Incorporating Biometric and Two-Factor Authentication into User Authentication

Kathy Wang
Cornell University
Ithaca, NY 14850, USA
kw496@cornell.edu

Lionel Chambers
Cornell University
Ithaca, NY 14850, USA
lzc4@cornell.edu

Kun Bi
Cornell University
Ithaca, NY 14850, USA
kb622@gmail.com

Abstract
The problem with user authentication revolves around finding a medium between security and usability. While some methods are highly secure, they can be very complicated to use. In contrast, other methods are extremely convenient, yet completely insecure. We thus implemented this project to design a user-centric solution that strikes a balance between security and convenience. Our low-fidelity mockup asked users to choose two out of three forms of recognition. Moreover, we identified several areas of improvement, including ambiguous progress indication, fingerprint scanner reachability and accessibility, and unlocked time frame. Ultimately, we chose to narrow down to two forms of recognition: facial and fingerprint recognition. Moreover, we incorporated several new features to address the findings from user testing. Because the two biometric authentications systems occur simultaneously, our final design improves security without compromising usability.

Author Keywords
Usable Security; Graphical User Authentication; Biometric Identification; Two-Factor Authentication; Facial Recognition System; Fingerprint Recognition.

Figure 1. A Nymi band that is based on an individual's ECG.

ACM Classification Keywords

H.5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous

Introduction

There exists a large amount of data in the world today. Some of that data is public, while other parts of it are private and need to be protected. Herein lays the need for authentication systems.

One of the most common authentication systems is the password. Passwords are commonly used to protect personal accounts, devices, and services. However, having a password requires memorization. People often write their passwords down on post-it notes, or create a running list of them in a notebook or on their phone [5]. Such records can easily be found, thereby defeating the purpose of having a password in the first place.

The problem with user authentication is that the characteristics of security and usability seem to be mutually exclusive [2]. It appears that increasing security inevitably means decreasing usability, and vice versa. For instance, passwords have relatively low security, but because they are convenient and easy to implement, they are commonly used. On the other hand, a more secure system, like two-factor authentication (2FA), might be more secure, but users are less likely to use them, as seen in Google's and Yahoo's difficulty with introducing 2FA on their own platforms.

While striking a balance between security and usability may be difficult, we aim to offer a solution that shows that the two factors are not necessarily mutually exclusive. In order to do so, we underwent research, ideated solutions, created a low-fidelity mockup, conducted user testing, and designed a final prototype. This paper will thus discuss relevant technologies, present the findings from our user testing, and justify the final design based on those findings.

Related Work

2FA

Recently, more and more platforms have started using two-factor authentication (2FA). 2FA essentially incorporates another layer of authentication for both the user and the service provider [6]. For instance, the user may be prompted to enter a password, and then asked to input a code via a confirmation text. While this user authentication method creates an added layer of security, it also lowers usability, as it requires users to undergo an extra step, as well as potentially having to carry an extra device.

Biometric Authentication

FINGERPRINT, VOICE, AND FACIAL

Many companies have started to implement biometric authentication, which includes facial recognition, voice recognition, and fingerprint identification [3]. Biometric authentication has been well-received because of its combination of security, convenience, and accuracy. Some of the most popular usages of this form of authentication can be seen in smartphones, where users can unlock their phone with via fingerprint recognition or facial recognition.

ELECTROCARDIOGRAM (ECG)

Another form of biometric authentication is via a user's electrocardiogram (ECG), as seen in the Nymi Band (Fig. 1) [1]. Each individual's ECG is unique, thereby

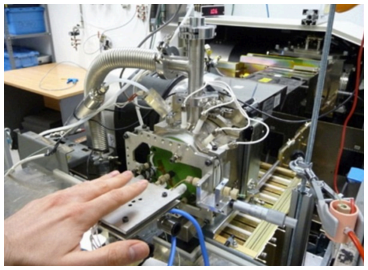

Figure 2. Odor-based technology is still a work in progress.

allowing the ECG to be used as an identifier. As long as the user is wearing the band (and allowing the band to detect their heart activity, and record their ECG), authentication is always on [1]. While this system allows for a high degree of security, it lacks in usability in that it requires an additional device for the user.

SCENT

On top of fingerprint, voice, facial, and ECG recognition, we can also detect individuals by their scent [4]. While odor-based technology is not fully developed yet, it has potential (Fig. 2). While the usability of such a system would be high, as emitting odor does not require any action on the user's part, the security of the system may face issues, as odor-based technology is currently only 85% accurate [4].

