AirAuth: A Biometric Authentication System using In-Air Hand Gestures

Anonymized for Review
AuthorCo, Inc.
123 Author Ave.
Authortown, PA 54321 USA
author1@anotherco.com

Abstract
AirAuth is a biometric authentication technique that uses in-air hand gestures to authenticate users tracked through a short-range depth sensor. Our method tracks multiple distinct points on the user's hand simultaneously that act as a biometric to further enhance security. We describe the details of our mobile demonstrator that will give Interactivity attendees an opportunity to enroll and verify our system's authentication method. We also wish to encourage users to design their own gestures for use with the system. Apart from engaging with the CHI community, a demonstration of AirAuth would also yield useful gesture data input by the attendees which we intend to use to further improve the prototype and, more importantly, make available publicly as a resource for further research into gesture-based user interfaces.

Author Keywords
in-air gestures, authentication, shoulder surfing, user experience; acceptability, biometric

ACM Classification Keywords
H.5.m [Information interfaces and presentation (e.g., HCI)]: Miscellaneous.

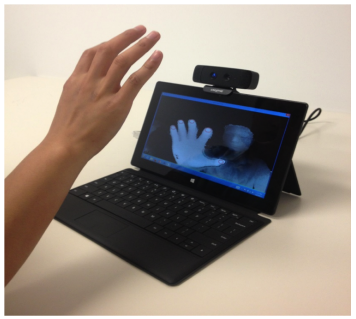

Figure 1: The mobile AirAuth prototype consists of a tablet PC and a short-range depth camera.

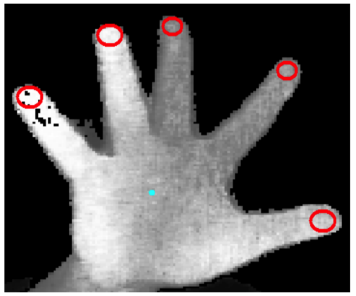

Figure 2: AirAuth tracks the 3D locations of the user's fingertips as well as the hand center as feature data for authentication.

Introduction

A growing number of users store and manipulate important and sensitive information online, on their personal computers and mobile devices. As such, finding methods of secure and easy-to-use authentication is of increasing importance, since tradeoffs exist between the users' desire for security and the compromises in user experience they are willing to take [4].

At present, passwords and PINs are the most widely-used authentication methods for gaining access to PCs, mobile devices and online accounts, and they are well-understood by users.

However, for these authentication methods there are usability tradeoffs—although a large number of complex passwords is preferred for users having multiple accounts, users typically resort to using variants of a simple *base* password, which puts users at high risk if it is compromised [7].

On mobile devices, traditional password entry can be prone to *shoulder-surfing attacks* [6] by observation of the password entry or to *smudge attacks* [1], by observing the residue of a touch-based password or stroke gesture entry.

As a possible solution to the previously mentioned problems, we present AirAuth, a biometric authentication method that uses in-air hand gestures to authenticate the user. Instead of relying solely on the user's knowledge of a secret, biometric authentication systems, such as AirAuth can enhance security by directly using the distinct physical features of a the legitimate user and analyzing behavioral traits of the legitimate user during the authentication process. As biometrics, AirAuth uses distinct points on the user's hands (finger tip locations and hand center) as well as an (implicit) analysis of the user's movement style obtained from entered gestures.

We also believe that authentication interfaces like AirAuth have usability advantages. The additional biometric allows the users to use a less complex secret, which can basically be an everyday gesture they perform, such as their signature in the air. Thus, it is reasonable to assume that the mental burden of password-based gestures is reduced. Because of the lower mental burden, and the activity-based nature of authentication through a gesture, we also believe that authenticating in this way is more engaging than traditional authentication methods.

The AirAuth Demonstrator

AirAuth can be deployed on mobile as well as fixed devices. In the following, we describe our mobile demonstrator which suitable for use at an Interactivity.

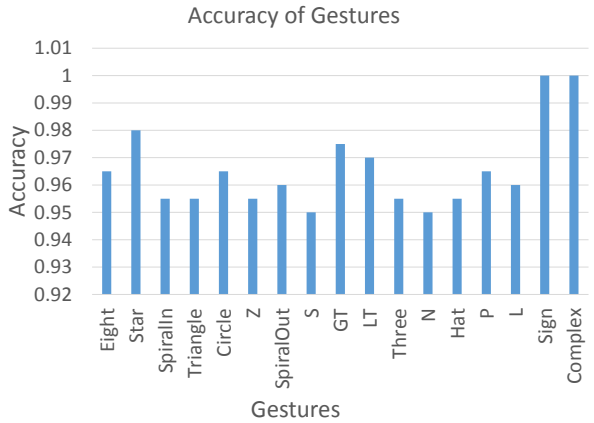

Figure 3: Achieved accuracy of AirAuth in a user study with 15 participants. Note that the user-defined gestures (*sign* and *complex*) achieved 100% accuracy.

Overview
The hardware for the AirAuth demonstrator consists of a small tablet computer and a short range depth camera (Figure 1). The tablet runs the AirAuth software.

Attendees of the Interactivity will be able to enroll with the system by entering an in-air gesture of their design three times and thus create their own ID to log on to the system. Other attendees will be able to watch legitimate users entering their gesture and try to forge them, and legitimate users will be able to login to the system at a later time to verify that the system can authenticate them even with a large database of users.

