OpenID-Enabled Browser: Towards Usable and Secure Web Single Sign-On

San-Tsai Sun
University of British Columbia
Vancouver, BC, Canada
santsais@ece.ubc.ca

Kirstie Hawkey
Dalhousie University
Halifax, NS, Canada
hawkey@cs.dal.ca

Eric Pospisil
University of British Columbia
Vancouver, BC, Canada
ericpospisil@gmail.com

Konstantin Beznosov
University of British Columbia
Vancouver, BC, Canada
beznosov@ece.ubc.ca

Ildar Muslukhov
University of British Columbia
Vancouver, BC, Canada
ildarm@ece.ubc.ca

Nuray Dindar
University of British Columbia
Vancouver, BC, Canada
nuraydindar@gmail.com

CHI 2011, May 7–12, 2011, Vancouver, BC, Canada.
ACM 978-1-4503-0268-5/11/05.

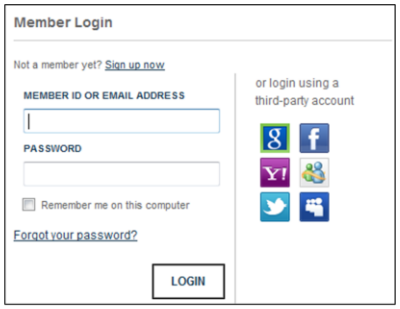
Abstract
OpenID is an open and promising Web single sign-on solution; however, the interaction flows provided by OpenID are inconsistent, counter-intuitive, and vulnerable to phishing attacks. In this work, we investigated the challenges web users face when using OpenID for authentication; and we designed a phishing-resistant, privacy-preserving browser add-on to provide a consistent and intuitive single sign-on user experience for the average web users.

Keywords
OpenID, Web Single Sign-On, Identity-Enabled Browser

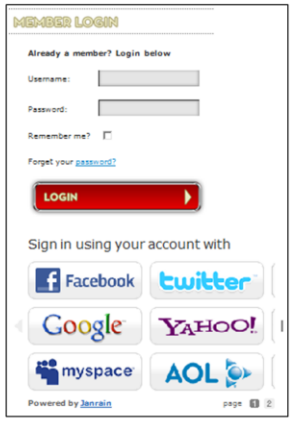
ACM Classification Keywords
H5.0 Information interfaces and presentation: General. D.4.6 Software: Security and Protection.

General Terms
Human Factors, Security

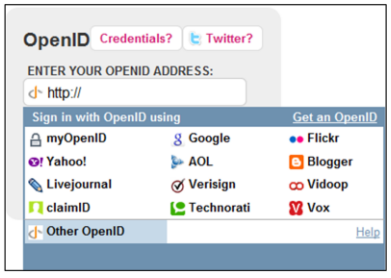
Introduction
Today's Web is site-centric; a typical web user has about twenty-five accounts that require passwords and enters approximately eight passwords per day [2]. Web users face the burden of managing this increasing number of accounts and passwords, which leads to



(a) Fox News, **http://www.foxnews.com**



(b) Itrackmine, **http://www.itrackmine.com**



(c) Skitch, **http://www.skitch.com/**

figure 1. Relying party login forms.

"password fatigue". In addition, the site-centric Web makes online profile management and personal content sharing difficult, as each user account is created and managed in a separated administrative domain.

Web single sign-on (SSO) systems are meant to address the root causes of the site-centric Web. A Web SSO system separates the role of identity provider (IdP) from that of relying party (RP). An IdP collects user identity information and authenticates users, while an RP relies on the authenticated identity to make authorization decisions. OpenID (http://openid.net) is an open and promising user-centric Web SSO solution. According to the OpenID Foundation, there are currently more than *one billion* OpenID-enabled user accounts provided by major service providers (e.g., Google, Yahoo, and AOL).

Many OpenID researchers [1, 3, 5] have recommended best practices and design guidelines for implementing usable login user interface on RP websites. However, with the diverse needs for authentication and user management, the interfaces and interaction flows provided by current RP websites are inconsistent. When accessing *N* RPs using one IdP, the user must visit *N+1* 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, using more than one IdP in a single browsing session complicates the process for users even further. Finally, OpenID is vulnerable to phishing attacks [4]; and it has to rely on a users' cognitive capability to detect phishing sites.

