UniPass: Design and Evaluation of a Smart Device-Based Password Manager for Visually Impaired Users

Natã M. Barbosa, Jordan Hayes, Yang Wang
SALT Lab, School of Information Studies, Syracuse University
{nmbarbos | jhayes05 | ywang}@syr.edu

ABSTRACT

Visually impaired users face various challenges in web authentication. We designed UniPass, an accessible password manager for visually impaired users based on a smart device. To evaluate UniPass, we tested and compared UniPass with two commercial password managers: LastPass, a popular password manager and StrongPass, a smart device-based password manager. Our study results of ten users, six blind and four with low vision, suggest that password managers are a promising authentication approach for visually impaired users. Participants using UniPass had the highest task completion rate and took the shortest time to complete an authentication related task. Furthermore, the majority (seven out of ten) of our participants preferred UniPass over LastPass and StrongPass.

ACM Classification Keywords

D.4.6 Security and Protection: Access Controls, Authentication, and Verification.

Author Keywords

Authentication; Password Manager; Smart Device; Accessibility; Visual Impairments;

INTRODUCTION

Despite the limitations of password schemes, they are still the most common form of logging into a website. To this date, there is still no alternative that outperforms passwords in all relevant aspects such as security, usability, and deployability [4]. Novel mechanisms expecting users to change behavior are less likely to exist long-term [5]. This supports the idea that passwords will be around for years to come, having users cope with issues such as reusing passwords and/or creating passwords that are insecure but easy to remember [12]. Some users adopt web browsers' built-in password reminders or dedicated passwords managers for creating, maintaining, and remembering strong passwords. Password managers can be a viable mechanism to help users deal with complex password policies and a large number of online accounts, although the underlying technology remains replayable [4]. Historically, most password managers rely on a master password either stored in the cloud or locally on a computer.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.
UbiComp '16, September 12 - 16, 2016, Heidelberg, Germany
Copyright is held by the owner/author(s). Publication rights licensed to ACM.
ACM 978-1-4503-4461-6/16/09...$15.00
DOI: http://dx.doi.org/10.1145/2971648.2971722

The recent advent of smart devices and wearable technology has motivated a great amount of existing research dedicated to authentication on those devices (e.g., unlocking the device). Because of the great capabilities and ubiquitous presence of these devices, systems such as Knock x Knock [13], UbiKiMa [11], Tapas [20], and StrongPass [1] aim to provide an authentication system centered around a smart device. We believe this will soon become the trend for password management software. However, such systems are not designed considering the needs of users with disabilities, making them struggle with these systems. Users with visual impairments face various issues when dealing with password-based authentication on the web [10]. Our work tries to bridge this gap, leveraging smart-device based password management while making password schemes more accessible and inclusive.

We propose a solution by evaluating web authentication from an accessibility perspective. Our research aims to provide accessible web authentication through a password manager prioritizing both usability and security. We have designed UniPass to leverage the richness of sensors and the processing capacity of smartphones, combined with capabilities of modern browsers to bridge usability gaps and expand the possibilities for logging into a website. People with disabilities may not have their own computers and thus may need to use public or shared (e.g., library) computers [10]. With UniPass, users needing to use a public computer to log into an online account would visit the website, hold the phone near the computer and confirm their identity by scanning their fingerprint, then the login form will be filled and submitted automatically assuming their credentials for the site are stored in the phone.

To evaluate UniPass, we recruited visually impaired users to conduct tasks such as creating new website accounts, saving passwords to the password manager and logging in using UniPass as well as two commercial password managers: LastPass [17] and StrongPass [1]. We aim to understand whether password managers are a viable option for users with visual impairments as well as whether design decisions in our system simplify logging into a website for users with visual impairments while offering them the benefits of a password manager. Additionally, we also seek to understand this population's mental models, perceived security, perceived necessity and acceptance, perceived ease of use, comfort level, and perceived

accessibility when using password managers. Our main contribution is twofold: (1) we designed an accessible smart-device-based password manager for people with visual impairments and (2) we conducted a comparative evaluation of our proposed system and existing password managers with visually impaired users. The study sheds light on users' perceptions of password managers in general, but also uncovers accessibility challenges of existing password managers. In addition, the study results suggest that password managers are actually a promising approach for accessible authentication. We discuss how current password managers can be improved to be more accessible, particularly for users with visual impairments.

RELATED WORK

Smart Device-Based Password Managers

Everts *et al.* [11] proposed UbiKiMa, a system using a smartphone to authenticate users on the web. The system introduces an authentication scheme based on public key cryptography as a password replacement while supporting compatibility with usernames and passwords as a way of gradually transitioning to the newly proposed scheme. McCarney *et al.* [20] design Tapas, a password manager without a master password that is based on the concept of dual-possession authentication, where two independent devices are required to log in. Our earlier work [3] introduces an inclusive authentication framework by transferring the authentication task to a smart device (e.g., a smartphone) when logging into websites. Instead of a master password, the system leverages the smart device's sensors to authenticate (e.g., biometrics). Hayashi and Hong [13] propose Knock x Knock, a system that allows users to authenticate to a smartphone or wearable device, which can then log in to websites on the user's behalf, using the device as a password manager. Authentication will leverage the device's sensors instead of relying on a master password. Additionally, the authors introduce tiered (e.g., sensitive *vs.* secure websites) and location-aware (e.g., trusted locations) authentication incorporated into the password manager. Our UniPass system differs from these existing systems mainly in terms of accessibility and deployability. We discuss these differences after describing UniPass in the next section.

Usability Evaluation of Password Managers

Chiasson *et al.* [7] report results of a study with 27 participants to evaluate the usability of two password managers, including major usability problems related to users' mental models in understanding how password managers work, users' views on the necessity of adopting a password manager as well as users' willingness to relinquish control of passwords to a computer program. In addition, the authors point out that incorrect mental models may cause leakage of sensitive information and render password management systems vulnerable. Karole *et al.* [15] evaluate the usability of three password managers of distinct categories: online and portable. The authors report that all users preferred portable password managers over online managers because users did not feel comfortable giving control to an online entity as opposed to retaining such control over their own portable devices. McCarney [19] extends Bonneau *et al.*'s [4] framework to evaluate different password managers including Tapas, the author's proposed system. After comparing Tapas with Firefox's built-in password manager with and without a master password, the author concludes that users found the dual-possession workflow introduced in Tapas (e.g., using a computer and a smartphone) to offer similar conveniences to that of Firefox's built-in password manager protected by a master password. Despite these evaluations, we are not aware of any prior user testing of password managers by visually impaired users.

