A3C: An Image-Association-Based Computing Device Authentication Framework for People with Upper Extremity Impairments

BRITTANY LEWIS and PRIYANKAN KIRUPAHARAN, The University of Rhode Island, Kingston, RI, USA
TINA-MARIE RANALLI, Independent Scholar, Providence, RI, USA
KRISHNA VENKATASUBRAMANIAN, The University of Rhode Island, Kingston, RI, USA

Current computing device authentication often presents accessibility barriers for people with **upper extremity impairments (UEI)**. In this article, we present a framework called **Accessible image-Association-based Authentication for Computing devices (A3C)**, a novel recognition-based graphical authentication framework specifically designed for people with UEI to authenticate to their computing devices. A3C requires users to provide a set of primary images the user knows that are recognizable to them and subsequently associate each primary image with a secondary image. To evaluate the efficacy of the A3C framework, we instantiated the framework by implementing a version of A3C called **A3C-FA**, which uses images of faces of people the user knows as the primary image and animal images as the secondary image. We then performed three studies to evaluate A3C-FA: a shoulder-surfing attack study ($N = 319$), a close-adversary attack study ($N = 268$), and a usability study with people with UEI ($N = 14$). We found that A3C was robust against both shoulder-surfing and close-adversary attacks. We also performed a detailed study to evaluate the accessibility of A3C-FA. Our participants reported that A3C-FA was more usable and more secure than the authentication approaches with which they were familiar. Based on these findings, we suggest four areas of future research to further improve the design of the A3C framework.

CCS Concepts: • **Human-centered computing** → **Accessibility technologies**; **Empirical studies in accessibility**;

Additional Key Words and Phrases: Upper extremity impairments, computing device authentication, graphical authentication, accessibility

ACM Reference format:
Brittany Lewis, Priyankan Kirupaharan, Tina-Marie Ranalli, and Krishna Venkatasubramanian. 2024. A3C: An Image-Association-Based Computing Device Authentication Framework for People with Upper Extremity Impairments. *ACM Trans. Access. Comput.* 17, 2, Article 6 (May 2024), 37 pages.
https://doi.org/10.1145/3652522

This work is supported in part by the National Science Foundation grant CNS-1947022.
Authors' Contact Information: Brittany Lewis, The University of Rhode Island, Kingston, RI, USA; e-mail: bflewis@uri.edu; Priyankan Kirupaharan, The University of Rhode Island, Kingston, RI, USA; e-mail: pkirupaharan@uri.edu; Tina-Marie Ranalli, Independent Scholar, Providence, RI, USA; e-mail: ranalli@gmx.com; Krishna Venkatasubramanian (Corresponding author), The University of Rhode Island, Kingston, RI, USA; e-mail: krish@uri.edu.

ACM 1936-7236/2024/5-ART6
https://doi.org/10.1145/3652522

1 INTRODUCTION

When a user starts using one of their computing devices (e.g., laptop, tablet, smart phone), often the first action they need to perform is to authenticate to that device (e.g., type a PIN, use facial recognition). However, the current ways of authenticating on personal computing devices typically require users to perform complex actions with their arms, hands, and fingers. This is the case from typing complex passwords to accurately positioning one's face in front of a camera for facial recognition. Such authentication options are thus often not accessible to people with **upper extremity impairments (UEI)** [47, 54]. People with *UEI* experience reduced **range of motion (ROM)**, strength, endurance, speed, and/or accuracy associated with movement in the shoulders, upper arms, forearms, hands, and/or fingers. People experience UEI for a variety of reasons, such as traumatic injuries, degenerative conditions, amputations, and movement disorders [94]. Over 20 million people in the United States have conditions that can lead to UEI [87].

Authentication is the process of proving one's identity (in our case, to a personal computing device) [54]. Broadly speaking, authentication has two main stages: *setup*, where one initializes the personal computing device and registers a credential (e.g., a password or a biometric); and *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. In our prior work, we found that all stages of authentication present barriers to people with UEI, from credential setup to credential verification. Further, these problems persist not only with password/PINs but also with biometric-based solutions. People with UEI often use **assistive technologies (AT)**, such as eye-gaze trackers, voice-interfaces, and so forth, to interact with computing devices, including the act of authenticating to them. Finally, people with UEI have devised a wide range of workarounds to overcome the obstacles to authentication, which typically prioritize usability over the security that authentication provides [54]. *Consequently, in this article we aim to develop an authentication approach for people with UEI that is: secure, usable (in terms of not requiring dexterous use of one's upper extremities), and works with any AT a user with UEI may utilize.*

To this end, we present a novel authentication framework called **A3C: Accessible image-Association-based Authentication for Computing devices**. A3C is based on a recognition-based graphical authentication framework[1] that is designed specifically for people with UEI to authenticate to their computing devices. During *setup*, A3C requires users to provide a set of *primary images* that the user knows are *recognizable* to them. Subsequently, the user is asked to *associate* each primary image with a *secondary image* (from a list of potential images provided by A3C). We define association as the process of mentally linking two disparate images for any reason and the user registers this association into the A3C system. Next, A3C's credential verification consists of a two-phase process. During the first phase, the user is asked to *recognize* and *select* (i.e., point and click an image) the one-to-three user-selected primary images present in a grid of images that predominantly contains *decoy* images of the same type as the user-selected images. Then, in the second phase, the user is presented with one of the images from phase one that A3C chooses at random and is asked to *identify* and *select* the one secondary image with which it is associated, again from a grid of images, which contain decoy images except the one correct secondary image. Thus, to authenticate successfully, users have to select *all* of the one-to-three correct primary images as well as the correct secondary image that is associated with the one randomly selected primary image.

[1] *Recognition-based graphical authentication* generally asks users to memorize a portfolio of images during setup and then recognize their images from among decoys to authenticate [11].

It can be seen that all A3C requires is for the user to select—that is, point and click—images on the screen. A3C's focus on simple selection rather than more complex physical tasks allows it to provide several *accessibility advantages* to people with UEI, including the following: (1) it avoids complex or dexterous input and instead only requires the selection of several large images on the screen; (2) it works with any variety of AT that people with UEI already use for computing, such as voice, eye-gaze tracking, mouth sticks, or adaptive mice and keyboards—all of which fundamentally support the selection action that A3C requires; and (3) it leverages the advantages of recognition-based graphical authentication solutions and it decreases the cognitive and memory effort for authentication [11].

A3C is, however, simply a framework that provides a general approach to authentication. To determine its efficacy, we have to instantiate it by implementing it with a specific type of primary and secondary images. To this end, we implemented A3C-FA that uses face images of people the user knows as the primary images and has the user associate an animal image, as the secondary image, with each primary face image. We then performed three studies to evaluate the security and accessibility of A3C-FA. The first was a shoulder-surfing attack study ($N = 319$). We found that A3C-FA was robust against shoulder-surfing attacks with 68.6% of attackers failing to authenticate, even after five attempts, as opposed to only 11.3% of attackers failing to authenticate after five attempts with the well-known recognition-based graphical authentication system called Passfaces that we used as the control for our study [15]. Next, we conducted a close-adversary attack study ($N = 268$) that simulated A3C-FA being attacked by a person with prior knowledge about the target-user. A3C-FA was robust against in this case, with 81.7% of attackers failing to authenticate, even after 15 attempts. Finally, we conducted an accessibility evaluation of A3C-FA with people with UEI ($N = 14$). We found that A3C-FA was usable, that is, its images were easy to remember over time. Thirteen of the 14 individuals with UEI from our study were able to authenticate without any errors a month after the initial authentication setup. Further, we did a detailed qualitative analysis of A3C-FA by conducting semi-structured interviews with the 14 individuals with UEI. We found that they thought A3C-FA was more usable and secure than other alternatives, such as passwords, biometrics, and other graphical authentication methods they had used in the past. These 14 individuals with UEI also provided suggestions for updating A3C-FA to better fit their personal needs. Based on the findings of all these studies, we present four areas for future work to improve the larger A3C framework as a secure and accessible authentication solution for computing devices for people with UEI.

2 RELATED WORK

To contextualize this article, we cover the following three categories of research that relate to our work here: available authentication solutions for people with UEI, AT for people with UEI, and recognition-based authentication solutions. We next explore research in these areas in more detail. Table 1 summarizes various prior authentication methods designed for people with UEI and their limitations.

2.1 Authentication Solutions for People with Disabilities

Recent years have also seen a variety of new authentication solutions for people with disabilities. Most of this work has focused on people with visual impairments [2, 6, 8, 16, 27, 36, 51, 67, 75, 99] and the rest focused on people with cognitive impairments (e.g., Down syndrome) [44, 56, 57].

Recent authentication solutions have also been designed for people with UEI, including the use of credentials such as voice trait [65], cardiac signal [53, 77], QR codes [23]; and new entry methods via password dictation [104], foot-based entry [93], and through wearables [34]. However, almost none of these studies was evaluated by people with UEI. Hence, it is not clear how well they would

Table 1. A Summary of the Limitations of Existing Authentication Solutions for People with UEI

Authentication factors	Modality	Study details	Limitation
Something you are	Biometric	Voice trait [65]	Not evaluated for people with UEI, hence it is not clear how well they would work for the population for which they are designed
	Physiological	Cardiac signal [77]	Not evaluated for people with UEI, hence it is not clear how well they would work
		Cardiac signal [53]	Requires the use of a head-mounted device (i.e., Google Glass), which is not always available to users
Something you have	Smart devices	Through wearables [34], QR codes [23]	None of these studies was evaluated for people with UEI, hence it is not clear how well they would work for the population for which they are designed
Something you know	Foot	Foot-based entry [93]	Not evaluated for people with UEI, hence it is not clear how well they would work for the population for which they are designed
	Voice	New entry methods via password dictation [104],	Not evaluated for people with UEI, hence it is not clear how well they would work for the population for which they are designed
	Cognitive	Recall-based approaches [28, 37, 39, 45, 76, 82, 96], cued-recall-based approaches [10, 13, 19, 20, 97]	Both recall-based and cued-recall-based approaches are known to require the user to create a specific pattern or gesture and then recall this pattern/gesture to authenticate. However, such solutions often require considerable motor control to use effectively [11]
		Recognition-based approaches [26, 41, 48, 66, 69, 81, 84, 85, 95]	Susceptible to attacks, such as shoulder surfing [11]
		Introducing distortion to images [38, 43, 101]	Even with distortion, recognition-based models are vulnerable to user-knowledge attackers who know the user and can use that knowledge to guess the user-uploaded images [84]
		A study that uses an additional association is PassTag [41]	Not ideal for someone with UEI because it requires text entry, which is considerably burdensome for people with UEI [54]

work for the population for which they are designed. The one exception is [53], which is our own prior work. However, the authentication solution requires the use of a head-mounted device (i.e., Google Glass), which is not always available to users. The goal of the present work is to create an authentication framework that is conducive to the abilities of various people with UEI, including whatever AT they may use.

2.2 Compensating for Reduced ROM for People with UEI

One of the main impairments that people with UEI experience with their limbs is limited ROM, which directly affects their ability to interact with computing devices [98]. Consequently, people with UEI often use AT to compensate [55]. There have been numerous studies on designing novel AT solutions to help people with UEI, especially with limited ROM, when interacting with computing

devices. These include the use of: voice input [12, 42, 72], eye-based input [32, 33, 50, 103], head-movement input [21, 70], brain-computer input [29, 62], facial or mouth-based gestures [40, 61, 92], touch input [18, 78, 89], hand or arm gestures [4, 5, 74], and biometrics [49, 52, 63]. All of these solutions support the basic operation of selecting objects (e.g., images) on the screen. In the present work, we have developed a new authentication framework that works with any of these existing AT solutions designed for people with UEI.

2.3 Recognition-Based Authentication Solutions

Over the years, many graphical authentication approaches have been proposed [11]. These generally fall into three categories: recall-based approaches [28, 37, 39, 45, 76, 82, 96], cued-recall-based approaches [10, 13, 19, 20, 97], and recognition-based approaches [26, 41, 48, 66, 69, 81, 84, 85, 95]. Both recall-based and cued-recall-based approaches are known to require the user to create a specific pattern or gesture and then recall this pattern/gesture to authenticate [11]. However, such solutions are known to often require considerable motor control to use effectively [11], which is typically difficult for users with UEI.

Recognition-based approaches, on the other hand, rely on the user recalling information, usually images, that they choose during setup. The user then selects those images out of a set that also includes *distractor* images provided by the system. These systems distinguish themselves according to the type of images they use. For example, one class of approaches uses face images originally obtained from a stock collection [15], a personal photograph collection [84], or celebrity photos [48]. Recognition-based approaches need not use images of people. Approaches have been proposed that use a variety of images, such as random art [26], icons [9], and a portfolio of diverse images [24, 60]. Recognition systems work more effectively for people with UEI, as compared to other graphical authentication solutions in general, because they only require the user to click on images to authenticate, which is something that people with UEI can often perform using the AT they already have.

Even though these basic recognition-based approaches are potentially usable for people with UEI, they have issues with being susceptible to attacks such as shoulder surfing [11]. Consequently, over the years, some work has been done to make such recognition-based authentication solutions more robust against attacks by introducing distortion to the images [38, 43, 101]. However, even with distortion, recognition-based models are vulnerable to user-knowledge attackers who know the user and can use that knowledge to guess the user-uploaded images [84]. One proposed method of foiling a knowledge-based attacker is to require an additional secret, such as through a secondary association. A recent study that uses an additional association is PassTag [41]. During setup, PassTag requires the user to provide images to the system or select images from stock images. However, the user is also expected to provide a short phrase for each image. During authentication, the user is expected to identify the images they provided during setup (similar to Passfaces, the well-known recognition-based graphical authentication system that we used as the control for our study) and also type the text they want to associate with each image. PassTag is not ideal for someone with UEI because it requires text entry, which is considerably burdensome for people with UEI [54]. Like PassTag, our proposed authentication framework (i.e., the A3C framework) also uses a recognition-based authentication system with two phases. However, A3C's second phase is image-based instead of requiring typing, which is more conducive to users with UEI.

3 THREAT MODEL

Before describing A3C in detail, it is important to understand its *threat model*, which describes the assumptions we, as its designers, made about the capabilities of the adversaries against whose actions A3C has to be resilient.

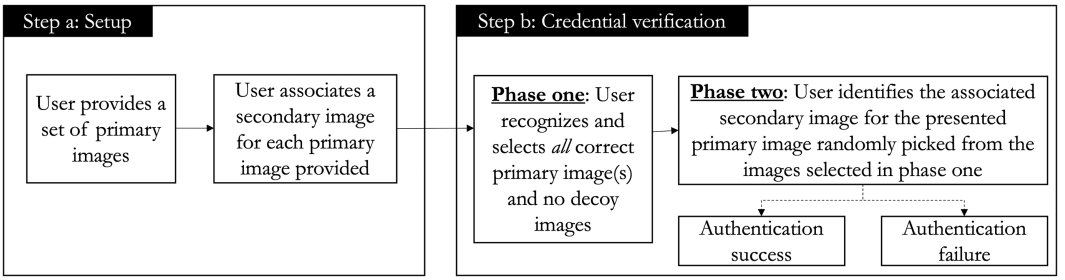


Fig. 1. A diagram illustrating the operation of the A3C framework.

