Examining the Privacy of Login Credentials Using Web-Based Single Sign-On: Are We Giving up Security and Privacy for Convenience?

Charles Scott, Devin Wynne, and Chutima Boonthum-Denecke
Department of Computer Science
Hampton University
Hampton, VA USA
{charles.c.scott26@gmail.com, devin.m.wynne@gmail.com, chutima.boonthum@hamptonu.edu}

***Abstract*— There is a drastic increase in the amount of individuals that have access to the World Wide Web in order to complete daily tasks. Many of these tasks include keeping up with friends by using social media, checking bank account statements, and transferring files to colleagues all over the world. This ubiquitous tool has virtually revolutionized our entire daily life activities, as we know it. With the introduction of mobile smartphones and other digital advancements, a number of debates have been raised regarding security and privacy issues. A number of which have seamlessly stemmed from the trade-offs between privacy and convenience. With the boom of web services and social media, Web-based Single Sign-On (SSO) schemes are being deployed and used by individuals all over the world. This raises concerns that could potentially allow users to give up on their privacy and security personal credentials for convenience. This paper will take a look into the popular Web-based SSO system security posture. A survey was conducted in order to examine the usage and understanding of individuals utilizing these convenient and precarious schemes. The use of this study will ultimately aid in answering the underlying question: are we as a society slowly giving up security and privacy for convenience?**

Keywords—Privacy; Security, Web-based Single Sign-On

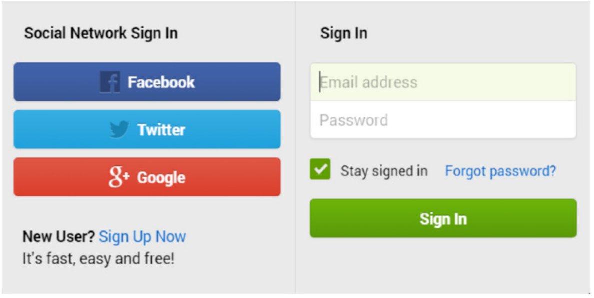
I. Introduction

A Single Sign-On (SSO) is an authentication process that allows a user to authenticate only once with one credential and then have access all authorized resources and multiple applications within an enterprise [1, 2]. Web-based Single Sign-Ons (SSOs) are becoming a regular used technique to allow users to easily register and sign-in to websites with the use of social media accounts (Shown in Fig. 1). These websites can be associated with new applications downloaded from Apple's App Store, Android's Google Play store, or even accessing website accounts like at The New York Times. A typical web user has about twenty-five accounts that require passwords, and enters about eight passwords per day [3]. Additionally, many users are suffering from "password fatigue," which is the burden regular web-users face when managing an increase amount of accounts and passwords [4]. The described examples play a pivotal role in the use of Web-based SSOs because just about all users are utilizing this tool. In fact, Blue Research, a top market research firm estimates that about 66% of web users prefer Web-based SSO to be offered by websites and applications [5]. This percentage is proof to user experience (UX) developers, industry, and users that Web-based SSO schemes will continue to be utilized in the future. The push of Web-based SSO tools is deriving from the leading web technology companies that web users are familiar with which include: Facebook, Google, Twitter, PayPal, and Yahoo. All of these companies offer Web-based SSO services to relieve users of the burden of registering for many online accounts and remembering passwords.

With the rise of these tools and its convenience, there have been a number of security vulnerabilities that are associated with the scheme. This may include credential transactions between the Relaying Party (RP) and the Identity Provider Account (IdP), or using phishing schemes associated with the use of Web-based SSOs. Like any authentication scheme, their number one mission is to prevent unauthorized parties from gaining access to a user's account. Web-based SSOs should not be different.

As we become more dependent on computational tasks and its information associated with web technologies, it becomes increasingly important to protect authentication flaws. Additionally, as organizations move toward cloud-based products, criminals will potentially have more access to critical information related to its users or the company itself. The conveniences offered by Web-based SSOs are just the beginning of authentication flaws that could expose critical personal assets to the unwanted individuals.

Fig. 1. Example of Web-based Single Sign-On Page



In this paper we will take a look into the Web-based SSO implementation and its security vulnerabilities that may be associated. The research will aim to understand a modern users' point of views as it relates to these technology schemes. Ultimately the paper will seek to tackle issues associated with the trade-offs between the advancement of convenience technologies to a user's security and privacy desires.

