Brigham Young University
BYU ScholarsArchive

All Theses and Dissertations

2015-04-01

Authentication Melee: A Usability Analysis of Seven Web Authentication Systems

Scott Ruoti
Brigham Young University - Provo

Follow this and additional works at: https://scholarsarchive.byu.edu/etd

Part of the Computer Sciences Commons

BYU ScholarsArchive Citation

Ruoti, Scott, "Authentication Melee: A Usability Analysis of Seven Web Authentication Systems" (2015). *All Theses and Dissertations*. 4376.
https://scholarsarchive.byu.edu/etd/4376

This Thesis is brought to you for free and open access by BYU ScholarsArchive. It has been accepted for inclusion in All Theses and Dissertations by an authorized administrator of BYU ScholarsArchive. For more information, please contact scholarsarchive@byu.edu, ellen_amatangelo@byu.edu.

www.manaraa.com

Authentication Melee: A Usability Analysis of Seven Web Authentication Systems

Scott Ruoti

A thesis submitted to the faculty of
Brigham Young University
in partial fulfillment of the requirements for the degree of

Master of Science

Kent Seamons, Chair
Charles Knutson
Dan Olsen

Department of Computer Science

Brigham Young University

February 2015

Copyright © 2015 Scott Ruoti

All Rights Reserved

www.manaraa.com

ABSTRACT

Authentication Melee: A Usability Analysis of Seven Web Authentication Systems

Scott Ruoti
Department of Computer Science, BYU
Master of Science

Passwords continue to dominate the authentication landscape in spite of numerous proposals to replace them. Even though usability is a key factor in replacing passwords, very few alternatives have been subjected to formal usability studies and even fewer have been analyzed using a standard metric. We report the results of four within-subjects usability studies for seven web authentication systems. These systems span federated, smartphone, paper tokens, and email-based approaches. Our results indicate that participants prefer single sign-on systems. We utilize the Systems Usability Scale (SUS) as a standard metric for empirical analysis and find that it produces reliable, replicable results. SUS proves to be an accurate measure of baseline usability and we recommend that going forward all new authentication proposals be required to meet a minimum SUS score before being accepted by the security community. Our usability studies also gather insightful information from participants' qualitative responses: we find that transparency increases usability but also leads to confusion and a lack of trust, participants prefer single sign-on but wish to augment it with site-specific low-entropy passwords, and participants are intrigued by biometrics and phone-based authentication.

Keywords: Usable Security, Authentication, User Study, System Usability Scale

www.manaraa.com

ACKNOWLEDGMENTS

Thanks go to Brent Roberts for help administering the user studies and providing some basic analysis of collected data. A special thanks goes to my wife, Emily Ruoti, for helping edit this thesis and the WWW'15 submission based on this thesis, and for all the other support she gave me throughout my Master's program.

www.manaraa.com

Table of Contents

List of Figures **vii**

List of Tables **ix**

1 Introduction **1**

2 Related Work **3**

3 Authentication Tournament **7**

3.1 System Usability Scale 8

3.2 Tournament Structure 9

3.2.1 Federated Single Sign-on 11

3.2.2 Email-based Single Sign-on 11

3.2.3 QR Code-based 12

4 System Walkthroughs **13**

4.1 Google OAuth 2.0 13

4.2 Facebook Connect 15

4.3 Mozilla Persona 17

4.4 Simple Authentication for the Web 22

4.5 Hatchet 23

4.6 WebTicket 26

4.7 Snap2Pass 28

www.manaraa.com

5 Methodology **33**

5.1 Study Setup . . . 33

5.1.1 Quality Control . . . 34

5.1.2 Participants Demographics . . . 35

5.2 Task Design . . . 36

5.2.1 Authentication System Implementation . . . 37

5.3 Study Questionnaire . . . 37

5.4 Survey Development . . . 38

5.5 Limitations . . . 39

6 Results **40**

6.1 First Study – Federated . . . 40

6.2 Second Study – Email-based . . . 44

6.3 Third Study – QR Code-based . . . 44

6.4 Fourth Study – "Championship Round" . . . 45

7 Discussion **46**

7.1 System Usability Scale . . . 46

7.2 Transparency . . . 47

7.3 Single Sign-on Protocols . . . 48

7.3.1 Additional Low-entropy Passwords . . . 49

7.3.2 Reputation . . . 49

7.3.3 Dedicated Identity Providers . . . 50

7.4 The Coolness Factor . . . 50

7.4.1 Biometrics . . . 51

7.5 Physical Tokens . . . 51

7.6 Implementation Lessons . . . 52

8 Conclusion **54**

www.manaraa.com

References **56**

A Usability Study Survey **61**

A.1 Introduction 61

A.2 Demographics 63

A.3 Tasks 64

A.3.1 Task 1 64

A.3.2 Task 2 64

A.3.3 Task 3 65

A.3.4 Task 4 65

A.3.5 Task 5 66

A.3.6 Task 6 67

A.4 Questionnaire 67

A.5 End-of-survey Questionnaire 68

B Federated Single Sign-on Usability Study – Participant Responses **69**

C Email-based Usability Study – Participant Responses **88**

D QR Code-based Usability Study – Participant Responses **110**

E "Championship Round" Usability Study – Participant Responses **134**

www.manaraa.com

List of Figures

3.1 An adjective-oriented interpretation of SUS scores 9

3.2 Authentication tournament bracket 10

4.1 Google OAuth 2.0 login button 14

4.2 Google OAuth 2.0 login screen 14

4.3 Google OAuth 2.0 user account selection screen 15

4.4 Google OAuth 2.0 permission grant screen 15

4.5 Facebook Connect login button 16

4.6 Facebook Connect login screen 16

4.7 Facebook Connect permission grant screen 17

4.8 Mozilla Persona login button 18

4.9 Mozilla Persona account confirmation 18

4.10 Mozilla Persona remember-me option 19

4.11 Mozilla Persona authentication complete dialog 19

4.12 Mozilla Persona email entry 19

4.13 Mozilla Persona account verification (Google) 20

4.14 Mozilla Persona account verification (Yahoo) 20

4.15 Mozilla Persona account creation 21

4.16 Mozilla Persona account verification (Email-based) 21

4.17 Mozilla Persona login dialog 21

4.18 SAW login form 22

4.19 SAW login message 22

www.manaraa.com

4.20 SAW email message (Inbox) 23
4.21 SAW email message (Full) 23
4.22 SAW completion screen 23
4.23 Hatchet login form 24
4.24 Hatchet code entry dialog 24
4.25 Hatchet email message (Phone) 25
4.26 Hatchet email message (Inbox) 25
4.27 Hatchet email message (Full) 26
4.28 A WebTicket 27
4.29 WebTicket webcam video feed 28
4.30 Snap2Pass registration QR code 29
4.31 Snap2Pass Android application 30
4.32 Snap2Pass application – QR code scanner 30
4.33 Snap2Pass application – registration confirmation 31
4.34 Snap2Pass application – accounts page 31
4.35 Snap2Pass login QR code 32
4.36 Snap2Pass application – login confirmation 32

www.manaraa.com

List of Tables

2.1 Authentication proposals cited by Bonneau et al. 4

3.1 The ten SUS questions 8

3.2 SUS score card 8

5.1 Participant demographics 35

6.1 SUS scores and participant preferences 41

6.2 Comparison of system SUS scores 42

6.3 Mean time to authenticate 43

A.1 System specific text replacements 62

A.2 Additional text replacements for WebTicket and Snap2Pass 63

www.manaraa.com

Chapter 1

Introduction

Passwords continue to dominate the authentication landscape. Bonneau et al. [5] analyzed a broad collection of systems designed to replace passwords. They demonstrated that passwords have a unique combination of usability, security, and deployability that has proven difficult to supplant. While some success is being made by Federated identity systems (i.e., Google OAuth 2.0, Facebook Connect) and password managers (e.g., LastPass), these systems are not disruptive, but are designed to enhance the use of passwords.

While Bonneau et al. presented a heuristic-based approach for evaluating the usability of authentication schemes, it is also imperative that authentication systems are subjected to empirical usability analysis. We survey the publications cited by Bonneau et al. and discover that only four of the twenty-three publications report the results of an empirical study. Moreover, only one of these four publications compares its proposed system against another competing authentication system. Most troubling, none of the systems are analyzed using a standard usability metric, making it impossible to determine which of the four systems has the best usability. This problem is not limited to the publications cited by Bonneau et al., as only a single study of authentication systems has used a standard usability metric [25]. Without a standard metric there is no means by which a new proposal can be evaluated to determine whether it has better than existing systems.

In this paper, we report the results of a series of within-subjects empirical usability studies for seven web authentication systems. The seven authentication systems are heterogeneous and span federated, smartphone, paper token, and email-based approaches. Our

www.manaraa.com

studies are the first to compare a heterogeneous collection of authentication proposals. Our research goals are two fold:

1. *Determine which system has the best overall usability.* This is accomplished using the the System Usability Scale (SUS) [7, 8], a standard usability metric which has been used in hundreds of studies [3, 4].[1]
2. *Explore which authentication features users prefer and which features they dislike.* In our studies, participants use multiple authentication systems and provide feedback describing what they like and what they would change.

The result of our studies is that federated and smartphone-based single-sign on were rated as having the best overall usability. Also, our results validate SUS as an appropriate metric for comparing the usability of authentication systems, with the SUS score for a given system being consistent across different participant groups and proving to be a strong indicator of users' preferences. We recommend that all new authentication proposals be evaluated using SUS, and that a proposal should not receive serious consideration until it achieves a minimum acceptable SUS score of 70.

Our usability studies also gather insightful information from participants' qualitative responses. We find that systems with minimal user interaction are rated as highly usable, but are also described by participants as confusing and unworthy of trust. Additionally, while participants rate the usability of single sign-on highly, they are interested in augmenting it with additional low-entropy passwords. Finally, our results show that over half of participants are willing to use new authentication systems in their everyday life, but that they are most interested in adopting systems that they perceive as different and innovative (e.g., biometrics, phone-based authentication).

[1] Based on participants' feedback, SUS assigns a scalar value [0-100] to each system, with higher scores indicating greater usability. A full description of SUS is given in Section 3.1.

www.manaraa.com

Chapter 2

Related Work

The field of usable security was started in 1999 by Whitten et al.'s study of the popular PGP 5.0 encryption tool [47]. Their results demonstrated that PGP 5.0 was unusable and that users were unable to complete even simple tasks using it. Since then, there has been a significant amount of research into the usability of security systems, but these efforts continue to lag behind those of the usability community at large [18].

We conduct an exhaustive search of usability studies in the field of security and identify only five cases where a standard usability metric are applied: Polaris [12], graphical password systems [25], secure operating systems [39], secure Facebook chat [16], and our own previous studies on secure email [36]. In all cases, the selected metric was the System Usability Scale [7, 8].

The usability of authentication systems is very poorly understood. Bonneau et al. performed a full survey of the literature and selected a representative sample of authentication systems. We review the publications cited for this representative sample and found that only four of the twenty-three publications include a usability study [10, 24, 43, 46]. Moreover, only one of the four publications compared the proposed system against another authentication system [10]. These results are summarized in Table 2.1.

There are previous user studies that evaluate the usability of multiple authentication systems. This includes studies that looked at a homogeneous collection of systems (e.g., graphical password systems) as well as studies that compare new proposals to current password- or pin-based authentication. No prior study included a head-to-head comparison

www.manaraa.com

Category	Scheme	Year	Reference	User Study	Comparison[1]
Proxy	URSA	2008	[17]		
	Imposter	2004	[31]		
Federated	OpenID	2006	[32]		
	Passport	2000	[26]		
	BrowserID	2011	[21]		
	SAW	2007	[45]		
Graphical	PCCP	2012	[10]	✓	✓[2]
	PassGo	2006	[43]	✓	
Cognitive	GrIDsure	2011	[24]	✓	
	Weinshall	2006	[46]	✓	
	Hopper Blum	2001	[23]		
	Word Assoc.	1987	[40]		
Paper tokens	PIN+TAN	2004	[48]		
Hardware tokens	CAP reader	2009	[15]		
	Pico	2011	[41]		
Phone-based	Phoolproof	2006	[30]		
	MP-Auth	2011	[28]		
Biometric	Fingerprint	2007	[34]		
	Iris	2004	[11]		
	Voice	2006	[2]		
Biometric	Personal knowledge	2007	[34]		
	Preference-based	2004	[11]		
	Social re-auth	2006	[2]		

[1] Compared against other authentication proposals (not current password-based authentication).
[2] Between subject.

Table 2.1: Authentication proposals cited by Bonneau et al.

www.manaraa.com

of new authentication systems from two or more categories. The remainder of this chapter reports on key usability studies from the literature.

Chiason et al. [9] conducted a 26-person user study comparing two password managers: PwdHash and Password Multiplier. They found significant usability issues with both systems. Even though the original papers for both systems discussed usability, it required a formal study to reveal some significant usability challenges. Password Multiplier [20] included an informal usability analysis comparing it to earlier, lesser-known systems. PwdHash [35] included a five-person user study that identified any obvious problems that could be immediately addressed. It also contained a detailed usability discussion.

Tapas [29] is a password manager supporting dual-possession authentication. The evaluation of Tapas included a 30-person user study that compared it to two configurations of the Firefox password manager. Participants preferred Tapas and a follow-up study of ten users was conducted after improvements identified in the initial user study were made.

Deja Vu is a graphical password system proposed by Dhamija et al. [13]. The evaluation of Deja Vu included a user study that compared Deja Vu to both passwords and pins. This is the earliest study we identified that compared the proposed authentication method against current password-based authentication.

Kumar et al. [27] conducted the first comprehensive and comparative user study of secure device pairing methods. The study included 22 users comparing 11 device pairing methods (within-subjects). They used the System Usability Scale as a standard metric to compare the pairing methods. This is the most extensive evaluation we are aware of in terms of number of systems evaluated.

Shaub et al. [37] explored the space of graphical passwords by implementing five proposed systems from the literature. They conducted a user study involving 60 participants (between subjects) across six systems, including a PIN-based system that was used as a baseline. Their study resulted in a number of helpful insights and guidelines for designers of these kinds of systems.

www.manaraa.com

Sun et al. [42] conducted a user study of OpenID. They found problems with the design of OpenID that prevented users from forming correct mental models and ultimately led to mistakes. Based on these results they proposed a new system that wrapped OpenID to make it more understandable to users. This system proved more effective at helping users understand and correctly use OpenID.

www.manaraa.com

Chapter 3

Authentication Tournament

There exists a plethora of authentication systems, both old and new; nevertheless, adoption of these authentication systems continues to languish. Bonneau et al. found that this is largely because passwords have a unique combination of usability, deployability, and security that has been hard to surpass [5]. In order to attain widespread deployment it is essential that new authentication systems not only be more secure than passwords, but they must also provide tangible usability benefits that incentivize adoption.

While Bonneau et al. presented a heuristic-based approach for evaluating the usability of authentication schemes, it is also imperative that authentication systems are subjected to empirical usability analysis. As discussed in the Related Work chapter, very few authentication systems have been evaluated using an empirical study. Fewer still have been analyzed using a standard usability metric or compared to alternative authentication systems. This makes it impossible to determine which of the existing systems is most usable.

As a first step to answering these two questions, we conduct empirical usability studies on seven web authentication systems. Our studies are the first to study a heterogeneous collection of authentication proposals. We use the System Usability Scale to determine which system is most usable. Also, we structure our usability studies as a tournament to gather qualitative data from participants regarding which authentication features are most important to them.

www.manaraa.com

1) I think that I would like to use this system frequently.
2) I found the system unnecessarily complex.
3) I thought the system was easy to use.
4) I think that I would need the support of a technical person to be able to use this system.
5) I found the various functions in this system were well integrated.
6) I thought there was too much inconsistency in this system.
7) I would imagine that most people would learn to use this system very quickly.
8) I found the system very cumbersome to use.
9) I felt very confident using the system.
10) I needed to learn a lot of things before I could get going with this system.

Table 3.1: The ten SUS questions

	Questions 1,3,5,7,9	Questions 2,4,6,8,10
Strongly Agree	10	0
Agree	7.5	2.5
Neither Agree or Disagree	5	5
Disagree	2.5	7.5
Strongly Disagree	0	10

Table 3.2: SUS score card

3.1 System Usability Scale

The System Usability Scale (SUS) [7, 8] is a standard metric from the usability community that we adopt as part of our methodology. The SUS metric is a single numeric score between 0 and 100 (higher is better) which provides a rough estimate of a system's overall usability. To calculate a system's SUS score, participants first interact with the system and then answer ten questions relating to their experience (see Table 3.1). Answers are given using a five-point Likert scale (*strongly agree* to *strongly disagree*). The questions alternate between positive and negative statements about the system being tested. Participants' answers are assigned a scalar value (see Table 3.2) and then summed to produce the overall SUS score, and the system with the highest average SUS score is the most usable.

We select SUS as our standard usability metric because it is well regarded in the usability community and is reliable across different sets of participants. SUS has been used in hundreds of usability studies [4] and the original SUS paper [7] has been cited over 2,200

www.manaraa.com

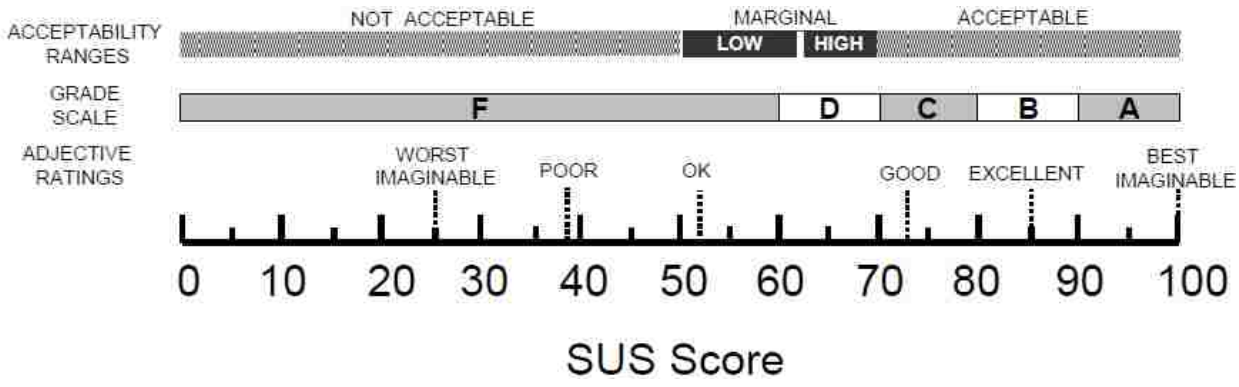

Figure 3.1: An adjective-oriented interpretation of SUS scores

times[1]. Our prior work has also shown that a system's SUS score is consistent across different sets of users [36]. Moreover, Tullis and Stetson compare SUS to four other usability metrics (three standard metrics from the usability literature and their own proprietary measure) and determined that SUS gives the most reliable results [44].

SUS produces a numeric score for a non-numeric measure (i.e., usability), making it difficult to intuitively understand how usable a system is based solely on its SUS score. As part of an empirical evaluation of SUS, Bangor et al. [4] reviewed SUS evaluations of 206 different systems and compared these scores against objective measurements of the various systems' success in order to derive adjective-based ratings for SUS scores. These ratings and their correlation to SUS scores are given in Figure 3.1. We report these adjective-based ratings along with SUS scores to provide readers with a better intuition of each system's usability.

3.2 Tournament Structure

To address our second research goal, *which features of authentication do users prefer and which do they dislike*, we have participants use multiple authentication systems and then have them provide feedback on their experience. We believe that after participants have used multiple systems that they will be better able to articulate their opinions on authentication. One

[1]Citation count retrieved from Google scholar on 2014/11/05.

www.manaraa.com

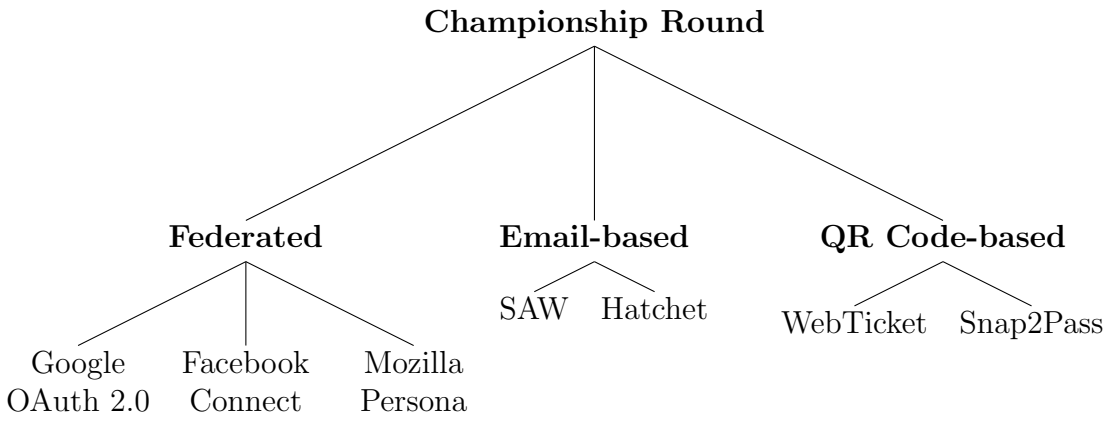

Figure 3.2: Authentication tournament bracket

option would be to perform a full combainatorial comparison, but this would be prohibitive in terms of time and cost. For example, if each system is tested by 20 participants,[2] and an individual participant tests two systems, it would require $\binom{7}{2} * 20 = 21 * 20 = 420$ participants, 27 person-days of effort, and $4,200 USD to complete the study.[3] Alternatively, having each participant using all the authentication systems could result in study fatigue that would bias the results.

Instead, we model our study after a tournament bracket. We first arrange the seven web authentication systems into three groups based on common features. These groups are federated single sign-on, email-based, and QR code-based. For each of the groups we conduct a separate usability study, and the system with the highest SUS score in each study is selected as a winner. The three winners are then compared to each other in a "championship round" usability study. This methodology allows us to gather qualitative user feedback from participants who have tested similar systems also participants who have tested dissimilar systems.

The breakdown of systems into the tournament bracket is given in Figure 3.2 and the remainder of this section describes the contestants in our authentication tournament.

[2]20 participants is an average sample size used in security usability studies.
[3]These costs grow factorially in the number of systems tested.

www.manaraa.com

3.2.1 Federated Single Sign-on

In federated single sign-on, all authentication responsibility is centralized in a single identity provider (IDP). Instead of websites maintaining their own collection of usernames and passwords, websites instead rely on the IDP to verify the identity of users visiting their website. The IDP is free to use whatever method it wants to authenticate users, though the three systems in our tournament all use usernames and passwords.

We select three federated single sign-on systems for inclusion in our tournament: Google OAuth 2.0, Facebook Connect, and Mozilla Persona. Google OAuth 2.0 and Facebook Connect are chosen because they are the only authentication systems other than current password-based authentication that are widely adopted. Since both Google and Facebook store personal information for users, it is possible that users might reject both systems for fear that their personal information will be leaked [33]. To address this concern, we also include Mozilla Persona, a federated single sign-on system that does not store users' personal information.

3.2.2 Email-based Single Sign-on

Email-based single sign-on is similar to federated single sign-on, but instead of centralizing authentication responsibilities into a single entity (e.g., Google, Facebook), they are instead delegated to email providers [19]. Users prove their identity by demonstrating their ability to either send or receive email. The advantage over federated single sign-on is that users have the freedom to choose which email providers they trust to be an identity provider.

We select two systems for this group: Simple Authentication for the Web (SAW) [45] and Hatchet. SAW authenticates a user by sending them an email with a link they can click to log into the website. To increase the security of authentication, SAW requires the user to click the link on the device they want to be authenticated on. Hatchet is a variant of SAW that we developed for the purpose of this study. Hatchet replaces the link sent in SAW with a one-time password (OTP). This OTP is then entered into the website the user is logging

www.manaraa.com

into.[4] Unlike SAW, Hatchet allows users to retrieve email on one device and be authenticated on another device.

3.2.3 QR Code-based

For our last group, we select the two most recent authentication proposals we are aware of: WebTicket [22] and Snap2Pass [14]. Both of these systems use QR codes and require a physical token to authenticate the user: a piece of paper and a smartphone respectively. In WebTicket, a user's credentials are encoded in a QR code which is printed and stored by the user (their WebTicket). The user authenticates to the website by scanning their WebTicket with their computer's webcam. WebTicket was originally presented as a browser plugin, but we have modified it to allow websites to deploy WebTicket for authentication. We believe that this is a more likely deployment scenario, as users have proven to be reticent to install browser plugins [33, 36].

Snap2Pass is a single sign-on authentication system where the user's phone acts as an IDP. The user first pairs their phone with the website by using the Snap2Pass application to scan a QR code provided by the website. Later, when the user authenticates to the website they are presented with another QR code to scan. After scanning this QR code, participants phones will verify the identity of the user to the website and the user is logged in.

[4]This use of OTPs is not unique to Hatchet [1], but to our knowledge there is no authentication system which employees OTPs and can be used to authenticate to arbitrary websites.

www.manaraa.com

Chapter 4

System Walkthroughs

This chapter walks through each of the seven authentication systems. In all cases, authentication begins when the participant clicks on the study website's login link. Steps in the authentication process are given as an ordered list. The figures provided in this section are screenshots of the authentication systems used in our studies and match exactly what participants in our studies see.

4.1 Google OAuth 2.0

1. The user clicks on the "Log in using Google" button (Figure 4.1).
2. Depending on whether the user is already authenticated with Google, one of three possible interactions occur:
   (a) If the user is not already logged into any Google accounts, then they are redirected to a Google login dialog (Figure 4.2).
   (b) If the user is logged into multiple Google accounts, then they are redirected to the account selection screen (Figure 4.3).
   (c) If the user is logged into exactly one Google account, then no interaction occurs and they continue to the next step.
3. The user is shown a dialog asking them to grant various permissions to the website (Figure 4.4). If the user has previously granted these permissions to the website then this step is skipped.

www.manaraa.com

4. The user is now in logged into the website.

Figure 4.1: Google OAuth 2.0 login button

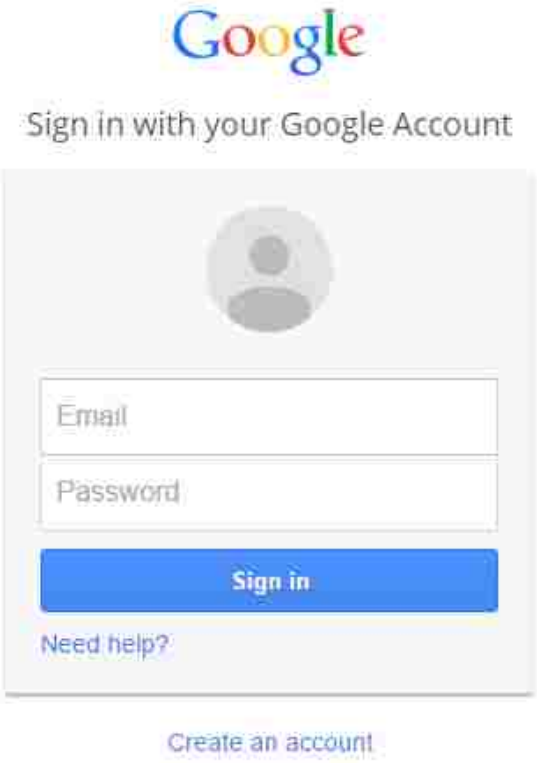

Figure 4.2: Google OAuth 2.0 login screen

www.manaraa.com

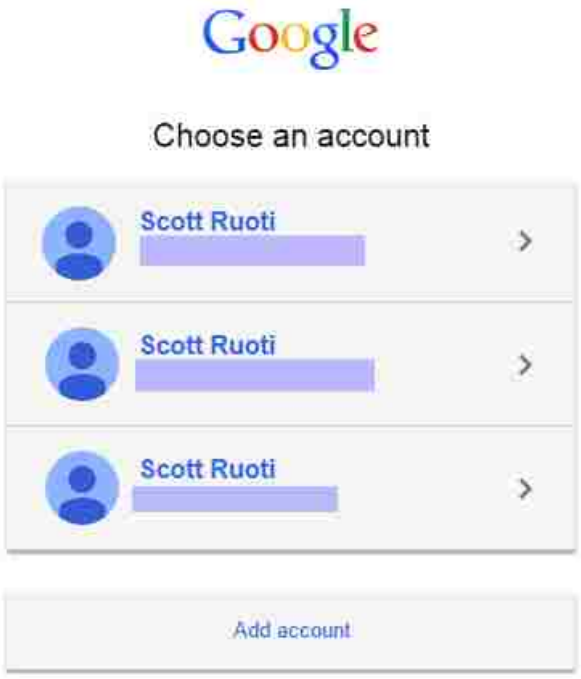

Figure 4.3: Google OAuth 2.0 user account selection screen

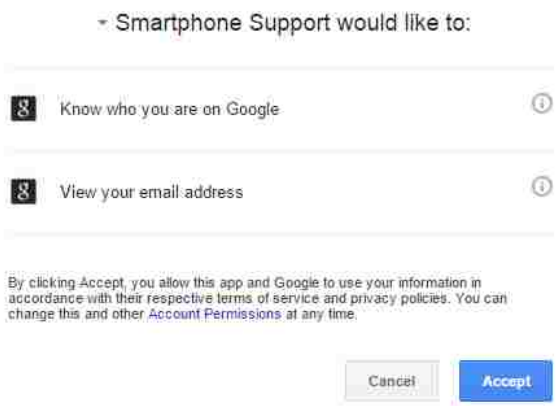

Figure 4.4: Google OAuth 2.0 permission grant screen

4.2 Facebook Connect

1. The user clicks on the "Log in using Facebook" button (Figure 4.5).

www.manaraa.com

2. If the user is not already logged into Facebook then they are prompted to do so (Figure 4.6).

3. The user is shown a dialog asking them to grant various permissions to the website (Figure 4.7). If the user has previously granted these permissions to the website then this step is skipped.

