

行为截获技术对鼠标动力学身份认证的影响

王 淼, 蔡忠闽, 沈 超, 华 涛

(西安交通大学 智能网络与网络安全教育部重点实验室, 陕西 西安 710049)

摘 要: 本文在 Windows 操作系统中研究并实现了三种截获用户鼠标行为数据的方法: 消息钩子、WM_INPUT 消息处理和过滤驱动, 并从采样时钟分辨率、时间精度和位置信息等方面分析了不同方法所获取数据之间的区别. 本文实验中同时使用这三种方法获取了多个用户的鼠标行为数据, 从特征层面对不同数据截获方法带来的影响进行了对比分析, 并利用神经网络分类器构建了身份认证模型, 对使用不同方法下采集的鼠标行为数据进行用户身份认证的效果进行了实验研究. 结果表明由三种数据截获方法采集到的数据都取得了较好的身份认证效果, 其中使用消息钩子获取的数据进行认证的准确率最高, 达到了 94% 以上.

关键词: 鼠标动力学; 行为特征; 身份认证

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2013)04-0014-08

The Effect of Interception Techniques on Mouse Dynamics Based Authentication

WANG Miao, CAI Zhong-min, SHEN Chao, HUA Tao

(MOE Key Lab for Intelligent Networks and Network Security (KLINNS),
Xi'an Jiaotong University, Xi'an 710049, China)

Abstract: This paper presents a comparative analysis of three different mouse activity data interception techniques in the Windows operating system and studies their impacts on the performance of mouse dynamics based authentication. The differences between three interception techniques were analyzed from perspectives of sampling resolution, timer resolution and position information. A controlled environment for intercepting mouse activity data from multiple users using three interception techniques was designed. The effects of the different techniques were at first studied from the level of mouse activity features. Then an authentication model based on neural networks was established to classify mouse activity data, and the effect of the different interception techniques on the performance of authentication was evaluated. The results show the message hooking technique appears to be a better interception technique achieving an accuracy rate above 94%.

Key words: mouse dynamics; behavioral biometrics; identity authentication

1 引言

准确验证计算机或网络用户的身份, 对保护各种各样的网络账户和数据资源具有至关重要的意义. 随着军事信息化进程的迅速推进, 计算机设备在

各类军事任务中发挥着越来越重要的作用. 而敏感军事系统的远程访问必须有安全可靠的身份认证技术保驾护航. 但是当前主要使用口令、ID 卡等手段来进行个人身份的验证, 这些手段无法避免盗用、伪造或者遗失等身份安全问题. 使用生理特征或行为

收稿日期: 2012-07-15; **修回日期:** 2012-08-20

基金项目: 国家自然科学基金项目(61175039, 60905018); 国家自然科学基金创新群体(60911003); 国家杰出青年科学基金(60825202); 国家“八六三”计划项目(2007AA01Z464); 教育部博士点新教师基金(20090201120032); 中央高校基本科研业务费专项(xjj20100051)

特征可以解决这些问题,但以指纹、虹膜识别为代表的生理特征识别方法都要求特殊的硬件支持,无法在现有的计算环境中大规模使用。

近些年,有研究者提出可利用用户在使用键盘、鼠标时体现出的独特行为特征在现有的计算环境下进行更为安全的身份认证。键盘/鼠标动力学身份认证是指根据计算机用户的键盘/鼠标输入行为特征进行用户身份的判定。目前的研究主要围绕着用户操作计算机的击键行为进行^[1-3]。随着鼠标逐渐取代键盘成为图形交互环境下计算机用户的主要输入设备,从2003年开始出现鼠标动力学身份认证的研究工作^[4-9]。Ahmed等^[7]研究了鼠标动力学身份认证的可能性,通过一些简单的鼠标行为特征,例如鼠标移动速度、鼠标移动距离实现了计算机用户身份的认证。M. Pusara和C. E. Brodley在文献^[4]中对18个用户使用IE浏览器浏览相同网页时的鼠标行为数据进行了分析,对鼠标移动等事件进行量化得到行为特征,再用决策树算法研究这些统计特征对不同用户的可分性。H. Gamboa和A. Fred等^[5]研究了50个实验者在一种记忆力测试游戏中的鼠标行为,对这些人的鼠标移动轨迹的速度、加速度、角速度、曲率等特征量进行了统计分析,实验发现基于90秒鼠标操作行为数据,可以得到超出手写签名4倍的身份认证准确率。D. Schulz在文献^[9]中也使用鼠标移动的行为特征对用户的鼠标行为进行分析,提取出的特征包括鼠标移动轨迹的长度、弯曲度和直线性,并且使用欧几里得距离度量不同鼠标行为特征之间的差异,结果表明使用这些特征进行用户身份认证的平均错误率在10.9%到24.3%之间。在国内,也有研究人员对基于鼠标动力学的身份认证和监控技术进行了研究,他们提出过程性行为特

