“I...Got my Nose-Print. But it Wasn’t Accurate”: How People with Upper Extremity Impairment Authenticate on their Personal Computing Devices

Brittany Lewis
bflewis@uri.edu
The University of Rhode Island
Kingston, Rhode Island, USA

Krishna Venkatasubramanian
krish@uri.edu
The University of Rhode Island
Kingston, Rhode Island, USA

ABSTRACT

Authentication has become increasingly ubiquitous for controlling access to personal computing devices (e.g., laptops, tablets, and smartphones). In this paper, we aim to understand the authentication process used by people with *upper extremity impairment (UEI)*. A person with UEI lacks range of motion, strength, endurance, speed, and/or accuracy associated with arms, hands, or fingers. To this end, we conducted semi-structured interviews with eight (8) adults with UEI about their use of authentication for their personal computing devices. We found that our participants primarily use passwords and PINs as a verification credential during authentication. We found the process of authentication to have several accessibility issues for our participants. Consequently, our participants implemented a variety of workarounds that prioritized usability over security throughout the authentication process. Based on these findings, we present six broad subareas of research that should be explored in order to create more accessible authentication for people with UEI.

CCS CONCEPTS

• **Human-centered computing** → **Accessibility**; • **Security and privacy** → **Usability in security and privacy**; • **Social and professional topics** → People with disabilities.

KEYWORDS

authentication, upper extremity impairment, personal computing devices

ACM Reference Format:
Brittany Lewis and Krishna Venkatasubramanian. 2021. “I...Got my Nose-Print. But it Wasn’t Accurate”: How People with Upper Extremity Impairment Authenticate on their Personal Computing Devices. In *CHI ’21: The ACM CHI Conference on Human Factors in Computing Systems, May 28-13, 2021, Yokohama, Japan.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/1122445.1122456

1 INTRODUCTION

Current ways of *authenticating* on personal computing devices typically require users to perform complex actions with their arms, hands, and fingers. Common examples include typing complex passwords or positioning one’s face in front of a camera accurately for facial recognition. This need for dexterous use of one’s arms, hands, and fingers during the authentication process creates barriers for people with **upper extremity impairment (UEI)** [1] [41].

Authentication is the process of proving one’s identity to a personal computing device. Broadly speaking, authentication has three main stages: *setup* where one initializes the personal computing device and registers a *credential* (e.g., a password or a biometric); *credential verification* where a fresh credential is presented (e.g., typing a password or presenting a biometric) and compared to the registered credential from the setup stage to verify the user’s identity; and *failure resolution* that is invoked only if the credential verification fails to match the fresh credential with the registered credential (e.g., from a mistyped password or inadequate biometric measurement) and provides additional means to authenticate successfully.

In this paper we aim to explore the use of authentication on personal computing devices (referred to as *devices*, for brevity, going forward) by people with UEI. The **goals** of this study are to determine: (1) how and why people with UEI used authentication on their devices and (2) the nature of the barriers they encountered during the authentication process (if any) and how they work around those barriers (if at all).

To answer these questions we conducted a series of semi-structured interviews with eight (8) adults with UEI. These interviews provided us with critical insight into the authentication use by people with UEI and allowed us to make several interesting observations. We found our participants extensively used passwords/PINs as the primary form of credential during authentication. Further, we found our participants faced barriers at all three stages of the larger authentication process and not just at the credential verification stage while entering a password or presenting a biometric. Depending on the type/severity of their impairment, available devices, and computing needs, our participants used a wide range

CHI ’21, May 28-13, 2021, Yokohama, Japan

ACM ISBN 978-1-4503-XXXX-X/18/06…$15.00
https://doi.org/10.1145/1122445.1122456

[1] People with *upper extremity impairment (UEI)* experience reduced range of motion, strength, endurance, speed, and/or accuracy associated with movement in the shoulders, upper arms, forearms, hands, and/or fingers. UEI manifests in people for a variety of reasons, including traumatic injuries (e.g., spinal cord injuries), degenerative conditions (e.g., osteoarthritis,) and movement disorders (e.g., cerebral palsy) [89]. It presents itself at different levels of severity ranging from a lack of fine motor control to a complete inability to use one’s arms [89]. Over 20 million people in the US alone have conditions that can lead to UEI [87]

of workarounds to overcome the barriers they face with authentication. These workarounds typically prioritize usability over the security that authentication provides. In this paper, we analyze the significance of these findings. Specifically, we call for further research in six broad areas to foster an accessible authentication experience for people with UEI.

2 RELATED WORK

To contextualize our work, we reviewed some of the research done with respect to authentication and people with disabilities. This research can be divided into three categories: evaluation of existing credential verification methods during authentication, novel methods for the credential verification stage of the authentication process, and improving the accessibility of text entry.

Evaluation of existing credential verification methods during authentication. As established in [10], research into authentication for people with motor impairments has thus far been limited. Only a few research efforts have investigated elements of the authentication process for people with UEI [17, 37, 41, 75, 84]. In [37], the author discussed password-based and PIN-based credential verification. The author described the difficulties these credential verification methods would most likely cause for people with disabilities (including those with UEI). However, the author does not directly engage with any participants with disabilities for this work. In [17] the authors performed a quantitative evaluation of how people with various disabilities used facial recognition, PIN entry, voice recognition, pattern-based graphical passwords, and fingerprint recognition. While the authors worked primarily with people with cognitive disabilities, a few of the participants had motor disabilities and visual impairments. Their results emphasized the difficulty for their participants in using authentication. However, the paper did not describe the use of authentication by people with UEI in any significant detail. In [84], the authors performed a qualitative study of password sharing (including ATM PINs) between people with disabilities and their caregivers in rural Australia. The authors described how sharing of passwords is essential for people with disabilities to get goods and services. In [41] the authors interviewed participants with disabilities, including those with motor disabilities, on their experience with using various, ubiquitous sensing technologies. A part of this work did discuss difficulties that people with disabilities have with biometrics. However, because this work was focused on sensing infrastructure, it was limited in its analysis of the interaction of people with motor disabilities with the larger authentication process. Finally, in [75], the authors used three fictional examples of older adults to critically examine authentication solutions. Since older adults often have reduced motor function or physical disabilities, there is mention of UEI in the form of one example of an older adult with arthritis. This work, however, mostly focuses on cognitive impairments. In addition, the authors used fictional examples rather than conducting interviews with people with disabilities as we do in this work.

Novel credential and credential verification in the authentication process. Recent years have also seen the use of a variety of new credentials and their verification for people with disabilities. Most of this work has been focused on people with visual impairments [8, 12, 14, 19, 24, 33, 50, 72, 80, 91] or people with cognitive impairments (e.g., Down syndrome) [36, 58]. Some works have focused on people with motor disabilities. These include the use of new credentials such as voice trait [40], cardiac signal [55, 83], and QR-codes [23] as well as new credential entry methods via password dictation [23, 34, 97] and wearables [30].

Our findings in this paper complement these previous findings. In fact, we are able to look at the entire authentication process and not just credential verification stage, which has been the focus of most past works on authentication. Thus, we can provide a more detailed understanding of how the typical authentication process on personal computing devices presents barriers for people with UEI. We hope that our work will help to inform the design of a better authentication process for people with UEI.

Improving the accessibility of text entry. In addition to works focused specifically on authentication, some forms of authentication credentials such as passwords and PINs involve entering text during the authentication process. There have been numerous works on improving text entry for people with UEI including designing novel AT [3, 4, 7, 9, 13, 20, 22, 28, 38, 39, 49, 60–62, 66, 68–71, 73, 76–78, 95, 96], changes to text entry interfaces [15, 42], dynamic user interface design [35], and studies to understand and improve touchscreen interactions [63–65]. In this work we focus only on those forms of AT or text entry assistance which our participants currently use as part of their authentication process. This allows us to understand the barriers they currently face in authentication and how AT may help or interfere with their process.

3 AUTHENTICATING TO A PERSONAL COMPUTING DEVICE

At this point, it is useful to define a few terms we use in this work. We use the term **authentication** to refer specifically to the process of verifying a person's identity *to a personal computing device* (e.g., laptops, smartphones, tablets, etc.) [81]. Based on the identity of the user, the computing device can then allow or deny them access to the device. In this paper we are interested in authentication by people with UEI. Authentication is a **process** that has three stages: setup, credential verification, and failure resolution (see Figure 1).

Setup: This stage involves preparing the computing device to accept a *credential.* This is done by first registering a credential such as a password/PIN or a biometric (e.g., fingerprint). Then any subsequent tasks are performed that are necessary prior to credential verification. This may include setting up any required assistive technology (AT) or performing additional tasks necessary to reach the credential verification page. For example, older Windows machines required the pressing of Control+Alt+Delete before the credential verification could occur. Once the setup stage is completed, the device is ready to verify a user.

Credential verification: This is the stage when the identity of the person trying to access the device is verified. This is done by asking the user to enter a fresh instance of the credential and comparing it to the credential registered in the setup stage. Credentials can come in three basic forms — something only the *user knows* (e.g., passwords/PINs), something the *user has/possesses* (e.g., a smart card or token), or something the *user is* (e.g., biometrics). At the conclusion of this stage, if the verification is successful, the user

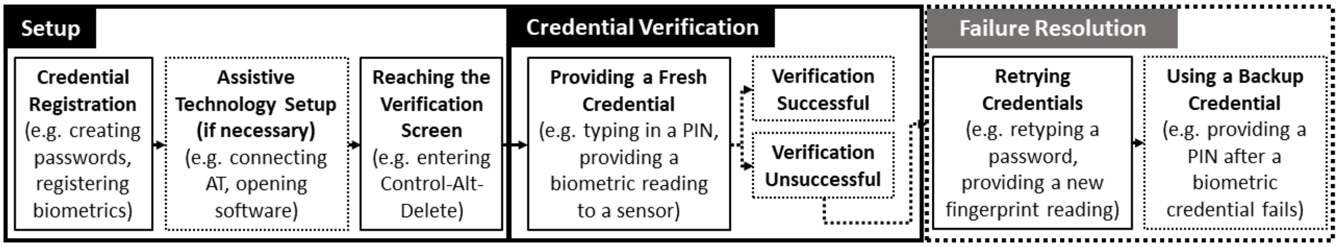
Setup
Credential Registration (e.g. creating passwords, registering biometrics)
Assistive Technology Setup (if necessary) (e.g. connecting AT, opening software)
Reaching the Verification Screen (e.g. entering Control-Alt-Delete)
Credential Verification
Providing a Fresh Credential (e.g. typing in a PIN, providing a biometric reading to a sensor)
Verification Successful
Verification Unsuccessful
Failure Resolution
Retrying Credentials (e.g. retyping a password, providing a new fingerprint reading)
Using a Backup Credential (e.g. providing a PIN after a biometric credential fails)

Figure 1: Illustration of a typical authentication process for people with UEI. Some stages of the authentication process only occur under certain conditions. For instance, failure resolution only occurs if there is a failure during credential verification. These conditional stages are marked with dotted lines.

will have access to the device. If the verification is unsuccessful, the user will proceed to the failure resolution stage.