Recommendations and Gaps in the Literature

Although not focused on accessibility, several studies in the literature compare the usability of password managers and provide recommendations for designers of these systems. We made specific design decisions based on these recommendations when designing UniPass: (1) provide clear feedback when saving and protecting a password [7]; (2) provide clear feedback when accessing a password [7]; (3) make the current state of the system easily determinable at all times [7]; (4) store credentials on a device controlled by users in order to increase acceptance, perceived security, and perceived necessity [13, 15] and (5) avoid the use of a master password to simplify the workflow [20].

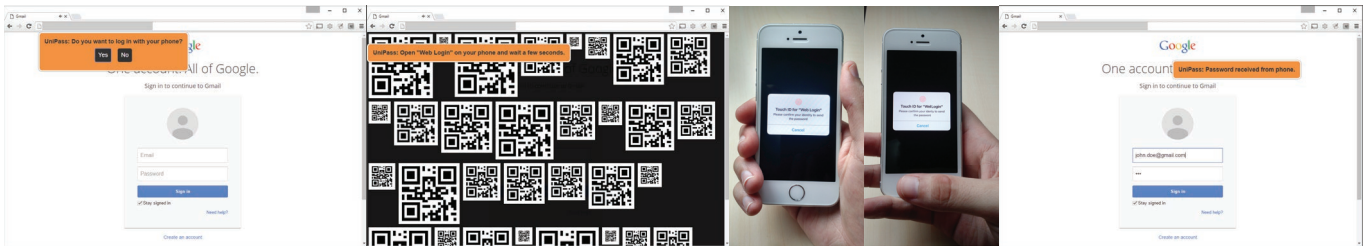
UniPass was also inspired by the literature on the issues visually impaired users face when logging into websites [6, 10, 16, 21]. For instance, it is particularly time-consuming for visually impaired users to locate the login form on a web page and correctly type their user names and passwords [10].

UNIPASS

The key idea of UniPass is to leverage a password manager and smart devices, where users simply authenticate to a smart device, allowing their login credentials to be used on another device (e.g., a laptop or a desktop computer).

UniPass consists of three main components: a password manager application, a proxy server, and a browser client. The password manager application could be installed on a smart device, such as a smartphone. The proxy server could be a web sockets server to mediate the connection between the password manager and the browser client. The browser client could be a browser extension or a piece of JavaScript code handling the browser side, managing tasks such as broadcasting a device-pairing code as well as detecting, completing, and submitting the login form automatically. Both the password manager application and the browser client know how to reach the proxy server (i.e., the address of the server).

The system works by having users transfer login information to the smart device either when creating a new account to a website (e.g., signing up) or when logging into a website with the intent of allowing the smart device to remember the login information in the future. With the login credentials for a website stored on the smart device and users at the login page, the users will be prompted whether to use the login information stored on the smart device for said website. If users choose to do so, then the website and the smart device complete a pairing process and users are asked to authenticate to the smart device in order to authorize sharing of the credentials with the



(a) (b) (c) (d) (e)

Figure 1: Prototype 2 of UniPass. (a) Prompt asks if a user wants to log in with her phone. (b) Browser broadcasts multiple QR codes and high-frequency audio tones. (c) Phone recognizes audio tones and asks the user for fingerprint. (d) User scans fingerprint. (e) Login form is filled and submitted.

computer. Once the login information is transferred, the login form on the computer is filled and submitted automatically.

UniPass differs from other password managers in two aspects: **Accessibility:** This system features a minimalistic design approach favoring accessibility. Only the minimum necessary steps and graphical elements are included to complete the task of authentication on the smart device and to send passwords to the computer in order to avoid overwhelming users who rely on assistive technologies, such as screen readers. For example, there is no user interface to see and change passwords stored on the smart device and there are no buttons except those on confirmation dialogs. Besides, users enter their credentials into the password manager on the computer instead of the phone, improving the accessibility over our earlier work [3].

Deployability: UniPass makes relatively minor software/hardware assumptions such as a public (desktop) computer having a speaker. Our device pairing mechanism does not require Bluetooth as in Knock x Knock [13]. It is reasonable to assume that desktop computers are more likely to have speakers than Bluetooth. In addition, any custom sensor (e.g., fingerprint sensor) used for authentication to the smart device could be replaced by other, more accessible sensors (e.g., gyroscope, accelerometer, camera, microphone) as long as they provide a reliable method (e.g., face/voice recognition, behavioral biometrics) to authenticate to the phone. UniPass runs through a browser extension or JavaScript library (e.g., website developers can support UniPass on their websites without a browser extension). This design decision was informed by the commodity principle of the ability-based design [24], which suggests people with disabilities may only afford or own low-end devices and thus accessible systems should not rely on custom hardware or software components.

In order to evaluate UniPass, we iteratively developed and tested two prototypes with visually impaired users.

Prototype 1

In our early exploration, we designed a prototype and conducted a preliminary user study. In this version of UniPass, users paired the phone and the computer by scanning a QR code on the computer screen and authenticated to the smartphone by performing a secret movement with the phone (e.g., shaking the phone). The first prototype was developed for Android. The computer and the phone communicated together with the help of a browser extension. From the beginning, we presumed users with visual impairments would have great difficulty scanning the QR code on the computer screen. Therefore, we developed an alternative QR code broadcast changing the position and the size of the code randomly at every 100 milliseconds for faster scans.

Preliminary User Study

During the spring and summer of 2015, we conducted a formative evaluation with nine users to test our initial design: five blind users, three users with low vision, and one sighted user. Users were given Prototype 1 to test and were asked questions about the overall ease of use, perceived security, and accessibility. We found users encountered difficulties in embracing the steep learning curve of our prototype. We also found the most challenging part for users was dealing with speech from screen readers on both the computer and the smartphone. Another common issue was confusion between distinguishing authentication to the phone and authentication to the website. Users also struggled to complete the task of scanning the code, even though the QR code was optimized to randomly change its position in order to reduce the need to point accurately to various parts of the screen.

This study greatly guided our design decisions to accommodate the needs and preferences of users with visual impairments. We learned that we needed to simplify the workflow. We also needed to improve prompts and user feedback as well as the overall compatibility with screen readers. Specific design decisions were also made based on users' comments and observations, which were incorporated into UniPass: (1) make messages and prompts clearer and more specific; (2) offer biometric authentication; (3) provide little context to bystanders when authenticating to the smartphone; (4) show messages only on one device (e.g., either the computer or the smartphone) to avoid switching devices; (5) avoid touchscreen interactions since they rely too much on visual navigation; and (6) provide an alternative device pairing method without visual elements (e.g., QR codes).

Prototype 2

Based on the results of the preliminary user evaluation, we developed the 2nd version of UniPass (see Figure 1) where users would pair the computer with the phone via high-frequency audio tones and authenticate to the phone by scanning a fingerprint. Our implementation of this device-pairing mechanism

was inspired by the Ultrasonic Networking project on Github [23]. We still provided the QR code as a fallback pairing approach, broadcasting codes of multiple sizes on the computer screen as we empirically verified this approach yielded reasonably faster scans.