A. *Motivation*

The motivation behind this research stems from the ease of advanced technologies to lift the tensions off every day human tasks. Technology has enabled new levels of convenience at home, in the office, and any and everywhere we can think of. The notion of "always-on, always connected" drives the technology of convenience for almost every individual in an industrialized country [6]. As we become more reliant on these technologies there are many trade-offs that may come with it. Some of these huge trade-offs could include an individual's privacy and security. Convenience and security is not a cut and dry choice but can be considered a sliding scale that requires finding the right balance between the two [7].

A simple example that will guide us into our case study is the issue of strong passwords. Strong password security causes almost as many problems as it solves [7]. Most users understand that a complex password provides for better protection but many are too lazy to come up with one. Complex passwords tend to lead to more users locking themselves out of their own accounts, or finding ways to undermine password policy and choose easily cracked passwords in spite of the rules [7]. In order to counter these issues developers have created a commercially adopted scheme to allow users to register and sign-in to online accounts by using their social media accounts. Web-based Single Sign-On has been extremely effective for many years as users no longer have the burden of completing registrations for new accounts. Janrain, a customer identity management company, also has determined that when a user forgets their username or password about 90% admit leaving the website [8].

The research additionally explains that 41% of users prefer the use of social login while 35% wouldn't mind creating a new account and 24% would use a guest account [8]. It is estimated that the percentage of social login use has increased dramatically with the boom of more social media accounts over the past couple of years. Since this is a scheme that is clearly here to stay, this research wants to understand if users are aware of the type of technologies they are submitting themselves to. If they are aware of the vulnerabilities that can be associated with Web-based SSO: what's causing them to continue their use? If users are willing to give up their security and privacy (i.e. user credentials and personal information) for Web-based SSO convenience schemes, what else as a society are we willing to give up in the future? These highlighted questions and more will be addressed in the following surveyed research.

II. WEB-BASED SSO SECURITY VULNERABILITIES

In order to discuss Web-based SSO and its vulnerabilities, the tool must be broken down and understood. The security framework behind these tools faces a critical challenge because commercially deployed SSO systems typically neither publish detailed specifications for their operations nor have their code of the RP and IdP sides accessible to the public [9].

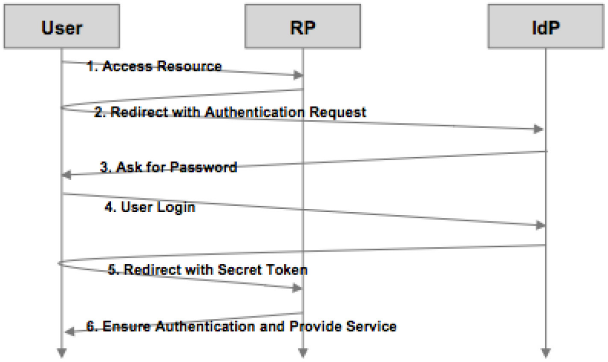
A related research paper by representatives from Indiana University Bloomington and Microsoft conduct a security analysis of this tool by using what is left to public users. Given the limited data associated, researchers are able to study the web traffic behind Web-based SSO's that take place through a web browser. These interactions involve 3 main parties, which include: Commercial Identity Providers (IdP), Relying Parties (RP), and the Browser/User. The traffic involved between these three main parties is critical to the understanding of how Web-based SSO's operate (shown in Fig. 2). Additionally, these interactions are the beginning stages of how vulnerabilities may be associated with this widely used tool.

During the transaction, Web-based SSO's are primarily built upon the relying party (RP) integration of the web application program interface (API) exposed by the IdP [9]. While using these APIs, the RP virtually redirects the browser to the IdP to authenticate the user when s/he attempts to log in. After succeeding, the browser is given either a secret token or a certified token for directly signing into the relaying party. Essentially the SSO process is for an IdP to convince an RP that because this browser has signed onto the IdP as Alice, the same browser is now granted the capability to sign onto the RP as Alice [9]. This communication between HTTP responses and exchanging of tokens can be called Browser-Relayed Message (BRM) [10]. Another associated tool used during these transactions includes OpenID. OpenID is an open and promising user-centric Web-based SSO solution [11]. The OpenID foundation estimates that there are more than one billion OpenID-enabled user accounts provided well-known service providers like Google, Yahoo, and AOL [11]. It is repeatedly discussed in related research that this process is riddled with logic flaws [9, 11, 12]. These logic flaws can allow a malicious user to be able to log into a user account or even steal personal data ranging from email addresses, birthdate, and contact lists [10].