Failure resolution: Credential verification can fail to authenticate a person to the device because the person made an error in presenting a fresh instance of the credential. Examples include a mistyped password or an inaccurate biometric measurement. In such events, the failure resolution stage provides additional means for a person to authenticate. This is typically done in one of two ways: (1) allowing the multiple *retries* of the credential verification stage, or (2) providing a *backup credential* for verification. A retry is when the user is permitted multiple attempts at providing a fresh instance of the same credential. While all modern authentication processes allow for retries, the number of retries granted varies from device to device. In addition to retries, certain authentication processes provide a backup credential. These are alternate credentials that can be used if the main credential verification fails. For example, biometrics often use passwords as a backup credential. Backup credentials are usually used after one or more retries with the main credential have already been attempted. In addition, the user is often given multiple retries for the backup credential. Not all authentication processes include a backup credential. If both retries and backup credentials are unsuccessful, a user may encounter a *lockout.* A lockout is when an individual is barred from retrying credential verification and must wait a period of time or go through other administrative steps to regain access.

4 INTERVIEW STUDY

In this study, we aimed to understand the experience of people with UEI in negotiating the authentication process with their computing devices. To this end, we conducted semi-structured interviews with eight adults with UEI and asked them two core questions:

(1) How and why do people with UEI use (or not use) authentication with their personal computing devices?
(2) Where (if anywhere) in the authentication process do barriers arise and how do people with UEI work around those barriers (if at all)?

The responses to these questions presented several themes, that we compiled as areas for future research necessary to make the authentication process more accessible to people with UEI.

4.1 Interview participants

We interviewed eight participants. In order to take part in the study, participants had to be over the age of 18, have some form of UEI, and not have an intellectual or developmental disability. All the participants used at least one computing device regularly. We recruited participants through mailing lists from local non-profits who work with people with disabilities. We also posted flyers around our local area including places offering services for people with disabilities such as the office of disabilities service at our university as well as other public venues such as local libraries and coffee shops. Snowball sampling was further used to increase our participant pool. These methods were used as it can be difficult to recruit within this community. The demographics of our participants are shown in Table 1.

4.2 Interview design

We conducted semi-structured interviews with participants recruited for our study. All interviews were conducted in-person except for one participant who was interviewed over a video call. One hour was allocated for the entire interview process, including reviewing and signing informed consent, taking any breaks the participant wanted, and providing compensation at the conclusion of the interview. The interview was audio recorded for which consent was obtained. At the start of the interview and before beginning the audio recording, the participants were greeted and the interviewer went over the details of the study, answered questions, and obtained consent for the study and audio recording. The interviewer then informed the participant that the audio recording had begun before asking interview questions. Interviews lasted approximately 30-50 minutes. In addition to the audio recording, the interviewer took field notes. In order to avoid inconveniencing our participants, the interviews were conducted at a location chosen by the participant, often their home or workplace. Participants were interviewed individually, although P2 had a caregiver present during the interview. The caregiver helped interpret most of P2's responses for the interviewer, as P2's disability affected her speech. Some participants also had a caregiver to help them sign the consent form. Participants were compensated with a gift card for their time. The interview consisted of four core categories of questions: general questions about their personal computing devices and authentication process; questions about their use of passwords and PINs as a verification credential; questions about their use of biometrics as a verification credential; and broader questions about their knowledge and experience with authentication and security. Participants were asked demographic questions at the end. Our interview procedure was approved by The University of Rhode Island's institutional review board (ethics board).

ID	Age	Gender	Disability	Use of upper extremities
P1	58	Male	Multiple sclerosis	Unimpaired use of left hand; right (dominant) hand can grab objects but lacks strength and tires quickly
P2	21	Female	Cerebral palsy	Fine motor control of head and neck; gross motor control of other extremities, but balance and coordination are impaired
P3	76	Female	Quadriparesis from Guillain-Barré syndrome	Contractures in both hands; right hand (dominant) has greater movement than left hand; shoulders have a strength impairment, but elbows remain unimpaired, allowing for some range of motion
P4	59	Male	Spinal cord injury	Gross motor function when sitting; no motor function when lying down
P5	65	Female	Amputation due to complications from virus	Both arms are amputated below the elbow; no impairment above the elbow
P6	50	Female	Cerebral palsy	Coordination is impaired; fingers largely do not move independently; some fine motor control over index finger and thumb
P7	37	Female	Cerebral palsy	Able to use eye-gaze for computing; other upper body movement impaired
P8	46	Male	Cerebral palsy	Limited gross motor control over arms; uses toe for computing and AAC

Table 1: Demographics of interview participants

4.3 Interview analysis

The first author conducted all of the interviews. Audio recordings made during the interviews were transcribed afterwards by the first author. The interview transcription document was then merged with the field notes taken during the interview to understand the context of each response. For instance, field notes were made when a caregiver was interpreting for P2. Any personal information such as details about the characters in a password or the names of friends or coworkers was removed from the transcription and replaced with placeholder text to protect the privacy of the participants. After all of the interviews were transcribed, the first author read through all of the transcripts to identify important segments and group responses into thematic categories and sub-categories. The first and second authors iteratively reviewed and reorganized these thematic categories until the categories presented in sections 5 and 6 were produced.

4.4 Limitations of the methodology

The methodology of our study had a few limitations that we discuss briefly. One limitation of this work is that a major form of recruitment was through a local non-profit that focused on providing assistive technology (AT) to people with disabilities. As a result, it is possible that our participants were greater users of technology than the general population of people with UEI. In addition, since our participants were those who responded to our advertisements for participation, there may have been a self-selection bias. That is, our participants may have been disproportionately those who were most interested in computing technology or those who had particularly strong positive or negative experiences with authentication. Lastly, all of our participants were from the United States, and therefore their perspectives may differ from people from other countries.

5 INTERVIEW FINDINGS: PASSWORDS AND PINS ARE STILL COMMONLY USED

As a first step in understanding authentication use by people with UEI, we asked our participants what personal computing devices they used, how they authenticated to them, if at all, and why they used authentication on their devices.

5.1 Both computing device and authentication use are common for people with UEI

Six out of eight participants had multiple devices including smartphones, laptops, and tablets. The exceptions to this were P3 and P7. P3 had exclusive access to a flip phone with internet access. She also shared two desktop computers with other residents in her assisted living facility. P7 only used an eye-gaze enabled tablet. A full list of computing devices used by each participant is shown in Table 2. All of the participants reported using at least one of their devices daily.

Most, but not all of our participants used authentication on their devices. Two of the participants (P2 and P7) stated that they had disabled the authentication process completely on all their current devices. P2 reported to having used authentication in the past for devices which she no longer used. Both had interesting, practical reasons for disabling authentication. P2 did not use authentication because both password entry and biometrics had been very difficult for her to use. She also had a rotating roster of caregivers with whom she wanted to share access to her devices. She could not easily give them the required verification credential while also having a device that was easy for her to use. P7, on the other hand, used her eye-gaze enabled tablet as an Augmentative and Alternative Communication (AAC) device for communicating with her caregivers. She worried the authentication process on the device would slow down her ability to communicate when needed.

Out of the remaining six (6) participants who used authentication, three participants (P1, P6, and P8) used authentication on all their devices. Three others (P3, P4, and P5) used authentication on only some of their devices. For instance, P3 reported that she did not use authentication on her flip phone because the device did not provide it as an option. However, she stated that she used a password-based credential on one of her shared desktop computers at her assisted living facility. The authentication process was disabled on her other shared desktop. P5 had disabled the PIN credential on her iPhone. P4 had not set up the authentication process on his iPad even though

ID	Computing devices	Credential options known to be available	Credential used	Assistive technology used
P1	Personal PC laptop	Password, PIN, fingerprint	PIN	Voice recognition software
	Family business PC laptop	Password, PIN	PIN	Log-me-in login assistance program
	iPhone	PIN	PIN	None
P2	iPhone	Facial recognition, PIN	None	None
	Tobii tablet	Unknown	None	Eye-gaze tracking
	Mac laptop*	Password	Password	None
	iPad*	PIN	PIN	None
P3	Flip phone with internet access	None	None	None
	Shared desktop computer at residence	None	None	None
	Shared desktop computer at residence	Password	Password	None
P4	iPhone	PIN, facial recognition	PIN	None
	Mac laptop	Password	Password	None
	iPad	PIN	None	Mouth stick
P5	Personal laptop	Password	Password	Dowel bar
	Work laptop	Password	Password	Voice recognition software, dowel bar
	iPhone	PIN	None	None
P6	Personal Mac laptop	Password	Password	None
	Work PC laptop	Password	Password	None
	iPhone	PIN, fingerprint	Fingerprint	None
P7	Tobii tablet	Unknown	None	Eye-gaze tracking
P8	Mac laptop	Password	Password	AAC device for toe typing
	iPad	PIN, facial recognition	Facial recognition	None
	iPhone	PIN, fingerprint	PIN	None

*Participant reported that they no longer use the device.

Table 2: Computing devices used by participants, the authentication credential options participants were aware of on their devices, what authentication credentials the participants use, and any assistive technology used for that device. The manufacturer of the computing device is included when identified by the participant. The participants may not be aware of all of the authentication options on their devices.

he used authentication on his laptop and iPhone with password and PIN as credentials, respectively.

Participants may not be aware of all of the options for authentication credentials available on their devices. When asked about options for authentication credentials, most participants reported only one or two options available on their devices. These are listed in Table 2. However, it is unclear if there were more options available which participants were unaware of. For instance, P1 stated that he only had a choice of passwords or PINs on his laptop saying, *"I didn't know there were [other credential options] that existed."* It was only when we were discussing biometrics that he suddenly remembered his personal laptop had a *"fingerprint thing"* that he had never set up. Such observations indicated that while participants like P1 sometimes remembered additional credential options available to them, it was not possible to be sure if the options participants detailed were comprehensive or not.