We are aware that relying on a fingerprint sensor on the smartphone detriments the high deployability aspect of our system. However, we chose to deprecate the "shake the phone" device authentication strategy because it was perceived as unreliable in the preliminary user study. Fingerprint scanning works as a placeholder for other device authentication mechanisms (e.g., [2]). We used fingerprint because our earlier research found visually impaired users feel biometrics could be easy to use [10]. Fingerprint scanning is also reasonably reliable, easy to implement, and starts to be adopted on smartphones: the fingerprint scanner is available on the iPhone since its 5s version and on high-end Android phones.

Prototype 2 was developed for iOS and Android, using a Chrome browser extension to facilitate communication between the browser on the computer and the smartphone application. Our main user evaluation focuses on this prototype.

Features for Visually Impaired Users

We implemented specific features in order to make the workflow of UniPass accessible to users with visual impairments. These features are present so users can easily complete the tasks necessary to transfer data between the computer and the smartphone, authenticate to the phone, and log into a website. Instructions are present at all times and are as specific as possible. All prompts and messages are read aloud by the screen reader through accessible dialogs on the login and registration pages when the screen reader is activated. These dialogs are implemented with Accessible Rich Internet Applications Suite (ARIA) roles and other attributes. Buttons and other graphical elements are avoided throughout the workflow and are used only when absolutely necessary (e.g., confirmation dialogs). When a login page is detected by an algorithm, the system prompts users whether they want to log in with their phone or enter the password manually. All prompts and messages are displayed on the computer except for the fingerprint prompt. The prompt to scan the fingerprint on the smartphone can be read aloud by the smartphone's screen reader. The device also vibrates every time users must scan a valid fingerprint to authorize sending of the passwords.

Transferring login information between the smartphone and the web page requires establishing a communication channel between the two devices. This pairing task is usually done by scanning a QR code representation of a text token with the smartphone. However, our preliminary study showed users with visual impairments often required verbal guidance in order to scan the QR code. We offered the pairing task by broadcasting representations of the pairing code from the computer via high-frequency audio tones and multiple QR codes of random sizes simultaneously. When open, the smartphone app synchronously tries to detect the high-frequency tones via the smartphone's microphone and the QR code via the phone's camera in order to start the authorization process. Whichever is detected first is used as the pairing code to connect with the computer over the Transport Layer Security (TLS) protocol.

When login information is not available on the smartphone app, users complete the login form on the computer and then the credentials are transferred to the smartphone for future use: completing the login form on the phone's touchscreen keyboard is challenging for users with visual impairments. Finally, the UniPass mobile app is named "Web Login" in order for Siri/Google Now to easily detect the voice command to open the app, saving users' time.

USER STUDY

Between February and March 2016, we conducted a study with visually impaired users to test UniPass and compare our system with LastPass and StrongPass, two commercial password managers. We aim to understand visually impaired users' perceptions and experiences of these password managers and whether our system would outperform the other two systems.

LastPass is a web-based password manager providing a web browser extension capable of storing usernames and passwords in a centralized "vault" (i.e., a password database). To log into a website on a computer, users enter their LastPass master password into the browser extension and the browser extension will automatically fill the login forms of websites if the login information is in the "vault." We chose LastPass because it is a popular password manager.

StrongPass is a web-based password manager providing a mobile application capable of storing usernames and passwords on a smartphone. To log into a website with StrongPass, users enter a master password on their smartphone and connect the phone with the computer by scanning a QR code on the computer. Once connected, the login information is transferred to the web browser on the computer and the login form is filled automatically. StrongPass was chosen because it is a publicly available smart device-based password manager.

UniPass differs from StrongPass as follows: UniPass works without any master passwords; users enter login information the first time on the computer rather than on the phone; UniPass performs device pairing in an automated fashion with QR codes and audio tones with no time limits; and UniPass prompts consist of blocking dialog boxes so that these prompts will be read by screen readers instead of passive address bar icons or toolbars that cannot be read by screen readers. UniPass also differs from LastPass: LastPass does not support using a phone to log into accounts on another computer; UniPass does not require a master password; UniPass requires a smart device to function; UniPass asks users if they want to complete the login form instead of automatically completing the form; and UniPass has fewer steps before login information is stored. Finally, the major differences between UniPass and the other two systems are: UniPass has no credential management user interface (e.g., the ability to edit or delete passwords) and UniPass was designed from the beginning to work well with screen readers both on computers and phones.

We recruited visually impaired users for a study session in their preferred location (e.g., home, office, or our lab). We paid each participant $20 (USD) for a session lasting approximately

2 hours. Our study was approved by our University IRB. We created four fictitious websites mimicking the homepage, login, and registration pages of four real websites: Amazon, Facebook, Gmail, and the Chase bank. We hosted these test sites in our own server with a password so that they are not public and can only be accessed with the password. We also developed an account management server to allow accounts for those websites to be created and used. Our goal was to closely mimic the user interface of real websites without compromising our participants' real login credentials for those websites. Before the tasks, we explicitly told participants these are fictitious websites for testing purposes and they should not use their actual login credentials.

For every session, users tested two password managers with the fictitious websites, one password manager always being UniPass. We did not test all three password managers at every session in order to avoid user fatigue. We ensured the other two password managers (LastPass and StrongPass) were tested an equal number of times across all participants.

We provided a laptop computer with Windows 8, ZoomText 10, JAWS 17 screen reader, and the browser extensions for each password manager pre-installed. We also provided a smartphone with either iOS (either iPhone 6s, iPhone 5s, or iPhone 6) or Android (Samsung Galaxy Note 4), depending on participants' preference and background. For example, if participants were iPhone users, we gave them an iPhone with the password managers installed for the tests. If participants did not have a preference (e.g., did not own a smartphone), we arbitrarily chose a platform for them so both platforms were tested roughly the same number of times.

Participant Recruitment

We recruited prospective participants via private email, mailing lists of local organizations serving people with visual impairments as well as by phone. We also used snowball sampling (i.e., asking participants to refer us to other prospective participants). Despite our efforts and our willingness to travel to sites prospective participants chose (e.g., we drove about an hour to see one participant in a rural area), we had a difficult time recruiting participants. We suspect this is partly due to prospective participants finding testing new software to be overwhelming. In order to have a larger pool of participants, we contacted previous participants who had tested Prototype 1 of UniPass in the summer of 2015. In the end, 10 participants (six blind users and four users with low vision) finished the study and six of them (P2, P3, P5, P7, P9, and P10) had tested Prototype 1 previously.

Pre-Task Questionnaire

Before testing the password managers, we asked participants questions about demographics, disability condition, personal password management strategies, number of online accounts and passwords, password sharing, knowledge of password managers, devices used for the Internet, difficulties browsing the web, and assistive technology used.

