Pico in the Wild: Replacing Passwords, One Site at a Time

Seb Aebischer*, Claudio Dettoni*, Graeme Jenkinson*, Kat Krol*,
David Llewellyn-Jones*, Toshiyuki Masui† and Frank Stajano* ‡
*Computer Laboratory, University of Cambridge
Email: firstname.lastname@cl.cam.ac.uk
†Faculty of Environment and Information Studies, Keio University
Email: masui@masui.org

***Abstract*—Passwords are a burden on the user, especially nowadays with an increasing number of accounts and a proliferation of different devices. Pico is a token-based login method that does not ask users to remember any secrets, nor require keyboard entry of one-time passwords. We wish to evaluate its claim of being simultaneously more usable and more secure than passwords, whilst testing its support for frictionless deployment to web-based services. Our main aim is to collect actionable intelligence on how to improve it. In our study, we teamed up with an Alexa Top 500 website, Gyazo, to offer this alternative login mechanism to users intent on performing a real task of image sharing. We focused on the ecological validity of the trial, and gained knowledge both through the challenges of the trial and the results generated. Users appreciated the ability to avoid password entry but the overall benefit was mitigated by the existing measures put in place by Gyazo to minimise the number of times users are presented with a password entry box. Our main finding is that providing enough benefit requires a solution that applies across sites, rather than focusing on authentication for a single site in isolation.**

I. Introduction

Nowadays, users are asked to create passwords everywhere they go, which poses a significant cognitive and physical burden. Creating and memorising a unique and strong password for every service is an impossible undertaking [1]. In this situation, users resort to different kinds of strategies ranging from writing passwords down through reusing the same password for multiple accounts to employing a password manager (*e.g.*, [2]). Not only are passwords a burden on memory, but also the physical effort of password entry can cause disruption leading to frustration and distraction from users' actual work. Users' coping strategies make the pain of passwords more bearable but have been shown to lead to an authentication fatigue over time [3]. At the same time, even if the user manages to create and memorise a strong password, there is no guarantee that their accounts and accesses will stay secure. Almost every month, we hear about high-profile password breaches [4] and learn about companies' poor password storage practices [5].

In this paper, we present the findings of a user study conducted to evaluate a token-based password replacement solution called *Pico*. Faced with the significant usability and security shortcomings of passwords, Stajano [6] proposed Pico as an alternative authentication scheme. In the implementation we studied, Pico is a smartphone application that performs authentication to a website, replacing the need for the user to enter a username or password. The website displays a QR code on its login page alongside the usual text entry fields. Rather than typing into the fields, the user can instead open the Pico app and use it to scan the QR code. A few seconds later, the user is authenticated and the website automatically refreshes to show that the user is logged in.

This interaction has the potential to reduce the cognitive and physical burden of password creation, memorisation or storage and entry. Pico would also make credentials more resilient to security breaches – with Pico, even if the credentials file is stolen, the credentials are of limited value and so the users do not need to change them, and the damage to the company's reputation is limited.

We conducted a three-part user study exploring the usability, deployability and perceived security of Pico when used for authentication to a real-world image-sharing service called Gyazo[1]. We carefully targeted the groups of users who would find Pico most useful and asked them to use Pico to log in to Gyazo for a period of two weeks. We collected participant feedback and produced a rich set of quantitative and qualitative data including telemetry, ratings, free-text responses and interviews.

The main contributions of this paper are as follows. We conducted the first user study of fully-functional Pico for login to a real-world service. We collected quantitative and qualitative data in a three-stage user study exploring the usability, deployability and perceived security of a token-based solution. Our study also highlights the challenges associated with conducting an authentication user study "in the wild" and we share some lessons that we learned.

‡All authors contributed equally, author listing alphabetical

EuroUSEC '17, 29 April 2017, Paris, France

http://dx.doi.org/10.14722/eurousec.2017.23017

[1] https://gyazo.com/

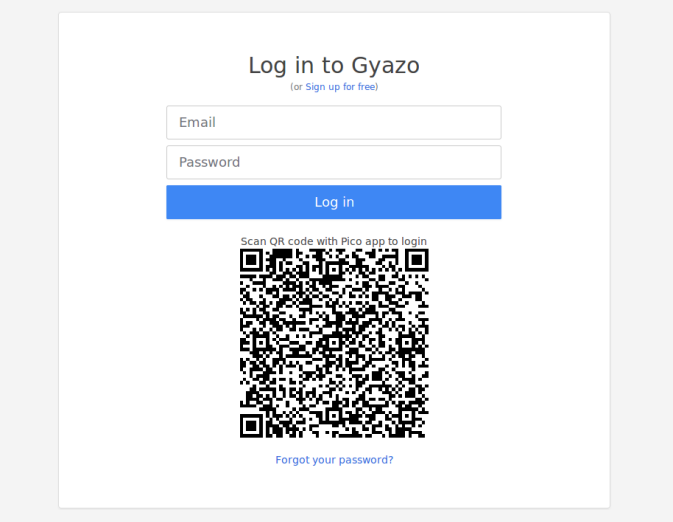

Fig. 1. The Gyazo login screen with a Pico QR code.

II. Background

Gyazo, an Alexa Top 500 website, is an image capture and sharing website that offers two modes of operation. Users can either capture a portion of their desktop as a screenshot using an application installed on their computer, or upload images captured through other means directly to the site. The website interface then allows images to be organised, tagged and shared with others, but Gyazo has focused particularly on providing a frictionless workflow for capturing partial screenshots. The user simply launches the application, at which point they can drag a bounding box over the screen to capture an image. The interface is minimal: the mouse cursor switches to a crosshair design and once the drag is complete the image is automatically uploaded and displayed in the browser. The authentication process is subtle. The Gyazo application stores a non-expiring identity token that it uses to authenticate when uploading an image. This is stored in the user's home folder so that images can be uploaded without any further credentials being needed from the user. While this token allows images to be uploaded, it does not allow any deeper web access to the user's account. For this, the user must log in manually using username and password. The gyazo.com website also uses browser cookies to maintain a login session, which expire after one month.

Our Pico implementation does not affect image upload and the identity token, but rather focuses on access to the website. As shown in Figure 1, Pico adds a QR code to the login page that a user scans with their smartphone. The user loads up the Pico app on their phone, scans the QR code and is then presently logged in to the site. Pico uses the data in the QR code to trigger a background authentication, and from the user's perspective the site refreshes and moves from the login page to their account dashboard.

III. Related Work

The literature identifying systemic problems with passwords as an authentication mechanism is well-known and goes back decades [7], but the quest to replace them has turned out to be a war of attrition. Over the years, numerous password replacement schemes have been proposed and tested, each with benefits that turned out to be too niche to achieve widespread adoption.

Biddle *et al.* [8] survey research into graphical passwords as a replacement for textual passwords. They conclude that studies lack consistency, often failing to achieve rigorous evaluation of security or usability. The evaluation checklist they provide for addressing these failings identifies user studies and ecological validity as an important factor.

The majority of studies evaluating authentication mechanisms have been laboratory-based trials. The mechanisms studied include graphical passwords [8], Passfaces [9] and grids (*e.g.* [10], [11]) to name a few. In reality, security-related actions are secondary tasks and a study has to mimic this set-up. Although researchers have been calling for robust authentication studies for a long time now [12], many studies still rely on simulated interactions in artificial set-ups [13], failing to consider how authentication fits in with users' daily activities. If the interactions and logins are not real, the validity of the studies is limited [14].

While in-the-wild studies have been conducted for other security interactions such as warnings [15], testing authentication mechanisms in the wild is rare. A notable exception is the work by Brostoff and Sasse [16] who studied Passfaces in a three-month field trial with 34 students. The students had to use Passfaces and passwords to access their course materials. The authors found that when using Passfaces participants logged in with a third of the frequency of logging in with passwords since the login process was more time-consuming. Participants also stayed logged in for longer when using Passfaces.

