Proceedings of The National Conference
On Undergraduate Research (NCUR) 2013
University of Wisconsin La Crosse, WI
April 11 – 13, 2013

“Do I know you? – Ask Google”. The single sign-on revolution

Hien Trinh
Marketing and Information Systems
Seattle University
901 12th Avenue
Seattle, WA 98122

Faculty Advisor: Professor Eric Larson

Abstract

Single sign-on is a software system that allows users to log in once and acquire access to multiple independent applications without being asked to log in again at each application. Single sign-on services have been promising to deliver great benefits to the users; however, it also underlines dangerous risks of identity theft and loss of privacy. The advantage of having one single username and password to access all available software programs is so great that it might prevent users from considering what they have to give up for the service. More websites are offering their subscribers the option to sign in with a Facebook account or Gmail account. How do we know that Facebook or Google does not share or sell our information when we allow them to authenticate us online? Internet users need to be careful of identity privacy as many web applications store user information as assets and even sell as goods with little or no notice to the owner. Once the users’ information is available everywhere, it is not private anymore which makes it easier for identity theft to occur. What do applications like Gmail and Facebook do with their single sign-on features to really bring true values to their users? This research will analyze how Google and Facebook are currently implementing single sign-on service, conduct a literature review of current research in the area, collect opinions from professionals in the industry about the topic, and then identifies issues in order to propose and evaluate potential solutions. We hope to aid development of the next generation of single sign-on services, to provide the convenience the users desire and the privacy and security they deserve.

Keyword: Single sign-on service, golden triangle, social graph, IdP (identity provider), SP (service provider)

1. Introduction

On average, one user has to remember five or six passwords if s/he has around 30 accounts. S/he mostly relies on the trial method—trying each password in turn to find the right one—or password reset option to log into an account [1]. At best it will take her/him 20 seconds to log in. However, at worst it can take up to 20 minutes. Moreover, researchers have found that coming up with secured passwords to remember is a very challenging task for all users; therefore, their passwords tend to be weak and can be easily stolen [2].

Acknowledging those weak points and feeling incapable of fixing them, users have been looking for a better way to log in. Single sign-on (SSO) services offered by Facebook and Google simplify the log in process for the users: they can use one username and password registered with Facebook and Google to log into many accounts associated with Facebook or Google. This SSO service certainly solves the efficiency problem of the traditional method mentioned above. It is also offered to users at no monetary cost. As more and more websites adopt SSO service from both Facebook and Google, greater convenience is generated for the users.

This research requires the study of the most recent research on web security and privacy. This includes collecting information directly from Google and Facebook’s websites specifically describing their current implementation of SSO. This research study also examines several social engineering, social psychology, and entrepreneurial marketing topics in order to fully assess the true benefits and pitfalls that SSO service could bring to the users.

Experts in the industry were interviewed to provide more detailed and up-to-date information regarding SSO services. This study concludes with a proposed solution involving a separate control application.

2. Single Sign-on Implementation

Single sign-on (SSO) feature can be explained with a simple model consisting of three components: identity provider (IdP), service provider (SP), and the end user (U), as illustrated in Figure 1.

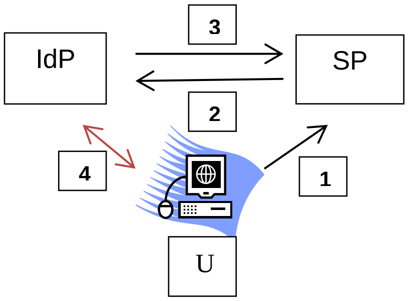


Figure 1: Single Sign-on Model

When a user requests access to an application hosted by the SP, she will be asked to provide username and password (or any other form of user information) to be authenticated (step 1). Her information will then be sent over to the IdP to be checked (step 2). Notice that this model will only work if and only if the user has already had an account registered with the IdP (step 4). Once the IdP receives information from the SP, it will then verify that (a) the information is from the right person, and (b) is correct. If the information satisfies the two conditions, the IdP will respond to the SP indicating it is safe to log her into the SP's system. Moreover, all data transmitted within this model of SSO service is encrypted in order to protect the user's username and password, and to verify that the information transmitted in step 2 actually comes from the SP and the response in step 3 actually comes from the IdP. This three-component relationship established in SSO model is generally referred to as a golden triangle of trust model to emphasize the importance cooperation among the three components.