Tasks

Before beginning the testing portion of the study, we gave each participant a brief introduction to password managers and an overview of the two password managers he or she will test. We also briefly explained the tasks participants will perform.

For each password manager, we enabled the browser extension for participants, saving them time from setting up any software during the test session. If the password manager required a master password, we asked participants to create one and tell us in order for us to configure the chosen password into the password manager on their behalf. If the password manager required a smartphone to be used, we briefly explained how to navigate the touchscreen and open an app with the help of the smartphone's screen reader or the voice commands available through the operating system. To test UniPass, we helped participants register their fingerprints in the smartphone and briefly explained how to use the fingerprint scanner.

For every session, we randomly chose three test websites and randomized the order of the sites. For each password manager, we first provided participants a training by verbally guiding them to: (a) create a new account on website #1, saving the password to the password manager; and (b) log into website #1 with the password manager. We provided this training so that participants can have a basic and comparable understanding of how each password manager works.

Next, participants conducted the actual testing tasks: (1) create a new account on website #2, saving the password to the password manager; (2) log into Website #2 with the password manager; (3) log into website #3 with existing login information provided by our team, saving the password to the password manager; and (4) log into website #3 with the password manager. Every participant executed these tasks twice – once for a password manager. We asked participants to think aloud and express their thought processes. With the participant's consent, sessions were video and audio recorded.

Post-Task Questionnaire

At the end of the test with each password manager, we asked participants to complete a five-point Likert-Scale questionnaire about the password manager. We reused some groups and questions from Chiasson *et al.*'s study [7]. We presented the questions ungrouped and in random order for every session. We did not disclose the group of questions to users. Participants were given statements such as *"My passwords are secure when using this password manager"* and *"This password manager is difficult to use"* and then asked to rate on a 1-5 scale how much they agreed with the statement, ranging from "1 - Strongly Disagree" to "5 - Strongly Agree."

In addition, we asked participants some mental model questions such as describing steps and where they thought their passwords were stored. Next, we posed a scenario where they would need to use a public library computer to reply to an urgent email, further capturing their mental models and learning whether they would choose to use the password manager in such case. We also asked participants whether they would suggest any improvements for the system. Upon completing the tasks with the two password managers, we asked users to tell us which password manager they prefer. We asked them which of the systems offered more security and convenience in their opinion and, on a 1-5 scale, how likely they would start

using password managers after the study and to explain their answers. We wrapped up by asking them whether they had any suggestions to improve password managers in general.

RESULTS

Participants

We had a total of 10 participants who finished the study. In terms of age, one participant reported in 20's, two in 40's, three in 50's, two in 60's, and two in 70's. Seven participants were male and three were female. Six participants reported being completely blind (P2, P3, P6, P7, P8, and P9), two legally blind (P1 and P10), and two visually impaired with limited eye-sight (P4 and P5). Our participants had various backgrounds such as a consultant, a librarian and a reporter. Six participants owned a smartphone: five owned an iPhone and one owned a Windows Phone. Three participants reported their smartphones as being their primary device for Internet use. Four users reported using public/shared computers. Six out of ten participants reported having more online accounts than passwords, suggesting the reuse of passwords.

Exposure to Password Managers

None of the participants reported using a dedicated password manager. Four participants had heard of dedicated password managers before the study and their understanding was somewhat correct. For instance, P2 described password managers as *"software to remember passwords so you don't need to remember them."* Two participants incorrectly thought password managers as a feature provided by a website to remember a user session. For instance, P7 explained *"I guess Amazon has a password manager. Bookshare has a password manager. [...] a process that enables you to automatically go on and not have to use a password."*

Reasons Not to Use Password Managers

Three participants did not want to use a password manager either because it is difficult to learn or they prefer to control their passwords themselves. For instance, P2 said it would be time-consuming for her to figure out how password managers work. P10 thought password managers are cumbersome. He would use a password manager only for storing but not for generating passwords. He added he would want to use a password manager that works across multiple devices. P3 would rather keep control of his passwords himself, saying *"It's like auto-complete. It will fill in and I can't see if it's correct. I prefer to type it."*

Performance and Perceptions of The Password Managers

Overall Preference

When asked about which password manager they preferred and why, seven out of ten participants preferred UniPass for several reasons. Two participants (P7 and P9) preferred LastPass and one participant (P6) was not able to complete any of the tasks. The two participants who did not prefer UniPass were in the group of six participants who had tested Prototype 1 of UniPass in the preliminary user study. Although six out of ten participants had previous experience with UniPass, participants who have never used UniPass before (P1, P4, and P8) were the most enthusiastic about our system. They also preferred UniPass over the other system they tested.

Success Rate

UniPass had the highest success rate (97.3%) of completing tasks (e.g., create accounts, log into accounts), followed by LastPass (83.3%) and StrongPass (68.7%). Specifically, throughout the study, 36 out of 37 tasks were succeeded with UniPass, 15 out of 18 tasks were succeeded with LastPass, and 11 of out 16 tasks were succeeded with StrongPass.

Task Completion Time

In terms of the task completion time, UniPass took the least time, followed by LastPass and StrongPass. Figure 2 presents the median of how long it took participants to complete tasks using the three password managers of all test sessions[1]. We used the median to reduce the impact of outliers in the time measurements. Considering all the tasks (i.e., summing up the median time of tasks), UniPass (368.5 seconds) took approximately 13.9% less time than using LastPass (428 seconds) and 44.5% less time than using StrongPass (664 seconds).

Ease of Use

We now present participants' perceptions of the three password managers. In terms of ease of use, several participants appreciated that they do not need to remember or type their passwords because of the password manager. Some participants liked having passwords on their phone for convenience (StrongPass and UniPass). For instance, P1 talked about the mobility of phones: *"I like UniPass because it is connected to your phone and your phone is with you more than your laptop."* P1 preferred UniPass and mentioned the accessibility of device paring: *"[...] it is connected to your phone and it has an auditory beep so you know when it's connected."* P10 liked UniPass because of the ease of fingerprint scanning. He said *"UniPass. It was quick and sharp. [...] It uses the fingerprint and it works well, it's quick."* However, he was also concerned about switching to another device, saying *"I don't like the idea of the phone being the only brain because if I invest time and energy for the phone to be that device, what happens if I upgrade to another phone? I wouldn't want to reconfigure."*

Perceived Security

In terms of perceived security, participants differed in their choice of password manager. P1 demonstrated more trust in UniPass because it was protected by multiple authentication factors. P1 said *"UniPass offers more security because it uses your phone and your fingerprint so there are more steps to complete."* Similarly, P10 perceived UniPass to be more secure because of the use of fingerprint. P3 thought UniPass to offer more security because the credentials are stored locally on the phone: *"If the password is stored on the phone, UniPass seems more secure than something secured on the cloud."* P2 thought StrongPass to be more secure, citing a similar reason: *"Probably StrongPass because it requires you to log into your phone."* P4 considered both StrongPass and UniPass equally secure by saying *"Passwords are stored in comparable way."* P5 stated that *"UniPass offers enhanced security compared to the normal process because it would connect to the phone not the general network."* These statements confirm Hayashi and Hong's [13] finding that proximity affects perceived security.

