

基于鼠标动力学模型的用户身份认证与监控

房超^{1,2}, 蔡忠闽^{1,2}, 沈超^{1,2}, 牛非^{1,2}, 管晓宏^{1,2}

(1. 西安交通大学制造系统国家重点实验室, 710049, 西安; 2. 西安交通大学
智能网络与网络安全教育部重点实验室, 710049, 西安)

摘要: 针对计算机系统安全中的用户身份识别和监控等基本问题,提出了一种利用鼠标动力学行为特征进行身份识别的新方法.通过采集各种应用环境下的鼠标行为数据,从交互和生理2个层面上对人机交互过程中计算机用户的鼠标行为特征进行建模、分析,以达到实时监测用户身份、检测非法用户的目的.所提方法可为身份监控原型系统实时采集用户的行为数据,并将当前的行为与用户的历史行为模型进行比较,以判断和检测用户身份,再依据判断检测结果产生实时的响应,从而有效防止非法用户侵入.实验采集并分析了10个用户的鼠标行为数据,通过特征降维与神经网络分类相结合的算法,得到了0.48%的误识率和2.86%的拒识率,充分展示了基于鼠标动力学行为模型进行身份认证和监控的可行性.

关键词: 鼠标动力学;身份认证;身份监控;计算机系统安全;人机交互

中图分类号: TP393 **文献标志码:** A **文章编号:** 0253-987X(2008)10-1235-05

Authentication and Monitoring of User Identities Based on Mouse Dynamics

FANG Chao^{1,2}, CAI Zhongmin^{1,2}, SHEN Chao^{1,2}, NIU Fei^{1,2}, GUAN Xiaohong^{1,2}

(1. State Key Laboratory for Manufacturing Systems, Xi'an Jiaotong University, Xi'an 710049, China; 2. MOE Key Laboratory for Intelligent Networks and Network Security, Xi'an Jiaotong University, Xi'an 710049, China)

Abstract: User identification and monitoring is one of the most important issues in computer system security. A new method for user identification is presented based on the dynamics of computer mouse behavior. Data of mouse behavior in various applications are collected, and users' mouse behavior in human computer interaction is analyzed and modeled, specifically from both the interaction layer and the physiological layer. Based on the dynamic model, a real-time identity authentication and monitoring prototype system is developed, which can intercept users' mouse behavior data, and compare user's current behavior with his history behavior model in order to detect and authenticate current user's identity. According to the result of authentication, system responds real-time and defends against the intrusion of illegal user. An algorithm that uses feature dimension reduction and neural network for classification is applied in experiments for ten users. The experimental results show that mouse dynamics is effective for authenticating and monitoring user identities with a false accept rate (FAR) of 0.48% and a false rejection rate (FRR) of 2.86%.

Keywords: mouse dynamics; identity authentication; identity monitoring; computer system security; human computer interaction

目前,计算机安全问题引起了人们的极大关注,而身份识别与认证是系统安全策略的重要组成部分

分. 现有的身份识别技术主要包括3类, 它们分别利用了不同的信息, 即: 所知道的, 如密码、PIN等; 所拥有的, 如ID卡、令牌等; 用户自身的, 如指纹、虹膜等生物特征^[1]. 这些传统的识别技术均存在缺陷, 如密码难于记忆并容易搞混和泄露, ID卡需要随身携带且易失窃或失效, 生物认证需要额外的硬件设备或容易伪造等, 而且它们均无法在计算机使用过程中进行用户身份的实时监控. 所以, 研究用户使用计算机的行为特征, 以此检测用户的异常行为、实时监控用户的身份便显得尤为重要.

研究计算机用户输入行为主要是围绕击键动力学特征进行的^[2-4], 作为图形化人机交互环境下的主要输入设备的鼠标, 其动力学特征研究尚处于初级阶段. 从2003年开始, 国外有4个小组对鼠标的使用行为特征进行了初步的探讨^[5-9], 内容多为基于统计的鼠标行为特征, 而在国内仅有个别文献有所提及^[10], 但未见具体内容.

综上, 本文提出了一种利用鼠标动力学特征的身份识别新技术.

1 鼠标动力学模型

本文定义的鼠标动力学特征主要分为交互层特征和生理层特征, 这些特征既包括基于统计的特征, 也包括基于人机交互模型的特征.