4. The user is now in logged into the website.

Figure 4.5: Facebook Connect login button

Figure 4.6: Facebook Connect login screen

www.manaraa.com

Figure 4.7: Facebook Connect permission grant screen

4.3 Mozilla Persona

1. The user clicks on the "Log in using Persona" button (Figure 4.8).
2. A popup is spawned and all further interaction happens within this popup.
3. Depending on whether the user has previously authenticated using Mozilla Persona, one of two possible interactions occur:

   (a) The user has previously authenticated using Mozilla Persona.

      i. The user is asked if they want to continue using the identity from the previous authentication (Figure 4.9). If they do not, then they move to step 3(b)i.

      ii. The user is asked whether they want Persona to remember their choice from step 3(a)i in the future (Figure 4.10).

   (b) The user has not previously authenticated using Mozilla Persona.

      i. The user is asked to enter their email address (Figure 4.12). One of three interactions then occur:

www.manaraa.com

A. If the email address is a GMail or Yahoo Mail addresses, then the user is asked to verify their ownership of the email account using OAuth (Gmail – Figure 4.13, Yahoo – Figure 4.14).

B. If this is the first time the user has used this email address with Persona, then they are asked to create a Mozilla Persona account (Figure 4.15). The user verifies ownership of their email address by clicking on a link sent to the email (Figure 4.16).

C. The user is prompted to enter the password they selected when creating their Mozilla Persona account (Figure 4.17).

4. The popup indicates that it is signing the user into the website and then closes (Figure 4.11).

5. The user is now in logged into the website.

Unlike the other two federated single sign-on systems, Mozilla Persona does not have a permission grant dialog.

Figure 4.8: Mozilla Persona login button

Figure 4.9: Mozilla Persona account confirmation

www.manaraa.com

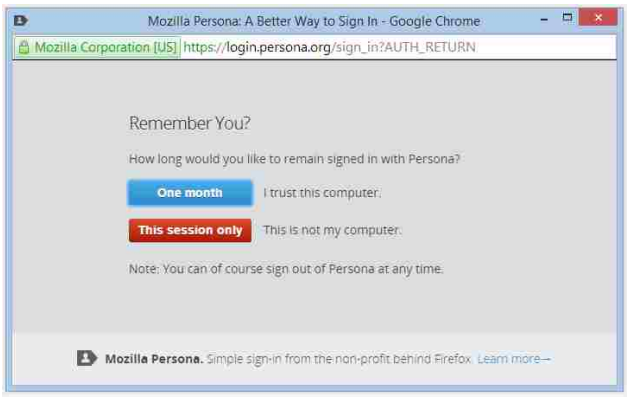

Figure 4.10: Mozilla Persona remember-me option

Figure 4.11: Mozilla Persona authentication complete dialog

Figure 4.12: Mozilla Persona email entry

www.manaraa.com

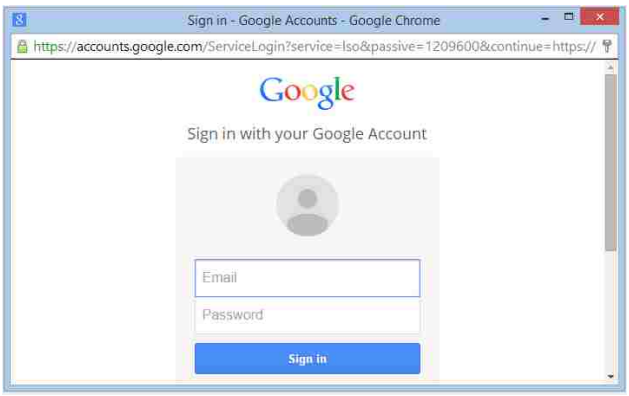

Figure 4.13: Mozilla Persona account verification (Google)

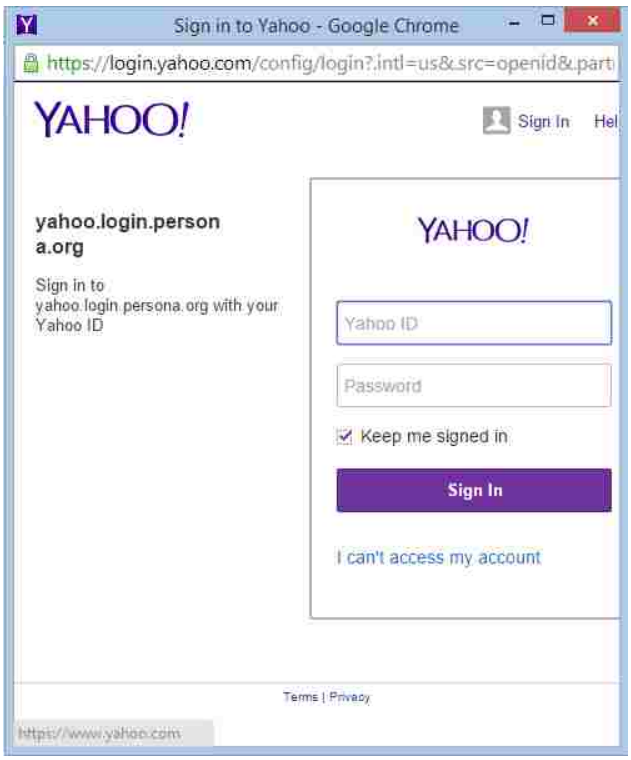

Figure 4.14: Mozilla Persona account verification (Yahoo)

www.manaraa.com

Figure 4.15: Mozilla Persona account creation

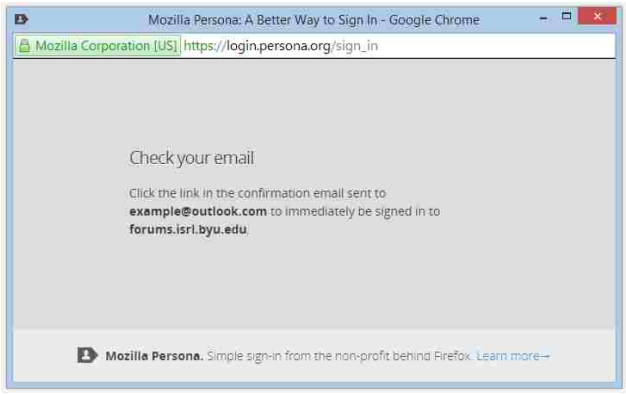

Figure 4.16: Mozilla Persona account verification (Email-based)

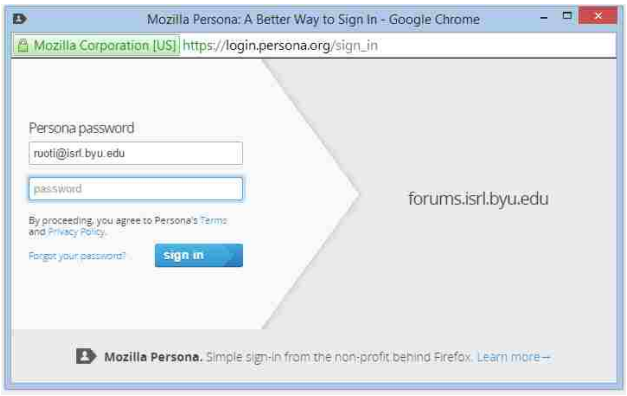

Figure 4.17: Mozilla Persona login dialog

www.manaraa.com

4.4 Simple Authentication for the Web

1. The user clicks on the "Log in using SAW" button (Figure 4.18).
2. The user is instructed to check their email for a link to complete authentication (Figure 4.19).
3. The user opens the email they were sent and clicks on the link it contains (Figure 4.20 and Figure 4.21).
4. The user sees a page informing them that they have been logged into the website (Figure 4.22).
5. The user is now in logged into the website.

Figure 4.18: SAW login form

Figure 4.19: SAW login message

www.manaraa.com

Figure 4.20: SAW email message (Inbox)

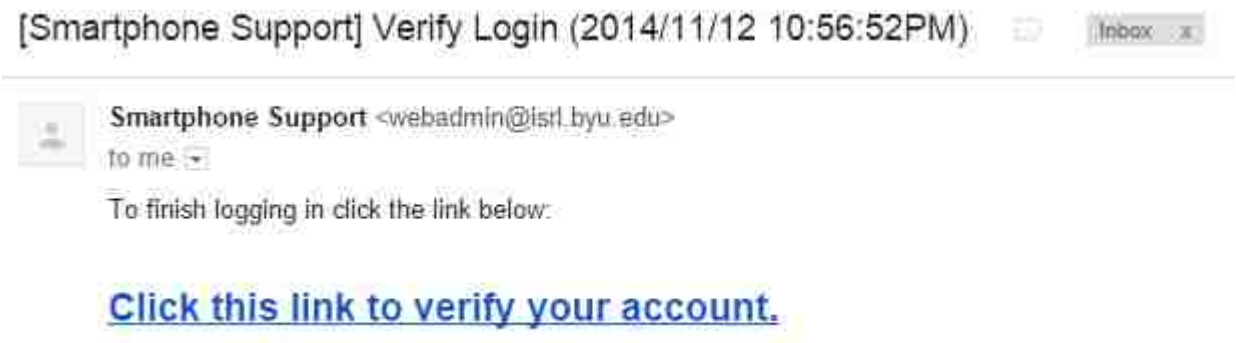

Figure 4.21: SAW email message (Full)

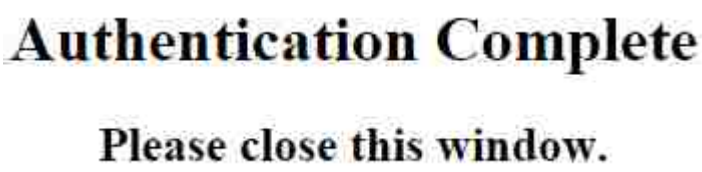

Figure 4.22: SAW completion screen

4.5 Hatchet

1. The user clicks on the "Log in using Hatchet" button (Figure 4.23).
2. The user is instructed to check their email for a code to complete authentication (Figure 4.24).
3. The user opens the email they were sent and retrieves their code. This can be done on a phone (Figure 4.25) or a webmail client (Figure 4.26 and Figure 4.27).
4. The user enters their code into dialog from step 2 (Figure 4.24).

www.manaraa.com

5. The user is now in logged into the website.

Figure 4.23: Hatchet login form

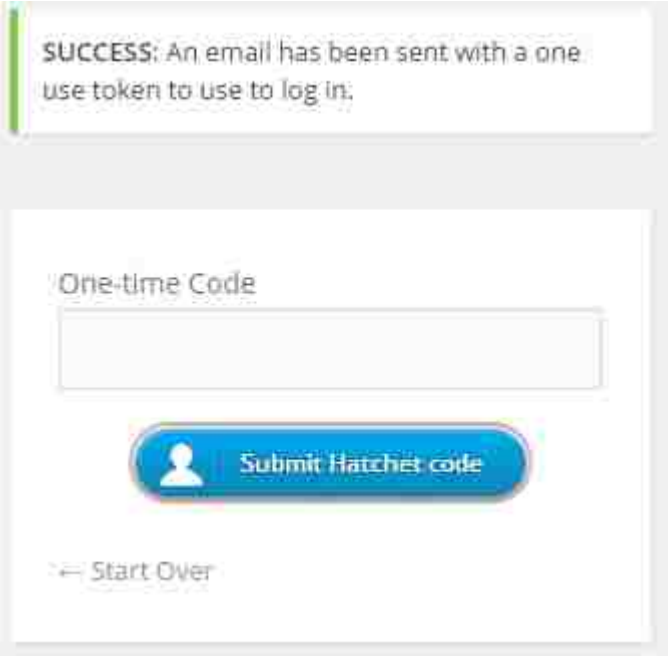

Figure 4.24: Hatchet code entry dialog

www.manaraa.com

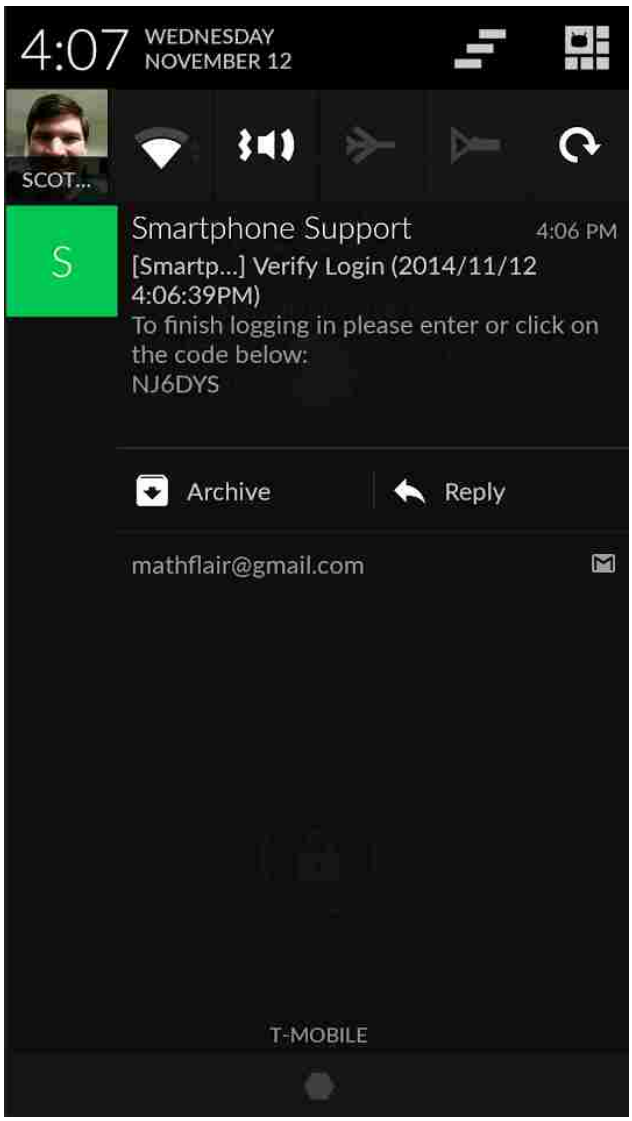

Figure 4.25: Hatchet email message (Phone)

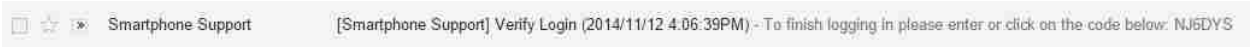

Figure 4.26: Hatchet email message (Inbox)

www.manaraa.com

Figure 4.27: Hatchet email message (Full)

4.6 WebTicket

Before authenticating with WebTicket, the user first prints out a WebTicket provided to them by the website (Figure 4.28). The below steps for authentication assume that the user has already printed a WebTicket.

1. The user is presented with a video feed of their webcam. They use this video feed to center and scan their WebTicket (Figure 4.29).
2. The user is now in logged into the website.

www.manaraa.com

Figure 4.28: A WebTicket

www.manaraa.com

Figure 4.29: WebTicket webcam video feed

4.7 Snap2Pass

Before authenticating with Snap2Pass, a user needs to perform several actions:

1. The user installs the Snap2Pass application on their smartphone.
2. The website provides a QR code that the user can scan to pair the phone with the website (Figure 4.30).
3. The user clicks on the "Scan QR Code" button in the Snap2Pass application and scans the provided QR code (Figure 4.31, Figure 4.32).
4. The user verifies the pairing operation (Figure 4.33).
5. The website is added to the list of accounts in the Snap2Pass application (Figure 4.34)

www.manaraa.com

The below steps for authentication assume that the user has already completed the above pairing process.

1. The website provides the user with a QR code (Figure 4.35). The user scans this QR code with the Snap2Pass application.
2. The user is prompted by the Snap2Pass application to confirm login (Figure 4.36).
3. The user is now in logged into the website.

Figure 4.30: Snap2Pass registration QR code

www.manaraa.com

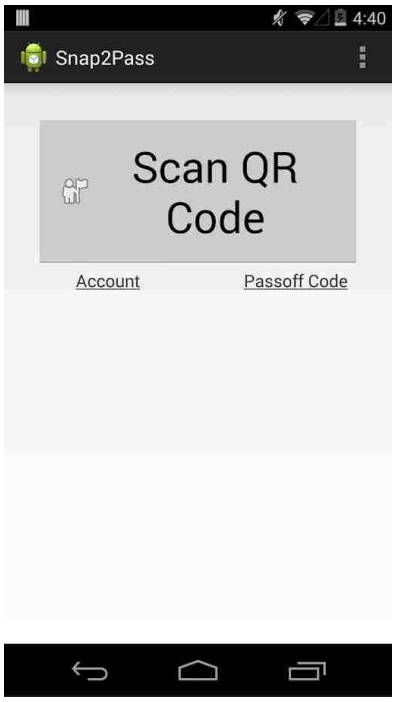

Figure 4.31: Snap2Pass Android application

Figure 4.32: Snap2Pass application – QR code scanner

www.manaraa.com

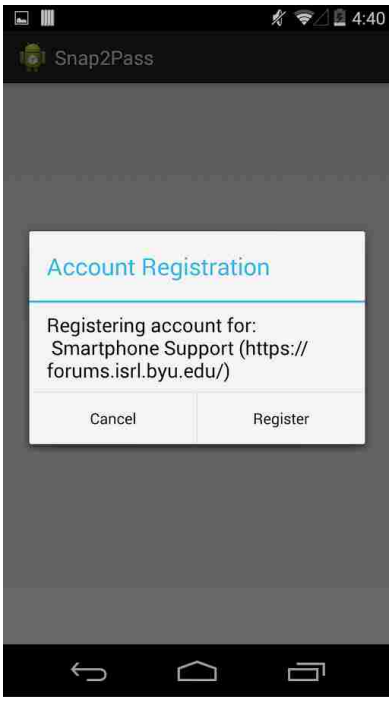

Figure 4.33: Snap2Pass application – registration confirmation

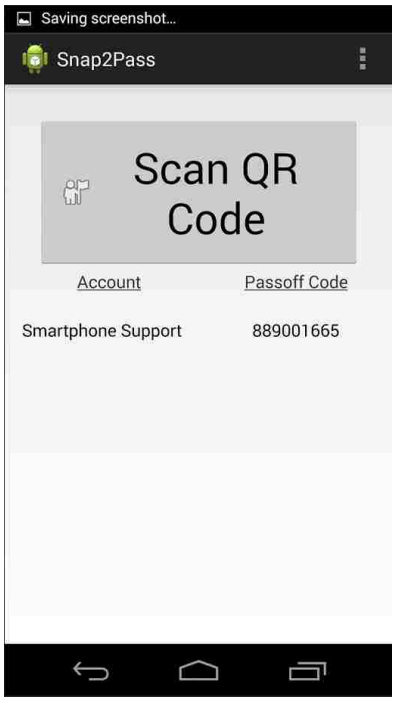

Figure 4.34: Snap2Pass application – accounts page

www.manaraa.com

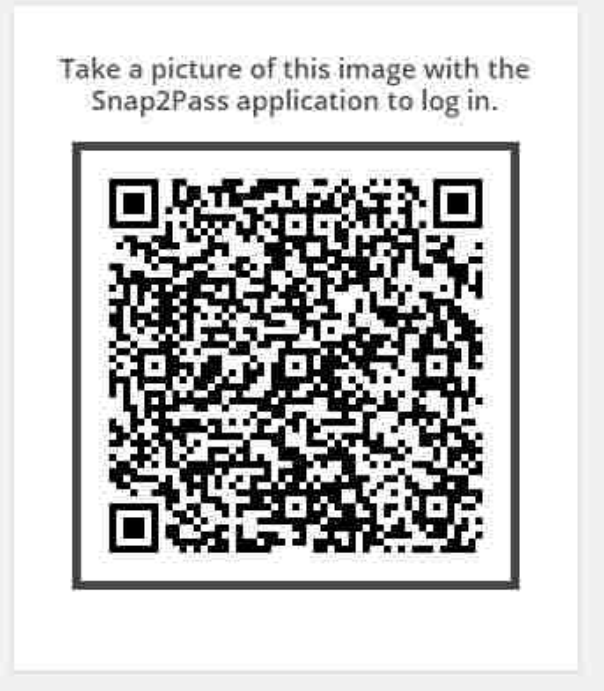

Figure 4.35: Snap2Pass login QR code

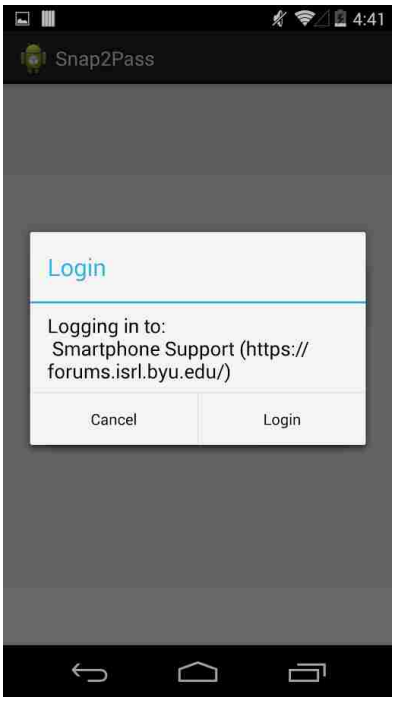

Figure 4.36: Snap2Pass application – login confirmation

www.manaraa.com

Chapter 5

Methodology

During the summer and fall of 2014, we conduct four studies analyzing the usability of seven web authentication systems. The studies vary as to which authentication systems are tested, but otherwise the content of the studies remains constant. This chapter gives an overview of the studies and describes the task design, study questionnaire, study development, and limitations.

5.1 Study Setup

The four studies were conducted between June and October 2014: June 24–July 12, July 28–August 23, October 7–October 11, October 13–October 24. The first three studies evaluate the federated, email-based, and QR code-based groups respectively, and the fourth study is the "championship round" usability study. In the first study (federated), participants are randomly assigned two of the three authentication systems in the group, and in second (email-based) and third studies (QR code-based) participants were assigned to use both systems in the group. In the fourth study ("championship round"), participants are assigned all three systems.[1]

[1] We modified the study to assign participants three systems for two reasons: (1) in the first three studies participants showed no signs of study fatigue after evaluating two authentication systems and (2) we were interested in the qualitative responses of participants who had been assigned three heterogeneous authentication systems.

www.manaraa.com

In total, 106 individuals participate in our studies: 24 participants in the first study, 20 participants in the second study,[2] 27 participants in the third study and 35 participants in the fourth study. Each individual is allowed to participate in only one of the four studies. Participants took a minimum of 20 minutes and a maximum of 45 minutes to complete their study and are compensated $10 USD for their efforts. When using Snap2Pass, participants are provided with a Nexus 5 smartphone with the Snap2Pass application pre-installed. When using WebTicket, participants are provided with a black and white laser printer, a pair of scissors, and a 1080p webcam.

5.1.1 Quality Control

The results for eight participants are discarded for various reasons:

- Two participants, both in the second study (email-based), had the authentication emails generated by SAW marked as spam.[3] The survey coordinator was unable to resolve this problem and the participants were unable to complete the study.
- Three participants, one in the third study (QR code-based) and two in the fourth study ("championship round"), were non-native English speakers and were unable to understand the assigned tasks.
- Three participants, one in the third study (QR code-based) and two in the fourth study ("championship round"), skipped a task and did not finish registering a necessary account. The study coordinator was unable to resolve this problem and the participants were unable to complete the study.

After removing results from these 8 participants we are left with results from 98 participants: 24 participants in the first study (federated), 18 in the second study (email-

[2]We are unsure why fewer students signed up for the second study, though we speculate that it might be due to the fact that the majority of our participants were undergraduate students at Brigham Young University and finals for that university's Summer term fell on the thirteenth and fourteenth of August.

[3]Emails were marked as spam because they contained both the words "bank" and "click on the link". Different wording could have avoided this problem.

www.manaraa.com

	Gender		Age		Technical Skill		
	Male	Female	18–24 years old	25–34 years old	Beginner	Intermediate	Advanced
Federated (n = 24)	58% 14	42% 10	83% 20	17% 4	13% 3	79% 19	8% 2
Email (n = 18)	67% 12	33% 6	78% 14	22% 4	28% 5	72% 13	0% 0
QR Code (n = 25)	52% 13	48% 12	88% 22	12% 3	12% 3	60% 15	28% 7
Championship (n = 30)[1]	67% 20	33% 10	77% 23	23% 7	13% 4	83% 25	4% 1
Total (n = 97)[1]	62% 59	38% 38	81% 79	29% 18	15% 15	75% 73	10% 9

[1] One participant in the QR code-based group did not provide demographic, explaining the smaller number of participants reported in this table.

Table 5.1: Participant demographics

based), 25 in the third study (QR code-based), and 30 in the fourth study ("championship round"). The remainder of this paper will refer exclusively to these 98 participants.

5.1.2 Participants Demographics

We recruit participants for our study at Brigham Young University. All participants are affiliated with Brigham Young University,[4] with the overwhelming majority being undergraduate students: undergraduate students (93; 96%), graduate students (3; 3%), faculty (1; 1%), did not provide demographic information (1; 1%). Participants had a variety of majors, 51 in total, with the highest percentage studying exercise science (8 participants). No other major had more than five participants. Participants were asked to self report their level of technical skill, with most reporting an intermediate level of knowledge.

[4]We did not require this affiliation.

www.manaraa.com

5.2 Task Design

We built two WordPress websites for the purpose of our studies: a **forum** website where users could get help with smartphones,[5] and a **bank** website.[6] We chose these two types of websites because they represented diametrically different information assurance needs. At a forum website there is little personal information stored, and so even if the user's account is stolen there is still only minimal risk of harm. Conversely, users have been shown to be extremely cautious when it comes to online bank accounts [38]. Studying websites with different information assurance needs allows us to examine whether users are amenable to a given authentication system being deployed to all websites, or only to websites that do not store personal information.

During the studies, participants are assigned two or three authentication systems. For each authentication system, participants were given six tasks to complete (three for each website). For each task, participants were instructed on how to use the website to complete the task. Participants were not instructed on how to use any of the authentication systems, as one aspect of usability is how well an authentication system facilitates a novice user. Between each task, participants are logged out of both websites, ensuring that participants use the assigned authentication system for each task.

The text of these tasks is given verbatim in Appendix A.3. Below is a summary of the six tasks:

Task 1. Participants create a new account at the **forum** website using the assigned authentication system.

Task 2. Participants modify an existing **bank** account to allow login using the assigned authentication system.

[5] `https://forums.isrl.byu.edu`
[6] `https://bank.isrl.byu.edu`

www.manaraa.com

Task 3. Participants log into the **forum** website and create a post in the "New User" forums.

Task 4. Participants log into the **bank** website and look up their checking account balance.

Task 5. Participants log into the **forum** website and search for a specific post.

Task 6. Participants log into the **bank** website and transferr money from one account to another.

5.2.1 Authentication System Implementation

For this study we implemented all seven authentication systems. We did this for two reasons: first, existing implementations of SAW, Hatchet, WebTicket and Snap2Pass are non-existent[7] and second, by implementing the systems ourselves we could assure a consistent user experience.

Source code for our implementations of these systems, as well as the **forum** and **bank** websites, is available at `https://bitbucket.org/isrlauth/battle-website`.

5.3 Study Questionnaire

We administer our study using Qualtrics' survey software. The survey begins with an introduction and a set of demographic questions.

Participants are then instructed to complete the study tasks for a particular authentication system. After completing the six tasks, participants answer the ten SUS questions. Next, participants describe which features of the assigned authentication system they enjoy and which they would change. Lastly, participants indicate whether they would prefer to use the assigned authentication system over current password-based authentication and why. This process is then repeated for each assigned authentication system.

[7]We contacted the authors of WebTicket and Snap2Pass and requested their implementations, but we received no reply.

www.manaraa.com

At the end of the survey, participants were asked several final questions. First, participants were asked what their favorite authentication system was: whether it was one of the systems they tested or current password-based authentication. They were also asked to explain why the selected system was their favorite. Lastly, participants were asked to describe their ideal authentication system. While most participants are not engineers, we believe that asking this question serves two purposes: (1) it allows participants to synthesize all the systems they have used and extract what they consider the best from each and (2) it allows participants to mention authentication features that excite them but are not a part of any of the assigned systems.

In addition to the questionnaire responses, we record participants' screens and use this data to calculate mean time to authenticate. Due to concerns raised by the IRB about video recording participants, we were unable to gather mean time to authenticate results for the second task of Snap2Pass, as authentication was completed on the phone.[8]

5.4 Survey Development

After implementing the federated single sign-on systems, we developed the study tasks and questionnaire. We then had a convenience sample of nine individuals from our research institute complete the study. Based on their feedback we made some alterations to wording of the task instructions. After making these changes we began the first usability study (federated).

During this first study (federated), we noticed that a small number of participants were confused about how to complete the second task. In each case, the study coordinator was able to explain to them where to go on the **bank** website to complete the task and we did not need to discard any of the participant's responses. To avoid having participants ask the study coordinator for assistance in the three remaining studies we made a slight

[8]It may be possible to instrument the Snap2Pass application to allow calculation of the mean time to authenticate, but we were unable to solve this problem in time for the studies.

www.manaraa.com

visual modification to the **bank** website. This change was universal for all the authentication systems and did not affect their functionality.

During the second usability study (email-based), Gmail began marking some of the authentication emails as spam. To our knowledge, four participants encountered this problem. This problem prevented the first two participants from completing the study and their results were discarded. For the latter two participants, the study coordinator was able to diagnose the problem and help them complete the study. In the fourth study, which once again included SAW, we added a note to the **bank** tasks to indicate to participants that this might occur and how to remedy the problem.

All four of the studies were approved by the Institutional Review Board of Brigham Young University.

5.5 Limitations

While our studies included students with a diverse set of majors and technical expertise, it would be beneficial for future studies to test authentication systems using a non-student population. It is likely that a large number of participants are already familiar with Google OAuth 2.0 and Facebook Connect and this may have affected their opinions. Also, we only study seven authentication systems, which is clearly insufficient to classify the usability of more than a small fraction of authentication proposals. Future research could examine different authentication systems in order to increase knowledge on the usability of authentication systems and help determine which systems are best-in-class and which system has the best overall usability.

www.manaraa.com

Chapter 6

Results

In this chapter we report the quantitative results we gathered. Table 6.1 gives the SUS scores from the four usability studies and summarizes participants' authentication system preferences. Table 6.2 records whether the difference in the systems' SUS scores is statistically significant. Finally, Table 6.3 reports the mean time to-authenticate for each system.