[1] P2's times with UniPass for website #3 were not considered because we did not have the video.

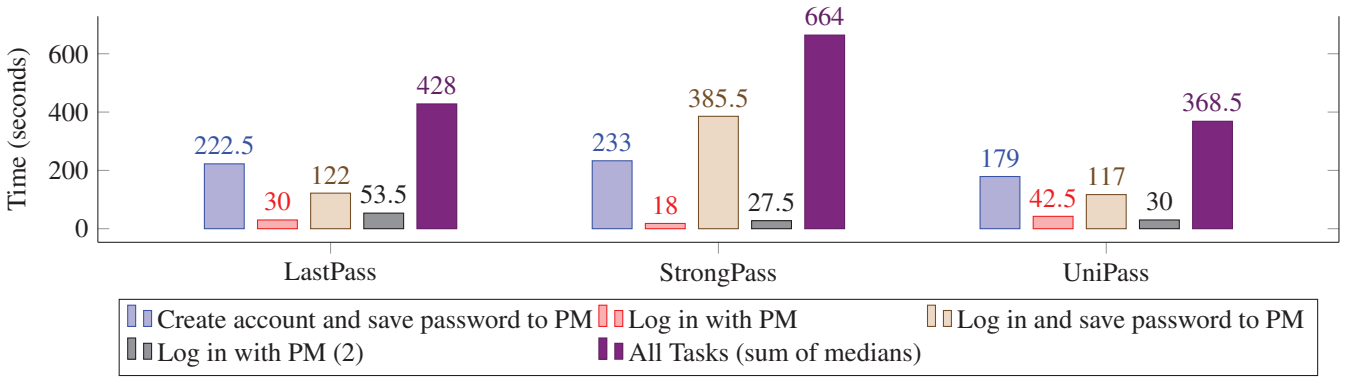


Figure 2: Median time of successfully completed tasks with each password manager. Across all completed tasks, participants took 13.9% less time using UniPass than LastPass and 44.5% less time than StrongPass in completing the tasks.

However, P5 felt phones are not secure and thus preferred LastPass, saying *"LastPass because it is the only device that you are using and not your phone. May be your phone is easier to hack into. If the phone is easier to hack than the website than there might be a backdoor."*

Features for Visually Impaired Users

The accessible features we incorporated into Prototype 2 were well received by our participants. Participants were able to complete the tasks without problems and within the shortest time overall, even when compared to LastPass, where there was only one device to interact with. We observed with the other two systems, participants employed strategies such as repeatedly pressing the TAB key until they found what they were looking for (e.g., "Save site" bar of LastPass), asked for verbal guidance (e.g., how to point the camera more accurately in StrongPass, what to do next in LastPass), or asked us to perform the task on their behalf (e.g., enter the master password in StrongPass, click the QR code button of StrongPass on the address bar). These observations suggest that the compatibility of our system with the users' assistive technology and the design of features targeted at helping visually impaired users helped our participants to have a seamless experience with UniPass. P5 said UniPass is more convenient because *"it involves less manual labor. You don't have to be clicking and punching keys. It takes fewer steps to use the iPhone because you don't have to press keys and press the mouse, if you count the steps you take there are fewer in the iPhone."* P8 was enthusiastic about the learning curve of UniPass, saying *"as a JAWS user it's exciting that you can pick up something really fast"*, referring to UniPass' accessible ease of use with a screen reader that he is familiar with using. P2 said *"[...] for UniPass I don't need to get used to it. It just works."* These comments also suggest these accessibility features of UniPass worked well for visually impaired users.

Why Not UniPass?

Two participants (P7 and P9) tested Prototype 1 of UniPass, but still preferred LastPass mainly because LastPass only needs one device or the participant did not have much experience with smartphones. These two users also preferred not to use a password manager when given a scenario where they would have to log into their email account from a public computer.

P7, an iPhone user, said *"you are using the phone with a computer. I don't think I would be doing that. Maybe if I were using somebody else's computer. I guess I'm a little bit up in the air about UniPass."* P7 added that he would prefer LastPass by saying *"Because I think I understand it a little bit better. It's a little simpler. I find the phone a little complicated. I think I got it right but at least that's my initial reaction."* While P7 preferred LastPass, he commented on UniPass, saying *"I feel it's new. I feel I am going to have to work at it. I have never used a public computer before. Never."* P9 noted *"I like LastPass because it's the first one we tested. I'm not familiar with using an iPhone so it's more challenging for me to use UniPass."* P9 also perceived LastPass to be more convenient, but added *"but if I get comfortable with using an iPhone then UniPass might be easier to use."*

Problems, Comments and Suggestions

Immediately after completing the tasks for each password manager, participants were asked whether they would have any suggestions to improve the password manager.

UniPass

P1 and P2 praised the device pairing feature based on high-frequency audio tones. They found it enjoyable and easy to use. P4 suggested a bigger scanner to read the fingerprint on the phone to simplify the authentication process. This is related to a hardware specification of the iPhone, yet clearly demonstrates how users can have difficulties with biometrics.

Because UniPass implements accessible dialogs, every prompt on the computer was read aloud by screen readers. However, when users did not use a screen reader and instead relied on screen magnification tools, participants experienced difficulties locating the prompts at the top left corner of the page. When screen readers were not used on the phone and on the computer, participants also missed feedback from UniPass, which was designed to work better with screen readers.

Throughout the user tests, we noticed the most difficult part for participants involved opening the UniPass app on the smartphone, particularly for those not familiar with smartphones. For this reason, we changed UniPass to remain open after each password was sent to the computer or stored on the phone, simplifying participants' user experience as they would only need

to open the app the first time. P10 was the only participant to test the system with this change and liked it.

LastPass

P3 said LastPass could improve its accessibility to enable users who rely on screen readers to fully participate. For example, the prompt to remember the password is not instantly detected by the screen reader, requiring users to navigate between the links in order to find the notification bar at the top. P5 echoed a similar sentiment by saying that LastPass should *"put information in a visual part of the screen so that it is easier to locate. I didn't know where the bar was going to come up or the size. It could be larger."*

LastPass' prompt to remember the password was never accessible to the screen reader. All participants had to navigate between the links of the page to find the prompt at the end of the page structure. This was very time consuming for all participants. Moreover, LastPass would take users to a separate screen after choosing "Save Site" to remember their passwords. This was an extra, time-consuming step for participants, who had to navigate the fields and buttons to find the "Save" button.