1.1 交互层特征

交互层有下列特征.

(1) 事件频率 f , 即各种鼠标行为事件在一定监控时间内发生的频数占事件总数的百分比.

(2) 静止时间占空比, 即在一定监控时间内鼠标静止或未进行任何操作的时间所占比率.

(3) 其他统计特征, 如以右单击结合左单击快捷方式的频率, 移动距离频率(用户习惯进行短距离或长距离移动)、屏幕坐标范围等.

1.2 生理层特征

生理层有下列特征.

(1) 单击时间间隔 Δt , 即鼠标左/右/中3键从按下到弹起的时间间隔.

(2) 双击内部时间间隔. 左键的双击共由4个鼠标动作组成, 即左键的第一次按下和弹起、第二次按下和弹起. 除了完成一次双击所需的总时间之外, 还存在3个内部时间间隔 Δt_1 、 Δt_2 、 Δt_3 .

(3) 平均移动速度与距离的关系. 根据人机交互学(HCI)中的经典定律 Fitts 法则^[11], 可以推导出速度与距离的关系式

$$S_{\text{speed}} = A/T_M = A/(a + b(\ln(\frac{2A}{w})))$$

式中: T_M 为平均移动时间; A 为一次移动的位移; w 为目标宽度(在此取常数); a 、 b 为系数.

(4) 平均移动速度与方向的关系. 实验中发现, 用户在不同方向移动鼠标时具有不同的速度, 那么通过分析用户在 n 个方向运动的 Fitts 法则关系, 可以得到向量 $\mathbf{A}=[a_1, a_2, \dots, a_n]$, $\mathbf{B}=[b_1, b_2, \dots, b_n]$, $i=1, \dots, n$. 其中, a_i 、 b_i 为第 i 个方向上 Fitts 法则的关系系数, 它们可反映设备使用者在进行快速定位运动时的协调控制能力.

(5) 移动中速度变化的微结构. 根据动力学和生物控制理论中的人类快速运动模型^[12-13], 可以推导出鼠标移动的速度微结构模型

$$\left. \begin{aligned} v(t) &= D_1 \Lambda(t; t_0, \mu_1, \sigma_1^2) - D_2 \Lambda(t; t_0, \mu_2, \sigma_2^2) \\ \Lambda(t; t_0, \mu_i, \sigma_i^2) &= \frac{1}{\sigma_i (2\pi(t-t_0))^{1/2}} \cdot \\ &\quad \exp\left\{-\frac{[\ln(t-t_0) - \mu_i]^2}{2\sigma_i^2}\right\} \end{aligned} \right\}$$

式中: D_1 、 D_2 分别表示驱动系统和阻尼系统力的幅值, 每个系统的脉冲响应均符合对数正态分布 $\Lambda(t; t_0, \mu_i, \sigma_i^2)$; t 是系统运动时间, 起始时间 $t_0=0$. 在相同的移动距离下, 可推导出 D_1 、 D_2 均为常量, 此时系数 μ_i 、 σ_i 可作为不同用户的特征参量.

(6) 组合操作中的反应切换时间. 用户完成不同操作之间的反应和切换时间, 如移动定位后到点击之间的反应时间等.

2 身份监控系统

2.1 用户身份监控系统

在鼠标动力学模型的基础上, 本文设计并实现了基于计算机输入行为特征的用户身份监控系统. 用户通过训练可自动生成鼠标行为特征模板, 并存入特征模板库. 在监控过程中, 系统通过实时采集用户的鼠标行为数据, 并对数据进行预处理和操作切分, 从中提取出用户的鼠标行为特征, 最后将提取出的特征与合法用户模板进行匹配. 如果检测出非法用户, 将锁定计算机, 并启动再认证功能. 当进行再认证时, 系统不仅对密码进行匹配, 而且要分析用户的击键行为特征, 这样可有效防止密码泄露等情况下的内部攻击, 从而实现系统的双重保护. 用户身份监控系统的运行流程如图1所示.

