A

Investigating Users' Perspectives of Web Single Sign-On: Conceptual Gaps and Acceptance Model

SAN-TSAI SUN, ERIC POSPISIL, ILDAR MUSLUKHOV, NURAY DINDAR, University of British Columbia
KIRSTIE HAWKEY, Dalhousie University
KONSTANTIN BEZNOSOV, University of British Columbia

OpenID and OAuth are open and simple web SSO protocols that have been adopted by major service providers, and millions of supporting websites. However, the average user's perception of web SSO is still poorly understood. Through several user studies, this work investigates users' perceptions and concerns when using web SSO for authentication. We found several misconceptions and concerns that hinder our participants' adoption intentions, from their inadequate mental models of web SSO, to their concerns of personal data exposure, and a reduction in their perceived web SSO value due to the employment of password management practices. Informed by our findings, we offer a web SSO technology acceptance model, and suggest design improvements.

Categories and Subject Descriptors: D.4.6 [**Security and Protection**]: Authentication

General Terms: Security, Human Factors

Additional Key Words and Phrases: Web Single Sign-On; OpenID; OAuth; Usable Security;

ACM Reference Format:
Sun, S., Pospisil, E., Muslukhov, I., Dindar, N., Hawkey, K., Beznosov, K. 2012.Investigating Users' Perspectives of Web Single Sign-On: Conceptual Gaps, Alternative Design and Acceptance Model. ACM Trans. Internet Technol. V, N, Article A (January YYYY), 35 pages.
DOI = 10.1145/0000000.0000000 http://doi.acm.org/10.1145/0000000.0000000

1. INTRODUCTION

In 2007, a large scale study of password habits found that a typical web user had about 25 password-protected accounts, and entered approximately eight passwords per day [Florencio and Herley 2007]. Web single sign-on (SSO) systems enable web users to leverage one single account on a service provider to sign onto multiple websites, reducing the number of passwords and registration information a user must manage. Fundamentally, the architecture of a web SSO solution separates the role of identity provider (IdP) from that of the relying party (RP). An IdP (e.g., Google, Facebook, Twitter) maintains the identity information of the users and authenticates them, while an RP (e.g., CNN, Sears, Groupon) relies on the authenticated identities to make authorization decisions and to customize user experience.

This research has been partially supported by the Canadian NSERC Internetworked Systems Security Network (ISSNet) Program.
Author's addresses: S. Sun, E. Pospisil, I. Muslukhov, N. Dindar, K. Beznosov, University of British Columbia, 2332 Main Mall, Vancouver BC, Canada V6T 1Z4; K. Hawkey, Dalhousie University, 6050 University Avenue, Halifax NS, Canada B3H 4R2.
Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies show this notice on the first page or initial screen of a display along with the full citation. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers, to redistribute to lists, or to use any component of this work in other works requires prior specific permission and/or a fee. Permissions may be requested from Publications Dept., ACM, Inc., 2 Penn Plaza, Suite 701, New York, NY 10121-0701 USA, fax +1 (212) 869-0481, or permissions@acm.org.
© YYYY ACM 1533-5399/YYYY/01-ARTA $10.00
DOI 10.1145/0000000.0000000 http://doi.acm.org/10.1145/0000000.0000000

OpenID [Recordon and Fitzpatrick 2007] and OAuth [Hammer-Lahav et al. 2011] are open and lightweight web SSO protocols that have been adopted by high-profile IdPs such as Facebook, Google, Microsoft, and Yahoo, and millions of RP websites. Together, these two protocols offer billions of potential web SSO users, but the user perspective with respect to web SSO is still poorly understood. Specifically, there is little understanding of the perceived risks and concerns users face when using web SSO, their mental models of web SSO, and how these models influence their perceptions of security and privacy, as well as their intentions to adopt web SSO. Our research aims to fill this gap through answering the following research questions:

— What are the mental models users have?
— How are these mental models formed?
— What are the gaps between users' mental models and the system model?
— How do these gaps affect users' security/privacy perceptions and adoption intentions?
— How can we reduce these conceptual gaps?

To answer these research questions, we first conducted an exploratory study to better understand users' experiences with web SSO. After identifying misconceptions and concerns common to most participants, we designed an identity-enabled web browser (IDeB) intended to explore possible improvements. The initial prototype was refined through several iterations of cognitive walkthroughs and pilot studies. We then conducted a formative within-subjects evaluation of the IDeB prototype to confirm the findings from the exploratory study and to further improve the prototype and study design. Through mental model drawings and semi-structured interviews, we identified several conceptual gaps that influenced our participants' perceptions and acceptance intentions. Finally, we conducted a within-subjects study to compare our IDeB design with the existing interfaces (denoted as "CUI" hereafter), to see whether the issues identified through the exploratory and formative studies had been addressed in IDeB. These studies were approved by the UBC's Behavioral Research Ethics Board (BREB), and the study documents are listed in a prior publication from this research study [Sun et al. 2011].

Our study revealed that current web SSO user interfaces could be misleading and lack of visibility of system states, resulting in users deriving inadequate mental models that negatively influence their risk perceptions and adoption intentions. Most participants in our study incorrectly believed that the way SSO works is to give their IdP login credentials to RPs. This misconception was initially "confirmed" for participants when they saw that *the IdP login page was skipped* when they were asked to log out and sign back into the first RP in the study. Later, this incorrect belief was "confused" during the subsequent task scenarios, when they could log into *another RP* and view their IdP profile (e.g., Gmail, Yahoo Mail, Facebook) without an explicit IdP login. In addition, most participants were uncertain about what types of data were being shared, what actions the RP could do to their IdP account, and how they could revoke their profile sharing. Many participants did not know that RPs could post messages back to the IdP on their behalf, while some participants expressed reluctance to use web SSO solutions due to a prior surprising and embarrassing experience of RPs posting their activities to their Facebook update streams. Furthermore, most of our participants did not know that IdPs can track when and which RP websites the user has visited, as well as the services and products in which the user is interested if the IdP is an OAuth-based IdP.

Besides security misconceptions and privacy concerns, our study also identified the following factors hindering the participants' intention to adopt SSO; however these are difficult to resolve by the improvement of the SSO protocol alone:

— No perceived urgent need for the web SSO that the websites offered: Most participants were "comfortable" with weak or reused passwords, while many used the password manager feature in the browser.
— Single point-of-failure concerns: Over a quarter of the participants identified this inherent property of web SSO, and expressed concerns about it.
— Phishing concerns: Once informed of the possibility of IdP phishing attacks, all participants expressed serious concerns about this common issue of redirection-based web SSO protocols.
— Trust concerns with RPs: Many participants stated that they would not use SSO on RP websites that contain valuable personal information, involve potential monetary loss, or are not trustworthy or familiar.
— Account linking misconceptions: Linking a traditional account to an IdP account allows an existing account on the RP website to sign in using SSO, and ensures that users are still able to log in when their IdP accounts are inaccessible. However, most participants did not understand the purpose and concept of account linking and became confused and frustrated when they were prompted for such a linking.

Our main contribution lies in a user-centric investigation of web SSO systems, offering informed design recommendations to web SSO development communities. Our study focused on OpenID and OAuth-based web SSO systems because together they offer a critical mass of the web SSO population [Janrain Inc. 2012]. We did not include high-value RPs in the study (e.g., banking, government) as they typically require a high degree of identity assurance provided by the SSO protocol and trust frameworks such as SAML-based identity federation solutions (e.g., Yodlee [Yodlee Inc. 2012], Shibboleth [Internet2 2008], Liberty Alliance [Kantara Initiative 2002]). In addition, we chose RPs that reuse software libraries from leading SSO integration providers (i.e., Gigya [Gigya, Inc 2011], Janrain [JanRain Inc. 2012]) as opposed to designing the SSO UI themselves, because those SSO UIs are professionally designed and have been widely used by many popular websites, including many of those listed on Google Top 1000 websites [Google Inc. 2012]. Our findings and insights were uncovered and derived mainly from the *qualitative* data collected through the observations of the task scenarios, mental model drawings, and semi-structured interviews during our iterative user centric process. We found that most of our participants exhibited similar misconceptions and concerns, and data saturation was achieved quickly. We strived to recruit a representative sample of participants to reduce potential sample bias. In addition to balancing age, education, and student/non-student attributes, participants had a variety of occupations, such as dance teacher, financial planner, dentist, accounts, and fulltime housewife. Nevertheless, we acknowledge that a population bias most likely exists as our participants were highly educated. It is likely that the proportion of actual web users who have inadequate mental models of web SSO would be higher than the proportion of our participants who do so.

Security mechanisms are only effective when adopted and used correctly by users [Whitten and Tygar 1999]. The user-centric design of security mechanisms is thus imperative to the development of security solutions that are intended to be used by average users [Adams and Sasse 1999; M. Angela Sasse 2003; Lampson 2009]. Our finding that dangerous mistakes and adoption concerns occurred due to inadequate mental models of web SSO is indeed yet another observed instance of "Why Johnny Cannot Encrypt" [Whitten and Tygar 1999]. In summary, our paper makes the following contributions:

— We identify the mental models users have of web SSO and how these mental models are formed.

— We identify conceptual gaps between the user's mental model and the system model, and analyze how these gaps affect user experience and perceptions in regards to SSO.
— We introduce a web SSO technology acceptance model that explains how each factor we found influences users' acceptance of a web SSO solution.
— We suggest design improvements for RP and IdP websites, and web SSO development communities. We do not claim that our IDeB design is ready for real-world adoption; it served solely as a discovery tool for the recommended design improvements. The recommended design improvements for RPs and IdPs can be implemented without additional supports from the browser.

The rest of this paper is organized as follows: the next section introduces web SSO and related work, and Section 3 provides an overview of our methodology. Section 4 describes the design and findings of the exploratory study, and Section 5 presents the design of the identity enabled browser. The formative and comparative studies and their results are presented in Sections 6 and 7. Sections 8, 9, and 10 discuss the identified conceptual gaps, web SSO technology acceptance model, and our recommendations, respectively. We discuss the limitations of our research in Section 11, and conclude in Section 12.

2. BACKGROUND AND RELATED WORK

The proliferation of web applications has caused web users to accumulate a multitude of user accounts and passwords [Florencio and Herley 2007]. The burden of managing this increasing number of accounts and passwords leads to "password fatigue" [Wikipedia 2009]. Aside from the burden to human memory, password fatigue may cause users to devise password management strategies (e.g., to write down, reuse, or choose weak passwords) that degrade the security of their protected information [Gaw and Felten 2006; Florencio and Herley 2007].

One approach to reduce the burden on human memory and the overhead of credential management is password managers [Mulligan and Elbirt 2005]. Password managers typically store encrypted password data in a local database and are able to automatically fill in the login forms of the websites that users visit. Gaw and Felten [2006] found that the most commonly used password managers are those built in to the browser itself (e.g., password auto complete), rather than those implemented as a browser extension (e.g., Password Multiplier [Halderman et al. 2005]). Password managers can reduce a user's memory burden as they only need to remember a single master password. However, users may have difficulty in migrating their existing passwords to the system [Chiasson et al. 2006]. Such systems typically have issues with the transportability of passwords between computers [Chiasson et al. 2006], and users may not trust the security of these systems [Gaw and Felten 2006]. In addition, when using password managers that improve security through custom generated passwords (e.g., Passpet [Yee and Sitaker 2006], PwdHash [Ross et al. 2005]), users may be uncomfortable not knowing the actual site passwords [Chiasson et al. 2006].

Another approach to reduce the problem of password fatigue is web single sign-on (SSO), which allows web users to use one single account to sign onto multiple unrelated websites. This is commonly accomplished by having an identity provider (IdP) that manages and authenticates the user's identity information (e.g., Facebook, Google, Yahoo), and then provides the asserted identity to other relying party (RP) websites upon login *through the user's browser*. Web SSO solutions were initially developed by various educational institutions in the mid-1990s. Early innovators in the field include Stanford University's WebAuth, Cornell University's SideCar, Yale's Central Authentication System (CAS), and PubCookie from University of Washington [Hodges et al. 2008]. Microsoft Passport [Oppliger 2004], the predecessor of Windows Live ID, was

the first commercial effort to improve web authentication through SSO. However, Microsoft Passport failed to gain widespread adoption, beyond Microsoft's own services, for reasons of trust. In addition to its security flaws, the system is proprietary and centralized, and thus perceived by many potential web users and RP websites as a vehicle that could allow Microsoft to monopolize the online identity landscape [Hodges et al. 2008].

2.1. Key Web SSO Protocols

Since 2000, four major open web SSO specifications have emerged: SAML Web Browser SSO Profile, InfoCard, OpenID, and OAuth. Any RP or IdP implementation adhering to the open specification or standard can achieve the full spectrum of use-cases and interoperability provided by these protocols.

Security Assertion Markup Language (SAML) [OASIS 2005], a framework of standards specified by the OASIS [2012] Security Services Technical Committee, offers an XML-based markup language that encodes security assertions and corresponding protocol messages for exchanging identity assertion information across domain boundaries. With versions standardized in 2002 (v1.0), 2003 (v1.1) and 2005 (v2.0), the SAML 2.0 standards are widely considered the most robust, extensible, and interoperable choice for enterprise-strength identity federations. Many successful SAML implementations exist in industry, government, and academia [Wisniewski et al. 2005], and other standards such as the Internet2 Shibboleth project [Internet2 2008], Liberty Alliance [Kantara Initiative 2002], OASIS Web Services Security (WS-Security) [Atkinson et al. 2002], and eXtensible Access Control Markup Language [Committee 2005] (XACML) are based on SAML. The modular design of the SAML framework allows its components to be combined to support a wide variety of deployment scenarios. One key use-case specification is the "SAML Web Browser SSO Profile", which defines how a web browser and the underlying HTTP protocol can be leveraged to transport assertion request and response messages between an IdP and an RP. Although the SAML framework is highly flexible and extensible and supports various degrees of identity assurance, the prerequisite of agreements on protocol details among organizations in a federation, and the complexity of XML parsing, signing and validation, make it difficult to scale to the Internet at large.

