Alternatives to traditional text-based authentication: An experiment, survey and literature review

Yujia Chen
School of Computer Science
North Carolina State University
Raleigh, NC 27695
Email: ychen71@ncsu.edu

Kaustubh Gondhalekar
School of Computer Science
North Carolina State University
Raleigh, NC 27695
Email: kgondha@ncsu.edu

Siddharth Sharma
School of Computer Science
North Carolina State University
Raleigh, NC 27695
Email: ssharm24@ncsu.edu

***Abstract*—The explosion of Internet services has made authentication an inescapable aspect of our digital lives. The traditional text-based password approach for authentication has been adequate until recently; but today with most users having at-least 20-50 accounts, storing and remembering passwords is becoming cumbersome day by day. The method is riddled with problems, and is not secure without proper user precautions. We think it is time for a paradigm shift in the way that we authenticate, where it should be as effortless as possible. Hence we detail problems with existing methods, and how new and improved methods address them. In this report, we propose and compare three different ways of authentication which can make authentication easier and potentially more safer than the traditional text-based password approach.**

***Keywords*—Authentication, biometrics, fingerprint, voice recognition, password-less logins, graphical password**

I. Introduction

Authentication is all around us. Increasing number of Internet services like social networking, video-streaming, e-commerce shopping, gaming etc. require the user to remember myriad passwords. Every service demands a different policy of creating a password for their service which the users need to satisfy. On top of that, no service takes into account the cognitive pressure levied on the users from concocting unique and weird passwords and then remembering them. Password management is deemed entirely the user's responsibility [2]. A literature review on this subject reveals the user-login problem. In order to get a better perspective on this problem, we conducted a user-survey asking them about their experience with text-based passwords. The survey revealed that there is indeed a problem with respect to the traditional text-based authentication. Section III-C explains the survey results in greater detail. The paper proposes the following three solutions to this problem which ease the pain of authentication via text-based passwords:
Biometric authentication:
1. Fingerprint authentication.
2. Voice-DNA authentication.
Password-less authentication:
3. Using 'magic link' via email.

II. Literature Review

Before we jump into this issue, we turn to several academic literature, trying to find existing research on the method and data solving this problem.

One problem we face is that people tend to forget their password, especially for those accounts which required a complicated password policy. For example, Carnegie Mellon University uses a comprehensive password policy that requires eight characters, four character classes, and includes a dictionary check. There's one prior research found that users struggled to create and recall passwords under this comprehensive policy [1]. But without those password-composition policies to force users to make stronger password, research has shown that many users would opt to create simple, easily guessed passwords. In a 1995 study, researchers requested that system administrators send them hashed passwords. The researchers were able to crack about 40% of the approximately 14,000 passwords using a dictionary attack[1].

This led to a call for proactive password checking to make sure passwords comply with a set of password-composition requirements [8]. Thus the users were forced to create a password which has a minimum said level of strength. But this creates another problem: Password reuse. Compliance to all the password-policies out there makes it difficult to whip out a unique password every time the user registers a new web-account and encourages password reuse. According to a study conducted on password management by Princeton University, "When a user creates an account they have little motivation to generate a unique password. They have not started storing private or financial information on the website. Reuse is encouraged because it makes a password easier to remember."[2]

This behaviour is completely against the password security lore which summarises to "Pick something you cannot remember and don't write it down"[3] Thus password managers were invented claiming to relieve the burden of password management from the users. But very few users actually use password managers. Most rely on memory for storing their passwords[2].

In the paper 'Using and managing multiple passwords: A week to a view' by Beate Grawemeyer and Hilary Johnson, they conducted an experiment trying to figure out what is the instance of actual password use over the study period, how many passwords do participants need to manage, what types of password are created, how often are they changed, how do people manage multiple passwords, and what are the incidences of failure to authenticate and manage passwords.

They gathered 22 participants and 991 password entries from HP Laboratories in Bristol. The result from the experiment shows that the mean number of password to manage is 7.95 across 175 reported services. Also over the 7-day period 48 failures to enter a password were reported. The different types of failures reported by participants include: mistyping the password (19); misremembering the password (15); uncertainty about which password to chose (6); forgetting the password altogether (4); some other problem (3); and, being interrupted during the authentication process (1)[4]

We thus have an explosion of new Internet services demanding authentication; most of the passwords we use just-comply with the password policies of the web-services and since we mostly rely on memory to store these passwords, we reuse them. This suggests that the text-based password system has a fundamental flaw : It doesn't scale well. This prompts the investigation of other authentication systems to remedy it.

