Poster: Users' Perceptions of and Willingness to Use Single-Sign-On Functionality[1]

Lujo Bauer, Cristian Bravo-Lillo, Elli Fragkaki, William Melicher, Michael Stroucken
{lbauer, cbravo, elli, billy, mxs}@cmu.edu

1. INTRODUCTION

Internet users are accumulating more and more identities. A seminal study by Florêncio and Herley found that a typical internet user has 25 different identities, each of which has different credentials [3]. In part because managing these identities and credentials is difficult for users and encourages behaviors like password reuse, the US Government has declared the creation of a digital identity ecosystem a national security priority.[2]

In such an ecosystem, *single sign-on* (SSO) systems allow users to authenticate to an *identity provider* (IdP); the IdP in turn vouches for the user to multiple *service providers* (SPs), absolving them of the need to authenticate users themselves. This frees users from remembering many sets of credentials, and service providers from the need to maintain their own authentication mechanisms. Identity providers such as Google and Facebook are increasingly used to sign in to third-party services like Flickr and USA Today. For users, this can increase convenience (e.g., fewer passwords to remember) and security (e.g., service providers need not keep passwords). At the same time, relying on identity providers that have rich information about users (e.g., all information in a Facebook profile) creates the risk that users will lose oversight or control over the access that service providers are given to this information. To address such concerns, identity providers show users consent interfaces at sign on and provide audit tools for post hoc review.

A study by Sun et al. found that users would value the convenience provided by SSO systems but have privacy and other concerns about adopting SSO systems. The authors found a large number of usability problems with OpenID[3], a distributed SSO system. They built and tested an identity-enabled browser tool based on their findings. Participants that used the tool made fewer mistakes in a number of tasks that involved logging into websites, compared to participants that used the unmodified version of OpenID [4]. This agrees with the findings of Egelman's study on the privacy and convenience tradeoff of single sign-on systems [2].

In this poster, we report on a 424-participant on-line study [1] through which we seek to understand the effectiveness of consent interfaces for single sign-on, and use this understanding to provide an alternative design for single sign-on dialogs. We induced participants to log in with one of three identity providers, and measured their awareness of the information that was being sent by identity providers to service providers, their awareness of identity

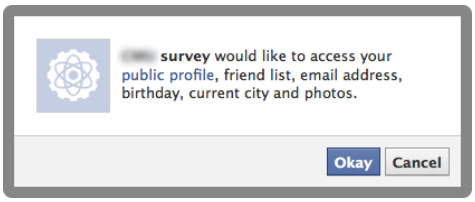

Figure 1: An example of a single sign-on consent dialog.

providers' audit tools, and their sentiment about various aspects of single sign-on. Participants logged in under one of two treatments: a basic treatment, which requested a minimum of personal data; and an invasive treatment, which requested data that most people would find invasive to their privacy.

In summary, our study reveals that several aspects of how user information is handled in single sign-on systems are currently largely opaque to users; users neither understand in detail what information about them is sent by identity providers to service providers, nor do they believe they have control over this process. On the other hand, both self-reported data and users' actions indicate a need for better insight and control—including in some specific, relatively easy to implement ways—and suggest that addressing this need would encourage greater adoption of, and satisfaction with, single sign-on.

We also present a new, alternative design for single sign-on dialogs, PrivacyLens, shown in Figure 3, which uses the recommendations of this study to improve the privacy of users. During this poster session, we would appreciate feedback on the proposed design, and discussion of how to test PrivacyLens.

2. RESULTS

Understanding consent dialogs.

We found participants to be somewhat aware of the range of attributes passed by the identity provider to the service provider, but the factors that affected their awareness were largely not exposed by this experiment. Participants appeared to have a preconceived idea of which attributes would be sent based on the identities of the identity provider and service provider. Their precise understanding of what is sent, and their willingness to log in, was not significantly affected by consent dialogs. Instead, it was affected by their privacy concern level. This suggests that users have already made a decision about whether to log in with the identity provider before viewing the dialogs. However, participants who see a consent dialog alerting them that a larger set of attributes will be sent to the service provider (our invasive conditions) do realize that more attributes are being sent, even if not which ones.

[1]Much of this work was previously published [1]. Supported in part by a grant awarded to the University Corporation for Advanced Internet Development (Internet2) under the sponsorship of the U.S. Department of Commerce, NIST; and by NSF grants CNS0831428, CNS1116934, CCF0917047, and DGE0903659.

[2]http://www.nist.gov/nstic/

[3]http://openid.net

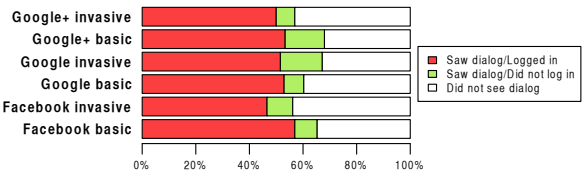

Figure 2: Participants' responses to consent dialogs, per condition.