Information Card [Nanda and Jones 2008], known as InfoCard, defines the Identity Selector Interoperability Profile specification [Nanda and Jones 2008] (v1.0 in 2007, v1.5 in 2008) underlying Windows CardSpace [Microsoft Corp. 2009], which is deployed in Windows operating systems. InfoCards are personal digital identities that are analogous to real-world identity cards, such as passports and driver's licenses. Each card contains assertions about a user's identity that are either self-issued or issued by an identity provider. When logging into a website, the user selects a card instead of typing a username and password directly into the website. Information cards are managed on the client's computer by a software component called an *identity selector* (e.g., Windows CardSpace [Microsoft Corp. 2009], Higgins Card Selector [The Eclipse Foundation 2009]). InfoCard has important features such as phishing-resistant authentication and IdP-to-RP unlinkability. However, due to week adoption by IdPs and RPs, Microsoft discontinued the development of Windows CardSpace in 2011 [Microsoft Corp. 2011].

OpenID [Recordon and Fitzpatrick 2007], a lightweight web SSO protocol developed in 2005 (v1.0) and finalized in 2007 (v2.0), provides a unique "dynamic IdP discovery" capability with major service providers (e.g, Google, Yahoo, Microsoft, AOL) and the US governments supporting it. Dynamic IdP discovery allows RPs to discover the service endpoints of IdPs and establish shared session keys at runtime. This interoperability capability benefits both RPs and users. RPs can employ a single OpenID

implementation to interact with any OpenID IdPs, and users are free to choose or even set up their own OpenID providers. OpenID uses a URI (Universal Resource Identifier) as a user identifier (e.g., http://ubc.ca/santsai); and with its core specification, only this user identifier is shared with RPs. To simplify account registration, most current OpenID IdPs employ OpenID Simple Registration or Attribute Exchange extensions for sharing a limited set of user attributes with RPs. According to the OpenID Foundation [2009], as of September 2009, more than one billion OpenID enabled user accounts were served by major service providers. At the time of writing, OpenID Foundation was drafting the next evolution of the OpenID protocol named "OpenID Connect" [Sakimura et al. 2011], which combines the best design features from the OpenID and OAuth 2.0 protocols.

OAuth [Hammer-Lahav et al. 2011] is a web resource authorization protocol that enables web users to grant third-party applications limited access (e.g., scope, duration) to their resources stored at a website, without revealing their login credential to the applications. Building upon the actual implementation experience from proprietary industry API authorization protocols (e.g., Google AuthSub, Yahoo BBAuth, and Flickr API), OAuth 1.0 was published in 2007 and quickly become the industry standard for web-based access delegation. A minor revision (OAuth 1.0 Revision A) was published in 2009 to patch a security hole [Hammer-Lahav 2009]. In April 2010, OAuth 1.0 was published as RFC 5849. Even though OAuth is designed as an authorization protocol, many implementations of OAuth are being deployed for web SSO. When using OAuth for SSO, user identity information hosted on an IdP is authorized by the user and shared as a web resource for RPs to identify the current SSO user. While the OAuth 2.0 specification [Hammer-Lahav et al. 2011] is still a work in progress within the IETF OAuth working group, implementations have already been developed and deployed by major service providers (e.g., Facebook, SalesForce, Twitter, LinkedIn, Google). OAuth enables not only web SSO, but also personalized, web-scale content sharing through social graphs and platform-specific services such as messaging, recommendations, ratings, and activity feeds. The enormous number of users from major service providers attracts millions of RP websites, which aim to reach a broader set of users, and integrate their services deep into the users' social contexts [Facebook, Inc. 2011].

Mozilla's Persona [Mozilla Identity Lab 2012] is a browser-supported web SSO scheme first released in July 2011, and fully deployed by Mozilla on its own websites in January 2012. With Persona, web users can maintain a list of their email addresses in the browser and choose one of them to sign onto the RP websites. Each email address is certified by the corresponding email provider through a digital certificate. Using email as the user identifier enhances usability and minimizes personal information disclosure. In addition, Persona stores the user's email certificate and conveys it to RP websites upon user login, which prevents IdPs from tracking the websites a user has visited. One main challenge Mozilla Persona faces is adoption of RPs. In particular, RPs need a rich set of user data from IdPs in order to motivate their adoption of Persona [Sun et al. 2010a].

2.2. How A Web SSO Works From The User's Perspective

Despite differences in protocol details, the interaction flows from the user's perspective are similar—the authentication request and response are passed between the RP and the IdP through the browser. Figure 1a illustrates the following steps, which demonstrate a high-level view of a *sign up* flow when a visitor attempts to log in to an RP website using one of her IdP accounts:

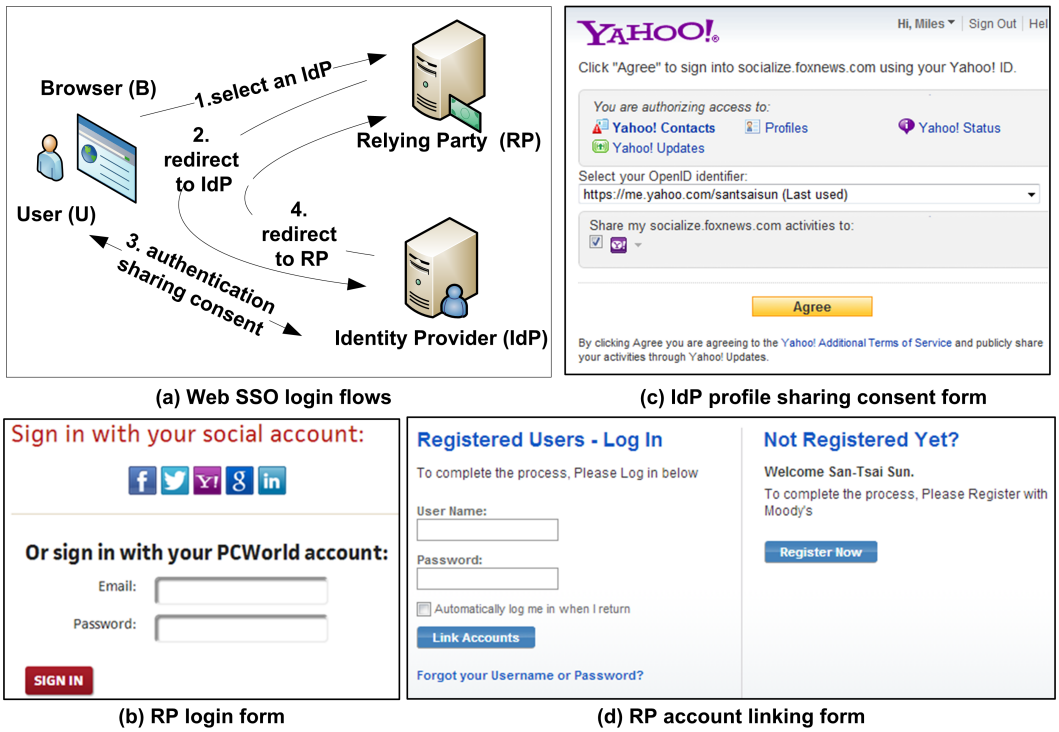


Fig. 1. Sample forms in web SSO sign-up and sign-in processes.

(1) A user selects an IdP via a login form presented by an RP. A web SSO-integrated login form typically combines traditional login fields (i.e., username, password) with a list of IdP icons for the user to choose from (see Figure 1b for an example).
(2) The RP redirects the user to the IdP for authentication.
(3) The user authenticates to the IdP by entering her username and password. Note that this step may be skipped if the user has previously been authenticated by the IdP in the browser session. After authentication, the IdP presents a profile sharing consent form for the user to authorize the release of her profile information (Figure 1c). This consent step could be omitted if permissions have already been granted by the user.
(4) The IdP redirects the user back to the RP with the requested profile attributes. Before granting access, the RP may prompt the user to complete a registration form to gather additional profile information or link to an existing account (Figure 1d).

For a returning user, only steps 1 to 3 are needed to *sign onto* the RP website (i.e., selecting an IdP and entering an IdP username and password if the user has not yet authenticated to the IdP in the browser session).

2.3. Related Work

There have been several usability studies and solutions to improve the usability of web SSO systems. To understand the conceptual and usability issues associated with enabling Yahoo OpenID on RP websites, Freeman [2008] conducted a usability study with nine female Yahoo users (aged 32–39 with a self-declared medium-to-high level of Internet savvy). The study found a number of usability problems that web users faced when using OpenID for authentication. Based on the results, the authors recom-

mended best practices and design guidelines for implementing usable login interfaces on both RP and IdP websites. For RP login forms, they suggest that RPs should clearly indicate that users have the choice of logging in using different login options. They also promote the ability to log in using an existing account (e.g., "Sign in with a Yahoo ID" button, IdP logo list), but not the technology itself. The design of most state-of-art RP login forms follows Yahoo's recommendations, including the RP websites in our study.

Sachs [2008] from Google OpenID Research found that using the IdP icon list as a guide for login imposes some limitations. Consistent with our findings, the author found that unless the buttons are large, they are only noticeable by a subset of the end-users. However, if the buttons are enlarged, then users can be confused about how they should login. In addition, if the list includes IdPs who are not email providers, then there is no good way to identify the same person logging on through SSO and traditional login, which requires an account linking step. As a result, Google suggests using "email as a key" to hide IdP icons from users completely. However, this approach is not widely adopted by RPs, because not all IdPs are email providers.

Plaxo.com, an online address book provider, conducted a "Two-Click Sign up" experiment with Google to enable Google users (1,000 participants) to sign up and import their Google contact list into Plaxo [McCrea 2009]. The result was encouraging; 92% of participants completed the import task. However, the login form was optimized to contain only one "Sign up with my Google Account" button without any other login options, which is not applicable to most RP websites.

VeriSign's Seatbelt [VeriSign Inc. 2009], a Firefox add-on, is designed to make OpenID more convenient to use by automatically filling in a user's OpenID URL when visiting relying parties. Seatbelt is easy to use; however, it may not detect OpenID login form fields, because it uses a simple text matching technique (e.g., openid, oidurl, open-id, open_id) to identify them. In addition, it requires Seatbelt-specific configurations from the participating OpenID IdPs.

Sxipper [Sxipper Inc. 2009] is a form manager implemented as a Firefox add-on that helps users to fill in web forms during registration or ordering processes. Similar to Mozilla Persona, Sxipper allows a user to maintain separate copies of their personas in the browser, and prompts the user to pick a persona and fills the corresponding form automatically. The main limitation of Sxipper is that it might not detect form fields correctly as websites can use different names for their registration or order form fields.

3. MOTIVATION AND APPROACH

There are several recommendations and design guidelines for implementing a usable login user interface on RP websites [Freeman 2008; Sachs 2008; Dhamija and Dusseault 2008]. However, users' perspectives of web SSO have not been thoroughly investigated. First, RP websites do not offer a consistent user experience as RPs have diverse needs for authentication and user management. When accessing N RPs using one IdP, the user must visit $N + 1$ possible different login forms (one for each RP website, and one at the IdP), choose an IdP to login N times via N possible ways, consent to the release of personal profile information on the IdP N times, and log out $N + 1$ times through $N + 1$ different interfaces. These complex and inconsistent user experiences may impose a cognitive burden on web users. In addition, there is a lack of visibility and feedback for users who use different IdP accounts for RP websites that vary in trustworthiness, which can make it difficult for them to determine why an access failed, and whom to contact if a problem is encountered. Moreover, many RPs combine sign-up or account linking steps at the end of an SSO process, which may confuse and frustrate users even further. Furthermore, sharing personally identifiable information with RPs can cause significant privacy concerns [DeVault et al. 2002; Maler

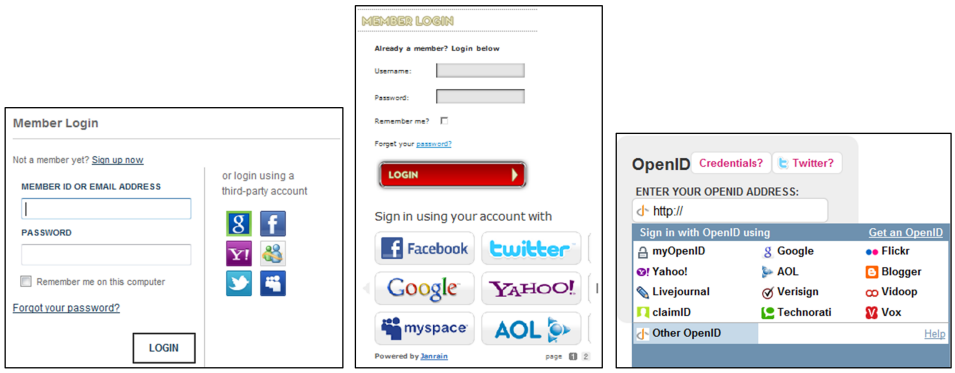
and Reed 2008; Spiekermann and Cranor 2009]. Users may be concerned about spam or misuse of their profile information when signing onto RP websites using their IdP account. Finally, HTTP redirection-based web SSO systems are vulnerable to phishing attacks [Laurie 2007; Dhamija and Dusseault 2008; Messina 2009]. As documented in the security considerations of the OpenID 2.0 (Section 15.3) and the OAuth 2.0 (Section 10.11) protocol specifications, a malicious RP could redirect users to a bogus IdP login form to steal the victim's login credential, and must rely on a user's cognitive capability to detect an IdP phishing attack.

