Project Title:

Protecting Your Personal Device: Improving Mobile Authentication With Behavioral Biometrics

Project Objective:

As mobile device usage continues to increase, a secure and user-friendly means of authentication becomes necessary. Traditional methods such as passwords and PINs are susceptible to breaches and misuse. This project aims at utilizing behavioral biometrics-including typing speed, swipe patterns, and device handling characters-as a means to improve security in mobile authentication. Apart from classical techniques, behavioral biometrics comes in handy in adding on top of conventional techniques to provide the added security while still maintaining an easy way to use.

Project Background and Significance:

With ever-growing dependence on mobile applications in daily lives, secure user authentication has gained attention. Mobile devices provide access to sensitive information involving both personal and financial aspects. Traditional methods of authentication are not only penetrable, but are also weak in accurate authentication (Skalkos et al., 2021). These approaches are usually compromised in other ways, such as weak or not unique passwords, and phishing and social engineering attacks. Thus, the security gap is expanding and creates a situation where the need has been created for robust, innovative, and user-friendly solutions to protect user data without compromising convenience.

Unlike traditional biometrics, such as fingerprints or facial recognition, behavioral biometrics use the data that originate directly from the habitual actions of users: keystroke speed, swiping patterns, handling of the device, and pressure applied to the touch screen. These patterns are inherently difficult for attackers to replicate, thus giving an added layer of security. They can also run seamlessly in the background, which may offer them a less intrusive and more user-friendly way of authentication compared to the current alternatives (Buriro et al., 2018).

The main goal of this research is to develop how behavioral biometrics can be embedded into mobile applications to better achieve authentication security. The research will seek to investigate how well behavioral biometrics are capable of detecting unauthorized access attempts, whether they work on human subjects, and explore possible solutions to the challenges such as data privacy and accommodating the changes in user behavior over time.

The theoretical framework of this research relies primarily on concepts of human-computer interaction (HCI) and cyber security methodologies. HCI theory is basically about how to make systems that someone would want to use based on human behavior, making biometric authentication reasonable and not intrusive (Gupta et al., 2023). Cyber security frameworks, on the other hand, will lead to evaluating robustness and efficiency.

The results of this project will most likely advance the acceptance of behavioral biometrics within mobile authentication. If this integration succeeds, it will lower the dependence on traditional methods and allow for new and improved methods to take its place. Moreover, outcomes of this study will inform the application of behavioral biometrics more widely across domains, especially banking, health care, and e-commerce, where seamless secure access is of prime importance.

Research Methods:

The research process will follow a detailed, multi-phase methodology in the exploration of a behavioral biometric authentication system for mobile applications. The project will commence in May with an extensive literature review that serves to build a theoretical basis, pinpointing gaps in current authentication methods and best practices. In parallel, a prototype mobile application will be designed to collect user interaction data, such as typing speed, swipe gestures, and device handling. Dedicated volunteers from varying demographics will be recruited to guarantee a strong and fair sample of the data. Techniques will be applied to enhance reliability, such as noise removal and normalization.

During the whole of June and early July, machine learning models will be built and evaluated based on the dataset collected. Various algorithms, such as Random Forest, Support Vector Machines, and neural networks, would be compared for establishing an effective approach to ensuring correct and secure authentication. Performance assessment shall be done using performance metrics such as accuracy, precision, recall, and false acceptance/rejection rates. This is a crucial phase for validating that behavioral biometrics would work for the mobile authentication purpose.

There will be some usability testing done in late July at which the integration of mobile applications with the system would be evaluated. Participants would be provided access to the authentication system, after which they would express feedback through surveys and focus groups regarding ease of use, user satisfaction, and perceived security. With these insights, the final refinements will make sure the system is practical and secure enough to demand use.

The final stage would be synthesizing findings and results analysis and a clear comprehensive report write-up on research outcomes, limitations, and recommendations for future work in August. The timeline for the summer semester includes: May for literature review and data collection setup, June for data collection and preprocessing, July for model development, testing, and usability evaluation, and August for final analysis and reporting. This structured methodology would ensure that behavioral biometrics are explored to the fullest, especially in their ability to enhance security in mobile authentication.

Expected Outcome:

Following the completion of this research will be provided several tangible and eager deliveries. The first main deliverable will be a detailed research paper providing the methodology, finding, and implications of using behavioral biometrics in mobile authentication systems. This paper will

be considered for publication in academic journals in computer science and cyber security, the IEEE Transactions on Information Forensics and Security. A poster presentation will also be made for the UCF Showcase of Undergraduate Research Excellence (SURE), to disseminate the findings to the academic community. A white paper called a Summary of Research Outcomes will also be developed for industry folk and organizations interested in adopting newer authentication methods.