In this work, we consider two main adversaries: opportunistic adversaries and close adversaries. *Opportunistic adversaries* are strangers who may have the opportunity to shoulder surf, that is, to observe and record the user authenticating (a limited number of times) to the device before trying to authenticate themselves [59]. *Close adversaries* are people, such as contracted caregivers, who have more intimate access to their victim. They may know the user from working with them and are able to use this knowledge (in addition to shoulder surfing a limited number of times) to gain access to the system [41]. We made the following global assumptions about the abilities of these two categories of adversaries:

(1) We assume the adversaries are not able to interfere with the setup of the authentication credentials.
(2) We assume the adversaries access the computing devices surreptitiously and therefore:
    (a) cannot threaten or intimidate the user into unlocking the device.
    (b) are only able to access the user's device a limited number of times while remaining surreptitious.
(3) We assume the adversaries are *UI-bound adversaries*, that is, adversaries who do not have sophisticated technical knowledge and are therefore limited to interacting with devices through the provided user interface [35].

We also assume that *none* of the adversaries is a *trusted caregiver*. Trusted caregivers are close family members or long-term caregivers who have known the user for a long time and have earned the user's trust. The user may share access or authentication credentials with trusted caregivers. As these caregivers are trusted by the user with disabilities, we do not consider them to be part of the threat model for this work.

4 ACCESSIBLE IMAGE-ASSOCIATION-BASED AUTHENTICATION FOR COMPUTING DEVICES

In this work, we propose a novel form of recognition-based graphical authentication framework called *Accessible image-Association-based Authentication for Computing devices* or A3C. The *A3C framework* is an authentication approach that leverages recognition-based graphical authentication to provide an accessible way for people with UEI to authenticate into their computing devices (e.g., laptop, tablet). In this section, we first provide an overview of the A3C framework and then describe an instantiation of this framework that uses face images and animal images.

4.1 The A3C Framework: Overview

Like all authentication approaches, A3C consists of two steps: (1) *setup*, where the user establishes their graphical authentication credentials and (2) *credential verification*, where the user provides their credentials to the system to be authenticated (see Figure 1).

During setup, the user (1) *provides* A3C with a set of *primary images* that the user knows that are *recognizable* to them and (2) *associates* a *secondary image* (from a list of potential images provided by A3C) with each primary image. We define association as the process of *mentally linking* two images. This link is entirely in the mind of the user and is never documented in any form. In addition to the user's recognition of the primary images, it is the undocumented link between the primary and secondary images that provides A3C's security. The type of association that the user makes between the primary and secondary image is unspecified. The association can be made for any reason.

Having a secondary image associated with a primary image also provides another advantage. The process of associating a secondary image with a primary image provides the advantage of the *levels-of-processing effect*, which suggests that the deeper one processes a piece of information (e.g., the stronger a connection one makes to it), the stronger one's ability to recall the information [22]. Further, prior research has shown that when memory connections are related to a person or thing for which someone cares, it increases their ability to recall them [71]. Therefore, having the user associate a secondary image with each selected primary image, as part of A3C, makes it easier for them to remember both images. The user has complete freedom to associate whatever secondary image they want for each primary image, including associating the same secondary image for multiple primary images.

Once the setup is complete, anytime the user wants to authenticate with A3C, they have to perform credential verification. A3C's credential verification has two phases: (1) *phase one*: the user is asked to *recognize and select* the one-to-three user-selected primary images present in a grid of images, generated by A3C, that predominantly contains *decoy* images of the same type as the user-selected images; (2) *phase two*: the user is presented with a randomly chosen primary image from their selection in phase one and asked to *identify and select* the associated secondary image. To authenticate successfully, the user must select *all* of the one-to-three correct primary images and then also correctly identify the secondary image that is associated with the randomly chosen primary image.

Even if the user incorrectly selects one or more of the faces in the first phase, the system will always continue to the second phase. The reason for always continuing to phase two regardless of the user's selection in the first phase is to avoid leaking information to potential adversaries about whether or not there was an error and the source of the error. Therefore, if a user (by mistake) or an adversary selects one or more of the decoy images in the first phase of verification, it is possible for one of these decoy images to be presented for the secondary image association in phase two, even though no secondary image was ever associated with the decoy image during setup. Figure 2 shows the various scenarios of operation for the A3C framework and the only scenario in which authentication succeeds. We believe this to be right usability versus security tradeoff for A3C because of the use of recognition-based authentication as its basis, which makes it easier for a legitimate user to remember their credentials.

A3C provides a general framework for authentication. The primary and secondary images used in A3C can be of any type. Further, the associations between the primary and secondary images can be anything that is easy to remember to the user, such as associations based on appearance, shapes, random reasons, and so forth. The type of association can also vary from one primary-secondary image pair to the next.

4.2 Our Instantiation of A3C: A3C-FA

A3C provides a larger framework for authentication. To deploy this framework, one must select the type of primary and secondary images to use. For our instantiation of A3C, we used images of the faces of people the user knows for the primary images and animal images for the secondary

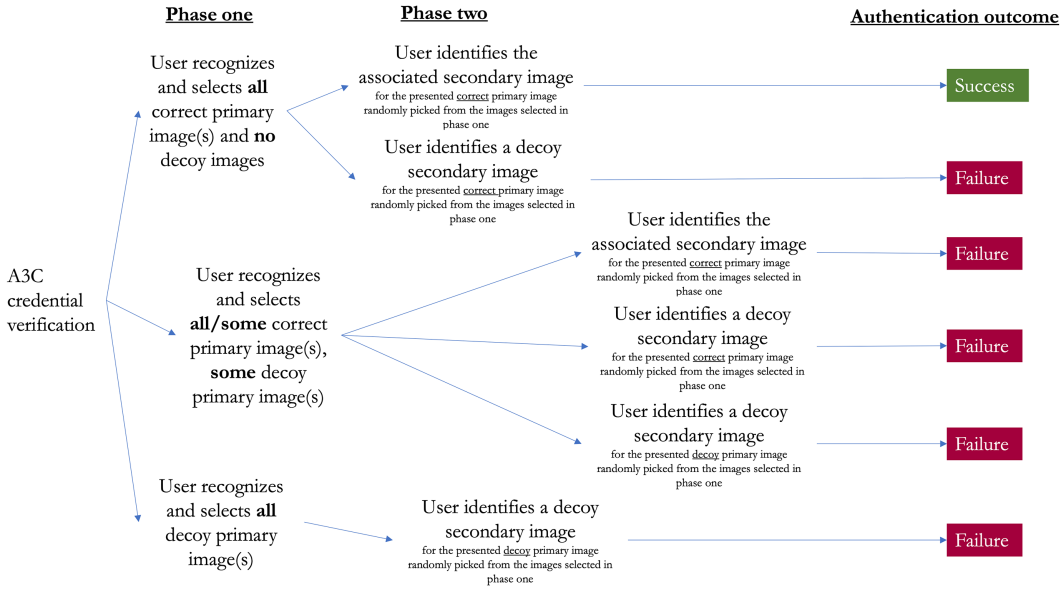


Fig. 2. A diagram illustrating the various scenarios of operation of A3C and the authentication success or failure it leads to.

images. To differentiate between the larger framework and an instantiation of it, we refer to the instantiation of A3C we used for this study as A3C-FA. Figure 3 illustrates the setup and credential verification steps of A3C-FA, which we describe below.

4.2.1 A3C-FA's Setup. During setup, the user provides a collection of images that contain people they know. The system then extracts the faces of those people from the images. A3C-FA uses the RetinaFace system [25] to extract and crop the faces from the images provided by the user. These images form the set of primary images the user will need to recognize during credential verification. The images of faces used for the primary image set needed to be front angle or 45° angle shots. This is because the decoy face images used by A3C-FA during credential verification come from the WIDER FACE dataset [100], which only have front or 45° angle images. For every primary image, A3C-FA asks the user to associate with it a secondary image of an animal from a dataset of 105 animal images maintained by the system [7].

4.2.2 A3C-FA's Credential Verification. To authenticate, the user is first presented with a grid containing nine images of human faces in *phase one* of the credential verification. The grid contains between one and three face images the user provided during setup. The rest of the images in the grid are decoy face images taken from the WIDER FACE dataset. The user must recognize and select *all* one-to-three face images they provided during setup that are present in the grid while selecting *none* of the decoy images.

After the user submits their face image selection, they are presented with one randomly chosen face image (from those they just identified in phase one) along with a grid of 10 animal images in *phase two* of the credential verification. The user then identifies the animal image they believe is associated with the given face image (based on the association they made during setup). As mentioned before, the animal images come from the same set of 105 stock images used during the setup phase.

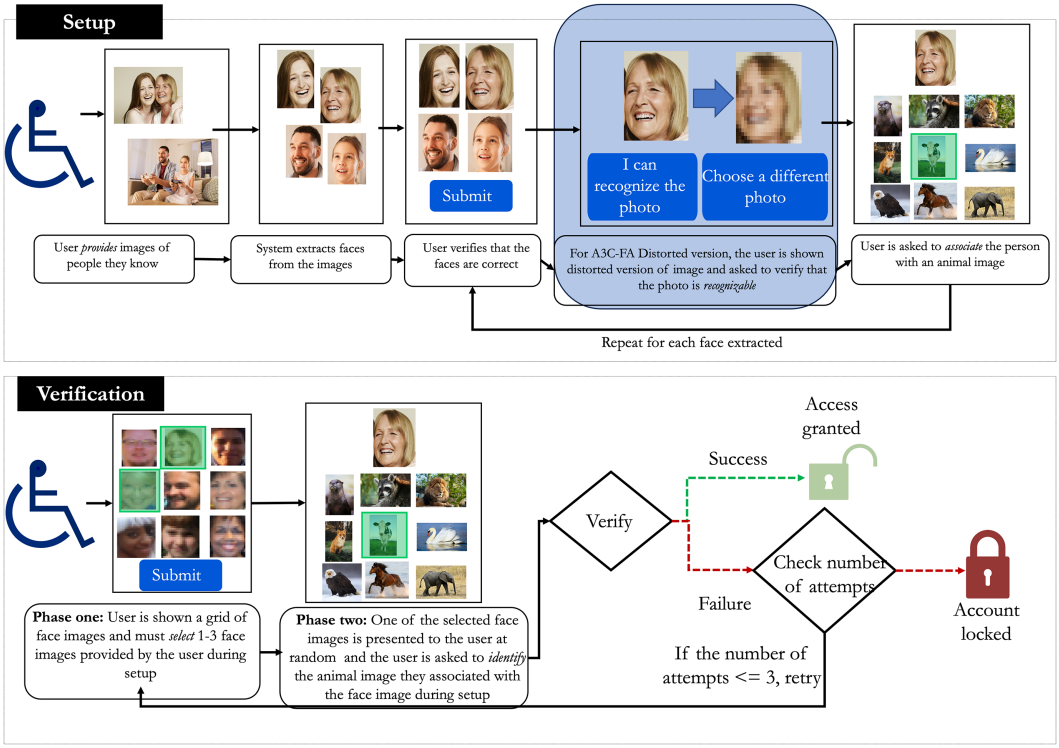


Fig. 3. A diagram illustrating the operation of A3C-FA.

If the user makes any mistakes during credential verification, they are allowed to have two additional *attempts* to authenticate. If they fail after all three, they are locked out.

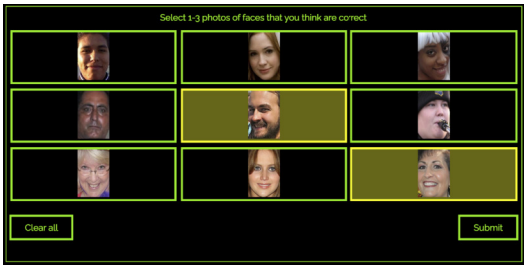
4.2.3 Distorted and Undistorted A3C-FA. We implemented two versions of A3C-FA, which we refer to as (1) A3C-FA Distorted and (2) A3C-FA Undistorted. In A3C-FA Distorted, the face (primary) images are distorted in some way. In A3C-FA Undistorted, the face images are unchanged. We applied distortion under the premise that it would make it more difficult for adversaries to select the correct faces without affecting the user's ability to do the same. Further, A3C-FA Distorted only distorts the face images and *not* the associated animal (secondary) images, since only the first set of images is subject to recognition by the user, whereas the second set of images is subject to association by the user. Figure 4 shows screenshots of the two versions of A3C-FA.

4.3 Entropy of A3C-FA

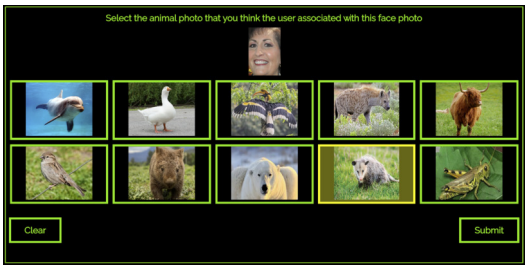
Since A3C-FA is an authentication solution, we provide a quick theoretical analysis of the effort it would take to brute-force it, expressed as its *entropy*. The entropy of an authentication solution represents the complexity of brute-forcing the solution, expressed in terms of guessing an n-bit, random, cryptographic key [58]. For A3C-FA, the entropy is given by the following equation:

$$E = \log_2 \left(\left[\sum_{i=1}^{k} \binom{n}{f-i} \binom{f}{i} \right] \binom{m}{a-l} \binom{a}{l} \right), \tag{1}$$

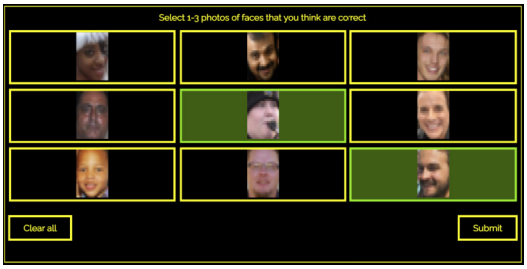
where n is the total number of decoy images in the database for phase one; k is the maximum number of correct images shown to the user in phase one; m is the total number of decoy images



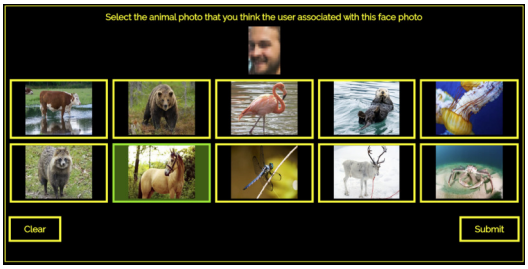
(a) Example of A3C-FA Undistorted - face grid



(b) Example of A3C-FA Undistorted - animal grid



(c) Example of A3C-FA Distorted - face grid



(d) Example of A3C-FA Distorted - animal grid

Fig. 4. Screenshots demonstrating the two main versions of A3C-FA.

in the database for phase two; f is the number of images shown to the user in phase one; a is the number of images shown to the user in phase two; and l is the number of images that can be selected by the user in phase two.

The entropy takes this equation because:

— *Equation part 1*: To successfully brute-force A3C-FA, the attacker has to be able to select all the one-to- three images that appear in the primary face images grid. However, when the attacker selects primary images from this grid, they do not get any feedback on their choices (unless they end up successfully authenticating, in which case they would know that they correctly guessed everything in both grids) (see Figure 2). Consequently, they would have to keep track of all the face grids possible in phase one of A3C-FA, given as $\binom{n}{f-i}$, and when the same face grid appears again, select the $1 \leq i \leq k$ correct face images from the f images shown in the grid. The product of these two will return the total number of combinations the user has to attempt for a given correct number of i faces shown in phase one. Now, since i is not a fixed number but varies between 1 and k, we take the summation of all these individual products for each value of i between 1 and k.

$$\sum_{i=1}^{k} \binom{n}{f-i}\binom{f}{i}$$

— *Equation part 2*: Subsequently, in phase two, the user is expected to pick the associated image for the one randomly chosen face image from phase one. Similar to phase one, the attacker has to again keep track of all the grids possible for phase two as well which is $\binom{m}{a-1}$. From this combination, the user has to select $l = 1$ correct images from a images shown in the grid to the user, which comes to

$$\binom{m}{a-l}\binom{a}{l}.$$

— *Equation part 3*: Consequently, to calculate the total number of combinations needed to successfully brute-force A3C-FA, we have to get the product of Equations (1) and (2). We then take the log_2 of the total number of combinations to calculate the entropy, as shown in Equation (1).

