Who You Are by way of What You Are: Behavioral Biometric Approaches to Authentication

Michael Karlesky, Napa Sae-Bae, Katherine Isbister, Nasir Memon
NYU Polytechnic School of Engineering
Five MetroTech Center
Brooklyn, New York, USA 11226
{michael.karlesky, nsb261, isbister, memon}@nyu.edu

ABSTRACT

We present our work in behavioral biometrics employed in the emerging contexts of gesture-based interfaces. We discuss novel approaches to authentication in signature, multi-touch gesture, and full body in-air gesture. Our work addresses security in these contexts not only in term of technical performance but also in terms of pleasurable interactions between user and system. We highlight opportunities to reframe security topics through ‘natural’ interactions. We also raise questions as to how to evaluate the usability of such approaches and how to incorporate these considerations into the evaluation of overall security.

1. MOTIVATIONS

Recent advances in user interface technology have remarkably transformed the way we interact with computing devices and the form factors of computing devices themselves. However, the change of user interaction interface and the usage pattern of these new devices have brought new security threats and usability issues as compared to traditional text password and token-based authentication. First, these devices are often used in a social context and in public spaces, and, in addition, users are surrounded by handheld recording devices and public surveillance. In such situations, the assumption that users can enter a password or other shared-secret credentials to the devices privately and securely is no longer guaranteed. Secondly, computing devices are no longer solely keyboard and mouse centric but employ other ‘natural’ user interfaces (NUI). As a result, input modalities are far less constrained and prescriptive than in previous generations, potentially reducing the usability of credential entry and simultaneously increasing opportunities for credential attacks. Finally, user demand and cost benefits of these NUI technologies are hastening their wide adoption while authentication schemes are yet being developed to meet both usability and security needs.

In response to these ongoing issues, we have worked to explore the possibilities of new interactive authentication mechanisms through two emerging interface technologies: multi-touch surfaces and depth-sensing cameras. We are particularly interested in designing mechanisms that can provide both intrinsic security and usability benefits to users. We have found that human movement affords a wealth of multidimensional data for use in authentication as well as a real opportunity to craft interactions that tap into the interrelation of body, affect, and cognition.

2. OUR WORK IN NOVEL BEHAVIORAL BIOMETRICS

2.1 Multi-touch Surfaces

Through multi-touch interfaces, we have conducted studies on two plausible biometric authentication alternatives matched to two different device form factors. These are biometric-rich multi-touch gestures for a large multi-touch surface, i.e., tablets and tables [4,5,6], and finger-drawn online signatures for smaller devices, i.e., smart phones [2,3]. The results from our studies have revealed several interesting findings about characteristics of the proposed authentication schemes. In particular, for multi-touch gestures, the experimental results from user feedback have revealed that their ease of use, pleasantness, excitement, and willingness to use were rated highly and were positively correlated with their respective biometric performance. In addition, the study has demonstrated that a user interface (UI) element like background images can help improve security and usability simultaneously. This is an encouraging result towards improving the security and usability tradeoff for an authentication mechanism. However, studies also revealed limitations with respect to verification performance and its degradation due to template aging issues that need to be overcome before moving forward on a deployment path. For online signatures, the experimental results on a new dataset collected from a 6-session experiment have demonstrated the effect of template aging towards verification performance degradation. They have also demonstrated that this problem can be alleviated by training a classifier with samples from multiple sessions and periodically updating the training samples to the most recent ones.

2.2 In-Air Gesture

We are currently implementing a multi-modal access control system to replace a traditional proximity card-based system at the entryway to a lab at our university [1]. The system uses a novel full body gesture matching technique as one of its authentication biometrics. Early testing results demonstrate that this full body gesture matching approach is able to discriminate among enrolled users and reject non-enrolled users with an effectiveness comparable to the traditional third-party face matching the system also employs. Matching in-air gestures increases the total amount of biometric information the system is able to process. However, gesture also communicates intent and provides users a sense of agency in unlocking the lab door. Further, we designed the system to support multiple gestures per user supporting different expressions of mood and use contexts consistent with behaviors observed in an initial Wizard of Oz-based design study. While the

Symposium on Usable Privacy and Security (SOUPS) 2014, July 9-11, 2014, Menlo Park, CA.

system is not yet complete, early feedback suggests that users find the system pleasurable to use. True performance, novelty effects, and secondary effects will be established in a forthcoming longitudinal study.

3. DISCUSSION POINTS: AIMS, BENEFITS, AND NEEDS

NUI interfaces provide a much higher dimensional data about user interaction, as compared to traditional keyboard input or access control tokens. On these systems, many behavioral biometric modalities have been proposed and studied. However, while some of the work has been on extracting biometric information from usual interactions, e.g, the slide to unlock gesture on iPhones and the pattern unlock on Android phones, seemingly very little work has been done on designing authentication mechanisms such that the authentication interaction itself can extract rich biometric information effectively. In other words, we believe that the ability of these emerging interfaces to detect large amounts of user interaction information has created a unique opportunity to redesign and develop authentication mechanisms that are inherently secure and usable, and even pleasurable. As such, this represents a departure from the usual discussion on authentication around a tradeoff between security and usability.

However, the most challenging question is that of designing usability studies that can effectively evaluate the authentication interaction. Similarly, establishing effectiveness in terms of user adoption is a challenge not yet met in security research. In typical studies, users are only asked to compare and rate different usability measurements of mutually exclusive authentication mechanisms. However, in reality, many users simply ignore these mechanisms leaving their devices unprotected or circumventing access control means entirely. In addition, the use of NUIs all but guarantees some form of biometric sensing for authentication. Given that biometric sensing cannot be perfectly executed, the questions of whether pleasurable interactions alter the relationship of users and authentication means to yield forgiveness on the part of users or whether pleasurable interactions limit circumvention are perhaps well-worth pursuing. We do hope that the SOUPS community can contribute much to identifying relevant work in this vein.

4. ACKNOWLEDGMENTS

This work was supported in part by the NSF (under grant 0966187). The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of any of the sponsors.

5. REFERENCES

[1] Karlesky, M., Melcer, E. and Isbister, K., 2013. Open sesame: re-envisioning the design of a gesture-based access control system. *CHI'13 Extended Abstracts on Human Factors in Computing Systems*, pp.1167–1172.

[2] Sae-Bae, N. and Memon, N., 2013. A simple and effective method for online signature verification. In Biometrics Special Interest Group (BIOSIG), 2013 International Conference of the. pp. 1–12.

[3] Sae-Bae, N. and Memon, N., 2014. Online Signature Verification on Mobile Devices. *Information Forensics and Security, IEEE Transactions on*, 9(6), pp.933–947.

[4] Sae-Bae, N., Ahmed, K., Isbister, K. and Memon, N., 2012a. Biometric-rich gestures: a novel approach to authentication on multi-touch devices. *CHI '12: Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems*, pp.977–986.

[5] Sae-Bae, N., Memon, N. and Isbister, K., 2012b. Investigating multi-touch gestures as a novel biometric modality. In Biometrics: Theory, Applications and Systems (BTAS), 2012 IEEE Fifth International Conference on. pp. 156–161.

[6] Sae-Bae, N., Memon, N., Isbister, K. and Ahmed, K., 2014. Multitouch Gesture-Based Authentication. *Information Forensics and Security, IEEE Transactions on*, 9(4), pp.568–582.