术的发展大致可以分为以下 3 个阶段。

(1) 第一阶段

20 世纪 60—70 年代,人脸识别属于初级阶段,Bledsoe^[36]作为最早的科研人员,首次利用人脸各部分比例特征作为参数,建立了一个人脸识别的雏形。

(2) 第二阶段

20 世纪 90 年代初,随着计算机软硬件的不断升级、信息技术的进步,人脸的整体识别成为研究的重点。主要研究方向为弹性图匹配方法、灰度处理、形状分离及人脸可变模型方法等。

(3) 第三阶段

20 世纪 90 年代末,人脸识别的商用逐渐成为全球的研究热点。但由于技术尚不成熟,也存在着相当大的缺陷,直至今日还在不断发展。

我国人脸识别技术研究始于 20 世纪 90 年代中国科学院与哈尔滨工业大学成立的联合实验室。2017 年,江苏的“人脸识别”厕所机、北京的“人脸识别”门禁系统等技术应用的新闻屡见不鲜。但随着人脸识别大范围的应用,它的安全问题得到各方的关注。

2.4.2 人脸识别攻击

安全研究员及黑客都重点研究人脸识别的攻击技术。当前已知以下 4 种攻击方式。

(1) 假冒攻击

此攻击方法利用两个极其相似的人特别是双胞胎,通过“刷脸”破解另一个人的人脸识别系统。人脸识别算法在一定阈值内会将攻击者识别成合法用户,从而通过人脸识别认证。

(2) 图片攻击

通过打印受害者照片或使用手机照片进行攻击,由于照片真实有效,一些没有活体检测技术的人脸识别系统能通过验证。

(3) 动图或视频攻击

通过 PS 技术将单张照片制作成 gif 动图或使用视频等做出系统认证所要求的摇头、张嘴、眨眼等动作,从而顺利通过活体检测及人脸识别系统的验证。

(4) 人脸面具攻击

通过戴上假脸伪装成受害者“骗”过人脸识别系统达到攻击目的。越南一家安全公司用类似石膏的材质进行 3D 面具打印,并用 3D 面具破解了 Face ID 的人脸识别系统。

2.4.3 人脸识别安全防护

上述几种人脸识别攻击的方法使用了仿冒、伪造等方法。针对这些攻击方法,有以下 6 种应对方法。

(1) 提升算法性能和使用语音识别

针对假冒攻击,由于攻击者与受害者长相相似,可采用小波变换及双字典协作稀疏表示分类的人脸识别方法^[37]有效识别人脸。也可增加语音识别的二次认证,提高系统安全性。

(2) 活体检测技术

可以添加活体检测的技术,辅助点头、摇头等动作,确保图片、视频等无法通过验证。也可结合场景分析技术,针对特定场景确定是否检测到纸张、屏幕的特征信息,确保活体检测的效果,从而保障验证安全。

(3) 手机短信的二次认证

增加手机短信的二次认证将提高安全性。

(4) 随机活体动作认证

针对攻击者使用动图或视频来攻击人脸识别系统,单一的点头、摇头等活体检测已不能满足要求,可使用随机的连续动作进行认证,使攻击者的动图或视频录像不符合动作要求,无法通过认证。

(5) 红外活体检测技术

红外光比可见光有更强的特性,由于红外光照射在真实人脸、纸张、屏幕、普通面具、3D 打印面具等的反射特性、红外成像十分不同,通过

分析特性能有效防范人脸面具攻击。

(6) 唇语分析^[38]

人脸识别中增加语音识别并结合图像唇语分析即读唇,能够检验声音源和图像源的同步性,能够有效抵挡动态图片及视频重放攻击,保证系统安全。

2.4.4 人脸识别类人机交互攻防效益分析

人脸识别类人机交互攻防效益分析见表4,4种攻击方法的影响范围相同,虽然人脸面具攻击成本最高,但成功率也高,需使用防御成本最高的红外活体检测技术进行防御。相似假冒攻击和图片攻击的成本最低,但后者的成功率高于前者,使用的防御技术也不同。动图或视频攻击的成本适中,攻击成功率和防御成本都较高,需使用活体检测或唇语分析技术。