Out of the available credential options, passwords/PINs were the most common form of credentials used. All six of the participants who used authentication used passwords or PINs on at least some of their devices either by choice or because they were unaware of any alternatives. Most participants reported that they were not aware of any alternate credential choices, such as biometrics, when setting up a password/PIN for a particular device. As a result, our participants often did not have definitive reasons for the choice of passwords or PINs over other possible credentials. For instance, when P8 was asked whether he liked using passwords for his laptop he responded, *"I don't know if I like that as a [verification credential] or not, but I don't know what else they could do."* Only two participants (P1 and P4) reported that their devices supported biometric credentials that they did not use. Both participants reported that they had not tried using the biometrics available on their devices.

Other forms of credentials were less prevalent than PINs and passwords. Only two participants (P6 and P8) used biometrics as credentials. P6 used fingerprint on her iPhone. P8, on the other hand, had a very unusual way of using facial recognition on his iPad. Since his arms had limited gross motor function, he placed the iPad on the floor and performed credential verification by leaning over its camera from above.

5.2 People with UEI use authentication for several reasons including and beyond securing their devices

The main purpose of introducing authentication into computing devices has been for security reasons. It was not surprising therefore that we found that five out of six participants who used authentication (P3, P4, P5, P6, and P8) reported that at least one of the reasons for using authentication was to keep their devices secure. That being said, the reasons for keeping the device secure were diverse. For instance, P8 was generally security conscious and wanted to keep others from accessing his device. He specified that he used authentication on all his devices because *"I can secure it when I'm not* *on it and nobody can get on unless somehow they know the password."* Similarly, P5 used authentication on her personal and work laptops because she did not keep them with her at all times. She stated, *"...you know anybody can come in and out. You know, use my data or see my data."* On the other hand, for P4 the use of authentication on his devices was motivated by a negative past experience: *"I lost one phone before that didn't have a password on it and had some difficulty with things....financial trouble afterwards... [with] personal information being disclosed."*

However, authentication use was not always motivated by security. Sometimes it was something that our participants could not avoid. In certain work situations or group homes, for example, authentication was mandatory on the computing devices and could not be disabled. We refer to this as **mandated** authentication use. In such situations, our participants were forced to use authentication (typically a password) to login to the computing devices. For instance, P3 reported that while she found authentication with password entry inconvenient, she still used it because it was enabled on one of her shared computers in her group home and she could not change it.

Yet another reason for the use of authentication was **social pressure** as stated by P2. P2, who currently does not use authentication on any of her devices, reported that she had previously used passwords, when she was younger, because others around her had used them. During the interview she reflected on the experience and concluded that peer pressure was not a good reason for using authentication: *"[I was using authentication] because everybody else was doing it..., which is bad."*

6 INTERVIEW FINDINGS: EACH STAGE OF THE AUTHENTICATION PROCESS PRESENTS BARRIERS, AND PEOPLE WITH UEI OFTEN USE WORKAROUNDS THAT PRIORITIZE USABILITY OVER SECURITY

The initial findings regarding device and authentication use confirmed that the authentication process imposed barriers on people with UEI. Not all of our participants were content with the use of authentication and some disabled it altogether. We next asked our interview participants to discuss these barriers in detail. We found each stage of the authentication process presented barriers for our participants, who often used interesting workarounds to address these barriers. Table 3 summarizes the barriers and workarounds.

6.1 The setup stage in the authentication process can be difficult for people with UEI

Barriers for people with UEI in the authentication process started from the setup stage itself. We list three specific barriers in this stage — challenges in registering credentials, problems with the assistive technologies (AT), and difficulties reaching the verification screen.

The challenge of choosing passwords/PINs and registering biometrics can discourage their usage. Registering a credential in the setup stage is essential for the authentication process to function. However, the initial registrations of the credentials can be difficult or time consuming. For example, P8, who uses facial recognition, reported barriers while setting up FaceID on his iPad because part of his disability involves involuntary movement of his body. As a workaround, he relied on a friend to help hold the device camera close to his face in order to set up the biometric. This process, *"took some time because I move a lot."* While this process did not discourage him from using facial recognition, he did state that it would have been nice to have an easier setup.

P4, however, found the process for registering password/PIN so cumbersome that he initially avoided enabling authentication altogether, even though he now uses authentication on all of his devices except for his iPad. This partially came from the cognitive requirement of not only entering but remembering PINs. P4 stated *"I was trepidatious of [PINs]. And I couldn't come up with a passcode that I could easily remember. So that's why I didn't do it."* This may be even more of a barrier for those with cognitive disabilities that are often associated with conditions that cause UEI. Since passwords were still commonly used by our participants, we cannot dismiss such cognitive concerns with password use.

The need to use assistive technology (AT) can interfere with authentication. AT can help people with UEI interact with their devices by enabling easier user input. Since credential registration and entry during the authentication process requires user input, ATs have been used in the authentication process as well. However, we found that AT use in the authentication can make the entire process slow and unreliable, especially if the person wants to perform an otherwise quick task. For instance, P8 uses an AAC board conducive to toe-typing to enter passwords on his laptop. He stated that even though it *"works well"* for login, he often felt impatient if he wanted quick access to his laptop. He states, *"Sometimes I just need to read an email and I don't have my [AAC] device right by the computer so I have to go get that."* Despite the difficulty in quickly getting his AAC device working for password entry, P8 endures the delay and does not choose to use a workaround for it.

Similarly, P5 reported that she used speech recognition software (Dragon Naturally Speaking [25]) to complete work tasks like writing e-mails. However, while she could use the speech recognition software for entering passwords as well, she often did not do so because the software was too slow to start. Instead she relied on a different mechanical AT, a dowel bar strapped to her arm, to type the password. She commented, *"If I have the Dragon on, I won't use the dowel but sometimes it's easier just to type [the password] with the dowel."* In a similar vein, P4 noted that he used his own hands to enter passwords for his laptop. Even though this was not easy, he did not trust speech recognition software for password entry based on the experience of his friends. He stated that, *"I have friends who have Dragon [speech recognition system] and they have a lot of trouble with it and they're locked out of their machines."*

Some ATs are hard to use independently and require someone to help the individual with UEI to set them up. In such situations the use of AT for credential entry becomes an even greater barrier. P5 commented on this issue: *"My brother brought me this typing thing that was a headset...to me that was a pain because...I couldn't get the headset on myself, I'd have to have someone help me...technology like that...it's useless to me."* She does not use the head-based AT anymore.

Security measures for reaching the verification screen may not be usable. Another source of impediment in the setup stage of

Authentication process stage	Barriers encountered	Workarounds used
Setup	Authentication can be difficult or intimidating to create/register	Getting help from a friend to set up biometrics (P8) Not setting up authentication (P4)
	AT can slow down authentication or make it unreliable	Not choosing to use a workaround (P8) Using a different AT instead (P5) Avoiding AT for authentication (P4)
	Multi-key sequences to reach the verification screen are difficult to enter	Using assistive technology to enter difficult sequences (P1) Using trial-and-error to find a way to enter the sequence (P3)
Credential Verification	Passwords/PINs are difficult to enter and remember	Using a shorter, four-digit PIN instead of a longer password (P1) Getting help to enter PIN (P4) Choosing passwords with characters that are close to each other (P5) Disabling PIN on a commonly used device (P5) Switching to biometrics (P6, P8)
	Available biometrics are not well suited to the abilities of people with UEI	Attempting "toe-print" (*Unsuccessful*) (P8) Attempting "nose-print" (*Unsuccessful*) (P2) Disabling authentication on all devices (P2)
Failure Resolution	Insufficient retries and limited options for backup credentials create lockouts	Restarting the computer to get more attempts at verification (P6) Resetting password credential (P5)

Table 3: A summary of barriers encountered during the authentication process and the workarounds used to address them. While many participants encountered similar barriers, the unique circumstances of their lives and disabilities meant that each individual had unique workarounds for those barriers.

the authentication process was difficulty gaining access to the verification screen (often on laptop or desktop devices). For instance, on older Windows machines users need to press Control-Alt-Delete to reach the verification screen[2]. However, this requirement to press three buttons simultaneously can be very difficult for some people with UEI. Two of the participants (P1 and P3) reported having major difficulty typing Control-Alt-Delete on their laptop and shared desktop, respectively. As pointed out by P1, *"It's a nightmare trying to do to Control-Alt-Delete with three fingers on your left hand."* P3 expressed a similar concern by stating, *"The one thing that's more complicated is when I have to use Control-Alt-Delete."*

Each adopted a different workaround for managing the need to simultaneously press the Control-Alt-Delete keys. For instance, P1 used a software called Log-me-in that entered the key combination and also the password for him. P3, on the other hand, used a physical workaround to enter the three keys. She demonstrated her approach during the interview using a folder as a proxy for her keyboard. She reported that she had invented the approach herself through a trial-and-error process. P3 explained how her process made it possible to enter the sequence with her disability. P3's disability affects the strength and range of motion in her shoulders. She therefore cannot reach up to use the keyboard on the table in her place of residence. Instead, she picks up the keyboard to use it in her lap. She then uses one hand to hold the keyboard and the other to type. Since Control-Alt-Delete requires the simultaneous pressing of three different keys, she is unable to use her usual method. Instead, she tilts her power wheelchair backwards before using both her hands to press the three keys. The tilting allows the keyboard to slide towards her body thus keeping it in place. After she is logged in, she straightens her wheelchair so that she can see the screen to use the computer. This allows P3 to work around the barrier represented by Control-Alt-Delete. However, others with UEI may not be able to use the same workaround depending on their particular disability.

This barrier took us somewhat by surprise as pressing Control-Alt-Delete is no longer required by default to reach the verification screen for Windows [90]. The security measure was removed as the default setting because it made the authentication process more difficult for people with physical impairments (like UEI) [90]. However, the need to press Control-Alt-Delete was still found to be a barrier by two of our participants. This indicates that in many practical situations people with UEI still may be using older operating systems that introduce barriers to authentication. Consequently, we need to be cognizant of those barriers.

6.2 Both passwords and biometrics present barriers during credential verification

Once the credential verification stage was reached, more challenges arose that made the authentication process difficult for our participants.