The current most popular protocol handling the messaging is called SAML (Security Assertion Markup Language). It is an XML-based language; therefore, it can be very flexible, making the transfer of different identity attributes easy. SP and IdP can list as many identity attributes as needed as long as those attributes can be represented in XML [2]. Regardless of SAML benefits and great contributions to SSO feature, it does have flaws: it is an assertion language meaning it is writable, and of course readable; therefore, if someone can intercept the transfer process of the message, he can not only read the message, but also monitor it for his own benefits [3][4]; SAML does not tell IdP and SP who the sender of the message is and, therefore, depends on the encryption and decryption mechanism of both parties and the honesty of both parties [5].

This paper, however, will not focus on SAML flaws or questioning the encryption and decryption mechanism. We will assume that those functions work well enough to maintain security for SSO features, and will instead focus on lower level communication and execution of SSO features by Facebook and Google: how SSO is implemented and commercialized, what the implementation means to the end user, and what improvements can be made.

2.1. Facebook

At the core of Facebook is its social graph consisting of user information, news feeds, wall posts, pictures, and videos [6]. The specific method used to retrieve data out of Facebook's social graph is called Graph API [7], and that is what enhances Facebook's SSO implementation. An example is shown in Figure 2: when a user, Alice, logs into Couchsurfing.com with her Facebook login information (e-mail and password), Couchsurfing.com server will then encrypt the information along with a request for access to some of Alice's Facebook's social graph, and send it to Facebook. Once Facebook receives the packet, it will decrypt it in order to authenticate Alice's login information, and then authorize Couchsurfing.com to retrieve Alice's information on Facebook for its own usage.

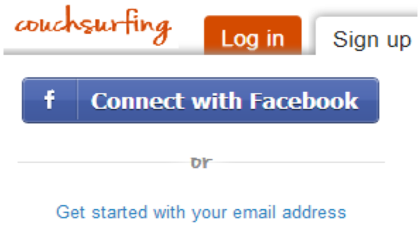
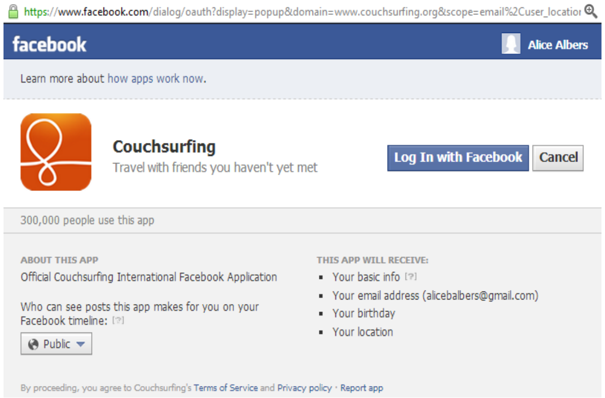


Figure 2: Logging in Couch Surfing for the First Time with Facebook Account

Facebook will not sign Alice's login information to mark that Facebook just authenticates Alice to log into Couchsurfing.com. What it does is that it sends back an encrypted secret token to Couchsurfing.com server which contains all the information of Alice. This secret token is only sent to trusted servers that already registered with Facebook. It is not possible to make Facebook send the token to an unregistered server [3].

Facebook recommends developers to disclose information request form(s) to gain permission(s) from users to retrieve other than their public information [8]. However, there is no information covering the enforcement of this action. If the website is honest, like Couchsurfing.com, they will show the user a confirmation window listing specific pieces of information Couchsurfing.com will have access to (Figure 3).


https://www.facebook.com/dialog/oauth?display=popup&domain=www.couchsurfing.org&scope=email%2Cuser_locatior

facebook

Alice Albers

Learn more about how apps work now.

Couchsurfing

Travel with friends you haven't yet met

300,000 people use this app

ABOUT THIS APP

Official Couchsurfing International Facebook Application

Who can see posts this app makes for you on your Facebook timeline: [?]

Public

THIS APP WILL RECEIVE:

- Your basic info [?]
- Your email address (alicebalbers@gmail.com)
- Your birthday
- Your location

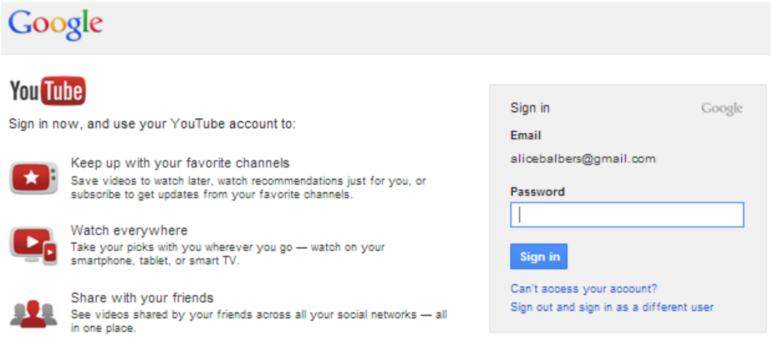
By proceeding, you agree to Couchsurfing's Terms of Service and Privacy policy · Report app