Finding the most impactful ways to distribute those results is part and parcel of how the project will ensure that it sees the light of day. Subsequently, the results would be presented in events of other undergraduate research, and also considered in professional conference areas related to cybersecurity or HCI. Special attention should be given to further engage the UCF community with hands-on workshops or guest lectures that will expose the implications of the research on securing personal data in an increasingly mobile-dependent society. Such an opportunity for harnessing will only promote collaboration, awareness, and further interest in behavioral biometrics.

The project will advance the horizon of authentication security by demonstrating whether behavioral biometrics are a feasible and effective method in mobile applications. Therein will be reviewed some literature on empirical indications of accuracy and reliability of such systems to detect unauthorized access during active usage, with minimum disturbance to the user. Add-on research perspectives include addressing privacy constraints and the adaptability of predictive models to the fluctuations of user behavior over time.

Meanwhile, for the UCF community, it will serve as an important learning experience and a foundation upon which innovation can be constructed further on. This will inspire students and faculty to think of applications of machine learning and biometrics in solving real-life security problems. Meanwhile, the findings could also give guidance for local businesses and organizations to start pursuing advanced authentication technologies to protect sensitive information. Overall, this project will change the impression on behavioral biometrics and their inner promise of redefining the convenient and secure user authentication process in the digital era.

Literature Review:

1. Sitová, Zdenka, et al. “HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users.” IEEE Transactions on Information Forensics and Security, vol. 11, no. 5, 2016, pp. 877-892. IEEE Xplore, https://ieeexplore.ieee.org/document/7349202/keywords#full-text-header
2. Buriro, Attaullah, et al. "AnswerAuth: A Bimodal Behavioral Biometric-Based User Authentication Scheme for Smartphones." Journal of Information Security and Applications, vol. 44, 2019, pp. 89-103. Elsevier, https://iris.unitn.it/bitstream/11572/228499/1/AnswerAuth-s2.0-S2214212618304435-main.pdf

3. Yang, Yafang, et al. "BehaveSense: Continuous Authentication for Security-Sensitive Mobile Apps Using Behavioral Biometrics." Ad Hoc Networks, vol. 84, 2019, pp. 9-18. Elsevier, https://www.sciencedirect.com/science/article/pii/S1570870518306899?via%3Dihub
4. Tumpa, Sanjida Nasreen, and Marina Gavrilova. "Linguistic Profiles in Biometric Security System for Online User Authentication." 2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC), 2020, pp. 1033-1038. IEEE, https://ieeexplore.ieee.org/document/9282937
5. Skalkos, Andreas, et al. "Users' Privacy Attitudes towards the Use of Behavioral Biometrics Continuous Authentication (BBCA) Technologies: A Protection Motivation Theory Approach." Journal of Cybersecurity and Privacy, vol. 1, no. 4, 2021, pp. 743–766. MDPI, https://www.proquest.com/docview/2655550469?pq-origsite=primo&sourcetype=Scholarly%20Journals
6. Gupta, Sandeep, et al. "A Survey of Human-Computer Interaction (HCI) & Natural Habits-Based Behavioral Biometric Modalities for User Recognition Schemes." Pattern Recognition, vol. 139, 2023, p. 109453. Elsevier, https://www.sciencedirect.com/science/article/pii/S003132032300153X?via%3Dihub

Preliminary Work and Experience:

My academic journey at UCF has laid a strong groundwork for my research on enhancing user authentication security through behavioral biometrics. I've taken relevant courses in computer science, machine learning, cybersecurity, and human-computer interaction. These classes have provided me with both the theoretical insights and practical abilities necessary to create secure, user-centered systems. My focus on human-computer interaction has been especially impactful, highlighting the need for intuitive and seamless user experiences, which is a key objective of this project. Beyond my coursework, I have gained practical experience in software development and data analysis. I've participated in projects that involved data collection, preprocessing, and applying machine learning algorithms, all of which are essential to this research. To prepare, I conducted a review of academic literature on behavioral biometrics and mobile authentication techniques. Additionally, I've investigated the tools and platforms required, including mobile app development environments and machine learning frameworks. These experiences combined emphasize my capability to tackle this project.

IRB/IACUC statement:

Since I will be conducting tests with human volunteers, this project will need IRB approval.

Budget:

Category	Description	Estimated Cost
Personnel	Compensation for participants (e.g., gift cards for volunteers to incentivize participation).	$400 ($20 per 20 participants)
Software Tools	Licensing fees for machine learning libraries, data analysis tools, or mobile app development software.	$150
Hardware	Purchase of smartphones or tablets for testing the prototype authentication system.	$600 (2 $300 devices)
Data Storage	Secure cloud storage or local server setup for collecting and processing user interaction data.	$100
Surveys and Usability Testing	Printing materials, survey software subscriptions, or focus group facilitation costs.	$50
Miscellaneous	General supplies (e.g., cables, chargers, stationery) and unforeseen expenses.	$50
Total		$1,350