Long, complex, secure passwords/PINs are difficult for people with UEI to use. Passwords are the most common form of credentials used during the credential verification stage of the authentication process. While longer or more complex passwords may help make a device more secure, they can also present barriers. This was described eloquently by P6 who discussed it in some detail. She reported that she had strict guidelines for her work computer password. The password was mandated to be long and complex. Further, the password had to be changed regularly. Consequently,

[2] Control-Alt-Delete was designed to prevent an attacker from creating a dialog that resembles the Windows login page in order to steal a user's credentials. Since only Windows is able to listen to the Control-Alt-Delete signal, its use ensures that the user is actually communicating with Windows and not a malicious login page [90].

P6 frequently made errors typing the password on her work computer and had additional difficulty remembering them. She stated, *"[Passwords] require...many different digits...You need to press more buttons...[You had to] press Shift at some point because you had to do [capital letters]. You had to do numbers and whatnot. So they're much more complicated [and] it's much more unforgiving."* Similar problems with password entry were reported by most of our participants.

In our interviews we found that four of the participants (P1, P4, P5, and P6) reported that they had strategies that made it easier, or in some cases *possible*, for them to enter passwords and PINs. However, these strategies often involved a tradeoff between security and usability, and often usability was favored at the expense of security.

P1, who had difficulty entering long passwords, had switched to using a four-digit PIN on his laptops. The short PIN was much less secure than a long, complex password but it was easy to use. P1 stated *"If I had a password that was more difficult, that would be harder to do...If you set up a real secure password with...symbols and numbers, uppercase letters and lowercase letters. I'm not doing that."*

P4 wanted to keep his device secure but found entering PINs on his iPhone difficult. He therefore shared the PIN with his caregiver and then asked them to help him perform tasks on the device such as looking up a word in the dictionary. He stated *"So a helper and I will discuss the derivation of a word, and then they'll pick up the phone. And I'll give them the [PIN] and they'll verify it."*

For P5, password entry was challenging. Further, her experience with AT was not always easy (as mentioned in Section 6.1). Consequently, she had an interesting workaround for entering long passwords, especially on her work laptop. P5 reported that she chose passwords with characters that were in the same general area on the keyboard: *"I like to have them all on one side of the keyboard."* Given her experience with credential verification and AT, it was therefore not surprising that P5 disabled authentication on the device she used most frequently where authentication was the greatest impediment: her iPhone. P5 specifically stated that she disabled authentication on her iPhone because she had her phone on her at all times and therefore did not need the security: *"Well, the phone I kinda carry with me all the time."* On a slight side note, choosing letters in a particular arrangement on the keyboard was not unique to P5. P3 also stated that she did something similar with her online passwords (e.g., email, social media, etc.). She reported picking letters that were close to each other, a few on one side of the keyboard, and a few on the other.

Another workaround two of our participants (P6 and P8) employed was to switch to biometric-based credentials. Both P6 and P8 liked their respective biometrics (fingerprint and facial recognition) better than passwords. One reason given was the speed that it brought to their authentication process. P6 uses fingerprint as a biometric on her phone because it is easier to use and faster than the passwords that she is mandated to use for her work and personal laptops. P6 said that *"[Fingerprint recognition] is much easier...and much faster."* P8 echoed a similar sentiment with respect to using facial recognition on his iPad, that (as mentioned in Section 5.1) he places on the ground where he leans over during the credential verification stage. He stated, *"Well I have to lean over so the camera can see my face, but it picks it [his face] up quickly and then I can open stuff quickly."*

Fingerprint biometrics were seen as beneficial for someone with degenerative impairments. P6 felt confident that fingerprint would always be available to her to authenticate as opposed to password entry, that had become more difficult for her over time. She stated, *"I feel confident that I'll always have a finger [for] fingerprint...I'm not getting any better with my issues coordination, typing, and stuff. So it feels like...no matter what happens I'll still be able to have access."*

Biometrics are not always well suited to the abilities of someone with UEI. Switching to biometrics may not be possible or practical for everyone with UEI. Biometrics themselves can create barriers to authentication. For instance, P2 tried using fingerprint on her old iPhone and it did not work for her. P2 then tried to register her nose-print using the fingerprint sensor on her device for authentication. However that too failed for her. She stated *"I...got my nose print [on the iPhone]. But it wasn't accurate."* Since then, she has a new iPhone with facial recognition on it. However, this too presented problems for her. P2 has several caregivers helping her during the day. She often wanted them to help her use her iPhone. She stated that facial recognition on her iPhone limited the number of faces it could register. That meant she could not give access to all her helpers. *"[The phone] only allows 5 faces [to be registered] and I have more than five (5) people who help [me]."* As a result of these experiences, P2 has now completely disabled authentication on all her devices. P2's attempt to use her nose-print was not unique. P8, who uses his toes to type, tried a similar strategy with his iPhone by trying to use his toe-print with the fingerprint sensor. That strategy also did not work.

P3, who did not use biometrics, was apprehensive about them altogether. She stated that she would probably not be able to use face recognition due to her shoulders: *"I don't think I could reach up...I don't really know. I would think I'd have problems...because my shoulders don't work."* P4, who had facial recognition available on his phone, expressed similar concerns that he had avoided trying it because the positioning was not practical for him. Similarly, with fingerprint, P3 expressed concern with positioning the finger properly due to lack of sufficient control: *"I would think the fingerprints would be difficult because I don't have a lot of control [of my fingers]."*

6.3 Insufficient retries and too few options for backup credentials can induce frustration

All modern authentication processes allow for failure resolutions when the credential verification fails. One way to perform failure resolution is to allow for multiple retry attempts at credential verification. Four participants (P1, P3, P4, and P8) reported that the retries provided by their devices were sufficient to verify their credentials to the devices. P4 described this process stating, *"Once I make a mistake, I step back and check the Caps Lock is on or not...[and] take it from there."* P8, who used facial recognition, commented that sometimes he was too far away from the camera for it to recognize him because it is on the floor. He would retry by leaning closer to the device from above: *"I just try again and make sure I am actually in the camera."*

As part of their failure resolution, some authentication processes provide a backup credential if the main credential fails. It is common for authentication processes that use biometrics as a credential to provide a password or PIN as a backup credential. However, this can create barriers given the difficulty people with UEI have with passwords and PINs. P6 summarizing this issue as, *"If you mess up with the initial log-on [using fingerprint recognition], then the second backup is the way the backup systems [backup credentials] work now, they're all awful."*

When neither the initial retries nor the backup credentials provided by the authentication process are sufficient, a lockout can occur. In these cases, a person with UEI may have to wait or use another administrative process to regain access to the device. To avoid such consequences, P6 reported an interesting workaround: *"So usually my strategy for that is [if] I log in twice incorrectly, if that happens, then I power down the computer, and then I have to wait for it to kick up again."* Unsurprisingly, she found this to be quite frustrating. P5, on the other hand, reported that she occasionally experienced lockouts at work where the password requirements were strict. In these cases, she is able to create a new password through workplace specific processes for forgotten passwords.

7 ACCESSIBILITY OF AUTHENTICATION FOR PEOPLE WITH UEI IS A NASCENT RESEARCH AREA THAT MERITS FURTHER EXPLORATION

In our literature review, we were surprised to find so little work had been done to examine the needs of people with UEI for authentication. While we found in our results that people with UEI use authentication on their computing devices, overall, there was a gap between what people with UEI want from their authentication process and the current research being done within this area. This gap presents an opportunity for further research in authentication accessibility for people with UEI. In order to explore this gap, we asked each of our participants what their ideal authentication process would be. In this section, we use their responses along with other information from the interviews to present six areas for future research. Each of these describe particular challenges regarding authentication for people with UEI and should be explored in order to create accessible authentication.

7.1 Opportunity: Evaluating AT in a security context for password/PIN entry

Passwords and PINs are here to stay for the near future. However, passwords and PINs present many barriers for people with UEI with respect to authenticating to their devices. Therefore, it is important for us to ease their entry. One way of doing this is by developing text-entry AT with the goal of easing authentication. As discussed in our related work section, there has already been research into various forms of AT for people with UEI. These works can help give an informative background on some strategies that may be worth exploring in an authentication context. Further, many of our participants used AT for computing more generally, including eye-gaze trackers (P2 and P7), Dragon Naturally Speaking speech recognition software (P1 and P5), a mouth stick (P4), and a foot-based AAC board conducive to typing with toes (P8). Several participants expressed interest in using authentication that worked with *their* AT.

However, creating AT that works well for computing more generally is not sufficient. We need to design the AT to work with the authentication process. Many participants experienced difficulties setting up AT for their devices in order to authenticate to the device. Therefore, more research is needed in designing AT systems that are reliable, available at boot-time, require minimal setup for the user, and can be used to quickly login to a computing device for short tasks such as reading an e-mail. Further, password entry presents unique challenges in that authentication needs to not only be usable for people with UEI, but also secure so that people with UEI can continue to have secure computing devices. This means that AT must be evaluated to ensure that it cannot be exploited by an attacker (e.g., ensuring that it does not leak information through a side channel that could be exploited by an attacker to gain knowledge about a password credential).

Some of the open research questions in this area include:

- What are the characteristics of the AT that can be used by people with UEI for authentication?
- How do we ensure that AT being used for password/PIN entry is secure and does not provide any opportunities (e.g., side-channels) to a potential attacker?
- How do we design new AT or repurpose currently used AT for people with UEI to enable password entry without creating a barrier for them?

7.2 Opportunity: Improving biometrics

Biometrics can be a more usable alternative to passwords for people with UEI. However, the currently predominant methods of face and fingerprint recognition are not sufficient. Several participants reported that they could not use biometrics because of their impairment. In fact, several of the participants tried to repurpose existing biometric sensors in new ways such as trying to use nose-print and toe-print. This is an opportunity for us to develop new credentials for people with UEI that leverage their abilities. Almost all of our participants expressed strong interest in newer biometrics that can help them login more easily.

Some of the ideas that emerged included verification credentials based on voice-print and eye-gaze. Voice-print credentials have been studied extensively in the past few years [16, 29, 52, 74, 79, 93, 94]. However, their use for people with UEI, many of whom may have speech impairments, is yet to be evaluated carefully. Similarly, eye-gaze trackers have been investigated as a method for producing verification credentials [1, 26, 27, 32, 43, 48, 51, 82, 85]. However, most of this work has been done with people without disabilities. There has yet to be work done to study eye-gaze authentication for people who use eye-gaze trackers regularly as AT. More generally, the way people with UEI use their AT can present novel options for biometrics. As newer AT modalities are developed (e.g., those listed in our related work section), they should be evaluated for their biometrics generation potential.