StrongPass

Many participants found StrongPass difficult or even annoying to use mainly due to its 60-second time limit to scan the QR code. Such time limit would log users out of the app automatically, impeding them from completing the tasks. For instance, P2 said StrongPass *"[...] is too hard for blind people. It is a hassle and I would not use it."* P2 and P8 also could not enter the master password on the phone or enter credentials into the app because of the time limit.

In addition, StrongPass requires users to enter their login credentials into the phone by typing on the touchscreen keyboard. This was a very difficult task for users with visual impairments. P7, a blind user who owns an iPhone said in the pre-tasks questionnaire the most difficult part of using the Internet on his mobile device is typing a password. P10 suggested adding a fingerprint reader feature as an authentication option. In addition, StrongPass' icon on the address bar of the browser was not activated nor readable by the screen reader. The StrongPass user interface on the phone would require users to enter the master password using a touchscreen keyboard with the ABC layout instead of the QWERTY layout. In addition to the different layouts, users were supposed to enter the master password by swipe-connecting the letters, which was inaccessible when the screen reader was on. There were cases in which participants gave up and the researchers had to enter the master password, scan the QR code or enter credentials on the phone. These cases were considered failed attempts and thus not considered in the results of task completion time.

Comparative Subjective Ratings of Password Managers

When analyzing the data from the post-task survey, we discovered mixed results with different top performing password managers in each group. We calculated the mean and standard deviation of answers to all questions in each category. The top performer in Perceived Security was StrongPass (Mean=3.88, SD=1.46), followed by UniPass (Mean=3.72, SD=0.89) and LastPass (Mean=3.70, SD=0.82). We suspect this could be due to the difficulty most users had when trying to unlock StrongPass due to the time limit. The highest rated system in Comfort Level with Giving Control of Passwords to a Program was also StrongPass (Mean=2.83, SD=1.27), followed by UniPass (Mean=2.63, SD=1.15), and LastPass (Mean=2.0, SD=0.85). The ratings in this category further support our reasoning about perceived security of StrongPass since most users were not able to get into the system. The ratings in Perceived Ease of Use were highest for UniPass (Mean=3.95, SD=1.27), followed by LastPass (Mean=3.70, SD=0.82) and StrongPass (Mean=3.38, SD=0.92), suggesting the UniPass accessibility features could contribute to the ease of use for visually impaired users. UniPass was also rated highest in Perceived Necessity and Acceptance (Mean=4.08, SD=1.48), followed by LastPass (Mean=3.57, SD=1.22) and StrongPass (Mean=3.17, SD=1.17). Finally, the highest scores in Perceived Accessibility were given to LastPass (Mean=4.40, SD=0.70), followed by UniPass (Mean=4.22, SD=0.65) and StrongPass (Mean=3.50, SD=1.07). We suspect LastPass was rated highest in Perceived Accessibility due to the fact that its process does not involve the added complexity of a second device (i.e. the smartphone), and because users never had to enter the master password.

Mental Models

We found most users (eight out of ten) were able to reasonably describe how to use each password manager when given the scenario of logging into their email on a public computer. However, for LastPass, participants could not describe how it works precisely or they did not have a good understanding about where their passwords were stored. For StrongPass and UniPass, participants generally understood their passwords were stored locally in their devices. Compared to StrongPass, participants more accurately described the required steps and the order of the steps in UniPass. We attribute the more accurate mental model of UniPass in part to informative and accessible prompts such as "password encrypted and saved on your phone," "password successfully received from phone," and "do you want to log in with your phone?"

While most users were able to reasonably understand the process for each password manager, five out of ten participants thought creating a new online account was a requirement of the password managers. Even though we included a task to migrate an existing account to a password manager, this was the common understanding among the users. We suspect this was because users were asked to create an account for two out of the three websites tested for each password manager, causing them to think creating an account as a system requirement.

Acceptance of Password Managers and Suggestions

After completing the test with each password manager, users were given a scenario where they would need to use a public library computer to reply to an urgent email. They were asked whether they would use the password manager or would prefer to enter the password manually on the public computer when logging into the email service. Three out of five who tested LastPass chose to use the system over manual entry. Two out of four users who tested StrongPass preferred using StrongPass over manual entry. Eight out of nine users who tested UniPass chose to use the system.

By the end of the study, users were asked to rate on a 1-5 scale whether participating in the study had changed their eagerness to start using password managers and to explain why. The average rating given by the participants for this question was 4.44 and the median was 4. P1 said *"I would consider it because it would be an easier way to do it but I would be nervous to do it on my own without training first."* P2 mentioned a hacking incident where she thought stronger passwords and a password manager would have protected her. P3 said that although he would be keen to using password managers, *"the systems could be unreliable and possibly cumbersome to set up."* P4 said she would be very eager to use password managers now because she did not know about them before and she found them to be *"wonderful."* P8 said participating in the study with the password manager had motivated him to start using a smartphone. P10 said the study has made him *"reconsider based on how well UniPass worked with the iPhone fingerprint reader."* We believe our participants' reported eagerness to start using a password manager is an indication that password managers are a promising approach for visually impaired users.

When asked whether they had any suggestions for password managers in general, participants complained about the time limits of StrongPass. The success rate for tasks with StrongPass was greatly affected by the time limit imposed by the system. P1 suggested making the systems easier to learn by suggesting that *"they could have more tutorials."* P5 suggested password managers to make prompts and messages more evident in order for users of screen magnifiers to easily locate them. Finally, P10 suggested password managers should be integrated into the browser with the goal of them being available on more computers.

DISCUSSION

Our results suggest that password managers are a promising authentication approach for users with visual impairments. Our participants also preferred UniPass. UniPass and StrongPass are more complex whereas they require a second device to participate in the process of logging into a website, compared to LastPass, which does not need this second device. This may explain why users rated LastPass higher in Perceived Accessibility. In addition, participants never had to enter their LastPass master password because we configured the browser extension on their behalf.

Even though UniPass requires dealing with the smartphone and the computer at the same time, on average users performed the authentication tasks faster with UniPass than with the other password managers, suggesting that the accessible features in UniPass helped users cope with the more complex workflow as compared to LastPass, which simply fills in the login form automatically when the page is loaded.

We also learned from the study about the perceptions of users with visual impairments toward password managers. Based on the feedback from the users who tested UniPass for the first time in this study, we believe a minimalistic approach to designing password managers can help users learn and understand password managers. We also believe more informative prompts and messages throughout the process help users construe a correct mental model of the system. Users with visual impairments may not be able to fully take advantage of password managers if they impose time limits to complete tasks. Our participants also enjoyed the alternative to device-pairing offered in UniPass via high-frequency audio tones.

We also found choosing to implement other authentication factors (e.g., biometrics) over implementing a master password into a password manager contributed to increased perceived security. Users verbally expressed their preference for UniPass as a more secure system because the system was based on the smartphone and because the system used the fingerprint sensor to share the login information with the computer.