A. Existing solutions

The literature presents lots of solutions to this problem. In today's modern era, almost everyone owns a 'smart-phone'. "Mobile devices are rapidly becoming a key computing platform, transforming how people access business and personal information" [6] Making users type out weird symbols and alpha-numeric characters on the small screens of their smartphones takes away all the great usability that a mobile device offers. A recent paper on biometric authentication beautifully states "Biometric authentication is often referred to as the secret weapon of authentication, mainly due to the fact that the password (e.g. a fingerprint) cannot be forgotten"[5]. It seems we have hit two birds in one shot! We now have the portability of a mobile device combined with the usability of a biometric password! The literature points to using biometrics as a solution to the plague that text-based passwords have become. Using biometrics also present us with lots of choices: fingerprints, voice, face-recognition, keystroke-DNA, gait analysis etc. The first biometric we chose (fingerprint) needs no justification in today's world. Apple's TouchID as well as Android's fingerprint authentication have taken the world by the storm. This feature is immensely popular and is a great candidate for our problem. We eliminated out keystroke-DNA and gait analysis as it wasn't a mature enough in both literature and real-world use. The title of the paper on understanding biometrics on smartphones explains our elimination of facial recognition; the paper is titled 'I Feel Like Im Taking Selfies All Day! Towards Understanding Biometric Authentication on Smartphones'[7] While analysing facial-recognition, the paper mentions "Besides bad lighting conditions leading to bad performance, the participants mentioned social awkwardness as an important external factor that kept them from using the system."[7] We thus decided on using fingerprint and voice as our biometric candidates for the solution to the problem.

The third candidate solution was inspired by Slack Messenger's authentication system. The authentication system eliminates the use of a password by sending you a 'magic-link' to your email. Thus one-click and you are through! The simplicity and usability of this solution made it reserve the third spot on our candidate solutions list.

III. Data Collection

A. Baselines

To establish a baseline for later evaluation of our alternatives, we benchmarked our users with the existing text-based authentication method. This was done in 2 ways. First, we asked user to log into their university management system. This method was chosen since our participants were primarily university students, and the account is frequently used. The second was a web authentication portal called User Login Experiment (Fig. 1), designed by our team to let users create an account and log into it. The interface was made as to represent the most common website registration systems used around the web. Our portal required an email address (which we did not validate), and a password, with length greater than 6. On the back-end of the website, we created a function that would mark the time required for the user to login (the time from when he/she opens to login page to the time till he/she is successfully logged-in). We also counted the number of times the user put in the wrong username and password combination. The device used for this experiment was a University issued Apple MacBook Pro 13" and a DELL Latitude E7440, to eliminate the factor that different device would affect user's log in time, also we want the participant to feel more safe about their privacy regarding their password.

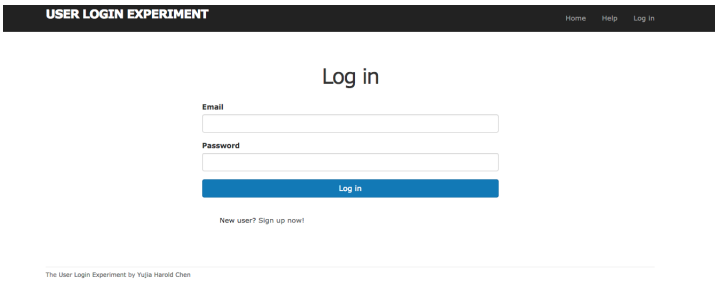

Fig. 1. Login page for the User Login Experiment website

The authentication portal also enabled us to measure the important parameter of the barrier to entry. We measure the time and effort for new users to register and log-in. Thus, we aim to minimize the 2 processes which are - user registration, and user authentication.

For the baseline we chose to observe people trying to log into Wolfware using their NC State UnityID account. Since the participants we chose have already logged into Wolfware for at least once before, we have created a User Login Experiment site with the basic user register and log in function, trying to see if there is any differences between log into a familiar site and an unfamiliar one. We gathered 24 participants, all of them are current NC State students. We observed their log-in procedure, and timed their login attempt, also measuring how many times they failed to log into the system, shown in TABLE 1.