User Testing

Low-Fidelity Prototype

Based off our research, we decided to combine 2FA and biometric authentication. We narrowed down from all biometric authentication methods to fingerprint, voice, and facial recognition as these three methods strike the best balance between security and usability out of all the other biometric authentication alternatives. While we hypothesized that users would prefer fingerprint and facial recognition due to their lack of public disturbance, we decided to incorporate all three recognition systems, and let users inform us of their preferences (Fig. 3, right). With these design decisions in mind, we created

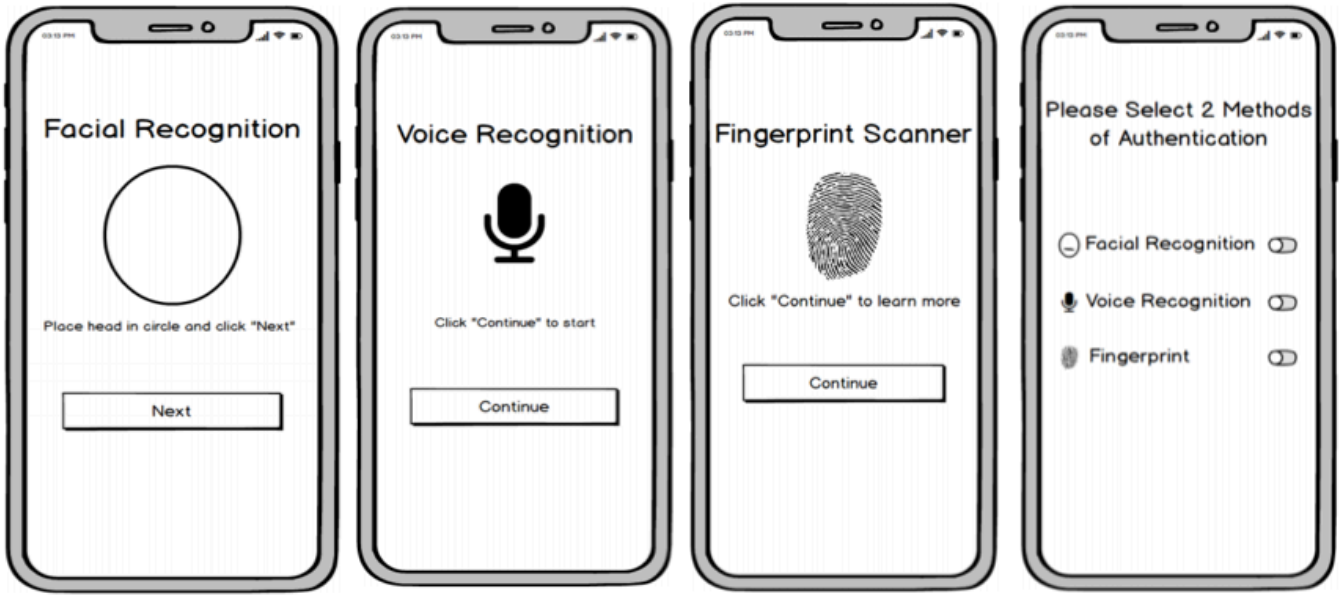

Figure 3. Four screens of the setup process in our low-fidelity prototype: Initial screens of facial recognition (left), voice recognition (middle left), and fingerprint (middle right) setup, and the selection of two methods of authentication screen (right).

a low-fidelity prototype via Balsamiq to utilize in user testing (Fig. 3).

Participants
We recruited five individuals (3 males, 2 females) aged between 20 and 30. All individuals were college-educated, and currently own a smartphone. One individual owned an Android, while the other four individuals used iPhones. Some participants had not had experience with a voice recognition system.

Interview
We asked each participant to undergo our setup, which included the setting up of voice recognition, facial recognition, and fingerprint recognition. At the end of the process, a screen prompts users to choose two of the three systems for future use. During the interview, we asked users seven questions: **1.** *"Why did you choose these two authentication methods?"* **2.** *"Why did you leave the other one out?"* **3.** *Do you think this setup process was tedious?"* **4.** *"Do you think this function is easy to use?"* **5.** *Would you be okay going through this process every time you unlock your phone?"* **6.** *"Do you feel more secure using this process?"* **7.** *"Are there any other improvements that you think can be made?*

The first two questions were used to help us narrow down our biometric authentication methods. The rest of the questions were used to measure the security and usability of our prototype.