Prominent open research questions in this area include:

- What new biometrics (such as toe-print and nose-print) would people with UEI like to use for authentication?

- What new biometrics can be obtained from ATs used by people with UEI for operating their computing devices?
- Can existing sensors such as a fingerprint sensor be repurposed to work with new biometrics better suited to people with UEI?

7.3 Opportunity: Exploring token-based authentication

Many of the verification credentials used by people with UEI are based on what a person knows (e.g., passwords) and what a person is (e.g., biometrics). However, the third obvious way to authenticate is based on what a person has (e.g., a token). Tokens were one of the methods that was brought up by our participants as a way to ease verification. Tokens such as Yubikey [92] could be tried in this regard. However, these credentials present their own usability problems in terms of (1) keeping the token secure, (2) interfacing the token with a computing device, and (3) then activating the token (e.g., YubiKey's touch interface). These usability considerations may not be easy for many people with UEI, though they may work for some. Interestingly, Apple has used a similar approach to ease credential verification on their devices. It is possible for a user to authenticate to their Mac laptop without using a password or a biometric when wearing their Apple watch [11]. Of course, the user has to type in a PIN to authenticate to their Apple Watch. This may present usability challenges for someone with UEI. In addition, some of our participants commented that financial strain was a deciding factor for choosing certain computing devices. For instance, P3 commented that despite being interested in iPhones and iPads she uses a flip phone with internet access because, *"I'm poor and I can't afford...an iPhone."* Premium products like the Apple watch may exclude people with UEI who do not have the means to afford them.

Open research questions in this area include:

- How can token-based credentials be kept secure?
- Which sorts of devices would a person with UEI want to be able to interface the token with?
- How should tokens be designed in order to be accessible to people with UEI especially if activation of the token is required?

7.4 Opportunity: Promoting interdependence through shared credentials

People with UEI sometimes want to be able to share access to their devices with caregivers. When sufficient trust is present between the individual with UEI and their caregiver(s), the authentication processes should be designed to promote partnership between people with UEI and their caregivers. For instance, people with UEI sometimes want help from trusted caregivers in using their computing devices. Often times, the caregivers rotate over the course of a day. Therefore, it can become tedious for people with UEI to share their verification credentials with others again and again. This presents a new opportunity for developing credentials that enable people with UEI to easily share those credentials with caregivers, even when the caregivers are constantly changing. Care needs to be taken to ensure that the credentials given to the caregivers limit their access to the specific tasks that the person with UEI wants them to perform. Further, access should be limited to specific periods of time set by the person with UEI. This is because we cannot assume that caregivers are always trusted by their clients and the clients should always be able to control access to their data and devices.

A few open research questions in this area include:

- Who do people with UEI want to share access to their computing devices with?
- What sort of access would a person with UEI want a trusted caregiver to have?
- How can we ensure that the person with UEI remains in control of the access to their devices?

7.5 Opportunity: Improving the failure resolution process

The entire authentication process has to be made usable for an individual with UEI. Based on our discussion with our participants, this involves improvements in two areas: (1) lockout procedures, and (2) backup credentials. Getting locked out of one's devices is a real concern for people with UEI. Therefore, when designing authentication processes for people with UEI in mind, we need to relax the conditions for lockout. This can be done by allowing more retries to enter the correct verification credential, or by making credential verification more tolerant to errors. Backup credentials are often used to gain additional attempts prior to lockout. Many authentication processes currently revert to passwords or PINs as a backup credential. Since people with UEI find password and PIN entry difficult, there is a need to improve the diversity in the backup credentials made available. Many of our participants expressed the desire to have more backup options like alternative biometrics. For instance, being able to use facial recognition if fingerprint recognition was unsuccessful. Other participants wanted multiple backup credentials such as having voice-print, fingerprint, and facial recognition all made available. This diversity of backup credentials would help to ensure that passwords/PINs can become the last option for backup credentials and not the very first alternative.

Some research questions in this area include:

- How can authentication processes be made more tolerant to mistakes and prevent people with UEI from experiencing lockouts?
- Which types of backup credentials would be effective for people with UEI?

7.6 Opportunity: Enabling physical rehabilitation through authentication

One point of discussion that came up in our interviews was the use of authentication to provide physical benefit to people with UEI. This was expressed clearly by P4 who stated that entering his password was something that he did as a way to maintain the use of his arms: *"I thought of Dragon Dictate and other voice command systems, but while I can use my arms, I'd rather do that to keep some strength and mobility."* This is interesting because it goes against the usual ideal that the authentication process should be made as effortless for the user as possible. One possible future area of research is exploring the role that authentication can play in physical rehabilitation for people with UEI. Of course, since rehabilitation generally involves effort to be expended in order to be effective, it could have a negative effect on usability if poorly implemented. Any proposed system would need to ensure that it remains usable such that any added rehabilitation exercises do not become a barrier. A variety of work has been done on the use of technology more generally to support rehabilitation including works around IoT devices [67], games [2, 5, 6, 31, 45, 88], virtual reality [21, 56, 57], robotics [54, 59], musical instruments [46, 47], sensing technology [18, 44], tangibles [53], and mobile devices [86]. However, authentication presents unique challenges due to its regular usage in daily computing and the need for it to remain secure.

Some of the research questions in this area include:

- What sort of physical rehabilitation and exercise do people with UEI want to have in their authentication process?
- How can credential entry be designed such that an individual with UEI is able to exercise their arms and fingers?
- How can the authentication process preserve usability while enabling physical benefits?

8 CONCLUSION

In this paper we wanted to understand the authentication process of people with upper extremity impairment (UEI). Consequently, we interviewed eight people with UEI in order to learn more about how and why they use authentication, where in the authentication process they encounter barriers, and what workarounds they use for those barriers. We found that many people with UEI used authentication, with PINs and passwords being the primary form of credentials used. Further, they face barriers throughout the entire authentication process and use workarounds that often prioritize usability over security. We then identified six areas for future research in order to make accessible authentication for people with UEI. In the future, we hope to propose improvements to the existing authentication process based on the results of this work.

9 ACKNOWLEDGMENTS

This work is supported in part by the National Science Foundation grant CNS-1947022. We would like to thank all the participants and reviewers who provided their time and experience to this work. We would also like to thank Molly Smith and Justin Moy for participating in mock interviews and providing feedback on the interview questions. We also thank Nancy Alterio, Kelly Charlebois, and Matthew Provost for helping with recruitment of participants. Last but not least, we would like to thank Tina-Marie Ranalli, Josh Lewis, and ML Tlachac for reading several drafts of this paper and providing comments.

REFERENCES

[1] Yasmeen Abdrabou, Mohamed Khamis, Rana Mohamed Eisa, Sherif Ismail, and Amrl Elmougy. 2019. Just Gaze and Wave: Exploring the Use of Gaze and Gestures for Shoulder-Surfing Resilient Authentication. In *Proceedings of the 11th ACM Symposium on Eye Tracking Research & Applications* (Denver, Colorado) *(ETRA '19)*. Association for Computing Machinery, New York, NY, USA, Article 29, 10 pages. https://doi.org/10.1145/3314111.3319837

[2] Imad Afyouni, Ahmad Muaz Qamar, Syed Osama Hussain, Faizan Ur Rehman, Bilal Sadiq, and Abdullah Murad. 2017. Motion-Based Serious Games for Hand Assistive Rehabilitation. In *Proceedings of the 22nd International Conference on Intelligent User Interfaces Companion* (Limassol, Cyprus) *(IUI '17 Companion)*. Association for Computing Machinery, New York, NY, USA, 133–136. https://doi.org/10.1145/3030024.3040977

[3] Hyunjin Ahn, Jaeseok Yoon, Gulji Chung, Kibum Kim, Jiyeon Ma, Hyunbin Choi, Donguk Jung, and Joongseek Lee. 2015. DOWELL: Dwell-Time Based Smartphone Control Solution for People with Upper Limb Disabilities. In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI EA '15)*. Association for Computing Machinery, New York, NY, USA, 887–892. https://doi.org/10.1145/2702613.2732862

[4] Areej Al-Wabil, Arwa Al-Issa, Itisam Hazzaa, May Al-Humaimeedi, Lujain Al-Tamimi, and Bushra Al-Kadhi. 2012. Optimizing Gaze Typing for People with Severe Motor Disabilities: The IWriter Arabic Interface. In *Proceedings of the 14th International ACM SIGACCESS Conference on Computers and Accessibility* (Boulder, Colorado, USA) *(ASSETS '12)*. Association for Computing Machinery, New York, NY, USA, 261–262. https://doi.org/10.1145/2384916.2384983

[5] Gazihan Alankus and Caitlin Kelleher. 2012. Reducing Compensatory Motions in Video Games for Stroke Rehabilitation. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Austin, Texas, USA) *(CHI '12)*. Association for Computing Machinery, New York, NY, USA, 2049–2058. https://doi.org/10.1145/2207676.2208354

[6] Gazihan Alankus, Amanda Lazar, Matt May, and Caitlin Kelleher. 2010. Towards Customizable Games for Stroke Rehabilitation. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Atlanta, Georgia, USA) *(CHI '10)*. Association for Computing Machinery, New York, NY, USA, 2113–2122. https://doi.org/10.1145/1753326.1753649

[7] Veronica Alfaro Arias, Amy Hurst, and Anita Perr. 2020. Designing a Remote Framework to Create Custom Assistive Technologies. In *The 22nd International ACM SIGACCESS Conference on Computers and Accessibility* (Virtual Event, Greece) *(ASSETS '20)*. Association for Computing Machinery, New York, NY, USA, Article 62, 4 pages. https://doi.org/10.1145/3373625.3418022

[8] Abdullah Ali. 2015. Sequential Gestural Passcodes on Google Glass. In *Proceedings of the 17th International ACM SIGACCESS Conference on Computers & Accessibility* (Lisbon, Portugal) *(ASSETS '15)*. Association for Computing Machinery, New York, NY, USA, 359–360. https://doi.org/10.1145/2700648.2811326

[9] F. Aloise, F. Schettini, P. Aricò, L. Bianchi, A. Riccio, M. Mecella, F. Babiloni, D. Mattia, and F. Cincotti. 2010. Advanced Brain Computer Interface for Communication and Control. In *Proceedings of the International Conference on Advanced Visual Interfaces* (Roma, Italy) *(AVI '10)*. Association for Computing Machinery, New York, NY, USA, 399–400. https://doi.org/10.1145/1842993.1843076