Our research goal is to improve the overall user experience of OpenID. To achieve this goal, we first conducted an exploratory study to better understand the problems and concerns web users face when using OpenID for authentication. Based on the findings of the exploratory study, we defined a prioritized list of requirements and designed a prototype intended to improve the OpenID user experience and reduce the chances of IdP phishing attacks. We then conducted a formative within-subjects study to compare the usability of our identity-enabled browser (IDeB) with OpenID and identify parts of the prototype and study design that require further improvement. Initial results suggest that web users value the concept of single sign-on and prefer our design. We also found that, in addition to usability, security, privacy, and trust are important factors in the adoption of a Web SSO solution.

We next describe the exploratory study, the design of the prototype, and the usability study. We then present our initial findings, discuss the implications of our results, and conclude with future research plans.

Exploratory Study

In the initial stage, our goal was to understand web users' perception, challenges, concerns, and perceived benefits when using OpenID during the sign up, sign on, and log out processes. In addition, we wanted to understand how the OpenID user interfaces and flows impact users' mental models. The findings from this study were used to inform the prototype design.

Study protocol

We conducted a one-hour lab study and recruited 9 participants (6 male and 3 female) from the University

Incorrect initial mental model. Most participants (8) entered their Google or Yahoo email and password into the login form directly.

Wrong mental model derived from the login process. Five participants thought after the login and consent processes, the website must have their IdP user name and password already.

Misleading affordance. Most participants (8) did not know they need to click on one of the IdP icons to initiate the login process; three participants thought the IdP icons were ads, and two thought the website had teamed up with the IdPs for content sharing.

IdP account association is confusing. Most participants (8) did not understand the purpose of account association with their OpenID account.

Phishing concerns. Most participants (7) correctly identified the fake Google or Yahoo website; but they expressed great concern that in future logins, they might not pay much attention to the URL bar.

Privacy concerns: Most participants (8) were concerned about spam or misuse when associating their IdP account.

table 1. OpenID problems and concerns.

of British Columbia (UBC) and the Greater Vancouver area. Four participants were 19-24 years old and five were 25-34. Most participants were fluent in English (8) and had a college or graduate degree (8), with a diverse range of majors. All had more than four web accounts, and two participants used a password manager for their passwords. Five participants had prior SSO experience using UBC campus-wide login.

After completing a background questionnaire, participants were asked to sign up for and sign in to three OpenID-supported websites using their existing account from other service providers (i.e., Google, Yahoo, or Hotmail). Figure 1 shows the login forms of the websites in the study, in the order presented. Next, we asked the participants 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. Finally, we asked participants to browse to an OpenID phishing demo website (http://idtheft.fun.de/) and select Google or Yahoo as the IdP for login. Before they entered their user name and password, we stopped participants and asked them whether they could identify any clues that this was not the real Google or Yahoo sign in page.

After the tasks, participants completed a questionnaire detailing their experiences with various aspects of the tasks. We then conducted a contextual interview with participants to understand the problems encountered, as well as some of their potential concerns, perceived benefits, and desired features in the OpenID system.

Findings

We found the current OpenID login UI and flow are inconsistent and counter-intuitive, which leads users to form incorrect mental models, and often to abandon the system altogether. Table 1 lists the main problems and concerns found by the study. In addition, all nine participants were very concerned that they had to explicitly log out from the IdP (to prevent others sharing the computer from accessing services provided by the IdP, e.g., Gmail in case of Google IdP) in addition to the websites, as they sometimes use a public computer or share a computer with their family members.

Prioritized list of requirements

Based on the above findings, we prioritized a list of requirements to inform the design of the solution. To be usable, (1) the solution must leverage the skills and experiences that an average web user already has. Based on our study results and prior user studies that evaluated the effectiveness of anti-phishing techniques [7], (2) the solution must avoid relying on users' cognitive capabilities to detect phishing sites. In addition, (3) it must provide a single logout mechanism that automatically ends all authentication sessions when the users log out. Further, (4) it must provide web users with a central location to manage their privacy settings.

In addition, (5) the solution should allow users to choose from different identities for websites that vary in the level of trust. Single point of failure is an inherent property of Web SSO, but (6) the solution should provide a multi-point of failure to prevent compromised accounts. Asking users to provide sign up information during first-time sign on is annoying to users. (7) If the solution could provide gradual engagement features that acquire additional user attributes only when there is value for the user to provide them, it could reduce form abandonment rate.