A. *Phishing Attacks*

Web-based SSO's are continually increasing in use each and every day. Due to this wide spread of adoption the tool must be criticized from a security standpoint. Research has suggested a number of logic and phishing flaws that can be

Fig. 2. Web-based SSO Traffic Analysis [9].


User
RP
IdP
1. Access Resource
2. Redirect with Authentication Request
3. Ask for Password
4. User Login
5. Redirect with Secret Token
6. Ensure Authentication and Provide Service

associated with this tool if they are not properly implemented or used effectively. Chuan Yue from the University of Colorado Springs conducted a study on the idea behind how Web-based SSO's can be used in phishing attacks [13]. It is stated that Web-based SSO's can be spoofed with ease to even trick regular web users who are familiar with the idea of phishing attacks. The study explains that the spoofed login page deceived 61% of the surveyed participants who have heard about phishing. Additionally, the survey also concluded that 71% of the participants answered yes regarding if the fake Facebook or Gmail login page was genuine or not [13]. The paper explains that a collective solution must be thought of between the IdP, RP, browser, and especially the users. A briefly discussed resolution involves a two-step authentication approach, which ultimately can mitigate the risk of phishing attacks but does not prevent or detect it [13].

B. BRM Traffic Analysis Vulnerability

As we can see, user aspect plays a critical role in the underlying security implementation of Web-based SSO's. It is also studied that the actual transactions commercially deployed by Web-based SSO's are susceptible to attacks. These transactions are associated with the Browser Relayed Message (BRM) process. Researchers from Indiana University Bloomington and Microsoft studied cases focused on the actual web traffic going through the browser. Within their research they used an algorithm to recover important semantic data and identified potential exploit opportunities. The concluded research discovered serious logic flaws in well-known ID providers and relying party websites such as Google ID, Facebook, JanRain, PayPal Access, Freelancer, FarmVille, and Sears.com. [9].

The discovered logic flaws allow an attacker to sign-in as a victim user. To complete their study, the researchers developed a "BRM analyzer" to perform a black-box, differential analysis on BRM traces associated with Web-based SSO's transactions. The in-house developed analyzer was used to capture and parse BRM and then further modify and replay HTTP requests. In an event that HTTP messages were involved, they also utilized Fiddler, a web proxy capable of uncompressing and parsing HTTP messages. In addition, they also utilized FireFox's debugging tool, firebug, to modify and replay browser requests [9]. The elaborate steps shown in this study exemplify serious logic flaws in Web-based SSO's, which can be discovered from browser-relayed messages and exploited by an attacker without access to source code or other insider knowledge of the systems.

All of the logic flaws were discovered through three-part mechanical procedures which consist of the following: 1) understand whether the SSO is based on a secret token or an authentic token; 2) locate the token in BRMs and understand how it is propagated or how it is covered by a signature; and 3) apply adversary scenarios to BRMs using a developed table set of three strategies – Bob acting as another client, Bob acting as another RP and Bob acting as a page in Alice's client [9]. The research expresses those developers of today's Web-based SSO systems fail to fully understand the security implications during token exchange, specifically, how to ensure that the token is well protected and correctly verified [9]. Although researchers have reported some flaws in Web-based SSO's, they explain that there are plenty others that this study cannot cover. The BRM analyzer tool is available to the public to allow developers and security analysts to conduct investigations similar to the ones conducted in the paper.

C. Covert Redirect

Another serious vulnerability that can be associated with Web-based SSO's involves the use of login standards OAuth and OpenID, founded by Wang Jing, a PhD student at the Nanyang Technological University in Singapore. Symantec defines OAuth as an open protocol to allow secure authorization from web, mobile, and desktop applications [14]. This vulnerability is known as the "Covert Redirect" and is loosely derived from the existing Open Direct vulnerability [15]. The open direct is an application that takes a parameter and redirects a user to the parameter value without any validation [16].

The covert redirect is very similar to an open redirect however it is preceded by a normal redirect from the Website to a partner that is exposed to Open Redirect attacks. A covert redirect vulnerability exists because of the website overconfidence in its partners, consequently giving leeway to the attacks [15]. In order for this flaw to be exploited, it requires interaction from web users [14]. A user would physically have to grant permissions to a susceptible application in order for the access token to be compromised [14]. Only then can an attacker obtain user account data, which could be used for further malicious purposes.