To gain an overall understanding of users' perceptions and concerns when using web SSO for login, we first conducted an in-lab exploratory study with nine participants. Participants were asked to sign up and log into three real-world RP websites using their existing account from Google, Yahoo, Microsoft or Facebook. To obtain objective data, we observed participants directly during task scenarios, recorded qualitative data on the nature of the interaction, and kept notes of particular items of interest to be investigated further in the post-session, semi-structured interview. We found several similar behaviors, misconceptions and concerns exhibited by most participants, and the results saturated quickly. Based on our findings, we compiled a list of requirements and brainstormed potential solutions to address the issues and concerns.

Our next step was to design and implement an alternative interface intended to provide web users with a consistent, intuitive, phishing-resistant and privacy-preserving single sign-on user experience. The design process was both incremental and evolutionary, as the prototype was refined and redesigned throughout, and user feedback was iteratively integrated into the design. We implemented a horizontal prototype, and used a "Wizard of Oz" approach for vertical communication functions to make users perceive that the websites in the study had adopted our new design (This is further discussed in Section 5.) This functional partition allowed us to compare our design with the existing interfaces using identical RP and IdP websites in order to achieve internal and ecological validity.

Once a working version of the prototype was complete, we conducted a formative, within-subjects study with seven participants to compare the initial IDeB prototype with the existing interfaces. The study design was chosen over a between-subjects design due to expectations that individual differences would be substantial. Additionally, the comparative comments of research subjects who experienced both conditions were essential for our evaluation. There was particular emphasis on examining the mental models formed for each system, and how they differed. A semi-structured interview was used to obtain additional feedback from the users. Moreover, it was desirable that the new system would compare favorably to traditional login methods, so we chose to also investigate users' preferences between the traditional login, the current user interface (CUI), and our design. We found participants' misconceptions and concerns in the formative study were consistent with the findings from the exploratory study, and that our design significantly improved their perceived ease of use, security protection and privacy control. We also identified parts of the prototype and study design that required further improvements.

In the final phase, we modified the prototype and study design to address the noted deficiencies. In particular, we revised the IDeB to (1) reuse the existing IdP login forms instead of using a customized one to make the IDeB look more trustworthy, and (2) we shrunk the browser before presenting the IdP login form to reduce the possibility of IdP phishing attacks, and to convey a more accurate mental model (This is further discussed in Section 5.) We then conducted a comparative within-subjects study with 35 participants to compare the usability of IDeB with CUI, to determine if there were any outstanding issues hindering the adoption of the new prototype. Our purpose was not to distribute IDeB to internet user at large. We used lab study to control variables in



Fox News **ITrackMine** Skitch

Fig. 2. Login forms of three chosen RP websites in the study.

Table I. RP SSO Properties

Property	Fox News	ITrackMine	Skitch
Popup window	Yes	Yes	No
Size of IdP icons	Medium	Large	Small
# of IdPs supported	6	12	12
Additional sign-up	No	Yes	Yes
Account linking	No	Yes	No
Well-known	Yes	No	No

Properties of the selected RPs in the study.

our conditions. Overall, 51 participants were used in the above studies, and each participant was included only in one study. Using criteria for theoretical sampling [Glaser and Strauss 1967], we stopped recruiting new participants when we observed no new findings arising in the study, and all comparison results were statistically significant.

4. EXPLORATORY STUDY

In the initial stage, our goal was to investigate web users' perceptions, challenges, concerns, and perceived benefits when using their existing IdP account to sign in to real-world RP websites. To find a representative sample of RP websites, we went through an RP site directory at MyOpenID.com, and categorized RPs into several groups based on their login form styles. RPs that use a simple OpenID textbox were excluded as this approach has already been found to be unusable for most web users [Freeman 2008; Sachs 2008]. In addition, RPs designed for a specific community of users, and those that had the potential to make participants feel uncomfortable or embarrassed (e.g., dating or gaming websites) were excluded as well. From the three most popular style groups, we chose one RP website from each group based on the properties listed in Table I. In the order presented in the study, we chose (1) Fox News, a premier news website from www.foxnews.com, (2) ITrackMine, an online collection manager (www.itrackmine.com), and (3) Skitch, an online photo sharing website (www.skitch.com). The login forms of these three RP websites are shown in Figure 2. Note that rather than designing the SSO login flow from scratch, all three RPs reuse software libraries from leading professional SSO integration providers for their SSO login UIs and implementations (Gigya [Gigya, Inc 2011], Janrain [JanRain Inc. 2012], and IDSelector [JanRain Inc. 2010], respectively).

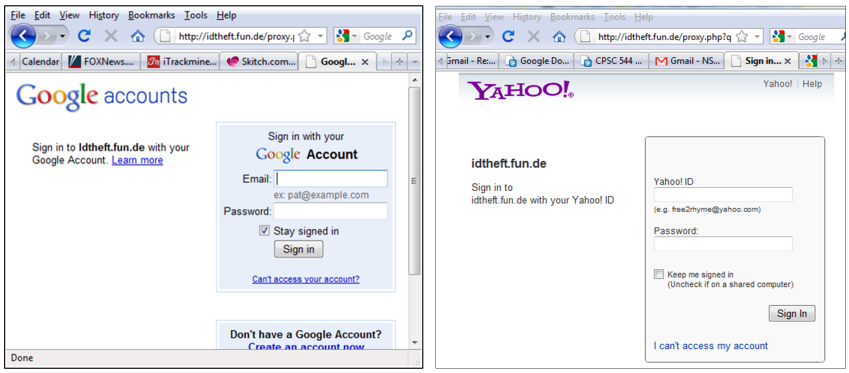


Fig. 3. Screen shots of the IdP phishing demo website.

4.1. Study Protocol

We recruited nine participants (six males and three females) from the University of British Columbia (UBC) and the Greater Vancouver area, and conducted a one-hour lab study with each participant. Four participants were 19-24 years old, and five were 25-34 years old. Most participants were fluent in English (eight), and had college or graduate degrees (eight) with a diverse range of majors. All had more than four web accounts, and two participants used a password manager. Five participants had prior SSO experience using the UBC campus-wide login.

After completing a background questionnaire, participants were asked to sign up for, and sign in to, three RP websites using one of their existing accounts from another service provider (i.e., Google, Yahoo, Facebook or Microsoft). Then the participants were asked to log out of all websites, as if the tasks had been performed on a public computer from which they were about to walk away. We then asked participants to check their email using the IdP account in the study (e.g., Gmail for Google IdP). Finally, participants were directed to an OpenID phishing demo website (http://idtheft.fun.de) and told to select Google or Yahoo as the IdP for login. Before they entered their username and password, we stopped participants and asked them whether they could identify any clues to indicate that this was not the real Google or Yahoo sign in page (see Figure 3).

Afterwards, the participants completed a questionnaire detailing their experiences with various aspects of these tasks. We then conducted a contextual interview with the participants in order to understand the problems that they encountered, as well as their potential concerns, perceived benefits, and desired features in a web SSO system.

4.2. Findings

We found that the current web SSO login UI was inconsistent and counter-intuitive, and that participants formed incorrect mental models of the SSO workflow. Of the three websites, we expected that the majority of our participants would be able to sign onto Fox News without any errors or concerns, as this website is well-known, listed on the Google Top 1,000 websites [Google Inc. 2012], uses a popup window, and does not require additional sign up or account linking process. It only requires three clicks and the username and password to be entered into the IdP login form to sign into the site. Surprisingly, most of the misconceptions and concerns that we found were uncovered when participants were trying to log in to this site. The main problems and concerns identified in our study are listed below. Note that the findings were confirmed again in the formative and comparative studies (Section 6 and 7):

— **F1: Misleading affordance**: On the Fox News login form (Figure 1a), most participants (eight) entered their IdP username and password into the traditional login fields directly. They stated that they believed the website must be integrated with the identity providers (IdPs) in some way so that they would be able to use their Google or Yahoo email and password directly on the login form to sign in. They did not know that they needed to click on one of the IdP icons to initiate the login process; three participants thought the IdP icons were advertisements, and two thought the website had teamed up with the IdPs for content sharing.
— **F2: Incorrect mental model derived from the login process**: Many participants (five) thought that after the login and consent processes, the website knew their Google or Yahoo username and password. We found that this misconception was formed because (a) the user-to-IdP authentication/authorization popup window was initiated from and surrounded by the Fox News website, and (b) when participants were logging back to Fox News, the popup window simply blinked open and then closed, because the participants had authenticated to their IdP account in the same browser session.
— **F3: Privacy concerns**: Most participants (eight) were concerned about spam or misuse of their information when consenting to profile sharing from their IdP account.
— **F4: Implicit IdP login concern**: Logging into an RP website with an IdP account actually signs the user into *both the IdP and the RP*. All participants (nine) were surprised that they could view their email without an explicit login. They were very concerned that they had to explicitly log out from the IdP in addition to the RP websites. Participants sometimes used a public computer or shared a computer with their family members, and wanted to prevent others who share the computer from accessing services provided by the IdP.
— **F5: Account linking is confusing**: The ITrackMine website in the study requires users to sign up for a new account or link to an existing account after users have authenticated to their IdP account, but none of our participants understood the purpose of account linking. Most participants (seven) believed that as soon as they were redirected back from the IdP, they had already logged in to the RP (not true in the case of ITrackMine website).
— **F6: Phishing concerns**: Most participants (seven) did correctly identify the fake Google or Yahoo website as a fake based on the URL that appeared at the address bar. However, they expressed concern that in future logins, they might not pay attention to the URL bar and other security indicators. In the following formative and comparative studies, we provided participants with a printout of a fake Google login form that obfuscates the URL (which most phishing websites could do), and found that most participants could not tell whether or not is was a real Google login form.

In last task of the study, we provided our participants with full step-by-step instructions for removing the RP websites' access to their IdP accounts. On the page that manages RP access, there is a list of granted RPs, each with a list of shared profile attributes and access histories. Most participants stated that they did not know how to remove RPs' access to their IdPs without help. In addition, although it is clear that the IdP is able to track which websites they have visited and when, none of our participants expressed privacy concerns about this IdP tracking capability.

4.3. Improvement Requirements

Based on the above findings and existing literature review, we compiled a list of requirements to inform the future design. To be usable, (R1) the RP login form must provide a clear login affordance that indicates to users that they can sign in using their existing IdP account (derived from F1). (R2) The solution must leverage the login

experience that an average web user already has, and transform a negative transfer effect (i.e., habituated to enter username and password directly) into a positive one (F1). (R3) It must avoid relying on users' cognitive capabilities to detect phishing sites [Wu et al. 2006; Dhamija et al. 2006; Zhang et al. 2007; Schechter et al. 2007; Sunshine et al. 2009]. (R4) It must provide web users with a fine-grained privacy control as opposed to the "all or nothing" sharing option offered by current IdPs (F1). (R5) The login state of the IdP must visible to the user (f2, F4). (R6) The solution should assist users in choosing from different identities for websites that vary in their level of trustworthiness [Dhamija and Dusseault 2008]. (R7) The solution should provide a single logout mechanism that automatically ends all authentication sessions when the user logs out of their IdP account (F4).

In addition, asking users to provide large amounts of sign up information during first ever sign on annoys them. If RP websites could provide gradual engagement features that acquire additional user attributes only when there is a reason for the user to provide them, it would increase the website's conversion rate (i.e., converting anonymous visitors into users) [Dhamija and Dusseault 2008; Maler and Reed 2008; Wroblewski 2008].

5. THE IDENTITY ENABLED BROWSER

We developed an alternative web SSO interface design by building identity support directly into the browser, thereby unifying and simplifying the interface across websites. In this section, we present the design details of this identity-enabled browser (IDeB). Note that our IDeB design is a "mock-up" system, and we mainly used IDeB to explore possible improvements.

5.1. IDeB Behind The Scene

In order to build SSO support directly into the browser, we could have adopted our proposed OpenID protocol extensions [Sun et al. 2010b] to perform authentication with IdPs directly in the browser, and convey the authenticated identity to RPs. However, as the websites in our study had not yet adopted the protocol extensions, doing so would have forced us to use different IdPs and RPs for subsequent studies. Because our main evaluation goal was a direct comparison with current web SSO solutions, performing study tasks on different websites could have substantially impacted the participants' impressions and preferences. Thus, we decided to employ a "Wizard of Oz" approach to *make it appear to participants that the websites that were used in the studies had adopted our new approach*.

Our IDeB design consists of two parts: a Firefox extension that integrates the websites in the study, and a Windows program developed in .NET framework 3.5 that implements our alternative designs of the SSO user interface. The Windows program runs as a background process on the study computer, and prompts the participant with the corresponding UI forms based on the requests from the Firefox extension.

To integrate with the RPs in the study (i.e., Fox News, ITrackMine), the Firefox extension modifies the event handlers of the login and logout links on the RP websites via dynamic HTML Document Object Model (DOM) modifications. When the participant clicks on the login link, the Firefox extension calls the Windows program to shrink the browser, block out the desktop, and then prompt the IdP login form (Figure 4a) or the IdP account selector (Figure 4d). When the logout link on the RP website is clicked, the "look and feel" and the contextual menu options of the IdP indicator (Figure 4f) are altered accordingly.