2.2 数据采集和预处理

输入数据源包括鼠标动作、屏幕坐标、系统时

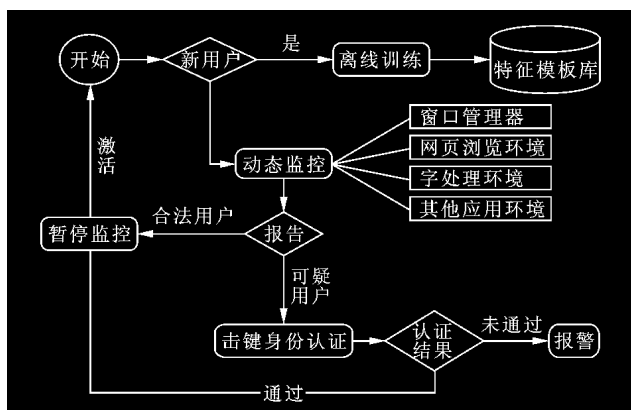


图1 用户身份监控系统的运行流程图

间、进程信息等,研究发现,鼠标动力学特征,尤其是交互层的特征与应用环境密切相关,所以,用户可以选择需监控的应用环境,如窗口管理器、网页浏览方式、字处理环境等。

系统对采集到的输入数据需进行冗余过滤、操作切分等预处理,得到鼠标操作序列,并且根据进程信息将鼠标行为事件归类。

2.3 特征提取

系统从不同环境的鼠标操作序列中计算并提取出各类鼠标行为特征,同时为每个合法用户生成特定应用环境下的行为特征模板,并存入特征模板库。用户可进行多次训练,每次的训练结果将作为用户特征模板库的更新数据。

2.4 模板匹配

在特征空间中,不同用户之间总是存在着一些较为相近的行为特征,而由于各种鼠标特征的属性不同,所以很难对这些特征进行归一化处理。为了研究不同用户的特征空间分布,本文采用了不同参数的类间距离分类或贝叶斯分类算法,并对所有特征经多数投票决策融合法处理来验证用户的身份。

令

$$S = \sum F_i = \begin{cases} S \geq Z & \text{当前踊跃} \\ S < Z & \text{当前踊跃} \end{cases}$$

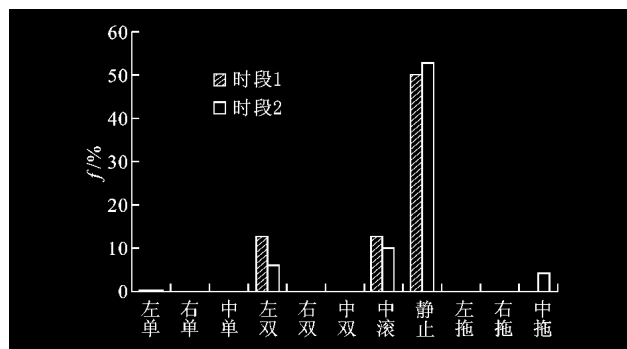
式中: F_i 表示第*i*个特征的分类结果; Z 表示总的决策阈值。决策阈值和各个特征分类阈值 H^i 可以通过优化的方法进行调节。

3 特征实验与分析

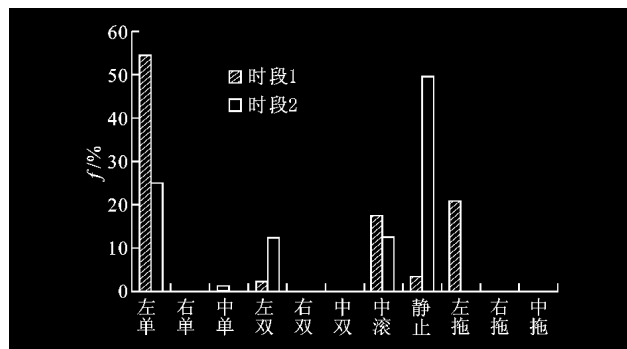
3.1 独立特征实验与分析

(1)事件频率分布。在不同的进程中,用户通过鼠标可以进行操作,如浏览网页、窗口管理及文字处理等。记录下用户的鼠标操作,分析不同用户在相同

时间段完成相同任务的鼠标行为事件的发生频率及各种频率事件占总事件的百分比(见图2),可以在统计层面上测定用户鼠标行为的特征。可以看出,同一用户在相同应用环境下的事件频率分布较为稳定,而不同用户在相同应用环境中的事件频率分布差异较大。