User	Wolfware login time	Exp site login time	computer skll	fail times
User1	25.1 seconds	23 seconds	expert	0
User2	10.4 seconds	14 seconds	expert	0
User3	6.3 seconds	5 seconds	expert	0
User4	15.2 seconds	17 seconds	expert	0
User5	17.3 seconds	17 seconds	expert	0
User6	12.0 seconds	11 seconds	intermediate	1
User7	8.0 seconds	8 seconds	expert	0
User8	21.0 seconds	22 seconds	expert	0
User9	14.9 seconds	13 seconds	expert	0
User10	19.1 seconds	20 seconds	expert	0
User11	23.3 seconds	31 seconds	expert	1
User12	25.9 seconds	24 seconds	intermediate	0
User13	1.1 seconds	2 seconds	expert	0
User14	6.8 seconds	10 seconds	expert	0
User15	11.0 seconds	12 seconds	expert	0
User16	15.4 seconds	18 seconds	expert	0
User17	15.7 seconds	17 seconds	expert	0
User18	7.3 seconds	6 seconds	expert	0
User19	16.3 seconds	36 seconds	intermediate	1
User20	14.2 seconds	12 seconds	expert	0
User21	11.1 seconds	12 seconds	expert	0
User22	13.9 seconds	16 seconds	expert	0
User23	9.7 seconds	10 seconds	expert	0
User24	9.5 seconds	11 seconds	expert	0

TABLE I. BASELINE DATA

B. User Evaluation

To analyse user attitude towards passwords, and authentication in general, we designed a user evaluation study. The study had two main parts - questionnaire (Fig.3 and Fig.4) and semi-interview session. The questionnaire was intended to determine patterns in password usage among users. The questions ranged from security to convenience, and tested users on their attitude towards other methods. We put in a trick question, which is How many accounts (requiring a username and password) do you have. If the user chose "I don't have any", we can throw away his/her answer since the survey was conducted via Google Form and you need a Google account to answer the survey.

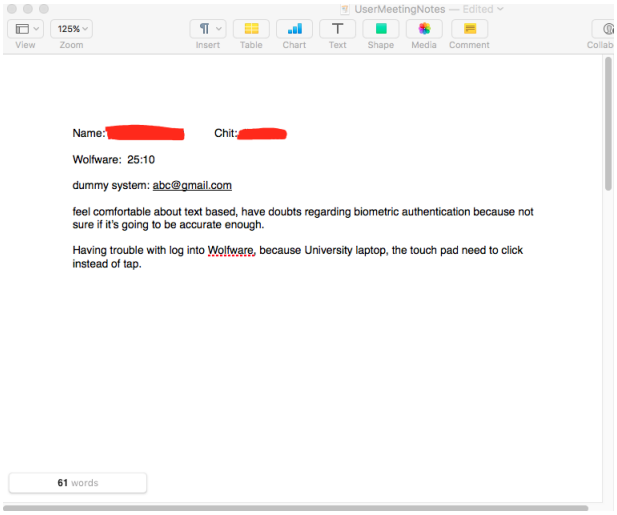

Fig. 2. Note from the interview session

The interview session was designed to be a informal session, about concerns regarding passwords, and trade-offs with other means of authentication. Several users said to have used biometric fingerprint authentication to log in. This was primarily due to newest models of smartphones(including Apple iPhone) introducing fingerprint recognition as a way to unlock the phone. Users in survey seemed to have a favorable view of technologies they had previously encountered.