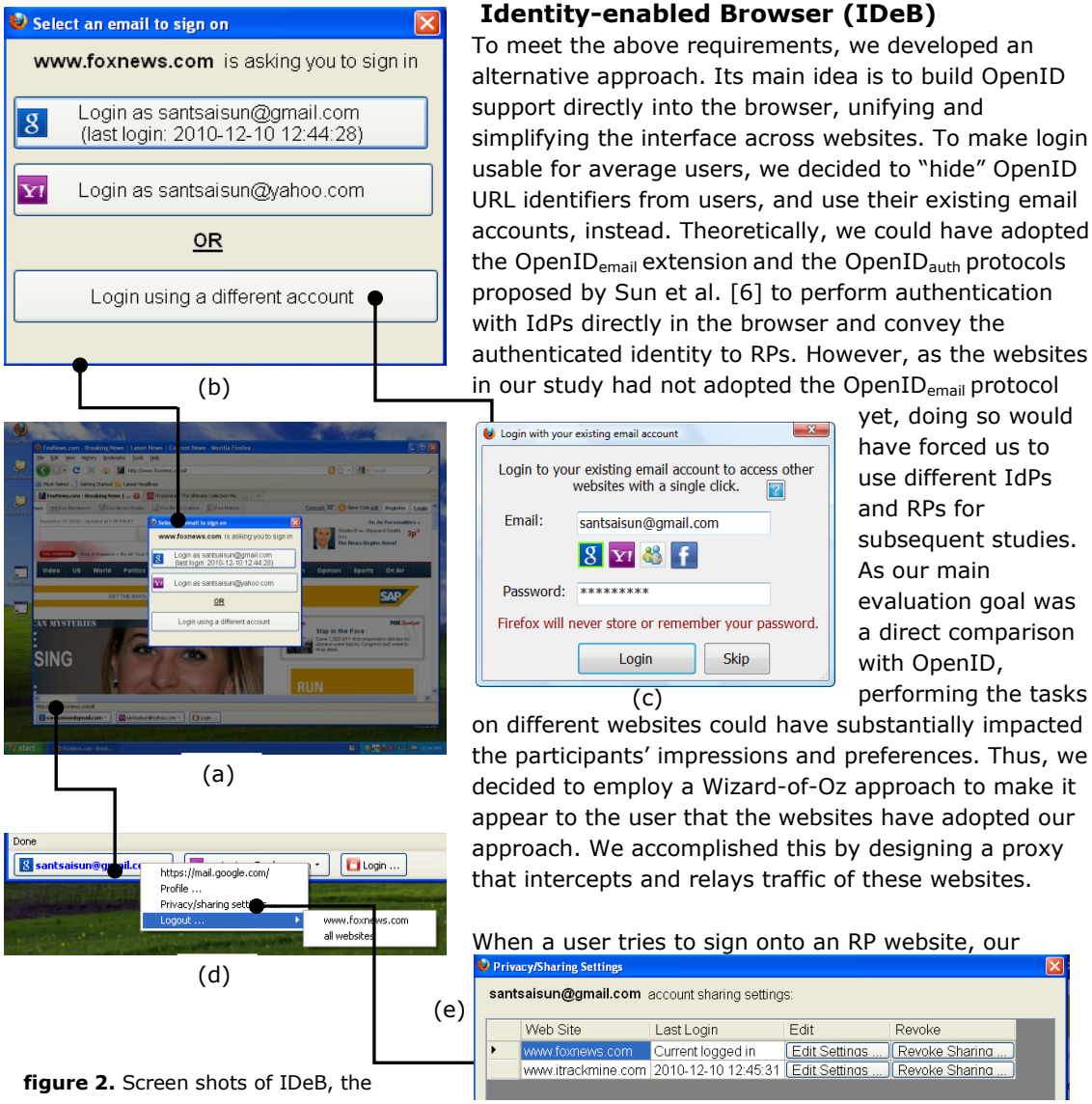


figure 2. Screen shots of IDeB, the identity-enabled browser.

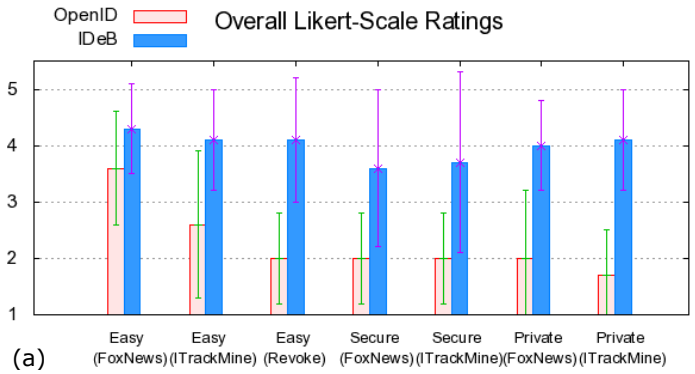
Identity-enabled Browser (IDeB)