In recent years, several studies have been conducted to assess the user experience of token-based credentials. Most of them looked at technologies that used a token as part of a two-factor authentication solution. Strouble *et al.* [17] studied the introduction of the Common Access Card (CAC) to the US Department of Defense (DoD). The CAC is a smart card and photo ID, which DoD employees use for both opening doors and logging in to computers. The introduction of the CAC significantly impacted organisational productivity: employees reported that the increased difficulty of accessing their emails led them to log in less often when outside their primary workplace. Also, over two thirds of employees inadvertently left their CAC in the computer. The authors estimated this resulted in a productivity loss of $10.4m. Similarly, Steves *et al.* [18] studied authentication in a large US governmental organisation. They found that employees disliked using RSA's SecurID and the elaborate login procedure discouraged them from logging in remotely. Krol *et al.* [19] studied the user experience of authentication tokens for UK online banking. They found that the need to have a hardware token was a source of inconvenience and it changed the way participants went about doing banking, decreasing the frequency of login. Participants reported being less satisfied with online banking when more steps were required for the login process and if they had to use a hardware token. UK banks have since been shifting from physical to software tokens to relieve their customers of the burden of carrying an additional device for generating a one-time password.

Payne *et al.* [20] conducted a study using prototypes of Pico created using plasticine and Polymorph. The researchers

found that although having a physical authentication token gave participants a feeling of tangible security, it also caused anxiety as they felt it would make them more responsible for their security. The usability problems of authentication tokens identified by prior research and the results from the study by Payne *et al.* [20] motivated the shift from Pico being a dedicated authentication device to it being a smartphone application. This reflects the shift in the industry from physical to software tokens as can be seen for RSA and online banking in the UK. Hence, the Pico project focused on developing a smartphone application, an implementation of which we test in this paper.

Bonneau *et al.* [21] identified three overarching benefits that an authentication mechanism should provide: usability, deployability and security. In this study, we assess Pico's usability, deployability and perceived security. The original idea of Pico was proposed by Stajano [6] in 2011. The work has generated many technical results (*e.g.* see Goldberg *et al.*, Stajano *et al.* and others [22], [23]), but only one user study has previously been conducted and published on non-functional Pico prototypes [20]. Some recent work by Urueña and Soto [24] has sought to empirically assess login times, but currently the work is in its early stages. Analysis of the empirical usability of a single-factor token-based password replacement that is *Memorywise-Effortless* and *Physically-Effortless* (in the jargon of Bonneau *et al.* [21]) remains an important gap that we aim to fill.

IV. Methodology

As described in Section III, many studies in the field have suffered from methodological shortcomings. To increase ecological validity, we established a collaboration with a real-life service – Gyazo – and asked users of this service to use Pico. We conducted a multi-stage study to learn about the user experience of Pico. We invited those Gyazo users who logged in with high frequency.

A. Study stages

1) Identifying potential participants: In the first stage, we requested that Gyazo identify a usergroup that logs in with high frequency, which was operationalised as at least once during the past week (note here that this is the number of times the users entered their passwords to log in, not the number of times they visited the site). This amounted to 1136 users. An email was sent out to all these Gyazo users inviting them to complete an initial questionnaire.

2) Initial questionnaire: The purpose of the questionnaire was to investigate the reasons why the users logged in with high frequency and to check whether Pico would fit into their authentication routines. For example, we assumed Pico would be of little use to those who had their Gyazo password automatically entered for them by the browser or a password manager. The questionnaire can be found in Appendix B. We first asked about demographics (gender, age range), then about their Gyazo login habits and general login behaviour. Finally, we asked them for their phone OS, as Pico was only available for Android, and their Google Play email address in order to add them as beta testers.

3) Use of Pico for Gyazo: Overall, 29 participants met our criteria, and we sent all of them an invitation email describing the study and outlining the next steps. They were asked to download the Pico Gyazo app and use it to log in to their Gyazo account for the duration of the trial, which was set to two weeks. Eleven went on to install the app and use it with their Gyazo account.

4) Exit questionnaire: Two weeks after the installation of the app, we sent each participant a link to the exit questionnaire via email. The exit questionnaire consisted of seven questions. (1) Participants were asked in how far they agreed or disagreed with eleven statements about the user experience of Pico. (2) They were asked to state how they would lock their phone if all their passwords were stored on it. (3) They were provided with a list of eight changes that could be made to Pico and asked to rank them in terms of their usefulness. (4) They were provided with a list of different real-life contexts and asked to indicate if they would be more comfortable authenticating with Pico, passwords or both in each context. (5) They were asked if they had any suggestions for improving Pico. (6) They were asked if they would continue using Pico. Finally, (7) they were asked if they had any thoughts they wanted to share about Pico and/or passwords. At the end of the survey, they were asked in what currency they would like to receive the incentive which was equivalent to £10.

5) Feedback interviews: All participants who completed the exit questionnaire were invited to take part in a feedback interview. Seven participants indicated their willingness to be interviewed and we were able to arrange interviews with five. One was conducted over landline, four over Skype. The interviews were semi-structured, with the sequence in which the questions were asked following the natural development of the conversation. Appendix D shows the list of questions that we used for one of our participants. While there was a basic set of questions that we asked every interviewee, we also tailored these to their questionnaire responses as far as possible.

B. Participants

We received 85 complete responses to the initial questionnaire; 69 respondents indicated they were male, twelve that they were female and four chose the option "Other/prefer not to say". Their ages fell into the following ranges: 18–24 years – 56 respondents, 25–34 – 18, 35–44 – 7, 45–54 – 2, and 55–64 – 2. They were based in 25 countries as follows: United States (26 respondents), Japan (13), United Kingdom (12), Canada (7), Russia (3), Israel (2), Lebanon (2), Netherlands (2), Norway (2), Bangladesh (1), Brazil (1), Colombia (1), Czech Republic (1), Estonia (1), France (1), Germany (1), Greece (1), Italy (1), Latvia (1), Portugal (1), Romania (1), Spain (1), Sweden (1), Taiwan (1) and Vietnam (1).

The final sample of participants who downloaded and used the Pico Gyazo app consisted of eleven individuals. One was female, eight were male, while two preferred not to disclose their gender. Their ages fell into the following ranges: 18–24 years – 9 participants, 25–34 – 2. Participants were resident in six countries: United States (6), Brazil (1), Greece (1), Japan (1), Latvia (1) and Spain (1).

We interviewed five participants; two male, one female and two who selected the option "Other/prefer not to say". Their

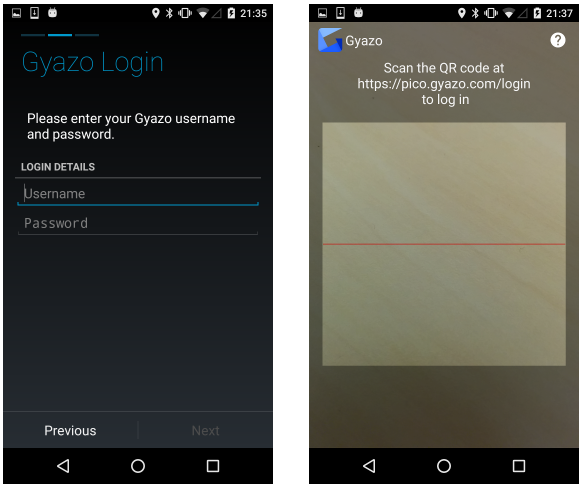

Fig. 2. The configuration screen (left) and scanner interface (right).

ages fell into the following ranges: 18–24 years – 4 participants, 25–34 – 1. Four participants were based in the United States (Illinois, Mississippi, New York and Oklahoma) and one in Latvia.