To integrate with IdPs in the study (i.e., Google, Yahoo, Microsoft, and Facebook), the IdP login form (Figure 4b) of IDeB passes the user's username and password to a proxy program that we developed. The proxy program is also running on the back-

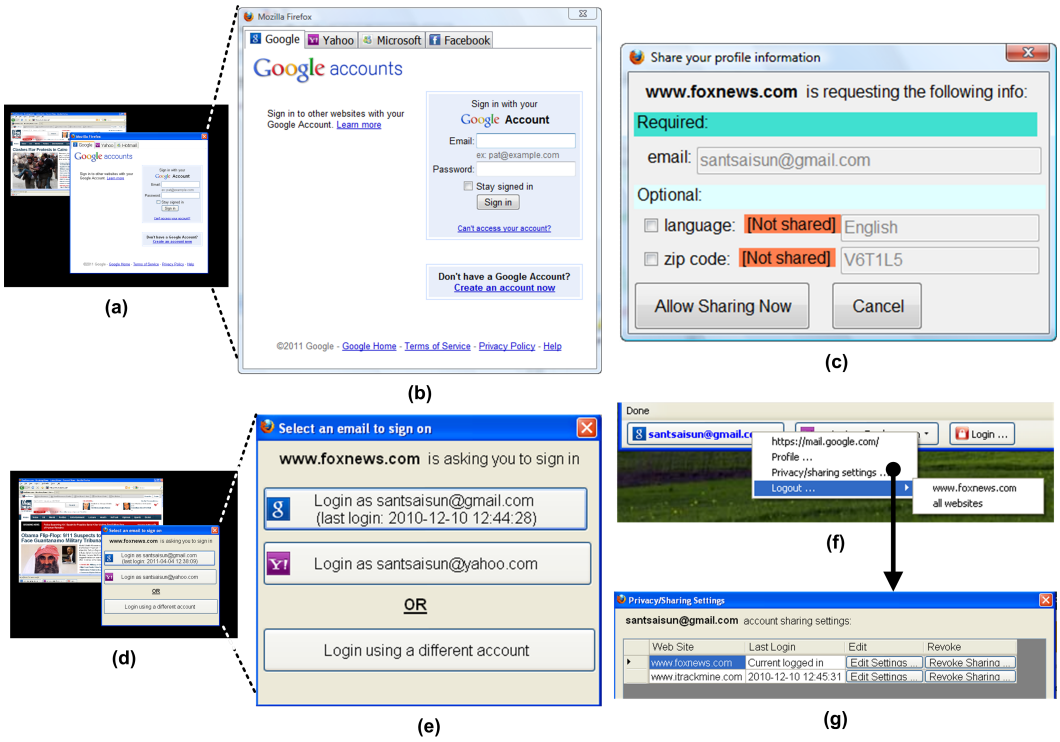


Fig. 4. Main screens of the identity-enabled browser (IDeB): (a) block-out desktop and IdP login form, (b) IdP login form that supports accounts from Google, Yahoo, Microsoft and Facebook, (c) profile sharing consent form, (d) block-out desktop and IdP account selector, (e) IdP account selector, (f) IdP identity indicator, (g) profile sharing setting form.

ground of the study computer. When the proxy receives the user's IdP username and password, it signs onto the IdP using the provided login credential, scrapes the user's profile information from the IdP's user profile page, collects cookies issued by the IdP, and then passes the collected user's profile information and cookies back to the IDeB. The collected information is then used by the IDeB for the subsequent tasks such as profile sharing consent (Figure 4c), shared profile editing and revoking (Figure 4g), integrating RPs by replacing the user information displayed on the RP website, and providing the participants with access to her email box on the IdP using the collected cookies.

5.2. IDeB From User's Perspective

Figure 4 shows the main screens of the IDeB. When a user begins to sign onto an RP website for the first RP login attempt in a browser session, the IDeB prompts the user to log in using one of their IdP accounts from Google, Yahoo, Microsoft or Facebook (Figures 4a and b). Before it presents any prompts to the user, the IDeB freezes and dims out the whole desktop (the *block-out* desktop), and shrinks the browser window (similar to the Windows User Account Control (UAC) prompt). This could redirect the user's attention to the IdP login form, and convey a more accurate mental model (i.e., they are giving their credentials only to the IdP)—requirement R1. We reused the existing IdP login forms to make the IDeB look more trustworthy through positive transfer effects—R2.

The block-out desktop and the shrunken browser could make it difficult for malicious websites to phish users' IdP login credentials with spoofing prompts, because the JavaScript of malicious websites cannot alter the UI elements outside the chrome area of a browser (e.g., tabs, address bar, tool bars, status bar), or take a screen shot of the current page—R3. Unless the user's browser or computer is compromised already, shrinking the browser by using a "zoom in" animation effect before the login prompts are presented prevents malicious websites from showing a similar dialog to the one prompted by the IDeB. Note that although only the browser itself can alter the UI elements outside the chrome area and screenshot the current page, this phishing-resistant feature may still need the attention of the user.

If the user uses an IdP account that has never been used to sign in to this particular RP before, a dialog that solicits the user's profile information will be presented (Figure 4c). The profile sharing form is pre-filled with the user's profile from the IdP, and the user can edit the profile attributes requested by the RP (i.e., a fine-grained privacy control)—R4. Once logged in, the user's current login information is shown on an *IdP identity indicator* located on the left-hand corner of the browser' status bar (Figure 4f)–R5. The user can manage her IdP profile and sharing information from the context menu of the IdP indicator. Using the profile sharing setting form (Figure 4g), the user can view the last login time (or whether currently logged in) for each RP website, edit the shared profile attributes, and revoke the RP's access to the IdP account–R4.

For the subsequent RP login attempts in the same browser session, the IDeB prompts the user to select an authenticated IdP account to sign onto the RP (Figures 4d and e)–R6. In the IdP account selector (Figure 4e), if the IdP account has been used to sign in to the RP website, the last login time to the RP website is shown on the button (i.e., santsaisun@gmail.com in Figure 4e). This can serve as a cue for the user to remember which IdP account is used for this RP website. If the user selects an IdP account that has never been used to sign in to the RP (i.e., santsaisun@yahoo.com in Figure 4e), a profile sharing consent form similar to the one in Figure 4c will be presented. From the IdP account selector (Figure 4e), the user can also click on "Login using a different account" button to use a different IdP account via the IdP login form (Figure 4b) for the visiting RP website.

When users sign onto RP websites with different IdP accounts, they traditionally have to remember which identities were used to access which RPs, and what profile information being shared with different websites. To support this, in addition to the visual cue for returning users on the IdP account selector (Figure 4e)–R6, the IdP indicators change their appearance based on the "signed-up" and "signed-on" status with the website on the current tab of the browser (Figure 4f)–R5. Users may also log out from all websites that used the selected IdP account for login (i.e., single sign out), or view and modify their profile sharing information with one click on the IdP indicator–R7.

6. FORMATIVE STUDY

To confirm the findings from the exploratory study (as only nine participants were interviewed), and to test the prototype, we conducted a formative within-subjects study. This study was designed in such a way that each subject spent only a limited amount of time (about 10 minutes) with each condition to reduce fatigue effects. We counterbalanced the order in which the interfaces were presented.

6.1. Study Protocol

Seven participants with similar demographics to the exploratory study were recruited. Each participant was asked to perform the same set of tasks similar to the exploratory

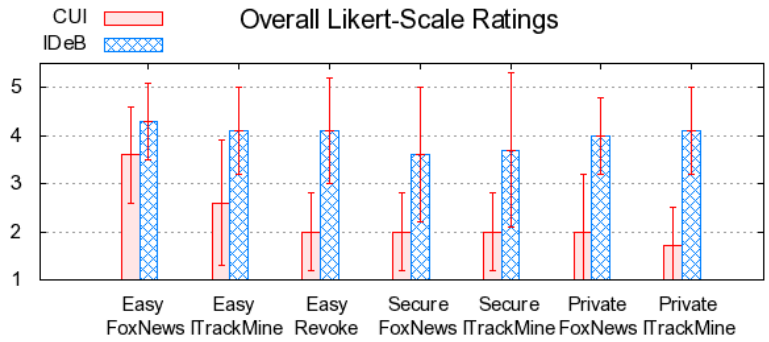


Fig. 5. The overall Likert-scale ratings from post-condition questionnaires in the formative study.

study using both the current user interface (denoted as "CUI") and the IDeB. After completing a background questionnaire, participants were instructed to sign onto two websites (only the Fox News and ITrackMine to reduce fatigue effects), and then log out of all websites as if the tasks had been performed on a public computer. We then asked the participants to check their email using the IdP account that was used to log in to the RP websites. At the end of each condition, we provided full step-by-step instructions for the participants to remove the access of Fox News and ITrackMine from their IdP accounts.

After each condition using CUI/IDeB, the participants were asked to draw how they think (their mental model) the information flowed from one location to another during the sign on process to the Fox News website. They were also asked to rate the ease of use, the security, and the level of privacy control of the interface from 1 to 5 (1=very poor, 5=excellent).

When both conditions were completed, participants were asked in a post-session questionnaire to compare the usability, security, and privacy of both systems, as well as to express their future preferred login system (the traditional login was included as an option). After the post-session questionnaire, a printout of a fake Google login form was presented to the participants, and we asked them if they could find a way to tell whether or not this was the real Google website. The phishing identification task was added to the very end of the session to prevent it from influencing the participants' responses in the post-session questionnaire. At the end of the session, the researcher conducted a contextual interview with the participants to understand their impressions of both systems. Participants were then debriefed.

6.2. Results and Findings

Most participants completed the study tasks successfully when working with the IDeB design, while exhibiting similar misconceptions and concerns from the exploratory study when using CUI. As consistently seen both in the post-condition and the post-session questionnaires, as well as the interview, our IDeB design was preferred by most participants. Note that we do not claim that IDeB is ready for real-world deployment; instead, we used IDeB mainly as a study tool to explore possible design improvements. We further discuss the conceptual gaps derived from the current interface (CUI), and how they were improved by the IDeB in Section 8.

Figure 5 shows the post-condition questionnaire results for the sub-tasks, where the x-axis represents the tasks and the y-axis is the mean rating of the seven participants, with standard deviation bars. The results suggest that our design is easier to use, is

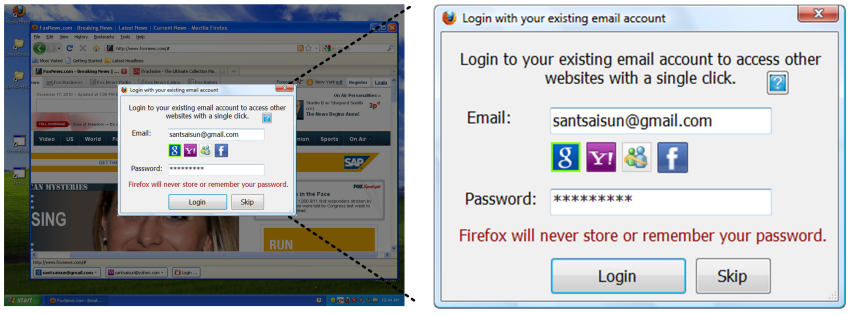


Fig. 6. The block-out desktop and IdP login form designed and used in the formative study.

perceived to be more secure, and affords more privacy control. In the post-session questionnaire, 29% of the participants stated that they would prefer to use the traditional login option instead of using a single-sign-on system; the remaining 71% would prefer to use our IDeB design, with none choosing CUI.

There were, however, issues that were revealed for our interface; in particular, the block-out desktop and the IdP login form as illustrated in Figure 6. First, two participants thought that the IdP login form was popped up by the RP website, and they were giving their username and password to the website directly. Second, three participants commented that the look and feel of our interface (Figure 6) was not familiar, and that this affected their trust of the system. Feedback from participants suggested that in addition to usability, the trust a user has in the interface plays a substantial role in the success of the approach. Finally, we found that this version of the IDeB still relied on the users' cognitive capabilities to detect IdP phishing attacks, as a malicious RP could dim out its website and then prompt the IdP login form to spoof the user.

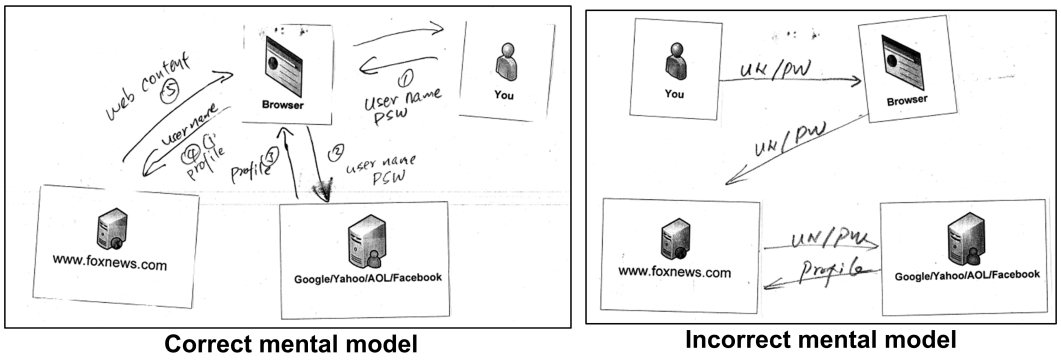
To address these issues, we redesigned IDeB as follows: (1) The IDeB shrunk the browser window before presenting the IdP login form (Figure 4a) to prevent malicious RP websites from showing a similar dialog to the one prompted by the IDeB. (2) We reused the existing login forms from IdP websites (Figure 4b) instead of presenting a customized one (Figure 6) to make the IDeB look more trustworthy through positive transfer effects. (3) The IDeB made the block-out desktop completely opaque instead of transparent in order to convey a more accurate mental model (i.e., users are giving their credentials only to the IdP).

7. COMPARATIVE STUDY

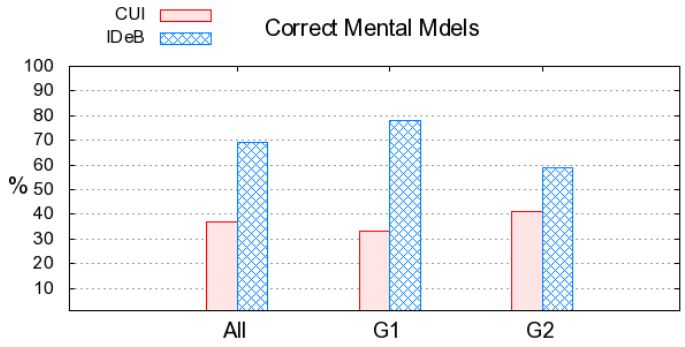
After revising the prototype based on the noted deficiencies from the formative study, we employed the revised interface to conduct a full within-subjects comparative usability study that compares the CUI and the IDeB.