征的概念,并取得了2.64%的平均错误率^[10-15]。

尽管不同研究者的研究思路和结论各不相同,但是作为鼠标动力学身份认证的第一步,鼠标行为数据的获取始终是不可缺少的。而使用不同的数据截获方法所获取到的鼠标行为数据在时间和位置信息上的表达和精度各不相同。因此,本文在考虑数据获取时的时间精度以及位置信息表达的基础上,研究并实现了Windows操作系统中截获用户鼠标行为数据的三种方法——消息钩子、WM_INPUT消息处理和过滤驱动。并通过实验使用这三种方法获取多个用户的鼠标行为数据,对比分析这三种数据采集方法对鼠标动力学身份认证的影响。

2 鼠标行为数据截获

鼠标输入消息由Windows内核接收,然后交由用户态的应用程序进行处理。本文在用户态分别采用消息钩子和WM_INPUT消息在应用程序前获取鼠标行为数据,在内核态使用过滤驱动截获鼠标行为数据。

2.1 基于消息钩子(Message Hook)的鼠标行为数据截获方法

鼠标消息钩子能够在应用程序处理之前截获鼠标行为数据,其加载在线程消息队列和光标所在窗口的消息传递路径中,截获所有由线程消息队列发来的鼠标数据。每一个消息钩子都有一个与之相关联的指针列表,称之为钩子(Hook)链表,由系统来维护。这个列表的指针指向由应用程序定义的被Hook子程调用的回调函数。当与指定的钩子类型关联的消息发生时,系统就把这个消息传递到钩子子程。鼠标消息钩子的基本原理如图1所示。

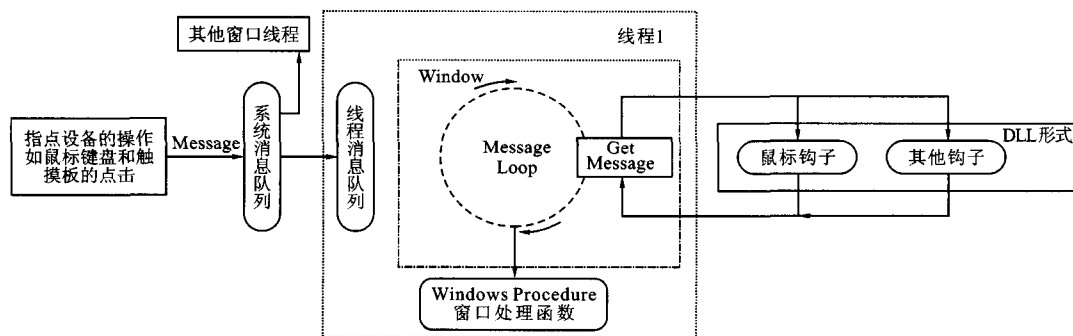


图1 鼠标消息钩子原理^[16]

2.2 基于WM_INPUT消息的鼠标行为数据截获方法

WM_INPUT消息采用的是原始输入模型。原

始输入模型及其相关的API能够比较容易地从计算机输入设备(包括鼠标和键盘)中获取原始的输入事件。原始输入模型不隐藏原始输入的细节,同时支

持 Windows 管理器不支持的 HID 设备. 原始输入模型和传统输入模型的区别在于: 在传统输入模型中, 应用程序通过发送到它窗口的消息来获取与设备相关的消息, 例如 WM_CHAR、WM_MOUSEMOVE 和 WM_APPCOMMAND 等. 在原始输入模型中, 一个应用程序想获取某个设备的原始输入数据, 必须首先注册该设备, 然后便会收到 WM_INPUT 类型的消息数据.

2.3 基于过滤驱动(Filter Driver)的鼠标行为数据截获方法

当用户有任何输入行为的时候, 将触发相应的设备中断, 引起中断服务例程的执行, 中断服务例程由相应的驱动提供. 驱动获取输入数据后, 经过一系列的处理之后, 把从输入设备得到的数据交给 IRP (I/O 请求包), 最后结束这个 IRP.