C. Apparatus

Participants were invited to install the Pico Gyazo app on their Android phones via Google Play, a 4.16 MB download. The first time the user opens the app, they are invited to enter their Gyazo account details (username, password) as shown in Figure 2. These are stored by the application to allow the app to perform the automatic login on future occasions. The user is then presented with a QR code scanner as shown in Figure 2. From this point on, until the user clears the app data (which only one of the users did during the trial), opening the app will bring the user directly to the scanner page. The interface is simple and consists of just this one screen.

The app represents the software needed on the client-side for Pico authentication. Since we did not have direct access to the backend server code, we developed a reverse proxy for overlaying the Pico interface onto the Gyazo site. With permission from Gyazo, we had the pico.gyazo.com subdomain redirected to our own nginx[2] reverse proxy relaying the Gyazo website. Users visiting pico.gyazo.com saw the same site as users visiting the gyazo.com website with two exceptions. The main change was to inject a few additional `<script>` HTML elements into the login page. These elements pulled in our own Javascript source that performed some client-side rewriting of the page to inject the dynamic Pico QR code into the login page (the result of which was as shown earlier in Figure 1). The second change was to add a new page that we passed to potential study participants. The page contained a brief description of the study, links through to the study information sheet and a direct link to the initial questionnaire. Since these changes were done with the cooperation of Gyazo, we were able to ensure that the certificate used for the pico.gyazo.com reverse-proxied site was valid (*i.e.* showed as a green padlock in participants' browsers).

[2] https://www.nginx.com/

TABLE I. EVENTS GENERATED BY THE PICO APP

Starting unconfigured	Successful authentication
Starting configured	Checking username and password
Configuration complete	Credentials checked out
Scanned QR code	Incorrect credentials
Scan cancelled by user	Open credentials page
Attempting login	

TABLE II. EVENTS GENERATED BY THE LOGIN PAGE

Page loaded and updated
Error getting new channel
Pico accepted message on Rendezvous channel
Message from Pico authenticated

The Pico process for websites involves the Pico phone app performing the login on behalf of the user. Gyazo returns a cookie to the app, which it then sends on to the client-side Javascript running on the website. This Javascript can then inject the cookie into the browser's cookie store in order to initiate an authenticated session for the user. As part of this process, the app must be able to communicate with the client-side Javascript. The channel of communication is chosen by the Javascript and the channel identifier (a URL) is embedded in the QR code. When the QR code is scanned, the app is able to extract this channel identifier, which can then be used by the app for communication with the Javascript. We use an untrusted external rendezvous point channel for this communication (see our earlier work for details [25]), identified using the unique channel name.

We peppered both the app and proxied site with keen.io[3] calls for collecting event-based telemetry data. These allowed us to measure timings for various stages of the login process, including startup, configuration, QR-scanning and completion. The full set of events is shown in Table I and II for the Pico app and login page respectively.

For the configured phone we were able to form an identifier for the user generated as a salted hash of their Gyazo username, sent with each event. This ensured data was kept anonymised as it passed through keen.io (since publicly the hashes cannot be reversed), but could be de-anonymised by us given our knowledge of the participants' Gyazo usernames. However, events generated for the unconfigured app and for the website had no access to the username. Consequently, we also collected the IP address and the random rendezvous channel identifier described earlier. This allowed us to correlate events even where the user was not immediately identifiable. Not all events could be tied to specific users, for example a portion of the events we received could be traced back to search engine webcrawlers accessing the pico.gyazo.com domain. Analysis of the IP addresses recorded against orphaned events and a process of elimination allowed us to account for all data generated by the participants.

D. Data analysis

Owing to the small sample sizes in our study, we report only on the quantitative results using descriptive rather than inferential statistics.

When it comes to qualitative data, we conducted five in-depth interviews that were audio recorded and later transcribed.

[3] https://keen.io/

TABLE III. SELF-REPORTED FREQUENCIES WITH WHICH RESPONDENTS MANUALLY TYPED IN THEIR PASSWORDS ON GYAZO.COM.

Fewer than once per week	59
Fewer than once per day	8
Roughly once per day	9
Roughly 2-4 times per day	7
Roughly 5 or more times per day	2

The interviews lasted 26 minutes on average (range: 19–36) and the transcripts were on average 3917 words long (range: 3099–5637). The transcripts were analysed using thematic analysis [26] by two researchers as follows. They coded the first interview independently and then created a joint codebook, based on which they coded the remaining four interviews. After this, they merged their codebooks and re-coded all five interviews in line with this codebook. The inter-rater reliability was high with a Cohen's Kappa coefficient of 0.84, which is considered to be excellent [27].

E. Research ethics

The study was conducted after having been approved by the Ethics Committee at the University of Cambridge Computer Laboratory (approval number: 384).

V. RESULTS

A. Initial questionnaire

We contacted 1136 users inviting them to take part and 85 respondents completed the initial questionnaire (out of 268 who followed the invitation and opened it). We asked the respondents how often they manually typed in their Gyazo password. Table III shows the results. Out of 85 respondents, 59 (69.4%) logged in fewer than once per week, 8 (9.4%) fewer than once per day and 9 (10.6%) roughly once per day.

This was followed by an open-ended question asking respondents to explain the main reason why they had to enter their password. Out of 85 respondents, 65 provided an answer to this question. Switching to another device was mentioned in 19 cases; for example, R82 wrote: *"Signing in on a different computer"*. 17 respondents explained they needed to enter a password in order to log in and access their images. Our intention had been to understand why respondents enter their password given the service sets long-lived cookies, and we were therefore surprised by the literal interpretation of the question, suggesting we should have phrased it more carefully. In 15 cases, respondents stressed they had to enter their password after clearing their cookies, R54 explained: *"Because i clear my cache at the end of the day to speed up the browser"*. Seven respondents mentioned having to log in to Gyazo when switching to another browser. Six respondents said their perception was that they were never asked to enter their password. In four cases, the respondents said that they had to enter it if their password manager/browser failed to do it for them; R57 explained: *"SafeInCloud doesn't actually work"*. Three respondents mentioned they entered their password manually because of security reasons; R17 wrote: *"I never use the option in Chrome save password because of that and also I think its safer to type the password everytime."* Interestingly, two respondents also mentioned they logged out intentionally in order to practise their password, as R18 explained: *"To better memorize it"*.

TABLE IV. SELF-REPORTED METHODS IN WHICH RESPONDENTS MANAGED THEIR PASSWORDS. RESPONDENTS COULD CHOOSE ALL THAT APPLIED.

Let my browser remember my password	63
Password manager/plugin/extension (*e.g.* LastPass, 1Password)	19
Password generator	13
Reset password by email when I need to login	14
Password containing personal information	4
Stored in a file/on a piece of paper	10
Using the same password on multiple sites	30
No special methods (I just remember all of my passwords)	17
Other	10

We asked respondents what their password management methods were. They could choose from a list of eight options and/or add their own. Table IV shows the results. The most popular password management strategy was letting the browser remember the password, employed by 74.1% of respondents, followed by 35.3% of respondents who used the same password across multiple sites and 22.4% who used a password manager/plugin/extension.

B. Telemetry results

The Pico app was downloaded by twelve participants but one participant never used it to authenticate. Overall, we recorded 45 authentication events across eleven active participants ($M = 4.1$, range: 1–14).