The remainder of this chapter breaks down the individual results for each of the four usability studies. As mentioned in Section 3.1, in order to provide the reader with great context, in addition to the SUS scores we also report where these scores fall on Bangor's adjective-based scale [3, 4]. Participants' responses are recorded verbatim in the appendix (federated – Appendix B, email-based – Appendix C, QR code-based – Appendix D, and "championship round" – Appendix E).

6.1 First Study – Federated

The SUS scores for Google OAuth 2.0, Facebook Connect, and Mozilla Persona were between 71 and 72, and the difference is not statistically significant. On Bangor's scale, all three systems are labeled as "good," classified as acceptable, and receive a C grade.

Both Facebook Connect and Google OAuth 2.0 had similar registration and authentication times. In contrast, Mozilla Persona's registration and authentication times were two and four times greater, respectively. Even though there was a clear difference in mean time to authenticate, participants never mention this difference in their qualitative responses.

www.manaraa.com

		SUS			Better than Passwords		Is Participants Favorite System
		Mean	Standard Deviation	Median	Yes	Maybe	
n=16	**Google**	**72.0**	12.4	72.5	**31%**	38%	**31%**
	Facebook	71.4	13.5	72.5	13%	31%	25%
	Mozilla	71.8	10.8	71.3	**31%**	44%	25%
n=18	**SAW**	**61.0**	17.5	62.5	**28%**	28%	**44%**
	Hatchet	53.5	16.4	52.5	22%	44%	17%
n=25	WebTicket	57.9	16.9	60	20%	28%	4%
	Snap2Pass	**75.7**	17.8	82.5	**36%**	40%	**76%**
n=31	**Google**[1]	**75.0**	14.8	77.5	**26%**	32%	**29%**
	SAW[1]	53.2	16.2	55	6%	29%	0%
	Snap2Pass[1]	68.4	16.7	70	**26%**	39%	**29%**

The best performing system and metric for each usability study is given in **bold**. For the second, third, and fourth studies, participants used all available authentication systems and so $100\% - \Sigma(Favorite\ System)$ gives the percent of participants who preferred current password-based authentication to any of the assigned authentication systems.

[1] Championship round.

Table 6.1: SUS scores and participant preferences

www.manaraa.com

	Google	Facebook	Mozilla	SAW	Hatchet	WebTicket	Snap2Pass	Google[1]	SAW[1]	Snap2Pass[1]
Google	—	.89	.94	.04	<.01	<.01	.47	.50	<.01	.45
Facebook	.89	—	.94	.06	<.01	.01	.42	.42	<.01	.54
Mozilla	.94	.94	—	.04	<.01	<.01	.43	.43	<.01	.47
SAW	.04	.06	.04	—	.05	.57	.01	<.01	.12	.15
Hatchet	<.01	<.01	<.01	<.05	—	.40	<.01	<.01	.96	<.01
WebTicket	<.01	.01	<.01	.57	.40	—	<.01	<.01	.30	<.01
Snap2Pass	.47	.42	.43	.01	<.01	<.01	—	.87	<.01	.12
Google[1]	.50	.42	.43	<.01	<.01	<.01	.87	—	<.01	.08
SAW[1]	<.01	<.01	<.01	.12	.96	.30	<.01	<.01	—	<.01
Snap2Pass[1]	.45	.54	.47	.15	<.01	<.01	.12	.08	<.01	—

2-tailed t-test. The participants for the second, third, and fourth study used all available authentication systems and within these groups statistical significance is calculated using the same population, while other significance values are calculated using equal variance. Only statistically significant results at the $p = .05$ level are shaded.

Row scheme scored higher than column scheme

Row scheme scored worse than column scheme

[1] Championship round.

Table 6.2: Comparison of system SUS scores

www.manaraa.com

		Registration			Authentication				
		Task 1	Task 2	Average	Task 3	Task 4	Task 5	Task 6	Average
n=16	Google	46	43	44	3	10	2	2	**4**
	Facebook	53	23	**38**	7	6	3	4	**5**
	Mozilla	80	81	81	22	30	15	10	19
n=18	SAW	72	30	51	22	17	14	15	**17**
	Hatchet	51	29	**40**	27	20	19	17	21
n=31	Google[1]	51	38	**44**	3	2	2	2	**2**
	SAW[1]	55	34	**45**	62	42	17	25	36
	Snap2Pass[1]	76	-	76	13	14	13	11	13

All times are reported in seconds. In the third study (QR code-based) the video recording software failed and there are no results from that study.

[1] Championship round.

Table 6.3: Mean time to authenticate

In deciding which authentication system they prefer, participants list trust in the federating party (i.e., Google, Facebook, Mozilla) as a key component. Many participants are hesitant to use Facebook Connect for fear that their social networking data would also be given to the website. Similarly, some participants are concerned that using Google OAuth 2.0 might increase the likelihood of their e-mail being hacked. There is little worry about Mozilla Persona in this regard.

According to our methodology, the winner of each usability study was decided based on highest SUS score. Since the difference of the all three systems' SUS scores is not statistically significant, we attempt to break this tie based on which system has the highest number of participants who rate it as their favorite system. Once again, we find that all three systems perform similarly (Google – six participants, Facebook – five participants, Mozilla – five participants), and so we declare all three systems as winners. We still need a single system to move forward in the tournament and so we select Google OAuth 2.0, which had both

www.manaraa.com

the highest SUS score and the highest number of participants who rated it as their favorite system.

6.2 Second Study – Email-based

SAW's SUS score was higher than Hatchet's SUS score and this difference was statistically significant. As such, SUS is the winner of this round. Still, SAW's usability is not impressive. According to Bangor's scale, SAW's SUS score of 61 is labled as "good," is classified as having low-marginal acceptability, and given a D grade. Similarly, Hatchet is labeled as "OK," is classified as having low-marginal acceptability, and is given a failing grade.

While SAW was clearly the SUS champion in this category, participants using Hatchet and SAW took roughly equal amounts of time to register and authenticate (differences not statistically significant: registration – $p = 0.46$, authentication – $p = .27$).

6.3 Third Study – QR Code-based

Snap2Pass was the clear winner of this group, with a SUS score 17.8 points higher than WebTicket's SUS score (this difference was statistically significant). Additionally, only one participant indicated they would prefer WebTicket to Snap2Pass. According to Bangor's scale, Snap2Pass is labeled as "excellent," is classified as acceptable, and receives a C grade. In contrast, WebTicket is labeled as "good," is classified as having low-marginal acceptability, and receives a D grade.

During the study, the video capture software corrupted all the screen records making it impossible to report mean time to authenticate. Participants' qualitative responses indicate that they felt both systems were fast, though comments made after the study indicate that they felt Snap2Pass was the faster of the two systems. These comments match the observations of the study coordinator who observed a significant number of participants struggle to authenticate quickly with WebTicket.

www.manaraa.com

Two statistics in this study (QR code-based) vary significantly from the statistics in the other three usability studies. First, the median SUS score for Snap2Pass is significantly higher than its mean SUS score, indicating that their are several outliers who rate Snap2Pass very negatively, pulling its average down. In all the other results, including the fourth study when Snap2Pass is evaluated a second time, SUS scores are normally distributed. Second, 76% of participants in this study indicated that they are willing to replace current password-based authentication with Snap2Pass. In the other three studies, only 60% of individuals indicated they were willing to replace current password-based authentication.

We are unsure as to what these anomalies mean, but report them in the interest of full disclosure. We are also unsure what caused these results, though we speculate it could be related to the fact that the second study had over a quarter of participants who rated themselves as having advanced technical skill (see Table 5.1).

6.4 Fourth Study – "Championship Round"

The "championship round" usability study consisted of the winners from the first three usability studies: Google OAuth 2.0, SAW, and Snap2Pass. The results are a tie between Google OAuth 2.0 and Snap2Pass, with SAW the clear loser. We apply the tie-break criteria from the first study (see Section 6.1), but the same number of participants choose Google OAuth 2.0 and Snap2Pass as their favorite system. For all three systems, there is no statistically significant difference between their scores in this study ("championship round") and the previous three studies.

Since all three federated single sign-on systems tied in the first study, we declare federated single sign-on (collectively) and Snap2Pass to be the winners of our tournament.

www.manaraa.com

Chapter 7

Discussion

In this chapter we begin with a discussion of SUS. We follow this with various insights gained from participants' qualitative responses. Finally, we report lessons learned while implementing the seven authentication systems.

7.1 System Usability Scale

SUS proves to be a highly reliable metric. SUS scores for Google OAuth 2.0, SAW, and Snap2Pass were consistent between the first three studies and the "championship round" study.[1] Within a single study, SUS scores for the systems are consistent regardless of the order in which participants use the systems, with all differences failing to be statistically significant.

Moreover, SUS is a good predictor of which system participants select as their favorite. In the first study (federated), all three federated systems had similar SUS scores, and an equal number of participants selected each of the three systems as their favorite. Likewise, in the second (email-based) and third (QR code-based) studies, when one system's SUS score was higher than the other system's SUS score, participants largely preferred the system with the higher SUS score. Most interesting, these preferences held between different sets of participants. The SUS score for Google OAuth 2.0 and Snap2Pass are similar and the difference between the two is not statistically significant (see Table 6.2). This would indicate

[1]The differences in SUS scores is not statistically significant (see Table 6.2).

www.manaraa.com

that equal number of participants should prefer both systems, and this is indeed the case when they are evaluated in the "championship round" study (see Table 6.1).

While mean time to authenticate is reported in nearly every authentication usability study, our results indicate that mean time to authentication is actually a poor measure of overall usability or participants' preferences. In the first study, Mozilla Persona had a much higher mean time to authenticate than either Google OAuth 2.0 or Facebook Connect, yet all three had similar SUS scores and were equally preferred by participants. Similarly, SAW and Hatchet did not differ significantly in mean time to authentication, yet there was a clear distinction in both systems SUS scores and participants' preferences.

Based on these results, we suggest that an empirical analysis using SUS be required for all future authentication proposal. This allows new systems' SUS scores to be compared against existing proposals and validate whether these new proposals are improving upon the state-of-the-art. Additionally, we recommend that all new systems achieve a SUS score of 70 before they receive serious consideration. In our studies, only systems with a score of at least 70 (Google OAuth 2.0, Facebook Connect, Mozilla Persona, Snap2Pass) received consistently positive reviews from participants.

7.2 Transparency

Upon reviewing the results of the usability study (federated) we found that participants preferred systems that were transparent and required minimal interaction.[2] To verify that transparency improves usability, we administered a mini-study to the end of the second usability study (email-based). After completing the questionnaire for the second study, participants are then assigned a modified version of SAW. This modified version of SAW automates the process of retrieving and clicking links sent to user's email. Before beginning the six tasks, participants entered their email credentials into the new authentication system, and from then on whenever they click the "Login with SAW" button (see Figure 4.18) they

[2]In the usable security literature, transparency refers to hiding implementation details from users.

www.manaraa.com

would be immediately logged into the website. Participants complete the same six tasks and answer the same questions as they did for all the other authentication systems.

The usability improvements of this modified version of SAW are striking. The modified version had a mean SUS score of 73.1, a standard deviation of 10.1, and median score of 75. This is an increase of 12.1 points over SAW's SUS score, and the difference is significant at the $p = 0.01$ significance level. This shows that transparency has a strong effect on perceived usability.

While these results demonstrate that transparency increases usability, transparency was not without its trade-offs. Minimal interaction with the authentication system prevents participants from understanding how the authentication system functioned and many participants have trouble trusting what they don't understand:

> *"I would like to understand more about how it works up-front. It doesn't feel secure."*

> *"If I understood how the system would prevent someone other than me from logging in I would use it."*

> *"I think it was very straightforward to use. Once again like with the other system, perhaps an explanation of how it protected information would give me more confidence in using it."*

This issue of transparency leading to confusion and lack of trust also appeared in our earlier research on secure webmail [36]. Future research could look closely at these trade-offs to discover what is an appropriate level of transparency in authentication.

7.3 Single Sign-on Protocols

Participants like the speed and convenience of single sign-on, though their qualitative responses also provide details about how existing systems could be improved.

www.manaraa.com

7.3.1 Additional Low-entropy Passwords

Participants liked having a single account was used to authenticate to multiple websites. Still, some participants were worried about the risks associated with only having one account for all their websites:

> *"The simplicity is also a downside–after the first log-in, you only have to press 'log in' and it doesn't ask you any verifying information. That doesn't seem like a very secure system. For something inconsequential like a social media site or a blog, I wouldn't mind it, but I want a MUCH more secure authentication system for my bank account. If my google account gets hacked, I assume all the connected accounts that use it to log in can also be jacked. I don't want to take that risk with my important accounts."*

Participants suggest a novel approach to solving this problem. To increase the security of a website, participants propose augmenting single sign-on with a low-entropy password shared with the website (e.g., pin). Security is provided by the high-entropy password of the single sign-on account, yet in the case of an account compromise attackers would be unaware of the low-entropy passwords and be unable to gain access to the website. The cognitive burden for users is also low, as they only need to remember a single high-entropy password, while all other passwords are low-entropy and easily remembered. This is an interesting avenue for future research to explore.

7.3.2 Reputation

With federated single sign-on, the reputation of the provider was key. Qualitative responses from participants indicated that trust in a federated single sign-on system was based on the federating identity provider (IDP) (e.g., Google, Faceboook). Participants often cite their opinions of the federating IDP when explaining why they preferr one system to another:

www.manaraa.com

"I would be worried about security. I've heard that Facebook is 'relatively' easy to hack. I would want to be sure that it was all secure before I started using it."

"I trust Google with my passwords."

7.3.3 Dedicated Identity Providers

Some participants prefer that the IDP only handle authentication and not store sensitive information. For example, one participant stated,

"It would be it's own company (not tied to my email, or social network accounts) but it would have the ability to be embedded into webpages as a login option since sometimes last pass doesn't do a great job of automatically recognizing where to fill in login info."

If they were forced to use Google or Facebook as their IDP, one participant indicated that they would create a new account used for authentication only:

"I would make an account separate from my social network and mail specifically for functions like banking etc."

7.4 The Coolness Factor

When participants described what authentication features they were most interested in, they often referred to the "coolness" of that feature. "Coolness" was often related to how different and innovative the technology was when compared to current password-based authentication. For example, participants love that Snap2Pass allows them to use their smartphones and obviates the need for passwords:

"Man was that cool!"

"Also, the feel of it made me enjoy doing it. I felt technologically literate and the app felt futuristic as a whole, which I enjoyed."

www.manaraa.com

"I thought the technology was cool. You can snap a code to sign yourself in!"

7.4.1 Biometrics

None of the seven authentication systems we analyzed used biometric-based authentication; nevertheless, over a quarter of participants (28; 29%) discuss biometrics as part of their ideal authentication system. In nearly every case, biometrics were described as being "cool:"

"A fingerprint system would be cool."

"retinal scanner so i just sit in front of my computer and it scans my eye. dope."

Participants liked biometrics because they did not involve an authentication factor that could be forgotten, lost, or stolen:

"The ideal system would scan some part of my body - either eye or thumb - because these are literally ALWAYS with me."

Participants also thought that biometrics were more difficult for hackers to compromise:

"People can hack accounts, but they can't fake your eye-scan pattern"

The list of suggested biometrics are fingerprint, facial, retinal, and voice recognition. While participants may not understand all the implications of biometrics, these results indicate that there is significant interest in adopting biometric-based web authentication. Future research should examine how biometric-based authentication can be implemented on the web while still preserving users' privacy [6].

7.5 Physical Tokens

When using a physical token (i.e., WebTicket, smartphone), participants want to have a fallback mechanism. They are worried that they might lose their phone or WebTicket. They are also concerned with theft, especially when a single token could be used to log in to multiple different accounts or sites. For example, one user stated their concern with Snap2Pass,

www.manaraa.com

"It would make me nervous having all the passwords I need on my phone. For instance, if I forgot or lost it somewhere I could be inconvenienced with having to then make a username and password for all the websites I need, or if it was stolen and the password on my phone compromised somebody could easily access all of my personal and financial information."

Participants also voice concern that if they ever forgot to bring their physical token with them, then they would be unable to log into any websites. Alternatively, some participants also dislike that Snap2Pass requires a smartphone. One participant expresses both concerns in their responses:

"It seems unfortunate that you have to have a smart phone and you also have to have it with you."

7.6 Implementation Lessons

As mentioned in Section 5.2.1, we implemented the seven authentication systems for our studies. In the case of Google OAuth 2.0, Facebook Connect, Mozilla Persona, and Snap2Pass we found existing software libraries that aided our implementation. SAW, Hatchet, and WebTicket were implemented from scratch. The remainder of this section gives lessons learned from implementing the systems.

Google OAuth 2.0, Facebook Connect, and SAW use GET requests during authentication. This caused problems with WordPress, which expects authentication to occur using POST requests. We were able to code around this limitation, but this still represents a significant impediment to a clean implementation. It would be best if web authentication proposals allow the use of POST requests, as this would reduce development costs.

Google OAuth 2.0 and Facebook Connect both require a security check to prevent impersonation attacks. Facebook Connect's software library handles this check for developers, but Google OAuth 2.0 library requires that developers implement the security check

www.manaraa.com

themselves. This check is easy to implement incorrectly, resulting in usability (e.g., failed authentication) and security problems (e.g., impersonation attacks). We recommend that authentication proposals provide publicly-available implementations that handle security details for developers.

Implementing WebTicket was straightforward, but the webcam struggled to recognize QR codes. It is unclear if this problem was a limitation of the webcam or with the current state-of-the-art HTML5 QR code scanning libraries. Regardless, developers need to pay particular attention to this issue if they choose to implement WebTicket or a similar system.

www.manaraa.com

Chapter 8

Conclusion

Very few proposals for new authentication systems are accompanied by a formal user study, leaving us with scant empirical data to determine a best-in-class system for the various types of authentication systems or to reason about how the usability of different authentication systems compare against each other. In this paper, we report the results of a series of within-subjects empirical usability studies for seven web authentication systems. Our studies are the first to compare a heterogeneous collection of authentication proposals.

The result of our studies is that federated single sign-on systems (i.e., Google OAuth 2.0, Facebook Connect, Mozilla Persona) and Snap2Pass are rated as having the best overall usability. Also, our results validate SUS as an appropriate metric for comparing the usability of authentication systems, with the SUS score for a given system being consistent across different participant groups and proving to be a strong indicator of users' preferences. A low SUS score indicates that a system needs more attention on usability in order to be successful. The security community should no longer accept new system proposals that lack empirical evidence that the system is usable. We recommend that all new systems should be evaluated using SUS, and that a proposal should not receive serious consideration until it achieves a minimum acceptable SUS score of 70. This requirement would help accelerate the move towards more usable authentication systems and avoid wasted effort on systems with little chance of significant impact due to poor usability.

Our usability studies also gather insightful information from participants' qualitative responses. We find that transparent authentication systems are rated as usable, but also lead

www.manaraa.com

to confusion and a lack of trust from users. Additionally, while participants rate the usability of single sign-on highly, they are interested in augmenting it with additional site-specific low-entropy passwords. Finally, our results show that over half of participants are willing to use new authentication systems in their everyday life, but that they are most interested in adopting systems that are disruptive (e.g., biometrics, Snap2Pass).

www.manaraa.com

References

[1] Steam Guard. `https://support.steampowered.com/kb_article.php?ref=4020-ALZM-5519`. [Online; accessed 2014/11/20].

[2] Petar S Aleksic and Aggelos K Katsaggelos. Audio-visual biometrics. *Proceedings of the IEEE*, 94(11):2025–2044, 2006.

[3] Aaron Bangor, Philip Kortum, and James Miller. An empirical evaluation of the System Usability Scale. *International Journal of Human–Computer Interaction*, 24(6):574–594, 2008.

[4] Aaron Bangor, Philip Kortum, and James Miller. Determining what individual SUS scores mean: Adding an adjective rating scale. *Journal of Usability Studies*, 4(3):114–123, 2009.

[5] Joseph Bonneau, Cormac Herley, Paul C Van Oorschot, and Frank Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Symposium on Security and Privacy*, pages 553–567. IEEE, 2012.

[6] Joseph Bonneau, Edward W Felten, Prateek Mittal, and Arvind Narayanan. Privacy concerns of implicit secondary factors for web authentication. In *SOUPS Workshop on "Who are you?!": Adventures in Authentication*, 2014.

[7] John Brooke. SUS — a quick and dirty usability scale. In *Usability Evaluation in Industry*. CRC Press, 1996.

[8] John Brooke. SUS: A retrospective. *Journal of Usability Studies*, 8(2):29–40, 2013.

[9] Sonia Chiasson, Paul C van Oorschot, and Robert Biddle. A usability study and critique of two password managers. In *USENIX Security*, 2006.

[10] Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle, and Paul C Van Oorschot. Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism. *IEEE Transactions on Dependable and Secure Computing*, 9(2):222–235, 2012.

www.manaraa.com

[11] John Daugman. How iris recognition works. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1):21–30, 2004.

[12] Alexander J DeWitt and Jasna Kuljis. Aligning usability and security: A usability study of polaris. In *Symposium on Usable Privacy and Security*, 2006.

[13] Rachna Dhamija and Adrian Perrig. Deja Vu — a user study: Using images for authentication. In *USENIX Security*, 2000.

[14] Ben Dodson, Debangsu Sengupta, Dan Boneh, and Monica S Lam. Secure, consumer-friendly web authentication and payments with a phone. In *International Conference on Mobile Computing, Applications, and Services*, pages 17–38. Springer, 2012.

[15] Saar Drimer, Steven J Murdoch, and Ross Anderson. Optimised to fail: Card readers for online banking. In *Financial Cryptography and Data Security*, pages 184–200. Springer, 2009.

[16] Sascha Fahl, Marian Harbach, Thomas Muders, Matthew Smith, and Uwe Sander. Helping Johnny 2.0 to encrypt his facebook conversations. In *Symposium on Usable Privacy and Security*. ACM, 2012.

[17] Dinei Florêncio and Cormac Herley. One-time password access to any server without changing the server. In *Information Security*, pages 401–420. Springer, 2008.

[18] Simson Garfinkel and Heather Richter Lipford. Usable security: History, themes, and challenges. In *Synthesis Lectures on Information Security, Privacy, and Trust*, volume 5. Morgan & Claypool Publishers, 2014.

[19] Simson L Garfinkel. Email-based identification and authentication: An alternative to PKI? In *Symposium on Security and Privacy*, pages 20–26. IEEE, 2003.

[20] J Alex Halderman, Brent Waters, and Edward W Felten. A convenient method for securely managing passwords. In *International Conference on World Wide Web*, pages 471–479. ACM, 2005.

[21] Mike Hanson, Dan Mills, and Ben Adida. Federated browser-based identity using email addresses. In *W3C Workshop on Identity in the Browser*, 2011.

[22] Eiji Hayashi, Bryan Pendleton, Fatih Ozenc, and Jason Hong. WebTicket: Account management using printable tokens. In *SIGCHI Conference on Human Factors in Computing Systems*, pages 997–1006. ACM, 2012.

www.manaraa.com

[23] Nicholas J Hopper and Manuel Blum. Secure human edentification protocols. In *Advances in Cryptology – ASIACRYPT 2001*, pages 52–66. Springer, 2001.

[24] Ravi Jhawar, Philip Inglesant, Nicolas Courtois, and Martina Angela Sasse. Make mine a quadruple: Strengthening the security of graphical one-time PIN authentication. In *International Conference on Network and System Security*, pages 81–88. IEEE, 2011.

[25] Alfred Kobsa, Rahim Sonawalla, Gene Tsudik, Ersin Uzun, and Yang Wang. Serial hook-ups: A comparative usability study of secure device pairing methods. In *Symposium on Usable Privacy and Security*. ACM, 2009.

[26] David P Kormann and Aviel D Rubin. Risks of the passport single signon protocol. *Computer Networks*, 33(1):51–58, 2000.

[27] Arun Kumar, Nitesh Saxena, Gene Tsudik, and Ersin Uzun. Caveat eptor: A comparative study of secure device pairing methods. In *International Conference on Pervasive Computing and Communications*. IEEE, 2009.

[28] Mohammad Mannan and Paul C van Oorschot. Leveraging personal devices for stronger password authentication from untrusted computers. *Journal of Computer Security*, 19 (4):703–750, 2011.

[29] Daniel McCarney, David Barrera, Jeremy Clark, Sonia Chiasson, and Paul C van Oorschot. Tapas: Design, implementation, and usability evaluation of a password manager. In *Annual Computer Security Applications Conference*, pages 89–98. ACM, 2012.

[30] Bryan Parno, Cynthia Kuo, and Adrian Perrig. *Phoolproof Phishing Prevention*. Springer, 2006.

[31] Andreas Pashalidis and Chris J Mitchell. Impostor: A single sign-on system for use from untrusted devices. In *Global Telecommunications Conference*, pages 2191–2195. IEEE, 2004.

[32] David Recordon and Drummond Reed. Openid 2.0: A platform for user-centric identity management. In *Workshop on Digital Identity Management*, pages 11–16. ACM, 2006.

[33] Chris Robison, Scott Ruoti, Timothy W van der Horst, and Kent E Seamons. Private facebook chat. In *International Conference on Privacy, Security, Risk and Trust and International Confernece on Social Computing*, pages 451–460. IEEE, 2012.

www.manaraa.com

[34] Arun Ross, Jidnya Shah, and Anil K Jain. From template to image: Reconstructing fingerprints from minutiae points. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4):544–560, 2007.

[35] Blake Ross, Collin Jackson, Nick Miyake, Dan Boneh, and John C Mitchell. Stronger password authentication using browser extensions. In *USENIX Security*, 2005.

[36] Scott Ruoti, Nathan Kim, Ben Burgon, Timothy Van Der Horst, and Kent Seamons. Confused Johnny: When automatic encryption leads to confusion and mistakes. In *Symposium on Usable Privacy and Security*. ACM, 2013.

[37] Florian Schaub, Marcel Walch, Bastian Könings, and Michael Weber. Exploring the design space of graphical passwords on smartphones. In *Symposium on Usable Privacy and Security*. ACM, 2013.

[38] Stuart E Schechter, Rachna Dhamija, Andy Ozment, and Ian Fischer. The Emperor's new security indicators. In *Security and Privacy*, pages 51–65. IEEE, 2007.

[39] Z Cliffe Schreuders, Tanya McGill, and Christian Payne. Empowering end users to confine their own applications: The results of a usability study comparing SELinux, AppArmor, and FBAC-LSM. *ACM Transactions on Information and System Security*, 14(2), 2011.

[40] Sidney L Smith. Authenticating users by word association. In *Human Factors and Ergonomics Society Annual Meeting*, volume 31, pages 135–138. SAGE Publications, 1987.

[41] Frank Stajano. Pico: No more passwords! In *International Workshop on Security Protocols*, pages 49–81. Springer, 2011.

[42] San-Tsai Sun, Eric Pospisil, Ildar Muslukhov, Nuray Dindar, Kirstie Hawkey, and Konstantin Beznosov. What makes users refuse web single sign-on?: An empirical investigation of OpenID. In *Symposium on Usable Privacy and Security*. ACM, 2011.

[43] Hai Tao. *Pass-Go, A New Graphical Password Scheme*. PhD thesis, University of Ottawa, 2006.

[44] Thomas S Tullis and Jacqueline N Stetson. A comparison of questionnaires for assessing website usability. Presented at *Usability Professional Association Conference*, 2004.

www.manaraa.com

[45] Timothy W van der Horst and Kent E Seamons. Simple authentication for the web. In *International Conference on Security and Privacy in Communications Networks and the Workshops*, pages 473–482. IEEE, 2007.

[46] Daphna Weinshall. Cognitive authentication schemes safe against spyware. In *Symposium on Security and Privacy*, pages 295–300. IEEE, 2006.

[47] Alma Whitten and J Doug Tygar. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *USENIX Security*, 1999.

[48] Alexander Wiesmaier, Marcus Fischer, Marcus Lippert, and Johannes Buchmann. Outflanking and securely using the PIN/TAN-system. *arXiv Preprint CS/0410025*, 2004.

www.manaraa.com

Appendix A

Usability Study Survey

This chapter replicates our usability studies as seen by participants. In several places, task descriptions and questions were modified to refer to the currently assigned authentication system. Text in **bold** indicates places where text is modified, and Tables A.1 and A.2 list the system-specific modifications.

A.1 Introduction

Welcome to the Internet Security Research Lab study on authentication.

During this study you will be using three alternatives to password-based authentication. To help test these authentication systems we have created two mock websites that use these alternative authentication systems. We have modified these websites so that they log you out at the end of every task. This was done to simulate using these sites over a period of several weeks.

You will only use one alternative authentication system at a time. For each system you will complete six tasks. After you have completed the six tasks for the first authentication system you will be given several questions about your experience. You will then complete the six tasks and another set of questions about the second authentication system.

During the course of the study we will record your screen. This is necessary to calculate information regarding the authentication systems. This video will not be given to anyone besides the researchers. It will be destroyed once the study is completed. We will not collect any personally identifying information and any other data, besides the screen capture and the answers to this survey, will be automatically deleted at the end of the survey.

You will receive $10.00 as compensation for your participation in this study. The expected time commitment is approximately 30-45 minutes. If you have any questions or concerns feel free to ask the study coordinator. You can end participation in this survey at any time and we will delete the results of your study upon request.

www.manaraa.com

System	**SystemName**	**SearchToken**
Google	Google OAuth 2.0	Google Auth Code
Facebook	Facebook Connect	Facebook Auth Code
Mozilla	Mozilla Persona	Persona Auth Code
SAW	SAW	SAW Auth Code
Hatchet	Hatchet	Hatchet Auth Code
WebTicket	WebTicket	WebTicket Auth Code
Snap2Pass	Snap2Pass	Snap2Pass Auth Code

System	**CodePlacement1**
SAW	This code will be sent to your personal email account. This is a different e-mail than the one you will receive to complete registration.
Snap2Pass	This code will be displayed in the Snap2Pass application, next to the Smartphone Support account.
Others	This code will be sent to your personal email account.

System	**CodePlacement2**
WebTicket	This code will be displayed at the bottom of your WebTicket.
Snap2Pass	This code will be displayed in the Snap2Pass application, next to the Bank of the Test account. You should now have two accounts registered with Snap2Pass.
Others	This code will be displayed at the top of the profile page.