7.1. Participants

We recruited 35 participants from both the University of British Columbia and general community for the study. All participants were paid $10 CAD for their participation. To ensure diversity, we screened interested participants by email, asking their age, gender, degree and major, occupation, and whether or not they were students. We counterbalanced the order of presentation by dividing participants into two groups: the 18 participants in Group 1 (G1) used the CUI before the IDeB, while the 17 in Group 2 (G2) used the IDeB before the CUI. Participants with similar demographics were divided among the two groups to reduce the individual differences that might affect the development of their mental models (see Table II for participant demographics). None of the differences in demographic properties between the two groups were statistically



(a) A representative sample of correct (left) and incorrect (right) mental model drawings.



(b) Percentages of participants who developed correct mental models.

Fig. 7. Sample mental model drawings and results.

Table II. Participant Demographics

Property		Group 1		Group 2		Total	
		N = 18	%	N = 17	%	N = 35	%
Gender (F / M)		10 / 8	56 / 44	6 / 11	35 / 65	16 / 19	46 / 54
Student (Y / N)		8 / 10	44 / 56	10 / 7	59 / 41	18 / 17	51 / 49
Age	19–24	8	44%	6	36%	14	39%
	25–34	5	28%	5	29%	10	29%
	35–44	5	28%	5	29%	10	29%
	45 or over	0	0%	1	6%	1	3%

Participants' demographics in the comparative study.

significant (Chi-square test). Participants had a wide range of education levels (from high school to Master's degree) and the 17 non-student participants had a variety of occupations, such as teachers, financial planners, dentists, business managers, and IT support technicians.

7.2. Results

In the following sections, we present results collected from post-condition and post-session questionnaires. Throughout, we specify the results overall (All), and by the two presentation order groups (G1 - CUI first, G2 - IDeB first) in order to examine whether the order of conditions affects the users' mental models and their preferences.

Table III. Rating Statistics

Type	Task $N = 35$	z	p Asymp. Sig.	$r = z/\sqrt{N * 2}$	50th (Median) CUI	IDeB
Ease -of-use	Fox News	-3.331	.001	0.40	4	5
	ITrackMine	-4.559	.000	0.55	2	5
	Revoke	-4.774	.000	0.57	2	5
Security	Fox News	-2.356	.018	0.28	3	4
	ITrackMine	-2.725	.006	0.33	2	3
Privacy	Fox News	-3.654	.000	0.44	2	4
	ITrackMine	-3.643	.000	0.44	2	4

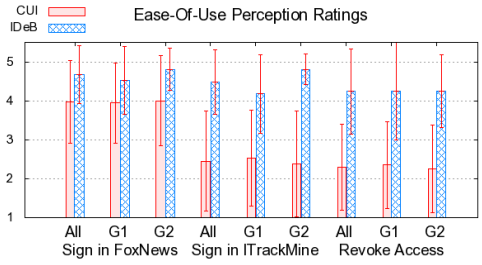
A Wilcoxon Signed Rank Test revealed a statistically significant difference between the CUI and the IDeB in the perceived ease-of-use, security protection and privacy control for all sub-tasks ($z = -2.356$ to -4.774, $p < .018$), with a medium to large effect size, ($r = 0.28$ to 0.57). The median rating scores for the CUI and the IDeB are listed on the last two columns respectively.

7.2.1. Mental model drawings. As Jonassen and Cho [2008] state, "drawings can be a complementary method of verbal reports" for capturing users' mental models. After each condition, we provided participants with four picture cut-outs ("You","Browser", "Fox News", "Google/Yahoo/Microsoft/Facebook") and asked them to express how they believe the information (in terms of their username, password, profile data) flows from one entity to the other when they sign onto the Fox News website. We categorized a mental model drawing as "correct" if the participant clearly indicated that they gave their username and password only to their IdP, but not the Fox News website. Figure 7a illustrates a representative sample of correct and incorrect mental model drawings from our participants. The percentages of participants who developed correct mental models in the study are shown in Figure 7b. We further examine the gaps between the participants' incorrect mental models and the underlying system model in Section 8.1.

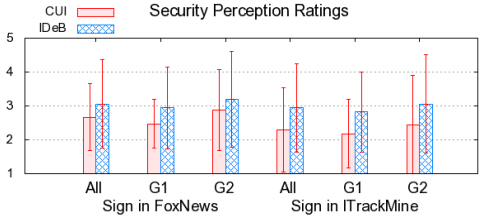
7.2.2. Ratings and rankings. After each condition (i.e., completing the study tasks using the CUI or the IDeB), participants were instructed to rate the perceived ease of use (Figure 8a), security protection (Figure 8b), and level of privacy control (Figure 8c) from 1 to 5 (1=very poor, 5=excellent). The rating differences between the CUI and the IDeB are statistically significant with a Wilcoxon Signed Rank Test as shown in Table III.

At the end of the session, participants were asked: "*For these two approaches that you used to sign onto different websites in the study, which one is easier for you to use / makes you feel more secure / makes you feel more in control of your privacy?*" Figure 9 shows the ranking results from post-session questionnaires, which conforms to the post-condition Likert-scale ratings in Figure 8. We only report the overall rankings in Figure 9, as there were no significant differences observed in participants' choices in terms of the order of interface presentation.

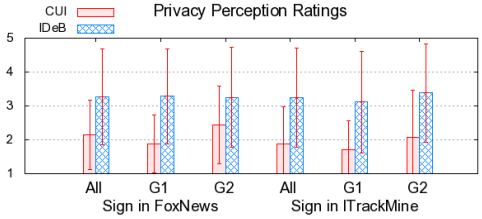
7.2.3. Login option preferences. In the post-session questionnaire, we asked all participants, "*In the future, if you encounter a website that supports using a third-party account to log in (similar to the websites in the study), which approach would you use to login?*" Possible options for the participants included: "CUI", "IDeB", "traditional login", "depends on which website they are logging into", and "Don't know/haven't decided." We then probed the reasons behind their choice. Figure 10a shows the participants' preference for future login. One interesting observation is that one-third of participants preferred using SSO (IDeB—29% or CUI—3%), another one-third chose to create a separate username and password on different websites (29%), and the rest



(a) The perceived ease-of-use Likert-scale ratings.

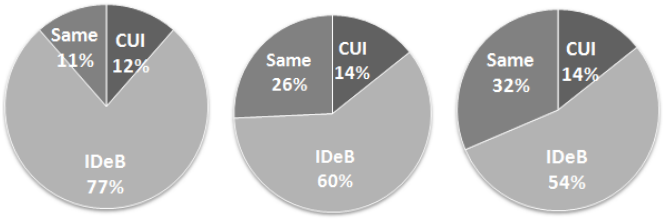


(b) The perceived security protection Likert-scale ratings.



(c) The perceived privacy control Likert-scale ratings.

Fig. 8. The average and standard deviation of Likert-scale ratings from post-condition questionnaires. The differences are statistically significant with a Wilcoxon Signed Rank Test (see Table III).

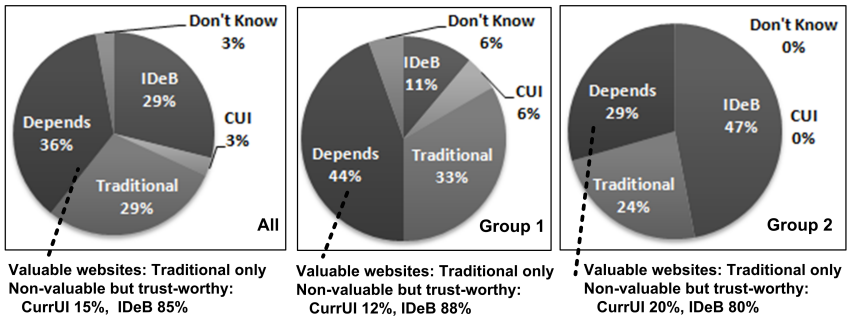


(a) Ease of use (b) Security (c) Privacy

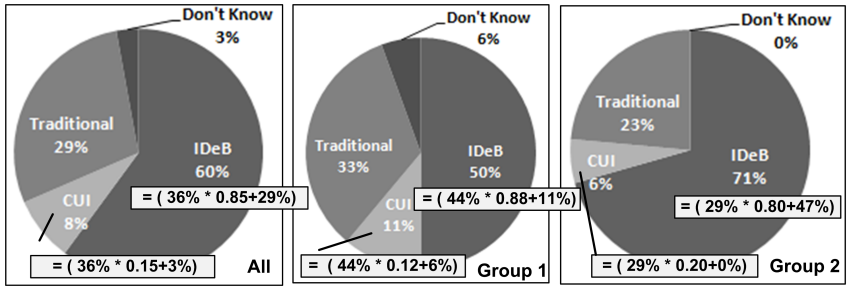
Fig. 9. The perceived ease of use, security protection, and privacy control ranking results from post-session questionnaires suggest that our design is favored by most participants.

based their preference decisions on the types of websites they are accessing. Possible factors that influence their adoption intentions are further discussed in Section 9.

We asked participants who chose “it depends” (36%) to provide their reasoning behind which login options they would prefer to use, and on what kinds of websites. All of them stated that they would not use the SSO on websites that contain valuable



(a) The login option preferences regardless types of websites.



(b) The login option preferences for non-valuable but trustworthy websites.

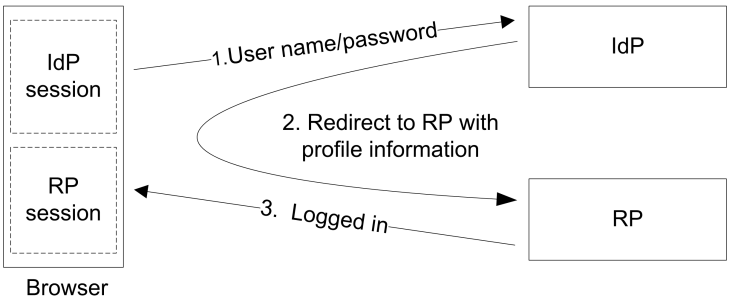
Fig. 10. The login option preferences from the post-session questionnaire indicate that 60% of study participants would use IDeB on the websites they trust.

personal information (e.g., bank, tax, stock websites). For the other websites, if the website itself is trustworthy (e.g., a website that they are familiar with or that has a good reputation), they would like to use an SSO solution, and would prefer to use the IDeB (All 85%, G1 88%, G2 80%), because of its ease of use and privacy control; otherwise, they would rather create a separate account on the website to avoid misuse of their IdP account.

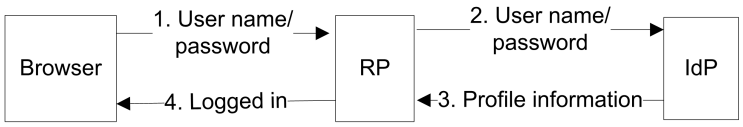
Figure 10b shows the participants' login preference for non-valuable, but trustworthy, websites. The percentage of the participants who chose "Depends" from Figure 10a is broken down and added to the CUI or IDeB, based on their indicated preference. For example, the percentage of all participants that preferred IDeB on websites they trust is calculated as 36% ("Depends") * 85% + 29% = 60%.

8. CONCEPTUAL GAPS

In the exploratory study, we noticed several common misconceptions and concerns exhibited by our participants (e.g., the incorrect belief that the RPs knew their IdP login credentials, implicit IdP login concern, uncertainty about what the RP could do to their IdP account after consent, and account linking confusion). We revised the design of our formative and comparative studies to better understand the root causes of those confusions. Through mental model drawings, questionnaires, and post-session interviews, we identified several conceptual gaps between the acquired mental model and the underlying system model. In this section, we examine how those gaps are formed, and how they influence participants' perceptions. Note that the statistic numbers reported in this and subsequent sections are based on the comparative study with 35 participants.



(a) The Web SSO system model.



(b) The incorrect mental model.

Fig. 11. The data flows of the system model and the acquired incorrect mental model. The system model has a *triangular* data flow with two distinct browser sessions with the RP and IdP, while the data flow of the incorrect mental model is *linear* (i.e., the user's login credential is given to the RP without an active session with the IdP.)

8.1. Triangular versus Linear Data Flow

Many of our participants developed an incorrect mental model via the interactions with the web SSO systems in the study. As illustrated in Figure 11a, the web SSO architecture has a *triangular* data flow in which the authentication request and response are passed between the RP and the IdP through the browser. There are two separated browser sessions with the RP and the IdP respectively; the user-to-IdP authentication and authorization (i.e., profile sharing consent) are performed *only* within the IdP session. The RP and IdP browser sessions are independent from each other, because the browser's same-origin policy [Ruderman 2008] prohibits a document or script of an RP website from accessing web content served by an IdP site. For each IdP, a user may need to authenticate only once in the same browser session, as an IdP typically issues an authentication cookie after a successful login, and then uses the cookie to authenticate the current user for the subsequent requests. Via an option on the IdP login form (e.g., "remember me") that causes a persistent session cookie to be stored on the user's computer, an authenticated IdP session could be retained across browser sessions (i.e., after the browser is closed).

As opposed to the triangular authentication flow in the system model, the data flow of an incorrect mental model is *linear*, as illustrated in Figure 11b. In this mental model, the user provides the RP with their username and password to retrieve profile information from their IdP account. In addition, the user believes they interact solely with the RP, and that the RP could access the user's profile information at anytime.

We observed that many participants formed an inaccurate mental model when they were signing into the Fox News website initially, and then the incorrect mental model was "confirmed" when they were asked to sign out and log back into Fox News. On the first login attempt, because the user-to-IdP authentication and authorization were performed on a pop-up window *originated from and surrounded* by the Fox News website, participants thought they were giving their IdP login credentials to the RP. On the second login attempt, as participants had already authenticated to their IdP in the

same browser session, the pop-up window simply *blinked open and then closed* without prompting users for authentication. We found that the lack of an IdP login prompt for subsequent RP login attempts reinforces participants' incorrect belief that the RP website possesses their IdP username and password.