In a user study we conducted with 15 participants, our system obtained a perfect (100%) accuracy score for user-defined gestures (Figure 3 *sign* and *complex*). We hope that attendees will enjoy interacting with out system due to the high accuracy, which leads to a low occurrence of false rejects during authentication.

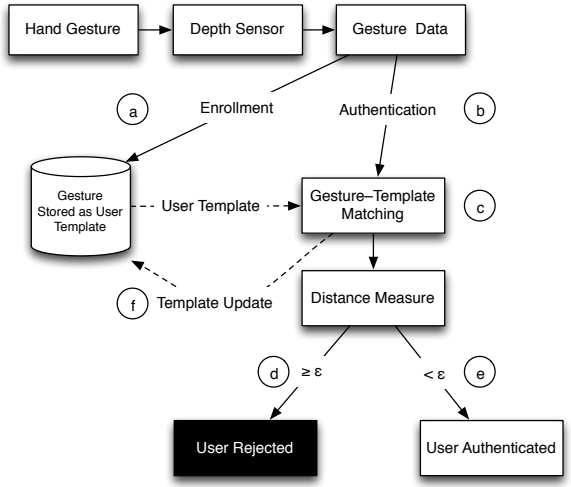

Figure 4: A conceptual overview of the AirAuth software implementation. Note the two main stages of the authentication system—enrollment (a) and authentication (b).

Implementation Details
The prototype software is implemented in C++. We use a Creative Senz3D short range depth camera to obtain a depth image of the user's hand while the user is entering a gesture. We use the Intel Perceptual Computing SDK[1] to extract the 3D location of the user's finger tips as well as the hand center point (Figure 2). The spatial arrangement of these six points are, effectively, a biometric that measures characteristic details of the user's hands. Gestures are preprocessed by normalizing their values and mean-shifting them to be able to use them as a template during gesture recognition. As a matching algorithm, we use Dynamic Time Warping (DTW) [5]. Figure 4 shows a conceptual overview of the AirAuth system.

Gestures are delimited based on passing a threshold distance from the device's screen. When the user's hand passes the threshold distance, the system starts recording the gesture data. When the user's hand is retracted past the threshold or ceases to move, recording stops.

Scientific Benefits of a Public Demonstration

Apart from being able to present AirAuth to the CHI community, we think that the opportunity to demo it at the CHI interactivity will benefit further research into our technique:

(1) by allowing the system to be used in field conditions, we gain the opportunity to study its performance under conditions that are significantly more variable than in the

[1] http://software.intel.com/en-us/vcsource/tools/perceptual-computing-sdk

lab; (2) at the Interactivity we hope to be able to collect gesture input from a larger number of participants than we were able to in our lab, which will give us an interesting insight into AirAuth's robustness as the user base grows; (3) we hope to obtain further qualitative feedback about the usage experience of our system either formally or informally; (4) attendees will also be able to sketch out their gestures on the touch screen—together with the recorded in-air gesture entries, we hope to obtain a useful database of labeled multi-point in-air hand gestures, that we will release publicly.

We hope that this database will represent a useful contribution to researchers in gesture-based interfaces or machine learning.

Target Audience and Relevance

By demonstrating our system, we aim to reach out and foster discussion with CHI attendees that are interested in novel user interface techniques (such as gestural input) as well as persons interested in usable security research.

We think AirAuth is highly relevant as a possible solution to the problem of improving the usability of authentication. We believe our method could enable casual authentication on many devices, with a low mental burden due to the biometric aspects.

Also, AirAuth is relevant to authentication on mobile devices, since robust and usable authentication methods for mobile devices still need to be improved. For instance, the fingerprint scanner on the most recent iPhone has been compromised within a week of the release of that device [2]. Furthermore, with the possibility of depth sensors being incorporated on future mobile devices [3], it may be easy to integrate AirAuth as an authentication mechanism for those devices.

References

[1] Aviv, A. J., Gibson, K., Mossop, E., Blaze, M., and Smith, J. M. Smudge attacks on smartphone touch screens. In *Proceedings of the 4th USENIX conference on Offensive technologies*, USENIX Association (2010), 1–7.

[2] Chaos Computer Club (CCC). Chaos computer club breaks apple touchid. http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid, 2013.

[3] Ehrenberg, R. The digital camera revolution: Instead of imitating film counterparts, new technologies work with light in creative ways. *Science News 181*, 2 (2012), 22–25.

[4] Kainda, R., Flechais, I., and Roscoe, W. A. Security and usability: Analysis and evaluation. In *Availability, Reliability, and Security, 2010. ARES'10 International Conference on*, IEEE (2010), 275–282.

[5] Sakoe, H., and Chiba, S. Dynamic programming algorithm optimization for spoken word recognition. *IEEE Transactions on Acoustics, Speech and Signal Processing 26*, 1 (1978), 43–49.

[6] Tari, F., Ozok, A., and Holden, S. H. A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. In *Proceedings of the second symposium on Usable privacy and security*, ACM (2006), 56–66.

[7] von Zezschwitz, E., De Luca, A., and Hussmann, H. Survival of the shortest: A retrospective analysis of influencing factors on password composition. In *Human-Computer Interaction–INTERACT 2013*. Springer, 2013, 460–467.