Table A.1: System specific text replacements

www.manaraa.com

System	**AdditionalInstructions1**
WebTicket	As part of this task you will use the camera attached to the computer. This camera is only used as part of the authentication method, and no video is recorded. You will also need to use a printer. The computer you are using is already setup to print to the printer "User Study". The printer itself is located by the door of the lab. We have also provided scissors for your use.
Snap2Pass	As part of this task you will be asked to use Snap2Pass, a smartphone application. We have provided a phone for you to use with this application already installed.

System	**AdditionalInstructions2**
WebTicket	As you share your impressions, remember that in order to use WebTicket personally you would need to own a web cam and a printer.
Snap2Pass	As you share your impressions, remember that in order to use Snap2Pass yourself you would need to own a smartphone and install Snap2Pass on that phone.

Table A.2: Additional text replacements for WebTicket and Snap2Pass

A.2 Demographics

What is your gender? (*Male, Female, I prefer not to answer*)

What is your age? (*18 - 24 years old, 25 - 34 years old, 35 - 44 years old, 45 - 54 years old, 55 years or older, I prefer not to answer*)

What is the highest degree or level of school you have completed? (*Some school, no high school diploma, High school graduate, diploma or the equivalent (for example: GED), Some college or university credit, no degree, College or university degree, Post-Secondary Education, I prefer not to answer*)

What is your occupation or major? (*free response*)

How would you rate your level of computer expertise? (*Beginner, Intermediate, Advanced*)

www.manaraa.com

A.3 Tasks

SystemName

In the following set of tasks you will be testing **SystemName**.

AdditionalInstructions1

A.3.1 Task 1

SystemName – Task 1

In this first task you will use **SystemName** to create a new account at `https://forums.isrl.byu.edu/`.

For this task please complete the following actions:

1. Click on the following link: `https://forums.isrl.byu.edu/`.
2. On the right side of the page you will see a link called "register", click on it.
3. Register an account. Use whatever account name you wish to.
4. When you have finished registering an account you will be given a code to use for completing this task. **CodePlacement1**

Enter the code you received:

A.3.2 Task 2

SystemName– Task 2

In this task you will be logging in to `https://bank.isrl.byu.edu/` and changing this account to allow you to log into it using **SystemName**.

For this task please complete the following actions:

1. Click on the following link: `https://bank.isrl.byu.edu/`.
2. Log into the site using the following username and password:
   Username: **auto-generated username**
   Password: **suto-generated password**

www.manaraa.com

3. In the top right corner of the page there is a link that says "Howdy, **auto-generated username**", click on it.
4. On this page you will find instructions on how to use **SystemName** with this account.
5. When you have finished setting up **SystemName** you will be given a code to use for completing this task. **CodePlacement2**

For the remainder of this set of tasks only use **SystemName** to log in!

Enter the code you received:

A.3.3 Task 3

SystemName – Task 3

In this task you will be logging in to `https://forums.isrl.byu.edu/` and creating a forum post.

For this task please complete the following actions:

1. Click on the following link: `https://forums.isrl.byu.edu/`.
2. Log in using **SystemName**.
3. On the right side of the page you will see a link called "New Users", click on it.
4. In this forum post a new topic saying hello. We will automatically respond to this post with a code to use for completing this task. If you do not see to this code refresh the page.

Enter the code you received:

A.3.4 Task 4

SystemName – Task 4

In this task you will be logging in to `https://bank.isrl.byu.edu/` and looking up a deposit.

For this task please complete the following actions:

www.manaraa.com

1. Click on the following link: `https://bank.isrl.byu.edu/`.
2. Log in using **SystemName**.
3. In the top right of the page you will see a link called "Account Details", click on it.
4. Click on the "Checking" link in the middle of the page.
5. On this page you will see a transaction with the description "User study transfer." Use the amount of this transfer as the code for completing this task (don't include the dollar sign).
6. *If using SAW:* Note: If you are using GMail, sometimes the authentication message is redirected to spam. You will need to go into your spam folder and remove the spam tag. This is a limitation of the study, and should not be considered a negative feature of SAW. If SAW were ever widely deployed these messages would never be marked as spam. If you have any questions please ask the study coordinator.

Enter the code you received:

A.3.5 Task 5

SystemName – Task 5

In this task you will be logging in to `https://forums.isrl.byu.edu/` and searching for a forum post.

For this task please complete the following actions:

1. Click on the following link: `https://forums.isrl.byu.edu/`.
2. Log in using **SystemName**.
3. On the right side of the page you will see a search box. Search for "**SearchToken**".
4. You will have found a topic which contains the code to use for completing this task. Note, you need to be logged in to find this topic. If you do not see it make sure you are logged in.

Enter the code you received:

www.manaraa.com

A.3.6 Task 6

SystemName – Task 6

In this task you will be logging in to `https://bank.isrl.byu.edu/` and making a transfer.

For this task please complete the following actions:

1. Click on the following link: `https://bank.isrl.byu.edu/`.
2. Log in using **SystemName**.
3. In the top right of the page you will see a link called "Transfer Funds", click on it.
4. Transfer $100 from the checking account to savings. Account number: **auto-generated username**.
5. Now click on "Account Details" followed by "Savings".
6. In the description for the transfer you just completed you will find the code for completing this task.
7. *If using SAW:* Note: If you are using GMail, sometimes the authentication message is redirected to spam. You will need to go into your spam folder and remove the spam tag. This is a limitation of the study, and should not be considered a negative feature of SAW. If SAW were ever widely deployed these messages would never be marked as spam. If you have any questions please ask the study coordinator.

Enter the code you received:

A.4 Questionnaire

You will now be asked several questions concerning your experience with **SystemName**.

AdditionalInstructions2

Please answer the following question about **SystemName**. Try to give your immediate reaction to each statement without pausing to think for a long time. Mark the middle column if you don't have a response to a particular statement.

1. I think that I would like to use this system frequently.
2. I found the system unnecessarily complex.

www.manaraa.com

3. I thought the system was easy to use.
4. I think that I would need the support of a technical person to be able to use this system.
5. I found the various functions in this system were well integrated.
6. I thought there was too much inconsistency in this system.
7. I would imagine that most people would learn to use this system very quickly.
8. I found the system very cumbersome to use.
9. I felt very confident using the system.
10. I needed to learn a lot of things before I could get going with this system.

(*Strongly disagree, Disagree, Neither Agree nor Disagree, Agree, Strongly Agree*)

What did you like most about using **SystemName**?

What would you change about **SystemName**?

Prefer Would you prefer to use **SystemName** over traditional password-based authentication?
(*Yes, No, Unsure*)

Please explain why.

A.5 End-of-survey Questionnaire

Now that you have finished using the authentication systems, please answer these questions comparing their use.

Which system would you prefer to use on a regular basis.
(**SystemName** *of first system tested,* **SystemName** *of second system tested,* **SystemName** *of third system tested, Current password-based authentication*)
Please explain why.

Based on your experience, if you could create your ideal authentication system, what features would it have? It does not need to be similar to either system you tried.

www.manaraa.com

Appendix B

Federated Single Sign-on Usability Study – Participant Responses

ID	Start	End	First system tested	Second system tested
R_0DLjWnAFkG98LZz	6/24/2014 16:37	6/24/2014 17:00	Google OAuth 2.0	Mozilla Persona
R_a3jhm86uFhsjZB3	6/25/2014 9:28	6/25/2014 9:58	Mozilla Persona	Google OAuth 2.0
R_b2E2mbLA82I8I9n	6/26/2014 9:06	6/26/2014 9:33	Facebook Connect	Mozilla Persona
R_5b6oEjWnrIu4M85	6/26/2014 11:55	6/26/2014 12:16	Google OAuth 2.0	Facebook Connect
R_3VRzzSgaPWuqU7j	6/26/2014 13:32	6/26/2014 13:59	Mozilla Persona	Google OAuth 2.0
R_2f584iP4iTQkt6d	6/26/2014 14:51	6/26/2014 15:16	Facebook Connect	Google OAuth 2.0
R_6FEBLvSCm2tVjeZ	6/26/2014 15:54	6/26/2014 16:22	Facebook Connect	Google OAuth 2.0
R_a8EaGglJfox9JHf	6/27/2014 13:22	6/27/2014 13:57	Facebook Connect	Mozilla Persona
R_ePeajbtklCnke6V	6/27/2014 14:09	6/27/2014 14:34	Facebook Connect	Mozilla Persona
R_cuvpRKCmakqtEZn	6/27/2014 14:57	6/27/2014 15:19	Google OAuth 2.0	Mozilla Persona
R_ezxRuMGWx4otQ4l	6/28/2014 12:01	6/28/2014 12:20	Google OAuth 2.0	Mozilla Persona
R_8j4JDxoOmPyY0EB	6/28/2014 13:25	6/28/2014 13:57	Mozilla Persona	Google OAuth 2.0
R_ahixe9VTPVvEhlb	6/28/2014 13:58	6/28/2014 14:20	Facebook Connect	Google OAuth 2.0
R_dnHkCnfHZRfucg5	6/28/2014 17:17	6/28/2014 17:41	Mozilla Persona	Google OAuth 2.0
R_bkZwCuSDTbZhgnX	6/30/2014 9:00	6/30/2014 9:33	Mozilla Persona	Facebook Connect
R_6sRr2B92X2YnLRr	6/30/2014 15:53	6/30/2014 16:14	Google OAuth 2.0	Facebook Connect
R_37VpLHXutR4oAzb	6/30/2014 16:14	6/30/2014 16:53	Mozilla Persona	Google OAuth 2.0
R_ePvTgp05qfhX8rP	7/1/2014 10:32	7/1/2014 10:53	Facebook Connect	Mozilla Persona
R_1NgWqbpXq2wXk8d	7/1/2014 16:26	7/1/2014 16:55	Google OAuth 2.0	Facebook Connect
R_56l6XoTISJVp8ih	7/2/2014 17:19	7/2/2014 17:52	Google OAuth 2.0	Facebook Connect
R_bdyuhU7RoScNHLL	7/3/2014 9:15	7/3/2014 9:40	Facebook Connect	Google OAuth 2.0
R_42vIMvRgaRu4tJX	7/3/2014 12:00	7/3/2014 12:40	Mozilla Persona	Facebook Connect
R_3U8EbALnELRCkK1	7/5/2014 10:28	7/5/2014 10:58	Mozilla Persona	Facebook Connect
R_blWEdiC7J16LWw5	7/12/2014 15:06	7/12/2014 16:10	Mozilla Persona	Facebook Connect

www.manaraa.com

ID	Gender	Age	Education
R_0DLjWnAFkG98LZz	Male	18 - 24 years old	Some college or university credit, no degree
R_a3jhm86uFhsjZB3	Female	18 - 24 years old	Some college or university credit, no degree
R_b2E2mbLA82I8I9n	Male	18 - 24 years old	Some college or university credit, no degree
R_5b6oEjWnrIu4M85	Male	18 - 24 years old	Some college or university credit, no degree
R_3VRzzSgaPWuqU7j	Female	18 - 24 years old	College or university degree
R_2f584iP4iTQkt6d	Male	18 - 24 years old	Some college or university credit, no degree
R_6FEBLvSCm2tVjeZ	Female	18 - 24 years old	High school graduate, diploma or the equivalent (for example: GED)
R_a8EaGglJfox9JHf	Male	18 - 24 years old	Some college or university credit, no degree
R_ePeajbtklCnke6V	Male	18 - 24 years old	Some college or university credit, no degree
R_cuvpRKCmakqtEZn	Male	18 - 24 years old	Some college or university credit, no degree
R_ezxRuMGWx4otQ4l	Male	18 - 24 years old	Some college or university credit, no degree
R_8j4JDxoOmPyY0EB	Female	18 - 24 years old	Some college or university credit, no degree
R_ahixe9VTPVvEhlb	Female	18 - 24 years old	Some college or university credit, no degree
R_dnHkCnfHZRfucg5	Female	18 - 24 years old	Some college or university credit, no degree
R_bkZwCuSDTbZhgnX	Male	18 - 24 years old	College or university degree
R_6sRr2B92X2YnLRr	Female	18 - 24 years old	College or university degree
R_37VpLHXutR4oAzb	Male	18 - 24 years old	College or university degree
R_ePvTgp05qfhX8rP	Female	18 - 24 years old	Some college or university credit, no degree
R_1NgWqbpXq2wXk8d	Male	25 - 34 years old	Post-Secondary Education
R_56l6XoTISJVp8ih	Male	25 - 34 years old	Post-Secondary Education
R_bdyuhU7RoScNHLL	Male	25 - 34 years old	College or university degree
R_42vIMvRgaRu4tJX	Female	25 - 34 years old	College or university degree
R_3U8EbALnELRCkK1	Male	18 - 24 years old	Some college or university credit, no degree
R_blWEdiC7J16LWw5	Female	18 - 24 years old	Some college or university credit, no degree

www.manaraa.com

ID	Major	Technical expertise
R_0DLjWnAFkG98LZz	Acturial Science	Intermediate
R_a3jhm86uFhsjZB3	Chemistry Major	Intermediate
R_b2E2mbLA82I8I9n	Public Health - Health Science	Intermediate
R_5b6oEjWnrIu4M85	Geography	Intermediate
R_3VRzzSgaPWuqU7j	geography	Beginner
R_2f584iP4iTQkt6d	Neuroscience	Intermediate
R_6FEBLvSCm2tVjeZ	PDBIO	Intermediate
R_a8EaGglJfox9JHf	Mechanical Engineering switching to Biotech	Beginner
R_ePeajbtklCnke6V	Chemistry Education	Intermediate
R_cuvpRKCmakqtEZn	Accounting	Intermediate
R_ezxRuMGWx4otQ4l	Photographer, Math	Advanced
R_8j4JDxoOmPyY0EB	Communications	Intermediate
R_ahixe9VTPVvEhlb	Family Studies	Beginner
R_dnHkCnfHZRfucg5	Dietetics	Intermediate
R_bkZwCuSDTbZhgnX	Mechanical Engineering	Intermediate
R_6sRr2B92X2YnLRr	Speech Technician	Intermediate
R_37VpLHXutR4oAzb	accounting	Intermediate
R_ePvTgp05qfhX8rP	Wildlife and Wildlands Conservation	Intermediate
R_1NgWqbpXq2wXk8d	Mechanical Engineering	Intermediate
R_56l6XoTISJVp8ih	accounting	Intermediate
R_bdyuhU7RoScNHLL	biochemistry	Intermediate
R_42vIMvRgaRu4tJX	Horticulture	Intermediate
R_3U8EbALnELRCkK1	Psychology	Intermediate
R_blWEdiC7J16LWw5	Family Life with an emphasis on Human Development	Intermediate

www.manaraa.com

ID	What did you like most about using Google OAuth 2.0	What would you change about Google OAuth 2.0	Would you prefer to use Google OAuth 2.0 over traditional password-based authentication?	Please explain why.
R_0DLjWnAFkG98LZz	I was able to log-in without having to type my ID and password	Making sure that it works	Yes	It saves time and it is less work
R_a3jhm86uFhsjZB3	It was super easy, I only had to click one button to sign in.	I would show a picture of the google account being logged into - like it does when you sign into gmail so when someone else uses the computer it is easy to know if you are signing in with your google oauth or not.	Yes	It is super easy, super quick, and super simple.
R_5b6oEjWnrIu4M85	The ease of a one-click sign in.	Nothing. Seems to serve its purpose.	No	I prefer to login using a password every time.
R_3VRzzSgaPWuqU7j	I liked it, but I don't know if anything stuck out; it seemed very similar to Mozilla Persona.	I don't think I'd change anything, it seemed to work quite well.	Unsure	Again, I feel like I don't know enough about the differences between Google OAuth and traditional passwords. If I was confident that this worked just as well, if not better than traditional methods, I would be very interested in using it.
R_2f584iP4iTQkt6d	Again one click and logged in	Better privacy	No	Again I feel that it doesn't take a whole lot just to type in a password and username. Same concern as before would be that of how it accesses my google account readily.
R_6FEBLvSCm2tVjeZ	Easy login.	Wouldn't use with my main accounts.	No	Wouldn't want one password for everything.

www.manaraa.com

ID	What did you like most about using Google OAuth 2.0	What would you change about Google OAuth 2.0	Would you prefer to use Google OAuth 2.0 over traditional password-based authentication?	Please explain why.
R_cuvpRKCmakqtEZn	I liked how easy it was to log in to various websites.	I would maybe include some instructions on all the features that it contains.	Yes	I trust google with my passwords and it is convenient.
R_ezxRuMGWx4otQ4l	one-click simplicity	I would like to understand more about how it works up-front. It doesn't feel secure.	No	I would like to understand more about how it works up-front. It doesn't feel secure.
R_8j4JDxoOmPyY0EB	It signed into my google account immediately and I didn't have to repeat any information that I'd already entered.	I liked it I think it's great the way it is	Yes	Because then I wouldn't have to reenter any information and it's connected to my email
R_ahixe9VTPVvEhlb	I liked that it used google. I trust google more than i would facebook.	I don't have any suggestions for change.	Unsure	Again i think it makes it easier to hack.
R_dnHkCnfHZRfucg5	It seemed the exact same as Mozilla Persona. I did better with Google OAuth because I had gotten the hang of it with Mozilla. Both are very good in the same ways.	It seemed good to me. I don't know anything I would change about it. I would need to use it more first.	Unsure	Same as with Mozilla - probably yes, if secure. It is easy to do and convenient.
R_6sRr2B92X2YnLRr	It was simple to use and required just pushing a button and it remembered the passwords.	I don't think there is anything I would change.	Yes	It is more simple and I don't have to remember a million passwords. I always forget which password goes to which website.
R_37VpLHXutR4oAzb	it really seemed like the exact same thing as the other one	nothing	Unsure	I dont see how it is significantly different than what i am already using/

www.manaraa.com

ID	What did you like most about using Google OAuth 2.0	What would you change about Google OAuth 2.0	Would you prefer to use Google OAuth 2.0 over traditional password-based authentication?	Please explain why.
R_1NgWqbpXq2wXk8d	I liked most that I didn't need to remember separate passwords for each site.	Of the top of my head, I can't think of anything I would change about it.	Unsure	I like it a lot but the if my Google OAuth account were ever compromised, they would have access to everything important to me. I'd have to decide if the added convenience is worth the risk.
R_56l6XoTISJVp8ih	Ease of logging in and the ability to avoid constantly logging in and out with usernames and passwords.	I didn't know I was using Google OAuth. I just thought I was signing in with Google. It seems like the request to login should be uniform.	Unsure	I am unsure whether this is as secure as having multiple passwords and usernames across systems. Would this mean if my e-mail account was hacked that I would have both my social forums and bank accounts susceptible to attack? If someone had access to my computer, could they simply sign in using google like they were me?
R_bdyuhU7RoScNHLL	easy	same as the facebook. I will not use this for banking. And every time I log in I like it to ask for a password, especially to a bank account	No	same as the facebook. I will not use this for banking. And every time I log in I like it to ask for a password, especially to a bank account

www.manaraa.com

ID	What did you like most about using Facebook Connect	What would you change about Facebook Connect	Would you prefer to use Facebook Connect over traditional password-based authentication?	Please explain why.
R_b2E2mbLA82I8I9n	The combination of one username and password to gain access to multiple sites was very attractive to me. I often forget passwords and sometimes usernames for websites and change my password every time I use them. Facebook connect solves this problem.	I wouldn't change anything other than the websites used. I would never use facebook connect for something as secure as a banking website.	Yes	I chose yes to the above question because today most people have their own computers, these computers are often already password protected. Facebook connect eliminates the need for multiple passwords.
R_5b6oEjWnrIu4M85	I liked the fact that it was easy to login once the link was set up.	I wouldn't change anything, but I probably wouldn't use it.	No	I don't like linking things to my facebook account; often the data the app will have access to is not apparent.
R_2f584iP4iTQkt6d	One click and I was logged in, but that gave me a lot of concern as to the security of it.	Not a programmer to really say.	No	I prefer entering in the username and password myself to make sure that I am the one accessing those websites. I am concerned that if it only takes one click and I thought I had logged out of facebook then how is it still accessing my facebook password?
R_6FEBLvSCm2tVjeZ	I like the simplicity of having one account for everything for simple things like phone forums.	I wouldn't connect it with everything because password theft would be so easily stolen.	No	I would worry about a person getting control of all of my accounts too easily.

www.manaraa.com

ID	What did you like most about using Facebook Connect	What would you change about Facebook Connect	Would you prefer to use Facebook Connect over traditional password-based authentication?	Please explain why.
R_a8EaGglJfox9JHf	The ease of use and the ability to connect one account to multiple accounts	Nothing	No	Having multiple passwords creates more privacy and more security than having one password for everything, or one account that ties multiple accounts together.
R_ePeajbtklCnke6V	It was fast to use and I didn't have to keep inputting my information to login.	I would be worried about security. I've heard that facebook is "relatively" easy to hack. I would want to be sure that it was all secure before I started using it.	Unsure	See the comment above.
R_ahixe9VTPVvEhlb	It was very quick and easy to sign in and use everything.	I would not really change anything right now.	Unsure	This system does seem easier and quicker to use it also feels like it could be hacked easier as well.
R_bkZwCuSDTbZhgnX	It was quick to log in. It required one click and the authentication time was minimal.	I think it was very straightforward to use. Once again like with the other system, perhaps an explanation of how it protected information would give me more confidence in using it.	No	I normally prefer to limit the amount of information I connect to Facebook as much as possible. So trusting all of my password information to Facebook as well would not be my favorite thing to do.

www.manaraa.com

ID	What did you like most about using Facebook Connect	What would you change about Facebook Connect	Would you prefer to use Facebook Connect over traditional password-based authentication?	Please explain why.
R_6sRr2B92X2YnLRr	It was easy to use and it didn't require me to remember a bunch of different passwords.	I wish it didn't have access to all my friends, pictures, etc. So, making it more secure.	No	I just feel that facebook isn't very secure. I don't like it having access to everything I put on and all my friends, and I feel that facebook gets hacked often. I also would be worried that these sites would post something to my facebook (hacking) because it has full access.
R_ePvTgp05qfhX8rP	Simple, quick	Was it secure?	Yes	It's easier
R_1NgWqbpXq2wXk8d	I didn't have to remember passwords for each individual website	Disconnect it from Facebook. I typically don't like to connect authorization things to Facebook since in the past it usually gave them more information than I wanted the 3rd party to have.	No	I dislike that it is connected to Facebook (see above response about changing things). I also dislike that if my Facebook account were compromised it would give the attacker access to much more. I also feel like Facebook is less secure than Google.
R_56l6XoTISJVp8ih	It was easy to login and avoided a lot of username and password typing.	It required that I had my email account linked to my facebook account. Something that I have resisted doing.	Unsure	I am still unsure how safe and secure this system is if you can login with a click of a button because the account is linked to Facebook. I think it would be easier to hack into Facebook's database than a bank's. Security would be the main deterrent.

www.manaraa.com

ID	What did you like most about using Facebook Connect	What would you change about Facebook Connect	Would you prefer to use Facebook Connect over traditional password-based authentication?	Please explain why.
R_bdyuhU7RoScNHLL	easy	I observed as I clicked the facebook connect button it automatically connects and login to the account. its fine for an account that does not involve money. For example I would never use facebook connect to login to my bank accounts. I prefer if it does not store my data so I have to log in each time I use it.	No	I don't want to share my personnel information with whom I don't know (i.e. bank officer etc)
R_42vIMvRgaRu4tJX	easy	nothing	No	less time consume and easy
R_3U8EbALnELRCkK1	Once again, I enjoyed the ease of logging in without using a password.	I understand understand that it logs you out so that someone else couldn't see whatever you were looking at. However, someone could simply log back in right? All they have to do is click on Facebook Connect. This concerns me.	Unsure	If I wasn't worried about security I would definitely use it. For the most part, I would use it on a personal computer. I'm not sure about a public computer.
R_blWEdiC7J16LWw5	Same as with Mozilla Persona: it was very easy to use and quicker than just using a password.	Same as with Mozilla Persona: it was somewhat confusing signing up or registering for it, so I would make that easier to understand.	Unsure	Again, same as with Mozilla Persona: it was very easy to use, better than traditional password-based authentication, but I'm unsure how safe it is and if someone could use it to sign in as me.

www.manaraa.com

ID	What did you like most about using Mozilla Persona	What would you change about Mozilla Persona	Would you prefer to use Mozilla Persona over traditional password-based authentication?	Please explain why.
R_0DLjWnAFkG98LZz	Being able to login with out having to put my password everytime	nothing	Yes	easy to use
R_a3jhm86uFhsjZB3	It was much easier than trying to remember passwords and usernames for different accounts.	When you click the "sign in using Persona" option, a new window pops up to the left of the screen. That threw me off a little, I would have expected it to pop up in the center or at least on top of where I clicked to use it. I don't know if that matters a ton though.	Yes	I recycle different combinations of usernames and passwords from my different accounts and frequently forget which one I used for what. Some websites require long passwords that are difficult to remember. Using Persona was much more convenient. (I really hate when you have to have a password with numbers and letters and different cases because they take longer to remember and to type. Persona allows me to avoid that once I set it up.) I would totally use it.
R_b2E2mbLA82I8I9n	It was very easy to sign up for this system, it only required me to use my email address.	I was unsure how secure this system was, it didn't ever explicitly ask for a password, not even to start. This made me think that it was less secure than other systems.	Unsure	Due to the feeling of less security I would probably use other systems, other than that Persona was very smooth and user friendly.
R_5b6oEjWnrIu4M85				

www.manaraa.com

ID	What did you like most about using Mozilla Persona	What would you change about Mozilla Persona	Would you prefer to use Mozilla Persona over traditional password-based authentication?	Please explain why.
R_3VRzzSgaPWuqU7j	I liked that I could use it to log into multiple sites.	I don't think I'd change anything. I liked that it asked me how long I'd like to stay logged into the persona.	Unsure	I feel like I don't understand the differences between the two well enough (why I'm unsure).
R_2f584iP4iTQkt6d				
R_6FEBLvSCm2tVjeZ				
R_a8EaGglJfox9JHf	nuetral	Logging in from one account to the other account, it would work on one and not the other.	No	I prefer a traditional password-based authentication.
R_ePeajbtklCnke6V	It seemed more secure than the Facebook login.	It asked me about staying logged in after the second time doing so. It would be nice to offer that option from the beginning, if at all. Also, there were more steps to authenticating.	Unsure	In addition to the above comments, it is nice to not have to remember a bunch of different passwords. But, is that as secure as it can be?
R_cuvpRKCmakqtEZn	I liked the sleek GUI whenever I logged in.	There was a part where I wasn't quite sure how to implement persona into a website and had to ask, whereas with the Google program, a red button appeared and did it for me.	Yes	It makes life simpler and you can log in faster. Once I got the hang of it, it was easy.
R_ezxRuMGWx4otQ4l	It is almost as simple as google oauth, but not provided by google	make it one-click like google oauth	No	I don't know enough about how it works. It doesn't feel as secure as a password.
R_8j4JDxoOmPyY0EB	It went quickly once I got the information in	I had to use two different email addresses before I got it to work and I think it should work on every email.	No	Because I get tired of typing in the same password over and over

www.manaraa.com

ID	What did you like most about using Mozilla Persona	What would you change about Mozilla Persona	Would you prefer to use Mozilla Persona over traditional password-based authentication?	Please explain why.
R_ahixe9VTPVvEhlb				
R_dnHkCnfHZRfucg5	It was very direct and clear. Easy to use. Very organized.	I don't know of anything I would change.	Unsure	I am unsure, but probably yes, if secure. Logging in was easier and more convenient. I liked that logging in was done through one system.
R_bkZwCuSDTbZhgnX	I didn't have to enter in a password and try multiple times before getting it correct.	I liked it. I would perhaps like some kind of explanation on how Mozilla persona keeps information safe so I would feel more confident trusting it and therefore more willing to use it.	Unsure	If I understood how the system would prevent someone other than me from logging in I would use it.
R_6sRr2B92X2YnLRr				
R_37VpLHXutR4oAzb	I don't know	I don't know	Unsure	I don't really know what it is still
R_ePvTgp05qfhX8rP	Simple, easy, and tied to email which everyone has	A little more time-consuming	Yes	Still quicker and easier than passwords
R_1NgWqbpXq2wXk8d				
R_56l6XoTISJVp8ih				
R_bdyuhU7RoScNHLL				
R_42vIMvRgaRu4tJX	easy to use.less complex	nothing	No	this is much more convienient
R_3U8EbALnELRCkK1	It's great not having to use a password, it just speeds up the process of signing in.	I'm not sure if I would change it, but it makes me a little nervous not putting in a password. However, because one is logged off after leaving the site, I suppose the risk is not great.	Yes	Mostly the speed with which one can access a secure website. I like not having to enter in a complex password.

www.manaraa.com

ID	What did you like most about using Mozilla Persona	What would you change about Mozilla Persona	Would you prefer to use Mozilla Persona over traditional password-based authentication?	Please explain why.
R_blWEdiC7J16LWw5	I liked how it was easier to use than using a password. It was a lot easier to just click log in, then click sign in, and it signed me right in.	I would change the registering part of it–that was a little confusing. But once I registered and then used it a few times, it was very easy from then on.	Unsure	Well, I liked how it was so easy. With traditional password-based authentication, sometimes it's annoying to use–for example, when I type it in wrong and then I have to type it in again, or when I forget what my password is and I have to find it. Mozilla Persona eliminated all of that, except I had to use a password and username to register for it. But, I'm unsure if it's safe–is it safer and better to use than traditional password-based authentication? I know passwords get stolen all the time. Could someone steal my Mozilla Persona password, username, or email so that they can use Mozilla Persona as me to sign into all the websites that use it? I don't know.