3 人机交互安全展望

上述人机交互技术包括键鼠交互和生物特征交互,生物特征交互中还存在诸如虹膜识别^[39]、视网膜识别、掌纹识别、掌静脉识别、步态识别^[40]等交互技术。这些生物特征技术可用于个人身份验证。但人机交互技术面临着严峻的威胁。最后,本文结合技术发展趋势从以下4个方面给出一些建议。

3.1 脑机智能与人机交互安全

近些年大力研究的脑机交互技术^[41]将交互技术带到新的高度,未来人们能通过“意念”控制机器。但存在安全风险,如果攻击者能够获取受

害者的脑机交互身份信息或者脑电特征信号,就能模仿受害者并入侵脑机交互系统,控制主机。甚至,攻击者在受害者的脑机交互系统中留下病毒,等受害者再次使用时,将面临风险甚至人身安全。

研究人员应在脑机交互应用之前就开始研究防范措施,可从以下3点展开:从协议、功能、策略上规避风险,建立健全身份认证体系;使用人工智能系统确保个人脑电信号不被恶意修改;建立个人脑电信号特征库以阻止恶意脑电信号的传播交流,保障人与系统的双向安全。

3.2 虚拟现实与人机交互安全

近两年,虚拟现实技术^[42]站上风口,产业发展欣欣向荣。但产品目前还处于初级阶段,没有一套完善的安全保障机制,所以必须先解决虚拟现实的人机交互安全问题,使其得到安全保障。

本文将探讨可能面临的一些问题:当医生对有心理问题的病人进行治疗时,患者的头盔设备突然给他发送一段恐怖血腥的画面;建筑设计师在3D建模时,被人偷偷修改了参数;当用户使用虚拟现实设备上网时,被不法分子窃取了个人数据。鉴于此,本文提出两点建议:需要虚拟现实产品的厂商根据产品的协议、模式和流程做好网络数据和隐私的保护;建立健全虚拟交互安全保障框架,确保在特定场景运行特定程序,可运用人工智能算法对异常数据、行为进行监控、拦截。

3.3 人工智能与人机交互安全

近些年,随着深度学习技术的突破,人工智

表4 人脸识别类人机交互攻防效益分析

人脸识别攻击方法	攻击成本	攻击成功率	影响范围	防御方式/防御成本
相似假冒攻击	低	低	小	提高算法精度/低
图片攻击	低	较高	小	活体检测技术/较高 人脸与场景分析技术/较高
动图或视频攻击	较高	较高	小	活体检测技术/较高 唇语分析/较高 随机活体动作认证/低
人脸面具攻击	高	高	小	红外活体检测技术/高



能作为一项高赋能的技术,为产业发展提供新机遇的同时,也带来了安全问题。可分为两部分:内部和外部。内部由于现今人工智能技术尚不成熟,且存在自身缺陷,在进行深度学习或机器识别时,很可能发生意外情况;外部由于黑客对人工智能系统的攻击,特别是运用对抗神经网络,使人工智能系统发生错误,且也有大量学者对人工智能伦理深感担忧。由于人工智能的发展离不开数据的支撑,也将面临大量隐私数据泄露的风险。黑客通过深度学习学习出一些反社会反人类的言论交互系统,入侵城市大脑,造成数据泄露,甚至破坏智能交通系统,引发交通事故。

对于人工智能安全问题,本文提出6点建议:限定人工智能的使用场景及功能,将人工智能分门别类,做专一的任务,并设置权限;建立数据保障体系,限制人工智能对数据的采集、使用和传播;建立健全人工智能安全保障体系,对智慧城市的人工智能设置多层保障体系;完善人工智能伦理规范和人工智能技术研发规范;推行人工智能产品安全认证;通过研究对抗神经网络完善人工智能算法。