分层的驱动程序模型, 允许一个驱动程序构造一个匿名的设备对象, 并把它附着在另一个设备对象上. 在相应的线程处理 IRP 之前, 如果有附着的匿名设备对象, IRP 首先传递给此匿名设备对象, 经过对象的过滤设备驱动程序处理之后才发给真正的目标处理线程, 而这个附着的匿名设备对象就是过滤设备对象(FiDO), 与它关联的驱动程序就称为过滤驱动程序^[17]. 因此, 可以在输入设备对象的上面设置一个过滤驱动程序, 这个过滤驱动程序可以首先获得鼠标输入行为的 IRP 数据. 如图 2 所示.

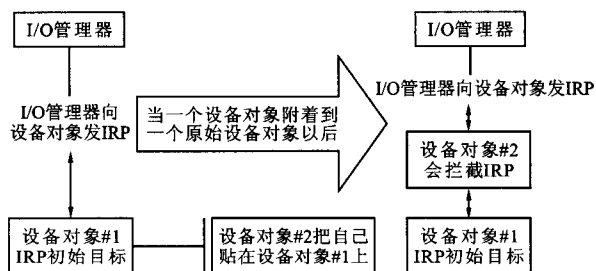


图 2 附着操作前后 I/O 管理器发送 IRP 次序变化

本文将鼠标过滤驱动附着在鼠标设备对象上, 便可以在内核态下载获鼠标行为数据.

3 鼠标行为特征提取

3.1 鼠标行为数据

本文同时使用消息钩子、WM_INPUT 消息和过滤驱动这三种方法截获鼠标行为数据. 消息钩子截获到鼠标行为对应的数据结构为 MouseLLHookStruct^[18]; WM_INPUT 消息获取到的数据对应的数据结构为 RAW_INPUT^[19], 其中包含了鼠标行为数据结构 RAW_MOUSE^[19]; 过滤驱动截获

到的鼠标行为数据对应的数据结构 MOUSE_INPUT_DATA^[20].

在三种方法获取的不同数据结构体中, 都包含有鼠标消息类型. 鼠标消息类型描述了鼠标操作事件类型, 如左键按下、右键弹起、滚动和移动等. 过滤驱动和 WM_INPUT 消息定义的鼠标消息类型相同, 而消息钩子与之不同. 为了便于提取行为特征, 本文结合所截获的数据结构体选取消息类型、位置信息和时间戳构成一个体现鼠标事件信息的新的结构体.

3.1.1 基于消息钩子(Message Hook)的鼠标截获数据分析

表 1 所示为使用消息钩子得到的 5 个连续鼠标事件的行为数据. 表中每一行表示一个鼠标行为事件, 消息类型中的“512”表示鼠标移动或者静止, “513”表示鼠标左键单击按下, “514”表示鼠标左键单击弹起.

表 1 使用消息钩子得到的鼠标行为数据

消息类型	屏幕坐标系中的 X 轴坐标	屏幕坐标系中的 Y 轴坐标	时间戳
512	359	295	419556140
512	358	295	419556171
513	358	295	419556281
514	358	295	419556390
512	358	295	419556562

通过对使用消息钩子得到的数据进行分析, 可以发现消息钩子截获到的结构体 MouseLLHookStruct 中包含有鼠标事件的时间戳. Windows 系统的时钟中断间隔是 15.625 毫秒, 所以消息钩子的采样时钟分辨率是 15.625ms, 即两鼠标事件的时间戳总是相差 15.625 毫秒 * a (a=1, 2, ..., n). 对数据中的坐标信息进行分析, 发现 MouseLLHookStruct 中记录的是鼠标事件在屏幕坐标系中的绝对坐标, 取值范围和屏幕分辨率对应. 而对于数据中的消息类型, 消息钩子对各种鼠标操作都提供了相应的类型编码, 例如左键单击对应操作序列为 513/514, 双击对应操作序列为 513/514/515, 正向滚动和反向滚动都用 522 表示.

3.1.2 基于 WM_INPUT 消息的截获数据分析

通过分析使用 WM_INPUT 消息截获到的数据结构, 发现对应于 WM_INPUT 消息的鼠标事件数据结构体 RAW_MOUSE 中不包含时间戳, 为了获取鼠标事件的准确的时间信息, 本文使用高精度计时器记录事件的产生时间. 其中, Windows API

函数 QueryPerformanceCounter 获得计算机硬件高精度定时器的时间脉冲信号的计数值,API 函数 QueryPerformanceFrequency 获得高精度定时器的时钟频率,两者相除得到当前时间戳.但是即使如此,因为时间戳标记时间和事件发生的真实时间不一致,容易引入时间误差.使用 WM_INPUT 消息得到的 5 个连续鼠标事件的行为数据如表 2 所示.其中,消息类型中的 0 表示鼠标移动或者静止,1 表示鼠标左键按下,2 表示鼠标左键弹起.