www.manaraa.com

ID	Which system would you prefer to use on a regular basis.	Please explain why.	Based on your experience with both systems, if you could create your ideal authentication system, what features would it have? It does not need to be similar to either system you tried.
R_0DLjWnAFkG98LZz	Mozilla Persona	it did not failed to login as Google Oauth did.	nothing. I am satisfied with Mozilla Persona.
R_a3jhm86uFhsjZB3	Google OAuth	You only needed to click one button to log in with Google. Persona required two and seemed to take longer	it would be the google oauth with identification like the popup window for persona- just so I know which account I am logging in with.
R_b2E2mbLA82I8I9n	Facebook Connect	I am more familiar with facebook connect. Also I don't use firefox, I don't know if this is a requirement for Mozilla Persona but that's what my brain immediately though. Facebook has proven to be decently secure in the past and has gained my trust.	Features: One or two click authentication. One time password use to log in. Auto-Fill information for registering for websites. That last one would be HUGE. If this was available i would use it every time.
R_5b6oEjWnrIu4M85	Neither	I prefer to keep my accounts separate and use email only for account creation, not login.	If I were to design a one-step authentication system it would likely be similar to these ones.
R_3VRzzSgaPWuqU7j	Neither	They seem really similar- in fact, I don't know if I can recall any differences between the two. Using Google OAuth went much faster, but I think that was because I was more familiar with the format overall.	I'm not sure- it doesn't seem like anything is fool-proof these days. Both of the systems I tried seemed to work well, but if I could somehow use something that is unique just to me (fingerprints for example? I don't know, and maybe that would be too expensive or could still be manipulated), I would incorporate that into my ideal authentication system.
R_2f584iP4iTQkt6d	Neither	Privacy	Some form of assurance to the user about the safety of using it like every time you first open a window you have to log in initially. Then during your internet session use the one click access, but as soon as the window closes it would be required to log in like normal.

www.manaraa.com

ID	Which system would you prefer to use on a regular basis.	Please explain why.	Based on your experience with both systems, if you could create your ideal authentication system, what features would it have? It does not need to be similar to either system you tried.
R_6FEBLvSCm2tVjeZ	Neither	Wouldn't want one password for everything.	I would make an account separate from my social network and mail specifically for functions like banking etc.
R_a8EaGglJfox9JHf	Neither	I like to have more privacy and protection between accounts.	Multiple passwords with the same username and certain locks and other doors for each specific account.
R_ePeajbtklCnke6V	Mozilla Persona	If I were to use one of the system, I would prefer the Mozilla Persona system. It allows for the option for it to remember me and seemed more secure (based on what I have heard).	I just heard a podcast on using fingerprints and/or retina for authentication. Assuming that the technology could be made reliably and cost effectively, I feel like that would be (perhaps) faster, more convenient and more reliable than current or proposed systems.
R_cuvpRKCmakqtEZn	Google OAuth	The red button appeared on the first website to let me implement it whereas with mozilla persona, I had to enter my email address to get it. Basically, it is just that Google OAuth is just a little easier to use.	It would have the easiness to operate of Google OAuth, but it would have the GUI of Mozilla Persona.
R_ezxRuMGWx4otQ4l	Neither	I don't know enough about how either system authenticates. It doesn't feel as secure as entering my password	I like two-step systems used by some banks, where you need 1. a username/password combination 2. a code or picture verification Google's system requiring "something you know and something you have" also inspires confidence. An example is a password (something you know) and a code sent via sms to your phone (something you have)

www.manaraa.com

ID	Which system would you prefer to use on a regular basis.	Please explain why.	Based on your experience with both systems, if you could create your ideal authentication system, what features would it have? It does not need to be similar to either system you tried.
R_8j4JDxoOmPyY0EB	Google OAuth	Google OAuth was much better because I only had to use one email address and I didn't have to keep reentering my information as much as I did in Mozilla Persona.	I think it would be able to be signed into multiple email accounts at the same time because I have a couple and if I could be signed into both at once that would be ideal. But I did like how both of these systems remembered my information and I didn't have to keep reentering it in as much as I would with a traditional password system.
R_ahixe9VTPVvEhlb	Google OAuth	I just find that i trust the google system more.	I think i would make it more password based actually. i feel like that is a safer method.
R_dnHkCnfHZRfucg5	Neither	They seem the same to me.	Both Mozilla Persona and Google OAuth seemed as ideal as anything I could ever come up with.
R_bkZwCuSDTbZhgnX	Mozilla Persona	It seems more secure in that Facebook is a social media site where sharing is the point, whereas with passwords, privacy and security is the goal.	An ideal authentication system for me would be simple, with the one click verification, but at the same time it would give me the feeling that my accounts were still secure.
R_6sRr2B92X2YnLRr	Google OAuth	I felt it was easy to use as well as safer.	I wish that you would have to enter your Google OAuth password every time you used it to log in to a site. I feel it would be more secure that way, and would still only make you remember one password.
R_37VpLHXutR4oAzb	Neither	they booth seemed exactly the same	I would have a system that used more than one password rather than the traditional one password system
R_ePvTgp05qfhX8rP	Facebook Connect	Facebook is faster	Quick and easy, email-based

www.manaraa.com

ID	Which system would you prefer to use on a regular basis.	Please explain why.	Based on your experience with both systems, if you could create your ideal authentication system, what features would it have? It does not need to be similar to either system you tried.
R_1NgWqbpXq2wXk8d	Neither	My preferred system for managing passwords is LastPass. I like it since that is it's only job. If I had to pick one of the 2 though, I'd pick Google OAuth since my Google account is more important to me and I typically have that account more secure. As far as actually using the system, both Google OAuth and Facebook Connect seemed fairly indistinguishable to me.	It would be it's own company (not tied to my email, or social network accounts) but it would have the ability to be embedded into webpages as a login option since sometimes last pass doesn't do a great job of automatically recognizing where to fill in login info. It would also be awesome if it could use some sort of a usb dongle as my actual password to log in. I plug in my dongle, and I'm logged in to everything, pull out my dongle and I'm logged out. Then the issue would be losing the dongle.
R_56l6XoTISJVp8ih	Google OAuth	I didn't have the email issues with Google, and I trust Google with data-gathering, privacy, and security issues more than facebook. That said, I think it is unlikely that I will adopt either anytime soon.	I like two step verification or systems that are very secure. Ideally it would be a system that only I could access but be quickly accessed without much effort. Biometric readings perhaps would fit that. It would also not require me to memorize useless passwords and usernames.
R_bdyuhU7RoScNHLL	Facebook Connect	I do not use google very much	I like to have a password system. If it is a bank account I would like the system reminds me to change the password after every 6 months or so and new password should not be similar to what I had before (may be last 3 passwords)
R_42vIMvRgaRu4tJX	Facebook Connect	easy to manage	easy logging

www.manaraa.com

ID	Which system would you prefer to use on a regular basis.	Please explain why.	Based on your experience with both systems, if you could create your ideal authentication system, what features would it have? It does not need to be similar to either system you tried.
R_3U8EbALnELRCkK1	Mozilla Persona	They seem equal. However, I might lean towards Persona because I would be worried that logging in with Facebook might result in some unwanted post or that others could see what I'm using even thought it said this would not be the case.	Hm.... I'm not sure. Maybe voice recognition, so that you could say your name and it would know by your voice frequencies that you were indeed the owner. Or by your fingerprint. Someone that is a little faster than a long password, yet secure at the same time.
R_blWEdiC7J16LWw5	Neither	I am just not sure. I think a lot of people would use either one of them, since it's a lot easier than using passwords, but is it safer? I think I would use either one of them if I knew that it was safer than using passwords. I am just wondering these would make it easier for people to commit identity theft, sign in as others, etc.	Well, I have known no other authentication system than passwords and usernames, so I'm not sure what my ideal one would be. I see authentication systems like using a key to unlock a door. I guess my ideal one would be to use a system similar to this, then have further verification by typing in a password, but shorter than regular passwords.

www.manaraa.com

Appendix C

Email-based Usability Study – Participant Responses

ID	Start	End	First system tested	Second system tested
R_bBiTHQ4jerwc3wF	7/28/2014 11:40	7/28/2014 12:05	SAW	Hatchet Auth
R_cIscKPoJf5NWqkl	7/31/2014 16:01	7/31/2014 16:31	Hatchet Auth	SAW
R_8kQBhfFqbMdNeF7	8/1/2014 15:07	8/1/2014 15:36	Hatchet Auth	SAW
R_eYfja7Rhrknn5aZ	8/5/2014 9:04	8/5/2014 9:39	Hatchet Auth	SAW
R_bymx6SVFNUBp9jL	8/5/2014 10:06	8/5/2014 10:46	Hatchet Auth	SAW
R_414o4WYMNSelGIJ	8/5/2014 14:00	8/5/2014 14:46	SAW	Hatchet Auth
R_eG4pegSEXcHRNtz	8/6/2014 9:01	8/6/2014 9:42	Hatchet Auth	SAW
R_5ApOOTWKJqWm40R	8/6/2014 17:06	8/6/2014 17:36	Hatchet Auth	SAW
R_3Cd0JE1AQnRpGAJ	8/7/2014 8:58	8/7/2014 9:39	Hatchet Auth	SAW
R_dfZmEpWvfuGG6hL	8/7/2014 9:58	8/7/2014 10:29	SAW	Hatchet Auth
R_5vVZMv8PuiAoKOx	8/7/2014 11:02	8/7/2014 11:34	Hatchet Auth	SAW
R_3Da2zPXX09raEwl	8/8/2014 17:02	8/8/2014 17:34	SAW	Hatchet Auth
R_6fJ9QBOoH3wFdkh	8/12/2014 11:01	8/12/2014 11:33	SAW	Hatchet Auth
R_3b1nB1v9YFrbFEF	8/12/2014 11:58	8/12/2014 12:31	Hatchet Auth	SAW
R_0As1Mhvj0h0Gs2V	8/18/2014 9:08	8/18/2014 9:39	SAW	Hatchet Auth
R_0SQx0TR5zz7jWHH	8/18/2014 10:08	8/18/2014 10:40	SAW	Hatchet Auth
R_2fVuZTxcAaetZeB	8/23/2014 11:04	8/23/2014 11:31	Hatchet Auth	SAW
R_0rfeCbeA5Nyww1T	8/18/2014 9:39	8/18/2014 10:07	SAW	Hatchet Auth

www.manaraa.com

ID	Gender	Age	Education
R_bBiTHQ4jerwc3wF	Male	18 - 24 years old	Some college or university credit, no degree
R_cIscKPoJf5NWqkl	Male	18 - 24 years old	Some college or university credit, no degree
R_8kQBhfFqbMdNeF7	Female	25 - 34 years old	Some college or university credit, no degree
R_eYfja7Rhrknn5aZ	Female	18 - 24 years old	High school graduate, diploma or the equivalent (for example: GED)
R_bymx6SVFNUBp9jL	Male	18 - 24 years old	High school graduate, diploma or the equivalent (for example: GED)
R_414o4WYMNSelGIJ	Female	18 - 24 years old	Some college or university credit, no degree
R_eG4pegSEXcHRNtz	Male	25 - 34 years old	College or university degree
R_5ApOOTWKJqWm40R	Male	18 - 24 years old	Some college or university credit, no degree
R_3Cd0JE1AQnRpGAJ	Male	18 - 24 years old	Some college or university credit, no degree
R_dfZmEpWvfuGG6hL	Male	18 - 24 years old	Some college or university credit, no degree
R_5vVZMv8PuiAoKOx	Male	18 - 24 years old	Some college or university credit, no degree
R_3Da2zPXX09raEwl	Male	18 - 24 years old	High school graduate, diploma or the equivalent (for example: GED)
R_6fJ9QBOoH3wFdkh	Male	18 - 24 years old	High school graduate, diploma or the equivalent (for example: GED)
R_3b1nB1v9YFrbFEF	Female	25 - 34 years old	College or university degree
R_0As1Mhvj0h0Gs2V	Male	25 - 34 years old	College or university degree
R_0SQx0TR5zz7jWHH	Male	18 - 24 years old	Some college or university credit, no degree
R_2fVuZTxcAaetZeB	Female	18 - 24 years old	Some college or university credit, no degree
R_0rfeCbeA5Nyww1T	Female	18 - 24 years old	Post-Secondary Education

www.manaraa.com

ID	Major	Technical expertise
R_bBiTHQ4jerwc3wF	Computer Science	Intermediate
R_cIscKPoJf5NWqkl	Exercise Science	Intermediate
R_8kQBhfFqbMdNeF7	Exercise Science	Intermediate
R_eYfja7Rhrknn5aZ	Food Science	Intermediate
R_bymx6SVFNUBp9jL	English Major	Intermediate
R_414o4WYMNSelGIJ	Exercise Science	Intermediate
R_eG4pegSEXcHRNtz	Recreation Management	Intermediate
R_5ApOOTWKJqWm40R	Food Science	Beginner
R_3Cd0JE1AQnRpGAJ	Statistics	Intermediate
R_dfZmEpWvfuGG6hL	Biomedical Engineer	Beginner
R_5vVZMv8PuiAoKOx	Psychology/Pre-Med	Intermediate
R_3Da2zPXX09raEwl	accounting	Intermediate
R_6fJ9QBOoH3wFdkh	open major	Beginner
R_3b1nB1v9YFrbFEF	Biochemistry	Beginner
R_0As1Mhvj0h0Gs2V	Business	Intermediate
R_0SQx0TR5zz7jWHH	Chemical Engineering	Intermediate
R_2fVuZTxcAaetZeB	Communication Disorders	Beginner
R_0rfeCbeA5Nyww1T	occupation–BYU faculty; education–TESOL MA	Intermediate

www.manaraa.com

ID	What did you like most about using SAW?	What would you change about SAW?	Would you prefer to use SAW over traditional password-based authentication?	Please explain why.
R_bBiTHQ4jerwc3wF	I liked that for the most part when I forget my password I have to reset it and go through email anyways. This just seems quicker and easier.	.	Yes	As explained above.
R_cIscKPoJf5NWqkl	One less code to enter in was nice.	Looks good.	Yes	Same reason as before. You only need to remember your email password in order to login to all of the SAW authentication systems.
R_8kQBhfFqbMdNeF7	I liked that I didn't have to retype any codes	I think that the window after clicking the link should say something like "you are now connected, this window will close in [] seconds"	Yes	I think that it is very quick, the email response was instant and it doesn't require me to go back and forth between pages with various codes
R_eYfja7Rhrknn5aZ	Again same with the other one, dont' need to remember another extra user name and password. And I like it better that you don't even need to copy and paste the code in like the another one.	I'm not sure if it can changeable, but having an extra pop up is always annoying.	Unsure	I do feel like it's easier. But i am not sure how I feel about if... my mom or brother knows my email address and that password they can get into my bank account... maybe for something some like a social thing or i dont' know i'm not sure.

www.manaraa.com

ID	What did you like most about using SAW?	What would you change about SAW?	Would you prefer to use SAW over traditional password-based authentication?	Please explain why.
R_bymx6SVFNUBp9jL	I liked how this program logs you onto an account without the need for a password at all. Just a verification of your email is all you need.	I would add on at least one or two security questions before just instantly logging into the account.	Unsure	This program is a lot easier to use then the password authentication I use on sites everyday. It is also simpler than the Hatchet program. However it has the same issue with the previous program as it only relies on your email address for verification. If someone were to get a hold of your email address and password, they could log into any of your accounts on web pages that use this software. That is why I would add on the security questions before allowing the program to automatically log in as that not only discourages would be hackers but it adds a feeling of security and sense of ease with people using the software.

www.manaraa.com

ID	What did you like most about using SAW?	What would you change about SAW?	Would you prefer to use SAW over traditional password-based authentication?	Please explain why.
R_414o4WYMNSelGIJ	That you don't have to remember passwords at all.	I would make it so you wouldn't have to have so many tabs open in order to log in quickly. Also, I would be concerned about my email password to which SAW connects to. If someone knew that one password into my email account, then they could get into everything that I use SAW to log into.	No	I didn't like how you have to use so many tabs and click on so many things. I also don't like the possibility that if someone knew my email password then they could access anything that I access with SAW. I also don't like that using SAW would spam up my inbox every time that I log into something. I also wouldn't like it in the situation where if you accidentally log yourself out of something, then you would have to do the whole long SAW thing all over again instead of just quick typing in your password. Cool idea, but I just don't like the logistics of using it.
R_eG4pegSEXcHRNtz	Definitely transferring the funds was easy and quick to use	Having a one time password to get in with saw, or just using my email address as my password.	No	I didn't like the fact that I had to keep requesting a new password using my email address and going through the hassle of transferring the password onto the SAW system.
R_5ApOOTWKJqWm40R	dope.	so sick	No	passwods are easier

www.manaraa.com

ID	What did you like most about using SAW?	What would you change about SAW?	Would you prefer to use SAW over traditional password-based authentication?	Please explain why.
R_3Cd0JE1AQnRpGAJ	Seems a lot like Hatchet :). It is much quicker the second use around and I didn't see why it's any different then needing a password.	It's a little scary if someone I didn't trust had my computer with my email logged in already as most people now a days seem to do. My email is just sitting there and now a hacker doesn't need a password anymore. I'm not sure what I would change other then I would still want a password in addition to an email sent.	No	Reasons explained above. A remote hacker would have to go through one more step which is nice, but if my computer was stolen and my email open for some reason I'm toast and all my accounts I have with SAW.
R_dfZmEpWvfuGG6hL	It only used my email address for the log in password, so it was not hard to remember what my password was.	I would change it to have it not authenticate through email only because it was tedious having to go back and forth to my email to authenticate.	No	Because I do not like to have to authenticate on email every time I need to log in.
R_5vVZMv8PuiAoKOx	It didn't involve copy and pasting like the Hachet one	I would not have it open up so many windows. You need to be on the website to login, and on your email, when you verify on your email it opens up a success page. Lots of older adults could get quite confused about it.	No	Too difficult. I can remember passwords. Why would I want to have to log in to my email and my bank when I just want to login to my bank
R_3Da2zPXX09raEwl	The email that is sent to the email to confirm.	Stop sending an email after the first time.	Yes	To make sure you are who you are supposed to be

www.manaraa.com

ID	What did you like most about using SAW?	What would you change about SAW?	Would you prefer to use SAW over traditional password-based authentication?	Please explain why.
R_6fJ9QBOoH3wFdkh	no need of password	no idea	Unsure	it seems safer without punching in password, but takes some time to open an email account, especially if someone has a slow computer.
R_3b1nB1v9YFrbFEF	It's nice not to have to type in the new passcode each time	The authentication window should close automatically	Unsure	I often log in to accounts on my phone and I worry that this would be difficult using a cell phone and opening multiple windows or logging in to multiple sites just to complete the login
R_0As1Mhvj0h0Gs2V	I didn't really understand what SAW is, but it was nice to use the same email address for everything without having to create multiple accounts	Nothing	Yes	It's nice not to have to register on every site.
R_0SQx0TR5zz7jWHH	No passwords were needed	Make it faster so I don't have to check my email every time I log into a website	No	It took too long to check my email every time I logged in. I prefer using passwords since they can be remembered by internet browsers. And I don't worry about getting hacked since it has never happened, so the additional security isn't appealing.

www.manaraa.com

ID	What did you like most about using SAW?	What would you change about SAW?	Would you prefer to use SAW over traditional password-based authentication?	Please explain why.
R_2fVuZTxcAaetZeB	Easy to use	Automatically close the new tab that confirms log in	Unsure	Same reasons as before - It's easy to use, but I don't know why I'd prefer this over traditional authentification
R_0rfeCbeA5Nyww1T	nothing	I did not like having to send a verification code and check my email every time. It is less effort to just type in a password than to open your email and copy and paste some code.	No	Too cumbersome & time consuming. I have all my important passwords easily memorized and don't like logging into my email and getting a verification code. It takes too long.

www.manaraa.com

ID	What did you like most about using Hatchet?	What would you change about Hatchet?	Would you prefer to use Hatchet over traditional password-based authentication?	Please explain why.
R_bBiTHQ4jerwc3wF	It just feels easier than what I already do after a few weeks of use on a certain system. I forget the password, have to reset it, and continue my life. Which all in all isn't the worst thing but it gets to the point where you just make up random passwords and never remember it so you can just reset it each time. Hatchet seems to the security element of this and take out a lot of the passwordy elements of it which is nice.	I felt like it was just like SAW if you decided to click on the auth code. Why does it need an auth code?	Yes	It still seems more secure and easier than most password based authentication measures. But this also hinges on the security of your email.
R_cIscKPoJf5NWqkl	I like the security that it provides by sending a special code to your email address. It feels secure.	Looks good.	Yes	Sometimes I forget my passwords and have to remember all of them and guess which password is for which website.
R_8kQBhfFqbMdNeF7	I liked that the code was instantly sent, I didn't have to wait for it, like some sites do	NA	Unsure	I often use the same websites multiple times a week, and if there was not a feature that kept me logged in, or a consistent password, the sheer volume of emails I would receive to keep getting into my accounts would be too much.

www.manaraa.com

ID	What did you like most about using Hatchet?	What would you change about Hatchet?	Would you prefer to use Hatchet over traditional password-based authentication?	Please explain why.
R_eYfja7Rhrknn5aZ	it's cool that i can just remember my email address and not worry about remembering another account name and passwords.	i do feel like it slows down the logger in process and your email inbox would end up having tons of code mails...	Unsure	as explained before
R_bymx6SVFNUBp9jL	I liked how I didn't have to remember or create my own password. I also liked how it only required my email address and the password that was sent to me from the websites.	I'd also ask for the username of the individual and a security question for the more important sites such as the bank account.	Unsure	Though it offers more protection to have a randomly assigned password, most people don't log off certain websites every time they are on their personal computers or at home. Many people just have the computer save their passwords for them, me included. But if someone went and hacked our accounts and changed the email address in the account, they wouldn't receive anymore passwords to get into their accounts.

www.manaraa.com

ID	What did you like most about using Hatchet?	What would you change about Hatchet?	Would you prefer to use Hatchet over traditional password-based authentication?	Please explain why.
R_414o4WYMNSelGIJ	That it gave you the option to click on the link or just type in the passcode	make it possible to easily copy/paste the passcode with maybe another place in the email where the code isn't a link already. I would make it consistent in emailing passcodes that worked the first time.	No	It was inconsistent with logging me in. I got like 20 emails from them trying to log into the bank during those tasks, and I never was able to log into the bank, so I will confess that I made my task numbers up. The passcodes need to work flawlessly. It makes you angry to not be able to log into your stuff.
R_eG4pegSEXcHRNtz	Definitely the convenience to use the system and it would be a more secure site if it can connect to other banks.	Have a one time password instead of a bunch of one time codes, which would logging in to the system more convenient.	No	Due to the inconvenience and spending a couple of extra minutes to get a password and submit a different password to the hatchet system.
R_5ApOOTWKJqWm40R	I liked that its called hatchet	use passwords that i choose	No	password is faster. It stinks having to look at an email every time. If you cant remember your password you shouldnt be using the internet
R_3Cd0JE1AQnRpGAJ	It does add a layer of security that a simple password does not, because you need a password to get into an email anyways.	Emails are cumbersome. I received a lot just in the time it took to take this study. If there was a way for the email to auto-delete or make it disappear once used that would be nice.	Unsure	I like the added step for security especially if I was on my own computer using my own tabs, but too many emails. I would probably consider using a junk email for this

www.manaraa.com

ID	What did you like most about using Hatchet?	What would you change about Hatchet?	Would you prefer to use Hatchet over traditional password-based authentication?	Please explain why.
R_dfZmEpWvfuGG6hL	It used just my email for authentication.	I would not have the user go to their email account to authenticate the log in every time you need to log in.	No	It was very tedious having to use my email to authenticate.
R_5vVZMv8PuiAoKOx	If someone gets a password to something it is only a one time use.	Nothing. It seems to be doing the idea you have it doing	No	It seems like too much. I mean what if I login to see something. Logout but then remember I need to log back in. I can't just type in the password I know, I will have to have them send somethign to my email and then use that to log back in again. It seems more secure but it isn't fast, and lots of people prefer fast on their computer. Maybe I would use it for really secure things but not some forum I signed up for or anything like that. It is nice because the password is one time use so it is safer, but I guess if someone gets your email password they can get everything
R_3Da2zPXX09raEwl	Using an email to authenticate	Only use an email once each day	Yes	It is a good way to make sure who you are
R_6fJ9QBOoH3wFdkh	safe	too much work	No	too much work, don't like to copy and paste

www.manaraa.com

ID	What did you like most about using Hatchet?	What would you change about Hatchet?	Would you prefer to use Hatchet over traditional password-based authentication?	Please explain why.
R_3b1nB1v9YFrbFEF	I think that using the email address and creating a new passcode each time you log in is a good way to make it harder to break into someone's account but it's somewhat cumbersome.	It's just a pain to have to log in to your email for the new code each time you want to get on.	Unsure	I think that it could be useful for things like bank accounts (like it's shown here) but not for other accounts.
R_0As1Mhvj0h0Gs2V	It's similar to SAW- don't have to create multiple accounts	Nothing	Yes	Don't have to create multiple accounts for each site
R_0SQx0TR5zz7jWHH	Didn't need passwords, had the option to click links in emails or copy a password.	Make it faster to use so I don't have to keep checking my email.	No	Same as with the SAW; using passwords is faster since browsers remember them. I would rather not have to check my email every time I log in to a website. But perhaps I would use it for something like a bank account where I would care more if my password was stolen. Having the option in any case would be good, I think.
R_2fVuZTxcAaetZeB	It was straightforward and pretty consistent.	Automatically shut the new tab that opens when you click on the link in your email to authorize log in	Unsure	I don't find traditional authentication too difficult, but this system is pretty simple too - I'm indifferent

www.manaraa.com

ID	What did you like most about using Hatchet?	What would you change about Hatchet?	Would you prefer to use Hatchet over traditional password-based authentication?	Please explain why.
R_0rfeCbeA5Nyww1T	nothing	I think it was the same as the other system, so I would have the same comments. Having to check your email & enter a verification code that's new every time is cumbersome.	No	Takes too much time. You have to copy & paste a code instead of just entering in your password.

www.manaraa.com

ID	Which system would you prefer to use on a regular basis.	Please explain why.	Based on your experience with both systems, if you could create your ideal authentication system, what features would it have? It does not need to be similar to either system you tried.
R_bBiTHQ4jerwc3wF	SAW	I just didn't understand why Hatched needed a code when I could just click on it and it did exactly what SAW did.	Perfect usability and perfect security.
R_cIscKPoJf5NWqkl	SAW	One less code to copy paste.	I like how these systems perform.
R_8kQBhfFqbMdNeF7	SAW	It is easier to use and cuts the time it takes to connect to the website	Ideally, I haven't thought about it before. I would do something similar to SAW and have the new tab close itself.
R_eYfja7Rhrknn5aZ	SAW	don't need to even copy and paste the code in.	I couldn't think of anything on top of my head but I would probably liek SAW but without the extra tap popping up.
R_bymx6SVFNUBp9jL	SAW	It is easier to use and it removes the need for a password all together.	I think my ideal system would be the SAW system but have it ask personal security questions before it automatically allows access to your account. For example , before it logged you into your bank account, a smaller but separate window would pop up on your screen asking for the date of your wedding anniversary or how many trophies you earned in elementary school. Basically it would ask you questions that you created and only you knew the answer to as they are personal to you. That would then add an extra feeling of safety and security for me as a customer as I know that having a form of 2-step identification is a greater hassle to hackers then it is to me.
R_414o4WYMNSelGIJ	None of the above	I like using a password better. Even though you have to remember them, you can at least get in more quickly and it doesn't fill up your inbox.	finger-print identification on the keyboard as you type your password?

www.manaraa.com

ID	Which system would you prefer to use on a regular basis.	Please explain why.	Based on your experience with both systems, if you could create your ideal authentication system, what features would it have? It does not need to be similar to either system you tried.
R_eG4pegSEXcHRNtz	Hatchet Auth	Hatchet Auth is more convenient than SAW due to the convenience of using less passwords than SAW	My ideal authentication system would required a user to have a password and a username, just like the BYU student portal, to add more security, but also the convenience to maintain your username and password without a period of time where you had to change your password, unless you really want to change your password.
R_5ApOOTWKJqWm40R	None of the above	I like traditional passwords better. Its dumb constantly navigating to my email. I just want to navigate to my email if i forget my password tahts it	passwords.
R_3Cd0JE1AQnRpGAJ	None of the above	It seems to take out the need for a password. I know you need one to get into your email which makes it seems like there is an extra layer of protection, but I keep my email open most times and never use the password.	I like the ideas presented with Hatchet Auth and SAW, but I need a password with it as well. Some would say that is too much, but I wouldn't mind using SAW or Hatchet if there was an added password that I could make different then the one I use for my email. Then a hacker has to get past my email password and my SAW or HA password. Meanwhile it would take me an extra 3 seconds to get from login to login.
R_dfZmEpWvfuGG6hL	None of the above	It was tedious using my email to authenticate the link each time I had to log in.	I would create a system that used a more complex password pattern or code that would be very difficult for another person to replicate. I do not like the use of email to ensure security log on.

www.manaraa.com

ID	Which system would you prefer to use on a regular basis.	Please explain why.	Based on your experience with both systems, if you could create your ideal authentication system, what features would it have? It does not need to be similar to either system you tried.
R_5vVZMv8PuiAoKOx	Hatchet Auth	It seemed safer. Also I would rather copy and past than open up a million windows all the time whenever I try to login to something	I would rather stay on the page I am trying to log onto. It is annoying to have to jump back and forth. Maybe if there was some way the page could verify me
R_3Da2zPXX09raEwl	None of the above	Too many times that I need to open my email to authenticate	First off with authenticated email then just look in using a password.
R_6fJ9QBOoH3wFdkh	SAW	easier	no clue
R_3b1nB1v9YFrbFEF	SAW	There's no way of getting codes mixed up using this sort of authentication system	Whatever the system is, it has to send the confirmation emails very quickly! I highly dislike waiting for emails to come so that I can log in to accounts I create.
R_0As1Mhvj0h0Gs2V	SAW	I had to choose one but I wouldn't care because they're so similar. I would use either.	It would be easy to use
R_0SQx0TR5zz7jWHH	None of the above	I find them similar enough to not have a preference.	Probably nothing different. The main problem, the inconvenience of having to check email when logging on a website, can't be automated without sacrificing security.
R_2fVuZTxcAaetZeB	Hatchet Auth	They were both very similar to me - either would be easy to use!	Not sure, these were both good systems and I can't think of any other way to create an authentification system
R_0rfeCbeA5Nyww1T	None of the above	Take too much time	Fingerprint recognition

www.manaraa.com

ID	What did you like most about using the plugin?	What would you change about the plugin?	Would you prefer to use the plugin over traditional password-based authentication?	Please explain why.
R_bBiTHQ4jerwc3wF	It was just so easy compared to anything else out there. Because it was using SAW I also felt like it was a lot more secure.	Even though I felt it was more secure than traditional password-based authentication, I question what the plugin does with my email credentials. A better explanation on that would be nice. "So we can access your account" sounds pretty bad to me.	Yes	Reasons explained above.
R_cIscKPoJf5NWqkl	I liked how the plugin automatically authenticated by login.	The plugin is cool because it is one less step; however, I personally like to know that I am in control as I do not know how the plugin works on the back end.	Yes	Easy.
R_8kQBhfFqbMdNeF7	It was so fast and seamless. I didnt have to keep going back to my email address	NA	Yes	It is simply easier and safer.
R_eYfja7Rhrknn5aZ	nothing much... i don't understand what the difference is between this one and the SAW	no popping up tab	Unsure	about security issue as before.
R_bymx6SVFNUBp9jL	I liked how it didn't even have to send me links or tokens to my email and how those were instantly just used on the page.	Again, I would still have the security question option.	Unsure	Again, I would add the security question option because it isn't very secure or confidence boosting to have only your email address between you and a potential hacker.