3.4 人机物融合的交互安全

随着5G^[43]的到来、人工智能技术的不断发展和物联网的大规模应用,今后将会是一个人机物三元融合^[44]发展的更加智能、便捷的时代。智慧制造、智慧小区、智慧城市^[45]等的不断涌现,必将面临人机物融合交互的安全问题。黑客恶意篡改物联网设备采集到的数据,使其做出错误决策;黑客恶意操作工业机器人,造成人员及设备的损害;在智慧小区中,黑客伪造住户信息与门禁进行人机交互,入侵智能家居,使智能家电过负荷运行导致火灾等恶性事件;在智慧城市中,黑客攻击车联网、智慧交通等设备,导致交通事故,攻击电网、水厂等引发城市瘫痪。

人机物的融合发展带来的交互安全必将影响人们的生活,必须在应用发展中同时发展相应安

全措施:建立健全多级安全保障体系,体系可以从不同领域、不同等级划分,以城市为第一级,以智慧物流、智慧制造工厂、智慧电网、智慧水厂等为第二级,以具体事务、设备为第三级,通过定制化安全框架的部署有效保障人机物的交互安全。建立智能设备、程序的严格审查及规范制度,限定设备功能,控制其行为。通过大数据分析技术^[46]建立集群事件分析机制,当大批物联网设备同时访问某个网站或设备时,可能出现DDoS攻击^[47],进行智能预警及智能保障。

4 结束语

人机交互技术不断推陈出新,也不断产生全新的攻击方式。从最初的USB攻击,到当前的语音攻击、指纹破解等,不断推动人机交互安全防护技术的发展。因此,人机交互是一把便利性与安全性共存的双刃剑。目前,快速发展的人工智能、虚拟现实等技术,将加速人类进入脑机交互和人机物融合的智慧生活,但同时智慧生活也可使人民面临更加严峻、威胁更大的安全问题,人机交互安全或将引起更广泛的关注。

参考文献:

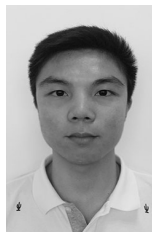
- [1] 赵永惠. 人机交互研究综述[J]. 信息与电脑(理论版), 2017(23): 24-25, 28.
ZHAO Y H. Survey of human-computer interaction research[J]. China Computer & Communication, 2017(23): 24-25, 28.
- [2] CARD S, MORAN T P, NEWELL A. The psychology of human-computer interaction[M]. Hillsdale: Lawrence Erlbaum Associates, Inc. 1983.
- [3] 吕志强, 薛亚楠, 张宁, 等. 恶意USB设备安全技术研究综述[J]. 信息安全研究, 2018, 4(7): 639-645.
LV Z Q, XUE Y N, ZHANG N, et al. Research on USB-HID device security[J]. Journal of Information Security Research, 2018, 4(7): 639-645.
- [4] NISSIM N, YAHALOM R, ELOVICI Y. USB-based attacks[J]. Computers & Security, 2017(70): 675-688.
- [5] CRENSHAW A. Programmable HID USB keystroke dongle: using the Teensy as a pen testing device[EB]. 2010.
- [6] MONTA E. URFUKED[EB]. 2010.
- [7] KAMKAR S. USBdriveby[EB]. 2014.