With the incorrectly formed mental model, participants make dangerous mistakes and exhibited surprise and concern:

— On the Fox News login form, many participants (69%) thought that they should enter their IdP username and password directly into the traditional login fields in order to initiate a login process.
— When logging back into the Fox News website, 29% of participants were surprised that they could sign in without any authentication and authorization (i.e., the pop-up window blinked and then closed).
— On the ITrackMine's login form, 29% of participants *again* entered their IdP username and password into the traditional login fields directly.
— When logging into ITrackMine website, 26% of participants were surprised that they were only prompted for profile sharing consent without needing to enter their IdP login credential (because of the authentication cookie); they were confused and wondered where their IdP user and password had been stored.
— When instructed to log out of all websites as if they were going to leave the computer, 71% of participants logged out of the RP websites only. After being asked to check their email, those who did not log out from their IdP account and left the browser open (or closed the browser but kept the "remember me" option checked when logging into the IdP) were surprised to see that they could access their email without an explicit login.
— 26% of participants expressed concerns about possible misuse of their login credential by RP websites, and stated that they would use the SSO only on trustworthy websites.

To aid in developing and maintaining an adequate mental model that could reduce users' security errors and concerns, our IDeB design (1) shrinks the browser in which the RP website is shown, and moves it to the top left-hand corner of the desktop before presenting the IdP login form to the user (see Figures 4a and b), and (2) prompts the user to select an authenticated IdP account for every subsequent RP login attempt (Figures 4d and e). Using our design, 69% of participants formed an adequate mental model (CUI 33%). Notably, 44% of participants in G1 acquired an incorrect mental model when they first used the existing interface, but later developed a correct mental model when using our design.

8.2. The By-value versus The By-token Profile Sharing Model

Many participants (40%) were hesitant to authorize the release of their IdP profile information to the RP website, because it was uncertain to them what the RP could do after consent: What was the scope of the authorization? Was the granted permissions limiting the RP's access only to basic identity attributes, or including personal generated contents and friend list as well? Could the RP post messages or update one's status to the IdP account? How long would the authorization last? Was the authorization still valid even after logged out from the IdP account? Could the authorization be revoked or not, and how?

The answers to the aforementioned questions largely depend on the profile sharing model supported by the web SSO protocol in question, but they also vary subtly among individual IdP implementations. We observed that there are two different profile sharing models supported by current web SSO solutions: *by-value* and *by-token*. With a sharing-by-value model, a copy of the requested profile information is passed to the

Table IV. Differences of By-value and By-token Sharing Models

model	**by-value**	**by-token**
protocol	OpenID	OAuth
scope	identity attribute	identity, social graph, content, streams, etc.
format	key-value pair	compound data
visibility	explicitly shown	implicitly described
action	read only	read, append, write
duration	one time	one time, time limited, permanent

The main differences between by-value and by-token profile sharing models.

RP via the browser when the user is redirected back to the RP website. Once the SSO login process is completed, the user's profile data is no longer accessible to the RP. In contrast, with the by-token model, instead of the actual profile attributes, an access token that represents the scope and duration of the authorization is passed back to the RP. Using the authorized access token, the RP then makes requests to access the user's data through a direct communication (i.e., not via the browser) with the IdP.

Currently, the by-value profile sharing model is provided by OpenID with Simple Registration [Hoyt et al. 2006] and Attribute Exchange [Hardt et al. 2007] extensions. Major OpenID providers such as Google, Yahoo, AOL, MyOpenID, and PayPal, support this sharing model. As opposed to OpenID, which is designed mainly for authentication with profile sharing as its extended function, the OAuth protocol [Hammer-Lahav 2010] is primarily designed for authorization, and is commonly used to realize the by-token profile sharing model. OAuth enables a user to grant a third-party site access to their information stored with another service provider, without sharing their login credential or the full extent of their data. Major social websites such as Facebook, Twitter, MySpace, Microsoft, Google, and Yahoo employ OAuth to achieve single sign-on and facilitate user content sharing between websites. Some IdPs, such as Google and Yahoo, support both sharing models; the authentication request from a specific RP determines which sharing model is activated.

The main differences between these two profile sharing models are listed in Table IV. With the by-value model, the user's profile attributes are shared as parts of the protocol payload; they are simple key-value pairs that could be shown explicitly on a profile sharing consent form. In contrast, an access token does not contain profile attributes, but the presence of the token allows the RP to retrieve, append or update the user's profile data by calling API services published by the IdP. With the by-token model, the scope and duration of an authorization could be customized for each IdP implementation. Typically, in addition to identity attributes, compound data such as a user's social graph (i.e., friends with roles), personal content (e.g., photos, videos, blogs) and message streams (e.g., status updates, comments) are shared with RP websites.

The duration of an authorization is another source of confusion among users. Varying by individual implementation, the duration of an authorization could be one-time, a limited period of time, or long-lived, and would depend on whether the user is onlined with the IdP; for instance:

— Twitter: The lifetime of an access token is long-lived until explicitly revoked by the user.
— Facebook and Google: One hour by default. When `offline_access` permission is explicitly authorized by the user, the RP could perform authorized requests on behalf of the user at any time.
— Microsoft: An access token is valid as long as the user is still signed into Microsoft Live Connect. A special authorized permission (`wl.offline_access`) enables an RP to read and update a user's information at any time.

— Yahoo: One hour by default; the access token could be renewed via OAuth Session extension [Tom et al. 2008].

Our prior work [Sun et al. 2010a] found that the by-token sharing model provides RPs with higher business incentives, because RPs could (1) get access to users' social graphs in addition to their profile data, (2) utilize platform-specific services such as messaging, and (3) provide a richer user experience through social plug-ins such as recommendations and activity feeds. Nevertheless, results from our study show that users' privacy concerns significantly influence their adoption intention. In addition, we noticed that most participants did not know how to manage their authorizations on each IdP website, and many found it difficult to do so even when told how.

To improve users' perceptions of privacy and control, our IDeB design (1) sets the email address as the only required attribute; the rest of profile attributes are not shared by default, (2) allows users to edit the requested profile attributes before authorization, and (3) provides a central location for users to manage all of their profile sharing. As shown in our participants' rating and ranking, as well as comments from the interviews, these design features enhance participants' perceived ease of use and privacy control. Shehab et al. [2011] propose an extension to the OAuth authorization protocol that enables the provisioning of fine-grained authorization to users when granting permissions to third party applications. They implemented the proposed OAuth extension as a browser extension, and collected data regarding user decisions. The extension was installed by 1,286 Firefox users, who installed 1,561 unique Facebook applications. Consistent with our findings, their results show that users do have varying willingness towards different profile attribute sharing.

8.3. The Transient SSO Account versus The Traditional Account

When signing into the ITrackMine website using the current interfaces (CUI), most participants (94%) could not complete the task without requiring assistance from us (i.e., explaining why they needed to sign up a new account or link to an existing one). Most participants thought they had already logged into ITrackMine after being redirected back from their IdP, but the RP website required them to complete an account linking process before granting access. As the concept of account linking was not clearly conveyed by the RP website, many participants exhibited confusion or frustration: "I thought I had already logged in." "Then, what was the point of signing into Google?" "Are you going to leave me struggling here?" "Argh? I am frustrated."

The purpose of account linking is to gathering additional profile information required for a new account, as well as to enable existing users to login using the SSO. Most RP websites integrate the SSO after many *traditional* accounts have been manually registered using a traditional login approach. A traditional account typically contains a unique username, password and a validated email along with other profile attributes. On the other hand, an RP website creates a *transient SSO* account after a successful SSO process, which contains a unique identifier and the user's profile data from the IdP. Before granting access, however, the profile information in the transient SSO account may not be sufficient (e.g., missing zip code or date-of-birth). In particular, some RPs require a unique username and password from every user to ensure the user can still login when their IdP account is inaccessible, and a valid email address for the password reset and future communications. If any of the required information is missing from the transient SSO account, the RP needs to prompt users to either provide it manually or log into an existing traditional account that has the required information already. In both cases, the SSO account is linked to a traditional account (a new or existing one), and the link can be checked by the RP in the future SSO process.

An account linking process migrates a transient SSO account into a traditional account, thereby unifying and simplifying access control after login. However, most of our participants did not understand the purpose and concept of account linking. To provide a frictionless SSO user experience, we suggest that RPs should avoid account linking during SSO, assign different levels of privilege for SSO accounts and traditional accounts, and allow the user to perform the task at hand with just a transient SSO account.

9. THE WEB SSO TECHNOLOGY ACCEPTANCE MODEL

One of our research goals is to understand what factors influence users' adoption intentions, and how. To represent the users' acceptance of web SSO solutions, our model is based on Davis's technology acceptance model (TAM) [Davis et al. 1989], one of the most widely-used models for explaining the factors that affect user acceptance of information technologies. The TAM posits that users' perceived ease of use and usefulness predict application usage. Several previous research efforts have extended and instantiated TAM with variables in different application domains, such as internet banking [Suh and Han 2003], mobile commerce [Wu and Wang 2005], World-Wide Web [Tino and Fenech 1998; Lederer et al. 2000; Moon and Kim 2001], and enterprise resource planning [Amoako-Gyampah and Salam 2004]. Pavlou [2003] proposes a model that integrates trust and perceived risk with the TAM to predict consumer acceptance of electronic commerce. They posit that both trust and perceived risk influence users' intentions to transact, and that consumer trust positively impacts the perceived usefulness and ease of use of a web interface.

Using insights from our studies, we introduce a technology acceptance model in the context of web SSO, as illustrated in Figure 12. Our study found several factors that hinder users' adoption intentions; we correlated them as *antecedent variables* to the intermediate factors in the existing technology acceptance model. Each identified variable was categorized as an *intrinsic variable* that could be improved by the design of a web SSO system, or an *extrinsic variable* that is difficult to resolve with technology alone. Consistent with Pavlou's findings, our study shows that users' risk perceptions influence their attitudes towards accepting a web SSO solution. We further found that, within the context of web SSO, the perceived risk actually involves users' personal information on *both* RP and IdP websites, and each is influenced by different variables.

9.1. Intrinsic Variables

As illustrated in Figure 12, users' perceived ease of use and their risk perception influence their intention to use a web SSO system. Intrinsic variables are mainly misconceptions, and uncertainties resulted from interactions with SSO systems, as we discussed in Section 8. We found misleading login affordance and account linking confusion are the main variables that impact the participants' perceived ease of use. Moreover, as participants were asked to use their real IdP account for the study tasks, we found that participants' risk perceptions with respect to their IdP account were significantly raised by their security misconceptions and privacy concerns.

Our IDeB design was intended to improve the intrinsic variables that hinder participants' adoption intentions. Compared to the current user interface, it was a preferred option for our participants. Nonetheless, from post-session interviews, we also found that extrinsic variables play a significant role in a user's preference of future login options.

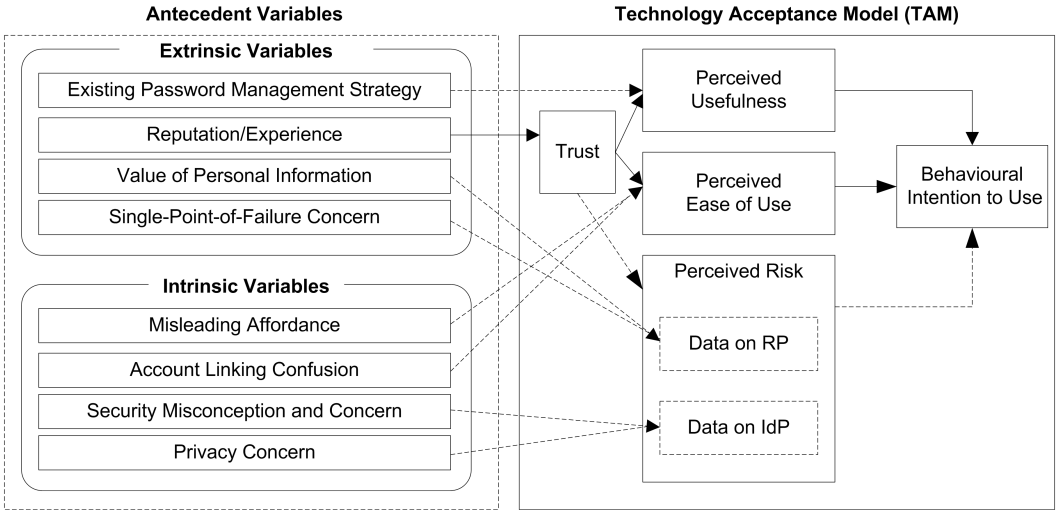


Fig. 12. Web single sign-on technology acceptance model. The acceptance factors we found are correlated as *antecedent variables* to the intermediate factors in TAM, and categorized as *intrinsic* and *extrinsic* variables. Solid arrowed lines indicate *positive* influences, while dashed arrowed lines represent *negative* influences.

9.2. Extrinsic Variables

Even with a highly usable web SSO system, some participants were reluctant to adopt it on any website, or preferred to use it only on certain websites. The extrinsic variables we found are listed as follows:

— Existing password management strategies: Web SSO solutions could reduce the number of passwords a user needs to manage. However, we found that the perceived usefulness of this feature is reduced by participants' existing password management strategies. Similar to Herley's findings (2009), as the majority of user experiences indicate that weak passwords typically do not lead to physical asset loss, most users are "comfortable" with weak or reused passwords. Some (23%) participants in our study used the password manager feature in the browser to reduce their memory burden. Password managers are inconvenient when users switch between computers or when they want to use shared or public computers. However, many of our participants view this as an acceptable solution, because they mostly work on one computer, and most websites provide a password recovery mechanism (e.g., a temporary password sent to the registered email account).
— Single point-of-failure concern: One inherent risk of using a web SSO is that one compromised account on an IdP can result in breaches on all services that use this compromised identity for authentication. Of those participants who favored traditional login, 90% of them expressed this concern.
— The value of personal information: The value of personal data on RP websites increases a user's perception of risk. All the participants that chose the "depends on which website they are logging into" (36%) future login option stated that they would not use SSO on websites that contain valuable personal information or involve potential risk of monetary loss (e.g., banking or stock trading websites). They preferred to create a separate account on those websites. Even though our questionnaires did not explicitly ask our participants about this concern, we believe that it is a general concern applicable to most web users, including participants who chose our design.