www.manaraa.com

ID	What did you like most about using the plugin?	What would you change about the plugin?	Would you prefer to use the plugin over traditional password-based authentication?	Please explain why.
R_414o4WYMNSelGIJ	That you didn't really have to do anything. It logged you in quickly.	Make it work consistently. I was never able to get into the banking website, so I will confess again that I just made up a number.	No	Because it was inconsistent in logging me in. If it was consistent, then I would like a LOT more.
R_eG4pegSEXcHRNtz	Definitely the convenience of searching for the plugin codes, which made the process go more quickly and smoothly.	Like the BYU portal, have the user the luxury of a one time username and password to use frequently and securely.	No	The price to have the traditional plugin requires a little more work to constantly retrieve passwords when a one time secure password works frequently without the risk of identity theft.
R_5ApOOTWKJqWm40R	Fast	Faster	Yes	Its dope
R_3Cd0JE1AQnRpGAJ	It skips the email process which is super nice and makes things just slightly quicker for me.	Again though with someone using my computer my email is wide open and the plugin working they have access to all my accounts.	No	Not as currently set up. If there is one more password to type in then yes I would consider using it all the time.
R_dfZmEpWvfuGG6hL	It was very fast to log on to my account	Nothing	Yes	It was very fast and easy.
R_5vVZMv8PuiAoKOx	It was faster and easier	Remind people to turn it off somehow because I could see a lot of people leaving it on and then everything is open to whomever gets on the computer	No	If i forget to turn it off one day it is just like I am having my computer save all my passwords for me. Everything is open to everyone
R_3Da2zPXX09raEwl	email to authenticate	too many emails	No	too many emails to authenticate
R_6fJ9QBOoH3wFdkh	fast and safe	nothing	Unsure	easy

www.manaraa.com

ID	What did you like most about using the plugin?	What would you change about the plugin?	Would you prefer to use the plugin over traditional password-based authentication?	Please explain why.
R_3b1nB1v9YFrbFEF	It's very nice not to have to log in to my email each time I want to access the account	I'm really not sure how it works or what it does, maybe explain that	Yes	It's much easier to use and doesn't require me to receive an email verification every time I want to authenticate my account.
R_0As1Mhvj0h0Gs2V	It did not work	It did not work	Yes	I would want to because it would make the process much faster, but it didn't work for me.
R_0SQx0TR5zz7jWHH	It was really fast and I don't have to remember passwords	Nothing as long as I don't get hacked somehow	Yes	I don't have to type or remember passwords
R_2fVuZTxcAaetZeB	Much simpler! Faster to log in and less clicking	Nothing	Yes	I don't have to deal with my email account

www.manaraa.com

ResponseID	Would you use the plugin if a site enabled SAW or Hatchet authentication?	Please explain why.
R_bBiTHQ4jerwc3wF	Yes	As long as I was 100% sure that nothing was being done with my credentials, this plugin combined with a better authentication method seems like a great combination of security and usability.
R_cIscKPoJf5NWqkl	No	I don't understand the back end workings of plugins and personally don't feel as secure using it. I feel as if someone else could get my passwords easier.
R_8kQBhfFqbMdNeF7	Yes	It is so simple. The security is top notch because the code is 1 time use, and the ease saves you the time of checking your email and clicking on extra things to get to where you want to go.
R_eYfja7Rhrknn5aZ	Unsure	I guess i didn't quite understand what difference it makes.
R_bymx6SVFNUBp9jL	No	Though it's easier to use, it also then makes it easier to hack as someone who has my email can use it to log into a site with SAW or Hatchet authentication and use it to get into my accounts.
R_414o4WYMNSelGIJ	Unsure	The inconsistency and I don't know how much "safer" it is when compared to using a password. Could internet hackers thwart the system easily and just get their own codes to everything?
R_eG4pegSEXcHRNtz	No	Again, You can have a one time secure password without having the constantly change passwords using SAW or plugin, the process is more time consuming and unnecessary.
R_5ApOOTWKJqWm40R	Yes	Its dope
R_3Cd0JE1AQnRpGAJ	Yes	I really like the ease that the plugin allowed me to use. If it would then just transfer me to one more page with an extra password authentication then I would be very pleased with it.
R_dfZmEpWvfuGG6hL	Yes	It was very simple with no email authentication.
R_5vVZMv8PuiAoKOx	Yes	It seems safe. As long as I don't have to do it all the time I might use it for secure financial information
R_3Da2zPXX09raEwl	Yes	so that I don't need to go back to my email all the time to authenticate it
R_6fJ9QBOoH3wFdkh	Unsure	no clue
R_3b1nB1v9YFrbFEF	Yes	So much easier!
R_0As1Mhvj0h0Gs2V	Yes	It would be more convenient
R_0SQx0TR5zz7jWHH	Yes	The plugin makes it a lot easier and faster, and the plugin offers the same advantages as mentioned above.
R_2fVuZTxcAaetZeB	Yes	It's easy to use

www.manaraa.com

Appendix D

QR Code-based Usability Study – Participant Responses

www.manaraa.com

ID	Start	End	First system tested	Second system tested
ID	Start Date	End Date	System tested first	System tested second
R_6KCTzeR7e5zpqxn	10/7/2014 10:52	10/7/2014 11:28	WebTicket	Snap2Pass
R_bClxjKppXDffxg9	10/7/2014 11:29	10/7/2014 12:03	Snap2Pass	WebTicket
R_1LFkuSVsS1QebAN	10/7/2014 16:25	10/7/2014 16:51	WebTicket	Snap2Pass
R_5sXtREpPzK9qjE9	10/8/2014 13:40	10/8/2014 14:12	WebTicket	Snap2Pass
R_51qDN7o1EQjrjeZ	10/8/2014 16:57	10/8/2014 17:36	Snap2Pass	WebTicket
R_6WiALrOVrhUUJ6Z	10/9/2014 9:06	10/9/2014 9:56	Snap2Pass	WebTicket
R_cT7Pc2p04RNLEzP	10/9/2014 10:33	10/9/2014 11:12	Snap2Pass	WebTicket
R_3UG1RXhhQ6s40bX	10/9/2014 11:13	10/9/2014 11:48	Snap2Pass	WebTicket
R_cNOWy7V7LzIASwJ	10/9/2014 12:39	10/9/2014 13:14	WebTicket	Snap2Pass
R_3mBEEslyB2IZ5dP	10/9/2014 13:15	10/9/2014 13:56	WebTicket	Snap2Pass
R_23rMao3vFfDRPV3	10/9/2014 14:58	10/9/2014 15:34	Snap2Pass	WebTicket
R_5mqZ2gmmRkiz4yN	10/10/2014 9:01	10/10/2014 9:35	Snap2Pass	WebTicket
R_2mkjlWunN1TwXyd	10/10/2014 10:02	10/10/2014 10:33	Snap2Pass	WebTicket
R_7aOgANH2pnRL0kR	10/10/2014 11:58	10/10/2014 12:29	Snap2Pass	WebTicket
R_eLP2c46TvdTmIlv	10/10/2014 12:32	10/10/2014 13:05	Snap2Pass	WebTicket
R_77mZgvoFdVDMru5	10/10/2014 13:11	10/10/2014 13:38	WebTicket	Snap2Pass
R_cx1B6PRQMET08fj	10/10/2014 13:06	10/10/2014 13:45	WebTicket	Snap2Pass
R_5p8eolZHXyg4kFD	10/10/2014 15:59	10/10/2014 16:36	Snap2Pass	WebTicket
R_cHmSPZ3ZfTgNf0N	10/10/2014 16:00	10/10/2014 16:44	WebTicket	Snap2Pass
R_5BJB54dO8nC5i2F	10/10/2014 16:57	10/10/2014 17:48	Snap2Pass	WebTicket
R_6KijBG8AxuEkjU9	10/11/2014 9:00	10/11/2014 9:41	WebTicket	Snap2Pass
R_9LfxuVw8nsdumIB	10/11/2014 10:25	10/11/2014 11:08	WebTicket	Snap2Pass
R_cunVi2n6jS4ESLb	10/11/2014 11:40	10/11/2014 12:06	WebTicket	Snap2Pass
R_eFp31sr7MoRhSpn	10/11/2014 13:38	10/11/2014 14:19	WebTicket	Snap2Pass
R_b3jcdxudSXLCsuN	10/11/2014 13:39	10/11/2014 14:34	WebTicket	Snap2Pass

www.manaraa.com

ID	Gender	Age	Education
R_6KCTzeR7e5zpqxn	Male	18 - 24 years old	Some college or university credit, no degree
R_bClxjKppXDffxg9	Female	18 - 24 years old	Some college or university credit, no degree
R_1LFkuSVsS1QebAN	Female	18 - 24 years old	High school graduate, diploma or the equivalent (for example: GED)
R_5sXtREpPzK9qjE9	Female	18 - 24 years old	Some college or university credit, no degree
R_51qDN7o1EQjrjeZ	Male	25 - 34 years old	Some college or university credit, no degree
R_6WiALrOVrhUUJ6Z	Male	18 - 24 years old	Some college or university credit, no degree
R_cT7Pc2p04RNLEzP	Female	18 - 24 years old	Some college or university credit, no degree
R_3UG1RXhhQ6s40bX	Male	18 - 24 years old	Some college or university credit, no degree
R_cNOWy7V7LzIASwJ	Female	25 - 34 years old	College or university degree
R_3mBEEslyB2IZ5dP	Male	18 - 24 years old	Some college or university credit, no degree
R_23rMao3vFfDRPV3	Male	25 - 34 years old	Some college or university credit, no degree
R_5mqZ2gmmRkiz4yN	Male	18 - 24 years old	Some college or university credit, no degree
R_2mkjlWunN1TwXyd	Male	18 - 24 years old	Some college or university credit, no degree
R_7aOgANH2pnRL0kR	Male	18 - 24 years old	Some college or university credit, no degree
R_eLP2c46TvdTmIlv	Female	18 - 24 years old	College or university degree
R_77mZgvoFdVDMru5	Male	18 - 24 years old	Some college or university credit, no degree
R_cx1B6PRQMET08fj	Female	18 - 24 years old	Some college or university credit, no degree
R_5p8eolZHXyg4kFD	Male	18 - 24 years old	Some college or university credit, no degree
R_cHmSPZ3ZfTgNf0N	Female	18 - 24 years old	Some college or university credit, no degree
R_5BJB54dO8nC5i2F	Male	18 - 24 years old	Some college or university credit, no degree
R_6KijBG8AxuEkjU9	Female	18 - 24 years old	Some college or university credit, no degree
R_9LfxuVw8nsdumIB	Female	18 - 24 years old	Some college or university credit, no degree
R_cunVi2n6jS4ESLb	Female	18 - 24 years old	Some college or university credit, no degree
R_eFp31sr7MoRhSpn	Male	18 - 24 years old	Some college or university credit, no degree
R_b3jcdxudSXLCsuN	Female	18 - 24 years old	College or university degree

www.manaraa.com

ID	Major	Technical expertise
R_6KCTzeR7e5zpqxn	physical education	Beginner
R_bClxjKppXDffxg9	Computer Science	Intermediate
R_1LFkuSVsS1QebAN	Pre-nursing	Beginner
R_5sXtREpPzK9qjE9	Biology	Intermediate
R_51qDN7o1EQjrjeZ	Chemical Engineering	Intermediate
R_6WiALrOVrhUUJ6Z	Business	Intermediate
R_cT7Pc2p04RNLEzP	Nutritional Science	Intermediate
R_3UG1RXhhQ6s40bX	Chemical Engineering	Intermediate
R_cNOWy7V7LzIASwJ	Art History Graduate Student	Intermediate
R_3mBEEslyB2IZ5dP	Undeclared major - considering Political Science	Intermediate
R_23rMao3vFfDRPV3	Psychology	Intermediate
R_5mqZ2gmmRkiz4yN	Exercise Science(Pre-Dent)	Intermediate
R_2mkjlWunN1TwXyd	Electrical Engineering	Intermediate
R_7aOgANH2pnRL0kR	Exercise Science	Intermediate
R_eLP2c46TvdTmIlv	Master's of Social Work student	Intermediate
R_77mZgvoFdVDMru5	Actor	Intermediate
R_cx1B6PRQMET08fj	Exercise Science	Intermediate
R_5p8eolZHXyg4kFD	Student	Intermediate
R_cHmSPZ3ZfTgNf0N	Media Arts	Advanced
R_5BJB54dO8nC5i2F	Public Health	Beginner
R_6KijBG8AxuEkjU9	English Teaching	Intermediate
R_9LfxuVw8nsdumIB	Japanese	Intermediate
R_cunVi2n6jS4ESLb	Pre-Nursing	Intermediate
R_eFp31sr7MoRhSpn	economics	Intermediate
R_b3jcdxudSXLCsuN	Bachelor of Sciencin Nursing	Intermediate

www.manaraa.com

ID	What did you like most about using Snap2Pass?	What would you change about Snap2Pass?	Would you prefer to use Snap2Pass over traditional password-based authentication?	Please explain why.
R_6KCTzeR7e5zpqxn	fast and easy	nothing	No	just not used to it and I dont have a smart phone either. i also would want to buy one just so i could log in to something faster
R_bClxjKppXDffxg9	I thought the technology was cool. You can snap a code to sign yourself in!	Maybe allowing it to take screen shots somehow so the users can use it on the internet on their mobile devices.	Unsure	To me, it's just as easy to type in my name a password. I can type the log in probably faster than taking my phone out and using the app. At the same time, I don't have to remember my password as long as I have my phone! So I'm not sure what I'd use.
R_1LFkuSVsS1QebAN	I liked that it was more convenient requiring only a phone and not the printer like the web ticket. It responded quickly and this time displayed an image of the code to line up the computer image with.	I can't think of anything I would change.	Unsure	It would make me nervous having all the passwords I need on my phone. For instance, if I forgot or lost it somewhere I could be inconvenienced with having to then make a username and password for all the websites I need, or if it was stolen and the password on my phone compromised somebody could easily access all of my personal and financial information. Other than that worry I liked it better than password-based authentication

www.manaraa.com

ID	What did you like most about using Snap2Pass?	What would you change about Snap2Pass?	Would you prefer to use Snap2Pass over traditional password-based authentication?	Please explain why.
R_5sXtREpPzK9qjE9	Perhaps your passwords are safer this way.	It seems unfortunate that you have to have a smart phone and you also have to have it with you. What if you want to log in and you do not have your phone on you?	No	I do not even have a smart phone, and sometimes people don't have their phone handy, or lost it. It is certainly not more convenient that just typing in a password. Maybe the benefit is supposed to be safety, but I'm not sure it's worth it.
R_51qDN7o1EQjrjeZ	It was fast. There also are not a lot of other confusing links or "noise".	Nothing	Unsure	I am not sure about how secure it would be. I just have not thought about it before and I would like to see if other people have concerns with it.
R_6WiALrOVrhUUJ6Z	I liked having to only have to scan a QR code to log into a site	I would like to have some type of password on the app so that if my phone was stolen no one could log into my websites	No	I feel a username and password would be more secure
R_cT7Pc2p04RNLEzP	taking a picture takes less time and has less room for error than typing a username and password	It is not very aesthetically pleasing on the phone screen	Yes	taking a picture takes less time and has less room for error than typing a username and password
R_3UG1RXhhQ6s40bX	It is much faster and much more intuitive than a system based on long passwords	I would give users more information about security or have them somehow confirm their identity in another way as well	Unsure	It's easier than using a traditional password system, but it requires the use of a device that could be lost or stolen. Also I don't have a smartphone.
R_cNOWy7V7LzIASwJ	Not having to remember passwords	I don't know much about smart phones	Yes	To avoid passwords

www.manaraa.com

ID	What did you like most about using Snap2Pass?	What would you change about Snap2Pass?	Would you prefer to use Snap2Pass over traditional password-based authentication?	Please explain why.
R_3mBEEslyB2IZ5dP	It was on my phone, so I did not have to worry about printing out paper, like on the WebTicket.	Nothing	Yes	I LOVE this! It was easier to use than a normal password and username, and since it uses a normal QR code reader, you can use it very easily - that was my favorite part, the simplicity of using a QR reader!
R_23rMao3vFfDRPV3	If it is as secure as password protected sites, it could be easier than typing in passwords and usernames. It's quick if the app is already open and your phone is on.	From the way I used it, it seemed like you had to rotate your phone to be horizontal in order to scan QR codes. I'd prefer the option of keeping it all vertical.	Yes	If I was in a hurry, I could start logging in to a computer (by opening the app on my phone) before reaching the keyboard. It could be fast, but wide adoption among all the sites that I frequently need to log into would have to be in place. I don't think I'd use it if it was only for 1-2 specific sites.
R_5mqZ2gmmRkiz4yN	Easy way to log in to an account without having to remember a password	I thought the instructions were somewhat vague so it took me a few minutes to get the hang of it.	No	I think I could log in to my accounts more quickly with traditional password-based athentication.
R_2mkjlWunN1TwXyd	I didn't have to type anything	take out the confirmation before log in, it wastes time before the connection can be made	Unsure	It was pretty fast, and logging in was really easy, but I think the time it takes is about the same

www.manaraa.com

ID	What did you like most about using Snap2Pass?	What would you change about Snap2Pass?	Would you prefer to use Snap2Pass over traditional password-based authentication?	Please explain why.
R_7aOgANH2pnRL0kR	It makes logging in pretty easy	It seems pretty easy to use.	Unsure	My passwords are all already saved in the computer so I just have to click the login button instead of taking a picture. I don't always have my phone out but it is often in my pocket. I would need the application to always be up in order to use it.
R_eLP2c46TvdTmIlv	I can log in quickly.	I think the application was fine. I was a little confused by the instructions.	No	Security reasons. If someone took my phone they could login to my accounts without having to type in the password.
R_77mZgvoFdVDMru5	it was fast. no paper. no camera	my user friendly look to the program	Yes	if it was able to remember my passwords in a way that I never had to use them to log in again. Like when you go to the computers in the library and have to login every time... it can be lame.
R_cx1B6PRQMET08fj	Super fast! The paper sometimes took a while to read, but the QR code was read instantaneously.	Nothing?	Yes	Seems safer since my phone is password protected and with me most of the time. Faster, pretty fun to use!
R_5p8eolZHXyg4kFD	It was quick, easy, and I did not need to worry about memorizing passwords.	I would want to have a secondary check, because then anyone who gets my phone on accident would have access to my banks ect.	Unsure	It would then put a much larger emphasis on a phone. Stolen or lost phones would allow easy access to virtually anything.

www.manaraa.com

ID	What did you like most about using Snap2Pass?	What would you change about Snap2Pass?	Would you prefer to use Snap2Pass over traditional password-based authentication?	Please explain why.
R_cHmSPZ3ZfTgNf0N	I liked how easy it was to use. The simple application and snapping of the photo was easy to use. I liked that the application scanned the code easily as long as the code was in the designated space rather than needing to hold the printed code still as to let the webcam focus better. So, I liked how much faster it was to use Snap2Pass.	I wouldn't change anything about it.	Yes	Snap2Pass was easy and fast to use. Also, the feel of it made me enjoy doing it. I felt technologically literate and the app felt futuristic as a whole, which I enjoyed.
R_5BJB54dO8nC5i2F	It was very simple to log in and everything was clearly placed on the screen. I thought it was pretty easy to navigate.	It seemed fine to me	Unsure	I would need a smartphone with me all the time, and a lot of the time it would be just as easy to log in using a traditional Username and password.
R_6KijBG8AxuEkjU9	It was really quick.	n/a	Unsure	I think I would like to use it because I don't have to remember a bunch of passwords but what happens if someone steals my phone?

www.manaraa.com

ID	What did you like most about using Snap2Pass?	What would you change about Snap2Pass?	Would you prefer to use Snap2Pass over traditional password-based authentication?	Please explain why.
R_9LfxuVw8nsdumIB	It was very handy and quick to not have to remember passwords and usernames every time I logged in. Taking the quick picture of the QR code was very easy.	I think my main problem was this nexus phone and not being familiar with it. I managed to figure out how to turn it on and get to the app every time the screen blacked out but it was frustrating. So mostly just this phone was a problem. The app was very simple and nice.	Unsure	Just a question of security– I don't know how safe it is to have your QR login codes so boldy shown on your screen where other people can take pictures of it. I'm sure the QR codes are changing every time but I still feel a little worried that once someone knows your email they could use that in conjunction with the app and "hack" your account?
R_cunVi2n6jS4ESLb	I think this is brilliant. I love that it's connected to the smart phone, which almost everyone has now. The directions were clear and I got the hang of it really fast.	Honestly, I can't think of much I would change. I think it's very well made and will simplify a lot of lives.	Yes	It was very simply and worked extremely fast. I caught on without too much difficulty.
R_eFp31sr7MoRhSpn	smartphone integration log in with a click of a button basically	wait time for waiting to log in is a little delayed i'd imagine that it would be even more delayed with 3/4g. what if couldnt connect to wifi? i would prefer the scanner to look like a QR code scanner rather than a barcode scanner, just so that it would flow more nicely	Yes	password safety, not needing to memorize a really complex password but can basically log in at a click of a button :) gives me more safety/keeps information safe and password on the code can be updated at regular intervals for even better protection :)

www.manaraa.com

ID	What did you like most about using Snap2Pass?	What would you change about Snap2Pass?	Would you prefer to use Snap2Pass over traditional password-based authentication?	Please explain why.
R_b3jcdxudSXLCsuN	its ok but i needed some help from the technical person to be able to use the system, and if youre a first time user, it takes time to learn it to be able to get used to it	nothing	No	it takes more time to process everything if you use the Snap2Pass over the traditional password-baased authentication :)

www.manaraa.com

ID	What did you like most about using WebTicket?	What would you change about WebTicket?	Would you prefer to use WebTicket over traditional password-based authentication?	Please explain why.
R_6KCTzeR7e5zpqxn	fast	combine it with some sort of facial recognition for more security	No	if i lost my ticket then someone would be able to log-in to my accounts
R_bClxjKppXDffxg9	It was nice that I could just show a scan code to log in.	Don't make it so tedious to do. The process of printing out then showing it to the camera took time.	No	It was too tedious. Printing out a ticket that was very small was a waste of paper. I could easily type in my own info faster than that process. I could also lose the ticket very easily.
R_1LFkuSVsS1QebAN	I liked the speed at which I could log in just holding up the ticket without having to worry about remembering passwords and usernames.	At first I was thrown off because I held it too close and it didn't recognize my ticket, so I would have an example image of how close it should be held/how much of the box the ticket should take up or a description so that the webpage doesn't say the ticket was for the wrong website.	Yes	Simplicity and ease as I explained in the first response.
R_5sXtREpPzK9qjE9	I guess no one can steal your password. But they can just steal your ticket.	I think I would not use WebTicket.	No	It feels less safe. A password only exists in your head, but this ticket is a hard object easily stolen. It seems like more work than just typing in your password. You need more equipment as well. I do not see an upside, but I see plenty of downsides.

www.manaraa.com

ID	What did you like most about using WebTicket?	What would you change about WebTicket?	Would you prefer to use WebTicket over traditional password-based authentication?	Please explain why.
R_51qDN7o1EQjrjeZ	It was quick.	I would inform the user which code was for what.	Unsure	I would want to feel more comfortable with it and I would feel less secure using it.
R_6WiALrOVrhUUJ6Z	It was very quick to use	I don't think I would change anything	No	I feel it is more secure for a person to remember their own password and username for an account
R_cT7Pc2p04RNLEzP	not having to type out my username and password each time	nothing	No	It uses paper unnecessarily. It gives you one more thing to not lose around your house. It took too long to verify the ticket costing me more time than simply typing in my username and password.
R_3UG1RXhhQ6s40bX	I liked how it was the same code every time so I knew what to do each time I was visiting a specific site. Using WebTicket from only one computer in one location would be easier because I could find places for the papers to go so I wouldn't lose them.	I would use a medium that doesn't degrade as fast or get lost as easily as paper, such as a plastic card like a credit card. I would also specify that each computer used would need a different ticket, so a ticket could not be taken from my desk and used to access my bank account from a different computer.	Yes	Because I generally use only one computer in one location where I could find safe, convenient places for the tickets Alternatively I could laminate the tickets and carry them in my wallet.
R_cNOWy7V7LzIASwJ	I really appreciated that you wouldn't have remember a stupid password.	Nothing	Yes	I always struggle to remember different passwords for different websites

www.manaraa.com

ID	What did you like most about using WebTicket?	What would you change about WebTicket?	Would you prefer to use WebTicket over traditional password-based authentication?	Please explain why.
R_3mBEEslyB2IZ5dP	I liked that I did not have to remember any passwords or log-in names - I could just sign in by holding something up to the camera.	The camera could be a little tricky at times, which could be a bigger problem with people who have Parkinson's Disease, or whose hands just shake more than others.	Yes	It is much more simple than having to remember a bunch of passwords.
R_23rMao3vFfDRPV3	I wouldn't need to use up cell phone battery.	I don't like the multiple tickets required. If I needed one for every site they'd get mixed up and lost etc.	No	Too much to worry about. I won't forget my phone when I go to or leave a place, but leaving a scrap of paper that would give anyone access to my bank account is really discomforting.
R_5mqZ2gmmRkiz4yN	Not having to remember a password.	Don't include what website the WebTicket will log in at on the paper.	No	It is faster for me to use a traditional password-based authentication.
R_2mkjlWunN1TwXyd	it focused and logged in pretty fast, and I didn't need to type anything to log it	maybe make the qr code appear on a smart phone, and then hold the phone up to the webcam ?? that way you don't need a printer	No	I don't have a printer
R_7aOgANH2pnRL0kR	You flash a piece of paper to get in.	Maybe one ticket to get into all websites.	No	Risky, too many papers. Too much clutter on the desk top and it could get lost.
R_eLP2c46TvdTmIlv	Logging in without typing.	At its foundation it's a good idea. I don't know what I would change.	No	Too time-consuming. Having to print something and cut it out and also I would need to have a camera on my computer. That isn't always accessible.

www.manaraa.com

ID	What did you like most about using WebTicket?	What would you change about WebTicket?	Would you prefer to use WebTicket over traditional password-based authentication?	Please explain why.
R_77mZgvoFdVDMru5	It was easy for the camera to pic it up. fast switching between websites. It could add a higher level of security	maybe offer a complex code that goes with the Webticket boxes that they could use in case their camera doesn't pick it up.	Unsure	I felt like web ticket was just a fast way to login. I feel like it would be more of a hassle for a personal based use. But it might be good on an academic level where you could pass out this paper to all of your students. Especially if the password was really hard.
R_cx1B6PRQMET08fj	It is a cool concept to not have to enter passwords and usernames.	Not printing the tickets but maybe just having them on a smartphone?	No	I think I might lose the web tickets. I would feel insecure having simple pieces of paper that allow anyone to access my information. I also don't have a webcam at home and don't find it necessary to buy one when I can remember my passwords.

www.manaraa.com

ID	What did you like most about using WebTicket?	What would you change about WebTicket?	Would you prefer to use WebTicket over traditional password-based authentication?	Please explain why.
R_5p8eolZHXyg4kFD	It was quick and easy to log into the various websites, again, didn't need to memorize any passwords.	Make it paperless, which would unfortunately defeat the purpose.	No	I had some confusion when I tried to use one code, but really the other one was the one that let me into the website. I feel that with more sites, this would only increase the issue. More papers would complicate the issue more then help it. Also, i have a hard time keeping track of books, keys, ect, so a small piece of paper would be difficult to keep safe, especially considering I would not consider it a security priority. What most confused me was when I used a code several times, and it worked, but then for the next time it did not. I had to use another code. I am not sure if this was simulating a different site where another code would be necessary, but I did find it confusing.

www.manaraa.com

ID	What did you like most about using WebTicket?	What would you change about WebTicket?	Would you prefer to use WebTicket over traditional password-based authentication?	Please explain why.
R_cHmSPZ3ZfTgNf0N	I liked that my account had a personal WebTicket, the ownership spectacle of it was nice.	I would change the need to print out the code.	Unsure	I find password authentication annoying in anyway but I understand that if I want my accounts to be safe, I must do so. However, I don't know if I would want to use WebTicket as an alternative method. It takes longer and thinking about how I don't have a printer or a smartphone, I wouldn't be able to use WebTicket effectively and/or efficiently. I thought it was innovative and creative but it is not something I would like to use.
R_5BJB54dO8nC5i2F	It was fast and easy to use	Not sure.	Unsure	It can be a little challenging lining up the ticket with the camera. It always seemed my hands were a little shaky so it took a couple seconds for the camera to focus in on the ticket

www.manaraa.com

ID	What did you like most about using WebTicket?	What would you change about WebTicket?	Would you prefer to use WebTicket over traditional password-based authentication?	Please explain why.
R_6KijBG8AxuEkjU9	Very secure	Make it more accurate/consistent.	No	It kept telling me I was using the wrong ticket in the bank and I was using the right one so I don't know what was going on there. I think it's cumbersome and I don't want to loose my ticket. I also don't have a printer.
R_9LfxuVw8nsdumIB	It was nice and easy not having to remember passwords and logging in felt fast and uncomplicated.	I guess depending on how shaky a user's hands are they might not be able to hold the ticket still enough for long enough for the camera to focus on the QR code, but I don't know how to fix that besides putting the camera at a place where you don't have to hold up your hand for so high for so long.	Unsure	It seems that having a physical copy of your password could be dangerous– what if someone stole your ticket and knew your email? It feels like you could easily get your accounts "hacked." Also, having a bunch of different tickets could get cluttered and disorganized even though they have labels on the top half of the ticket, it could turn into a messy Rolodex of tickets or a drawer full of them, etc.