For each authentication event, our telemetry collected the timings for the following authentication steps: starting the app, loading the Gyazo login page, scanning the QR code, successful authentication and confirmation from the website. An event lasted an average of 47.5 seconds (range: 8–292). Of the 45 authentication events recorded, three were missing telemetry data for some steps and were therefore excluded from subsequent analysis. Out of the remaining 42 fully recorded events, 23 started with the participant opening the Pico app and then opening the page, while 19 started with them loading the page and then opening the app. Table V show the average times and ranges for each of the steps. For the first step, if participants started by opening the app and then went on to open the Gyazo website, it took them on average 35.2 seconds, whereas the other way around it was 33.7. While Steps 1 and 2 were dependent on both the participants' speed and the system response time, steps 3 and 4 depended on the response time of various systems. The Pico protocol involves the usual `POST` request – sent by the Pico to the website – needed to authenticate the user, followed by four messages sent between the Pico and the user's browser (two in each direction) to securely install the cookie. The timings of these last two steps are in line with what we would expect to see.

C. Questionnaire and interview results

In what follows, we report on the findings from questionnaires and interviews. Since both touched upon similar themes, we group the results by theme. When we refer to participants in the questionnaires, we speak of "respondents" abbreviated as "R01" for "Respondent 1". When we refer to participants in the interviews, we speak of "interviewees", abbreviated as "I01".

TABLE V. A BREAK-DOWN OF STEPS NEEDED FOR AN AUTHENTICATION EVENT WITH DURATIONS.

Step no.	Authentication step	Mean time
Step 1	start Pico app – load page or load page – start Pico app	34.55
Step 2	start Pico app – scan QR code	9.62
Step 3	scan QR code – successful authentication	2.40
Step 4	successful authentication – confirmation from website	0.93

D. Primary task – Gyazo

We began each interview by asking the interviewee about their use of Gyazo in order to ground their perceptions of Pico in the primary task of using the service. Two interviewees had been using the service for two years, two for one year and one only signed up a month before the study. All interviewees used it for personal use, and one also used it for professional reasons because they were an artist. Four interviewees stated they were not currently premium users; one stated that they used to be but could not afford it any more. Two mentioned that they used Gyazo on a daily basis.

We asked the interviewees in what situations they had to enter their password. Two stated they had to enter it when they deleted cookies; two said they needed to enter it when they switched or shared devices. Most people stay logged in long-term, and as a result three interviewees reported they had to deliberately log out to use Pico in the trial.

E. Perceptions of Pico

Three interviewees found Pico to be easy to use. Two described it as "fairly quick", and two as convenient. I04 explained: *"I thought it was very effective, it was very quick, very easy, convenient... I definitely, I like the idea versus having to put in the password every time."* I02 explained how the swift login with Pico encouraged them to log in more often: *"I used [Pico] on my college computer a couple of times, and it was just more convenient [...] like I need to show a fellow student an image or something like that, so it was just a lot easier to just pop onto the desktop and scan in, so, slightly more, yeah, than using a password."* Two interviewees also described Pico as "cool".

In the exit questionnaire, we asked the respondents to what extent they agreed with eleven statements about Pico on a five-point Likert scale from strongly agree (1) to strongly disagree (5). The mean and median scores are shown in Figure VI.

Respondents disagreed the strongest with statement 9, that they were concerned about others observing the QR code when they logged in to Gyazo. Participants agreed the strongest with statement 7, that the Pico-Gyazo app was straightforward to download.

The scores for cognitive effort tended to be low with four participants indicating they disagreed strongly with statement 1 (*i.e.* they felt Pico does not require cognitive effort). In the interview, we asked one participant who agreed with the statement (score: 2) to elaborate on their rating. It turned out the participant was unsure about the meaning of the word "cognitive". After an explanation of what it meant, they revised their score saying: *"I don't think there's any [cognitive effort], because you don't really have to remember anything, you just have to unlock, you know, your password on your phone, and it's pretty much you use it daily, so the chances of you forgetting it is pretty much non-existent."* (I03).

F. Familiarity with QR codes

Three participants said they were already familiar with scanning QR codes: I01 had used them with the Nintendo 3DS, I05 as part of the LINE messaging app, and I02 as part of a school project. Two interviewees found QR codes inconvenient due to the fact that scanning them required having their phone at hand. I01 explained: *"I worked with QR codes before so it wasn't too hard to work with. It just seemed a little bit inconvenient. I mean, getting out my phone and, 'cos I don't usually have my phone on me when I'm at the computer, it's usually somewhere else, so I had to bring my phone over and I had to scan the screen."* I03 experienced some problems with scanning a QR code because of a low quality phone camera and monitor, saying: *"the problems were coming I think from my monitor, my old one, I had the really old one, the big one, CRT monitor, which basically, every time I tried to scan it, it was flickering, so it'd make it harder to scan it."*

G. Pico vs passwords

We asked our interviewees to compare Pico to passwords. Two participants found Pico was more convenient, and two found it was faster than passwords. Three interviewees thought that Pico was more secure than passwords. When asked about the security of Pico, I04 said: *"I think I put it as around the same"* but then explained that in its current state, Pico might be more secure because it had not been a target for attackers yet: *"I don't really know what the exact basics are between getting into an account using someone's password, so not exactly sure how someone would hack you using Pico, but I guess technically it would be more safe because the technology isn't out yet, but they'd figure it out eventually, if it becomes a major thing."*

Two interviewees argued that passwords were better because Pico was slower than entering a password. I03 thought that passwords were more secure because they existed only in the user's memory: *"if you have a secure password and you're pretty much the only one person who knows it, I think that's the most secure thing you could possibly have."*

H. Suggestions for improvements

In the exit questionnaire, we provided respondents with a list of eight possible improvements that could be made to Pico and asked them to rank these in order of priority from the most to the least important. Figure 3 shows the results. The improvement ranked first most often referred to introducing login with Pico to more websites than just Gyazo; it was ranked

TABLE VI. STATEMENTS CAPTURING THE VARIOUS ASPECTS OF THE USER EXPERIENCE OF PICO WITH MEAN AND MEDIAN SCORES ON A 1-5 LIKERT SCALE, 1 – STRONGLY AGREE, 5 – STRONGLY DISAGREE.

	Statement	**Mean**	**Median**
1	Using Pico requires cognitive effort.	3.5	3
2	Using Pico requires physical effort.	3.3	3
3	It is easy to learn how to use Pico.	1.4	1
4	Pico makes me more efficient.	2.3	2
5	I am afraid of losing my Pico device and losing access to my account.	3.5	4
6	I find scanning the QR codes reliable.	1.6	1
7	Installation of the Pico-Gyazo app was straightforward.	1.3	1
8	I feel secure using Pico to log in to Gyazo.	1.6	1
9	I am concerned about others observing the QR code when I log in to Gyazo.	4.3	4
10	Using Pico makes me more concerned about my smartphone being stolen.	3.8	4
11	Overall, I find Pico makes my online activity easier.	2.0	2

either first or second by seven out of eleven respondents. The issue that was ranked bottom most often (four times) was removing the need to scan the QR code, although it was also ranked first by two participants.

Apart from the ranking task, respondents were also asked if they had any other suggestions. Four respondents made suggestions related to security – login security and recovery from loss. The login-related suggestions included requiring the user to enter a username as an extra hindrance to potential attackers and requiring two-factor authentication in certain contexts. The suggestions relating to recovery from loss included creating a *"button to disable the Pico app in the website if the phone is lost or stolen"* (R01) and having a fall-back login method if the phone is lost. Otherwise, two respondents stressed they would like to see Pico integrated with more websites. R10 explained: *"Just more websites, this is way more easy to login into websites."* One respondent suggested other modes of logging in apart from scanning a QR code, such as *"timing tap and voice recognition"* (R03).