- [8] FERROZ R. Evilduino!-USB hack tool[EB]. 2015.
- [9] CLARK J, LEBLANC S, KNIGHT S. Compromise through USB-based hardware trojan horse device[J]. *Future Generation Computer Systems*, 2011, 27(5): 555-563.
- [10] NSA Playset. TURNIPSCHOOL[EB]. 2016.
- [11] MULLINER C, MICHÉLE B. Read it twice! A mass-storage-based TOCTTOU attack[C]//The 6th USENIX Conference on Offensive Technologies, August 6-7, 2012, Bellevue, WA, USA. New York: ACM Press, 2012: 105-112.
- [12] Samy. KeySweeper[EB]. 2015.
- [13] SRLab[EB]. 2014.
- [14] WANG Z, STAVROU A. Exploiting smart-phone usb connectivity for fun and profit[C]//The 26th Annual Computer Security Applications Conference, December 6-10, 2010, Austin, Texas, USA. New York: ACM Press, 2010: 357-366.
- [15] CAUDILL A, WILSON B. Making BadUSB work for you[EB]. 2014.
- [16] LANGNER R. Stuxnet: dissecting a cyberwarfare weapon[J]. *IEEE Security & Privacy*, 2011, 9(3): 49-51.
- [17] HALDERMAN J A, SCHOEN S D, HENINGER N, et al. Lest we remember: cold-boot attacks on encryption keys[J]. *Communications of the ACM*, 2009, 52(5): 91-98.
- [18] Wikipedia. Juice jacking[EB]. 2018.
- [19] GURI M, MONITZ M, ELOVICI Y. USBee: air-gap covert-channel via electromagnetic emission from USB[C]//2016 14th Annual Conference on Privacy, Security and Trust (PST), Dec 12-14, 2016, Auckland, New Zealand. Piscataway: IEEE Press, 2016: 264-268.
- [20] USB killer v2.0[EB]. 2015.
- [21] TIAN D J, BATES A, BUTLER K. Defending against malicious USB firmware with GoodUSB[C]//The 31st Annual Computer Security Applications Conference, December 7-11, 2015, Los Angeles, CA, USA. New York: ACM Press, 2015: 261-270.
- [22] BARBHUIYA F A, SAIKIA T, NANDI S. An anomaly based approach for HID attack detection using keystroke dynamics[M]//Cyberspace Safety and Security. Berlin: Springer, 2012: 139-152.
- [23] 王曙光. 指纹识别技术综述[J]. *信息安全研究*, 2016, 2(4): 343-355.
WANG S G. A survey of fingerprint recognition technology[J]. *Journal of Information Security Research*, 2016, 2(4): 343-355.
- [24] GALTON F. Fingerprints[M]. London: Macmillan, 1892.
- [25] 顾陈磊, 刘宇航, 聂泽东, 等. 指纹识别技术发展现状[J]. *中国生物医学工程学报*, 2017, 36(4): 470-482.
GU C L, LIU Y H, NIE Z D, et al. A review of fingerprint recognition technology[J]. *Chinese Journal of Biomedical Engineering*, 2017, 36(4): 470-482.
- [26] 温婧. 橘子皮能解指纹识别锁?专家:不要给手机贴指纹贴[J]. *广西质量监督导报*, 2018(2): 14-15.
WEN J. Orange peel can solve the fingerprint identification lock? Expert: do not give the mobile phone a fingerprint sticker[J]. *Guangxi Quality Supervision Guide Periodical*, 2018(2): 14-15.
- [27] 超声波指纹传感器将大体提升指纹传感器安全系数[J]. *电子世界*, 2015(13): 21.
Ultrasonic fingerprint sensor will greatly improve the safety factor of fingerprint sensor[J]. *Electronics World*, 2015(13): 21.
- [28] 范丽芳. 芯片安全防护技术助力指纹识别系统安全[J]. *电子产品世界*, 2017, 24(1): 72-73, 36.
FAN L F. Chip security technology guarantees the security of fingerprint identification system[J]. *Outlook of Electronic Technology*, 2017, 24(1): 72-73, 36.
- [29] 王群峰. 指纹识别系统活体检测技术研究[D]. 广州: 广东工业大学, 2016.
WANG Q F. Research on liveness detection technique in fingerprint identification system[D]. Guangzhou: Guangdong University of Technology, 2016.
- [30] 叶文炜, 何丽鹏, 林峰. 指纹静脉多模识别光学系统的设计[J]. *激光与光电子学进展*, 2018, 55(9): 370-376.
YE W W, HE L P, LIN F. Design of optical system for multi-mode recognition based on fingerprint and veins[J]. *Laser & Optoelectronics Progress*, 2018, 55(9): 370-376.
- [31] SCHLÜTER R, DOETSCH P, GOLIK P, et al. Automatic speech recognition based on neural networks[M]. Berlin: Springer, 2016: 3-17.
- [32] CARLINI N, WAGNER D. Audio adversarial examples: targeted attacks on speech-to-text[J]. *arXiv: 1801.01944*, 2018.
- [33] 李山路, 王泳, 甘俊英. 重录语音检测算法[J]. *信号处理*, 2017, 33(1): 95-101.
LI S L, WANG Y, GAN J Y. An algorithm of speech recapture detection[J]. *Journal of Signal Processing*, 2017, 33(1): 95-101.
- [34] 王志锋, 贺前华, 张雪源, 等. 基于信道模式噪声的录音回放攻击检测[J]. *华南理工大学学报(自然科学版)*, 2011, 39(10): 7-12.
WANG Z F, HE Q H, ZHANG X Y, et al. Playback attack detection based on channel pattern noise[J]. *Journal of South China University of Technology(Natural Science Edition)*, 2011, 39(10): 7-12.
- [35] PAL M, SAHA G. On robustness of speech based biometric systems against voice conversion attack[J]. *Applied Soft Computing*, 2015(30): 214-228.
- [36] 苏楠, 吴冰, 徐伟, 等. 人脸识别综合技术的发展[J]. *信息安全研究*, 2016, 2(1): 33-39.
SU N, WU B, XU W, et al. The Comprehensive Technology Development of Face Recognition[J]. *Journal of Information Security Research*, 2016, 2(1): 33-39.
- [37] 龚飞, 金炜, 朱珂晴, 等. 采用双字典协作稀疏表示的光照及表情稳健人脸识别[J]. *电信科学*, 2017, 33(3): 52-58.
GONG F, JIN W, ZHU K Q, et al. Illumination and expression robust face recognition using collaboration of double-diction-