In the context of our A3C-FA implementation, where the parameters were set as follows: $n = 32,203$, $k = 3$, $m = 105$, $f = 9$, $a = 10$, $l = 1$, the entropy comes to 152.4 bits. For comparison, one of the standard lengths of the encryption keys used for Advanced Encryption Standard (AES), a common and secure encryption algorithm, is 128 bits long [1]. An interesting aspect of A3C-FA is that we can, of course, arbitrarily increase the entropy of A3C-FA by increasing the size of the decoy datasets without affecting the usability of the system for the user.

5 STUDY METHODOLOGY

Similar to [41], we conducted three core studies to evaluate the efficacy of the A3C framework. To this end, we evaluated our instantiation of the A3C framework, which used face and animal images (i.e., A3C-FA). These studies sought to evaluate the (1) security and (2) accessibility of A3C-FA. The protocol for each of these three studies was approved by the University of Rhode Island's Institutional Review Board. The studies were as follows:

— *A shoulder-surfing attack study*: The goal of this study was to evaluate A3C-FA's resiliency against shoulder surfing, where adversaries watch the user authenticate (one or more times) and then use that information to authenticate as the user.
— *A close-adversary attack study*: The goal of this second study was to evaluate A3C-FA's resiliency against adversaries who have some knowledge about the user and can make educated guesses to attempt to authenticate as the user.
— *An accessibility study*: Finally, the goal of the third study was to evaluate how usable A3C-FA is for people with UEI and how well they are able to remember their authentication credentials over time.

Next, we will discuss these three studies in detail, along with their results.

6 STUDY 1: SHOULDER-SURFING ATTACK STUDY

Our first study involved evaluating the resiliency of A3C against shoulder-surfing attacks. A *shoulder-surfing attack* is when an adversary is able to watch the user authenticate and then use what they learned to attempt to authenticate as the user [14].

6.1 The Shoulder-Surfing Attack Process

The shoulder-surfing attack study was run online on the Amazon Mechanical Turk platform (i.e., MTurk) [3]. We use the term *participant* to refer to the person on MTurk acting as the adversary performing the shoulder-surfing attack. We use the term *target-user* to refer to the fictitious user (created by the first author) whose credentials the adversary is trying to guess via shoulder surfing. The shoulder-surfing attack is structured as a three-step process, as follows:

— *Watch video/Shoulder surf*: First, the participants were shown a video of one instance of the target-user successfully authenticating with A3C-FA. The participants could not pause, rewind, or re-watch the video. The purpose of this was to mimic an adversary observing a target-user authenticating in real life.
— *Play game*: Next, the participant was asked to play a short game of *snake* for a minimum of 1 minute. The purpose of the game was to clear the participant's immediate memory of the video. Using games or breaks are common approaches used in security studies for this purpose

[79, 102]. The use of games thus simulates the natural delay between the act of shoulder surfing and the attempt to authenticate with that information.
— *Attempt to authenticate as the target-user*: Subsequently, the participants were asked to use the information they gained from watching the video to authenticate as the target-user.

6.2 Shoulder-Surfing Attack Study: Treatments

We performed a *between-group* study for this project where participants were placed in one of three treatment groups: (1) A3C-FA Undistorted; (2) A3C-FA Distorted; and (3) Passfaces [15].

Passfaces was used as a control for this study. Passfaces acts like a PIN in that the user must select a series of faces in the correct order. For each page of Passfaces, there is a 3×3 grid containing nine images of human faces. The images are of the same faces every time. However, the positions of the faces are randomized every time to decrease the efficacy of shoulder surfing-based attacks. On each page, the user selects the one correct face image for that part of the sequence. The correct image does not depend on the face's position in the grid [15]. We used a four-page implementation of Passfaces, that is, the user had to identify the faces four times (in four separate grids) correctly to successfully authenticate. Participants assigned to the Passfaces treatment followed the same three-step attack process (watch video, play game, and perform attack) as described above for A3C-FA. Passfaces was chosen as the control for our study because it is a well-established recognition-based graphical authentication system which centers around identifying faces from a grid of face images [15]. Additionally, it has been shown to perform similarly or better than alphanumeric passwords of a similar length [46, 83].

6.3 Shoulder-Surfing Attack Study: Procedure

The study procedure consisted of three main parts: *the study introduction*, a *practice session*, *five attempts at the shoulder-surfing attack*, and an *end survey*. A diagram of the process for the shoulder-surfing attack study is shown in Figure 5.

For the *study introduction*, all participants were shown an online version of the consent form and were asked to agree to participate in the study. They were then asked to watch an approximately 5-minute video that gave an overview of A3C-FA and their role as the adversary performing the shoulder-surfing attack. The participants were allowed to pause, rewind, or re-watch the introduction video as many times as they wanted.

After the introductory video ended, they were given *one practice* session with a shoulder-surfing attack. The practice session was identical to the actual three-step shoulder-surfing attack described above except that it used different credentials, derived from different face (primary) images and different animal associations.

At the end of the practice session, participants were shown a video of the target-user authenticating and then given *one attempt* to authenticate using the information gained from the video. At the end of the attempt, participants were shown whether or not they were successful. If they were successful in authenticating, they would proceed to the survey and end the study early. If not, then they were shown another video of a different iteration of the target-user authenticating and then again given one attempt to authenticate. This continued three more times for a total of *five total authentication attempts* for each participant. To incentivize the participants, they were also told (at the beginning of the study) that if they they were successful before the fifth authentication attempt, they would immediately be taken to the survey and thus finish the study early. The participants were told that their compensation would not be affected by finishing the study early.

After the participants were successful or they completed all five attempts, they proceeded to the *survey* at the end of the study. The survey asked basic questions about their demographics and their experience with guessing the face and animal images. The survey also included what is commonly

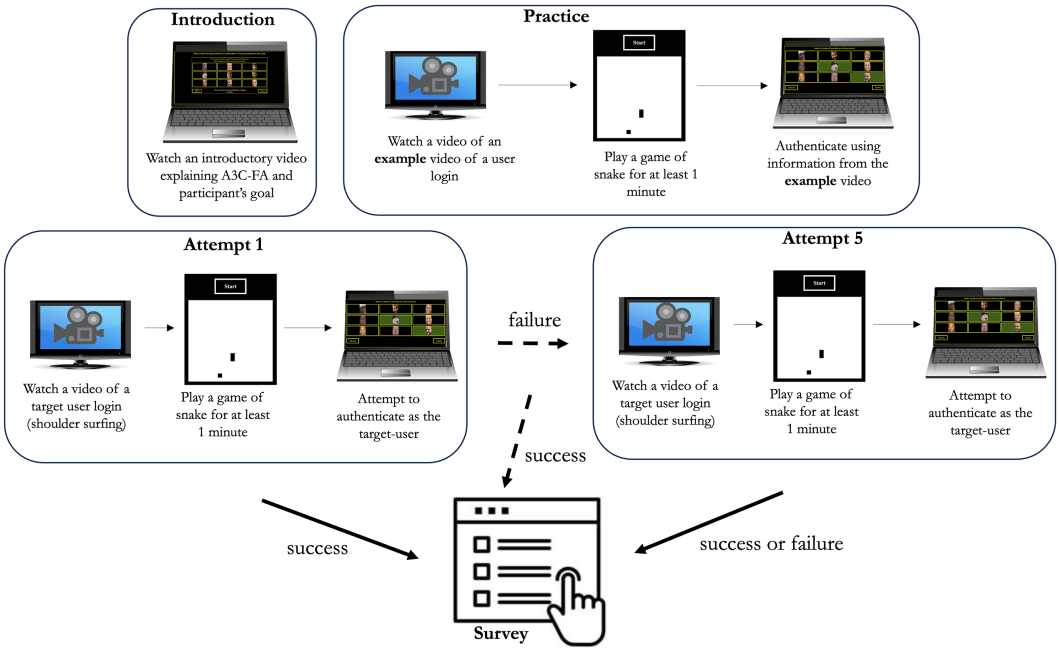


Fig. 5. This diagram summarizes the procedure for the shoulder-surfing attack study.

Table 2. Demographics for the Participants in the Shoulder-Surfing Attack Study

Treatment	Gender			Age					
	M	F	NB	18–24	25–34	35–44	45–54	55–64	65–74
A3C-FA Undistorted	73	32	0	6	58	27	7	5	2
A3C-FA Distorted	71	36	1	8	57	25	8	9	1
Passfaces	69	37	0	4	62	24	11	2	3
Total	213	105	1	18	177	76	26	16	6

"NB" stands for nonbinary.

referred to as a *self-reported honesty check*. Our *self-reported honesty check* asked participants if they had tried their best to authenticate. It has been shown in previous studies that such checks are successful in preserving data quality [30, 73]. The participants were also asked about any specific strategies they used while attempting to authenticate at the target-user.

6.4 Shoulder-Surfing Attack Study: Participants

Only participants located in the United States or Canada and 18 years of age or older were recruited on MTurk. Participants were given $4 for their participation[2] After removing all the participants who failed the self-reported honesty check (by reporting that they did not try their best to authenticate as the target-user), we had a total of 319 participants. These participants were in three treatment groups with 105 participants viewing A3C-FA Undistorted (*S-UD1 through S-UD105*), 108 participants viewing A3C-FA Distorted (*S-D1 through S-D108*), and 106 participants viewing Passfaces (*S-PF1 through S-PF106*). A summary of the participant demographics can be seen in Table 2.

[2]As the study takes about 20 minutes to complete, $4 is a rate of approximately $12 per hour.

Table 3. Results for the Shoulder-Surfing Attack Study for the Three Treatments: A3C-FA Undistorted, A3C-FA Distorted, and Passfaces (as Control)

	A3C-FA Undistorted	**A3C-FA Distorted**	**Passfaces**
Successful attacks on Attempt 1	9	2	55
Successful attacks on Attempt 2	7	7	27
Successful attacks on Attempt 3	5	8	6
Successful attacks on Attempt 4	6	11	5
Successful attacks on Attempt 5	6	2	1
Total successful participants	33 (31.4%)	30 (27.8%)	94 (88.7%)
Total failed participants	72 (68.6%)	78 (72.2%)	12 (11.3%)
Total participants	105	108	106

6.5 Shoulder-Surfing Attack Study: Quantitative Evaluation

Overall, A3C-FA performed considerably better than Passfaces in our study when it came to authentication success rates. We define *authentication success rate* as the percentage of participants who successfully authenticated within their five total attempts. With A3C-FA, the authentication success rate via a shoulder-surfing attack was ~30%, compared to over 88% for Passfaces. Table 3 shows the number of participants who successfully authenticated in each attempt. The number of times participants successfully authenticated for A3C-FA Undistorted was more or less steady across the five attempts. However, for A3C-FA Distorted, the participants were more likely to authenticate successfully as their number of attempts increased. These results show the potential benefit of distorting the face images because the greater the number of attempts an adversary needs, the more likely they are to be caught.

We next statistically compared the results of the three treatments. Since we are dealing with ordinal data, we performed Mann–Whitney U tests to compare the number of successful authentications for each of the three treatments. We assigned each participant who managed to successfully authenticate as the target-user a number based on the round in which they succeeded. If the participant did not successfully authenticate, they were represented as "6" (one more than the final attempt). We found that, as compared to Passfaces, the authentication success rates for both A3C-FA Undistorted ($p = 2.83 \times 10^{-20}$; $p < 0.01$) and A3C-FA Distorted ($p = 2.53 \times 10^{-25}$; $p < 0.01$) were statistically significant. This indicates that A3C-FA is significantly better at defending against shoulder-surfing attacks than Passfaces. It therefore shows promise as a secure alternative for people with UEI. In contrast, we found that the difference between authentication success rates for A3C-FA Distorted and A3C-FA Undistorted was not statistically significant ($p = 0.44$; $p < 0.01$). Therefore, while A3C-FA Distorted did perform better in our study, it was not a statistically significant difference over the security provided by the A3C-FA Undistorted.

To contextualize the results of the two versions of A3C-FA further, we next examined where, in terms of the two phases, the participants failed to authenticate successfully as the target-user. Table 4 shows the results of where the MTurk participants failed to authenticate in the two phases of A3C-FA's credential verification. The results are expressed as the number of attempts made over the course of the study by the participants. It can be seen that the participants made a large number of errors in recognizing at least one face image and the associated animal image.

6.6 Shoulder-Surfing Attack Study: Qualitative Evaluation

As part of the shoulder-surfing attack study, participants were asked to fill out a survey at the end of the study. The survey questions covered demographics, their thoughts on A3C-FA's two

Table 4. The Differences in Types of Errors Participants Made (Represented as Number of Attempts) for A3C-FA Distorted and A3C-FA Undistorted during the Shoulder-Surfing Attack Study

	Number of attempts		
	Face images	**Animal image**	**Face and animal images**
A3C-FA Undistorted	103	19	297
A3C-FA Distorted	113	18	323

phases, strategies they used to authenticate, and an honesty check. Below we present our findings based on an analysis of the survey results. Quotations from the survey are presented verbatim without editing. For each participant's quotation, we report the participant ID along with the attempt number where they succeeded at the shoulder-surfing attack. If the participant did not successfully authenticate as the target-user within the possible five attempts, we denote this as "failed."

6.6.1 Findings 1: Participants Tried to Just Memorize the Face and Animal Images. The most obvious strategy with shoulder surfing is to memorize the faces and the animals that go with it from the videos played. Some participants tried just that and were successful: "I simply tried to remember which photos were picked in regards to the human faces and the ones that lined up with their choices with the animal photos. No particular strategy." *(S-D42, 3rd)*. One participant stated that they devised descriptions for the face and animal images and repeated these in their mind to remember the combination: "Assigned verbal description of face and animal image to mentally repeat while [trying to authenticate]." *(S-D89, 2nd)*. That being said, as the overall quantitative results show, such attempts were generally not successful: "I remembered the faces tied to the animals. I also remember what kind of animals they chose in order to guess at an estimate of which one they would pick" *(S-D71, failed)*.

6.6.2 Findings 2: Participants Paid Attention to Specific Features of a Face or Used Various Mnemonic Devices to Remember the Face Images. One successful strategy used both for A3C-FA Distorted and A3C-FA Undistorted was to focus on memorizing particular facial features: "I tried to remember specific features of the person like hair color, gender, facial hair, wearing glasses or not." *(S-D106, 3rd)*. Similarly, participants also used facial expression to help remember the faces: "I REMEMBER THE FACE STRUCTURES AND FACE REACTIONS." *(S-UD99, 5th)*. Participants trying to authenticate with Passfaces used similar strategies: "Just in general what ethnicity, gender and skin color then just try to remember the order." *(S-PF18, 2nd)*. However, not all participants who memorized facial features were successful with A3C-FA: "I remembered characteristics [wore glasses, had a beard]" *(S-D60, failed)*.