During the interview, we also asked about suggestions for improvements. Two participants suggested extending the use of Pico to other websites or services. I03 explained: *"let's say from your desktop you just, you have like a, I don't know, a program that you can basically just open and then scan it, but instead of going on the website and trying to log in. I think that'd make it even more handy."* A further two participants suggested replacing scanning the QR code with a different interaction, I02 suggesting use of NFC (Near Field Communication) as they believed NFC would be more secure than a QR code.

Other security-related suggestions included blocking the Pico app remotely, asking for an email address as a username when logging in (mentioned by the same participant as in the questionnaires) and requiring a password when logging in from a new device. Additionally, one participant suggested removing the need of a data connection when using Pico.

I. Phone use habits

We also asked participants about their phone use habits to gauge how Pico fitted into their routine. In the interviews, two interviewees reported using a pattern lock, two using a 4-digit PIN, and one not having a lock at all. Participants provided all kinds of reasons for preferring one method over another. I02 explained: *"I don't particularly care for pattern locks because I have rheumatoid arthritis. So, using my thumbs in that particular way is a bit painful, so for convenience like I don't..."* When asked what they were using instead they told us: *"I have a PIN on it. [...] But, but it's also the PIN to my debit card!"* The interviewee then went on to discuss how they thought fingerprint scanners were the most convenient way of logging in. When asked to compare the security of the different methods of locking their phone, I02 responded: *"I know that they can be compromised, but at the same time I don't necessarily think that affects most users. Most people aren't going to be maliciously attacked and have their fingerprint stolen, but I think in higher security situations that might be a problem. I wouldn't, if I were say a diplomat, or something like that, I don't think I would trust my fingerprint that much you know, but if it's just an average Joe, sure, why not."*

In the exit questionnaire, we asked the respondents what method of locking they would use if all their passwords were stored on their phone. We provided them with six possibilities as shown in Table VII. The most popular options were a pattern lock and a fingerprint scanner with six mentions each, followed by a 6-digit PIN with five. A 4-digit PIN and a password both had three respondents select them. There was also the possibility to enter their own method of locking. One participant mentioned facial recognition, while another suggested no lock at all.

J. Password management strategies

When asked about their current password management strategies, three interviewees said they used password managers and three reused the same passwords for multiple systems.

I05 reflected on the fact that some accounts were more valuable than others as they guarded access to other things, they explained: *"for Google especially, it has to be incredibly secure because you're asking that to then be responsible for everything else; it's like putting your stuff in a safety deposit box in a bank where you don't trust the people running the bank."*

TABLE VII. PREFERRED WAYS TO LOCK PHONE WITH NUMBERS OF PARTICIPANTS WHO CHOSE IT. PARTICIPANTS COULD CHOOSE AS MANY AS THEY WISHED.

4-digit PIN	3
6-digit PIN	5
password	3
pattern lock	6
fingerprint	6
slide lock	1

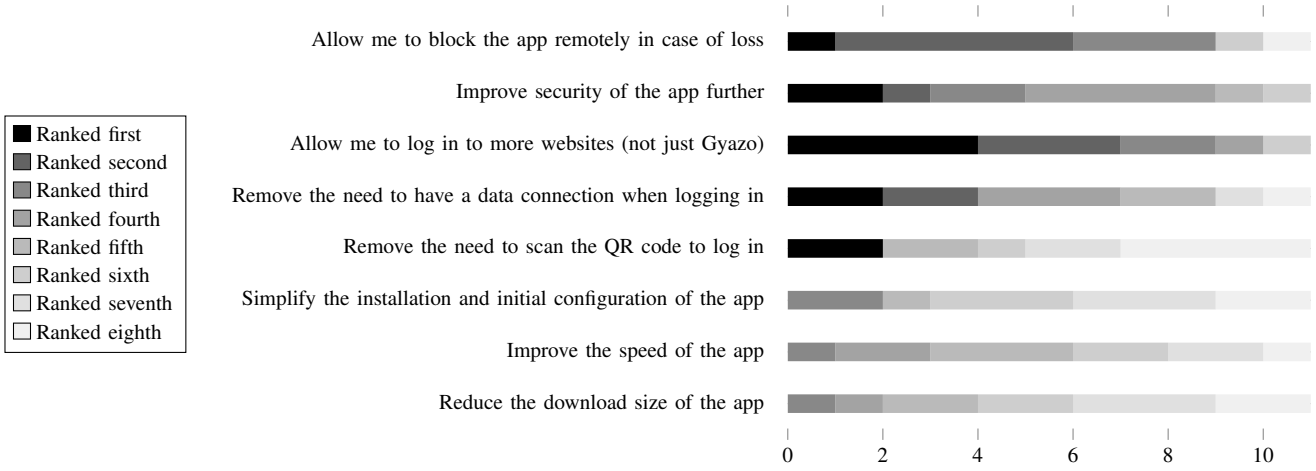

Fig. 3. Participants' ranking of the different improvements that could be made to Pico. The darker the shading the higher the priority ranking of the improvement.

K. Contexts of use

We showed our respondents a series of eleven activities for which they would normally authenticate, and asked them to choose if they would rather use Pico, passwords or both/neither in these situations. Figure 4 shows the results. While respondents' preferences tend to be evenly distributed between Pico, passwords and both/neither, no respondent chose passwords for logging in to a social networking site (*e.g.* Facebook) from a different computer.

In the interviews, I03 explained Gyazo was a low-security context saying: *"the chances of someone stealing your phone and trying to log in [to] your Gyazo is pretty low, and especially because there's nothing on it, you can just cheat the pictures and take pictures on that account."* Apart from the value of the account, frequency of use was a consideration our interviewees mentioned. While one interviewee felt passwords are more suitable for less frequent activities, two argued passwords would be better for more frequent ones saying: *"it's easy for me to memorise passwords that I frequently have to log in to, because that's just how you memorise, is through use"* (I05). The interviewee further explained where Pico would be a suitable authentication method: *"say it's that you only log into once a month, maybe it's to pay your car insurance or something or a forum that you don't go on very frequently. I could see [Pico] being really handy because it keeps it secure [. . .] instead of having to make a password for each and every single unique obscure thing that you do, you know that this, that the QR code gives you a level of security."*

L. Deploying Pico for Gyazo

One of the key observations from Bonneau *et al.* [21] is that uptake of effective password replacement solutions has been hindered by the relative difficulty of their deployment in comparison with passwords. This helps explain the otherwise perplexing endurance of passwords given their shortcomings in relation to security and usability.

Ease of deployment has therefore been an important consideration for Pico. We especially wanted the ability to integrate Pico with the Gyazo site, without having to make major changes to the site structure, backend code, or database.

As described in Section IV-C, we used a reverse proxy and injection of client-side Javascript using a `sub_filter` rewrite rule. This allowed us to add the Pico QR code onto the site's usual login form without altering any of the backend code. We applied this only to a subdomain (pico.gyazo.com), but we could have applied it to the main domain equally easily.

For this to work, all of Pico's server-side authentication code had to be executed on the client machine using Javascript in the browser. This is unusual: usually the interaction is between the backend server and the user (mediated by the client-side browser). In our case, the client-side browser actually initiates the protocol, while the authentication takes place between the Pico and the website over an entirely separate channel (the phone's data connection).

When developing the solution we were confident that this would be transparent to the end-user, but it was reassuring that none of the participants claimed to have any difficulty understanding the login procedure using Pico. Given the more involved protocol, and use of client-side Javascript, we were less certain that the implementation would run fast enough to satisfy user requirements. Once again we were pleased with the results. The average time taken for the protocol to complete was 3.33 seconds, a small proportion of the overall time users spent during the authentication process, which averaged 47.5 seconds. The opinion of the participants differed on whether they perceived Pico to be faster (two participants) or slower (two participants).