Because we left the set-up task out of the study, we suspect most users did not realize the security and usability implications of typing the master password for LastPass on a public library computer in the email scenario.

We believe users were able to more accurately construe mental models of UniPass and StrongPass due to the fact that the login credentials were being transferred from one device to another. The process of LastPass was more abstract to users since it was not clear how their credentials were being managed.

We also observed a point of conflict where the presence of visual elements (e.g., buttons and graphics) would hinder the experience of users who are blind while improving the experience of those with low vision. We had to carefully change the user interface as to not add clutter and distractions for users who rely on screen reader software while providing enough visual clues for those with low vision who use screen magnification and other assistive technologies. This resulted in changes such as adding audio feedback throughout the workflow, making dialogs appear close to the mouse pointer in order for users zooming in to a specific part of the screen to not have to look for prompts on the top of the screen, and adding subtle graphics to help users who do not use screen readers know what to do and expect.

Our work sheds light on how password managers could be more accessible and appealing to visually impaired users. Our user interface design focused on accessibility greatly helped participants learn and understand UniPass. We also observed participants found a password manager to be more secure when it combined the possession of the phone with biometrics (e.g., fingerprint scanning in UniPass). It was evident in our evaluation participants preferred to enter passwords on the computer instead of on the smartphone's touch screen. Furthermore, when authentication to the phone relied on a visual task (e.g., swipe-connecting letters and numbers in StrongPass), it was nearly impossible for participants to complete the task due to conflicts with the screen reader. The features in UniPass designed for both blind users and users with low vision were well received, contributing to better performance and highest overall preference. The only feature not used was opening the app via voice command. The cases where participants had difficulties using our system were either because they had no prior experience with a smartphone (P9) or found it hard to deal with the computer and the phone at the same time (P7).

When comparing our system to prior work [3, 13, 20], UniPass differs in its accessibility focus and few software and hardware assumptions (thus better deployability). UniPass takes a minimalistic approach to password managers, including only the steps necessary to log in. We also note that our system makes fewer assumptions about software installed on the computer, leveraging as much as possible of the Web APIs available on modern browsers. For example, instead of installing software on the computer, our system can be supported by either a browser extension, a bookmarklet or a JavaScript library. In addition, our system does not rely on a dual-possession approach as seen in Tapas [20], thus entrusting the authentication task only to a single, personal smart device.

Study and System Limitations

Due to the practical difficulty in recruiting users with visual impairments in our geographic area, we recruited six participants who had tested an earlier version of UniPass during the summer of 2015. This prior experience with UniPass could give this particular password manager some advantage in the user evaluation. To mitigate this prior experience, we provided two training tasks for all three password managers before participants conducted the actual testing tasks. Upon completing the training tasks, all participants expressed confidence in their familiarity with the password managers before jumping into the actual tasks. Therefore, we are reasonably confident participants had comparable experiences with all three password managers before the actual testing. Four participants who tested UniPass for the first time were also positive about their user experiences. While we did not tell our participants which system is ours to avoid potential social desirability bias (e.g., participants only say good things about our system to avoid confrontation), these six participants probably knew we designed UniPass, even though it was named differently in the 2015 tests. Nonetheless, the two studies were about one year apart and Prototype 2 of UniPass had significantly changed from Prototype 1, thus the learning effect should be limited. Testing both versions of UniPass could give it advantages, however, five out of these six participants still provided constructive criticism about UniPass.

The study was designed to randomize the order of password managers in each session, but due to a mis-communication within our team, UniPass was always tested the second. This could give UniPass advantages or disadvantages. For instance, one participant said he liked LastPass because it was the first password manager he tested.

We did not include the set-up of the password managers as part of the study because this would be quite time-consuming for the participants. We chose to focus on testing the actual usage of password managers. The entire testing session took about two hours for participants to test two password managers, which is already quite long and tiring for participants. Nevertheless, we plan to include this step when conducting a summative evaluation of UniPass.

Our study used fictitious websites and participants knew this. They were also observed by researchers when using these password managers, therefore the testing environment is not same as their natural environment, limiting the ecological validity of the results. However, given the formative nature of the study, the close observation and think aloud protocol are desirable because they allowed us to understand participants' mental models and challenges in using password managers. These insights are valuable in understanding these users but also in informing future designs of password managers.

While usability/accessibility is our top priority, security is equally important. We have performed a preliminary security/threat analysis of UniPass but do not present the detailed results here due to limited space. A common security technique is to derive an encryption key from the master password and/or other user information and use this key to protect sensitive user information [18]. UniPass currently has a limitation because the system does not involve using master passwords. However, we argue that a master key for each user or session could be derived from data used for authentication (e.g., from smartphone sensors) as well as from the one-time text token generated for each session, or a combination of both. Several studies have evaluated the security of password managers by exposing vulnerabilities and making security recommendations [18, 22, 25]. We plan to further evaluate the security of UniPass using these recommendations.

CONCLUSION AND FUTURE WORK

We designed UniPass, a smart-device based password manager for visually impaired users. We tested UniPass with visually impaired users alongside LastPass and StrongPass in order to understand how these users perceive and receive the different password managers as well as their preference among these password managers. Our results show that participants using UniPass took the shortest time to log in, and the majority of our participants preferred UniPass over LastPass and StrongPass. More generally, our results suggest that password managers are a promising approach to web authentication for visually impaired users. To improve UniPass, we plan to support other authentication related tasks such as logging out and changing/resetting passwords. Future research can also explore other sensors on smartphones as well as behavioral biometrics, providing multiple authentication options to smartphones to address the different user needs [9] and enabling continuous and passive authentication [8, 14].

ACKNOWLEDGEMENTS

The contents of this paper were developed under a grant from the National Institute on Disability, Independent Living, and Rehabilitation Research (NIDILRR grant number 90DP0061-01-00). We thank our participants for sharing their insights. We also acknowledge Sarah Folger, Xiao Li, Piranut Lapprathana, Pritesh Desai, Saurabh Patel, Yun Huang and others in the Social Computing Systems (SALT) Lab at Syracuse University as well as Jeffrey Bigham, Amy Hurst, Aaron Steinfeld, and anonymous reviewers for their feedback and help.