— Trust levels with RP websites: Web users need to be confident that their IdP profile would not be misused or abused by RP websites. Most of the participants who chose web SSO as their future login option stated that they would only use a web SSO solution for websites that are trustworthy or with which they are familiar; for websites they do not trust, they prefer to use the traditional login option. Two of our participants refused to use any web SSO solutions as their future login option due to a prior privacy compromise resulting from using Facebook Connect for login. They mentioned: "I had terrible experiences with websites that I used Facebook for login. They posted what I played there to my wall and make me feel embarrassed because all my friends knew about it." "I used Facebook Connect for a while, but then stopped, because I didn't like that it connects all the places to my Facebook account."

Web SSO TAM provides SSO solution designers with a holistic view of the causality dependencies between a user's adoption intention, intermediate factors, and the design and environmental factors. We could not measure the level of concerns for extrinsic factors as they were uncovered from the qualitative interview data. Nevertheless, for a given context or scenario when each factor is measured and the weight of each causality dependency is computed, the weight-populated SSO TAM model can be used to identify strengths and weaknesses of a given web SSO design, prioritize design improvements, and predict how likely it would be that a potential user would adopt a given SSO solution based on measures taken from a brief interaction with the system.

10. RECOMMENDATIONS

Based on our findings, we recommend UI and login flow improvements for RP and IdP websites. To enhance the workflow efficacy of future web SSO solutions, we also offer recommendations for web SSO development community.

10.1. Recommendations for RPs and IdPs

RPs play a substantial role in the success of a web SSO solution. We recommend the following UI and login flow improvements for RPs:

— Provide clear login affordance: Our study found that simply placing a list of IdP icons beside traditional login fields could be misleading. To provide a clear login affordance, our IDeB design separates a traditional login form from SSO login options, with each existing IdP login form located on a separate browser tab (see Figure 4b). This design was intended to transform the observed *negative transfer effect* into a *positive* one in which the user's prior knowledge or experience facilitates the acquisition of a mental model rather than leading to an incorrect one.
— Provide visual cues for returning users: Web users may use different IdP accounts for RP websites, which vary in trustworthiness in order to preserve privacy and prevent single point-of-failure. However, it might be difficult for a user to remember which IdP account was used for accessing which RP, and to determine why an access failed or whom to contact when a problem is encountered. To reduce the memory burden on users in this IdP-to-RP mapping problem, we suggest that RPs should provide visual cues for returning users. One way to accomplish this is by using a persistent browser cookie that encodes the last login-related information (e.g., login option used, selected IdP, username, login time). By checking whether the cookie in question is presented in the HTTP request, the RP could present a customized login screen showing the username, last login time, login options and the corresponding IdP icon to guide the returning user for login.
— Practice the principle of gradual engagement: Requiring sign up for an account before granting access could discourage potential visitors from trying out a new web service. When an anonymous visitor consents to use one of their IdP accounts for the visiting

RP, the RP should grant the user the required permissions for the task at hand without requesting any additional personal information from the user–the principle of *gradual engagement* [Wroblewski 2008]. This instantly turns the visitor into a marketable lead, who is identifiable by the unique user identifier issued by the IdP or their email address. Once the visitor is identifiable, the RP could gradually engage with the user to acquire additional attributes *when there is value for the user to provide them*. Ultimately, the RP may be able to convert the user from performing simple actions, such as page browsing and commenting, to more desired transactions, such as sales of products or software downloads.

— Avoid account linking in the SSO process: As our results suggest, account linking could diminish the usability gain of SSO. We suggest that RP websites should avoid including account linking at the end of an SSO login process and follow the principle of gradual engagement that allows users to perform the task at hand with just a transient SSO account. To enable the existing users to log in using the SSO, we suggest that RPs should prompt existing users to link to an IdP account *during a traditional login* if the association has not been established yet, instead of including account linking in an SSO login flow.

In our study, we found that about one half of our participants did not have prior SSO experience. Based on our SSO research experience [Sun et al. 2010a] and literature reviews, we suggest that RPs should convey the value of the web SSO, and promote the SSO login option on their websites in order to enhance its perceived usefulness to users:

— Convey the benefits of the web SSO: The traditional login approach typically requires new users to fill out a sign up form and remember their chosen password. In addition to profile information, a sign up form normally requires a user to choose a unique username, pick a memorizable password that conforms to the password policy, validate the provided email address through an activation link, and pass a CAPTCHA challenge. In contrast, a properly designed web SSO implementation allows users to sign up and log in with few clicks by reusing login credentials and profile attributes from their IdP account. RPs should clearly convey this “two-click sign up and log in” usability gain to web users.

— Promote the web SSO login option: A high conversion rate, where anonymous visitors are turned into users, is desirable for many websites; however, most websites enjoy only small conversion rates. The average online conversion rate is around 3%, with the highest at approximately 9% [Strouchliak 2009]. Compared to the traditional login approach, the web SSO could encourage an anonymous visitor to try out a site’s services with a few simple clicks. Hence, RPs should promote web SSO login option by placing it on the top or left-hand side of a traditional login option, or requiring one additional click to reach the traditional login form.

Privacy concerns are another major obstacle that impedes users’ SSO adoption. To minimize users’ privacy concerns, we recommend the following suggestions for IdPs:

— Provide a fine-grained privacy control: Our results indicate that users want to control the degree of disclosure of their IdP profile information to RP websites, but this control is lacking from the current IdP implementations. The current option for profile sharing is now all or nothing, which might be intended by IdPs to trade users’ privacy for the websites’ adoption as RPs. To reduce users’ privacy concerns, IdPs should provide a fine-grained privacy control that allows users to edit the scope and duration of the requested permissions before consent.

— Explicit user consent: Prompting user consent for each RP sign-on request could increase users’ privacy awareness and control. Automatic authorization granting (i.e.,

consent only once for a given RP) should be offered only to RPs that explicitly request it during registration. To encourage the practice of the principle of least privilege by RPs, IdPs could also prompt a user consent for *every* authorization request originated from RPs that ask for extended permissions, such as `offline` or `publish_actions`.

— Support of multi-persona accounts: Four participants who favored our design told us that the IdP account they used in the study is a spare or garbage account, and that they used this account to sign onto untrustworthy websites in order to avoid their security and privacy concerns. Using a fake account for SSO is a good strategy for users to minimize their risks, but it requires users to remember and to switch to a corresponding IdP account when visiting an RP website. In particular, if both fake and real accounts are from the same IdP, the user needs to log out the real account and then log in with the fake one, or use a different instance of browser for each account. Participants who used a fake account in the study preferred the IDeB, because it could cue them to switch to an IdP account with one simple click. Based on this insight, we suggest that IdPs should allow a user to maintain multiple profiles in one account; each profile represents a particular persona of the user. During the SSO, a user could choose an appropriate persona for the visiting RP website, with the profile previously used for the RP selected by default. Note that this recommendation does not address the risk of IdP phishing attacks. Despite making it easier for those users who want to use a different persona for different websites, the user still needs to enter her master password for the IdP account.

10.2. Recommendations for the Web SSO Development Community

Based on the successful experience of the password manager enabled browser, a web SSO solution would be more likely to be trusted and adopted by web users when supported by the browser directly. In addition, as shown in our study, an SSO-supported browser could provide users with (1) a consistent interface and flow across RP websites that could unify users' SSO experiences and encourage positive transfer, (2) clear login affordances and visual cues that guide both first-time and returning users through the login process and convey an adequate working mental model, (3) privacy preserving features such as a fine-grained permission control, identity selector, and in-browser profile authorization management, and (4) phishing resistant mechanisms that prevent IdP phishing attacks without relying on the users' cognitive capabilities and continuous attention. Moreover, an SSO-enabled browser could eliminate the need for RPs to design a customized SSO login form, and would reduce the RPs' integration efforts by providing a unified protocol interface for them to integrate a diverse range of web SSO protocols.

As the browser is the central piece that communicates with all actors in the identity ecosystem, we conjecture that the browser can potentially provide a driving force for users to adopt SSO when the browser is directly augmented with identity support. At the time of writing, we are delighted to learn that Mozilla will release a new browser-supported SSO proposal (Mozilla Persona [Mozilla Identity Lab 2012]), and its design is conceptually and architecturally aligned with the IDeB and our previously proposed OpenID$email$ enabled browser [Sun et al. 2010b].

An identity-enabled browser could be more usable for emerging application domains as well. Current HTTP redirection-based web SSO solutions could be problematic in Web 2.0 mashup applications that aggregate personal data located on multiple websites. For server-site mashups that integrate a user's personal content from different providers, being presented with a login form on each service provider could be annoying, and impose a cognitive burden on the user [Austel et al. 2008]. For client-side mashups that use AJAX-style web services to acquire user data from several websites, login forms will block such communications. In addition, existing solutions may be

more difficult to use on mobile or appliance devices that have limited input capabilities.

11. LIMITATIONS

The design of our study supported a direct usability comparison of our IDeB prototype with current SSO solutions. However, because of the inherent limitations of this within-subjects study, we could not evaluate the effectiveness of some important features provided by our design (e.g., phishing protection, multiple IdP sessions, in-browser profile editing and sharing, and single sign-out), and validate the proposed web SSO technology acceptance model. In addition, our empirical study results have the following limitations:

— Generalizability: Participants were primarily young adults, with only one participant over 45 and none under 19. All of the participants reported browsing the web daily or more, and thus might be less prone to errors or misunderstandings while using the interface.
— Realism: The participants were restricted to using the computer and RP websites provided to them during the study. In addition, only the first-time user experience was studied; we did not examine daily usage behaviors. Expanded (more websites) and longer term studies are recommended to address this. In addition, we revised the design of the block-out desktop and the IdP login form used in the formative study to the one employed in the comparative study solely based on our observations and feedback from our participants. Due to the limitations of this short-term laboratory study, we could not evaluate the familiarity impact of the customized login dialog on the user's level of trust, which requires a long-term field study.
— Precision: Carry over and fatigue effects due to the within-subjects format may have affected the study results (although responses were similar between the two groups). A between-subjects study will be required to validate whether those negative effects did exist in our study. Moreover, in the post-session interview, most participants expressed serious concerns about IdP phishing once informed about the issue, and of those participants who preferred traditional login, 90% of them expressed the single point-of-failure concern. These two concerns—as well as other extrinsic factors—were uncovered and identified from the analysis of the qualitative interview data. As those factors were unknown to us before the study, we did not measure the level of each concern. The degree of concern regarding the factors we uncovered, however, can be further quantified and validated by large-scale surveys or laboratory studies. Likewise, four participants in the interview stated that they use multiple IdP accounts for websites that vary in degree of trustworthiness, and that our IDeB design could help them remember which RP website they linked to with which IdP. But as the interviews with those participants occurred in the middle of the whole study, we did not have a chance to ask participants, who have a prior experience of web SSO, how many IdPs they utilize on how many RP websites. This statistical information is, however, an important support for the needs of our multiple-persona recommendation.

We also found issues with our IDeB interface that require further improvement. First, most participants did not notice the identity indicator at the bottom left-hand corner of the screen. Second, it was not clear to the participants that the IDeB does not store their password on the local computer, and some participants were consequently concerned that the stored password and profile information could be compromised. Third, some participants thought that they were giving their username and password to the websites directly. Moreover, we suggest that the account linking task should be performed during a traditional login rather than at the end of an SSO process;

nevertheless, how to convey the concept and benefits of account linking and how to design a usable interface for managing account linking-related tasks (e.g., linking to one or several IdP accounts, unlinking, auditing) are research questions that require further investigation.

12. CONCLUSION

Similar to the way that credit cards reduce the friction of paying for goods and services, web SSO systems are intended to reduce the friction of using the Web. The proliferation of web SSO solutions attracts millions of supporting websites. However, our study found that current implementations of web SSO solutions impose a cognitive burden on web users, and raise significant security and privacy concerns. Moreover, web users do not perceive an urgent need for SSO, and many would only use a web SSO solution on RP websites that are familiar or trustworthy. With an improved design, we found that many users (60%) would use web SSO on the websites they trust if the SSO option is clear to them, and they have control over the sharing of their profile information. In addition, our results suggest an extension to the technology acceptance model in the context of web SSO. With further validations, the model could be used to explain and predict user acceptance of a web SSO solution from measures taken after a brief period of interaction with the system.

Through our empirical investigation, we found that web users could perform SSO correctly after having been taught, but many of them may not want to trade their privacy and security for usability gains. To reduce users' privacy concerns, it is crucial that RPs practice the principle of gradual engagement, and IdPs provide a fine-grained privacy control and on-login profile switching option. In addition, future research should investigate how to enhance users' security perceptions and mitigate IdP phishing attacks without relying on users' cognitive capabilities. We do not claim that our design is ready for real-world adoption as only horizontal user interface functions were designed and evaluated. Nevertheless, we hope that our design and study results will inform the design of future web SSO solutions.

Acknowledgements

We thank study participants for their time, and members of the Laboratory for Education and Research in Secure Systems Engineering (LERSSE), who provided valuable feedback on the earlier drafts of this paper. Cormac Herley provided feedback in his capacity as shepherd, as well as during his visit to UBC in May 2010. Comments from the anonymous reviewers were instrumental in improving the SOUPS conference version of this paper. This research has been partially supported by the Canadian NSERC Internetworked Systems Security Network (ISSNet) Program. Comments from the participants of the ISSNet annual workshop helped us to improve this research.