VI. Discussion

The obtained findings imply that Pico provided a good experience for our participants. For example, they found that it was easy to learn how to use Pico and that it was secure. Our findings also imply that the added value of Pico was not significant for a service like Gyazo that uses long-lived cookies expiring every month. This was most evident in the answer to the question about how Pico could be improved, where a large proportion of participants ranked extending the use of Pico to other websites as their top preference. All these findings have the caveat that we obtained insufficient data to be able to statistically validate them. This followed from our decision to invite users who logged in more frequently and entered

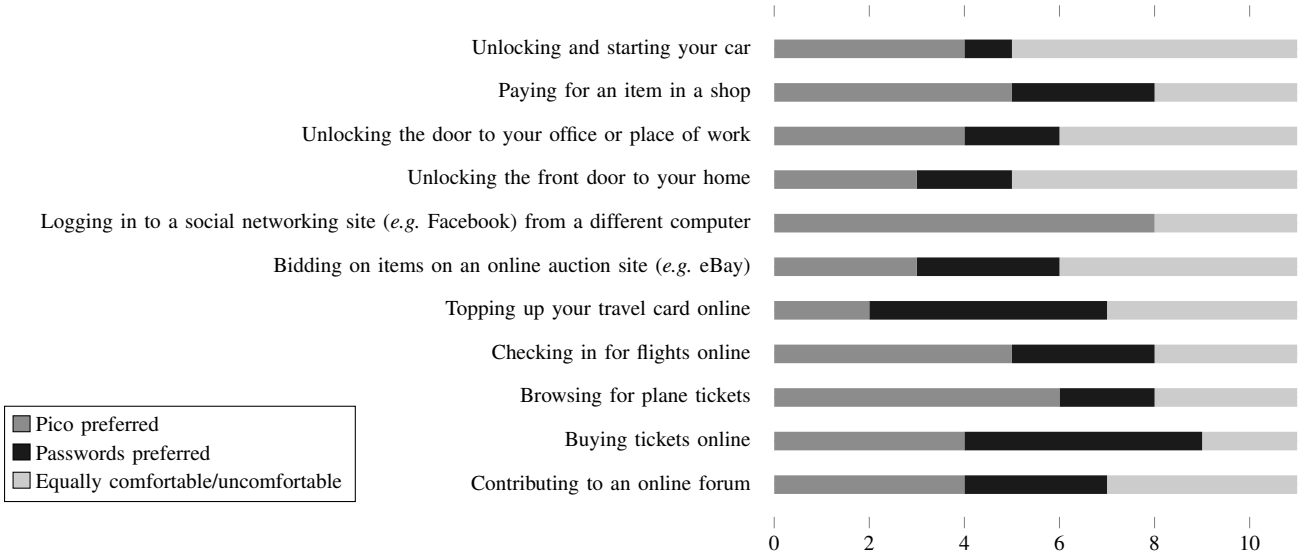

Fig. 4. Numbers of participants who would prefer using Pico, passwords or both/neither for different every-day activities.

their passwords manually. This choice made the technical and logistical aspect of the study simpler but produced very limited data. Our take-away message is that in order to validate the preliminary conclusions that were implied by this study we must conduct further studies to collect more data. A way to validate these conclusions would be to extend the deployment of Pico to more websites or extend the duration of the study on Gyazo. Given that Gyazo's cookies are set to expire after a month, even a year-long study might be expected to collect only around twelve logins per user, so extending it this way would have a prohibitive cost given the limited data involved. Therefore, our focus should be on deploying Pico to more websites.

A. *Lessons learned from conducting an in-the-wild study*

Researchers may not have a choice when it comes to the service where the mechanism is deployed. We had a collaboration with Gyazo, which was a great advantage, but users' frequency of login to the service was low since Gyazo uses long-lived cookies. We attempted to mitigate this by inviting users who logged in more often.

Another problem we encountered related to participant recruitment. Participation in the trial was on an opt-in basis and the number of participants who volunteered and later participated was low for a service that has seven million users.

VII. Conclusions

We conducted a three-part study to understand how users would react to Pico as a replacement for passwords on a major website. It was the first study of fully functional Pico. The study stands out from previous research through its high ecological validity due to deployment in front of a real-world service. Our findings show that participants liked the idea of Pico and generally found it to be secure and less cognitively demanding than passwords. However, some disliked the need to scan QR codes and suggested replacing them with another modality of interaction. There was also a general consensus that participants wanted to see Pico extended for use with more sites.

Our findings will help us shape the future development of Pico. We are planning to look into offering users more choice when it comes to the modalities of authentication, including use of Bluetooth and NFC. Our plan is also to enable login not just to more websites but other types of systems and physical devices as well. Future iterations of the Pico authentication scheme will be tested in different contexts, for accesses of different value. Moreover, more work is needed in providing a comparison with possible alternatives, to establish the types of context in which Pico is particularly effective.

We presented several challenges that we faced when deploying Pico to a real-world service. We were fortunate to have an excellent collaboration with Gyazo, who were very helpful and responsive to our requests. The trial demonstrated how Pico can be deployed to a large website passively, that is without having to change the code or database of the site, and without affecting the running of the service.

We were satisfied that Pico could be integrated as a method of logging in to Gyazo with ease. Technologically the trial was a success, and users had no difficulty in understanding and using Pico. Our recruitment difficulties were our biggest challenge in the study. On the one hand, it is a result of our deliberate methodological approach of not relying on "professional participants" or psychology or computer science undergraduates. On the other hand however, this might be an early warning sign that achieving wide-spread consumer adoption of Pico could be a struggle.

Users tend to prefer to stick with the familiar despite its significant drawbacks, following the rule of "better the devil you know" [28]. Users are accustomed to passwords and understand them very well. Our future efforts will focus on creating a smoother path to the adoption of Pico. We shall develop Pico to more seamlessly fit into users' daily lives, be adaptable to their security and usability needs and provide greater utility than passwords.

Both the trial findings and challenges support the conclusion that developing a suitable replacement for passwords requires

breadth, not just depth. Our struggle to collect sufficient data stemmed significantly from the low frequency of password use on the Gyazo site. At the same time, the possibility of accessing more websites using Pico came out clearly as the most desired feature. Running a similar trial but across a larger range of participant-selected sites would help us validate these findings.

ACKNOWLEDGEMENTS

We are particularly indebted to NOTA Inc., the parent company of Gyazo, for allowing us to integrate Pico into their site and recruit their users into our study. We would also like to thank the European Research Council (ERC) for funding this research through grant StG 307224 (Pico) and the Engineering and Physical Sciences Research Council (EPSRC) through grant EP/M019055/1.

REFERENCES

[1] D. Florêncio, C. Herley, and P. C. van Oorschot, "Password portfolios and the finite-effort user: Sustainably managing large numbers of accounts." in *USENIX Security*, 2014, pp. 575–590.

[2] D. Florêncio and C. Herley, "A large-scale study of web password habits," in *International Conference on World Wide Web*. ACM, 2007, pp. 657–666.

[3] M. A. Sasse, M. Steves, K. Krol, and D. Chisnell, "The great authentication fatigue – And how to overcome it," in *International Conference on Cross-Cultural Design*, vol. LNCS 8528. Springer, 2014, pp. 228–239.

[4] D. Mirante and J. Cappos, "Understanding password database compromises," *Dept. of Computer Science and Engineering Polytechnic Inst. of NYU, Tech. Rep. TR-CSE-2013-02*, 2013.

[5] J. Bonneau and S. Preibusch, "The password thicket: Technical and market failures in human authentication on the web," in *Workshop on the Economics of Information Security (WEIS 2010)*, 2010.