Login rates per service provider.

There was no statistically significant difference by condition in which participants logged in to our study via an identity provider (Figure 2). Two variables had a significant influence on participants' willingness to click on the "log-in-with" button: the privacy concern level, and familiarity with the identity provider. Remarkably, all factors stop being significant for the decision to log in after seeing the dialog. Since participants could only find out what attributes would be passed to a service provider after examining the consent dialog that popped up during the second decision, this strongly suggests that the knowledge of what information was passed to the service provider did not influence participants' decision about whether to use the log-in-with functionality.

Awareness of transmitted information.

We compared participants' self-reported knowledge of what was sent to what was actually sent. If consent dialogs were effective, we would expect strong correlation between an attribute being shared and participants indicating that it was shared. In general, however, we found that the majority of participants believed that various attributes were not shared even when they were. Since there is little correspondence between actual data being passed and the data participants believed was passed, this suggests that participants simply acknowledged the dialog without examining it, and later made an educated guess about what information was shared.

Trust and willingness to share.

Participants' self-expressed willingness to share specific attributes differed depending on their level of trust in the service provider. Notably, there is a mismatch between participants' comfort level with sharing certain attributes and the sets of attributes that are usually shared. E.g., participants are very uncomfortable sharing their friend lists with a service provider, yet these are always shared. Participants had little insight into the level of access service providers received from identity providers to user attributes. 38% of participants (161 of 424) erroneously thought that the service provider could access the attribute exactly once; 45% (192 of 424) were unsure.

Need for Control.

About half (210 of 424) of participants reported feeling that they had no control over the information passed by an identity provider to the service provider. Only 4.5% (19 of 424) reported that they had "a lot of" control. At the same time, 94% of participants (399 of 424) thought it was "very" or "extremely" important to them to have such control, with another 5% calling it "important." Two thirds of participants (283 of 424) expressed a desire to have some level of control over or insight into which information is sent by an identity provider to a service provider during every transaction between the two.

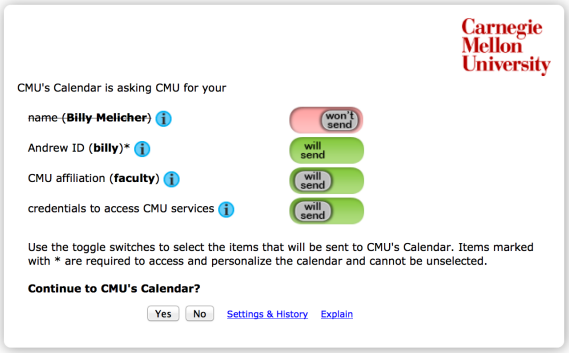

Figure 3: PrivacyLens consent dialog interface.

3. PRIVACYLENS

PrivacyLens attempts to improve the design of single sign-on dialogs based on the results of this study. To better communicate to users what data is being shared, PrivacyLens presents users with human readable information without jargon. PrivacyLens also shows the user only the information is necessary to understand the interaction, but provides additional information when needed. To provide more control to users about what data is sent, PrivacyLens allows users to select what data about them will be shared provided it is not required for the application to function. PrivacyLens also gives users more control by providing an interface to audit previous visits, and control information sent in subsequent visits.

4. CONCLUSIONS

Our results show that participants' understanding of which information is passed to service providers largely was not affected by the consent dialogs shown by identity providers. However, participants did have a general idea of the types of data that can be sent. Few participants saw the dialogs and chose not to proceed with the login, which strongly suggests that this general idea is formed largely before the participant is actually shown the specifics of the information that will be sent. Our participants were unable to recognize what data types were passed from identity providers to service providers during the login process, meaning current consent dialogs which are meant to convey this information are ineffective at doing so. explanation for Our results show significant misalignment between current single sign-on processes and users' expectations and needs. We hope that the results of this study can inform the design of alternative consent dialogs like PrivacyLens.

5. REFERENCES

[1] L. Bauer, C. Bravo-Lillo, E. Fragkaki, and W. Melicher. A Comparison of Users' Perceptions of and Willingness to Use Google, Facebook, and Google+ Single-sign-on Functionality. In *Proc. of ACM DIM Workshop*, 2013.

[2] S. Egelman. My profile is my password, verify me! The privacy/convenience tradeoff of Facebook Connect. Proc. CHI, 2013.

[3] D. Florencio and C. Herley. A large-scale study of web password habits. In *Proc. WWW*, 2007.

[4] S.-T. Sun, E. Pospisil, I. Muslukhov, N. Dindar, K. Hawkey, and K. Beznosov. What makes users refuse web single sign-on? An empirical investigation of OpenID. In *Proc. SOUPS*, 2011.