(a)同一用户

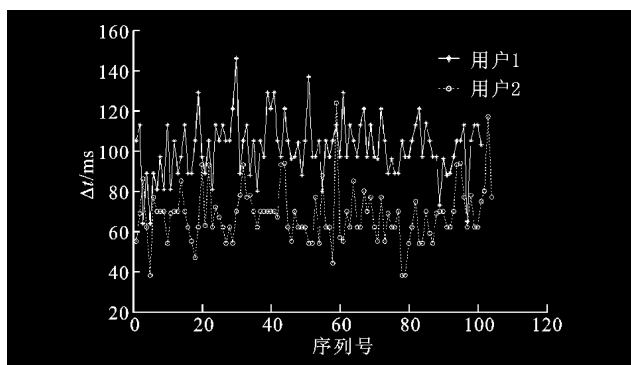


(b)不同用户

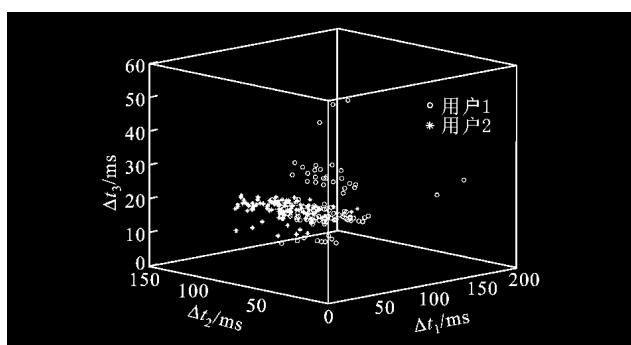
图2 用户鼠标行为事件频率分布

(2)点击时间间隔 Δt 。用户通过单、双击鼠标操作来完成计算机控制。不同用户左键单击鼠标的的时间间隔对比如图3a所示,不同用户双击鼠标时间间隔的内部三维聚类特性如图3b所示。从图中可以看出,不同用户的单、双击时间间隔存在差异,同一用户单、双击间隔时间的分布比较稳定。

(3)移动速度与距离、方向、目标大小的关系。在模拟图形交互界面实验环境中,要求用户将鼠标从起点移动到目标位置并点击,目标的大小是固定的,位置是随机弹出的,目标离起点的距离是随机产生的,距离在0~700像素之间,在由此构成的环境中,本文测定了不同距离下用户的鼠标移动速度。用模型公式对不同用户的鼠标平均移动速度与距离的关系进行拟合,结果如图4所示。从图中可以看出,鼠标一次移动的距离越大,移动的平均速度就越大,而不同用户移动速度的增长程度有所不同,这种增长关系是非线性的。