表 2 使用 WM_INPUT 消息得到的鼠标行为数据

消息类型	逻辑坐标系 中的 X 轴 物理位移	逻辑坐标系 中的 Y 轴 物理位移	时间戳
0	0	-1	1.87732969116536
0	-1	0	1.90935112780447
1	0	0	2.00602213036417
2	0	0	2.11742970586859
0	1	0	2.28538067294004

通过对使用 WM_INPUT 消息得到的数据进行分析,可以发现因为 WM_INPUT 消息采用高精度计时器,所以采样时钟分辨率等于高精度定时器的时钟周期,两行为数据点的时间戳相差是该时钟周期的整数倍.本文实验所用计算机的时钟频率为 2992520000,两行为数据点的时间戳相差为 5—9 毫秒.另外,WM_INPUT 消息中的位置信息是鼠标相对于上一个位置的相对位移,并且对于单击和双击在消息类型上没有明显区分,例如左键单击表示为 1/2,而左键双击为 1/2/1/2,在提取行为特征时需要通过计算两次连续单击的间隔时间来区分单、双击事件.此外,使用 WM_INPUT 消息还可以获得和设备相关的其他信息.

3.1.3 基于过滤驱动的截获数据分析

通过分析过滤驱动截获到的鼠标事件数据结构 MOUSE_INPUT_DATA,发现其中也不包含时间戳,为了获取数据点的时间,在内核态使用 Windows API 函数 KeQuerySystemTime 获取当前系统时间,这个时间的精度达到 100 纳秒.因为时间戳标记时间和事件发生的真实时间不一致,容易引入时间误差.表 3 所示为使用过滤驱动得到的 5 个连续鼠标事件的行为数据,其消息类型的表示和 WM_INPUT 消息相同.

分析过滤驱动得到的数据,可以发现使用 KeQuerySystemTime 得到的数据点时间戳相差 15.625 毫秒的整数倍.和 WM_INPUT 消息一样,

表 3 使用过滤驱动得到的鼠标行为数据

消息类型	逻辑坐标系 中的 X 轴 物理位移	逻辑坐标系 中的 Y 轴 物理位移	时间戳
0	0	-1	129175816693906250
0	-1	0	129175816694218750
1	0	0	129175816695312500
2	0	0	129175816696406250
0	1	0	129175816698125000

过滤驱动得到的也是鼠标的物理位移,对单、双击鼠标事件无明显区分.此外通过过滤驱动也能获得和设备相关的其他信息.

通过以上分析发现:消息钩子截获到的数据结构中含有鼠标行为数据点的屏幕坐标和时间戳,并且对不同鼠标事件的区分明显;而 WM_INPUT 消息和过滤驱动截获到的数据结构体中包含的是鼠标的相对物理位移,且无时间戳,需要在采集环节人工添加,容易引入额外的时间误差;且对单、双击鼠标事件无明显区分.所以消息钩子能够更加方便地反映用户的鼠标操作语义,是进行鼠标行为认证时一种较易使用的数据源.

3.2 鼠标行为特征

通过上一节的分析,本文使用三种方法得到的鼠标行为数据体现为按时间顺序排列的 4 维数据集: $\text{InputData} = \{(type_i, x_i, y_i, time_i)\}$,其中 i 表示第 i 个鼠标事件,分别表示了该事件的类型、 x 、 y 坐标以及发生时间.在此基础上,本文提取了鼠标移动速度、移动加速度、移动偏移量、移动持续时间和点击时间间隔的统计量这 5 类鼠标行为特征.

(1) 鼠标移动速度

在鼠标操作过程中,鼠标移动的轨迹通常不是直线,鼠标在移动方向和垂直移动方向都有位移,单点的速度方向并不总是和移动方向一致,有时甚至偏差很大.将单点的速度 v 分解为移动方向的速度 $v_{\parallel}$ 和垂直移动方向的速度 $v_{\perp}$,由于 $|v_{\parallel}| > |v_{\perp}|$,所以本文忽略 $v_{\perp}$,只计算 $v_{\parallel}$.对于水平移动,计算水平方向上的速度,数据点的速度定义为当前数据点和前一数据点水平位移之差除以它们的时间戳之差.类似地,对于垂直移动,本文只考虑垂直速度.对于斜线方向的移动,先对数据点进行坐标变换,将原坐标系下的该点转换为新坐标系下的点,新坐标系中的横轴表示移动方向坐标,纵轴表示垂直移动方向的坐标,然后计算在新坐标系中的移动方向速度.