[10] Sarah Andrew, Stacey Watson, Tae Oh, and Garreth W. Tigwell. 2020. A Review of Literature on Accessibility and Authentication Techniques. In *The 22nd International ACM SIGACCESS Conference on Computers and Accessibility* (Virtual Event, Greece) *(ASSETS '20)*. Association for Computing Machinery, New York, NY, USA, Article 55, 4 pages. https://doi.org/10.1145/3373625.3418005

[11] Apple Inc. 2020. *Unlock your Mac and approve tasks with Apple Watch.* Apple Inc. https://support.apple.com/guide/imac/unlock-and-approve-with-apple-watch-apda4d638ecf/mac

[12] Shiri Azenkot, Kyle Rector, Richard Ladner, and Jacob Wobbrock. 2012. PassChords: Secure Multi-Touch Authentication for Blind People. In *Proceedings of the 14th International ACM SIGACCESS Conference on Computers and Accessibility* (Boulder, Colorado, USA) *(ASSETS '12)*. Association for Computing Machinery, New York, NY, USA, 159–166. https://doi.org/10.1145/2384916.2384945

[13] Tanya Bafna. 2018. Gaze Typing Using Multi-Key Selection Technique. In *Proceedings of the 20th International ACM SIGACCESS Conference on Computers and Accessibility* (Galway, Ireland) *(ASSETS '18)*. Association for Computing Machinery, New York, NY, USA, 477–479. https://doi.org/10.1145/3234695.3240992

[14] Natã M. Barbosa, Jordan Hayes, and Yang Wang. 2016. UniPass: Design and Evaluation of a Smart Device-Based Password Manager for Visually Impaired Users. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (Heidelberg, Germany) *(UbiComp '16)*. Association for Computing Machinery, New York, NY, USA, 49–60. https://doi.org/10.1145/2971648.2971722

[15] Mohammed Belatar and Franck Poirier. 2008. Text Entry for Mobile Devices and Users with Severe Motor Impairments: Handiglyph, a Primitive Shapes Based Onscreen Keyboard. In *Proceedings of the 10th International ACM SIGACCESS Conference on Computers and Accessibility* (Halifax, Nova Scotia, Canada) *(Assets '08)*. Association for Computing Machinery, New York, NY, USA, 209–216. https://doi.org/10.1145/1414471.1414510

[16] Bella, Janson Hendryli, and Dyah Erny Herwindiati. 2020. Voice Authentication Model for One-Time Password Using Deep Learning Models. In *Proceedings of the 2020 2nd International Conference on Big Data Engineering and Technology* (Singapore, China) *(BDET 2020)*. Association for Computing Machinery, New York, NY, USA, 35–39. https://doi.org/10.1145/3378904.3378908

[17] Ramon Blanco-Gonzalo, Chiara Lunerti, Raul Sanchez-Reillo, and Richard Michael Guest. 2018. Biometrics: Accessibility challenge or opportunity? *PLOS ONE* 13, 3 (03 2018), 1–20. https://doi.org/10.1371/journal.pone.0194111

[18] Cati Boulanger, Adam Boulanger, Lilian de Greef, Andy Kearney, Kiley Sobel, Russell Transue, Z Sweedyk, Paul H. Dietz, and Steven Bathiche. 2013. Stroke Rehabilitation with a Sensing Surface. In *Proceedings of the SIGCHI Conference on*

Human Factors in Computing Systems (Paris, France) *(CHI '13)*. Association for Computing Machinery, New York, NY, USA, 1243–1246. https://doi.org/10.1145/2470654.2466160

[19] Mary Brown and Felicia R. Doswell. 2010. Using Passtones Instead of Passwords. In *Proceedings of the 48th Annual Southeast Regional Conference* (Oxford, Mississippi) *(ACM SE '10)*. Association for Computing Machinery, New York, NY, USA, Article 82, 5 pages. https://doi.org/10.1145/1900008.1900119

[20] Christian P. Carvajal, Fernando A. Chicaiza, Renato Carvajal, and Víctor H. Andaluz. 2017. Robotic Stimulation for Fine Motor Skills of the Upper Extremities. In *Proceedings of the 2017 9th International Conference on Education Technology and Computers* (Barcelona, Spain) *(ICETC 2017)*. Association for Computing Machinery, New York, NY, USA, 268–271. https://doi.org/10.1145/3175536.3176652

[21] Tanvir Irfan Chowdhury, Sharif Mohammad Shahnewaz Ferdous, Tabitha C. Peck, and John Quarles. 2018. "Virtual Ability Simulation" to Boost Rehabilitation Exercise Performance and Confidence for People with Disability. In *Proceedings of the 24th ACM Symposium on Virtual Reality Software and Technology* (Tokyo, Japan) *(VRST '18)*. Association for Computing Machinery, New York, NY, USA, Article 129, 2 pages. https://doi.org/10.1145/3281505.3283386

[22] Muratcan Cicek, Ankit Dave, Wenxin Feng, Michael Xuelin Huang, Julia Katherine Haines, and Jeffry Nichols. 2020. Designing and Evaluating Head-Based Pointing on Smartphones for People with Motor Impairments. In *The 22nd International ACM SIGACCESS Conference on Computers and Accessibility* (Virtual Event, Greece) *(ASSETS '20)*. Association for Computing Machinery, New York, NY, USA, Article 14, 12 pages. https://doi.org/10.1145/3373625.3416994

[23] Dimitrios Damopoulos and Georgios Kambourakis. 2019. Hands-Free one-Time and continuous authentication using glass wearable devices. *Journal of Information Security and Applications* 46 (2019), 138–150.

[24] Bryan Dosono, Jordan Hayes, and Yang Wang. 2015. "I'm Stuck!": A Contextual Inquiry of People with Visual Impairments in Authentication. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, Ottawa, 151–168. https://www.usenix.org/conference/soups2015/proceedings/presentation/dosono

[25] Nuance Communications 2020. *Dragon Speech Recognition*. Nuance Communications. https://www.nuance.com/dragon.html

[26] Andrew T Duchowski. 2002. A breadth-first survey of eye-tracking applications. *Behavior Research Methods, Instruments, & Computers* 34, 4 (2002), 455–470.

[27] Simon Eberz, Giulio Lovisotto, Kasper B. Rasmussen, Vincent Lenders, and Ivan Martinovic. 2019. 28 Blinks Later: Tackling Practical Challenges of Eye Movement Biometrics. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (London, United Kingdom) *(CCS '19)*. Association for Computing Machinery, New York, NY, USA, 1187–1199. https://doi.org/10.1145/3319535.3354233

[28] Mingming Fan, Zhen Li, and Franklin Mingzhe Li. 2020. Eyelid Gestures on Mobile Devices for People with Motor Impairments. In *The 22nd International ACM SIGACCESS Conference on Computers and Accessibility* (Virtual Event, Greece) *(ASSETS '20)*. Association for Computing Machinery, New York, NY, USA, Article 15, 8 pages. https://doi.org/10.1145/3373625.3416987

[29] Huan Feng, Kassem Fawaz, and Kang G. Shin. 2017. Continuous Authentication for Voice Assistants. In *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking* (Snowbird, Utah, USA) *(MobiCom '17)*. Association for Computing Machinery, New York, NY, USA, 343–355. https://doi.org/10.1145/3117811.3117823

[30] Chad R Fenner and Cherie Noteboom. 2018. *How Wearable Technology Will Replace Verbal Authentication or Passwords for Universal Secure Authentication for Healthcare.* Technical Report. Dakota State University.

[31] Eletha Flores, Gabriel Tobon, Ettore Cavallaro, Francesca I. Cavallaro, Joel C. Perry, and Thierry Keller. 2008. Improving Patient Motivation in Game Development for Motor Deficit Rehabilitation. In *Proceedings of the 2008 International Conference on Advances in Computer Entertainment Technology* (Yokohama, Japan) *(ACE '08)*. Association for Computing Machinery, New York, NY, USA, 381–384. https://doi.org/10.1145/1501750.1501839

[32] Alain Forget, Sonia Chiasson, and Robert Biddle. 2010. Shoulder-Surfing Resistance with Eye-Gaze Entry in Cued-Recall Graphical Passwords. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Atlanta, Georgia, USA) *(CHI '10)*. Association for Computing Machinery, New York, NY, USA, 1107–1110. https://doi.org/10.1145/1753326.1753491

[33] K. Fuglerud and O. Dale. 2011. Secure and Inclusive Authentication with a Talking Mobile One-Time-Password Client. *IEEE Security Privacy* 9, 2 (2011), 27–34.

[34] K. Fuglerud and O. Dale. 2011. Secure and Inclusive Authentication with a Talking Mobile One-Time-Password Client. *IEEE Security Privacy* 9, 2 (2011), 27–34.

[35] Krzysztof Z. Gajos, Jacob O. Wobbrock, and Daniel S. Weld. 2008. Improving the Performance of Motor-Impaired Users with Automatically-Generated, Ability-Based Interfaces. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Florence, Italy) *(CHI '08)*. Association for Computing Machinery, New York, NY, USA, 1257–1266. https://doi.org/10.1145/1357054.1357250

[36] Jordan Hayes, Xiao Li, and Yang Wang. 2017. "I Always Have to Think About It First": Authentication Experiences of People with Cognitive Impairments. In *Proceedings of the 19th International ACM SIGACCESS Conference on Computers and Accessibility* (Baltimore, Maryland, USA) *(ASSETS '17)*. Association for Computing Machinery, New York, NY, USA, 357–358. https://doi.org/10.1145/3132525.3134788

[37] K. Helkala. 2012. Disabilities and Authentication Methods: Usability and Security. In *2012 Seventh International Conference on Availability, Reliability and Security*. IEEE, New York, NY, USA, 327–334. https://doi.org/10.1109/ARES.2012.19

[38] Yuhan Hu, Sang-won Leigh, and Pattie Maes. 2017. Hand Development Kit: Soft Robotic Fingers as Prosthetic Augmentation of the Hand. In *Adjunct Publication of the 30th Annual ACM Symposium on User Interface Software and Technology* (Québec City, QC, Canada) *(UIST '17)*. Association for Computing Machinery, New York, NY, USA, 27–29. https://doi.org/10.1145/3131785.3131805