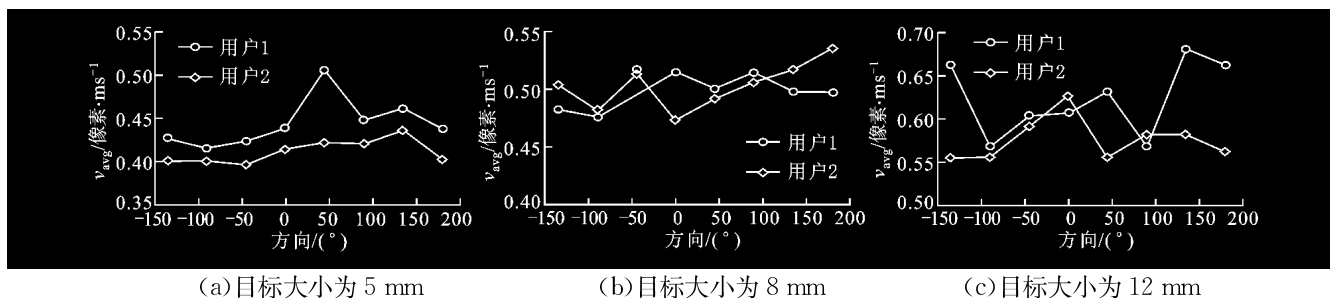
(a) 单击时间间隔散点



(b) 双击三维时间间隔散点

图3 鼠标单、双击时间间隔对比

基于类似的实验环境,在8个方向上采取随机弹出对话框的方式来测试平均移动速度与移动方向



(a) 目标大小为 5 mm

(b) 目标大小为 8 mm

(c) 目标大小为 12 mm

图5 平均移动速度与方向和目标大小的关系

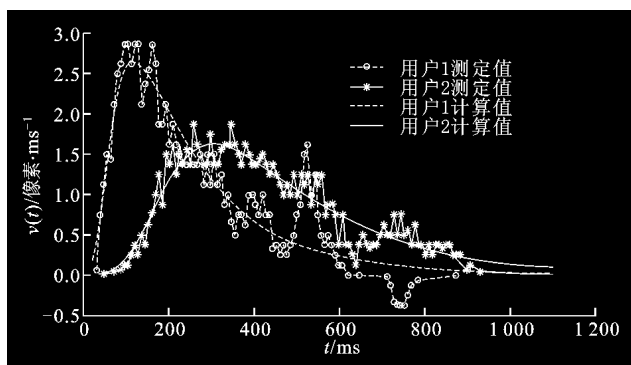


图6 平均移动速度微结构

3.2 身份识别实验

本文采集了自然状态下10个用户在一周内的鼠标行为数据,并进行了身份识别实验.本实验的部分特征是在同一应用环境下的统计特征,采集到的数据一部分作为分类模型训练的输入数据,另一部分作为模型的测试数据.

和目标大小的关系,结果如图5所示.从中可以看出,鼠标在各个方向上的移动速度以及速度随着方向的变化趋势均存在差异,其中移动速度随目标面积的增加而增大,原因是:目标越小,定位操作精度

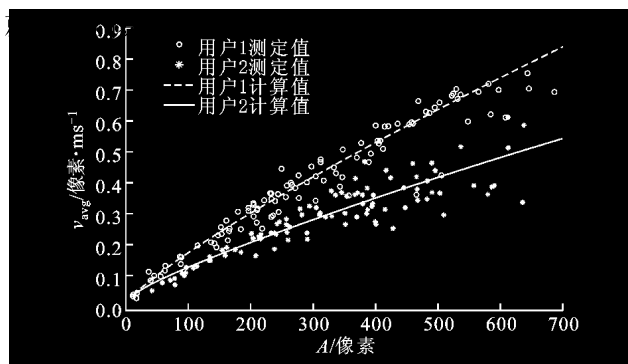


图4 平均移动速度与距离的关系

(4)移动中速度的微结构.不同用户在鼠标移动过程中的速度变化微结构如图6所示.从图中可以看出:在一个用户的情况下,鼠标移动速度的总体趋势是先增后减,其加速度的变化是先正向增大后减小,然后负向增大,最后减为0值;从不同用户的对比来看,瞬时速度的最大值及到达最大值时的距离或时间各不相同,这充分体现出了用户固有的生理特征.

采集到的数据经过操作切分和特征提取,将成为定义中的每组34维的特征量,具体构成包括:8维事件频率分布;1维静止时间占空比;5维单击时间间隔,即单击时间间隔的均值、方差、最大值、最小值、极差;20维双击时间间隔,即双击时间间隔的总和及内部3个时间间隔的均值、方差、最大值、最小值、极差.

为了挖掘用户鼠标行为模式的本征维数,应对数据进行降维、去噪处理,将高维特征空间数据映射到低维空间,并保持源数据的某些拓扑结构不变.

首先,构造邻近图:对整个数据点集定义图 G .如果点 i 和点 j 的距离 $d_x(i,j)$ 小于 ϵ ,或点 i 是点 j 的 K 个邻近点之一,连接点 i 和点 j ,使边界的距离与 $d_x(i,j)$ 相等.

其次,计算最短路径:①如果点 i 和点 j 由边界

线连接,初始化 $d_G(i, j) = d_x(i, j)$, 否则令 $d_G(i, j) = \infty$; ②轮流对点 k 进行变换, 用 $\min\{d_G(i, j), d_G(i, k) + d_G(k, j)\}$ 替代 $d_G(i, j)$. 最后得到的矩阵 $\mathbf{d}_G = \{d_G(i, j)\}$, 将包含图 G 所有点之间的最短路径距离.

再次,构造 d 维嵌入: ①令 λ_p 作为矩阵 $\tau(\mathbf{d}_G)$ 的第 p 个特征值(按降序排列), 则 v_p^i 为第 p 个特征向量的第 i 个分量; ②将 d 维坐标向量 $\mathbf{y}_i$ 的第 p 个分量置为 $(\lambda_p v_p^i)^{1/2}$.