To meet the above requirements, we developed an alternative approach. Its main idea is to build OpenID support directly into the browser, unifying and simplifying the interface across websites. To make login usable for average users, we decided to "hide" OpenID URL identifiers from users, and use their existing email accounts, instead. Theoretically, we could have adopted the $\text{OpenID}_{\text{email}}$ extension and the $\text{OpenID}_{\text{auth}}$ protocols proposed by Sun et al. [6] 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 adopted the $\text{OpenID}_{\text{email}}$ protocol yet, doing so would have forced us to use different IdPs and RPs for subsequent studies. As our main evaluation goal was a direct comparison with OpenID, performing the 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 the user that the websites have adopted our approach. We accomplished this by designing a proxy that intercepts and relays traffic of these websites.

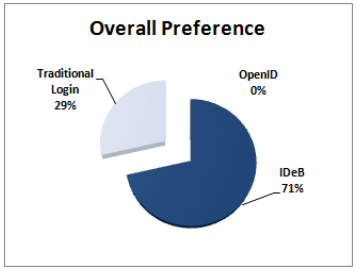
When a user tries to sign onto an RP website, our identity-enabled browser prompts the user to *select* an identity to sign on to the RP (one-click sign on), without creating or entering a user name and password on the website (Fig. 2a, 2b). If the user has not logged in to an IdP account yet or she wants to use a different IdP account for the RP, IDeB prompts the user to login with her email account directly in the browser (Fig. 2c), instead of performing authentication on the IdP's web site. Once logged in, the user's current login information is shown on an icon (identity indicator) located on the left corner of the status bar (Fig. 2d). The user can manage her IdP profile and sharing information from the context menu on the IdP indicator (Fig. 2e).

To prevent malicious websites from phishing users' emails and passwords with spoofing prompts, the IDeB freezes and dims out the whole desktop (*block-out desktop*) before presenting any prompt to the user. This also disables and dims out the original browser user interface so that a malicious website could not mimic the IDeB's prompt behavior. Figure 2a illustrates an IDeB-related prompt that is presented on the block-out desktop.

When users sign on with multiple IdPs in one browser session, they traditionally have to remember which identities were used for accessing which RPs, and what profile information is shared with different websites. To address this problem, we altered the "look and feel" and menu options of the IdP indicators based on the 'signed-up' and 'signed-on' status with the website on the current tab of the browser (Fig. 2d). Users can also view and modify their profile sharing information with a simple click on the IdP indicator (Fig. 2e).



(a)



(b)

figure 3. (a) The overall Likert-scale ratings from post-condition questionnaires. (b) The overall preferences of OpenID, our IDeB design, and traditional login.

Usability Study

To compare the usability of our IDeB design with OpenID and to determine if the issues identified with OpenID have been resolved, without introducing any major new concerns or usability issues, we conducted a performance-based within-subjects study. Every participant was asked to perform the same set of tasks using both OpenID and IDeB. We counterbalanced participants by dividing them into two groups: those who first used OpenID before IDeB, and those who first used IDeB. The study was designed in such a way that each subject spent only a limited amount of time (10 minutes) with each condition to reduce fatigue effects.

Study protocol

Seven participants (2 female, 5 male), with similar demographics to the exploratory study, were recruited. Each participant was asked to sign onto two websites (Fox News and ITrackMine) using both OpenID and our IDeB design. After each condition, the participant was asked to draw how they think the information flows from one location to another during the sign on process, as well as to complete a post-condition questionnaire detailing their satisfaction with various aspects of the tasks. At the end of the session, the researcher conducted a contextual interview with the participant to understand their impressions about both systems and to debrief the participant.

Results

In our evaluation, we asked the participants to rate the ease of use, security, and level of privacy control of the two conditions from 1 to 5, where 1 is very poor and 5 is excellent. In the post-session questionnaire, we asked them to express their login system preference (including traditional login as an option). We found that our design was preferred by most of the participants. This was seen both in the post-task and the post-session questionnaires, as well as the interview. Figure 3a shows the post-task questionnaire results for different sub-tasks, where the x-axis represents the tasks and the y-axis is the average ratings of the 7 participants. The average responses and the standard deviations of the subjects' ratings suggest that our design is easier to use, perceived to be more secure, and gives more privacy control to the user. In the post-session questionnaire, 29% (2/7) of the subjects stated that they would prefer to use the traditional login option instead of using a single-sign-on system. The remaining 71% (5/7) of subjects would prefer to use our IDeB design, with none choosing OpenID (Fig. 3b).