(2) 鼠标移动加速度

加速度的计算使用已经计算出来的速度,加速度方向和速度方向一致. 某一数据点的加速度定义为当前数据点和前一数据点速度之差除以它们的时间戳之差.

(3) 鼠标移动偏移量

对于水平移动,本文计算垂直方向上的偏移量,某段移动的偏移量定义为移动轨迹中,两相邻数据点垂直坐标之差的绝对值的总和. 类似地,对于垂直移动,本文计算水平偏移量. 斜线方向的移动偏移量的计算和速度类似,也需要先进行坐标变换.

(4) 鼠标移动持续时间

一次移动的持续时间是一次移动中首尾两个数据点的时间间隔.

(5) 鼠标点击时间间隔统计特征

一段鼠标操作过程中的点击时间间隔统计特征包括鼠标单击和双击时间间隔(包括单击持续时间,双击中两次单击的持续时间、间隔时间和双击持续时间)的均值和方差.

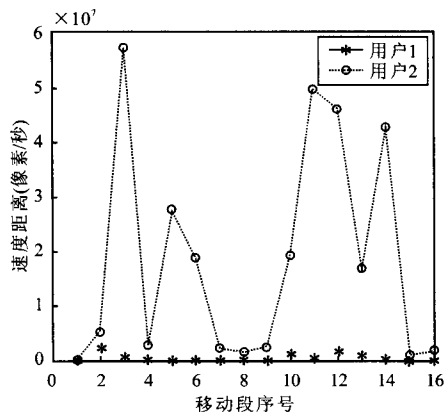
3.3 特征的距离度量

上一节中定义的特征包含的数据量较大,比如移动速度,16次鼠标移动就能产生上千个速度值,无法直接作为用户身份认证分类器的输入,因此本文使用特征向量之间的距离进行身份认证. 因为两个速度值序列的长度一般不同,所以本文使用动态时间规整(Dynamic Time Warping, DTW)方法计算两个不等长速度值序列之间的编辑距离. 编辑距离的概念由俄国科学家莱文斯坦在1965年提出,因此又称为莱文斯坦距离,可以处理长度不等的序列^[21]. 与此类似,也使用DTW计算加速度值序列对的编辑距离. 两个移动偏移量的距离为对应移动偏移量之差的绝对值,持续时间距离和点击时间间隔统计量距离的计算与移动偏移量距离类似.

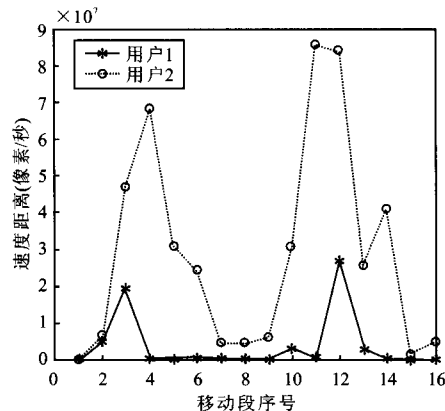
根据以上过程,本文使用三种鼠标行为数据截获方法得到的数据来分别计算行为特征距离. 图3表示的是两个用户完成规定16次鼠标移动时的速度特征,图中显示的是两个用户的实测速度曲线和用户1的基准速度曲线进行比较后求得的编辑距离.

在图3中,曲线上的点离横轴越近,表明当前用户和用户1的移动速度特征越相似. 根据三种鼠标数据截获方法所得数据计算出的特征距离不尽相同. 图3(a)中用户1和自己的移动速度特征距离较小,在图3(b)和3(c)中,用户1和自己的移动速度特征距离较大,并且图3(c)中的用户2和用户1的

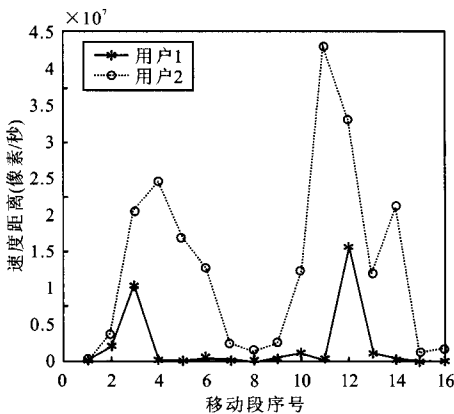
移动速度特征距离也没有图3(a)和3(b)中明显. 这表明通过消息钩子截获的数据可以更好地表达用户的行为特征.