REFERENCES

ADAMS, A. AND SASSE, M. A. 1999. Users are not the enemy. *Communications of the ACM 42,* 12, 40–46.

AMOAKO-GYAMPAH, K. AND SALAM, A. 2004. An extension of the technology acceptance model in an ERP implementation environment. *Information and Management 41,* 6, 731–745.

ATKINSON, B., DELLA-LIBERA, G., HADA, S., HONDO, M., HALLAM-BAKER, P., (EDITOR), C. K., KLEIN, J., LAMACCHIA, B., LEACH, P., MANFERDELLI, J., MARUYAMA, H., NADALIN, A., NAGARATNAM, N., PRAFULLCHANDRA, H., SHEWCHUK, J., AND SIMON, D. 2002. Web services security (ws-security) v1.0. Tech. rep., IBM, Microsoft, Verisign. April 5.

AUSTEL, P., BHOLA, S., CHARI, S., KOVED, L., MCINTOSH, M., STEINER, M., AND WEBER, S. 2008. Secure delegation for web 2.0 and mashups. In *Workshop on Web 2.0 Security And Privacy*.

CHIASSON, S., VAN OORSCHOT, P. C., AND BIDDLE, R. 2006. A usability study and critique of two password managers. In *Proceedings of 15th USENIX UNIX Security Symposium*. USENIX, Vancouver, Canada, 1–16.

COMMITTEE, X. T. 2005. OASIS eXtensible Access Control Markup Language (XACML) version 2.0. OASIS Standard.

DAVIS, F. D., BAGOZZI, R. P., AND WARSHAW, P. R. 1989. User acceptance of computer technology: A comparison of two theoretical models. *Management Science 35*, 982–1003.

DEVAULT, J., TRETICK, B., AND OGORZELEC, K. 2002. Privacy and independent verification: What consumers want. http://consumerprivacyguide.com/privacy/ccp/verification1.pdf. [Online; accessed 23-August-2011].

DHAMIJA, R. AND DUSSEAULT, L. 2008. The seven flaws of identity management: Usability and security challenges. *IEEE Security and Privacy 6*, 24–29.

DHAMIJA, R., TYGAR, J. D., AND HEARST, M. 2006. Why phishing works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI'06)*. ACM, Montréal, Québec, Canada, 581–590.

FACEBOOK, INC. 2011. Facebook platform statistics. `http://www.facebook.com/press/info.php?statistics`. [Online; accessed 09-Decembe-2011].

FLORENCIO, D. AND HERLEY, C. 2007. A large-scale study of web password habits. In *Proceedings of the 16th International Conference on World Wide Web (WWW'07)*. ACM, New York, NY, USA, 657–666.

FREEMAN, B. 2008. Yahoo! OpenID: One Key, Many Doors. http://developer.yahoo.com/openid/openid-research-jul08.pdf. [Online; accessed 23-August-2011].

GAW, S. AND FELTEN, E. W. 2006. Password management strategies for online accounts. In *Proceedings of the Second Symposium on Usable Privacy and Security (SOUPS'06)*. 44–55.

GIGYA, INC. 2011. Social sign-on. http://www.gigya.com/.

GLASER, B. AND STRAUSS, A. 1967. *The discovery of grounded theory: Strategies for qualitative research*. Aldine de Gruyter.

GOOGLE INC. 2012. The 1000 most-visited sites on the web. http://www.google.com/adplanner/static/top1000/. [Online; accessed 16-October-2012].

HALDERMAN, J. A., WATERS, B., AND FELTEN, E. W. 2005. A convenient method for securely managing passwords. In *Proc. of WWW 2005*. 471–479.

HAMMER-LAHAV, E. 2009. OAuth security advisory: 2009.1. `http://oauth.net/advisories/2009-1/`.

HAMMER-LAHAV, E. 2010. The OAuth 1.0 protocol. http://tools.ietf.org/html/rfc5849. [Online; accessed 28-September-2011].

HAMMER-LAHAV, E., RECORDON, D., AND HARDT, D. 2011. The OAuth 2.0 authorization protocol. `http://tools.ietf.org/html/draft-ietf-oauth-v2-22`.

HARDT, D., BUFU, J., AND HOYT, J. 2007. OpenID attribute exchange 1.0 - final. http://openid.net/specs/openid-attribute-exchange-1_0.html. [Online; accessed 28-September-2011].

HODGES, J., HOWLETT, J., JOHANSSON, L., AND MORGAN, R. 2008. Towards Kerberizing web identity and services. http://www.kerberos.org/software/kerbweb.pdf.

HOYT, J., DAUGHERTY, J., AND RECORDON, D. 2006. Openid simple registration extension 1.0. http://openid.net/specs/openid-simple-registration-extension-1_0.html. [Online; accessed 28-September-2011].

INTERNET2. 2008. Shibboleth System. http://shibboleth.internet2.edu/. [Online; accessed 23-August-2011].

JANRAIN INC. 2010. IDSelector. http://www.idselector.com/.

JANRAIN INC. 2012. Engage: Social login and share. http://janrain.com/products/engage/.

JANRAIN INC. 2012. Social login and social sharing trends across the web for Q3 2012. http://janrain.com/blog/social-login-and-social-sharing-trends-across-the-web-for-q3-2012/.

JONASSEN, D. AND CHO, Y. H. 2008. *Understanding Models for Learning and Instruction*. Springer, Chapter Externalizing Mental Models with Mindtools, 145–159.

KANTARA INITIATIVE. 2002. Liberty Alliance Project. http://www.projectliberty.org/. [Online; accessed 23-August-2011].

LAMPSON, B. 2009. Privacy and security: Usable security: How to get it. *Commun. ACM 52*, 25–27.

LAURIE, B. 2007. OpenID: Phishing Heaven. http://www.links.org/?p=187. [Online; accessed 23-August-2011].

LEDERER, A. L., MAUPIN, D. J., SENA, M. P., AND ZHUANG, Y. 2000. The technology acceptance model and the world wide web. *Decision Support Systems 29,* 3, 269–282.

M. ANGELA SASSE, I. F. 2003. *Security and Usability: Designing secure systems that people can use*. O'Reilly, Chapter Usable Security: Why Do We Need It? How Do We Get It?

MALER, E. AND REED, D. 2008. The venn of identity: Options and issues in federated identity management. *IEEE Security and Privacy 6*, 16–23.

MCCREA, J. 2009. Introducing two-click signup. http://blog.plaxo.com/archives/2009/01/introducing_two_1.html. [Online; accessed 23-August-2011].

MESSINA, C. 2009. OpenID Phishing Brainstorm. http://wiki.openid.net/OpenID_Phishing_Brainstorm. [Online; accessed 23-August-2011].

MICROSOFT CORP. 2009. Windows CardSpace. http://www.microsoft.com/windows/products/winfamily/cardspace/default.mspx.

MICROSOFT CORP. 2011. Beyond Windows CardSpace. http://blogs.msdn.com/b/card/archive/2011/02/15/beyond-windows-cardspace.aspx. [Online; accessed 23-August-2011].

MOON, J.-W. AND KIM, Y.-G. 2001. Extending the TAM for a World-Wide-Web context. *Information and Management 38,* 4, 217–230.

MOZILLA IDENTITY LAB. 2012. Mozilla persona. http://identity.mozilla.com/.

MULLIGAN, J. AND ELBIRT, A. 2005. Desktop security and usability trade-offs: An evaluation of password management systems. *Information Systems Security 14,* 2, 10–19.

NANDA, A. AND JONES, M. B. 2008. Identity Selector Interoperability Profile V1.5. http://informationcard.net/specifications. [Online; accessed 23-August-2011].

OASIS. 2005. Assertions and protocols for the OASIS security assertion markup language (SAML) v2.0.

OASIS. 2012. Organization for the Advancement of Structured Information Standards. http://www.oasis-open.org/.

OPENID FOUNDATION. 2009. Promotes, protects and nurtures the OpenID community and technologies. http://openid.net/foundation/. [Online; accessed 23-August-2011].

OPPLIGER, R. 2004. Microsoft .NET Passport and identity management. *Information Security Technical Report 9,* 1, 26–34.

PAVLOU, P. A. 2003. Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce 7*, 101–134.

RECORDON, D. AND FITZPATRICK, B. 2007. OpenID authentication 2.0. http://openid.net/specs/openid-authentication-2_0.html. [Online; accessed 23-August-2011].

ROSS, B., JACKSON, C., MIYAKE, N., BONEH, D., AND MITCHELL, J. C. 2005. Stronger password authentication using browser extensions. In *Proceedings of the 14th Usenix Security Symposium*. Vol. 5.

RUDERMAN, J. 2008. The same origin policy. http://www.mozilla.org/projects/security/components/same-origin.html. [Online; accessed 23-August-2011].

SACHS, E. 2008. Usability research on federated login. http://sites.google.com/site/oauthgoog/UXFedLogin. [Online; accessed 23-August-2011].

SAKIMURA, N., BRADLEY, J., DE MEDEIROS, B., JONES, M. B., AND JAY, E. 2011. OpenID Connect standard 1.0 - draft 07. http://openid.net/specs/openid-connect-standard-1_0.html. [Online; accessed 03-January-2012].

SCHECHTER, S. E., DHAMIJA, R., OZMENT, A., AND FISCHER, I. 2007. The emperor's new security indicators. In *Proceedings of the 2007 IEEE Symposium on Security and Privacy*. IEEE Computer Society, Washington, DC, USA, 51–65.

SHEHAB, M., MAROUF, S., AND HUDEL, C. 2011. ROAuth: Recommendation based open authorization. In *Proceedings of Symposium on Usable Privacy and Security (SOUPS'11)*.

SPIEKERMANN, S. AND CRANOR, L. 2009. Engineering privacy. *IEEE Transactions on Software Engineering 35,* 1, 67–82.

STROUCHLIAK, I. 2009. Conversion rate optimization. http://www.seochat.com/c/a/Website-Marketing-Help/Conversion-Rate-Optimization/. [Online; accessed 28-September-2011].

SUH, B. AND HAN, I. 2003. The impact of customer trust and perception of security control on the acceptance of electronic commerce. *Int. J. Electron. Commerce 7*, 135–161.

SUN, S.-T., BOSHMAF, Y., HAWKEY, K., AND BEZNOSOV, K. 2010a. A billion keys, but few locks: The crisis of web single sign-on. In *Proceedings of the New Security Paradigms Workshop (NSPW'10)*. 61–72.

SUN, S.-T., HAWKEY, K., AND BEZNOSOV, K. 2010b. OpenIDemail enabled browser: Towards fixing the broken web single sign-on triangle. In *Proceedings of the 6th ACM Workshop on Digital Identity Management (DIM'10)*. ACM, New York, NY, USA, 49–58.

SUN, S.-T., POSPISIL, E., MUSLUKHOV, I., DINDAR, N., HAWKEY, K., AND BEZNOSOV, K. 2011. What makes users refuse web single sign-on? An empirical investigation of OpenID. In *Proceedings of Symposium on Usable Privacy and Security (SOUPS'11)*.

SUNSHINE, J., EGELMAN, S., ALMUHIMEDI, H., ATRI, N., AND CRANOR, L. F. 2009. Crying Wolf: An empirical study of SSL warning effectiveness. In *Proceedings of 18th USENIX Security Symposium*. 399–432.

SXIPPER INC. 2009. Sxipper form manager Firefox extension. http://www.sxipper.com/. [Online; accessed 23-August-2011].

THE ECLIPSE FOUNDATION. 2009. Higgins Card Selectors. http://www.eclipse.org/higgins/.

TINO AND FENECH. 1998. Using perceived ease of use and perceived usefulness to predict acceptance of the world wide web. *Computer Networks and ISDN Systems 30,* 1-7, 629–630. In Proceedings of the 7th International World Wide Web Conference.

TOM, A., ALAVILLI, P., AND FLETCHER, G. 2008. Oauth session 1.0 draft 1. http://oauth.googlecode.com/svn/spec/ext/session/1.0/drafts/1/spec.html. [Online; accessed 28-September-2011].

VERISIGN INC. 2009. VeriSign OpenID SeatBelt Plugin. https://pip.verisignlabs.com/seatbelt.do. [Online; accessed 23-August-2011].

WHITTEN, A. AND TYGAR, J. 1999. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *The 9th USENIX Security Symposium*. 169–183.

WIKIPEDIA. 2009. Password fatigue. http://en.wikipedia.org/wiki/Password_fatigue. [Online; accessed 23-August-2011].

WISNIEWSKI, T., NADALIN, T., CANTOR, S., HODGES, J., AND MISHRA, P. 2005. SAML executive overview. Tech. rep., OASIS. March 2005.

WROBLEWSKI, L. 2008. *Web Form Design: Fill in the blanks*. Rosenfeld media, Chapter Gradual Engagement.

WU, J.-H. AND WANG, S.-C. 2005. What drives mobile commerce?: An empirical evaluation of the revised technology acceptance model. *Information and Management 42,* 5, 719–729.

WU, M., MILLER, R. C., AND GARFINKEL, S. L. 2006. Do security toolbars actually prevent phishing attacks? In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems(CHI '06)*. ACM, New York, NY, USA, 601–610.

YEE, K.-P. AND SITAKER, K. 2006. Passpet: Convenient password management and phishing protection. In *SOUPS '06: Proceedings of the Second Symposium on Usable Privacy and Security*. ACM, New York, NY, USA, 32–43.

YODLEE INC. 2012. Personal finance data platform for powering innovation in financial services. http://www.yodlee.com.

ZHANG, Y., EGELMAN, S., CRANOR, L., AND HONG, J. 2007. Phinding phish: Evaluating anti-phishing tools. In *Proceedings of the 14th Annual Network and Distibuted System Security Symposium (NDSS 2007)*.