Figure 3: Alice logs into Couchsurfing.com and receives pop-up notification

For a website to implement Facebook's SSO feature on their server, there are guides and even code available on Facebook Developers [9]. It is free of charge to use and to implement the feature. Facebook will only ask the server to agree to its Facebook platform policies [10].

2.2. Google

Google's approach to SSO implementation is slightly different than Facebook's. All Google's applications (Gmail, Google Calendar, Google Drive, YouTube, etc.) are accessible through one single Gmail address. Looking back to the point when a user starts registering for a Gmail account, we see that Google only requires user to provide first name, last name, date of birth, and gender. A user might think that is all Google knows about her. However, since she uses her Gmail address to log into all of her Google Apps, it is quite easy for Google to track her activities and knows more about her. For example: Alice logs into Youtube.com with her Gmail address allowing Google to gain access to her viewing patterns on YouTube (Figure 4).



Sign in now, and use your YouTube account to:

Keep up with your favorite channels
Save videos to watch later, watch recommendations just for you, or subscribe to get updates from your favorite channels.

Watch everywhere
Take your picks with you wherever you go — watch on your smartphone, tablet, or smart TV.

Share with your friends
See videos shared by your friends across all your social networks — all in one place.

Sign in

Email: alicebalbers@gmail.com

Password:

Google
Sign in
Can't access your account?
Sign out and sign in as a different user

Figure 4: Alice logs into YouTube.com

Regardless of the similarity that both Google and Facebook have very good knowledge about their users, Google is different than Facebook because their SSO implementation only authenticates users to access certain applications, but not authorizes applications to retrieve any more than the users' very basic information for their own usages. When Alice logs into Foxnews.com with her Gmail address, Alice's information will be sent over to Google to authenticate. What Google does every time Alice tries to log into Foxnews.com is signing off Alice's provided to Foxnews.com and telling Foxnews.com that Alice provided the news server with correct identity information [3].

Google's SSO implementation is also available for any developers for free of charge on Google Developers site [11]. If developers do not want to host or design the application themselves, Google will help them do that with charges according to the amount of space the application takes up on their server [12].

3. Benefits of Facebook and Google Single Sign-on Implementation

SSO is absolutely not a brand new idea. Its first appearance was actually around late 1990s and early 2000s – the dot com era [14]. Even though we are not sure whether the booming of internet services is the force that help developed SSO service, we know that it certainly did nothing to help the service grow. An example is Microsoft Passport. The idea was to use one single Windows Live ID to access all Microsoft web commerce sites as well as any other participating sites. People turned away from the idea because it was found to give Microsoft full access to all user information [15]. Therefore, Microsoft Passport did not do so well in the dot com era, and even in today's market (Microsoft Passport still exists in today's market under the name Windows Live ID). So what have Facebook and Google been doing to be leading players in today's SSO service industry? What could they convince users and SPs about SSO that make the adoption of SSO easier?

3.1. Facebook

Marketing and customer relationship management (CRM) are key focuses for every business nowadays [18]. The cost of the initial CRM software can be up to $3.5 billion to run per year [16]. For small- and medium-size companies, that is an unaffordable amount of money. Therefore, for those companies, adopting SSO service leaves them more room to better allocating their financial resources.

One billion active users [17] on Facebook are definitely a great market size to offset any cost associated with adopting Facebook SSO service [14]. The economy of scale that Facebook achieved has brought confidence to all of their potential SSO service customers. Once the businesses sign up to integrate Facebook SSO service into their system, the access to user information that Facebook provides ultimately means a lot more. But what exactly does it mean?

Businesses then can retrieve user information much faster, easier, and in variety of forms, such as: photos, videos, likes, news feeds, status posts, etc. With that information, almost all strategic marketing questions are answered, for example: "Who are our customers?", "What do they like?", "What did they do yesterday?", "How likely will they make a repeat purchase with our company?", etc. How much does it cost Facebook customers for those answers? Does it cost them $3.5 billion a year? The answer is obviously no. As of right now, Facebook does not imply any fee on their SSO service. Therefore, developers choosing to implement Facebook SSO system are looking at a very cost effective option.