www.manaraa.com

ID	What did you like most about using WebTicket?	What would you change about WebTicket?	Would you prefer to use WebTicket over traditional password-based authentication?	Please explain why.
R_cunVi2n6jS4ESLb	It was really simple to just pick it up and log on without having to remember which password was for which account.	If there was only one ticket that got you into every website, that would be easier than trying to remember which ticket went with which website. But the tasks were simple and overall, I think it worked great!	Unsure	I think it would take some getting used to, and I it would be challenging for every website to integrate it into their current log-in systems. But once that initial step was taken, I think it would be very useful! No forgetting your password again!
R_eFp31sr7MoRhSpn	I like the new idea of using a QR code as a password to log in. There's great potential in many user situations/markets. Saves time and hassle. My passwords can be complex/and safe rather than something that needs to be remembered.	I think it'd be great if i can pull up the picture of the QR code from my Iphone and just show that for logging in instead of paper.	Yes	It seems like it would also protect passwords- instead of using MONKEY, it could be a very complex password that I don't need to remember- this would give me and businesses comfort in security.
R_b3jcdxudSXLCsuN	It was easy to use	nothing	Unsure	It would be a lot easier if we will just use the traditional password-based authentication than to use the WebTicet, but either way, it was fun to use WebTicket though :)

www.manaraa.com

ID	Which system would you prefer to use on a regular basis.	Please explain why.	Based on your experience with both systems, if you could create your ideal authentication system, what features would it have? It does not need to be similar to either system you tried.
R_6KCTzeR7e5zpqxn	Snap2Pass	just because it seems like someone would now have to steal my phone to log into my stuff instead of a loose peice of paper. but i still wouldnt use because i dont have a smart phone.	facial and voice recognition with maybe one of the phone scanners
R_bClxjKppXDffxg9	Snap2Pass	Snap2Pass was easy and quicker of the too. I didn't have to print anything out; I could just use my phone to log in and that was nice.	I think it would be cool to do some sort of print match. I know some laptops have that now, but I think that way would be fastest and most convenient.
R_1LFkuSVsS1QebAN	Snap2Pass	I wouldn't want to have to carry around different pieces of paper whenever I thought I might be logging into a website I need it for–although they are small and labeled well it's another thing to remember and that could make it more inconvenient than simply remembering a password or having my phone.	I would have it be similar to the snap2pass but maybe with a password to get into that app so that it is more secure–there is no way to have a system perfectly secure but if the snap2pass app was harder to access by just anybody on my phone I would like it better.
R_5sXtREpPzK9qjE9	None of the above	I feel no need to stop using just the simple password system. It does not rely on you needing anything else, like a piece of paper or a phone. It is fast and easy.	I do not particularly see a problem with the usual system of passwords. Maybe we could use webcam to do a facial recognition. Or maybe a touch pad with fingerprinting.
R_51qDN7o1EQjrjeZ	Snap2Pass	It was more user friendly and more secure upon my first impression.	I would like it to be quick, but also difficult to log on to without knowing something. I would not want it to have something that was just scan-able.
R_6WiALrOVrhUUJ6Z	WebTicket	I liked webticket because I physically had an authorization I could hold	I liked the webticket but I would also include another way to identify it as well
R_cT7Pc2p04RNLEzP	Snap2Pass	It uses your phone which you are less likely to use than a piece of paper and took less time than typing out a username and password over and over	I liked the Snap2Pass system and would probably do something similar. I also think facial recognition would be easy or voice recognition.

www.manaraa.com

ID	Which system would you prefer to use on a regular basis.	Please explain why.	Based on your experience with both systems, if you could create your ideal authentication system, what features would it have? It does not need to be similar to either system you tried.
R_3UG1RXhhQ6s40bX	Snap2Pass	WebTicket seems needlessly complex, while Snap2Pass is much simpler. The camera system for Snap2Pass also seems more reliable than for WebTicket.	A WebTicket-like system using plastic cards instead of papers
R_cNOWy7V7LzIASwJ	WebTicket	I don't have a smart phone so while the snap2pass is more convenient, for me the web ticket would work better	I don't know. I like the visual element of the snap to pass over traditional passwords that need punctuation and capitals
R_3mBEEslyB2IZ5dP	Snap2Pass	I did not have to print a piece of paper for every code. I can use my phone, which is always with me!	The main key for me is safety. I want my data to be protected, but it is a hassle to remember passwords for every site I visit. The ideal system would scan some part of my body - either eye or thumb - because these are literally ALWAYS with me. A phone may get lost or stolen, but it is much harder to loose a body part.
R_23rMao3vFfDRPV3	Snap2Pass	All in one place, consistent. The webticket requires printing something. Printing things is how people used to do stuff. I don't want the bother	quick. All-in-one. secure.
R_5mqZ2gmmRkiz4yN	None of the above	I would rather use a traditional authentication system because it makes me feel like I am in control. It is also faster for me to just type it in myself	For systems that need a high level of security, I would like a traditional username and password system followed by a biometric sign in where it had face recognition or finger print scanning.
R_2mkjlWunN1TwXyd	Snap2Pass	I don't have a printer with me everywhere I go, so it wouldn't make sense to use webticket most of the time	I think a retina scanner is ideal, zero labor to look into a scanner, and still don't need to worry about anyone seeing my password.

www.manaraa.com

ID	Which system would you prefer to use on a regular basis.	Please explain why.	Based on your experience with both systems, if you could create your ideal authentication system, what features would it have? It does not need to be similar to either system you tried.
R_7aOgANH2pnRL0kR	None of the above	I like having my passwords stored in the computer. It is the easiest. One click, and you are in. Don't have to take a picture or flash something.	Not sure.
R_eLP2c46TvdTmIlv	None of the above	Snap2Pass requires a smartphone/internet which is not always accessible to me. WebTicket requires printing and cutting out when it is easier for me to just type it in and be done.	Simple, quick, universally accessible. Does not require extra work.
R_77mZgvoFdVDMru5	Snap2Pass	way more user friendly. Don't need a camera and dont need a printer.	I really like mobile based things so I would just make a secured one similar to snap2pass.
R_cx1B6PRQMET08fj	Snap2Pass	The paper one was too cumbersome and vulnerable. It seems the Snap2Pass is faster but keeps all the authenticated passwords stored, where the web ticket you'd have to keep track of multiple pieces of paper, which is worse than remembering all of the passwords.	Fingerprints, but that would probably be super expensive. The QR code seems really clever.

www.manaraa.com

ID	Which system would you prefer to use on a regular basis.	Please explain why.	Based on your experience with both systems, if you could create your ideal authentication system, what features would it have? It does not need to be similar to either system you tried.
R_5p8eolZHXyg4kFD	Snap2Pass	It was easier, and did not involve the need to keep track of papers. It worked every time, and was the least confusing to start using . It was easy for me to gab onto, even though I have never used a smart phone before.	Something important is that it would need to be based on something that could not readily be stolen. Paper is easy to steal, and easier to lose. A phone is easy to steal. Either scenario would leave all my confidential information in the hands literally of anyone who took my phone, or found it (if I lost my phone). I think it is important to have something more personal for a password, something that can not be stolen or lost so easily. I think that is why memorized passwords do well. This is a great system, (snap2pass) but I feel it would be better if it had a follow up question pertaining to something personal.
R_cHmSPZ3ZfTgNf0N	Snap2Pass	Snap2Pass was more technilogically friendly and it was a faster process.	heated fingerprint system, where we would put our hands up to the computer screen and the computer would read the fingertips with heat waves from our fingertips.
R_5BJB54dO8nC5i2F	Snap2Pass	I would always have to carry around the web ticket which is not likely. I usually have a smart phone on my however so it seems more convenient to use snap2pass.	I think the featurs that are offered in snap2pass are fine I dont really think there is anything I could add to that
R_6KijBG8AxuEkjU9	Snap2Pass	It was easier, quicker, more accurate	Honestly, I don't know what is and is not secure but I know that I am not good at making secure passwords. I also wouldn't want it to be taken over by someone who found my password journal or ticket or what have you. I just want it to be easy to use mostly.

www.manaraa.com

ID	Which system would you prefer to use on a regular basis.	Please explain why.	Based on your experience with both systems, if you could create your ideal authentication system, what features would it have? It does not need to be similar to either system you tried.
R_9LfxuVw8nsdumIB	Snap2Pass	It was much easier (physically, like holding up your hands-wise) and felt safer than webticket.	Something like Snap2Pass and traditional login username/password seems the best to me, but not necessarily using both together every time, more like alternatives for the same website. If your phone dies you can't use Snap2Pass obviously so you'd need to traditionally log in. I hate those authentication codes that want to make sure you're not a robot though, the ones that make you type in illegible letters and numbers and can take a few frustrating tries and refreshing of codes to get to actually work. I would never want to use that for logging in to online accounts.
R_cunVi2n6jS4ESLb	Snap2Pass	It didn't require any paper, it was just simple and easy to use. It was also a lot more consistent than WebTicket and i didn't have to hold the ticket up to the video monitor.	I think the ideal authentication program would use some kind of DNA tracker that instantaneously recognized that the user was who they said they were and logged in automatically. I think we might be a little far from making that available to the general public though.
R_eFp31sr7MoRhSpn	Snap2Pass	i prefer Snap2pass- for user experience of administrator and for normal user- passwords can be quickly changed without having to reprint papers. Also dont need a webcam. Saves on costs especially for businesses using computers that dont likely have webcams at each computer. Just Scan. It's that simple.	as a potential customer i am still not sold on the security of using this product. but that can be easily solved :) I would definitely use this, especially if it can be used for all of my accounts on any website!
R_b3jcdxudSXLCsuN	Snap2Pass	it takes more time to use the WebTicket thAn of the Snap2pASS thing	nothing

www.manaraa.com

Appendix E

"Championship Round" Usability Study – Participant Responses

www.manaraa.com

ID	Start	End	First system tested	Second system tested	Third system tested
R_9miCYXQ9i3d79kh	10/13/2014 12:02	10/13/2014 12:33	SAW	Google OAuth	Snap2Pass
R_cV02ky60s5h7do9	10/13/2014 12:47	10/13/2014 13:43	SAW	Google OAuth	Snap2Pass
R_0lex09JAUq6vnEh	10/13/2014 14:59	10/13/2014 15:37	Google OAuth	SAW	Snap2Pass
R_ehsAS4vN3w3wLtj	10/13/2014 15:44	10/13/2014 16:35	SAW	Google OAuth	Snap2Pass
R_72Kju3xXcu84ITz	10/14/2014 9:00	10/14/2014 9:46	SAW	Google OAuth	Snap2Pass
R_0ecbAlJyGCZNZGt	10/14/2014 17:22	10/14/2014 17:55	Google OAuth	Snap2Pass	SAW
R_00b6aKUvJ4SmRet	10/15/2014 9:13	10/15/2014 10:10	Snap2Pass	SAW	Google OAuth
R_e3UAnpHjDrOspw1	10/16/2014 11:23	10/16/2014 11:56	Snap2Pass	SAW	Google OAuth
R_eDHzNCOQ9qVWgSN	10/16/2014 12:10	10/16/2014 12:52	SAW	Google OAuth	Snap2Pass
R_4GHGcW8GSkFHTpz	10/16/2014 12:50	10/16/2014 13:25	SAW	Google OAuth	Snap2Pass
R_a5WesSGHcXhv9wF	10/17/2014 12:18	10/17/2014 12:57	Google OAuth	Snap2Pass	SAW
R_37RtpyQWZ6o535H	10/17/2014 13:30	10/17/2014 14:08	Google OAuth	Snap2Pass	SAW
R_0rIOatexMv4gnLD	10/20/2014 12:15	10/20/2014 12:50	Snap2Pass	Google OAuth	SAW
R_9GBx0vLPrWkIlW5	10/20/2014 17:07	10/20/2014 17:45	Google OAuth	SAW	Snap2Pass
R_0wuVuFDRca1ms97	10/21/2014 8:58	10/21/2014 9:29	SAW	Snap2Pass	Google OAuth
R_01G89gBeQkDJzG5	10/21/2014 11:15	10/21/2014 12:02	Google OAuth	SAW	Snap2Pass
R_6KdTYG2JUTNXX6d	10/21/2014 14:02	10/21/2014 14:42	Google OAuth	SAW	Snap2Pass
R_bDVSULp9mIXqeb3	10/21/2014 15:04	10/21/2014 15:36	Google OAuth	Snap2Pass	SAW
R_1HcR75ONOJi7GCx	10/21/2014 14:59	10/21/2014 15:49	Snap2Pass	Google OAuth	SAW
R_9oY48Q67whV8IwB	10/22/2014 9:03	10/22/2014 9:44	SAW	Google OAuth	Snap2Pass
R_9oa0T0VXhLZqAQZ	10/22/2014 11:59	10/22/2014 12:25	SAW	Snap2Pass	Google OAuth
R_8nPTOBrAed4NNVr	10/22/2014 15:38	10/22/2014 16:20	Snap2Pass	SAW	Google OAuth
R_2ht7JxR6ykwtn3n	10/22/2014 17:11	10/22/2014 17:40	Snap2Pass	SAW	Google OAuth
R_0HfLkdsANADLDkp	10/22/2014 17:03	10/22/2014 17:50	Snap2Pass	SAW	Google OAuth
R_3gyXV0lEeDSTVWd	10/23/2014 9:52	10/23/2014 10:33	Snap2Pass	Google OAuth	SAW
R_1RY2gmwyq37Nwjz	10/23/2014 12:04	10/23/2014 12:52	Google OAuth	SAW	Snap2Pass
R_brq2IoDKDaKO0Pr	10/23/2014 17:08	10/23/2014 17:54	Snap2Pass	Google OAuth	SAW
R_dbYw7L1js1hwgLP	10/23/2014 17:08	10/23/2014 17:56	Snap2Pass	Google OAuth	SAW
R_3smFl1r0rn5VCdv	10/24/2014 9:04	10/24/2014 9:41	SAW	Snap2Pass	Google OAuth
R_bDU6qh6foqy618x	10/24/2014 11:52	10/24/2014 12:37	SAW	Google OAuth	Snap2Pass
R_40K63SEypIKCmXP	10/24/2014 14:00	10/24/2014 14:28	SAW	Google OAuth	Snap2Pass

www.manaraa.com

ID	Gender	Age	Education
R_9miCYXQ9i3d79kh	Male	18 - 24 years old	Some college or university credit, no degree
R_cV02ky60s5h7do9	Male	25 - 34 years old	Some college or university credit, no degree
R_0lex09JAUq6vnEh	Female	18 - 24 years old	Some college or university credit, no degree
R_ehsAS4vN3w3wLtj	Female	18 - 24 years old	Some college or university credit, no degree
R_72Kju3xXcu84ITz	Male	25 - 34 years old	College or university degree
R_0ecbAlJyGCZNZGt	Male	18 - 24 years old	Some college or university credit, no degree
R_00b6aKUvJ4SmRet	Male	25 - 34 years old	College or university degree
R_e3UAnpHjDrOspw1	Female	18 - 24 years old	High school graduate, diploma or the equivalent (for example: GED)
R_eDHzNCOQ9qVWgSN	Male	18 - 24 years old	Some college or university credit, no degree
R_4GHGcW8GSkFHTpz	Female	18 - 24 years old	Some college or university credit, no degree
R_a5WesSGHcXhv9wF	-	-	-
R_37RtpyQWZ6o535H	Female	18 - 24 years old	Some college or university credit, no degree
R_0rIOatexMv4gnLD	Male	25 - 34 years old	Some college or university credit, no degree
R_9GBx0vLPrWkIlW5	Male	18 - 24 years old	Some college or university credit, no degree
R_0wuVuFDRca1ms97	Male	18 - 24 years old	Some college or university credit, no degree
R_01G89gBeQkDJzG5	Male	18 - 24 years old	Some college or university credit, no degree
R_6KdTYG2JUTNXX6d	Male	18 - 24 years old	Some college or university credit, no degree
R_bDVSULp9mIXqeb3	Male	25 - 34 years old	Some college or university credit, no degree
R_1HcR75ONOJi7GCx	Female	18 - 24 years old	Some college or university credit, no degree
R_9oY48Q67whV8IwB	Female	18 - 24 years old	High school graduate, diploma or the equivalent (for example: GED)
R_9oa0T0VXhLZqAQZ	Female	18 - 24 years old	Some college or university credit, no degree
R_8nPTOBrAed4NNVr	Male	25 - 34 years old	College or university degree
R_2ht7JxR6ykwtn3n	Male	25 - 34 years old	College or university degree
R_0HfLkdsANADLDkp	Male	18 - 24 years old	Some college or university credit, no degree
R_3gyXV0lEeDSTVWd	Male	18 - 24 years old	Some college or university credit, no degree
R_1RY2gmwyq37Nwjz	Male	18 - 24 years old	High school graduate, diploma or the equivalent (for example: GED)
R_brq2IoDKDaKO0Pr	Male	18 - 24 years old	Some college or university credit, no degree
R_dbYw7L1js1hwgLP	Female	18 - 24 years old	Some college or university credit, no degree
R_3smFl1r0rn5VCdv	Male	18 - 24 years old	Some college or university credit, no degree
R_bDU6qh6foqy618x	Male	18 - 24 years old	Some college or university credit, no degree
R_40K63SEypIKCmXP	Female	18 - 24 years old	Some college or university credit, no degree

www.manaraa.com

ID	Major	Technical expertise
R_9miCYXQ9i3d79kh	Neuroscience	Intermediate
R_cV02ky60s5h7do9	Genetics and Biotechnology	Intermediate
R_0lex09JAUq6vnEh	Elementary Education	Intermediate
R_ehsAS4vN3w3wLtj	Communication Disorders	Intermediate
R_72Kju3xXcu84ITz	Recreation Management	Intermediate
R_0ecbAlJyGCZNZGt	exercise science	Intermediate
R_00b6aKUvJ4SmRet	Public Administration	Intermediate
R_e3UAnpHjDrOspw1	Business	Intermediate
R_eDHzNCOQ9qVWgSN	Accounting	Intermediate
R_4GHGcW8GSkFHTpz	Neuroscience and English majors	Beginner
R_a5WesSGHcXhv9wF	Business Management	Intermediate
R_37RtpyQWZ6o535H	Commmunication Disorders	Intermediate
R_0rIOatexMv4gnLD	entreprenuership	Intermediate
R_9GBx0vLPrWkIlW5	Chemical En	Intermediate
R_0wuVuFDRca1ms97	Neuroscience Major	Intermediate
R_01G89gBeQkDJzG5	Finance	Intermediate
R_6KdTYG2JUTNXX6d	Business	Beginner
R_bDVSULp9mIXqeb3	Mechanical Engineering	Advanced
R_1HcR75ONOJi7GCx	Human Development	Intermediate
R_9oY48Q67whV8IwB	Pre-Illustration	Beginner
R_9oa0T0VXhLZqAQZ	Psychology	Intermediate
R_8nPTOBrAed4NNVr	English major	Intermediate
R_2ht7JxR6ykwtn3n	Urban and Regional Planning	Intermediate
R_0HfLkdsANADLDkp	Political Science	Intermediate
R_3gyXV0lEeDSTVWd	Psychology	Beginner
R_1RY2gmwyq37Nwjz	Accounting major	Intermediate
R_brq2IoDKDaKO0Pr	Elementary Education	Intermediate
R_dbYw7L1js1hwgLP	Elementary Education	Intermediate
R_3smFl1r0rn5VCdv	Neuroscience	Intermediate
R_bDU6qh6foqy618x	Business	Intermediate
R_40K63SEypIKCmXP	Exercise Science	Intermediate

المنارة للاستشارات
www.manaraa.com

ID	What did you like most about using Snap2Pass?	What would you change about Snap2Pass?	Would you prefer to use Snap2Pass over traditional password-based authentication?	Please explain why.
R_9miCYXQ9i3d79kh	Seems safe and secure.	An explanation of what is it/does.	Unsure	I don't necessarily see the problem with the current system. Also, I don't understand how this new one would work.
R_cV02ky60s5h7do9	Man was that cool! :D, so i'm not a smartphone owner, but this app has made me see how cool, practical and safe it can be to log in using a picture from your phone.	I think it's OK	Yes	practical, fast, easy...i would feel a little lazy for not even wanting to type, but I loved the "fun part" of taking the picture and matching the squares, I felt more interaction. (sorry if it sounds a bit childish, but i'm new to this).
R_0lex09JAUq6vnEh	Having two devices involved in logging in makes it securer, I believe, without it being hard. It's really easy to use, and the two responded quickly to each other.	The user interface of the app itself is pretty bare bones. It's functional, but the design isn't especially intuitive. (Really not a problem, though.)	Unsure	Well, if my smartphone was reliable and the two devices could work quickly with each other (I'm afraid the network/wifi/bluetooth would sometimes drop) then yes! I like it. It's simple. But sometimes I wouldn't have my phone–still, it always gave me the option to log in traditionally, so that's not a complaint.

www.manaraa.com

ID	What did you like most about using Snap2Pass?	What would you change about Snap2Pass?	Would you prefer to use Snap2Pass over traditional password-based authentication?	Please explain why.
R_ehsAS4vN3w3wLtj	The use of the phone to log in is nice because only my phone can log me in, which is a good security measure. I also like that I don't have to remember another password and user name, but can simply use my phone instead.	Not sure.	No	I think it is cumbersome to have to pull out my phone every time I want to log in somewhere. I personally am trying to cut back on the amount of time I use my phone and this wouldn't really help with that. It seems too involved and just an added thing that I would have to do to log in.
R_72Kju3xXcu84ITz	The convenience of just taking a picture of the QR code and getting it by email would make the settings a little more private.	I would make the Snap2 Pass to give the option of having to send the QR scanner by email or on the website since some like me would perfer to keep the QR scanner private to get the code on the website only. / / / / /	Yes	These days it's more convenient to just take a picture of a QR code and take
R_0ecbAlJyGCZNZGt	pretty fast and it felt a bit safer than the google one.	nothing. it's pretty cool. I just don't have a smartphone so it wouldn't be very useful for me right now...	Yes	idk, its just cooler and feels safer, even though I don't know if it really would be. placebo affect.

www.manaraa.com

ID	What did you like most about using Snap2Pass?	What would you change about Snap2Pass?	Would you prefer to use Snap2Pass over traditional password-based authentication?	Please explain why.
R_00b6aKUvJ4SmRet	It was super nice to not have to remember which passwords I use for which sites. I've been locked out of my online banking before because I couldn't remember for the life of me which passwords I had used where. Also, Snap2Pass (in theory) seems more secure than using a password that can be stolen so easily, but what would happen if my phone were stolen?	A more interesting GUI might be appealing, though not necessary. A simple tutorial that helps new users learn how to use the app would be great, though not needed in this study.	Unsure	As I mentioned above, it seems like it would be more secure than traditional password authentication, but I can't be sure about that. If somebody stole my phone they'd suddenly have access to all of my accounts associated with Snap2Pass.
R_e3UAnpHjDrOspw1	Easy and fast	Nothing really	Yes	Faster and seems more secure
R_eDHzNCOQ9qVWgSN	It's cool!	Nothing	No	It's not convenient to have to pull out a smart phone and open the app in order to log in. I would be able to log in faster simply by inputting my own password.
R_4GHGcW8GSkFHTpz	I liked not having to go to my email account	I would like to change the fact that you need a phone to use it	No	I don't like using QR codes, it's way easier to just type things in
R_a5WesSGHcXhv9wF	Easy to use.	Nothing	Unsure	Doesn't matter, takes about the same amount of time.

www.manaraa.com

ID	What did you like most about using Snap2Pass?	What would you change about Snap2Pass?	Would you prefer to use Snap2Pass over traditional password-based authentication?	Please explain why.
R_37RtpyQWZ6o535H	It was a lot easier to log in. I can scan a QR code faster than I can input my account name and password.	I don't have a problem with it, except that I would rather that I could do all of the stuff I just did on the smartphone. If I have to go back and forth between the phone and the computer, what's the point of having a smart phone?	No	I lose my phone a lot for one thing. For another, I would rather just log in on the computer where I can have multiple tabs instead of going back and forth between my phone and the computer.
R_0rIOatexMv4gnLD	It was kind of cool to see that it would log in from my phone	make it a three step process. 1. instal snap2pass 2. enroll 3. use	Unsure	well it may create a new form of cyber-crime, that I am not interested in using, and it is not integrated into known products
R_9GBx0vLPrWkIlW5	i think is really innovative	nothing	Unsure	It is really innovative but i don't think is really useful
R_0wuVuFDRca1ms97	It was very fast to log in. Even faster than typing in a username and password, in some cases.	Man, that sound effect was really annoying whenever it would scan a code. I'm sure you can just make the phone vibrate or something, but...definitely consider removing that sound effect.	Unsure	Well, it is fast and easy, but if my computer is out I normally have my phone in my pocket. I don't know if I really want to have to get a new app and start a new habit of keeping my phone out all the time while using certain websites. But in certain circumstances it could be very convenient. Basically I have an overall positive feeling about this system, compared to my negative feeling about the SAW system.

www.manaraa.com

ID	What did you like most about using Snap2Pass?	What would you change about Snap2Pass?	Would you prefer to use Snap2Pass over traditional password-based authentication?	Please explain why.
R_01G89gBeQkDJzG5	I like that instead of a normal code, i was given a QR code that needs to be photographed by a cell phone. It was easy and it was very fast. I loved how quickly it signed in after i took the picture.	Nothing. I loved the way it worked and how quickly it allowed me to access my profile.	Yes	I like the security it brings without having to go between multiple windows in chrome. I like that it uses the mobile device as a means of authentication.
R_6KdTYG2JUTNXX6d	its cool to log on with your phone	more/clearer instructions?	Unsure	how do i know someone else couldnt just use their smartphone to login to my acct?
R_bDVSULp9mIXqeb3	Signed in quickly.	Seems like it is less secure than having a password. Anyone who got a hold of your phone would be able to do banking, access your personal information, etc. / I also don't find QR codes very intuitive or easy to use. Maybe I just don't like having my phone out to take pictures all the time, but I'd rather just sign in the normal way or type in a URL instead of using a QR code.	No	Seems like more of a hassle, need to have my phone with me and take it out to take a picture.

www.manaraa.com

ID	What did you like most about using Snap2Pass?	What would you change about Snap2Pass?	Would you prefer to use Snap2Pass over traditional password-based authentication?	Please explain why.
R_1HcR75ONOJi7GCx	QR codes are just cool	I feel like I still want a password so someone can't get a hold of my phone and automatically get to my banking accounts, so maybe I would change it by adding a password to the Snap2Pass app.	No	I don't find entering my email all that cumbersome in the first place. Having Snap2Pass means that I'd a) have to have a smartphone, b) always have it on me, and c) be extra paranoid about not letting it get into someone else's hands.
R_9oY48Q67whV8IwB	It makes logging in easy–I don't have to worry about forgetting a password, all I need is my phone!	I don't have a Smartphone, so this app wouldn't do me much good.	No	Again, I don't have a smartphone. Also, I'm still worried about security. What happens if I lose my phone? Am I locked out of my accounts? What if someone else gets my phone? Is it safe to leave an opening like this in my secure accounts?
R_9oa0T0VXhLZqAQZ	I loved how convenient and fast it was.	Nothing	Unsure	While Snap2Pass is much easier, phones are easily stolen.
R_8nPTOBrAed4NNVr	It was pretty impressive to login in using the Snap2Pass code. It was interesting to see how quickly the computer website logged me in after I clicked login on my phone.	I have no recommendations at this time.	Unsure	I am unsure of any of the security risks Snap2Pass may involve. Could someone access my information wirelessly by using my phone to computer communication? Is the security really better, or just a new twist on an old idea?

www.manaraa.com

ID	What did you like most about using Snap2Pass?	What would you change about Snap2Pass?	Would you prefer to use Snap2Pass over traditional password-based authentication?	Please explain why.
R_2ht7JxR6ykwtn3n	How easy it was to use	I feel that it was a lot of going back and forth to gain access to things.	Unsure	I feel safer typing in a password. Plus I don't want the NSA or Obama having my passwords.
R_0HfLkdsANADLDkp	the remote log in	maybe the tasks were the frustrating part, but the whole time i wanted to ask the people in charge for help. that was mostly on the setup though	No	no because it was slightly more complected, and anyone with my phone would have password pretty much
R_3gyXV0lEeDSTVWd	being able to log in on the computer from the phone	nothing	Yes	It is easy to scan a code on my phone than try to remember the password.
R_1RY2gmwyq37Nwjz	I like the use of the Smartphone to log in. Integrating the mobile device with the computer is a good idea.	What if you were accessing the site on the mobile device? How would you scan the code?	No	Just because it means i would be unable to use these things on my mobile device. only on my computer
R_brq2IoDKDaKO0Pr	It was easy to use.	More instruction.	No	I feel more comfortable with a password-based authentication.
R_dbYw7L1js1hwgLP	The fact that nobody could just go in and hack your account or anything like that since it is based purely on your specific code with the app	From what I used, I liked it...	Unsure	I like the password because you can access it anywhere, even if you don't have the app handy. But I did like the security the app brought
R_3smFl1r0rn5VCdv	Super easy to just scan it.	I don't want the extra screen that says "login". When I use the app I am wanting to login so no need to ask me. When it is scanned just log me in.	Yes	I have only used the one prior to this one and I hated that one so this one was a huge step up.