Final Design

Using the findings from our user testing, we designed our final product via Adobe XD. We found that the majority of users chose facial and fingerprint recognition, and left out voice recognition. The rationale behind this was that a voice system is personally inconvenient because of its potential to create a public disturbance (*"I need to talk. It is not suitable in public. Everyone would know."*). Thus, in the final design, we only used facial and fingerprint recognition ((See full design at: https://xd.adobe.com/view/48fa1f48-b851-4746-878f-0b88435b7eb2/?fullscreen).

The other benefit of using facial and fingerprint recognition is that they can occur simultaneously. Thus, unlike in normal 2FA authentication methods, the user does not have to sacrifice time in order to increase security.

The final design also incorporates a progress bar, as one user pointed toward the lack of progress indication (*"I hate to do these steps without knowing when it ends"*) (Fig. 4, left).

Moreover, while we originally had the fingerprint scanner in the back of the phone to increase accessibility, we ended up moving it to the front, as a user brought up the inconvenience of reaching behind the phone to unlock it while one is watching videos (Fig. 4, left). We also incorporated the option to add multiple fingerprint IDs in order to accommodate for the same instance—a user may not be able to position their finger in the same way when their phone is propped up (Fig. 4, middle left, middle right).

The final design also includes a screen in which the user can choose how long they would like the phone to remain unlocked before they must go through the user authentication. A user brought up the inconvenience of undergoing authentication every time they want to

Figure 4. Four screens from our final design: Instructions for fingerprint setup (left), prompt for adding more fingers (middle left), record of added fingers (middle right), and unlock time settings (right).

access their phone (Fig. 4, right). While one can currently change the settings on iPhone, it is difficult to find. Thus, we

incorporated the option to keep the phone unlocked in the setup process to allow for greater convenience for users.

A final design consideration involved the scenario of using one's phone while driving. The user brought up the potential inconvenience of having to undergo both fingerprint scanning and facial recognition while on the road. While we considered adding a feature that would include a driving mode (pairing facial and voice recognition) and a normal mode (pairing facial and fingerprint recognition), we ultimately decided against it. We decided that a user should not be using their phone while driving. If they are using a navigation app, there is no need to unlock the phone, as the app usually remains on the entire time. Thus, the inconvenience of the 2FA biometric authentication system in a driving scenario actually doubles as a safety precaution—because the app is inconvenient to use while driving, drivers will be less likely to use the phone and more likely to focus on driving.

Conclusion

This paper addressed the issues behind current authentication systems, specifically the apparent mutual exclusivity of security and usability. In past authentication methods, it appears that one must sacrifice security for the sake of usability, or vice versa. However, as seen in our final design, this is not necessarily true. Security does not have to be increased at the expense of usability.

Facial recognition and fingerprint scanning occur simultaneously in our design. Because the user is likely to have their finger on and their eyes directed toward their phone, the authentication systems do not require the user to go out of their way. In this way, the user is not sacrificing usability at the cost of added security. Thus, our design shows that it is possible to maintain usability and increase security at the same time.

Acknowledgements

We would like to thank all the volunteers who took the time to participate in our study. We would also like to thank our professor who guided us through the study.

References

1. 2018. Nymi. Nymi Band. https://nymi.com/product_overview.
2. BETTS, G. 2016. CO.DESIGN. Security Vs. UX: How to reconcile one of the biggest challenges in interface design. https://www.fastcodesign.com/3059293/security-vs-ux-how-to-reconcile-one-of-the-biggest-challenges-in-interface-design.
3. COX, S. 2017. Forbes. Biometrics: a stepping-stone to eliminating the password forever. https://www.forbes.com/sites/forbestechcouncil/2017/09/13/biometrics-a-stepping-stone-to-eliminating-the-password-forever/#610a335d21db.
4. EGLINTON, J. 2016. LinkedIn. Smell you later: scent as authentication. https://www.linkedin.com/pulse/smell-you-later-scent-authentication-james-eglinton.
5. KOBIE, N. 2018. Security v usability: cracking the workplace password problem. The Guardian. https://www.theguardian.com/media-network/2015/oct/27/password-security-usability-workplace-problem.
6. THOMAS, D. 2016. Smashing Magazine. The current state of authentication: we have a password problem. https://www.smashingmagazine.com/2016/06/the-current-state-of-authentication-we-have-a-password-problem.