Another common strategy for remembering the faces was to create a name or short phrase to help the participant remember the face image. Sometimes, these nicknames or titles were also based on the features of the person: "I said to myself 'asian guy' 'smiling indian woman' 'happy guy' etc" *(S-UD82, 5th)*. Some people used a combination of methods for coming up with the nicknames: "I just gave them names that had something to do with a facial feature or maybe they looked like someone famous." *(S-UD83, 5th)*. Participants trying to authenticate using Passfaces also used the same strategy: "I remembered their race and compared them to celebrities. Like one black guy made me think of Busta Rhymes and the other was Wayne Brady." *(S-PF103, 1st)*. In addition to giving faces nicknames, participants also related the faces to people they knew personally as a way to remember them: "I related them to people I know" *(S-D22, 2nd)*. Similar to the use of facial features,

the use of mnemonics did not always work either: "I tried to associate them with famous actors based on look to remember which face and then just kept it in my head along with the animal." *(S-D54, failed)*.

6.6.3 Findings 3: Despite Having Strategies, Participants Felt Frustrated by How Difficult It Was to Authenticate as the Target-User. Overall, participants felt that trying to authenticate as the target-user using A3C-FA was very difficult: "Seems impossible" *(S-D57, failed)*. One participant wrote about how frustrating they found acting as an adversary to be, stating: "There was no way to authenticate because it was set up for me to fail." *(S-D59, failed)*. It seems that one reason for the difficulty the participants experienced was that A3C-FA does not provide the user with information as to what aspects of their input were correct or incorrect: "I just watched and tried as best as I could to recall them. I'm very certain I remembered one exactly but it said login failed anyway…" *(S-D25, failed)*.

Additionally, the randomization of the which images were selected out of the provided set of face images meant that even when participants remembered information from the shoulder-surfing videos, it might not help them right away or at all: "I remembered the photos but the ones in the second part were never the same, there was no way to get the right answer." *(S-D59, failed)*. This randomization within A3C-FA also makes A3C-FA resilient to situations where participants take notes or screenshots to remember the face and animal images: "I cheated with a screenshot a couple times and saw that none of the images even were there to click on to match!" *(S-D63, failed)*. However, some participants who took notes or images of the screens did feel as though they gained an advantage: "I look very carefully to that image and also I take quick notes." *(S-UD20, 3rd)*.

7 STUDY 2: CLOSE-ADVERSARY ATTACK STUDY

The purpose of the close-adversary attack study was to determine the ability of A3C-FA to protect against close adversaries who have some knowledge of the user, such as knowledge of people they know and some animals the user likes [41].

7.1 The Close-Adversary Attack

Similar to the shoulder-surfing attack study, the close-adversary attack study was run online via MTurk [3]. We again use the term *participant* to refer to the person on MTurk acting as the adversary performing the close-adversary attack. We use the term *target-user* to refer to the fictitious user (created by the first author) whose credentials the adversary is trying to guess, based on their knowledge of the target-user. The *close-adversary attack* study was structured as a three-step process:

— *Participants are given information about people the target-user knows*: The first step in this process was to inform the MTurk-based participants about people the target-user knows. This was done by showing the participants a list of 12 face images of people the target-user knows. A3C-FA used five of these face images as the target-user's primary image set. Of course, the participant was not told which five would be selected. Showing the participant images of 12 people the target-user knows simulates the situation where a close adversary is aware of several acquaintances of the target-user, some of whose face images likely would be used by the target-user for A3C-FA. The participants were allowed to record the 12 images in anyway they wanted (e.g., taking notes, screenshots).
— *Receive information about animals the target-user likes*: Next, the participants received the names of 12 animals the target-user likes. The participants were allowed to record this information in anyway they wanted (e.g., taking notes, screenshots).

— *Attempt to authenticate as the target-user*: Subsequently, the participants were asked to use these two aforementioned pieces of information to impersonate the target-user and authenticate as the target-user.

For the participants to mount a close-adversary attack, we had to create a realistic target-user for A3C-FA to make it possible to provide information on their acquaintances and preferences to the participants. The information given to the participants was intended to help mimic the knowledge that a close adversary might have.

To provide realistic information to the participants about people the target-user knows, the first author set up A3C-FA using face images of five people they know and created an animal association for each of the five face images, using the dataset with 105 animal images used by ALPCA-FA [7]. To protect the privacy of these individuals on a public platform like MTurk, the first author swapped these five images with similar-looking face images from the WIDER FACE dataset [100].[3] In terms of the soundness of the methodology of this study, the replacement of the images did not have any impact on our results. The first author then found an additional seven face images of people they know and also swapped those images with similar-looking face images from the WIDER FACE dataset as well. These seven additional images did not have any animal images associated with them.

Further, we asked someone very close to the first author to provide the rest of the team a list of 12 animals the first author likes. This animal list was kept private from the first author so that they did not know which animals were on the list when they set up the A3C-FA credentials as the target-user. The animal list was uploaded into the MTurk platform by the second author.

7.2 The Close-Adversary Study: Treatments

We performed a *between-group* study for this project, where participants were placed in one of two treatment groups: (1) A3C-FA Undistorted and (2) A3C-FA Distorted. Passfaces was not included in this study since, given how it works, there is no meaningful information a close adversary would be able to leverage to improve their attack.

7.3 The Close-Adversary Attack Study: Procedure

There were four main parts of the study procedure: *the study introduction*, *a practice attack*, *learning information about the target-user*, *15 possible consecutive authentication attempts*, and then *a survey*. A summary of the procedure for this study can be seen in Figure 6.

For this *study introduction*, all participants were shown an online version of the consent form and were asked to agree to participate in the study. They were then asked to watch an approximately 5-minute video that explained (1) how A3C-FA worked, (2) how the participants were expected to act as a close adversary, and (3) how participants were expected to try to authenticate to A3C-FA, given the information about the target-user. The participants were once again told that if they succeeded before the 15th attempt, they would get to finish the study early without affecting their compensation. The participants were allowed to pause, rewind, or re-watch the introduction video as many times as they wanted.

After the video ended, the participants were given a chance to *practice* the close-adversary attack. They were shown a collection of face images that a sample user knows and a list of animals that the sample user likes. Participants were then given *one* opportunity to practice authenticating to A3C-FA using the face images and animal list for the example target-user.

[3]The replacement images were chosen by the researcher to have similar features to the people the researcher knows (e.g., similar age, same facial hair, glasses or no glasses).

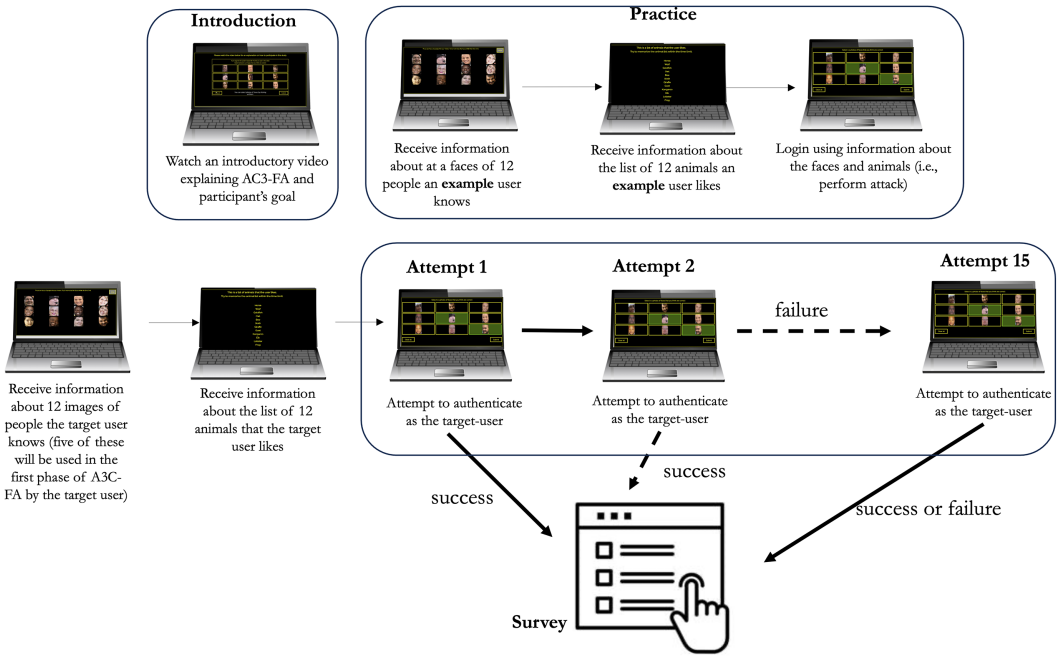


Fig. 6. This diagram summarizes the procedure for the close-adversary attack study.

Next, participants were given information about the target-user. This included 12 images of people the target-user knows and the 12 names of animals the target-user likes. Participants were given 1 minute to memorize/record each of these pieces of information.

After viewing the information, participants were given *15 possible consecutive authentication attempts*. After each authentication attempt, they were informed whether or not they were successful. They were never given any information about whether the individual face/animal images they selected were correct or incorrect.

If they succeeded in authenticating as the target-user before finishing all 15 attempts, participants were allowed to proceed to the *survey* at the end of the study. If not, they had to complete all 15 attempts before proceeding to the survey. The survey asked questions about demographics, any notes they took during the process, and any strategies they used to try to authenticate. A *self-reported honesty check* (similar to the shoulder-surfing attack's honesty check) was included, as it has been shown to be successful in preserving data quality in previous studies [30, 73].

7.4 The Close-Adversary Study: Participants

For this study, participants were chosen from the United States or Canada, via MTurk, and had to be 18 years of age or older. Participants were compensated $4 for their time, as in the previous study. After removing all the participants who failed the self-reported honesty check, we had a total of 268 participants. Out of these 268 participants, 131 participants viewed A3C-FA Undistorted and 137 participants viewed A3C-FA Distorted. We labeled the participants in each treatment group as follows: (1) A3C-FA Undistorted: *K-UD1 through K-UD131* and (2) A3C-FA Distorted: *K-D1 through K-D137*. Participant demographics can be seen in Table 5.

Table 5. Demographics for the Participants in the Close-Adversary Attack Study

	Gender		Age					
	M	F	18–24	25–34	35–44	45–54	55–64	65–74
A3C-FA Undistorted	116	21	5	96	18	10	4	4
A3C-FA Distorted	101	30	1	86	26	9	7	2
Total	217	51	6	182	44	19	11	6

Table 6. Results of the Observations and Attempts for Each Round of the Close-Adversary Attack Study

	A3C-FA Undistorted	A3C-FA Distorted
Successful attacks on Attempt 1	4	3
Successful attacks on Attempt 2	3	3
Successful attacks on Attempt 3	1	2
Successful attacks on Attempt 4	2	0
Successful attacks on Attempt 5	1	2
Successful attacks on Attempt 6	1	1
Successful attacks on Attempt 7	2	1
Successful attacks on Attempt 8	2	4
Successful attacks on Attempt 9	0	0
Successful attacks on Attempt 10	1	0
Successful attacks on Attempt 11	1	3
Successful attacks on Attempt 12	2	2
Successful attacks on Attempt 13	2	2
Successful attacks on Attempt 14	1	1
Successful attacks on Attempt 15	1	1
Total successful participants	24 (18.3%)	25 (18.2%)
Total failed participants	107 (81.7%)	112 (81.8%)
Total participants	131	137

7.5 The Close-Adversary Study: Quantitative Evaluation

For the close-adversary attack, we compared the performance of the participants in both A3C-FA Undistorted and A3C-FA Distorted. Our study found that, for both treatments, the participants performed very similar to one another with respect to authentication success rates. Again, we define authentication success rates as the percentage of participants who successfully authenticated within their 15 allotted attempts. For both treatments, around 81% of the participants failed to successfully authenticate into A3C-FA. Table 6 shows the full list of the number of successful authentications by the participants in each of their 15 attempts. The success rates for the close-adversary attack study were lower than that of the shoulder-surfing attack study, even over a greater number of attempts. These results demonstrate high resiliency for A3C-FA.

As with the shoulder-surfing attack study, we ran a Mann–Whitney U test between the two treatments. The difference between A3C-FA Undistorted and A3C-FA Distorted was not statistically significant ($p = 0.95$; $p < 0.01$). This is in line with the shoulder-surfing study results, which also found no statistically significant difference between the two treatments.

Finally, as in the case of the shoulder-surfing attack study, we looked at where, in terms of A3C-FA's two-phase credential verification, the participants failed to authenticate successfully as

Table 7. The Differences in Types of Errors Made by Participants (Represented as Number of Attempts) for Each Version of A3C-FA during the Close-Adversary Attack Study

	Number of attempts		
	Face images	**Animal image**	**Face and animal images**
A3C-FA Undistorted	38	226	1,357
A3C-FA Distorted	54	175	1,478

the target-user. Table 7 shows these results. The results are expressed as the number of attempts made by the participants over the course of the study. It can be seen that the participants made a large number of errors in identifying both (at least one) face image and the animal image. The lowest number of errors were in the face image only column, this to be expected because the study shows the five face images (along with seven others) used as credentials by the target-user.

7.6 The Close-Adversary Study: Qualitative Evaluation

As in the shoulder-surfing attack case, participants in the close-adversary attack study were asked to complete a survey at the end of the study. The survey questions covered topics relating to demographics, opinion about A3C-FA, strategies they used to authenticate, any notes that the participants took, and an honesty check. The first author then analyzed the survey results, the findings of which are summarized below. As with the shoulder-surfing attack section, we report participants' quotations with the attempt number (out of 15) where individual participants successfully authenticated. If individual participants did not successfully authenticate within the 15 attempts, we ascribed the label "failed."

7.6.1 Despite Having Been Provided All of the Face Images Used for the Study, Participants Nonetheless Were Unable to Identify the Correct Face Images. One reason for this is that participants seemed to have difficulty in successfully memorizing the face images, "I looked at each face individually and formed an impression of each person so I could recall them more easily. I did that a few times to help memorize them." *(K-UD12, failed)*. This difficulty is interesting, given that participants were allowed to take notes during the study when they were given information about the target-user. Interestingly many participants only took notes about the animal images and not the faces, "I just wrote down the names of the animals." *(K-D18, failed)*. Other participants did try to take notes or screenshots to remember the faces. However even in these cases, the participants were often unsuccessful, due to the inherent randomness built into A3C-FA's design: "I tried to take notes describing faces and which animals they didn't match up with." *(K-D33, failed)*.

7.6.2 Participants Used Similar Strategies to Those Used by Participants during the Shoulder-Surfing Study, without Much Success. As with the shoulder-surfing attack study, some participants used the features of the face images to remember them: "[I focused on] [r]ace, gender, glasses, facial expression." *(K-D18, failed)*. Other participants used the strategy of nicknaming the face images to remember them, which, as in the shoulder-surfing study, was sometimes successful: "I came up with nicknames for the faces. For instance the blond guy with the square jaw I nicknamed him Chad after the popular meme. Another person presented looked like the actor Alexander Siddig so I called him Dr. Bashir (character from a Star Trek series)." *(K-UD58, 15th)*. However at other times, nicknames did not help the participant authenticate: "I tried to give each face a 'nickname' and match the name to a face." *(K-UD8, failed)*. Another strategy that was successful for remembering

the faces was to relate the face images to people that the participant knew in real life: "I pick the images based on my friends faces." *(K-D6, 6th)*. However, this strategy did not work for everyone: "I tried to match faces with real people I know that looked similar." *(K-D33, failed)*.