It is even more convincing for companies to adopt Facebook SSO service when they acknowledge that the end users, their customers, are actually enjoying the convenience of the service [13]. Both buyers and sellers are happy. The interesting point is that they all voluntarily participate in one simple trust relationship. Therefore, as long as their trust remains strongly with the other party, everyone will win.

3.2. Google

Google has a fairly different approach compared to Facebook's and focuses on one of their key assets: cloud computing. As discussed in section **2.2.**, Google only signs to authenticate user information rather than focusing on providing additional user information back to SPs, SPs have a totally different set of reasons to choose Google SSO service. Let's look at an example to explain the benefits of Google SSO service easier: Khan Academy is a well-known website for educational lecture videos. Their user base just gets bigger and bigger, currently reaching 3.5 million visits every month [19]. They could not afford the large servers necessary to be able to support their growing business. After evaluating different solutions, Khan Academy decided to do business with Google. As a result, Khan Academy now has a Google App, a full ability to support 3.8 million unique visits each month, and a system that easily handles usage surges, including Google SSO service [20]. How? All of Khan Academy's data can now be stored on Google's servers for operation and maintenance [20].

Through the example, it is easy to acknowledge that SPs decide to adopt Google SSO service to take advantage of Google cloud based services: Google App Engine, Google server, Google Analytics, etc. The ultimate benefit here is not access to user information; it is ease of operation and maintenance. "The Khan Academy provides individual profiles to students so they can analyze their learning progress, which means the organization needs systems running in the background to collect and track of all this data. Because Google App Engine takes care of server support, the Khan Academy's five developers can spend almost all of their time improving site functionality." [20]

Google's customers do not have great access to individual user information like Facebook's customers. However, some businesses that value operation and maintenance over getting a lot of user information for market research will ultimately consider Google SSO service over Facebook. Facebook, with 1 billion users and 80% of them are from Canada and the United States, definitely has an advantage in terms of number of users [17]. However, Google's 425 million users is not a small number for a profitable market base [21]. Besides, both services still offer then end users the convenience they desire; therefore, Google's or Facebook's, in this case, does not matter much.

4. Issues of Facebook and Google Single Sign-on Implementation

Often when people think of SSO service issues, they think there is something wrong with the technology and question its ability to deliver what it ought to. There are numerous studies done by professors at universities, MBA students, and researchers at Microsoft specifically examining the security of SSO service provided by Google and Facebook. We certainly cannot deny their effort in pushing the current technology to the next level; however, we cannot deny also issues with the fundamental framework of SSO service.

As findings in the research paper called "A Billion Keys, but Few Locks: The Crisis of Web Single Sign-On" [13] by a group of professors from University of British Columbia suggested, if the SSO triangle framework is broken, there will not be any SSO service. Therefore, companies like Google and Facebook should allocate effort and resources to address issues relating to the golden triangle of trust. The issue is rarely technology as the technology is usually there already [14]. Instead, the trick is how to communicate its benefits to the users and trigger a change in behavior.

To further explain the issues, in this section, we will talk about potential backsplash from SPs, and more important, how the slow adoption of the end users has impaired SSO service growth and improvement for long term sustainability, based on the focus group research findings from the research paper mentioned above.

In addition we will also discuss the potential fourth component added into the golden SSO triangle: government regulation. What we are interested in this component is its influence on the golden triangle framework that is already established. We will also try to answer the question of whether this additional piece will provide more force to elevate SSO infrastructure to a higher level, or restrict the rapid growth of the structure.

4.1 SPs' Backlash

SSO service changes the dynamic of identity management, and eventually, customer relationship management. Even though most SPs enjoy lower cost and quick access to customer information (as a result of Facebook's SSO service), or lower cost and convenient operation management (as a result of Google's SSO service), some might argue for the right to store customer information, and some might argue for the confidence of user's security, usage ability [13].

Small- and medium-sized SPs might be able to work with the limited right to storing user information. However, bigger players, for example, financial institutions, will not consider SSO service unless they can have strict and complete control over the user information available to them. It is mostly in regard of the SPs' interest to avoid SSO service; however, it is also partly according to those SPs' users' interest [13] (which will be discussed in further details in 4.2.).