[39] Amy Hurst and Jasmine Tobias. 2011. Empowering Individuals with Do-It-Yourself Assistive Technology. In *The Proceedings of the 13th International ACM SIGACCESS Conference on Computers and Accessibility* (Dundee, Scotland, UK) *(ASSETS '11)*. Association for Computing Machinery, New York, NY, USA, 11–18. https://doi.org/10.1145/2049536.2049541

[40] R. C. Johnson, Walter J. Scheirer, and Terrance E. Boult. 2013. Secure voice-based authentication for mobile devices: vaulted voice verification. In *Biometric and Surveillance Technology for Human and Activity Identification X*, Ioannis Kakadiaris, Walter J. Scheirer, and Laurence G. Hassebrook (Eds.), Vol. 8712. International Society for Optics and Photonics, SPIE, Bellingham, Washington USA, 164 – 176. https://doi.org/10.1117/12.2015649

[41] Shaun K. Kane, Anhong Guo, and Meredith Ringel Morris. 2020. Sense and Accessibility: Understanding People with Physical Disabilities' Experiences with Sensing Systems. In *The 22nd International ACM SIGACCESS Conference on Computers and Accessibility* (Virtual Event, Greece) *(ASSETS '20)*. Association for Computing Machinery, New York, NY, USA, Article 42, 14 pages. https://doi.org/10.1145/3373625.3416990

[42] Shaun K. Kane, Jacob O. Wobbrock, Mark Harniss, and Kurt L. Johnson. 2008. TrueKeys: Identifying and Correcting Typing Errors for People with Motor Impairments. In *Proceedings of the 13th International Conference on Intelligent User Interfaces* (Gran Canaria, Spain) *(IUI '08)*. Association for Computing Machinery, New York, NY, USA, 349–352. https://doi.org/10.1145/1378773.1378827

[43] Christina Katsini, Yasmeen Abdrabou, George E. Raptis, Mohamed Khamis, and Florian Alt. 2020. The Role of Eye Gaze in Security and Privacy Applications: Survey and Future HCI Research Directions. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–21. https://doi.org/10.1145/3313831.3376840

[44] Maryam Khademi, Hossein Mousavi Hondori, Alison McKenzie, Lucy Dodakian, Cristina Videira Lopes, and Steven C. Cramer. 2014. Comparing Direct and Indirect Interaction in Stroke Rehabilitation. In *CHI '14 Extended Abstracts on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1639–1644. https://doi.org/10.1145/2559206.2581192

[45] Maryam Khademi, Hossein Mousavi Hondori, Alison McKenzie, Lucy Dodakian, Cristina Videira Lopes, and Steven C. Cramer. 2014. Free-Hand Interaction with Leap Motion Controller for Stroke Rehabilitation. In *CHI '14 Extended Abstracts on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1663–1668. https://doi.org/10.1145/2559206.2581203

[46] Pedro Kirk. 2015. Can Specialised Electronic Musical Instruments Aid Stroke Rehabilitation?. In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI EA '15)*. Association for Computing Machinery, New York, NY, USA, 127–132. https://doi.org/10.1145/2702613.2726965

[47] Pedro Kirk, Mick Grierson, Rebeka Bodak, Nick Ward, Fran Brander, Kate Kelly, Nicholas Newman, and Lauren Stewart. 2016. Motivating Stroke Rehabilitation Through Music: A Feasibility Study Using Digital Musical Instruments in the Home. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 1781–1785. https://doi.org/10.1145/2858036.2858376

[48] Tomasz Kocejko and Jerzy Wtorek. 2012. Gaze Pattern Lock for Elders and Disabled. In *Information Technologies in Biomedicine*, Ewa Piętka and Jacek Kawa (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 589–602.

[49] Kirk L. Kroeker. 2011. Improving Brain-Computer Interfaces. *Commun. ACM* 54, 10 (Oct. 2011), 11–14. https://doi.org/10.1145/2001269.2001275

[50] Ravi Kuber and Shiva Sharma. 2010. Toward Tactile Authentication for Blind Users. In *Proceedings of the 12th International ACM SIGACCESS Conference on Computers and Accessibility* (Orlando, Florida, USA) *(ASSETS '10)*. Association for Computing Machinery, New York, NY, USA, 289–290. https://doi.org/10.1145/1878803.1878875

[51] Manu Kumar, Tal Garfinkel, Dan Boneh, and Terry Winograd. 2007. Reducing Shoulder-Surfing by Using Gaze-Based Password Entry. In *Proceedings of the 3rd Symposium on Usable Privacy and Security* (Pittsburgh, Pennsylvania, USA) *(SOUPS '07)*. Association for Computing Machinery, New York, NY, USA, 13–19. https://doi.org/10.1145/1280680.1280683

[52] Il-Youp Kwak, Jun Ho Huh, Seung Taek Han, Iljoo Kim, and Jiwon Yoon. 2019. Voice Presentation Attack Detection through Text-Converted Voice Command

Analysis. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, Article 598, 12 pages. https://doi.org/10.1145/3290605.3300828

[53] Mikko Kytö, Laura Maye, and David McGookin. 2019. Using Both Hands: Tangibles for Stroke Rehabilitation in the Home. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3290605.3300612

[54] Narae Lee, Young Ho Lee, Jeeyong Chung, Heejeong Heo, Hyeonkyeong Yang, Kyung Soo Lee, Hokyoung Ryu, Sungho Jang, and Woohun Lee. 2014. Shape-Changing Robot for Stroke Rehabilitation. In *Proceedings of the 2014 Conference on Designing Interactive Systems* (Vancouver, BC, Canada) *(DIS '14)*. Association for Computing Machinery, New York, NY, USA, 325–334. https://doi.org/10.1145/2598510.2598535

[55] B. Lewis, J. Hebert, K. Venkatasubramanian, M. Provost, and K. Charlebois. 2020. A New Authentication Approach for People with Upper Extremity Impairment. In *2020 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. IEEE, New York, NY, USA, 1–6. https://doi.org/10.1109/PerComWorkshops48775.2020.9156171

[56] The-Kiet Lu, Edwin Foo, Bala S. Rajaratnam, and Kannappan. 2012. Semi Portable Rehabilitation System for Upper Limb Disability. In *Proceedings of the 6th International Conference on Rehabilitation Engineering & Assistive Technology* (Tampines, Singapore) *(i-CREATe '12)*. Singapore Therapeutic, Assistive & Rehabilitative Technologies (START) Centre, Midview City, SGP, Article 4, 4 pages.

[57] The-Kiet Lu, Edwin Foo, Bala S. Rajaratnam, and Kannappan. 2013. Configurable Augmented Virtual Reality Rehabilitation System for Upper Limb Disability. In *Proceedings of the 7th International Convention on Rehabilitation Engineering and Assistive Technology* (Gyeonggi-do, South Korea) *(i-CREATe '13)*. Singapore Therapeutic, Assistive & Rehabilitative Technologies (START) Centre, Midview City, SGP, Article 19, 4 pages.

[58] Yao Ma, Jinjuan Heidi Feng, Libby Kumin, Jonathan Lazar, and Lakshmidevi Sreeramareddy. 2012. Investigating Authentication Methods Used by Individuals with down Syndrome. In *Proceedings of the 14th International ACM SIGACCESS Conference on Computers and Accessibility* (Boulder, Colorado, USA) *(ASSETS '12)*. Association for Computing Machinery, New York, NY, USA, 241–242. https://doi.org/10.1145/2384916.2384973

[59] Matteo Malosio, Nicola Pedrocchi, and Lorenzo Molinari Tosatti. 2010. Robot-Assisted Upper-Limb Rehabilitation Platform. In *Proceedings of the 5th ACM/IEEE International Conference on Human-Robot Interaction* (Osaka, Japan) *(HRI '10)*. IEEE Press, New York, NY, USA, 115–116.

[60] Meethu Malu and Leah Findlater. 2014. "OK Glass?" A Preliminary Exploration of Google Glass for Persons with Upper Body Motor Impairments. In *Proceedings of the 16th International ACM SIGACCESS Conference on Computers & Accessibility* (Rochester, New York, USA) *(ASSETS '14)*. Association for Computing Machinery, New York, NY, USA, 267–268. https://doi.org/10.1145/2661334.2661400

[61] Meethu Malu and Leah Findlater. 2015. Personalized, Wearable Control of a Head-Mounted Display for Users with Upper Body Motor Impairments. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 221–230. https://doi.org/10.1145/2702123.2702188

[62] Andreia Matos, Vítor Filipe, and Pedro Couto. 2016. Human-Computer Interaction Based on Facial Expression Recognition: A Case Study in Degenerative Neuromuscular Disease. In *Proceedings of the 7th International Conference on Software Development and Technologies for Enhancing Accessibility and Fighting Info-Exclusion* (Vila Real, Portugal) *(DSAI 2016)*. Association for Computing Machinery, New York, NY, USA, 8–12. https://doi.org/10.1145/3019943.3019945

[63] Kyle Montague, Hugo Nicolau, and Vicki L. Hanson. 2014. Motor-Impaired Touchscreen Interactions in the Wild. In *Proceedings of the 16th International ACM SIGACCESS Conference on Computers & Accessibility* (Rochester, New York, USA) *(ASSETS '14)*. Association for Computing Machinery, New York, NY, USA, 123–130. https://doi.org/10.1145/2661334.2661362

[64] Martez E. Mott and Jacob O. Wobbrock. 2019. Cluster Touch: Improving Touch Accuracy on Smartphones for People with Motor and Situational Impairments. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3290605.3300257

[65] Maia Naftali and Leah Findlater. 2014. Accessibility in Context: Understanding the Truly Mobile Experience of Smartphone Users with Motor Impairments. In *Proceedings of the 16th International ACM SIGACCESS Conference on Computers & Accessibility* (Rochester, New York, USA) *(ASSETS '14)*. Association for Computing Machinery, New York, NY, USA, 209–216. https://doi.org/10.1145/2661334.2661372

[66] Shuo Niu, Li Liu, and D. Scott McCrickard. 2014. Tongue-Able Interfaces: Evaluating Techniques for a Camera Based Tongue Gesture Input System. In *Proceedings of the 16th International ACM SIGACCESS Conference on Computers & Accessibility* (Rochester, New York, USA) *(ASSETS '14)*. Association for Computing Machinery, New York, NY, USA, 277–278. https://doi.org/10.1145/2661334.2661395

[67] Stephen J Page and Peter Levine. 2007. Modified constraint-induced therapy extension: using remote technologies to improve function. *Archives of Physical Medicine and Rehabilitation* 88, 7 (2007), 922–927.