7.6.3 Knowing Which Animals the Target-User Likes Did Not Help Participants Guess the Animal Image Association. The animal preference information provided to participants did not seem to help participants guess the correct animal image association: "I tried to guess from the animal list … but I wasn't very successful." *(K-D18, failed)*. Since the participants had 15 attempts to authenticate, they often kept track of what they had already selected to try to narrow down the possible options: "I took notes…. During the log in attempts I just remembered which animals didn't work." *(K-UD16, 8th)*. Most of the time, however, eliminating animals that had already been guessed was not sufficient to allow a person to authenticate within the 15 possible attempts: "The only other strategy that I used was to keep track of the animals that I previously guessed for a particular photo. I tried to make sure not to repeat any of the same guesses." *(K-UD58, failed)*.

7.6.4 Participants Sometimes Used Their Own Associations between the Face and Animal Images, Again without Much Success. One participant reported that they tried to pretend they knew the people whose faces were used as credentials: "I tried to pretend like i've met these people before and I tried to memorize their character." *(K-UD61, failed)*. One participant tried to guess the animal image based on what could be potential pets: "I have mostly concentrated on the pet animals. What would people consider a pet?" *(K-D5, 1st)*. However, participants using strategies like these were often unsuccessful, as they only had superficial characteristics of the target-user to work with: "COMPARE THE ANIMALS AND FACE PHOTOS." *(K-D39, failed)*.

8 STUDY 3: ACCESSIBILITY STUDY

Given that A3C-FA was found to be secure against both shoulder-surfing and close-adversary attacks, we next evaluated its accessibility in terms of how easy it was for people with UEI to use and how easy it was for them to remember the primary and secondary images over time (a period of 1 month). Contrary to the previous studies, in this study, the term participant signifies the *legitimate user* of A3C-FA and not an adversary.

8.1 Accessibility Study: Treatment and Participants

For the accessibility study, we performed a between-group study where each participant was placed into one of two treatment groups: (1) A3C-FA Undistorted and (2) A3C-FA Distorted.

Participants were required to be 18 or older, have some form of UEI, and have a computing device with internet access that they could use for the study. Each participant took part in three study sessions that occurred over the course of a month. There were 14 participants with UEI who participated in all three sessions of the accessibility study. Participants were recruited through a combination of approaches, including: e-mailing participants from prior studies, recruiting via a local non-profit who provides technology access to people with disabilities, and recruiting via social media advertising on Facebook [31] and Twitter [86]. Participants were compensated with a $30 Amazon gift card for their participation. Participants were split evenly between the two treatment groups. We labeled the participants in each treatment group as follows: (1) A3C-FA Undistorted: *P-UD1 through P-UD7* and (2) A3C-FA Distorted: *P-D1 through P-D7*. Additionally, in the accessibility study, we asked participants to authenticate multiple times. Each time participants tried to authenticate, they had three possible attempts to authenticate successfully. Demographic information for the participants in the study can be seen in Table 8. All study sessions were conducted by the first author.

Table 8. Demographics of the Participants in the Accessibility Study

ID	Treatment group	Age	Gender	Disability
P-UD1	Undistorted	76	Female	Spinal cord injury with severe cervical stenosis and myelopathy
P-UD2	Undistorted	61	Male	Primary progressive multiple sclerosis
P-UD3	Undistorted	62	Male	C-5 spinal cord injury
P-UD4	Undistorted	50	Male	Amyotrophic lateral sclerosis
P-UD5	Undistorted	27	Female	Duprene's contracture in right hand
P-UD6	Undistorted	20	Male	Abnormal muscle tone primarily impacting ability to move and use left arm
P-UD7	Undistorted	31	Male	Hand-arm vibration syndrome
P-D1	Distorted	26	Male	Hand-arm vibration syndrome
P-D2	Distorted	29	Male	Spinal cord injury at the C-5/C-6 level
P-D3	Distorted	22	Male	Hand-arm vibration syndrome
P-D4	Distorted	32	Nonbinary	Injury across both hands causing lack of grip strength, swelling, pain, and difficulty performing fine motor tasks
P-D5	Distorted	26	Male	Complications post-injury causing stiffness and difficulty moving left hand
P-D6	Distorted	28	Male	Hand-arm vibration syndrome, also dislocation of left arm
P-D7	Distorted	30	Male	Injury causing limited ROM and "heavy" feeling in left arm

8.2 Accessibility Study: Procedure

Participants were invited to take part in a three-part study over Zoom [105]. Each study session included a semi-structured interview at the end. Interviews were audio-recorded with permission from the participants. One participant (P-UD4) communicates via text. Therefore, P-UD4's responses were copy-pasted into the transcription document from Zoom's chat feature, where the participant typed them. Below, we explain in detail each stage of the study. Figure 7 shows a summary of the procedure used for the accessibility study.

8.2.1 Prior to the Study. To protect the privacy of participants (i.e., not requiring them to share their personal images), we asked the participants to give us the names of celebrities (for the primary images in A3C-FA). Note that the use of celebrity images in lieu of personal images can alter the process of authentication for A3C from recognition of a known face to recall of a prior choice. Overall, though, we believe that such a change ultimately means that the results we obtained in this study are stronger if A3C-FA were deployed as intended with face images provided by the user that would be, consequently, recognizable.

Prior to the first study session, the participants were asked over e-mail to provide a list of six celebrities that they thought were the most recognizable to them. Participants were told that the celebrities could be any sort of public figure for whom color photographs could be found online. The first author then used the list of celebrities to find three images of each celebrity and prepared them for the first study session by cropping the images to just the faces.

8.2.2 The First Study Session. During the first session, the first author gave an *introduction* to A3C-FA to the participants using the screen-share capability on Zoom. The participants were

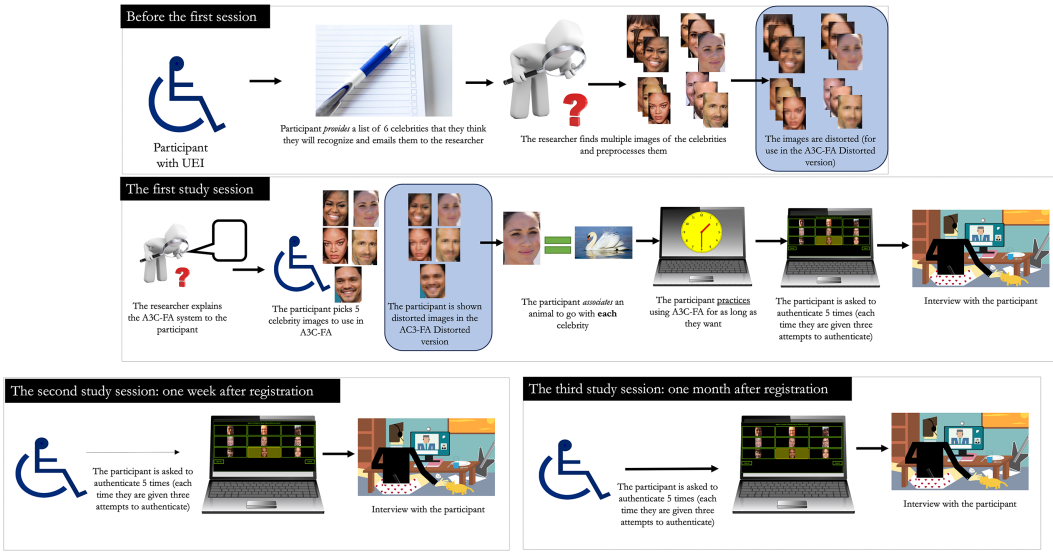


Fig. 7. This diagram summarizes the procedure for the accessibility study.

invited to ask any questions they had about the system at any time. After the introduction, the participants were shown the 18 face images of celebrities (i.e., 3 images for each of the 6 celebrities) the participants had named. They then were asked to *select 5 images of 5 different celebrities* that were the most recognizable out of the available 18 face images. If the participants were in the A3C-FA Distorted treatment group, they were shown the distorted images of the faces of the celebrities and their undistorted versions side-by-side to help them better select the face images that would be most recognizable for them. The participants were then shown a set of 105 distinct animal images from the animal dataset [7]. For each celebrity image, the participants were asked to associate an animal image with it. Participants were then given a break. During the break, the first author entered participants' provided authentication credentials (the celebrity face images and animal images associations) into A3C-FA.

After the participants were registered into A3C-FA, they were asked to *practice* authenticating. No data were collected during the practice session. Participants were not given any time constraints for practicing. However, they were asked to ensure that they were able to authenticate successfully at least a few times. Participants were again encouraged to ask any questions they had.

After the participants felt that they were done practicing, they were asked to *authenticate into A3C-FA a total of five times*. If they made a mistake in entering their credentials, they were given two additional attempts to authenticate. Therefore, participants had a total of a possible 15 attempts. Ideally, participants would only need five attempts—one for each time they were asked to authenticate.

After authenticating five times, the participants were asked to take part in an approximately 30-minute semi-structured interview. During the interview, they were asked about their opinions of A3C-FA, any barriers they encountered, and any design changes they would like to see made to A3C-FA.

8.2.3 The Second Study Session. The purpose of the second study session was to help determine how easy it would be for users to remember their A3C-FA credentials over time. The second session of the study was scheduled approximately 1 week after the first session. For the second session,

Table 9. The Number of Attempts Participants Needed to Authenticate Successfully in Each Session (Minimum 5 and Maximum 15 Per Session)

	Attempts needed for success														
	Session 1					Session 2					Session 3				
P-UD1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1
P-UD2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
P-UD3	1	1	1	1	1	1	2	1	2	1	1	2	2	1	1
P-UD4	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
P-UD5	3+	1	3	2	1	1	3	3+	1	3+	3+	3+	1	2	1
P-UD6	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2
P-UD7	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
P-D1	1	1	1	1	1	1	1	2	2	1	1	1	1	1	1
P-D2	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1
P-D3*	1	1	1	1	3+	3+	1	1	1	3+	1	1	1	1	1
P-D4	1	1	1	1	1	1	1	1	1	1	1	1	2	1	2
P-D5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
P-D6	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
P-D7	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

If a participant was unable to authenticate, the number of attempts is indicated as "3+." A value of 3+ is thus considered failure to authenticate and is therefore highlighted in red.
*P-D3 misunderstood the instructions given by the researcher and practiced logging in several times before recording the login attempts for session 2. This may have impacted his results for session 2 and session 3.

the participants were again asked to authenticate five times, as in the first session. They were then asked to participate in an approximately 15-minute semi-structured interview about their experiences in authenticating with A3C-FA and how well they remembered their credentials.

8.2.4 The Third Study Session. The third session was scheduled about a month after the first session. The third session's procedure was identical to that of the second session. Participants were then provided with compensation at the conclusion of the third interview.

8.3 Accessibility Study: Quantitative Findings

Table 9 shows the full enumeration of all the successes and failures in authenticating for all participants across all three study sessions. Most participants consistently were able to successfully authenticate in the first attempt for each of the five times they authenticated in each of the three sessions. Notably in the third session, which took place a month after the first session, all but one participant successfully authenticated all five times.

We again performed a Mann–Whitney U test to compare the authentication success rates of the A3C-FA Distorted and A3C-FA Undistorted treatments. We found that there was no statistically significant difference between the two success rates ($p = 0.12$; $p < 0.01$). We then performed a Mann–Whitney U test to compare A3C-FA Distorted with A3C-FA Undistorted in terms of the number of successful authentications achieved by participants each of the five times they authenticated during each of the three sessions. We again found there was no statistically significant difference between the two treatments ($p = 0.64$; $p < 0.01$).

Interestingly, the number of participants who successfully authenticated each of the five times they authenticated during each of the three sessions did not show degradation over time. In fact, the successful authentication rates actually increased in session three, as compared to the prior two sessions. We performed a Kruskal–Wallis test comparing the number of attempts needed

Table 10. A Summary of the Qualitative Analysis of the Accessibility Study of A3C-FA

The participants found A3C-FA easy to use	The participants found A3C-FA's credentials easy to remember
	The participants used five strategies for associating animal images with face images in AC3-FA
	The participants' opinions of A3C-FA became even more favorable over time
	The participants suggested that A3C-FA should be offered as an authentication method for diverse, non-UEI populations
The participants found A3C-FA to be more accessible than the authentication solutions familiar to them	The participants felt that A3C-FA has accessibility advantages over passwords, PINs, biometrics, and other graphical authentication methods
	The participants found that A3C-FA could support a variety of input methods and AT
	Some participants pointed out ways that A3C-FA could be physically difficult to use for users with certain conditions
The participants generally felt that A3C-FA was secure	In comparison with other available authentication options, participants found A3C-FA to be secure
	The participants felt secure using A3C-FA, due to its two-phase design and its inherent randomness

each of the five times they authenticated during each of the three sessions. There was no statistically significant difference between the number of attempts needed for any of the sessions ($p = 0.25$; $p < 0.01$). We then compared the difference between the number of authentication successes across all three sessions using a Kruskal–Wallis test. The difference was again not statistically significant ($p = 0.82$; $p < 0.01$). These results show that most participants were successful in remembering A3C-FA's credentials over time. This aligns with many participants' perception that A3C-FA's credentials are easy to remember, which will be discussed in more detail in the next section.

9 ACCESSIBILITY STUDY: QUALITATIVE FINDINGS

We ended each of the three sessions of the accessibility study with a semi-structured interview with the participants. The interview after the first session asked the participants about their computing device use, their impression of A3C-FA, potential things to improve in A3C-FA, and their demographics. The interviews after the second and third sessions featured questions related to their impression of A3C-FA with respect to using it a second and third time, respectively; remembering their credentials over time; and potential things to improve in A3C-FA. We then transcribed the interviews from the 3 sessions for all 14 participants and performed a reflective thematic analysis of the study transcripts. We used a recursive approach to thematic analysis for our work, as described in [17]. The coding and theme development were conducted inductively and evolved throughout the analytic process. The results of our analysis are described below and also summarized in Table 10.

9.1 Findings 1: Participants Found A3C-FA to Be Easy to Use

The participants felt that A3C-FA was very usable for them, given their UEI. Below we discuss four themes that emerged in this regard.

9.1.1 Theme 1: Participants Found That A3C-FA's Use of Visual Associations Made the Credentials Easy to Remember. Our participants found it easy to remember the A3C-FA credentials they created:

"You could probably ask me this five years from now, call me up in five years, let me do it again … I'd remember it." *(P-UD2, session 3)*. One known advantage of graphical authentication is that its credentials are generally easy to remember [80]. Some of our participants similarly linked their facility in recalling their credentials to the fact that A3C-FA is graphic-based: "I use visual cues to remember passphrases anyway. So when I associated a particular visual map in my head for a particular system password, I only have to walk through the well known visual recollection in my head. So picturing walking through your house and at each room or prominent artifact in the room, you associate a visual representation of what you needed to remember. This system cuts out the need to translate that visual back to a word." *(P-UD4, session 3)*.

According to some participants, the fact that A3C-FA is based on an association between two images made it easy for them to remember both images: "What makes me … remember the people in particular, it's the type of animal I choose for them." *(P-UD6, session 2)*. The same participant also reported how seeing the face images made it easier to remember the associated animal image: "You know, when you're concentrating on the pictures of the person, it tends to reflect the kind of animal you choose." *(P-UD6, session 3)*.

The ease of remembering A3C-FA credentials not only ensured that participants were able to use the system but also made it fun for participants to use: "When I was doing it today it was a bit kind of like fun to me also because, just, I was so amazed how I was able to remember the animals to each person I chose" *(P-D5, session 2)*. One participant even commented that they felt like A3C-FA helped them gain cognitive skills: "I've actually developed my memory and my reasoning ability." *(P-UD5, session 3)*.