(a) 消息钩子数据



(b) WM_INPUT 消息数据



(c) 过滤驱动数据

图3 不同数据截获方法下两用户鼠标移动速度距离的对比

4 实验及结果分析

4.1 实验设计

本文设计了移动和左键点击相结合的鼠标操作固定场景. 在一个固定大小的矩形窗体上设置了7

个固定位置,分别对应 7 个大小相同的矩形框. 用户点击“开始”按钮之后,第 1 个矩形框出现提示用户在框内单击或者双击鼠标,用户点击后矩形框消失,第 2 个矩形框出现并提示用户操作鼠标,以此顺序进行直至用户点击完所有出现的矩形框作为一次完整的固定场景鼠标操作. 一次操作用户总共需要完成 16 次鼠标移动和 16 次鼠标点击,包括 8 次左键单击和 8 次左键双击. 图 4 显示了前 8 次的移动路径,后 8 次的移动路径与之相同.

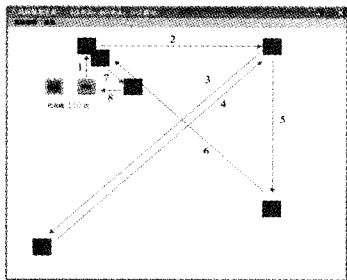


图 4 固定场景中的前 8 次鼠标移动

在一次固定场景操作中,前 8 次移动包含了 8 个不同的移动方向和 3 类不同的移动距离. 表 4 显示了前 8 次移动方向和移动距离,其中 4 个斜线方向与水平方向之间的夹角是 45° .

表 4 固定场景中的前 8 次鼠标移动方向和距离

移动编号	方向	距离(像素)
1	↑	100
2	→	400
3	↘	700
4	↗	700
5	↓	400
6	↖	524
7	↘	100
8	←	100

4.2 数据采集

本文实现了在同时使用三种方法进行鼠标行为数据截获的采集器,并用采集器采集了 5 个用户分别进行 30 次固定场景操作的数据. 采集器的运行环境要求为:计算机屏幕分辨率固定是 1280×1024 像素;鼠标双击速度:Windows 默认设置(默认时间间隔 500 毫秒,范围 200~900 毫秒);鼠标移动速度:Windows 默认设置(Mouse Sensitivity=10,范围为 1~20);是否提高指针精确度:是(默认为选中此项, MouseSpeed=1, MouseThreshold1=6, MouseThreshold2=10);滚轮:一次滚动 3 行;鼠标硬件:hp M-UAE96.

4.3 数据预处理

本文在数据预处理阶段完成了以下工作:(1) 去除冗余数据,即去掉时间间隔小于采样时间精度的数据点;(2) 切分移动和点击,一次操作中的移动和点击数据是存放在一起的,在特征提取时需要将移动和点击切分开来;(3) 剔除无效数据,在一次场景中,如果用户操作出错,可能导致切分出多余的移动和点击,本文设定此次操作的数据是无效数据并将其剔除.

4.4 特征提取

鼠标行为数据经过预处理后,提取出第 3 节所介绍的 5 种鼠标行为特征. 然后以合法用户的一次典型操作作为基准操作,计算得到 5 个特征距离向量: dV , dA , dB , dT , dC . 其中, dV 表示一次固定场景操作中的 16 次移动与基准操作中 16 次移动的速度编辑距离以及距离总和向量; dA 是相对于基准操作的 16 次移动的加速度编辑距离以及距离总和向量; dB 表示相对于基准操作的 16 次移动的移动偏移量距离以及距离总和向量; dT 代表相对于基准操作的持续时间距离向量; dC 有 10 维数据,是表示单双击时间间隔的均值和方差的统计量. 本实验中选取训练数据中与其他操作平均距离最小的那次操作作为典型操作,即基准操作. 因此,一次固定场景鼠标操作后得到的行为特征可以看作是一个 78 维的向量.

4.5 实验结果

本节通过训练神经网络分类器进行二元分类,来研究三种鼠标行为数据采集方法对用户身份认证效果的影响. 4.4 节所提取的 78 维鼠标行为特征作为神经网络分类器的输入,基于实验数据计算这三种方法对应的身份认证的准确率. 在实验中,5 个用户按照设计的固定场景,重复进行 30 次操作,每次操作时消息钩子、WM_INPUT 消息及过滤驱动各自会记录下一组行为数据. 这样对于每种采集方法,我们可以得到一个包含 5 个用户每个用户 90 组行为数据的数据集,分别对三种方法获取的数据进行身份认证实验. 在实验中,首先选取 1 个用户为合法用户,剩余的 4 个为非法用户,然后随机选取 5 个用户各 10 组行为数据提取行为特征进行二分类神经网络训练,剩余 20 组计算得到的行为特征用于神经网络分类器的测试. 对于用户 A 为合法用户的情况,训练数据包括用户 A 的 10 组行为特征作为正常数据,其他 4 个用户的 40 组数据作为非法数据;测试数据是用户 A 的剩余 20 组行为特征作为正常