[6] F. Stajano, "Pico: No More Passwords!"," in *Security Protocols XIX*, B. Christianson, B. Crispo, J. Malcolm, and F. Stajano, Eds. Springer International Publishing, 2011, pp. 49–81.

[7] R. Morris and K. Thompson, "Password security: A case history," *Communications of the ACM*, vol. 22, no. 11, 1979.

[8] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years," *ACM Computing Surveys (CSUR)*, vol. 44, no. 4, p. 19, 2012.

[9] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in *USENIX Security*, vol. 13, 2004, pp. 11–11.

[10] S. Brostoff, P. Inglesant, and M. A. Sasse, "Evaluating the usability and security of a graphical one-time PIN system," in *BCS Interaction Specialist Group Conference*. British Computer Society, 2010, pp. 88–97.

[11] K. Krol, C. Papanicolaou, A. Vernitski, and M. A. Sasse, " 'Too Taxing on the Mind!' Authentication Grids are not for Everyone," in *Human Aspects of Information Security, Privacy, and Trust (HAS), HCI International 2015*, vol. LNCS 9190, 2015, pp. 71–82.

[12] A. Beautement and M. A. Sasse, "Gathering realistic authentication performance data through field trials," in *Usable Security Experiment Reports (USER) Workshop at the Symposium on Usable Privacy and Security (SOUPS)*, 2010.

[13] J. Bonneau and S. E. Schechter, "Towards reliable storage of 56-bit secrets in human memory," in *USENIX Security*, 2014, pp. 607–623.

[14] K. Krol, J. M. Spring, S. Parkin, and M. A. Sasse, "Towards robust experimental design for user studies in security and privacy," in *The LASER Workshop: Learning from Authoritative Security Experiment Results (LASER)*. IEEE, 2016.

[15] A. P. Felt, R. W. Reeder, H. Almuhimedi, and S. Consolvo, "Experimenting at scale with Google Chrome's SSL warning," in *Conference on Human Factors in Computing Systems (CHI)*. ACM, 2014, pp. 2667–2670.

[16] S. Brostoff and M. A. Sasse, "Are Passfaces more usable than passwords? A field trial investigation," *People and Computers XIV – Usability or Else!*, pp. 405–424, 2000.

[17] D. D. Strouble, G. Schechtman, and A. S. Alsop, "Productivity and Usability Effects of Using a Two-Factor Security System," in *Annual Conference of the Southern Association for Information Systems*, 2009.

[18] M. Steves, D. Chisnell, M. A. Sasse, K. Krol, M. Theofanos, and H. Wald, "Report: Authentication Diary Study," National Institute of Standards and Technology (NISTIR) 7983, 2014.

[19] K. Krol, E. Philippou, E. De Cristofaro, and M. A. Sasse, " 'They brought in the horrible key ring thing!' Analysing the Usability of Two-Factor Authentication in UK Online Banking," in *NDSS Workshop on Usable Security (USEC)*, 2015.

[20] J. Payne, G. Jenkinson, F. Stajano, M. A. Sasse, and M. Spencer, "Responsibility and tangible security: Towards a theory of user acceptance of security tokens," in *NDSS Workshop on Usable Security (USEC)*, 2016.

[21] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in *IEEE Symposium on Security and Privacy (S&P)*. IEEE, 2012, pp. 553–567.

[22] I. Goldberg, G. Jenkinson, and F. Stajano, *Low-Cost Mitigation Against Cold Boot Attacks for an Authentication Token*. Springer, Cham, Jun 2016, pp. 36–57.

[23] F. Stajano, B. Christianson, M. Lomas, G. Jenkinson, J. Payne, M. Spencer, and Q. Stafford-Fraser, "Pico without public keys," in *Security Protocols XXIII*, B. Christianson, P. Švenda, V. Matyáš, J. Malcolm, F. Stajano, and J. Anderson, Eds. Springer International Publishing, 2015, pp. 195–211.

[24] M. Urueña and I. S. Campos, "User experience of current authentication mechanisms and a proposal for future ones," in *Passwords 2016*, 2016.

[25] G. Jenkinson, M. Spencer, C. Warrington, and F. Stajano, "I Bought a New Security Token and All I Got Was This Lousy Phish – Relay Attacks on Visual Code Authentication Schemes," in *Security Protocols XXII*, B. Christianson, J. Malcolm, V. Matyáš, P. Švenda, F. Stajano, and J. Anderson, Eds. Springer International Publishing, 2014, pp. 197–215.

[26] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative research in psychology*, vol. 3, no. 2, pp. 77–101, 2006.

[27] J. L. Fleiss, B. Levin, and M. C. Paik, *Statistical Methods for Rates and Proportions*. John Wiley & Sons, 2013.

[28] K. Krol, S. Parkin, and M. A. Sasse, "Better the devil you know: A user study of two CAPTCHAs and a possible replacement technology," in *NDSS Workshop on Usable Security (USEC)*, 2016.

APPENDIX A
CONSENT FORM TEXT

As part of this research study, I am willing for the following data to be recorded during the course of the experiments (you must agree to all three to participate):

1) My answers to the questionnaires.
2) The analytics generated by the Pico Gyazo App running on my phone.
3) The analytics about my use of the Gyazo website.

All information will remain strictly confidential. At no time will my name, personal details, any identifiable recording, or any other identification be used externally. I understand that I am free to ask questions and can withdraw my consent and stop participation at any time during the study. By agreeing to this form, I am authorising the researchers conducting this study to collect and analyse the data that is generated as a result of my participation in the study. If I do not agree then I will not be able to participate in the study.

Please read each of the statements below carefully. By accepting this form you are agreeing to them all.

1) I am over 18 years old.
2) I have been given the information sheet that I have read and understood.
3) I have been informed in advance as to what my task(s) would be and what procedures would be followed.
4) I understand that I can ask questions at any time during the trial by emailing cl-pico-gyazo@lists.cam.ac.uk.
5) I understand that not everyone who completes the initial questionnaire will be accepted on to the trial. Acceptance is at the sole discretion of the researchers.
6) I am aware that data collected will be anonymised, kept in accordance with the data protection act, and analysed by the research team as part of their studies.
7) I am aware that the Pico Gyazo App is provided without warranty.
8) I am aware that the Pico Gyazo App will send data on a secure connection to an external server, that I may incur data charges from my mobile operator for this, and that I am responsible for any such charges.
9) I am aware that the Pico Gyazo App will continue to send data about its usage to the research team for as long as I use it, but that I can uninstall it from my phone at any time.
10) I am aware that I have the right to withdraw consent and discontinue participation before or during the study. I understand that if I do withdraw I will not be asked any questions about why I no longer want to take part.
11) I have freely volunteered to participate in this study.

Be aware: The withdrawal process is only available during the study. Should this be requested then all data relating to you will be deleted. After this time, data will be analysed collectively and it may no longer be practical to remove the data completely.

I state that I have read the information sheet and am willing to participate in the experiment being conducted by Dr Frank Stajano and the Pico Team with the gathering of data as mentioned above.

To finalise acceptance, please enter your Gyazo account username (email address) and click on the 'Accept' button.

APPENDIX B
INITIAL QUESTIONNAIRE

Many thanks for agreeing to take part in the study. If you could please complete the single page of questions below. We will then get in contact using your Gyazo email address.