9.1.2 Theme 2: The Participants Used a Variety of Strategies for Associating Animal Images with Face Images. One of the factors that makes A3C-FA secure is the undocumented connection that the user makes between the primary face image and the secondary animal image. Further, A3C-FA does not prescribe any specific way to associate the face and animal images. Consequently, we found that participants used a variety of methods to associate the animal images with the face (in this case, celebrity) images. In our study, we determined that there were six core ways our participants reported that they used to associate the animal images with the face images:

(1) Name-based association: In this type of association, the participant used the name of the person and the name of the animal to associate them: "Snoop Dogg, you know, first thing that comes to my mind is a dog." *(P-UD7, session 1)*.
(2) Memory-based association: Another type of association was based on a memory the participant had about the person in the primary image: "Leno, I knew—I used to watch his show all the time and—how fond he was of cats, including wild cats. I mean, he would just play with a lion like he was the, you know, house tabby." *(P-UD1, session 1)*.
(3) Characteristic-based association: In this type of association, the participant formed an association by starting with a characteristic of a given person, then selecting an animal that, to them, exhibits the same trait. These characteristics ranged from *physical*: "For [Christoph] Schneider [member of the band Rammstein], I had picked the fox, mainly because … Rammstein as a band are in, like, their 60s. Schneider is starting to go gray so I was just like, oh, silver fox, red fox, that's close enough" *(P-D4, session 1);* to *ability-based*: "Carlos Santana is a very fast guitarist, so I chose the cheetah." *(P-UD3, session 1);* and *perceived-personality-trait based*: "David Ortiz was the lion and he was that type of character here. You know, ferocious?" *(P-UD2, session 1);*
(4) Rank-based association: Here, the participant used some method for ranking the animals and faces, then used that ranking to link them: "I tried matching them to the celebrities I like the most and then the … animals that I'm also more familiar with. I was matching them

on that, so that was more easy for me to remember.... The strategy was based on the person I like most and then also the photo I like most, matching them together." *(P-D5, session 1)*.

(5) Personal or imaginative association: Finally, this type of association was based on a general impression or feeling: "So, I watch movies. Today I will see Will Smith as a policeman or I'll see him as ... so many different characters. So I just had to give him a butterfly because, you know, a butterfly has so many colors and they're so beautiful." *(P-D7, session 2)*.

9.1.3 Theme 3: After Using A3C-FA Over the Course of a Month, Participants' Opinions of the System Became Even More Favorable. For some participants, using A3C-FA over the course of the study increased their comfort with it: "Pretty novel approach; it grew on me" *(P-UD4, session 3)*. Similarly, during the first session, another participant felt they might prefer to stick to passwords and PINs over A3C-FA: "I think [A3C-FA is] really good. So for someone like me that, you know, can use their fingers enough to, you know, type out stuff. I don't know if I would change from what I'm doing now to [A3C-FA]." *(P-D2, session 1)*. However, by the end of session three, they had changed their mind: "Well, I mean, just through the kind of trials I've done with you, I know it works. I know that it's something I can do and I do think it's a pretty, just pretty good system overall.... Definitely, it's something that I could use, would use ... Definitely a fan." *(P-D2, session 3)*. Other participants had a positive opinion of A3C-FA from the beginning, which strengthened over time: "I'd say [A3C-FA] was reinforced as a great idea." *(P-UD4, session 3)*. None of the participants stated that their opinion of A3C-FA had worsened over the three sessions.

9.1.4 Theme 4: Participants Suggested That A3C-FA Should Be Offered as an Authentication Method for Diverse, Non-UEI Populations. Participants also felt that A3C-FA would work for more than just adults with UEI. A couple of participants thought that A3C-FA would work well for children: "Would be great for kids.... They can't remember passwords worth a crap." *(P-UD4, session 1)*. Another participant also felt that A3C-FA would work well for children and that it would work even better for this population if cartoon images were used: "Bringing in some cartoon features and characters like Scooby Doo, Simpsons, Powerpuff Girls, and all that, at least for children who have, you know, study tablets." *(P-D6, session 2)*. Additionally, some participants felt that, since A3C-FA's credentials were so easy to remember, it would be particularly useful for people who have memory or cognitive impairments: "I think the familiarity factor could go a long way for someone who's got cognitive or memory issues. I think faces and images seem to me ... I guess the word would be more recognizable." *(P-UD3, session 3)*.

9.2 Findings 2: The Participants Found A3C-FA to Be More Accessible Than the Types of Authentication Solutions Familiar to Them

The participants felt that A3C-FA was a usable alternative for computing device authentication. Below we discuss three themes that emerged in this regard.

9.2.1 Theme 1: The Participants Felt That A3C-FA Has Accessibility Advantages Over Passwords, PINs, Biometrics, and Other Forms of Graphical Authentication. Overall the participants had positive opinions of how easy A3C-FA is to use.

The participants found A3C-FA easier to use than passwords and PINs. Passwords are known to have accessibility barriers for people with UEI [54]. Our participants commented on having encountered similar barriers and frustrations using passwords: "When I mess up my password, I do begin to start the process of getting frustrated, which makes me more likely to miss-key my password and lock myself out of the system." *(P-D4, session 1)*. In contrast to the difficulties encountered when typing passwords, many participants found clicking on the images in A3C-FA much easier: "Typing words is difficult. Selecting images is easy." *(P-UD4, session 3)*.

Participants gave a number of different reasons to explain why A3C-FA makes authentication easier than passwords or PINs. One reason was because it completely avoids the need to use a keyboard: "If … I wasn't able to reach the keyboard to enter my PIN, I could still log in [with A3C-FA]." *(P-UD2, session 1)*. Similarly, another participant reported that entering passwords causes them a lot of physical strain that was not present when using A3C-FA: "[A3C-FA involves] less physical exertion but [is] equally secure … When I'm at the iMac, I have to use my hand and type in a password where on the picture ones, I just click the appropriate face and animal." *(P-UD3, session 1)*. Additionally, the use of a few large images means that A3C-FA has a large image selection area, which made it easier for participants with UEI to use the system: "I feel it's more easier compared to the PIN. Just a click, click, unlike … the PIN, you have to press and, you know, the keyboard is actually kind of small on a tablet or phone. So you can simply just press other stuff and your PIN gets incorrect and you'll be like, 'I know my number!' Meanwhile, you didn't know you actually pressed the wrong PIN." *(P-D1, session 1)*.

The participants found biometric authentication methods to be inconsistent in contrast to A3C-FA. Participants who had used biometrics commented that they felt that A3C-FA was more reliable than biometric authentication methods: "The camera of your face is not that perfect and it does not recognize the log on and then you can easily [use A3C-FA]. It's very easy to use. Anyone can use it, so I think that's why I think it's perfect." *(P-D7, session 1)*. Biometrics were often difficult to use in certain scenarios, such as low-light or high-noise environments: "So [A3C-FA] is actually better than [Face ID and voice recognition]. Especially because with the voice recognition, I have to, you know, be in a silent place or probably speak loud. And for the Face ID, to be in a place [that is] well-illuminated by light…. Unlike this one, you know, you just pick, pick, pick and you're done." *(P-UD7, session 1)*. Similarly, another user commented on how A3C-FA is also better than using fingerprint sensors on computing devices: "Depending on certain conditions, maybe your hand is wet, your fingerprint may not easily be recognized by a device and so it takes time. You have to do a lot of cleaning of your fingers and it can be really, really annoying…. I think I like [A3C-FA]" *(P-D6, session 1)*.

The participants stated that A3C-FA is more usable than other graphical authentication methods. A few participants had used graphical authentication methods in the past but these methods did not work well for them, due to their UEI. For instance, a participant stated that they had used an authentication system similar to PassPoints [97] but often had difficulty using it because of their hand tremors: "I've used [graphical authentication] on my Windows laptop before. You know, it's gonna tell you to pick on a particular place on the picture, you're going to click on those … three spots … but it's kind of stressful because there's … a kind of specific place. You know, sometimes you can make a mistake as a result of your hand shaking., so that's why I really don't like it." *(P-UD-7, session 1)*. The same participant commented that A3C-FA felt like an "upgrade," as it was "easier" than the graphical authentication systems they had used in the past. Similarly, another participant, who used a pattern-based graphical authentication method on their Android phone [91], commented that they thought tapping on the pictures in A3C-FA would generally be easier than swiping: "[I've been] using the swipe function on my phone lately because of my hands…. Tapping on pictures would be a lot easier on my hands than even using the swipe method because then it's just a single tap and not a repetitive motion that I have to do with my hands." *(P-D4, session 1)*.

9.2.2 Theme 2: The Participants Found That A3C-FA Is Able to Support a Variety of Input Methods, Including the AT That People with UEI Typically Use. Many people with UEI rely on AT to authenticate to their computing devices [54]. However, many authentication systems do not work with the types of AT that people with UEI use. For example, a participant stated that many current authentication

methods do not work with the voice-input device on which they rely for computing: "Until I'm logged in, I don't have any access to my Dragon and Dragon is what I use for most of my computing." *(P-UD1, session 1)*. In contrast, participants stated that A3C-FA worked well with speech recognition and that it was easy to for them to select the images: "[A3C-FA] worked really well with the speech recognition, so that combination really did work for me." *(P-UD1, session 2)*. Additionally, A3C-FA also worked well with other forms of AT the participants used, such as a mouth stick: "Hitting the buttons was just as easy with the mouth stick as opposed to the mouse and trackball with cursor." *(P-UD3, session 2)*.

9.2.3 Theme 3: Some Participants Pointed Out Ways in Which A3C-FA Could Be Physically Difficult to Use for Users with Certain Conditions. Despite the A3C-FA's advantages, not all participants found it easy to use: "Depending and due to my present condition of my hand issue … and the issue is I kind of fidget, it kind of shakes. Having to click what is actually in my mind to click is actually challenging and difficult." *(P-UD5, session 2)*. Similarly, even though some participants found A3C-FA to be more convenient than biometrics, others still preferred the biometric authentication they already used: "Voice recognition might be easier because you don't even need to move your body. You just kind of say something and that gets done." *(P-D3, session 1)*.

9.3 Findings 3: Participants Generally Felt That A3C-FA Was Secure

Participants in our study reported that they felt secure using A3C-FA. Below we present two themes that emerged with regard to the security of A3C-FA.

9.3.1 Theme 1: In Comparison with Other Available Authentication Options, Participants Found A3C-FA to Be Secure. Participants felt secure using A3C-FA because it was picture-based. Some participants felt that the use of pictures increased the security over text-based options: "You can use any picture … It's [private] and it's personal." *(P-UD5, session 1)*. Additionally, a participant commented that A3C-FA seemed to be more secure than passwords, as they thought it would be more robust against key-logging programs: "I know that there are like, programs out there that … keep track of your, like, your keystrokes and stuff. And it's not, that's not necessarily something that I would have to be concerned about with using the pictures." *(P-D4, session 1)*. That being said, the same participant guessed that A3C-FA may be vulnerable to attacks if a combination of technologies were used: "screen grab and key-logger [could] still [potentially] defeat it." *(P-UD4, session 1)*.

Further, participants often felt that A3C-FA felt more secure than biometric authentication methods: "Voice recognition is not always so secure because … a lot of times … people have similar voices, things like that. So if voice recognition is 60% secure, I would say picture-based systems are about 80% secure. I think it's more secure since you have to match each picture with the celebrity; that's quite hard." *(P-D3, session 1)*. A similar comment was made about how A3C-FA seemed more secure than fingerprint recognition: "[A3C-FA] feels secure because … it would be very hard for someone to guess. Maybe if I know that … maybe he just likes a pet, like a dog, I can choose a kind of different animal that doesn't relate to any one that he likes. That will be so hard for someone trying to intrude my device, to be able to guess easily. Unlike using the fingerprint or face-based [where] someone can easily pick up the device and then pull your hand and then unlock it … using the picture-based, [hacking in] would be kind of difficult." *(P-D5, session 1)*.

9.3.2 Theme 2: Participants Felt Secure Using A3C-FA, Due to Its Two-Phase Design and Its Inherent Randomness. Participants often felt that A3C-FA's security was enhanced by the fact that, even if an attacker were able to guess the face image, they would not be able to guess the animal image: "Even if you get to know the person I love … you will not know the animal that I've attached to my

[person] and, so, it will get you confused. So I think [A3C-FA] is quite secure." *(P-D6, session 1)*. Another participant commented on how A3C-FA's two-phase process increases the effort required for an attacker to succeed: "I think I'll feel confident knowing that it's a secure system for me to use. You know, it's not like your passwords where it's just numbers or it's not like your fingerprints. This has to do with, like, a calculation, trying to connect the dots, stuff like that." *(P-UD6, session 3)*. In a similar vein, the randomness in the number of face images that need to be identified in A3C-FA also made participants feel that it was quite secure: "I like how you don't always just, like, pick one and one how sometimes it's, you know, pick two and it will show you only one of them. It just feels like another layer of security." *(P-D2, session 1)*.

10 DISCUSSION

The results from the A3C-FA studies show that the larger A3C framework provides a promising alternative approach for authentication for people with UEI. Further research is still essential to explore how the A3C framework can become made more accessible and secure over time. Based on the results from our studies of A3C-FA, we propose a list of three areas for future research to improve the larger A3C authentication framework.

10.1 Exploring A3C as a Backup Authentication Method

A3C has shown promise as a secure and usable option for people with UEI to authenticate to their computing devices. However, breaking into the hegemony of current authentication systems based on biometrics and passwords would not be easy. Therefore, one of the possible deployment venues for A3C could be as a backup authentication system. Currently, passwords/PINs dominate backup authentication for computing devices. Of course, the use of passwords/PINs is known to be difficult for people with UEI [54]. The inherent relative ease of remembering the credentials provided by recognition-based approaches like A3C would provide an effective alternative to the use of passwords/PINs as a backup measure. Some research questions in this regard include (1) Would people with UEI want to use an A3C-like system as a backup authentication method and, if so, in what contexts? (2) What accessibility barriers, if any, would arise when using A3C as a backup authentication system?

10.2 Determining Credential Security Guidelines for A3C

One important factor in knowledge-based authentication is to help users not select credentials that are too easy for an adversary to guess. Prior work has been conducted on guidelines to help users create secure graphical passwords [64, 68, 88]. Given that A3C is a novel form of graphical authentication, work should be done to explore guidelines for creating secure credentials specifically for the A3C framework. Once the guidelines are in place, for every instantiation of A3C, we need to then find a way to implement the guidelines. Some research questions in this area include (1) What aspects of A3C's credentials have the possibility of making them predictable to adversaries? (2) For a given instantiation of A3C, how can we find ways to detect predictable credentials and warn users?

10.3 Designing A3C for People with Other Disabilities

Another area of future research for A3C would be to determine how to increase its accessibility to other populations. One community of people that could benefit from A3C are those with **intellectual and developmental disabilities (I/DD)**. From our prior work we know that people with I/DD often have difficulty using extant authentication solutions and have to share their credentials with others as backup [90]. We believe that, given the accessibility advantages of A3C, it could be easily adapted for the authentication needs of people with I/DD to use independently.

Additionally, since the current A3C implementation is graphical, one pitfall is the lack of accessibility for blind or low-vision users. However, A3C's underlying concept for credentials need not be inherently visual. One possible variation of A3C could be to have people identify the voices of people they know well (whether that be people they know personally or celebrities) and associate them with other sound effects. Some research questions in this area include (1) Which communities of people with disabilities could benefit from A3C and how should A3C's design be altered to be accessible for that specific community? (2) Can A3C be used as an alternative to traditional authentication for individuals with I/DD? (3) What other types of associations (e.g., sound associations) can be used to help make A3C accessible to people with visual disabilities?