Since the authentication and maintaining of user information functions have been "out-sourced" to the IdPs in SSO model, the ability to authenticate and manage customer information is no longer in the control of SPs. Therefore, some SPs refer to SSO service as an event where IdPs' actions' costs are paid by SPs [13]. For example: Bank of America (BOA) adopts Google SSO service for their online banking service which allows consumers that bank with BOA to log into their bank account with their Google identification information. One day Google fails to log a consumer into his or her bank account, when he or she really needs to make a payment online otherwise the account will be charged for over-drafting. BOA charges the consumer the fee without knowing the circumstance. The consumer will not come to Google to file complaints, or to argue for his or her money back. He or she will come to BOA, and expect them to be the one that is fully responsible for the incident.

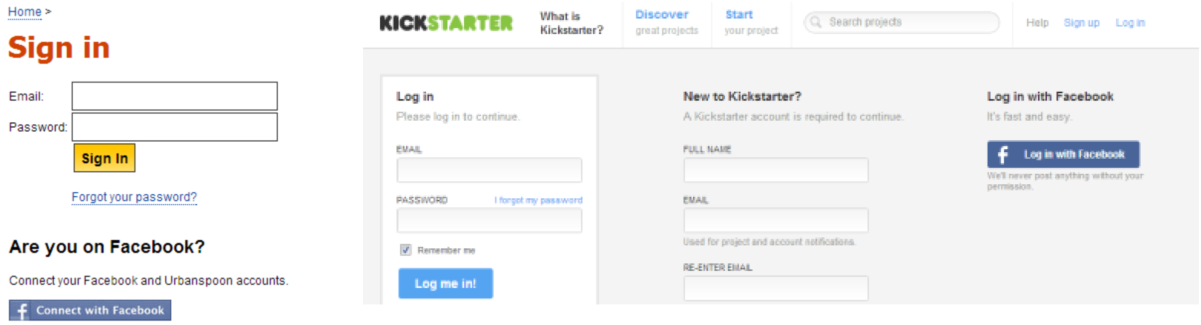
Furthermore, SSO service from Google and Facebook (or any other SSO service providers) does not seem to provide any attractive incentives to encourage the adaptation of SSO by institutional organizations [13]. It might make more sense when we think of it in the following example: Yelp and Urban Spoon are considered competitors for user-review based websites. Yelp offers their customers the choice to log into their websites using Facebook account information. Of course having the ability to use Facebook account information for many websites is convenient for the customers; however, customers will not simply choose Yelp over Urban Spoon because they can use their Facebook account with Yelp. Facebook SSO service is not aiding Yelp's competitive advantage, at least not to the level that will make a difference in their customers' decision.

4.2. The End User's Hesitation To Adopt SSO Service

The third component of the SSO service golden triangle, end users, is considered the most complicated, important, and unpredictable. End users are extremely complicated because they are human beings. They are not machines; therefore, they do not act in the same way that researchers think they all should in certain circumstances. If researchers do not study end users precisely, critical patterns might be missed affecting the reliability of the research result. Moreover, researchers have to take in account the unpredictability of the end users: end users'—human beings'—behavior patterns can be twisted dramatically by emotions, mood, and physical health [28]. Thus in order to be successful, SSO service providers should take a close look at what is at stake for the end users' so that they can act accordingly without bearing high costs of being rejected.

One of the most obvious patterns in the end users' behaviors—in response to the introduction of SSO service—is the hesitation to change. Many people are comfortable with the features their web browsers offer: remembering username and password—sometime, automatic log-in as well. They do not think that they need SSO service, not right at this moment because their current systems still work well—why even bother to get a new one and start learning to be comfortable with it? Beside the fact that SSO service is somewhat convenient, is it significantly better that it can convince people to change from their behavioral or comfortable way of doing things to SSO service?

The first pattern is about the end users' confusion of SSO service interface on different SPs' websites in different circumstances [13]. Using the two examples: Urbanspoon.com and Kickstarter.com, it is not hard to see that there is not a common presentation of Facebook SSO service interface on different websites (Figure 5).



Connect your Facebook and Urbanspoon accounts.

Please log in to continue.

A Kickstarter account is required to continue.

Used for project and account notifications.

It's fast and easy.

We'll never post anything without your permission.

Figure 5: Using Facebook to log in to UrbanSpoon.com and Kickstarter.com

When users click on the Facebook icon, however, the log in interface looks the same. This experience is consistent across web browser and across different computers. Yet it will be different if the user is using a web browser, and already logged into Facebook in one tab. Then when the user wants to use Facebook account information to log into UrbanSpoon.com, he or she will see a notification instead of a log in interface (similarly illustrated in Figure 3). Some might argue that the differences here are not significant enough to confuse users. It is true that some users will not find it confusing. At the same time, it is also true to say that majority of user will find it confusing [13].