表 5 用户身份认证的实验结果

鼠标行为 数据截获方法	用户 1	用户 2	用户 3	用户 4	用户 5
消息钩子	误拒率:13.167% 误纳率:1.875% 准确率:95.867%	误拒率:14.000% 误纳率:1.167% 准确率:96.267%	误拒率:17.500% 误纳率:2.417% 准确率:94.567%	误拒率:20.000% 误纳率:1.705% 准确率:94.417%	误拒率:1.000% 误纳率:0.125% 准确率:99.700%
WM_INPUT 消息	误拒率:19.500% 误纳率:2.625% 准确率:94.000%	误拒率:17.000% 误纳率:3.500% 准确率:93.800%	误拒率:21.333% 误纳率:2.250% 准确率:93.933%	误拒率:21.333% 误纳率:3.208% 准确率:93.167%	误拒率:8.333% 误纳率:0.167% 准确率:98.200%
过滤驱动	误拒率:14.167% 误纳率:1.875% 准确率:95.667%	误拒率:17.667% 误纳率:1.542% 准确率:95.233%	误拒率:19.500% 误纳率:2.208% 准确率:94.333%	误拒率:17.333% 误纳率:3.250% 准确率:93.933%	误拒率:6.000% 误纳率:0.000% 准确率:98.800%

数据,其他 4 个用户的剩余 80 组数据作为非法数据. 根据对测试数据的分类结果,计算误拒率表示合法用户被错误拒绝的比率;计算误纳率表示非法用户被错误接受的比率;计算准确率表示合法用户和非法用户被正确分类的总比率;得到的认证结果如表 5 和表 6 所示.

表 6 用户身份认证实验的总体结果

实验结果 数据截获方法	平均 误拒率	平均 误纳率	平均 准确率
消息钩子	13.1334%	1.4578%	96.1636%
WM_INPUT 消息	17.4998%	2.35%	94.62%
过滤驱动	14.9334%	1.775%	95.5932%

从实验结果可以看出:使用消息钩子所得的数据进行鼠标动力学身份认证的准确率比 WM_INPUT 消息和过滤驱动要高. 同时,消息钩子的误纳率和误拒率都是最低的,特别是在误拒率上,消息钩子明显占优势. 对这三种方法所获取到的鼠标行为数据的分析,消息钩子携带的系统时间戳比其他两种方法中自行生成的时间戳要准确,并且消息钩子直接得到用户的绝对屏幕位移,轨迹位置表示的误差也较小. 此外,消息钩子对不同鼠标事件的区分十分明显,在特征提取时我们能够准确地识别出鼠标的单、双击操作;而 WM_INPUT 消息和过滤驱动的数据结构体中没有时间戳,获取到的是用户的相对物理位移,同时由于它们对单、双击鼠标事件的区分不明显,需要根据两次连续单击的间隔时间来主观地区分单击和双击,导致提取出的行为特征可能和实际情况存在偏差. 所以使用消息钩子得到的数据进行鼠标动力学身份认证的准确率更高,实验结果同前面的机理分析基本吻合.

5 结束语

本文研究并实现了三种在 Windows 操作系统中截获鼠标行为数据的方法(消息钩子、WM_INPUT 消息以及过滤驱动). 通过固定场景数据采集器同时使用这三种方法采集用户在一个固定场景操作中的鼠标行为数据,对获取的原始行为数据进行分析,研究三种方法在采样时钟分辨率、时间精度、位置信息等方面的不同. 然后提取出新的鼠标行为特征,计算这些特征和合法用户的基准行为过程之间的距离作为身份认证模型的输入. 使用神经网络分类器对比分析了这三种方法的用户身份认证准确率. 实验结果表明使用 WM_INPUT 消息和过滤驱动所截获的数据进行身份认证,准确率不及消息钩子,特别是在误拒率上表现欠佳. 基于过滤驱动和 WM_INPUT 消息的身份认证准确率相近,但是过滤驱动方法实现过程较为复杂,在运行时易发生错误,并且操作系统平台移植性不好. 通过消息钩子方法截获的数据时间准确性高,轨迹位置表示的误差较小,用于身份认证的效果较好,而 WM_INPUT 消息方法优于过滤驱动.

参考文献:

[1] Gaines R, Lisowski W, Press S. Authentication by keystroke timing[R]: Rand Corporation; Rand Report R225602, NSF, 1980.