11 LIMITATIONS

Our studies have a few limitations. First, in the close-adversary attack evaluation, we created a simulation of an attacker who has some knowledge of the user by providing them with information that could be available to someone very close to the user. However, it is quite plausible that an actual close adversary would have knowledge about how the user thinks or associates that is not possible to capture easily in the type of experiment we designed. Additionally, the target-user credentials for the close-adversary attack evaluation were created by the first author of the study, who is a usable security researcher and who knew ahead of time that the credentials would be used for a security evaluation. The researcher tried to ensure that the credentials would be easy to remember and that they would be what the author would have chosen if using A3C-FA for actual authentication instead of a study. However, it is possible that they unwittingly may have chosen stronger credentials than an average user, due to their background and foreknowledge. Future work should conduct additional experiments with people who actually know one another other to compensate for some of these difficult-to-capture factors when evaluating the resilience of A3C-FA against close adversaries. Moreover, we did not evaluate the case of a combination attack where the close adversary was also able to shoulder surf. It would interesting to see how well A3C-FA performs in such a situation. Given the resilience of A3C-FA against close-adversary attacks (the way we performed our study), though, we believe that it would remain resilient against such combination attacks. How well, however, still needs to be determined.

Second, while we tried to give participants a realistic setup in using A3C-FA by giving them practice time to get used to the system and conducting the study remotely to ensure that they could use their own computing devices and AT, our study was still not the same as the participants using A3C-FA regularly as a daily authentication system. Additionally, there may be other benefits or barriers to using A3C-FA that would not be apparent until participants are able to use A3C-FA over time. Future research should explore A3C-FA "in the wild," over time to determine what, if anything, could be done to tweak A3C-FA or its larger framework to ensure it works well in real life situations.

Third, given that this was the first study to evaluate the A3C framework, we deliberately used an instantiation with a limited set of options for each credential phase (i.e., for A3C-FA, these were the primary and secondary image sets). Both for future studies on evaluating the A3C framework more thoroughly as well as designing A3C for deployment in the real world, we strongly recommend offering the user a choice of several types of options for both the primary and secondary credential components. Further, the A3C framework is not intended to be limited to images but can support other modalities, such as audio or even haptic alternatives. Any evaluation or implementation of A3C based on these other modalities also should provide diverse primary and secondary options to allow users to choose something that works for them.

12 CONCLUSION

In this article, we presented a framework called A3C, specifically designed for people with UEI to authenticate to their computing devices. A3C requires users to provide a set of *primary images* that the user knows are *recognizable* to them. Subsequently, the user is asked to *associate* each primary image with a *secondary image* (from a list of potential images provided by A3C). To study this framework, we instantiated it by implementing a version of A3C called A3C-FA, which uses images of faces of people the user knows as primary images and animal images as the secondary image. We analyzed A3C-FA in terms of its security and accessibility. We found that A3C-FA shows promise as a computing device authentication system, as our results show that it is both secure against shoulder-surfing attacks as well as close-adversary attacks. Subsequently we performed an accessibility study for A3C-FA with 14 individuals with UEI. We found that the participants were able to authenticate consistently, even after a full month past the setup. Participants also reported that they found the system easy to use and secure, as compared to other authentication options with which they were familiar. Based on these findings, we suggested four areas of future research to further improve the design of the larger A3C framework.

ACKNOWLEDGMENTS

We would like to thank all of our reviewers and participants for their invaluable help with this article.

REFERENCES

[1] Ako Muhamad Abdullah. 2017. Advanced encryption standard (AES) algorithm to encrypt and decrypt data. *Cryptography and Network Security* 16, 1 (2017), 11.

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

[3] Amazon Mechanical Turk, Inc 2005. *Amazon Mechanical Turk*. Amazon Mechanical Turk, Inc. Retrieved from https://www.mturk.com/

[4] Rúbia E. O. Schultz Ascari, Roberto Pereira, and Luciano Silva. 2020a. Computer vision-based methodology to improve interaction for people with motor and speech impairment. *ACM Transactions on Accessible Computing* 13, 4, Article 14 (Oct. 2020), 33 pages. 1936–7228. DOI: https://doi.org/10.1145/3408300

[5] Rúbia E. O. Schultz Ascari, Luciano Silva, and Roberto Pereira. 2020b. Personalized gestural interaction applied in a gesture interactive game-based approach for people with disabilities. In *Proceedings of the 25th International Conference on Intelligent User Interfaces (IUI '20)*. Association for Computing Machinery, New York, NY, 100–110. DOI: https://doi.org/10.1145/3377325.3377495

[6] 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 (ASSETS '12)*. Association for Computing Machinery, New York, NY, 159–166. DOI: https://doi.org/10.1145/2384916.2384945

[7] Sourav Banerjee. 2022. *Animal Image Dataset (90 Different Animals)*. Kaggle. Retrieved from https://www.kaggle.com/datasets/iamsouravbanerjee/animal-image-dataset-90-different-animals

[8] 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 (UbiComp '16)*. Association for Computing Machinery, New York, NY, 49–60. DOI: https://doi.org/10.1145/2971648.2971722

[9] Kemal Bicakci, Nart Bedin Atalay, Mustafa Yuceel, Hakan Gurbaslar, and Burak Erdeniz. 2009a. Towards usable solutions to graphical password hotspot problem. In *Proceedings of the 2009 33rd Annual IEEE International Computer Software and Applications Conference*, Vol. 2. IEEE, New York, NY, 318–323.

[10] Kemal Bicakci, Mustafa Yuceel, Burak Erdeniz, Hakan Gurbaslar, and Nart Bedin Atalay. 2009b. Graphical passwords as browser extension: Implementation and usability study. In *Proceedings of the IFIP International Conference on Trust Management*. Springer, Berlin, 15–29.

[11] Robert Biddle, Sonia Chiasson, and P. C. Van Oorschot. 2012. Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys* 44, 4, Article 19 (Sep. 2012), 41 pages. DOI: https://doi.org/10.1145/2333112.2333114

[12] Jeff A. Bilmes, Xiao Li, Jonathan Malkin, Kelley Kilanski, Richard Wright, Katrin Kirchhoff, Amar Subramanya, Susumu Harada, James Landay, Patricia Dowden, and Howard Chizeck. 2005. The vocal joystick: A voice-based human-computer interface for individuals with motor impairments. In *Proceedings of Human Language Technology Conference and Conference on Empirical Methods in Natural Language Processing*. Raymond Mooney, Chris Brew, Lee-Feng Chien, and Katrin Kirchhoff (Eds.). Association for Computational Linguistics, Vancouver, BC, Canada, 995–1002. Retrieved from https://aclanthology.org/H05-1125

[13] J.-C. Birget, Dawei Hong, and Nasir Memon. 2006. Graphical passwords based on robust discretization. *IEEE Transactions on Information Forensics and Security* 1, 3 (2006), 395–399.

[14] Leon Bosnjak and Bostjan Brumen. 2020. Shoulder surfing experiments: A systematic literature review. *Computers & Security* 99 (2020), Article 102023.

[15] Sacha Brostoff and M. Angela Sasse. 2000. Are passfaces more usable than passwords? A field trial investigation. In *People and Computers XIV—Usability or Else!* Sharon McDonald, Yvonne Waern, and Gilbert Cockton (Eds.), Springer, London, 405–424.

[16] Mary Brown and Felicia R. Doswell. 2010. Using passtones instead of passwords. In *Proceedings of the 48th Annual Southeast Regional Conference (ACM SE '10)*. Association for Computing Machinery, New York, NY, Article 82, 5 pages. DOI: https://doi.org/10.1145/1900008.1900119

[17] David Byrne. 2022. A worked example of Braun and Clarke's approach to reflexive thematic analysis. *Quality & Quantity* 56, 3 (2022), 1391–1412.

[18] Patrick Carrington, Amy Hurst, and Shaun K. Kane. 2014. The gest-rest: A pressure-sensitive chairable input pad for power wheelchair armrests. In *Proceedings of the 16th International ACM SIGACCESS Conference on Computers & Accessibility (ASSETS '14)*. Association for Computing Machinery, New York, NY, 201–208. DOI: https://doi.org/10.1145/2661334.2661374

[19] Sonia Chiasson, Robert Biddle, and P. C. van Oorschot. 2007. A second look at the usability of click-based graphical passwords. In *Proceedings of the 3rd Symposium on Usable Privacy and Security (SOUPS '07)*. Association for Computing Machinery, New York, NY, 1–12. DOI: https://doi.org/10.1145/1280680.1280682

[20] Sonia Chiasson, Alain Forget, Robert Biddle, and P. C. van Oorschot. 2008. Influencing users towards better passwords: persuasive cued click-points. In *Proceedings of the People and Computers XXII Culture, Creativity*, Vol. 1, 121–130.

[21] 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 *Proceedings of the 22nd International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS '20)*. Association for Computing Machinery, New York, NY, Article 14, 12 pages. DOI: https://doi.org/10.1145/3373625.3416994

[22] Fergus I. M. Craik and Robert S. Lockhart. 1972. Levels of processing: A framework for memory research. *Journal of Verbal Learning and Verbal Behavior* 11, 6 (1972), 671–684.

[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] Antonella De Angeli, Lynne Coventry, Graham Johnson, and Karen Renaud. 2005. Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. *International Journal of Human-Computer Studies* 63, 1–2 (2005), 128–152.

[25] Jiankang Deng, Jia Guo, Evangelos Ververas, Irene Kotsia, and Stefanos Zafeiriou. 2020. Retinaface: Single-shot multi-level face localisation in the wild. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. IEEE, New York, NY, 5203–5212.

[26] Rachna Dhamija and Adrian Perrig. 2000. Déja Vu: A user study using images for authentication. In *Proceedings of the 9th Conference on USENIX Security Symposium, Vol. 9. (SSYM'00)*. USENIX Association, Berkeley, CA, 4.

[27] Bryan Dosono, Jordan Hayes, and Yang Wang. 2015. "I'm stuck!": A contextual inquiry of people with visual impairments in authentication. In *Proceedings of the 11th Symposium on Usable Privacy and Security (SOUPS 2015)*. USENIX Association, Ottawa, 151–168. Retrieved from https://www.usenix.org/conference/soups2015/proceedings/presentation/dosono

[28] Paul Dunphy and Jeff Yan. 2007. Do background images improve "draw a secret" graphical passwords? In *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07)*. Association for Computing Machinery, New York, NY, 36–47. DOI: https://doi.org/10.1145/1315245.1315252

[29] Alban Dupres, José Rouillard, and Francois Cabestaing. 2014. Hybrid BCI for palliation of severe motor disability. In *Proceedings of the 26th Conference on l'Interaction Homme-Machine (IHM '14)*. Association for Computing Machinery, New York, NY, 171–176. DOI: https://doi.org/10.1145/2670444.2670466

[30] Malin Eiband, Mohamed Khamis, Emanuel Von Zezschwitz, Heinrich Hussmann, and Florian Alt. 2017. Understanding shoulder surfing in the wild: Stories from users and observers. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, 4254–4265.

[31] Facebook Inc. 2004. *Facebook*. Facebook Inc. Retrieved from https://www.facebook.com/

[32] Mingming Fan, Zhen Li, and Franklin Mingzhe Li. 2020. Eyelid gestures on mobile devices for people with motor impairments. In *Proceedings of the 22nd International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS '20)*. Association for Computing Machinery, New York, NY, Article 15, 8 pages. DOI: https://doi.org/10.1145/3373625.3416987

[33] Mingming Fan, Zhen Li, and Franklin Mingzhe Li. 2021. Eyelid gestures for people with motor impairments. *Communications of the ACM* 65, 1 (Dec. 2021), 108–115. DOI: https://doi.org/10.1145/3498367

[34] 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.

[35] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2018. "A stalker's paradise" how intimate partner abusers exploit technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, 1–13.

[36] 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.

[37] Joseph Goldberg, Jennifer Hagman, and Vibha Sazawal. 2002. Doodling our way to better authentication. In *Proceedings of the CHI '02 Extended Abstracts on Human Factors in Computing Systems (CHI EA '02)*. Association for Computing Machinery, New York, NY, 868–869. DOI: https://doi.org/10.1145/506443.506639

[38] Philippe Golle and David Wagner. 2007. Cryptanalysis of a cognitive authentication scheme. In *Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP'07)*. IEEE, New York, NY, 66–70.

[39] Naveen Sundar Govindarajulu and Sriganesh Madhvanath. 2007. Password management using doodles. In *Proceedings of the 9th International Conference on Multimodal Interfaces (ICMI '07)*. Association for Computing Machinery, New York, NY, 236–239. DOI: https://doi.org/10.1145/1322192.1322233

[40] Harkishan Singh Grewal, Aaron Matthews, Richard Tea, Ved Contractor, and Kiran George. 2018. Sip-and-puff autonomous wheelchair for individuals with severe disabilities. In *Proceedings of the 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*. IEEE, New York, NY, 705–710. DOI: https://doi.org/10.1109/UEMCON.2018.8796679

[41] Joon Kuy Han, Xiaojun Bi, Hyoungshick Kim, and Simon S. Woo. 2020. PassTag: A graphical-textual hybrid fallback authentication system. In *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security (ASIA CCS '20)*. Association for Computing Machinery, New York, NY, 60–72. DOI: https://doi.org/10.1145/3320269.3384737

[42] Susumu Harada, Jacob O. Wobbrock, and James A. Landay. 2007. Voicedraw: A hands-free voice-driven drawing application for people with motor impairments. In *Proceedings of the 9th International ACM SIGACCESS Conference on Computers and Accessibility (Assets '07)*. Association for Computing Machinery, New York, NY, 27–34. DOI: https://doi.org/10.1145/1296843.1296850

[43] Eiji Hayashi, Rachna Dhamija, Nicolas Christin, and Adrian Perrig. 2008. Use your illusion: Secure authentication usable anywhere. In *Proceedings of the 4th Symposium on Usable Privacy and Security (SOUPS '08)*. Association for Computing Machinery, New York, NY, 35–45. DOI: https://doi.org/10.1145/1408664.1408670

[44] 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 (ASSETS '17)*. Association for Computing Machinery, New York, NY, 357–358. DOI: https://doi.org/10.1145/3132525.3134788

[45] Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel Rubin. 1999. The design and analysis of graphical passwords. In *Proceedings of the 8th USENIX Security Symposium (USENIX Security 99)*. USENIX Association, Berkeley, CA, 14.

[46] Teoh Joo Fong, Azween Abdullah, N. Z. Jhanjhi, and Mahadevan Supramaniam. 2019. The coin passcode: A shoulder-surfing proof graphical password authentication model for mobile devices. *International Journal of Advanced Computer Science and Applications* 10, 1 (2019), 302–308.