[68] Mariah Papy, Duncan Calder, Ngu Dang, Aidan McLaughlin, Breanna Desrochers, and John Magee. 2019. Simulation of Motor Impairment With "Reverse Angle Mouse" in a Head-Controlled Pointer Fitts' law Task. In *The 21st International ACM SIGACCESS Conference on Computers and Accessibility* (Pittsburgh, PA, USA) *(ASSETS '19)*. Association for Computing Machinery, New York, NY, USA, 545–547. https://doi.org/10.1145/3308561.3354623

[69] Diogo Pedrosa, Maria da Graça Pimentel, and Khai N. Truong. 2015. Filteryedping: A Dwell-Free Eye Typing Technique. In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI EA '15)*. Association for Computing Machinery, New York, NY, USA, 303–306. https://doi.org/10.1145/2702613.2725458

[70] Diogo Pedrosa and Maria da Graça C. Pimentel. 2014. Text Entry Using a Foot for Severely Motor-Impaired Individuals. In *Proceedings of the 29th Annual ACM Symposium on Applied Computing* (Gyeongju, Republic of Korea) *(SAC '14)*. Association for Computing Machinery, New York, NY, USA, 957–963. https://doi.org/10.1145/2554850.2554948

[71] Dharani Perera. 2005. Voice Recognition Technology for Visual Artists with Disabilities in Their Upper Limbs. In *Proceedings of the 17th Australia Conference on Computer-Human Interaction: Citizens Online: Considerations for Today and the Future* (Canberra, Australia) *(OZCHI '05)*. Computer-Human Interaction Special Interest Group (CHISIG) of Australia, Narrabundah, AUS, 1–6.

[72] N. Poh, R. Blanco-Gonzalo, R. Wong, and R. Sanchez-Reillo. 2016. Blind subjects faces database. *IET Biometrics* 5, 1 (2016), 20–27.

[73] Melissa Quek, Daniel Boland, John Williamson, Roderick Murray-Smith, Michele Tavella, Serafeim Perdikis, Martijn Schreuder, and Michael Tangermann. 2011. Simulating the Feel of Brain-Computer Interfaces for Design, Development and Social Interaction. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Vancouver, BC, Canada) *(CHI '11)*. Association for Computing Machinery, New York, NY, USA, 25–28. https://doi.org/10.1145/1978942.1978947

[74] Yogachandran Rahulamathavan, Kunaraj R Sutharsini, Indranil Ghosh Ray, Rongxing Lu, and Muttukrishnan Rajarajan. 2019. Privacy-Preserving IVector-Based Speaker Verification. *IEEE/ACM Trans. Audio, Speech and Lang. Proc.* 27, 3 (March 2019), 496–506. https://doi.org/10.1109/TASLP.2018.2882731

[75] Karen Renaud, Kenneth C. Scott-Brown, and Andrea Szymkowiak. 2018. Designing authentication with seniors in mind. In *Proceedings of the Mobile Privacy and Security for an Ageing Population workshop at the 20th International Conference on Human Computer Interaction with Mobile Devices and Services (MobileHCI) 2018, Barcelona, Spain*. Association for Computing Machinery, New York, NY, USA, 7. https://mobilehci.acm.org/2018/,https://csalsa.gitlab.io/mobilehciageing/index.html 20th International Conference on Human-Computer Interaction with Mobile Devices and Services : Beyond mobile: the next 20 years, MobileHCI 2018 ; Conference date: 03-09-2018 Through 06-09-2018.

[76] Andreia Sias Rodrigues, Vinicius Kruger da Costa, Rafael Cunha Cardoso, Marcio Bender Machado, Marcelo Bender Machado, and Tatiana Aires Tavares. 2017. Evaluation of a Head-Tracking Pointing Device for Users with Motor Disabilities. In *Proceedings of the 10th International Conference on PErvasive Technologies Related to Assistive Environments* (Island of Rhodes, Greece) *(PETRA '17)*. Association for Computing Machinery, New York, NY, USA, 156–162. https://doi.org/10.1145/3056540.3056552

[77] Lucas Rosenblatt, Patrick Carrington, Kotaro Hara, and Jeffrey P. Bigham. 2018. Vocal Programming for People with Upper-Body Motor Impairments. In *Proceedings of the Internet of Accessible Things*. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3192714.3192821

[78] David Rozado, Jason Niu, and Martin Lochner. 2017. Fast Human-Computer Interaction by Combining Gaze Pointing and Face Gestures. *ACM Trans. Access. Comput.* 10, 3, Article 10 (Aug. 2017), 18 pages. https://doi.org/10.1145/3075301

[79] Zia Saquib, Nirmala Salam, Rekha P. Nair, Nipun Pandey, and Akanksha Joshi. 2010. A Survey on Automatic Speaker Recognition Systems. In *Signal Processing and Multimedia*, Tai-hoon Kim, Sankar K. Pal, William I. Grosky, Niki Pissinou, Timothy K. Shih, and Dominik Ślęzak (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 134–145.

[80] Sidas Saulynas and Ravi Kuber. 2017. Towards Brain-Computer Interface (BCI) and Gestural-Based Authentication for Individuals Who Are Blind. In *Proceedings of the 19th International ACM SIGACCESS Conference on Computers and Accessibility* (Baltimore, Maryland, USA) *(ASSETS '17)*. Association for Computing Machinery, New York, NY, USA, 403–404. https://doi.org/10.1145/3132525.3134785

[81] Syed W Shah and Salil S Kanhere. 2019. Recent Trends in User Authentication–A Survey. *IEEE Access* 7 (2019), 112505–112519.

[82] Anjana Sharma and Pawanesh Abrol. 2013. Eye Gaze Techniques for Human Computer Interaction: A Research Survey. *International Journal of Computer Applications* 71 (06 2013), 18–25. https://doi.org/10.5120/12386-8738

[83] Tsu-Wang Shen. 2008. Applied ECG Biometric Technology for Disability Population Personalization. In *Proceedings of the 2nd International Convention on Rehabilitation Engineering & Assistive Technology* (Bangkok, Thailand) *(iCREATe*

'08). Singapore Therapeutic, Assistive & Rehabilitative Technologies (START) Centre, Midview City, SGP, 103–107.

[84] Supriya Singh, Anuja Cabraal, Catherine Demosthenous, Gunela Astbrink, and Michele Furlong. 2007. Password Sharing: Implications for Security Design Based on Social Practice. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '07)*. Association for Computing Machinery, New York, NY, USA, 895–904. https://doi.org/10.1145/1240624.1240759

[85] Ivo Sluganovic, Marc Roeschlin, Kasper B. Rasmussen, and Ivan Martinovic. 2018. Analysis of Reflexive Eye Movements for Fast Replay-Resistant Biometric Authentication. *ACM Trans. Priv. Secur.* 22, 1, Article 4 (Nov. 2018), 30 pages. https://doi.org/10.1145/3281745

[86] Madoka Toriumi, Yuta Sugiura, and Koji Fujita. 2019. An Application for Wrist Rehabilitation Using Smartphones. In *Proceedings of the 21st International Conference on Human-Computer Interaction with Mobile Devices and Services* (Taipei, Taiwan) *(MobileHCI '19)*. Association for Computing Machinery, New York, NY, USA, Article 65, 6 pages. https://doi.org/10.1145/3338286.3344416

[87] "U.S. Census Bureau Reports" 2012. *Nearly 1 in 5 People Have a Disability in the U.S., Census Bureau Reports.* "U.S. Census Bureau Reports".

[88] Pan Wang, Gerald Choon-Huat Koh, Christian Gilles Boucharenc, and Ching-Chiuan Yen. 2017. Designing Two-Player Competitive Games for the Rehabilitation of Upper-Limb Motor Function after Stroke. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI EA '17)*. Association for Computing Machinery, New York, NY, USA, 2201–2209. https://doi.org/10.1145/3027063.3053069

[89] WebAIM 2012. *WebAIM: Motor Disabilities Types of Motor Disabilities.* WebAIM.

[90] Windows security 2017. *Interactive logon Do not require CTRL ALT DEL (Windows 10) - Windows security.* Windows security. https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-do-not-require-ctrl-alt-del

[91] Flynn Wolf, Ravi Kuber, and Adam J. Aviv. 2017. Perceptions of Mobile Device Authentication Mechanisms by Individuals Who Are Blind. In *Proceedings of the 19th International ACM SIGACCESS Conference on Computers and Accessibility* (Baltimore, Maryland, USA) *(ASSETS '17)*. Association for Computing Machinery, New York, NY, USA, 385–386. https://doi.org/10.1145/3132525.3134793

[92] Yubikey 2020. *YubiKey.* Yubikey. https://www.yubico.com/products/

[93] Linghan Zhang, Sheng Tan, and Jie Yang. 2017. Hearing Your Voice is Not Enough: An Articulatory Gesture Based Liveness Detection for Voice Authentication. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (Dallas, Texas, USA) *(CCS '17)*. Association for Computing Machinery, New York, NY, USA, 57–71. https://doi.org/10.1145/3133956.3133962

[94] Linghan Zhang, Sheng Tan, Jie Yang, and Yingying Chen. 2016. VoiceLive: A Phoneme Localization Based Liveness Detection for Voice Authentication on Smartphones. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (Vienna, Austria) *(CCS '16)*. Association for Computing Machinery, New York, NY, USA, 1080–1091. https://doi.org/10.1145/2976749.2978296

[95] Qiao Zhang, Shyamnath Gollakota, Ben Taskar, and Raj P.N. Rao. 2014. Non-Intrusive Tongue Machine Interface. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Toronto, Ontario, Canada) *(CHI '14)*. Association for Computing Machinery, New York, NY, USA, 2555–2558. https://doi.org/10.1145/2556288.2556981

[96] Xiaoyi Zhang, Harish Kulkarni, and Meredith Ringel Morris. 2017. Smartphone-Based Gaze Gesture Communication for People with Motor Disabilities. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 2878–2889. https://doi.org/10.1145/3025453.3025790

[97] Shaojian Zhu, Yao Ma, Jinjuan Feng, and Andrew Sears. 2009. Don't Listen! I Am Dictating My Password!. In *Proceedings of the 11th International ACM SIGACCESS Conference on Computers and Accessibility* (Pittsburgh, Pennsylvania, USA) *(Assets '09)*. Association for Computing Machinery, New York, NY, USA, 229–230. https://doi.org/10.1145/1639642.1639689