[2] Saleh Bleha, Charles Slivinsky, Bassam Hussien. Computer—access security systems using keystroke dynamics[J]. IEEE Transaction on Pattern Analysis and Machine Intelligence, 1990,12(12):1217—1222.

[3] 朱明,周津,王继康. 基于击键特征的用户身份认证新方法[J]. 计算机工程,2002,28(10):138—140.

[4] Pusara M, Brodley C E. User re—authentication via

- mouse movements[C]//Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security, DMSEC Session, Washington DC, USA, 2004:1-8.
- [5] Gamboa H, Fred A. A behavioral biometric system based on human computer interaction[J]. Proceedings of SPIE, 2004(54): 4-36.
- [6] Ahmed A A E, Traore I. Anomaly intrusion detection based on biometrics[C]//Proceedings of 6th IEEE Information Assurance Workshop, New York, USA, 2005, 452-453.
- [7] Ahmed A A E, Traore I. Detecting computer intrusions using behavioral biometrics[C]//3rd Annual Conference on Privacy, Security and Trust, St. Andrews, Canada, 2005:91-98.
- [8] Garg A, Vidyaraman S, Upadhyays S, et al. USim: a user behavior simulation framework for training and testing idses in GUI bases systems[C]//Proceedings of 39th Annual Simulation Symposium, Huntsville, AL, 2006:196-203.
- [9] Schulz D. Mouse curve biometrics[C]//2006 Biometrics Symposium: Special Session on Research at the Biometric Consortium Conference, Baltimor, 2006:1-6.
- [10] Shen C, Cai Z M, Guan X H. Continuous authentication for mouse dynamics: a pattern-growth approach [C]//Proc. IEEE/IFIP Int. Conf. Dependable Systems and Networks (DSN). Boston, MA, 2012.
- [11] Shen C, Cai Z M, Guan X H, et al. On the effectiveness and applicability of mouse dynamics biometric for static authentication: a benchmark study[C]//Proc. IAPR/IEEE Int. Conf. Biometrics (ICB). New Delhi, India, 2012.
- [12] Shen C, Cai Z M, Guan X H. Can it be more practical? Improving mouse dynamics biometric performance[C]//Proc. ACM Conf. Computer and Communications Security (CCS). Chicago, IL, 2011, 853-856.
- [13] Shen C, Cai Z M, Guan X H, et al. A hypo-optimum feature selection strategy for mouse dynamics in continuous identity authentication and monitoring[C]//Proc. IEEE Int. Conf. Information Theory and Information Security (ICITIS). Beijing, China, 2010.
- [14] 沈超,蔡忠闽,管晓宏,等. 基于鼠标行为特征的用户身份认证与监控[J]. 通信学报, 2010, 31(7):68-75.
- [15] Shen C, Cai Z M, Guan X H, et al. Feature analysis of mouse dynamics in identity authentication and monitoring[C]//Proc. IEEE Int. Conf. Communication (ICC). Dresden, Germany, 2009:1-5.
- [16] 房超,蔡忠闽,沈超,等. 基于鼠标动力学模型的用户身份认证与监控[J]. 西安交通大学学报, 2008, 42(10): 1235-1239.
- [17] 谭文. Windows 内核安全编程[M]. 北京:电子工业出版社, 2009:17-83.
- [18] MicroSoft Development Network: Hooks (Windows) [EB/OL]. (2010-4-26). [http://msdn.microsoft.com/en-us/library/windows/desktop/ms632589\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/ms632589(v=vs.85).aspx).
- [19] MicroSoft Development Network. RAWINPUT structure(Windows) [EB/OL]. (2010-5-11). [http://msdn.microsoft.com/enus/library/windows/desktop/ms645562\(v=vs.85\).aspx](http://msdn.microsoft.com/enus/library/windows/desktop/ms645562(v=vs.85).aspx).
- [20] MicroSoft Development Network. MOUSE — INPUT — DATA structure(Windows Drivers) [EB/OL]. (2010-6-26). [http://msdn.microsoft.com/en-us/library/windows/hardware/ff542403\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/hardware/ff542403(v=vs.85).aspx).
- [21] Marzal A, Vidal E. Computation of normalized edit distance and applications[J]. IEEE Transactions on pattern analysis and machine intelligence, 1993, 15(9):926-932.

作者简介:

王 森 硕士研究生. 研究方向为计算机网络安全、模式识别.

蔡忠闽 博士. 研究方向为计算机网络安全、数据挖掘、可信计算.

沈 超 博士研究生. 研究方向为计算机及网络信息安全.

华 涛 硕士研究生. 研究方向为计算机网络安全.