[47] Shaun K. Kane, Anhong Guo, and Meredith Ringel Morris. 2020. Sense and accessibility: Understanding people with physical disabilities' experiences with sensing systems. In *Proceedings of the 22nd International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS '20)*. Association for Computing Machinery, New York, NY, Article 42, 14 pages. DOI: https://doi.org/10.1145/3373625.3416990

[48] Touraj Khodadadi, Yashar Javadianasl, Faranak Rabiei, Mojtaba Alizadeh, Mazdak Zamani, and Saman Shojae Chaeikar. 2021. A novel graphical password authentication scheme with improved usability. In *Proceedings of the 2021 4th International Symposium on Advanced Electrical and Communication Technologies (ISAECT)*. IEEE, New York, NY, 01–04. DOI: https://doi.org/10.1109/ISAECT53699.2021.9668599

[49] Ki-Hong Kim, Jae-Kwon Yoo, Hong Kee Kim, Wookho Son, and Soo-Young Lee. 2006. A practical biosignal-based human interface applicable to the assistive systems for people with motor impairment. *IEICE Transactions on Information and Systems* E89-D, 10 (Oct. 2006), 2644–2652. DOI: https://doi.org/10.1093/ietisy/e89-d.10.2644

[50] Vinay Krishna Sharma, Kamalpreet Saluja, Vimal Mollyn, and Pradipta Biswas. 2020. Eye gaze controlled robotic arm for persons with severe speech and motor impairment. In *Proceedings of the ACM Symposium on Eye Tracking Research and Applications (ETRA '20 Full Papers)*. Association for Computing Machinery, New York, NY, Article 12, 9 pages. DOI: https://doi.org/10.1145/3379155.3391324

[51] 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 (ASSETS '10)*. Association for Computing Machinery, New York, NY, 289–290. DOI: https://doi.org/10.1145/1878803.1878875

[52] Jonathan Lazar and Michael Ashley Stein (Eds.). 2017. *Disability, Human Rights, and Information Technology*. University of Pennsylvania Press, Philadelphia, PA. Retrieved from http://www.jstor.org/stable/j.ctv2t4d02

[53] Brittany Lewis, Joshua Hebert, Krishna Venkatasubramanian, Matthew Provost, and Kelly Charlebois. 2020. A new authentication approach for people with upper extremity impairment. In *Proceedings of the 2020 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*. IEEE, New York, NY, 1–6. DOI: https://doi.org/10.1109/PerComWorkshops48775.2020.9156171

[54] 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 *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, Article 379, 14 pages. DOI: https://doi.org/10.1145/3411764.3445070

[55] Franklin Mingzhe Li, Michael Xieyang Liu, Yang Zhang, and Patrick Carrington. 2022. Freedom to choose: Understanding input modality preferences of people with upper-body motor impairments for activities of daily living. In *Proceedings of the 24th International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS '22)*. Association for Computing Machinery, New York, NY, Article 39, 16 pages. DOI: https://doi.org/10.1145/3517428.3544814

[56] Yao Ma, Jinjuan Feng, Libby Kumin, and Jonathan Lazar. 2013. Investigating user behavior for authentication methods: A comparison between individuals with down syndrome and neurotypical users *ACM Transactions on Accessible Computing* 4, 4, Article 15 (Jul 2013), 27 pages. DOI: https://doi.org/10.1145/2493171.2493173

[57] 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 (ASSETS '12)*. Association for Computing Machinery, New York, NY, 241–242. DOI: https://doi.org/10.1145/2384916.2384973

[58] Bishop Matt. 2018. *Computer Security: Art and Science*. Stockholm Environment Institute (SEI), Stockholm.

[59] Peter Mayer, Nina Gerber, Benjamin Reinheimer, Philipp Rack, Kristoffer Braun, and Melanie Volkamer. 2019. I (don't) see what you typed there! Shoulder-surfing resistant password entry on gamepads. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. Association for Computing Machinery, New York, NY, 1–12. DOI: https://doi.org/10.1145/3290605.3300779

[60] Wendy Moncur and Grégory Leplatre. 2007. Pictures at the ATM: Exploring the usability of multiple graphical passwords. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '07)*. Association for Computing Machinery, New York, NY, 887–894. DOI: https://doi.org/10.1145/1240624.1240758

[61] Imad Mougharbel, Racha El-Hajj, Houda Ghamlouch, and Eric Monacelli. 2013. Comparative study on different adaptation approaches concerning a sip and puff controller for a powered wheelchair. In *Proceedings of 2013 Science and Information Conference*. The Science and Information (SAI) Organization, Cleckheaton, UK.

[62] John E. Muñoz, Ricardo Chavarriaga, and David S. Lopez. 2014. Application of hybrid BCI and exergames for balance rehabilitation after stroke. In *Proceedings of the 11th Conference on Advances in Computer Entertainment Technology (ACE '14)*. Association for Computing Machinery, New York, NY, Article 67, 4 pages. DOI: https://doi.org/10.1145/2663806.2671211

[63] Syifaun Nafisah, Oyas Wahyunggoro, and Lukito Nugroho. 2016. Evaluating the usage of short-time energy on voice biometrics system for cerebral palsy. In *Proceedings of the 2016 8th International Conference on Information Technology and Electrical Engineering (ICITEE)*. IEEE, New York, NY, 1–6. DOI: https://doi.org/10.1109/ICITEED.2016.7863303

[64] Deholo Nali and Julie Thorpe. 2004. *Analyzing User Choice in Graphical Passwords*. Technical Report. Carleton University.

[65] Olayemi Mikail Olaniyi, Jibril Abdullahi Bala, Juliana Ndunagu, Adamu Abubakar, and Ahmad Ishaq. 2019. V-Authenticate: Voice authentication system for electorates living with disability. In *Proceedings of the Cyber Secure Nigeria 2019 Conference*. Cyber Security Experts Association of Nigeria, Nigeria, 10.

[66] Trevor Pering, Murali Sundar, John Light, and Roy Want. 2003. Photographic authentication through untrusted terminals. *IEEE Pervasive Computing* 2, 1 (2003), 30–36.

[67] Norman Poh, Ramon Blanco-Gonzalo, Rita Wong, and Raul Sanchez-Reillo. 2016. Blind subjects faces database. *IET Biometrics* 5, 1 (2016), 20–27.

[68] George E. Raptis, Christina Katsini, Andrew Jian-Lan Cen, Nalin Asanka Gamagedara Arachchilage, and Lennart E. Nacke. 2021. Better, funner, stronger: A gameful approach to nudge people into making less predictable graphical password choices. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, 1–17.

[69] Karen Renaud. 2009. On user involvement in production of images used in visual authentication. *Journal of Visual Languages & Computing* 20, 1 (2009), 1–15. DOI: https://doi.org/10.1016/j.jvlc.2008.04.001

[70] Syed Asad Rizvi, Ella Tuson, Breanna Desrochers, and John Magee. 2018. Simulation of motor impairment in head-controlled Pointer Fitts' Law task. In *Proceedings of the 20th International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS '18)*. Association for Computing Machinery, New York, NY, 376–378. DOI: https://doi.org/10.1145/3234695.3241034

[71] Timothy B. Rogers, Nicholas A. Kuiper, and William S. Kirker. 1977. Self-reference and the encoding of personal information. *Journal of Personality and Social Psychology* 35, 9 (1977), 677.

[72] Lucas Rosenblatt, Patrick Carrington, Kotaro Hara, and Jeffrey P. Bigham. 2018. Vocal programming for people with upper-body motor impairments. In *Proceedings of the 15th International Web for All Conference (W4A '18)*. Association for Computing Machinery, New York, NY, Article 30, 10 pages. DOI: https://doi.org/10.1145/3192714.3192821

[73] Steven V Rouse. 2015. A reliability analysis of Mechanical Turk data. *Computers in Human Behavior* 43 (2015), 304–307.

[74] David M. Roy, Marilyn Panayi, Roman Erenshteyn, Richard Foulds, and Robert Fawcus. 1994. Gestural human-machine interaction for people with severe speech and motor impairment due to cerebral palsy. In *Proceedings of the Conference Companion on Human Factors in Computing Systems (CHI '94)*. Association for Computing Machinery, New York, NY, 313–314. DOI: https://doi.org/10.1145/259963.260375

[75] 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 (ASSETS '17)*. Association for Computing Machinery, New York, NY, 403–404. DOI: https://doi.org/10.1145/3132525.3134785

[76] Florian Schaub, Marcel Walch, Bastian Könings, and Michael Weber. 2013. Exploring the design space of graphical passwords on smartphones. In *Proceedings of the 9th Symposium on Usable Privacy and Security (SOUPS '13)*. Association for Computing Machinery, New York, NY, Article 11, 14 pages. DOI: https://doi.org/10.1145/2501604.2501615

[77] Tsu-Wang Shen. 2008. Applied ECG biometric technology for disability population personalization. In *Proceedings of the 2nd International Convention on Rehabilitation Engineering & Assistive Technology (iCREATe '08)*. Singapore Therapeutic, Assistive & Rehabilitative Technologies (START) Centre, Midview City, SGP, 103–107.

[78] Young Chol Song. 2010. Joystick text entry with word prediction for people with motor impairments. In *Proceedings of the 12th International ACM SIGACCESS Conference on Computers and Accessibility (ASSETS '10)*. Association for Computing Machinery, New York, NY, 321–322. DOI: https://doi.org/10.1145/1878803.1878892

[79] Huiping Sun, Ke Wang, Xu Li, Nan Qin, and Zhong Chen. 2015. PassApp: My app is my password! In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI '15)*. Association for Computing Machinery, New York, NY, 306–315. DOI: https://doi.org/10.1145/2785830.2785880

[80] Xiaoyuan Suo, Ying Zhu, and G Scott Owen. 2005. Graphical passwords: A survey. In *Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC'05)*. IEEE, New York, NY, 463–472.

[81] Tetsuji Takada and Hideki Koike. 2003. Awase-E: Image-based authentication for mobile phones using user's favorite images. In *Human-Computer Interaction with Mobile Devices and Services*. Luca Chittaro (Ed.). Springer, Berlin, 347–351.

[82] Hai Tao and Carlisle Adams. 2008. Pass-go: A proposal to improve the usability of graphical passwords. *International Journal of Network Security*. 7, 2 (2008), 273–292.

[83] Furkan Tari, A. Ant Ozok, and Stephen H. Holden. 2006. A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. In *Proceedings of the 2nd Symposium on Usable Privacy and Security (SOUPS '06)*. Association for Computing Machinery, New York, NY, 56–66. DOI: https://doi.org/10.1145/1143120.1143128

[84] Thomas S. Tullis and Donna P. Tedesco. 2005. Using personal photos as pictorial passwords. In *Proceedings of the CHI '05 Extended Abstracts on Human Factors in Computing Systems (CHI EA '05)*. Association for Computing Machinery, New York, NY, 1841–1844. DOI: https://doi.org/10.1145/1056808.1057036

[85] Thomas S. Tullis, Donna P. Tedesco, and Kate E. McCaffrey. 2011. Can users remember their pictorial passwords six years later. In *Proceedings of the CHI '11 Extended Abstracts on Human Factors in Computing Systems (CHI EA '11)*. Association for Computing Machinery, New York, NY, 1789–1794. DOI: https://doi.org/10.1145/1979742.1979945

[86] Twitter, Inc. 2006. *Twitter*. Twitter, Inc. Retrieved from https://www.twitter.com/

[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] Paul C. van Oorschot and Julie Thorpe. 2011. Exploiting predictability in click-based graphical passwords. *Journal of Computer Security* 19, 4 (2011), 669–702.

[89] Radu-Daniel Vatavu and Ovidiu-Ciprian Ungurean. 2019. Stroke-gesture input for people with motor impairments: Empirical results & research roadmap. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. Association for Computing Machinery, New York, NY, 1–14. DOI: https://doi.org/10.1145/3290605.3300445

[90] Krishna Venkatasubramanian, Jeanine L. M. Skorinko, Mariam Kobeissi, Brittany Lewis, Nicole Jutras, Pauline Bosma, John Mullaly, Brian Kelly, Deborah Lloyd, Mariah Freark, and Nancy A. Alterio. 2021. Exploring a reporting tool to empower individuals with intellectual and developmental disabilities to self-report abuse. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, Article 373, 13 pages. DOI: https://doi.org/10.1145/3411764.3445150

[91] Emanuel von Zezschwitz, Paul Dunphy, and Alexander De Luca. 2013. Patterns in the wild: A field study of the usability of pattern and pin-based authentication on mobile devices. In *Proceedings of the 15th International Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI '13)*. Association for Computing Machinery, New York, NY, 261–270. DOI: https://doi.org/10.1145/2493190.2493231

[92] Ker-Jiun Wang, Quanbo Liu, Yifan Zhao, Caroline Yan Zheng, Soumya Vhasure, Quanfeng Liu, Prakash Thakur, Mingui Sun, and Zhi-Hong Mao. 2018. Intelligent wearable virtual reality (VR) gaming controller for people with motor disabilities. In *Proceedings of the 2018 IEEE International Conference on Artificial Intelligence and Virtual Reality (AIVR)*. IEEE, New York, NY, 161–164. DOI: https://doi.org/10.1109/AIVR.2018.00034

[93] Kieran Watson, Robin Bretin, Mohamed Khamis, and Florian Mathis. 2022. The feet in human-centred security: Investigating foot-based user authentication for public displays. In *Proceedings of the Extended Abstracts of the 2022 CHI Conference on Human Factors in Computing Systems (CHI EA '22)*. Association for Computing Machinery, New York, NY, Article 441, 9 pages. DOI: https://doi.org/10.1145/3491101.3519838

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

[95] Daphna Weinshall. 2006. Cognitive authentication schemes safe against spyware. In *Proceedings of the 2006 IEEE Symposium on Security and Privacy (S & P'06)*. IEEE, New York, NY, 6.

[96] Roman Weiss and Alexander De Luca. 2008. PassShapes: Utilizing stroke based authentication to increase password memorability. In *Proceedings of the 5th Nordic Conference on Human-Computer Interaction: Building Bridges (NordiCHI '08)*. Association for Computing Machinery, New York, NY, 383–392. DOI: https://doi.org/10.1145/1463160.1463202

[97] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. 2005. PassPoints: Design and longitudinal evaluation of a graphical password system. *International Journal of Human-Computer Studies* 63, 1–2 (2005), 102–127.

[98] Linda Wilson. 2023. *Assistive Technology for the Disabled Computer User*. Institute of Educational Sciences. Retrieved from https://eric.ed.gov/?id=ED364189

[99] 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 (ASSETS '17)*. Association for Computing Machinery, New York, NY, 385–386. DOI: https://doi.org/10.1145/3132525.3134793

[100] Shuo Yang, Ping Luo, Chen Change Loy, and Xiaoou Tang. 2016. WIDER FACE: A face detection benchmark. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*. IEEE, New York, NY, 5525–5533.

[101] Xingjie Yu, Zhan Wang, Yingjiu Li, Liang Li, Wen Tao Zhu, and Li Song. 2017. EvoPass: Evolvable graphical password against shoulder-surfing attacks. *Computers & Security* 70 (2017), 179–198. DOI: https://doi.org/10.1016/j.cose.2017.05.006

[102] Nur Haryani Zakaria, David Griffiths, Sacha Brostoff, and Jeff Yan. 2011. Shoulder surfing defence for recall-based graphical passwords. In *Proceedings of the 7th Symposium on Usable Privacy and Security (SOUPS '11)*. Association for Computing Machinery, New York, NY, Article 6, 12 pages. DOI: https://doi.org/10.1145/2078827.2078835

[103] 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 (CHI '17)*. Association for Computing Machinery, New York, NY, 2878–2889. DOI: https://doi.org/10.1145/3025453.3025790

[104] 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 (Assets '09)*. Association for Computing Machinery, New York, NY, 229–230. https://doi.org/10.1145/1639642.1639689

[105] Zoom. 2021. *Zoom*. Zoom. Retrieved from lhttps://zoom.us/

Received 28 August 2023; revised 2 January 2024; accepted 1 March 2024