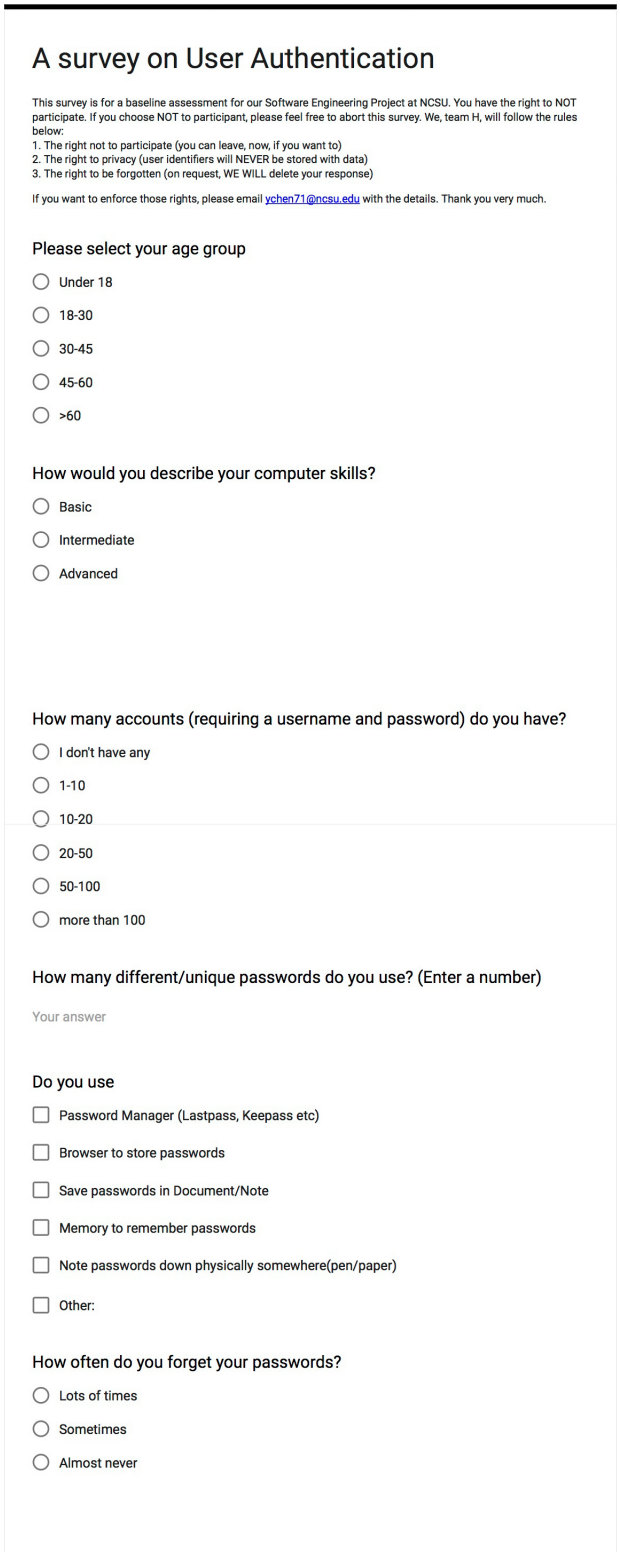

Fig. 3. First part of the questionnaire using Google Form

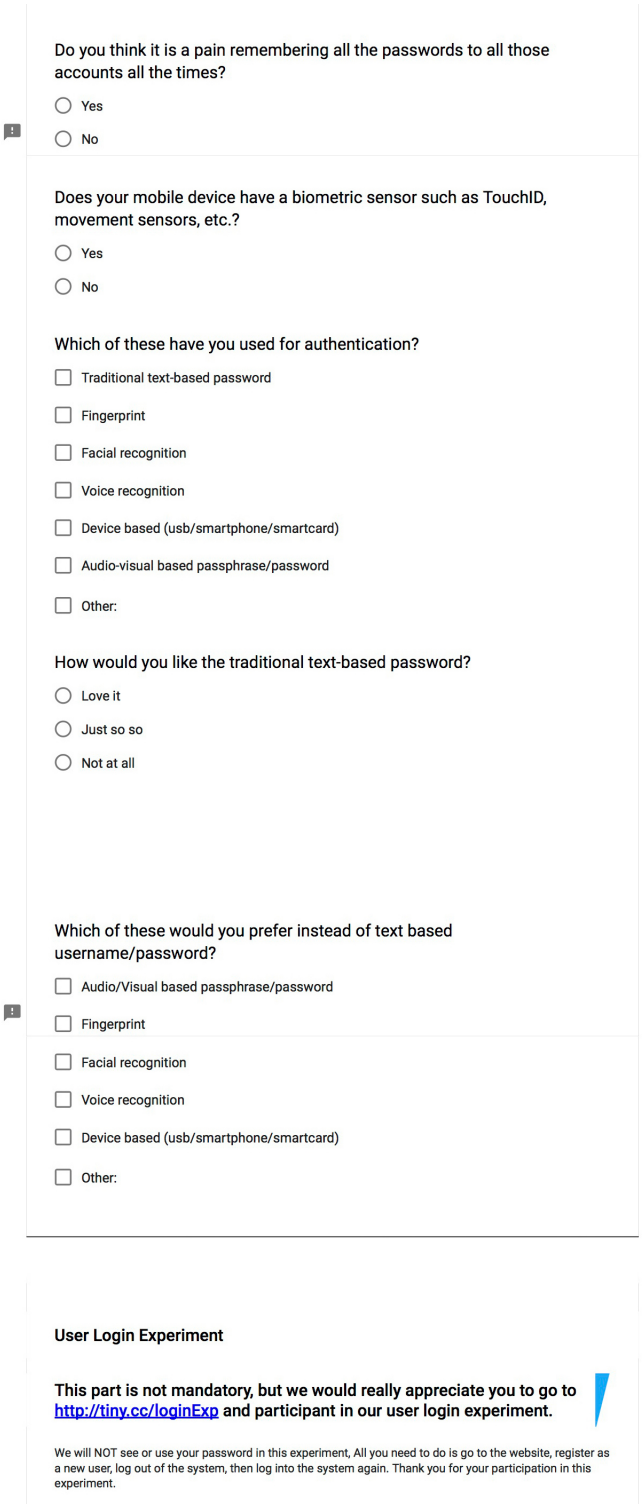

Fig. 4. Second part of the questionnaire using Google Form

C. Data Analysis

Website logged in	Average time	Average login fail times
Wolfware	13.771 seconds	0
User Login Experiment	15.217 seconds	0.087

TABLE II. BASELINE DATA

From the data we can see that the average time for a user to log into these two systems is 1.446 seconds, and no one failed to log into Wolfware, a system they use regularly. For the User Login Experiment website, 2 of the participants failed to log in the first try, but succeed on the second try. Also, from our observation, we found that people who are familiar with the device can log into the system quicker than those who use the device for the first time. Also, we found that users who consider themselves as 'expert computer users' tend to have a quicker log in time and a higher success rate.

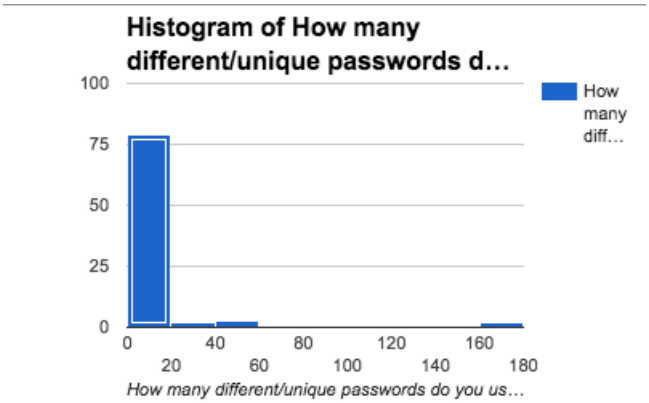

Fig. 5. Quantity of passwords the participants have