1) What gender are you?
   - Female
   - Male
   - Other/prefer not to say
2) Please tell us the age range you fall into.
   - Under 18
   - 18 - 24
   - 25 - 34
   - 35 - 44
   - 45 - 54
   - 55 - 64
   - 65 - 74
   - 75 - 84
   - 85 or older
3) How often do you manually type in your Gyazo password?
   - Fewer than once per week
   - Fewer than once per day
   - Roughly once per day
   - Roughly 2-4 times per day
   - Roughly 5 or more times per day
4) When you type your Gyazo password, explain the main reason why you have to enter it?
5) Which of these methods for managing your passwords do you generally use?
   - Let my browser remember my password
   - Password manager/plugin/extension (*e.g.* LastPass, 1Password)
   - Password generator
   - Reset password by email when I need to login
   - Password containing personal information
   - Stored in a file/on a piece of paper
   - Using the same password on multiple sites
   - No special methods (I just remember all of my passwords)
   - Other
6) Optionally, please tell us any other thoughts you may have about your experience using passwords.
7) What sort of smartphone do you use?
   - Android
   - iOS
   - Windows Phone
   - Blackberry
   - None
   - Other
8) Please enter your Google Play email address if you're interested in continuing with the trial.
9) That's all of the questions. Please hit the submit button to register your answers.

10) Browser Meta Info
    - Browser
    - Version
    - Operating System
    - Screen Resolution
    - Flash Version
    - Java Support
    - User Agent
11) Timing
    - First Click
    - Last Click
    - Page Submit
    - Click Count

APPENDIX C
EXIT QUESTIONNAIRE

Thank you for using Gyazo, and for participating in our Pico-Gyazo study. Please complete the questions below. At the end, you'll be given the opportunity to take part in a debriefing interview, and we'll provide details of how you can claim your reward. Note that your answers won't be saved until you click on the Submit button at the bottom of the page.

1) Your Gyazo user name (email address)
2) Please tell us to what extent you agree or disagree with each of the following statements (Strongly agree; Somewhat agree; Neither agree nor disagree; Somewhat disagree; Strongly disagree).
    - Using Pico requires cognitive effort.
    - Using Pico requires physical effort.
    - It is easy to learn how to use Pico.
    - Pico makes me more efficient.
    - I am afraid of losing my Pico device and losing access to my account.
    - I find scanning the QR codes reliable.
    - Installation of the Pico-Gyazo app was straightforward.
    - I feel secure using Pico to log in to Gyazo.
    - I am concerned about others observing the QR code when I log in to Gyazo
    - Using Pico makes me more concerned about my smartphone being stolen.
    - Overall, I find Pico makes my online activity easier.
3) If you were storing all of your passwords on your phone, which methods would you feel comfortable securing your phone with (select as many as you like)?
    - 4-digit PIN
    - 6-digit PIN
    - Password
    - Pattern lock
    - Fingerprint
    - Slide lock
    - Facial recognition
    - No phone lock (I always know where my phone is)
    - Other
4) Please drag each of the items below into the box on the right to rank the ways of improving the Pico app in order of priority (1=most useful; 8=least useful).
    - Reduce the download size of the app.
    - Improve the speed of the app.
    - Simplify the installation and initial configuration of the app.
    - Remove the need to scan the QR code to log in.
    - Remove the need to have a data connection when logging in.
    - Allow me to log in to more websites (not just Gyazo).
    - Improve security of the app further.
    - Allow me to block the app remotely in case of loss
5) Drag each of the items below into one of the three boxes provided (Pico; Passwords; Equally comfortable/uncomfortable) to indicate whether you would feel more comfortable using Pico or passwords for that activity.
    - Contributing to an online forum.
    - Buying tickets online.
    - Browsing for plane tickets.
    - Checking in for flights online.
    - Topping up your travel card online.
    - Bidding on items on an online auction site (*e.g.* eBay).
    - Logging in to a social networking site (*e.g.* Facebook) from a different computer.
    - Unlocking the front door to your home.
    - Unlocking the door to your office or place of work.
    - Paying for an item in a shop.
    - Unlocking and starting your car.
6) Can you suggest ways that the Pico approach to authentication could be improved for you?
7) Would you be interested in continuing to use the Pico Gyazo App to log in to your Gyazo account?
    - Yes
    - No
8) Optionally, please tell us any other thoughts you may have about your experience using Pico, or using passwords.
9) Thank you for answering our questions. In order to claim your 10 GBP online voucher as reward, please select which store you would like the voucher for.
    - amazon.com
    - amazon.com.au
    - amazon.com.br
    - *etc.*
10) Would you be willing to take part in an audio-only debriefing interview via Skype (or similar)? Anyone who takes part in the debriefing interview will be rewarded an additional 10 GBP online voucher. If you answer 'Yes' we'll get in contact by email to arrange a suitable time.
    - Yes
    - No
11) We'll contact you with information on how to claim your reward using your Gyazo email address. If you prefer us to contact you using an alternative email address, please enter it below.

That's all of the questions. Please hit the submit button to register your answers.

APPENDIX D
INTERVIEW QUESTIONS

List of questions used in the interviews, here for interviewee I05.

Claudio: Hi *[participant's first name]*! How are you?

My name is Claudio Dettoni and I'm a researcher at the University of Cambridge and there is also Kat Krol with me here in the room.

Kat: Hi *[participant's first name]*! My name is Kat.

Claudio: Thank you so much for taking part in the Pico-Gyazo trial for the past two weeks and thank you for agreeing to this interview. *[pause]*

Claudio: Can we just check that you received the Amazon voucher for taking part in the trial? *[pause]*

Claudio: Great, thank you.

Kat: So just to give you an overview, this interview now will take around 20 minutes and we audio-record it because we can't take notes fast enough. Can we start the audio-recording? *[pause]* In this interview, we will ask you general questions about how you found using the Pico app during the trial. There are obviously no right or wrong answers here, we are just interested in your perceptions and opinions. Have you got any questions? *[pause]*

If not, are you happy to start?

1) How did you come to use Gyazo?
    a) How long have you been using it?
    b) What do you use it for?
    c) What devices do you use Gyazo on? [web or app]
2) How do you normally log in to Gyazo?
3) In what situations are you asked to log in? [If no constructive answer, use this more direct phrasing: "Why do you log in this often?"]
4) Are you a premium user? If yes: Do you use password protected clips? If yes: How do you manage the passwords for them?
5) In the last two weeks, you used Pico: How was your experience of using it?
6) You mention that you somewhat disagree that you're afraid of losing your Pico. Why is this? Are you concerned about losing your phone at all? What would you do in case of a loss?
7) How do you currently lock and unlock your phone?
8) If you were storing all of your passwords on your phone, you mention you would be happy with a 6-digit PIN, pattern lock or slide lock. Is this correct? Is this a change from what you do now?
9) You mention that you would like to remove the need to scan a QR code to log in. Do you have any thoughts about how you'd like it to work instead?
10) You also mention that you'd prefer to use passwords for online forums, buying flights or tickets online. Why is this?
11) How would you feel about using Pico to bid on eBay items?
12) How often did you log in using Pico during the two weeks? [If no constructive answer: Did it change from how often you previously logged in with passwords?]
13) Did you experience any problems using Pico?
14) What is your general experience with passwords? How do you manage your passwords? [I05 chose in the first questionnaire "Let my browser remember my password"]
15) What was the best thing about Pico?
16) What was the worst thing about Pico?
17) How does Pico compare to passwords? In terms of:
    a) Ease of use
    b) Speed of login
    c) Errors
    d) Security
18) What would you change about Pico to make it better?
19) What do you think about the security of Pico?
20) What is the value of the things you share on Gyazo? How does this value compare to other things that you need to authenticate to access?
21) Although the trial is over, the Pico-Gyazo service is going to continue, what are you going to do with the app? Have you been using the app since you had sent the final questionnaire?
22) In our implementation, Pico was dedicated to logging in to Gyazo. What if it was possible to use a Pico app to log in to other services you are using, such as email, online shopping *etc.*? How would you feel about this? [Logic: Do they see it as a means of logging in to Gyazo or would they think it could work for other services too?]