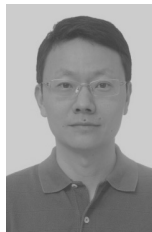


- ary's sparse representation-based classification[J]. Telecommunications Science, 2017, 33(3): 52-58.
- [38] RONG C, YUE Z. A novel feature selection and extraction method for sequence images of lip-reading[M]//Advances in Automation and Robotics. Berlin: Springer, 2011: 347-353.
- [39] ELREFAEI L A, HAMID D H, BAYAZED A A, et al. Developing iris recognition system for smartphone security[J]. Multimedia Tools and Applications, 2018, 77(12): 14579-14603.
- [40] SIVARATHINABALA M, ABIRAMI S, BASKARAN R. A study on security and surveillance system using gait recognition[M]//Intelligent Techniques in Signal Processing for Multimedia Security. Berlin: Springer, 2017: 227-252.
- [41] TAN D, NIJHOLT A. Brain-computer interfaces and human-computer interaction[M]//Brain-Computer Interfaces. New York: ACM Press, 2010: 3-19.
- [42] SU M L, FENG Z Y. Virtual reality technology[M]. New York: ACM Press, 2003.
- [43] 陈山枝. 发展 5G 的分析与建议[J]. 电信科学, 2016, 32(7): 1-10.
CHEN S Z. Analysis and suggestion of future 5G directions[J]. Telecommunications Science, 2016, 32(7): 1-10.
- [44] 潘教峰. 新科技革命与三元融合社会——关于雄安新区建设的宏观思考[J]. 中国科学院院刊, 2017, 32(11): 1177-1184.
PAN J F. New science and technology revolution and ternary fusion society——macroscopic views on xiongan new area construction[J]. Bulletin of Chinese Academy of Sciences, 2017, 32(11): 1177-1184.
- [45] KITCHIN, ROB. The real-time city? Big data and smart urbanism[M]. Berlin: Springer, 2014.
- [46] 吴军. 大数据和机器智能对未来社会的影响[J]. 电信科学, 2015, 31(2): 7-16.
WU J. Big data, machine intelligence and their impacts to the future world[J]. Telecommunications Science, 2015, 31(2): 7-16.
- [47] 徐川, 杜成, 唐红. DDoS 攻击检测研究综述[J]. 电信科学, 2011, 27(3): 85-89.
XU C, DU C, TANG H. A survey of detection research on DDoS attack[J]. Telecommunications Science, 2011, 27(3): 85-89.

[作者简介]



葛凯强 (1992-), 男, 浙江工业大学教育科学与技术学院硕士生, 主要研究方向为物联网教育、物联网安全。



陈铁明 (1978-), 男, 博士, 浙江工业大学计算机科学与技术学院教授、博士生导师, 浙江省网络安全创新研究中心主任, 主要研究方向为网络与信息安全。