84 responses were received from the survey, we exported the data to Google Sheets and created bar charts and pie charts to help visualize the data. We can see in the bar chart in Fig. 5 that users tend to have 0 20 passwords for their accounts, one participant even reported more than 100 passwords (175). We also found out that 28.6% of the participants almost never forgot their password (Showed in Fig. 6). We looked into these participants, and find out that these participants are either using a password managing software to manage all their passwords, or they have few passwords to remember.

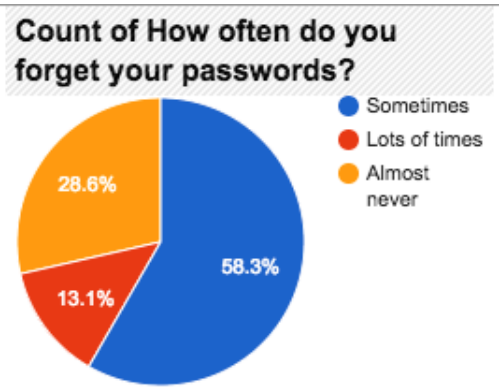

Fig. 6. Frequency for participant to forgot their password during log in

Biometric sensors on mobile devices have been in the market for quiet a few years, from the basic movement sensor, digital cameras to the more advanced fingerprint sensor like

	easy-to-use	easy-to-setup	easy to remember	offline ability	security	accuracy
Text-based	+	+	-	+	+/-	+
Fingerprint	+	-	+	+	+	+/-
Voice-DNA	+	-	+	+	+/-	+/-
Magic link	+	+	-	+	+/-	+

TABLE III. TRADE-OFF TABLE FOR DIFFERENT AUTHENTICATION APPROACH

TouchID, in these 84 participants, 66.7% of the participants reported that their mobile device have a biometric sensor built in.