REFERENCES

1. Authomate. 2016. StrongPass. http://x.authomate.com/StrongPass/signup.html. (2016). Feb. 23, 2016.
2. 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)*. ACM, New York, NY, USA, 159–166. DOI: http://dx.doi.org/10.1145/2384916.2384945

3. Nata M. Barbosa. 2014. Strategies: An Inclusive Authentication Framework. In *Proceedings of the 16th International ACM SIGACCESS Conference on Computers & Accessibility (ASSETS '14)*. ACM, New York, NY, USA, 335–336. DOI: http://dx.doi.org/10.1145/2661334.2661413
4. Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. 2012. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In *Proceedings of the 2012 IEEE Symposium on Security and Privacy (SP '12)*. IEEE Computer Society, Washington, DC, USA, 553–567. DOI:http://dx.doi.org/10.1109/SP.2012.44
5. Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. 2015. Passwords and the Evolution of Imperfect Authentication. *Commun. ACM* 58, 7 (June 2015), 78–87. DOI:http://dx.doi.org/10.1145/2699390
6. Yevgen Borodin, Jeffrey P. Bigham, Glenn Dausch, and I. V. Ramakrishnan. 2010. More Than Meets the Eye: A Survey of Screen-reader Browsing Strategies. In *Proceedings of the 2010 International Cross Disciplinary Conference on Web Accessibility (W4A) (W4A '10)*. ACM, New York, NY, USA, 13:1–13:10. DOI: http://dx.doi.org/10.1145/1805986.1806005
7. Sonia Chiasson, P. C. van Oorschot, and Robert Biddle. 2006. A Usability Study and Critique of Two Password Managers. In *Proceedings of the 15th Conference on USENIX Security Symposium - Volume 15 (USENIX-SS'06)*. USENIX Association, Berkeley, CA, USA, Article 1. http://dl.acm.org/citation.cfm?id=1267336.1267337
8. Alexander De Luca, Alina Hang, Frederik Brudy, Christian Lindner, and Heinrich Hussmann. 2012. Touch Me Once and I Know It's You!: Implicit Authentication Based on Touch Screen Patterns. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '12)*. ACM, New York, NY, USA, 987–996. DOI:http://dx.doi.org/10.1145/2207676.2208544
9. Alexander De Luca and Janne Lindqvist. 2015. Is secure and usable smartphone authentication asking too much? *Computer* 48, 5 (May 2015), 64–68. DOI: http://dx.doi.org/doi:10.1109/MC.2015.134
10. Bryan Dosono, Jordan Hayes, and Yang Wang. 2015. "I'm Stuck!": A Contextual Inquiry of People with Visual Impairments in Authentication. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, Ottawa, 151–168. https://www.usenix.org/conference/soups2015/proceedings/presentation/dosono
11. Maarten Everts, Jaap-Henk Hoepman, and Johanneke Siljee. 2013. UbiKiMa: Ubiquitous Authentication Using a Smartphone, Migrating from Passwords to Strong Cryptography. In *Proceedings of the 2013 ACM Workshop on Digital Identity Management (DIM '13)*. ACM, New York, NY, USA, 19–24. DOI: http://dx.doi.org/10.1145/2517881.2517885
12. Shirley Gaw and Edward W. Felten. 2006. Password Management Strategies for Online Accounts. In *Proceedings of the Second Symposium on Usable Privacy and Security (SOUPS '06)*. ACM, New York, NY, USA, 44–55. DOI:http://dx.doi.org/10.1145/1143120.1143127
13. Eiji Hayashi and Jason I. Hong. 2015. Knock x Knock: The Design and Evaluation of a Unified Authentication Management System. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '15)*. ACM, New York, NY, USA, 379–389. DOI: http://dx.doi.org/10.1145/2750858.2804279
14. Markus Jakobsson, Elaine Shi, Philippe Golle, and Richard Chow. 2009. Implicit Authentication for Mobile Devices. In *Proceedings of the 4th USENIX Conference on Hot Topics in Security (HotSec'09)*. USENIX Association, Berkeley, CA, USA, 9–9. http://dl.acm.org/citation.cfm?id=1855628.1855637
15. Ambarish Karole, Nitesh Saxena, and Nicolas Christin. 2011. A Comparative Usability Evaluation of Traditional Password Managers. In *Proceedings of the 13th International Conference on Information Security and Cryptology (ICISC'10)*. Springer-Verlag, Berlin, Heidelberg, 233–251. http://dl.acm.org/citation.cfm?id=2041036.2041056
16. Patrick Langdon, John Clarkson, and Peter Robinson. 2008. Investigating the security-related challenges of blind users on the Web. In *Designing Inclusive Futures*, Patrick Langdon, John Clarkson, and Peter Robinson (Eds.). Springer, Cambridge, UK, Chapter 13, 129–138.
17. LastPass. 2016. LastPass. http://lastpass.com/. (2016). Feb. 23, 2016.
18. Zhiwei Li, Warren He, Devdatta Akhawe, and Dawn Song. 2014. The Emperor's New Password Manager: Security Analysis of Web-based Password Managers. In *Proceedings of the 23rd USENIX Conference on Security Symposium (SEC'14)*. Berkeley, CA, USA, 465–479. http://dl.acm.org/citation.cfm?id=2671225.2671255
19. Daniel McCarney. 2013. *Password Managers: Comparative Evaluation, Design, Implementation and Empirical Analysis*. Master's thesis. Carleton University, Ottawa, ON, Canada.
20. Daniel McCarney, David Barrera, Jeremy Clark, Sonia Chiasson, and Paul C. van Oorschot. 2012. Tapas: Design, Implementation, and Usability Evaluation of a Password Manager. In *Proceedings of the 28th Annual Computer Security Applications Conference (ACSAC '12)*. ACM, New York, NY, USA, 89–98. DOI: http://dx.doi.org/10.1145/2420950.2420964

21. Emma Murphy, Ravi Kuber, Graham McAllister, Philip Strain, and Wai Yu. 2008. An Empirical Investigation into the Difficulties Experienced by Visually Impaired Internet Users. *Univers. Access Inf. Soc.* 7, 1 (March 2008), 79–91. DOI: http://dx.doi.org/10.1007/s10209-007-0098-4

22. David Silver, Suman Jana, Dan Boneh, Eric Chen, and Collin Jackson. 2014. Password Managers: Attacks and Defenses. In *Proceedings of the 23rd USENIX Conference on Security Symposium (SEC'14)*. USENIX Association, Berkeley, CA, USA, 449–464. http://dl.acm.org/citation.cfm?id=2671225.2671254

23. Boris Smus. 2016. Ultrasonic Networking. https://github.com/borismus/sonicnet.js. (2016). Mar. 30, 2016.

24. Jacob O. Wobbrock, Shaun K. Kane, Krzysztof Z. Gajos, Susumu Harada, and Jon Froehlich. 2011. Ability-Based Design: Concept, Principles and Examples. *ACM Trans. Access. Comput.* 3, 3, Article 9 (April 2011), 27 pages. DOI:http://dx.doi.org/10.1145/1952383.1952384

25. Rui Zhao and Chuan Yue. 2013. All Your Browser-saved Passwords Could Belong to Us: A Security Analysis and a Cloud-based New Design. In *Proceedings of the Third ACM Conference on Data and Application Security and Privacy (CODASPY '13)*. ACM, New York, NY, USA, 333–340. DOI: http://dx.doi.org/10.1145/2435349.2435397