www.manaraa.com

ID	What did you like most about using Snap2Pass?	What would you change about Snap2Pass?	Would you prefer to use Snap2Pass over traditional password-based authentication?	Please explain why.
R_bDU6qh6foqy618x	It was quick, and I assume it's relatively safe, unless someone physically steals my phone.	I actually really liked it! the one thing would maybe be after i press the "scan qr code" button, it should leave the phone in the vertical frame. Make it easier to use one handed too. So i can press it with one finger, and hold the device one handed to scan the code. You should have a backup way to log in though, in case I lost my phone, or it's dead.	Yes	It's simple.
R_40K63SEypIKCmXP	That it's a one click thing, and that it uses your phone so it's a two-source protection type thing	Make sure the app doesn't kill your battery on your phone? / Have a back up way to log in to stuff, in case your phone in inaccessible	Yes	It's easier and you don't have to remember passwords

www.manaraa.com

ID	What did you like most about using Google Oauth 2.0?	What would you change about Google Oauth 2.0?	Would you prefer to use Google Oauth 2.0 over traditional password-based authentication?	Please explain why.
R_9miCYXQ9i3d79kh	Easy to log in.	I don't know that it is very secure.	Unsure	I don't know that I would use it.
R_cV02ky60s5h7do9	I guess i liked that I could just log in without typing anything	no comment	No	I don't find it very user friendly or really convenient.
R_0lex09JAUq6vnEh	That it's so easy and doesn't slow you down, but it does log you out when you close. So it has the benefits of security without being annoying to log in every time.	Perhaps if it does make you enter login details periodically, like every two weeks or every month–to maintain some privacy?	Yes	I wouldn't have to remember so many different passwords–that's probably me sacrificing some security right there, though.
R_ehsAS4vN3w3wLtj	I didn't have to go back to my email account every time I wanted to log in. That was nice.	Not sure.	No	Although the system was easy to use due to the fact that I just needed to click on one button to sign in, that is a little scary. I would like to have to authenticate myself every time, so as to preserve my information and identity as best as possible.
R_72Kju3xXcu84ITz	The convenience of just clicking on Google Authorization makes it so nice not to go back to my emails and get my password.	Making sure it has the necessary private settings so that Google would not be authorized to look at your checking account.	Unsure	While I love the convenience of not having to check my emails to use my password, it would be a privacy threat since google could access this account. I would use it If google would not have authority to see my checking or savings account.

www.manaraa.com

ID	What did you like most about using Google Oauth 2.0?	What would you change about Google Oauth 2.0?	Would you prefer to use Google Oauth 2.0 over traditional password-based authentication?	Please explain why.
R_0ecbAlJyGCZNZGt	It made for really quick logins	I just don't understand enough about it to know how safe my online identity is to really trust linking it with all of my personal accounts.	Unsure	Again, I'm sure the security level is pretty good, but it links all important accounts...seems to me like it could be easily hacked.
R_00b6aKUvJ4SmRet	Super easy, very streamlined. One click is all it takes.	The request to access certain information might seem intimidating to skeptical computer users. Further explanation of why Google needs the user's information or what it will be doing with that information might help with that.	Unsure	While it is ridiculously easy to use, it doesn't provide the same feeling of security that other authentication systems would. If someone got a hold of my Google Account credentials, they'd have access to so many other things.
R_e3UAnpHjDrOspw1	Easy to use	If people don't have a google account, can they log in through another email? Or do they have to have one?	Yes	It's very easy to use and takes less time than the app or email verification
R_eDHzNCOQ9qVWgSN	It was super easy and fast.	I don't feel secure using it-maybe just a little more authentication	Yes	Super fast and easy
R_4GHGcW8GSkFHTpz	I liked that I only had to press one button and I was in.	I can't think of anything I would change about it.	Yes	It is easier and faster. I guess it might be less secure, though.
R_a5WesSGHcXhv9wF	It is simple, streamlined, and easy.	Nothing, I just would't want to use it.	No	I don't want my passwords saved by Google or any other cloud service not matter how convenient.

www.manaraa.com

ID	What did you like most about using Google Oauth 2.0?	What would you change about Google Oauth 2.0?	Would you prefer to use Google Oauth 2.0 over traditional password-based authentication?	Please explain why.
R_37RtpyQWZ6o535H	It was easy to sign in and out because I didn't have to keep entering the same data over and over again. [however, this would make me nervous because I'm a bit paranoid about account/internet security issues]	Not really. Seemed to work well.	No	I don't want someone to be able to access my social media forums, bank account info, and other such things because I left my email open. I prefer having separate accounts with separate info and passwords that I keep in my head.
R_0rIOatexMv4gnLD	it is automatic	nothing	No	google chrome already does this
R_9GBx0vLPrWkIlW5	you don;t need to fill name and password	I would not use it for banking or other private websites	Unsure	I would like it but not for banking websites
R_0wuVuFDRca1ms97	It's very simple - one click and you're signed on.	Well, this isn't your fault. But I don't necessarily want to link my Google account to all of my other accounts. I used an alternate Gmail account for this, and I'd imagine that for various forums and websites I might not want to use my primary account (where I have my main email and blog). But that's just a fault inherent in the system.	Unsure	As I said, in some cases I would prefer it. In other cases, I don't know that I would. For example, with a bank, I prefer to have a separate username and password, perhaps one that is completely unrelated to my other usernames and passwords, for security. But for things like the smartphone forum, sure - it's very convenient.

www.manaraa.com

ID	What did you like most about using Google Oauth 2.0?	What would you change about Google Oauth 2.0?	Would you prefer to use Google Oauth 2.0 over traditional password-based authentication?	Please explain why.
R_01G89gBeQkDJzG5	It was fast and easy to connect with.	Contain more instructions within the Google OAuth. Such as: what certain codes or areas mean? What is going on behind the scenes? I would simply like to know what is going on with the system.	Unsure	Im not really sure of the obvious benefits of this system. It is a little more complex but that doesn't harm my idea of it. Sometimes people think security requires complexity. I would just like to know more about the system. What makes it better than other systems.
R_6KdTYG2JUTNXX6d	easy and fast, convenience	i prefer more security	No	not secure enough
R_bDVSULp9mIXqeb3	Did not require signing in multiple times to perform different tasks on different sites.	I would worry that if someone got my Google account information they could access all of my sites, e.g. social media, banking and school. / Or if I needed to change my Google account or forgot the password, it would be a big hassle to fix.	Unsure	Quick, easy to use. / Not sure about security.
R_1HcR75ONOJi7GCx	It's quick - just one click for everything	Once again, it scares me that a single thing (in this case my google password) could get someone else into all of my personal accounts. I can't think of a change; I just wouldn't use it.	No	I want to have separate passwords for all of my accounts - especially critical sites like banking information. It makes me feel like I have more protection.

www.manaraa.com

ID	What did you like most about using Google Oauth 2.0?	What would you change about Google Oauth 2.0?	Would you prefer to use Google Oauth 2.0 over traditional password-based authentication?	Please explain why.
R_9oY48Q67whV8IwB	It's quick because it's linked to another account, and it apparently remembers my Google account info so all I have to do is press "log in" after the first time.	I wouldn't let it be used for my bank account.	No	The simplicity is also a downside–after the first log-in, you only have to press "log in" and it doesn't ask you any verifying information. That doesn't seem like a very secure system. For something inconsequential like a social media site or a blog, I wouldn't mind it, but I want a MUCH more secure authentication system for my bank account. If my google account gets hacked, I assume all the connected accounts that use it to log in can also be jacked. I don't want to take that risk with my important accounts.
R_9oa0T0VXhLZqAQZ	It was very convenient.	I hate Google. Use something else.	No	See above.

www.manaraa.com

ID	What did you like most about using Google Oauth 2.0?	What would you change about Google Oauth 2.0?	Would you prefer to use Google Oauth 2.0 over traditional password-based authentication?	Please explain why.
R_8nPTOBrAed4NNVr	There was less clicking, less typing. Once I was set up, it was one-click, done.	No recommendations at this time other than I would wonder about how safe it would be if I lost my laptop or cell phone.	Yes	It is just so much easier to do a one-click login. It does remove the advantage of staying anonymous, perhaps. What I mean is, if I wanted to avoid logging in under my personal email and instead wanted to use my junk email for something (like BYU surveys), then I could. I'm not sure if this is an issue but it was a thought I had.
R_2ht7JxR6ykwtn3n	easily accessible	nothing	Yes	easy to use
R_0HfLkdsANADLDkp	just one click! it was great! set up was fairly easy too!	nothing! it was perfect! yay!	Yes	just one click! as long as no one was using my computer, because theres no security really
R_3gyXV0lEeDSTVWd	It was very easy to use and log in.	nothing	No	I'm not sure if I would feel safe using google to log in to all my accounts.
R_1RY2gmwyq37Nwjz	I like how it was so easy to interconnect so many things through Google OAuth. The site is very user friendly and easy to use.	I think it is fine the way it is.	Yes	Because it is a way to save time and also connect everything to the same gmail account. It's a very neat idea.
R_brq2IoDKDaKO0Pr	It required less instructions.	Explanation on how it works.	No	Pasword-based authentication is more simplistic.
R_dbYw7L1js1hwgLP	I liked that you could just link it to your account instead of continuously logging in	I also didn't like that it was linked with my google account. I would rather keep them separate	Unsure	Maybe if I continued to use it I would be more confident as to whether or not I liked it enough to continue using it.

www.manaraa.com

ID	What did you like most about using Google Oauth 2.0?	What would you change about Google Oauth 2.0?	Would you prefer to use Google Oauth 2.0 over traditional password-based authentication?	Please explain why.
R_3smFl1r0rn5VCdv	Super fast. No need to do anything really.	It is super easy but I don't feel exactly secure with it because I don't understand how it knows the password to all the different sites and that it is all automatic.	No	I don't like that I had to enter in just one password and then it would let me into anything. If anyone ever got that one password or stole my computer they would be able to access all of my sites and information.
R_bDU6qh6foqy618x	It was fast. I only had to log in once to the Google account, and that was it.	If all i have to do to log in is click "log in with google" why not just auto log me in when I visit a site? Also, I don't like the idea of all my accounts for every page being linked to the same account.	No	1. I don't like google. / 2. If my google account is hacked, then every single other account I have is hacked as well. / 3. I usually don't log into all that many pages when I'm on the computer. It's just as easy to log into each of them individually than to log into gmail so i can log into these other pages.
R_40K63SEypIKCmXP	It was a one click thing!	Nothing...	Unsure	I don't know if I want google to have access to all of my stuff...

www.manaraa.com

ID	What did you like most about using SAW?	What would you change about SAW?	Would you prefer to use SAW over traditional password-based authentication?	Please explain why.
R_9miCYXQ9i3d79kh	It seems somewhat secure.	Depends on what you want the program to do - its purpose.	No	Too much time.
R_cV02ky60s5h7do9	It was easy and fast	well, i guess you can't really change it , but I found it a little bit frustrating to go to my e-mail and click on the link to log in. I think I did that way too many times.	Yes	I tend to forget passwords (for security reasons I tend to have a different password for each of my accounts i.e. e-mail, banking, facebook etc.). This will help me a lot with that.
R_0lex09JAUq6vnEh	I like that it checks with the email before logging in anywhere, that seems very secure.	But it is also annoying to have to go to my email every time. Realistically I have so many tabs open at once, a lot of them with logins–that would be a ton of emails to get everyday! I might even set up a different email just for SAW use.	No	I think it is secure, and it really isn't that complex, but it is a bit annoying to use.
R_ehsAS4vN3w3wLtj	The graphic design was easy on my eyes, and my security seemed protected due to the email that was sent to my inbox every time I logged in.	I'm not sure.	Unsure	Hmmm. Password authentication is definitely more convenient, but maybe not as safe for the user. It was slightly cumbersome to use, but if my safety on the internet was more protected, then I would use it.
R_72Kju3xXcu84ITz	I have an email confirmation of my password so It would prevent me from having to lose my password.	Not sure, I would keep giving the options of having a code sent by email or online.	No	It was inconvenient for me to have to keep checking my emails just to get my password. It much more convenient for me to have to write a password

www.manaraa.com

ID	What did you like most about using SAW?	What would you change about SAW?	Would you prefer to use SAW over traditional password-based authentication?	Please explain why.
R_0ecbAlJyGCZNZGt	it seemed secure...	you had to jump through way too many hoops just to login to a site. overcomplicated.	No	way too much work to log in to a website.
R_00b6aKUvJ4SmRet	It's easy to remember my email address. That's pretty much the only thing I liked about it.	When I entered my email address, I always got a message that said that I'd be sent some code. However, in the email that always came in, there was never a code. It was just a link to finish authentication. That was confusing, and could be fixed with a simple change in wording that tells me to expect a link, not a code.	No	It was just a pain to enter my email address, then click the link in the email I received, then go back and enter my username and password. Is it more secure? Maybe, but there's got to be a more streamlined process.
R_e3UAnpHjDrOspw1	Email verification	I liked the email verification but not every time, it becomes annoying. Find a way to make it easy for people just on their phones because this is easy for computers but not phones as much. (switching from email to website)	No	It's annoying and there are too many steps
R_eDHzNCOQ9qVWgSN	It was easy to use after practice.	It really isn't convenient to have to go back and check one's email before everything.	No	It really isn't convenient to have to go back and check one's email before everything.

www.manaraa.com

ID	What did you like most about using SAW?	What would you change about SAW?	Would you prefer to use SAW over traditional password-based authentication?	Please explain why.
R_4GHGcW8GSkFHTpz	It made logging in pretty easy?	I don't like having to go to my email every time	Unsure	I don't really see what the benefit of SAW is, maybe that was explained at the beginning and I missed it somehow. I don't like the email verification step every single time.
R_a5WesSGHcXhv9wF	Security Confidence	Make it simpler to use.	No	You have to go back and forth between your email and the webpage.
R_37RtpyQWZ6o535H	I like that I have to have access to my email so at least to me it seems like there's a bit more security to this.	The only thing is that I would want to be able to tell my email that the notifications were not spam. On one of the tasks in particular, the link went straight to my spam box and it took me a while to find it.	Unsure	I don't mind it. However, that could be because a lot of sites I use already use this (at least to authenticate a new computer, such as Steam or Blizzard apps)
R_0rIOatexMv4gnLD	nothing	not have to go to email everytime	No	have to go to email everytime.
R_9GBx0vLPrWkIlW5	nothing	the email confirmation after every task	No	waste of time

www.manaraa.com

ID	What did you like most about using SAW?	What would you change about SAW?	Would you prefer to use SAW over traditional password-based authentication?	Please explain why.
R_0wuVuFDRca1ms97	I really was impressed that the website responded so quickly to the link that I was sent. If I had had to wait a long time in order to access the website, I would have really been annoyed, but it was quick and (as the survey puts it) well-integrated.	If this is the system that you want to implement, I don't know that I have any specific complaints. I still prefer ordinary password entry.	No	I don't like having to refresh my email all the time and keep it open. I'm a simple guy; I like to have only a couple of tabs open, and I usually don't like to pull up my email unless I'm reading email. I understand that SAW might be a little better on the security end, but if someone can get my "Bank of the Test" password, I'm sure they can get my email password too, so in the end I'm not convinced.
R_01G89gBeQkDJzG5	It is a real-time authentication system. It would be difficult to hack a system like this and it gave me peace of mind	Maybe add a text authentication as well. Some people like to use their phone as a means of authentication as well.	Unsure	I don't necessarily like getting constant emails for verification. It clogs up my email and sometimes its annoying to have to open your email and refresh it. If the system is down, it might be annoying if you cant access your account. I liked the first authentication better.
R_6KdTYG2JUTNXX6d	its more secure	idk	No	i wouldnt like going to my email every time

www.manaraa.com

ID	What did you like most about using SAW?	What would you change about SAW?	Would you prefer to use SAW over traditional password-based authentication?	Please explain why.
R_bDVSULp9mIXqeb3	Verifies you have access to the email account you provide.	Seems unnecessarily complex. Could make it a one-time verification process, not every time you log in.	No	My email put first email into Spam folder so I couldn't log in. / I don't want to get an email every time I log into online banking or another site. / Just having access to my email doesn't verify my identity any more than using a username and password.
R_1HcR75ONOJi7GCx	nothing	I know it's a quick fix, but the messages initially went to my junk inbox. I guess just a message reminding users to check that would be helpful since it is a new/unfamiliar system.	No	Still doesn't feel secure to have everything connected to a single password/email. And it's kind of annoying to have to switch between windows.
R_9oY48Q67whV8IwB	it is an added security measure–you don't just need someone's email address, you'd need access to their email to hack their accounts.	It's so tedious! I don't want to have to go to the website, then back to my email, then to the website again every time I log in.	No	Passwords are much more direct, take less time, and are just as secure as the SAW system if one is clever about making them. Besides, with the SAW system, if your email gets hacked then the hacker would have access to all your SAW linked accounts. It's more secure to have different passwords for all your accounts.
R_9oa0T0VXhLZqAQZ	I liked being able to log into multiple sites with just one account.	It was inconvenient to check my e-mail every time I wanted to log in to a website.	Unsure	While SAW seems more secure, it's definitely more cumbersome.

www.manaraa.com

ID	What did you like most about using SAW?	What would you change about SAW?	Would you prefer to use SAW over traditional password-based authentication?	Please explain why.
R_8nPTOBrAed4NNVr	It was tailored to my email, so as long as that remains secure I should hopefully be all right in terms of security.	I know it was still less than a minute, but sometimes I had to resubmit my login in several times before I would receive an email in my inbox giving me permission to log in.	Unsure	While it is a little obnoxious having to go back to my email every time I want to login, on the plus side, I wouldn't have to have that many passwords memorized for different things. It would streamline everything a little better.
R_2ht7JxR6ykwtn3n	I felt like I had more control as to giving access through my email	NA	Yes	I felt like I had more control
R_0HfLkdsANADLDkp	It was pretty straight forward, not extremely complex	the idea of having to log into my email so that i can log into something else is very repetitive. having to switch windows is annoying at times too.	No	What frustrated me most was the set up, afterwards it was pretty straight forward / also unnecessarily bothersome. too many steps to log in
R_3gyXV0lEeDSTVWd	I felt secure using it.	It can be annoying getting all of the emails and having to refresh your email.	No	I wouldn't want to have to open my email every time I need to log in somewhere.
R_1RY2gmwyq37Nwjz	Saw is easy to use and you get use to the process fast.	The authentication email was annoying to do everytime.	No	Opening my email every time to log into the different systems was too cumbersome
R_brq2IoDKDaKO0Pr	I actually didn't like it at all.	I don't like that it requires you to check your email every time.	No	I prefer not to check my email every time I need to log in to something.
R_dbYw7L1js1hwgLP	I liked how easy it was to use	I didn't like how I needed to go to my email every time to validate my login	No	I like how easy it is to enter a password rather than to scavenger through my email every time to login

www.manaraa.com

ID	What did you like most about using SAW?	What would you change about SAW?	Would you prefer to use SAW over traditional password-based authentication?	Please explain why.
R_3smFl1r0rn5VCdv	I don't have to remember anything. I just need my email address.	It is too slow. When I want to get into a website I don't want to have to wait for emails and toggle between screens.	Unsure	I have not tried any other password-based authentications so I can't make an accurate decision.
R_bDU6qh6foqy618x	The email verification process was pretty fast. It's nice that I don't have to worry as much about someone stealing a password or something. It's nice for not having to remember passwords for multiple sights. I am glad at how fast it was though, and after clicking on the link, I could simply go back to the previous tab.	The big thing is that it's a pain to have to log into my email every time. For the exercise, i left it open, but in practice, I generally don't have my email open all times when I'm using a computer.	Unsure	I like some parts of it, but i really don't like having to log into my email every single time I want to log into something else. It seems a little redundant to put my email in as a username, and then have to actually log into my email. If i have to log into something, it might as well just be the site. Also, if someone steals my email, they'd have access to everything on every page.
R_40K63SEypIKCmXP	It's fast and you don't have to remember a password	I don't know...	Unsure	I would be afraid of someone getting my email password and then having access to everything I used SAW for.

www.manaraa.com

ID	Which system would you prefer to use on a regular basis.	Please explain why.	Based on your experience with both systems, if you could create your ideal authentication system, what features would it have? It does not need to be similar to either system you tried.
R_9miCYXQ9i3d79kh	Google OAuth 2.0	I already have a Google account.	The system has to be fast. Time is important. No one likes waiting a long time to log in.
R_cV02ky60s5h7do9	Snap2Pass	As I said before, i find it not only fast and practical, but also fun. is not dull. There is way more motion interaction other than typing I find that so satisfying since not many other things offer that type of experience.	user friendly, fast, practical, safe, "fun" interaction, personalized,
R_0lex09JAUq6vnEh	Google OAuth 2.0	I trust Google to give me a very simple, user-friendly experience. I don't know how much else I trust them with, but I have a lot of accounts linked to google already–this just seems like the next stage of authenticating.	Perhaps something to recognize when it was the same user every time without always being logged in, which is so convenient but seems risky. I like that about the Snap2Pass system, because the phone represents the user, and yet, relying on another device will complicate the procedure–like what if the phone is misplaced, or breaking down? I know some computers have an optional facial recognition authentication system. I don't know how well those work right now, but those seem ideal–I've heard it's very hard to fake facial structures, so it seems safer, and it could be just as convenient and easy to use as the Google OAuth.
R_ehsAS4vN3w3wLtj	Current password-based authentication	It is the most convenient type. The only cumbersome thing about it is having to memorize a lot of names and passwords, but it makes using the computer more efficient.	A fingerprint system would be cool. Maybe if the space bar on the keyboard could register my thumb as me, then I could use the computer and access the account without having to be inconvenienced. One can dream.

www.manaraa.com

ID	Which system would you prefer to use on a regular basis.	Please explain why.	Based on your experience with both systems, if you could create your ideal authentication system, what features would it have? It does not need to be similar to either system you tried.
R_72Kju3xXcu84ITz	Google OAuth 2.0	Google OAuth would be the most private use since I don't have a smartphone vs Google since I have gmail. The password base authentication would be inconvenient because If I forgot my password, it would be harder to retrieve it and with Google O Auth he would have the password saved up and can look back on what it was.	Much like the Google OAuth, I would allow viewers the options of creating a password through the website or from google, since some would like to create their password online base on privacy issues.
R_0ecbAlJyGCZNZGt	Snap2Pass	Assuming I had a smartphone, I would use this one because it felt pretty safe, yet it wasn't overly complicated. The only downfall would be if my phone died or something like that, I wouldn't be able to login to my personal accounts.	I would use something similar to snap2pass, but instead of having a QR code, it just texted a code to your phone. That way even people without smartphones (even though there arent that many anymore) could still use the application.
R_00b6aKUvJ4SmRet	Google OAuth 2.0	Google Auth is the easiest and fastest system. Although it doesn't seem to be secure, in my experience Google Account credentials are pretty secure. But Snap2Pass comes in at a close second.	Ideally, it would offer the complete security of being accessible only to me, yet without adding additional devices or multiple steps to the process. Retina scan, anyone?
R_e3UAnpHjDrOspw1	Google OAuth 2.0	It's very easy to use.	Similar to google but having it with all emails and having it connected through our phones. Most of us have our email set up on our phones so they would take the info from that and automatically sign us in
R_eDHzNCOQ9qVWgSN	Current password-based authentication	While each of these systems were innovative and interesting, it is still (1) faster and (2) more convenient for me to simply input my password rather than having to open an email account or check a smart phone.	Voice recognition or bio-metrics. It would save time and I wouldn't have to remember 5000 passwords.

www.manaraa.com

ID	Which system would you prefer to use on a regular basis.	Please explain why.	Based on your experience with both systems, if you could create your ideal authentication system, what features would it have? It does not need to be similar to either system you tried.
R_4GHGcW8GSkFHTpz	Google OAuth 2.0	It is only a one button thing, and I guess I'm lazy.	I think it would be easy access like google OAuth but would also have security checks... like on unrecognized computers you have to first type in passwords or something. I don't know, Google seems pretty good.
R_a5WesSGHcXhv9wF	Current password-based authentication	I can remember my password. It is just as fast.	Simple, stream line, easy to use.
R_37RtpyQWZ6o535H	Current password-based authentication	I'm used to it. I don't have problems remembering passwords for websites and I'd rather have that in my head and have a different password for each website. That way if one thing gets hacked, I still have the other websites secure or whatnot. It's also just what I'm used to and I'm really not interested in getting a smart phone.	I don't know. Passwords are fine by me. I've never been hacked and I can access my stuff fine, so, I don't know.
R_0rIOatexMv4gnLD	Snap2Pass	it is kind of phone. but at the same time, I think google 0auth is used already and it is simple	dont care
R_9GBx0vLPrWkIlW5	Current password-based authentication	i find it really easy and not time wasting	fingerprint
R_0wuVuFDRca1ms97	Current password-based authentication	Meh - of the three, Google is the best, but I have a good system for keeping track of my passwords, and I prefer it because it's familiar and secure. Maybe I'm just resistant to change, but I think I'm still the happiest with my good old username and passwords when all is said and done.	Honestly, I prefer the Google one. In fact, I would consider that the closest to "ideal" that I've seen - if you have one secure password you can use it over and over. The only downside is that all of your website accounts are somewhat linked together, which isn't what I always want. But except for that, the one-button login (which works because I'm already logged on to Google) is my favorite that I've seen.

www.manaraa.com

ID	Which system would you prefer to use on a regular basis.	Please explain why.	Based on your experience with both systems, if you could create your ideal authentication system, what features would it have? It does not need to be similar to either system you tried.
R_01G89gBeQkDJzG5	Snap2Pass	It was the easiest to use and it allowed me to be more secure than my current methods.	I would like it to have the ability to save a particular computer in its memory, that way i wouldn't have to take pictures of QR codes all the time when I'm on my personal laptop/desktop computer. It would be great to use though when I'm at other locations or using other computers.
R_6KdTYG2JUTNXX6d	Current password-based authentication	i feel its the best mix of ease and protection for me	retinal scanner so i just sit in front of my computer and it scans my eye. dope.
R_bDVSULp9mIXqeb3	Current password-based authentication	The other options don't seem to offer increased security or speed at a reasonable cost. Either they are too cumbersome to use and would feel like a hassle or they make everything too easy to sign in to.	I think an ideal system for logging into my accounts, if they have sensitive information, would be a system that asks questions about me that only I would know; that, in conjunction with a password/username system is the best one I have found, and it is only used by one online bank I've had.
R_1HcR75ONOJi7GCx	Current password-based authentication	Having a different password for everything makes me feel the most protected. I can see that all these other methods are fairly simple, but it's not like entering my email and password on each different site really takes me that long, even if I have to spend a few seconds remembering.	- nothing needed outside the site I'm on (no smartphone, no extra tabs open) / - a different verification for every site/account
R_9oY48Q67whV8IwB	Current password-based authentication	I feel it's safer in terms of security– harder to hack. There is the danger of forgetting passwords, but overall I feel the system is both easy and more secure.	An ideal authentication system would be a retinal scanner. People can hack accounts, but they can't fake your eye-scan pattern. And you'd never have to worry about forgetting it (hopefully– if you lose your eye, you've got bigger problems than logging into accounts).

www.manaraa.com

ID	Which system would you prefer to use on a regular basis.	Please explain why.	Based on your experience with both systems, if you could create your ideal authentication system, what features would it have? It does not need to be similar to either system you tried.
R_9oa0T0VXhLZqAQZ	Snap2Pass	Snap2Pass was the most convenient, and I always have my phone.	I like the features of Google OAuth. My ideal system would be like that, without having to have a Google account.
R_8nPTOBrAed4NNVr	Google OAuth 2.0	Easiness to navigate continuously without interruption or frustration of forgetting my password.	Something quick, that reduces the time and stress of having to remember or use multiple passwords (or even one password, but is more secure). Something that is universally acknowledged by multiple websites.
R_2ht7JxR6ykwtn3n	Current password-based authentication	I keep the passwords to myself	fingerprint
R_0HfLkdsANADLDkp	Google OAuth 2.0	much simpler and easier to use. although possibly less secure	the simple username and password is what i like best. possibly one that had a 1 click system for the username and then a password feature for security
R_3gyXV0lEeDSTVWd	Snap2Pass	Snap2Pass was the easiest to use and it was also the most convenient. Also, I liked how the phone connected with the computer to log me in.	It would be user-friendly, and it wouldn't require having to check my email often. But it would require double verification, like using my phone or another device.
R_1RY2gmwyq37Nwjz	Google OAuth 2.0	This was the fastest and most simple. There was no unnecessary extra steps needed to log into the accounts.	I would create one similar to the google based one because of the ability to log in with a single click. The system that remembers your information for you is the most convenient. Of course, if you are a secretive person, this is not the system for you as it makes it easier for others to access your accounts.
R_brq2IoDKDaKO0Pr	Current password-based authentication	For me it's the easiest and the most common.	I would not have the email part of SAW incorporated. I might just stick to the original password-based authentication.

www.manaraa.com

ID	Which system would you prefer to use on a regular basis.	Please explain why.	Based on your experience with both systems, if you could create your ideal authentication system, what features would it have? It does not need to be similar to either system you tried.
R_dbYw7L1js1hwgLP	Snap2Pass	I liked how easy it was and how secure the account would be with the specific code reader sent for a specific account	I would have some type of recognition that is personal to only that individual. Things like Snap2Pass are actually really nice. But I wouldn't be surprised if, in the future, things like fingerprint or eye scanners were used to verify identification. Especially with accounts involving money.
R_3smFl1r0rn5VCdv	Snap2Pass	It is easy but still gives me some sense of being in control of the situation and not giving all my information and stuff over to one system.	I like the Google Oauth but I wish there was a way that it felt more secure, like it asked me a question or made me draw a pattern or something else in addition.
R_bDU6qh6foqy618x	Current password-based authentication	I don't like the idea of all my accounts being linked to one thing. The only one of these I'd even consider using on a regular basis is the snap2pass one. I just don't want to lose my phone, or have it die, and not be able to log in. And if it has a 2nd log in with a username and password, were back to the everything linked to one account. If someone wanted to steal my stuff, it'd make it a lot easier for them. And unless you could make EVERY single website I use be on board with these systems, it wouldn't be very useful.	I personally like traditional password authentication, but some ideas could be a webcam retina scanner, or fingerprint, or something. I personally want whatever is going to be the most secure (or i believe to be most secure), saving me ten seconds of typing isn't worth the trade off, in my opinion.
R_40K63SEypIKCmXP	Snap2Pass	It's easy, uses 2 sources for more protection than the others, and it's a one click thing	I really liked the snap2pass idea! I think it just needs a back up way to log in.

www.manaraa.com