根据剩余方差 $E = \|\tau(\mathbf{d}_G) - \tau(\mathbf{d}_Y)\|_{L^2}$ 的大小可确定算法中的邻近点的 K 值和本征维数 d , 这样经过映射就得到了用户在低维特征空间中的数据. 那么, 经过运算便将 34 维的特征空间映射到了 3 维特征空间. 将经过降维处理的低维空间特征数据作为 BP 神经网络的输入数据, 由此构建出基于 BP 神经网络的身份识别模型.

将 10 个用户的鼠标行为数据进行训练和测试, 求其误识率、拒识率的平均值并与文献[4]对比, 结果如表 1 所示.

表 1 身份识别结果

用户鼠标身份识别结果		用户击键身份识别结果	
误识率/%	拒识率/%	误识率/%	拒识率/%
0.48	2.86	7.36	3.77

从表 1 可以看出, 用户在使用鼠标的过程中展示了更为丰富的特征, 较传统击键动力学模型具有更好的身份识别效果.

4 结束语

本文从交互层和生理层对计算机用户的鼠标动力学模型进行了研究, 并在此基础上设计、实现了实时身份监控系统. 对不同用户的鼠标使用行为进行了实验和分析, 结果表明不同用户的鼠标行为特征存在着显著的差异, 同时验证了鼠标动力学模型的用户身份的可区分性.

参考文献:

- [1] O'GORMAN L. Comparing passwords, tokens, and biometrics for user authentication [J]. Proceedings of the IEEE, 2003, 91(12):2021-2040.
- [2] BLEHA S, SLIVINSKY C, HUSSIEN B. Computer-access security systems using keystroke dynamics [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1990, 12(12):1217-1222.
- [3] OBAIDAT M S, SADOON B. Verification of computer users using keystroke dynamics [J]. IEEE Transactions on System, Man, Cybernetics, 1997, 27(2):261-269.
- [4] 高艳, 管晓宏, 孙国基, 等. 基于实时击键序列的主机入侵检测 [J]. 计算机学报, 2004, 27(3):336-400. GAO Yan, GUAN Xiaohong, SUN Guoji, et al. The host-based intrusion detection based on real time keystroke sequences [J]. Chinese Journal of Computers, 2004, 27(3):336-400.
- [5] 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. New York, USA: ACM, 2004: 1-8.
- [6] GAMBOA H, FRED A. A behavioral biometric system based on human computer interaction [EB/OL]. [2006-10-11]. <http://www.lx.it.pt/~afred/anawebit/articles/AFredSPIE2004.pdf>.
- [7] AHMED A A E, TRAORE I. Anomaly intrusion detection based on biometrics [C] // Proceedings of IEEE Information Assurance Workshop. Piscataway, NJ, USA: IEEE, 2005:452-453.
- [8] AHMED A A E, TRAORE I. Detecting computer intrusions using behavioral biometrics [EB/OL]. [2006-08-19]. <http://www.lib.unb.ca/Texts/PST/2005/pdf/ahmed.pdf>.
- [9] GARG A, SANKARANARAYANAN V, UPADH-YAYA S, et al. USim: a user behavior simulation framework for training and testing IDSes in GUI based systems [C] // Proceedings of 39th Annual Simulation Symposium. Los Alamitos, CA, USA: IEEE Computer Society, 2006:196-203.
- [10] 桑应朋. 基于计算机击键动力学的用户身份鉴别 [D]. 成都: 西南交通大学信息科学与技术学院, 2004.
- [11] FITTS P M. The information capacity of the human motor system in controlling the amplitude of movement [J]. Journal of Experimental Psychology, 1954, 47(6):381-391.
- [12] MITHAL A K, DOUGLAS S A. Differences in movement microstructure of the mouse and the finger-controlled isometric joystick [C] // Proceedings of the SIGCHI Conference on Human Factors in Computing Systems: Common Ground. New York, USA: ACM, 1996:300-307.
- [13] PLAMONDON R, FENG C, WOCH A. A kinematic theory of rapid human movement [J]. Biological Cybernetics, 2003, 89(2):126-138.

(编辑 苗凌)