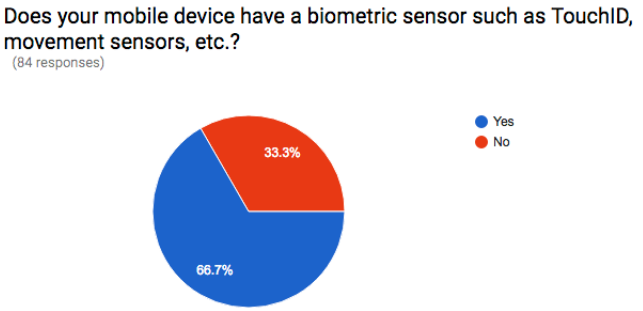

Fig. 7. Percentage of biometric sensors on mobile devices

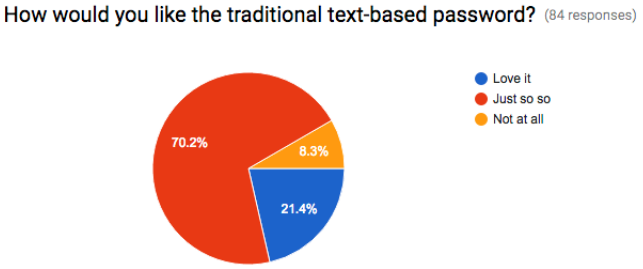

Fig. 8. Paticipants' attitide towards plaintext password

Only 21.4% of the participants love this idea, their reasons are password combinations are more safe, and easier to use comparing with the new methods such as using fingerprints to unlock your phone and log into your account. A majority of the participants (70.2%) find the idea just about okay.

IV. CONCLUSION

The text-based password has been with us for a long long time, and although it had a fairly good run till now, it has run into scalability issues. There are many researchers and academics are devoting themselves trying to find a replacement that is convenient to use, fast and accurate, secure enough against malicious attacks. From the literature and user survey, we have decided three approaches : Fingerprint authentication, Voice-DNA authentication, Using 'magic link' via email. We are going to implement these three password authentication methods, and compare them against their usability, accuracy and efficiency, then draw a conclusion on what we think is the best one. These approaches, along with the text-based password, have their own strength and shortcomings as shown in Table III. We will present concrete results of our analysis in the final leg of this project.

REFERENCES

[1] Saranga Komanduri, Richard Shay, Patrick Gage Kelley, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Serge Egelman. 2011. Of passwords and people: measuring the effect of password-composition policies. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11).

[2] 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.

[3] 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.

[4] Beate Grawemeyer, Hilary Johnson, Using and managing multiple passwords: A week to a view, Interacting with Computers, Volume 23, Issue 3, May 2011, Pages 256-267, ISSN 0953-5438, http://dx.doi.org/10.1016/j.intcom.2011.03.007.

[5] Bhagavatula, C., Iacovino, K., Kywe, S. M., Cranor, L. F., and Ur, B. Poster: Usability analysis of biometric authentication systems on mobile phones. SOUPS Poster (2014).

[6] Shari Trewin, Cal Swart, Larry Koved, Jacquelyn Martino, Kapil Singh, and Shay Ben-David. 2012. Biometric authentication on a mobile device: a study of user effort, error and task disruption. In Proceedings of the 28th Annual Computer Security Applications Conference (ACSAC '12). ACM, New York, NY, USA, 159-168. DOI=http://dx.doi.org.prox.lib.ncsu.edu/10.1145/2420950.2420976

[7] Alexander De Luca, Alina Hang, Emanuel von Zezschwitz, and Heinrich Hussmann. 2015. I Feel Like I'm Taking Selfies All Day!: Towards Understanding Biometric Authentication on Smartphones. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15). ACM, New York, NY, USA, 1411-1414. DOI: http://dx.doi.org.prox.lib.ncsu.edu/10.1145/2702123.2702141

[8] Bishop, Matt, and Daniel V. Klein. "Improving system security via proactive password checking." Computers Security 14.3 (1995): 233-249.