The second pattern issue raises concern for high risk of phishing attack. Taking advantage of the inconsistency of Facebook SSO service presentation, one can create a semi-functional website that looks exactly the same as Urbanspoon.com, but with fake Facebook SSO log in interface. Careless users will likely put in their information and get them “stolen”.

The third pattern is about the end users’ discomfort feeling of being watched or being stalked. It happens to both Facebook and Google SSO service end users: the user logs into a SP’s website using his or her Facebook or Google account information, and then consumes the service provided. Later on the user sees online ads about the specific service that he or she used everywhere he or she visits on his or her own Facebook wall, Google search, everywhere on the internet essentially. S/he considers this activity private information that should not be shared, let alone used for commercial purposes. Is privacy the price users have to pay for their free access to the IdPs’ services as well as the SPs’ services? Do users have to sacrifice the need to preserve their privacy to gain the benefits they wish for? These are questions everyone knows the answers for; however, not all answers agree with one another. Maybe the ultimate question to ask is that is it intrinsically wrong to monitor someone’s activity—i.e., knowing what the monitored target does but not doing anything to harm him or her [22]?

4.4. Addressing Issues Regarding SSO Service

The easiest step IdPs can do to make the benefits of SSO services more prominent is educating not only SPs at the business level, but also the end users at the consumer level. By emphasizing the benefits of SSO services, IdPs might encourage the migration of SPs and the end users from traditional username-password authenticating mechanism to SSO service [23]. This solution might seem too easy to be helpful. However, when we think of IdPs’ power to deliver good SSO services, we cannot leave their ability to network with SPs, and the end users out of the thinking process. Because IdPs are IdPs due to the great amount of end users registered with them, and if IdPs can connect with good SPs, more users will be likely to register with IdPs, driving the potential growth of their SSO services—more users, more power.

Moreover, IdPs also needs to emphasize the golden triangle of SSO model—becoming a trust agent, and potentially a love agent who consumers and SPs will voluntarily cooperate with to help IdP grow (they even sometimes protect IdP against strategic fall) [24]. IdPs need to become familiar to the end users as a super nerd they can trust, to SPs as a great business partner they can rely on. It is critical that IdPs think and act that way because, as we have learnt in the past, many services were not successful due to the lack of trust and communication between partners, not due to low quality product or service [24].

Once IdPs implement these two suggestions and do it well, the end users’ issues will be resolved—maybe not to the perfect extent, but definitely enough to scrape away users’ confusion, and shake up the loyalty of users to the traditional authentication mechanism. How about the end users’ worries of their privacy being violated? What can

IdPs do about that? What is a fair balance between maintaining the privacy – the right – of internet users, while not forcing IdP to become valueless to SP's?

It is quite hard to generalize the level of privacy each user values. Yet there is no argument against the users acting protectively toward their privacy—however it is defined by the users. Thus IdPs should have flexible service offers that allow users to customize accordingly to the level of privacy they can tolerate. Perhaps, IdPs are already aware of this solution, but have not executed it. Either way being helpful and up front with the end user will bring IdPs closer to becoming a trust agent, and the benefits of being a trust agent will outweigh any other benefits received from—for example—doing the opposite: lying to the users and damage their trust by selling information they valued to another party without their consent.

5. Solution/Recommendation

Acknowledging most of the managerial, theoretical problems and addressing them is only one step toward finding out what should be next. Below is a detailed presentation of a theoretical model in attempt to take one step further and actually create a genuine system to capture all the benefits that SSO service can have and potentially will have, while preserving the needs of the end users.

The idea is to create a control application on users' personal devices that looks similar to Skype or Yahoo Messenger (Figure 6). This control application is provided by IdPs and can be downloaded from the IdPs' website. What it does is that it stores all the personal information the user put into it locally on the his or her personal device, and only when he or she wants it to—or whenever he or she is online, it will upload those information to the IdP's server allowing the server to authenticate he or she across the web.