Discussion

The main strength of our new interface is that its design provides users with a consistent and intuitive sign up, sign on, and logout experience. Participants consistently rated our system easy to use and felt more secure with higher privacy control. Most of them completed the study tasks successfully without any help from the investigator when working with our IDeB design, while encountering more errors in OpenID.

We also found that many important features of our interface were not clearly visible to new users. First, most participants did not notice the identity indicator at

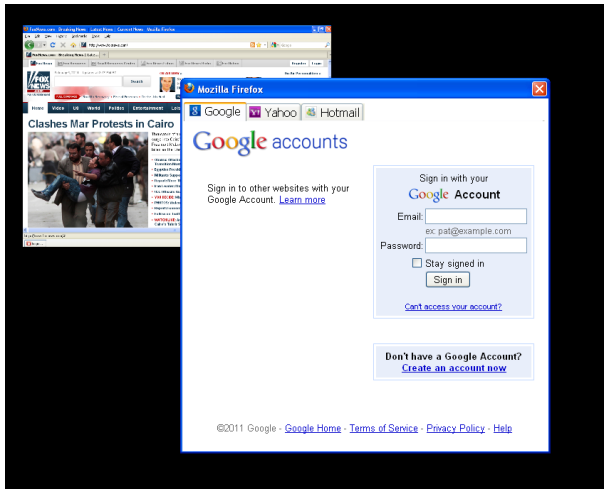


figure 4. IDeB blocks the desktop and shrinks the browser before presenting the IdP login form. It uses the existing login forms from IdP websites instead of a customized one.

the bottom left corner of the screen, and they did not realize that they could login with multiple IdP accounts simultaneously. Second, most participants did not know that the IDeB will not store their password on the local computer; and they were concerned that the stored password and profile information might get compromised. Third, two participants thought that the IdP login form originated from the RP websites; and they thought they were giving their user name and password to the websites directly. Finally, we found that this version of the IDeB still required users' cognitive capabilities to detect phishing attacks. To address these problems, we now shrink the browser window before presenting the login form and reuse the existing login forms from IdP websites instead of a customized one (Fig. 4). In addition, the login form "zooms" into the identity indicator after a successful login and uses a dialog box to draw users' attention.

Conclusion

In this work, we investigated the challenges web users face when using OpenID for authentication, and proposed an identity enabled browser intended to improve the OpenID user experience and reduce the chances of IdP phishing attacks. We do not attempt to show that our design is ready for real-world adoption; instead, we expect that our design and study results could be used to inform the design of future Web SSO solutions. We believe that Web SSO must be built into browser directly to achieve internet-wide adoption. Browser vendors should join in the future development of Web SSO technology to provide a consistent, intuitive, and phishing-resistant user experience. We also suggest RPs should follow the principle of "gradual engagement" to avoid users' privacy concerns.

We have modified our prototype to address feedback from this formative study. In the future, we plan to recruit a broader and more diverse participant pool to further evaluate the usability of our identity enabled browser approach.

References

[1] R. Dhamija and L. Dusseault. The seven flaws of identity management: Usability and security challenges. IEEE Security and Privacy, 6:24-29, 2008.

[2] D. Florencio and C. Herley. A large-scale study of web password habits. In Proceedings of the 16th International Conference on World Wide Web, pages 657-666, New York, NY, USA, 2007. ACM.

[3] B. Freeman. Yahoo! OpenID: One Key, Many Doors. http://developer.yahoo.com/openid/openid-research-jul08.pdf, July 2008.

[4] B. Laurie. OpenID: Phishing Heaven. http://www.links.org/?p=187, January 2007.

[5] E. Sachs. Usability Research on Federated Login. http://sites.google.com/site/oauthgoog/UXFedLogin, October 2008.

[6] S.-T. Sun, K. Hawkey, and K. Beznosov. OpenIDemail Enabled Browser: Towards Fixing the Broken Web Single Sign-On Triangle. In Proceedings of the 6th ACM Workshop on Digital Identity Management, October 8 2010.

[7] Y. Zhang, S. Egelman, L. Cranor, and J. Hong. Phinding phish: Evaluating anti-phishing tools. In Proceedings of the 14th Annual Network and Distributed System Security Symposium, 2007.