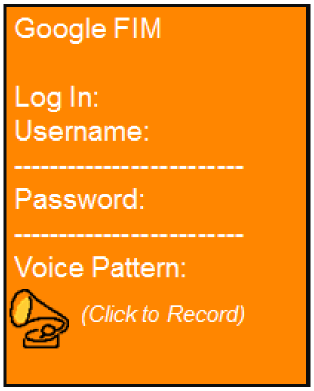
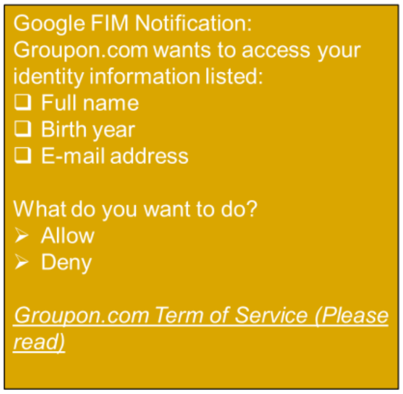


Figure 6: Control Application Interface

For example, the user did all the steps described above and then accessed Groupon.com from any of his or her browser. What he or she will see is simply a link saying that: "One-click log in with X", as X here is the SSO service provider of the user. When he or she clicks the link, Groupon.com will generate a notification saying that this IP Address is trying to use "One-click log in with X" and send it to X's server. Since X's server is already communicating with the user's control application, it knows what the user's IP Address is, and therefore being able to identify specific user it needs to authenticate. Hence, all X needs to do then is reply to Groupon.com with something like this: "Hey Groupon.com, I do know that IP Address, what do you need me to provide in order to authenticate it?" Once received, Groupon.com will send over a list containing the pieces of information it requires. X's server, then, will communicate Groupon.com's requirement to the user through the control application. What the user sees is illustrated in Figure 7. Accordingly, if the user picks yes, X's server will send over to Groupon.com all the information it listed and authenticate the user.

In addition, when the users are offline or just simply do not want to use SSO service, they can just change the option in the control application and tell it to stop syncing. Then all of the users' information stored on the IdP's server will be downloaded onto the users' personal devices and deleted from the server. While staying in synced, the control application and the users' devices work on a two-way communication system (Figure 7) allowing users to engage in the decision making process of SSO service.



Google FIM Notification:
Groupon.com wants to access your identity information listed:

- □ Full name
- □ Birth year
- □ E-mail address

What do you want to do?

- ➢ Allow
- ➢ Deny

Groupon.com Term of Service (Please read)

Figure 7: Notification Message from the Control Application on the user's desktop

The model also allows users to enjoy the ease of authentication on public computers. He or she can log into the IdP's website and use an online version of the control application instead. The online version will look the same and function similarly to the one installed on the user's personal device.

This model is, anyhow, not perfect. It still heavily relies on the use of username and password—therefore, still bear the risk of being stolen, requires extra effort in consuming SSO service, and might increase the risk of personal device theft. It is useful though in ways that capture benefits of SSO service while preserving the needs of the end users: users have more control over the transaction or communication between IdP and SP. Besides, those shortcomings can easily be filled to enhance the functionality of the model.

First, username and password can now be aided by key card, voice pattern, or even finger print. Therefore, instead of combination of only username and password, users can choose to put on their accounts more protection. By doing this, it will decrease the probability of an account being stolen because of lost username and password. Second, educating users will not be a problem blocking the adaptation of this model because in order be successful with the SSO service idea alone. IdPs have to actively educate users already. In other words, teaching users to implement this model will not be hard, if IdPs are successful in telling the story of SSO services. Third, in case of stolen personal device, users can still be protected. They can log into the IdP's website and report a loss, then ask the IdP to withdraw all saved personal information stored on the devices.

6. Conclusion

One single user will not stop and limit the number of website or application s/he wants to gain access to, especially in today's world where the Internet is becoming more and more popular in many aspects of a human life. Thus, five or six passwords will not be able to do any good to the user then i.e. they are not secured enough to protect user information from the harmful profiteers. In that case, SSO model seems to be a great option for any user to adopt. However, not everything can be moved into the Internet in a day or two, changes are not happening overnight. In addition, SSO service providers like Google and Facebook are not educating the users about the necessity of their products. Therefore, not many users are either aware of their potential need to be safe online in the future, or feeling the urge to change their method of logging into website and application on the Internet.

Besides, the SSO model though has not been charged with having any technical problem that challenges its ability to securely deliver what it promises to the users. The questionable aspect of the model, therefore, lies on its trustworthiness to respect its users' privacy. Facebook and Google have certainly not been good communicators to their users. Information transmitted between Facebook or Google and any website is not submitted to be shared with the users. Are Facebook and Google doing the right thing? Do users not have the right to know how the information they have given to Facebook and Google being used?

The proposed solutions are limited in term of their scope, as well as their infrastructure i.e. they are not the one solution that will fix all the problems for everyone. However, if one is highly interested in the potential of SSO model and their privacy online, these solutions might be highly relevant. Someone paying a lot of attention to the question for government about their ability or duty to protect online users against any potential harm can also gain useful knowledge from the solutions. Adding a fourth component, i.e. the government, into the golden triangle of trust might not be the only answer to all issues related to SSO model.

7. References

[1] Dinei Florencio, Cormac Herley (2007), “A Large-Scale Study of Web Password Habits,” http://research.microsoft.com/pubs/74164/www2007.pdf, 16th International Conference on World Wide Web 2007.
[2] Ping Identity (2013), “SAML Tutorial and Resources,” https://www.pingidentity.com/resource-center/SAML-Tutorials-and-Resources.cfm.
[3] Rui Wang, Shuo Chen, XiaoFeng Wang (2012), “Signing Me onto Your Accounts through Facebook and Google: a Traffic-Guided Security Study of Commercially Deployed Single-Sign-On Web Services,” http://www.informatics.indiana.edu/xw7/papers/websso.pdf, IEEE Symposium on Security and Privacy May 2012.
[4] Thomas Groß (2003), "Security analysis of the SAML single sign-on browser/artifact profile," ACSAC 2003.
[5] Alessandro Armando, Roberto Carbone, Luca Compagna, Jorge Cuéllar, Giancarlo Pellegrino, Alessandro Sorniotti (2012), “An authentication flaw in browser-based Single Sign-On protocols: Impact and remediations,” Computer & Security journal, Volume 33, pages 41-58, ISSN 0167-4048, 10.1016/j.cose.2012.08.007, http://www.sciencedirect.com/science/article/pii/S0167404812001356.
[6] Facebook Developers (2013), “Open Graph Overview,” https://developers.facebook.com/docs/concepts/opengraph/overview/.
[7] Facebook Developers (2013), “Getting Started: The Graph API,” https://developers.facebook.com/docs/getting-started/graphapi/.
[8] Facebook Developers (2013), “Facebook Platform Policies: policy,” https://developers.facebook.com/policy/.
[9] Facebook Developers (2013), “Platform & Developer Support,” https://www.facebook.com/help/224125207600132/.
[10] Facebook Developers (2013). Facebook Platform Policies: Introduction and principles. https://developers.facebook.com/policy/.
[11] Google Developers (2013), “Google Apps Marketplace Developer’s Overview,” https://developers.google.com/google-apps/marketplace/.
[12] Google Developers (2013), “Single Sign-On,” https://developers.google.com/google-apps/marketplace/sso?hl=en.
[13] San-Tsai Sun, Yazan Boshmaf, Kirstie Hawkey, Konstantin Beznosov (2010), “A billion keys, but few locks: the crisis of web single sign-on,” (pages 61-720, Proceedings of the 2010 workshop on New Security Paradigms.
[14] Avijit Sinha (2013). Personal communication.
[15] Wikipedia (9 January, 2013). Microsoft Account. http://en.wikipedia.org/wiki/Microsoft_account
[16] Manuel Ebner, Arthur Hu, Daniel Levitt, and Jim McCrory (December, 2002). How to rescue CRM. http://www.mckinseyquarterly.com/Business_Technology/Application_Management/How_to_rescue_CRM_1254
[17] Facebook (2013), “Key Facts,” http://newsroom.fb.com/Key-Facts.
[18]Schindehutte, M., Morris, M., and Pitt, L. (2009) *Rethinking Marketing.* Upper Saddle River, New Jersey: Pearson.
[19] Rim Empson (19 October, 2011). Khan Academy Triples Unique Users To 3.5 Million. http://techcrunch.com/2011/10/19/khan-academy-triples-unique-users-to-3-5-million/
[20] Google (2011). The Khan Academy Scales and Simplifies with Google App Engine. https://cloud.google.com/files/KhanAcademy.pdf (page number)
[21] Dante D’Ozario (28 June, 2012). Gmail now has 425 million active users. http://www.theverge.com/2012/6/28/3123643/gmail-425-million-total-users
[22] Marc Cohen (2013). Personal communication.
[23] Sun, S., Pospisil, E., Muslukhov, I., Dindar, N., Hawkey, K., and Beznosov, K. (2001), “What makes users refuse web single sign-on?: an empirical investigation of OpenID,” http://cups.cs.cmu.edu/soups/2011/proceedings/a4_Sun.pdf, proceedings of the Seventh Symposium on Usable Privacy and Security (Article 4).
[24] David C. Wyld (May 9, 2010), Summary and Review of Trust Agent by Chris Brogan and Julien Smith, http://bookstove.com/book-talk/summary-and-review-of-trust-agents-by-chris-brogan-and-julien-smith/.