A popular online tech website called CNET explains an example using Facebook. It explains that most malicious phishing links involving pop-ups use a fake a domain name, but the Covert Redirect flaw uses the real site address for authentication [10]. If a user chooses to authorize the log in, personal data will be released to the attacker, depending on what is being asked. During this process, the website checks the domain name against the token, which is assigned to the partner as a means for verification all within the redirected URL. If the pair on the approved list is in its database, the Website would allow for that specific redirection to occur.

The researcher explains that if the URL belongs to a domain that has an Open Redirect Vulnerability, users could be redirected from the website to the vulnerable site and then to a malicious site [15]. His research has also expressed his concern about who is responsible for the vulnerability. There are a number of parties associated with this scheme, which include the website or the Relying Party (RP), and the partners or the Identity Provider (IdP). Existing weakness are associated with the partner websites and websites may feel as though it is not their responsibility to patch up the vulnerability. The partners on the other hand may be unaware of the vulnerability or there may be some that do not bother to fix it [16]. Jing believes that the website should be responsible to fix the vulnerability because the attacks are mainly targeting them. Although Wang Jing received a lot of discussion regarding his research, there are some in the security field that believe this is not a vulnerability related to the OAuth framework [16].

Many experts think that the problem is associated with how the framework is implemented by website developers [14, 17, 18]. Researchers believe that the solution will not be solved with a patch but only by proper implementation, which could mean utilizing techniques such as URL whitelisting. Whether this is a security flaw or vulnerability, it is clear that an issue exists and cannot be solved by one single party. The research above touches on some of the security flaws that can be associated with commercial Web-based SSO's. Each of them is unique in their own way but all of them can be dangerous to a creditable user if not used properly.

III. Survey Study and Results

The survey will be issued out via Google Forms for easy accessibility for study participants. The target audience will be college students and recent graduates from ages 16-30. Each of the participants were provided with a brief description of what Web-based SSO's are and how they are utilized. Participants are even introduced to the study being conducted and how their responses will impact the overall goal of the research. Additionally, the survey provides individuals with a screenshot showing an example of a traditional Web-based SSO may look like on the web. All of this information is conveniently provided before the questionnaire is started by the participants. Fig. 3 shows a front page of the survey using Google Form.

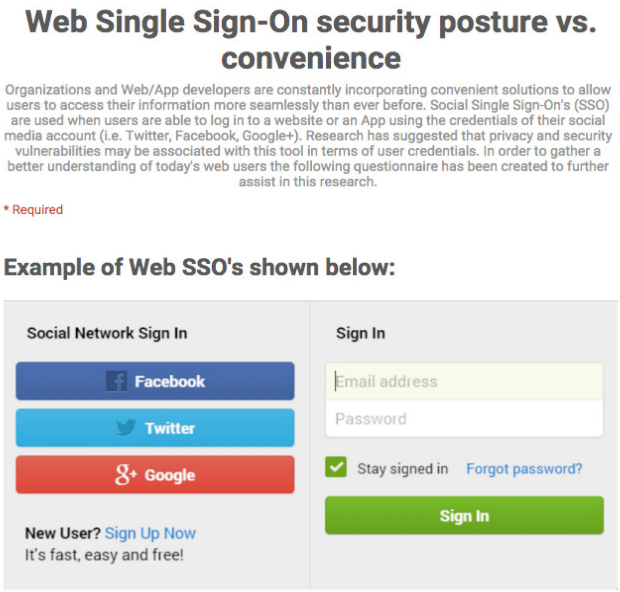
A. Survey Sample Questions

The questionnaire will be no longer than 20 questions in order to be transparent with the participant. Some of the sample questions that will be asked include the age, gender, level of education, and major/occupation of the selected individuals. The demographics will play a key role in discovering what types of users submit themselves to Web-based SSO tools. Additionally, we want to understand the average web user and how many web accounts they own that may require the use of a username and password. This can lead us into concluding how often they may use Web-based SSO technology schemes. Regardless if users are using this technology, the survey will ask questions about if they prefer the use of Web-based SSO's over registering for a new account. For example, we ask individuals if while they are creating a new account would they prefer to sign in using your social media credentials (i.e., Sign in with Twitter), or register for a new username and password. Some of these survey questions are listed below:

- What is your highest level of education?
- What is your gender?
- What is your highest level of education?
- What is your major or occupation?
- How often do you use the Web?
- How many web accounts do you use require a username and password?
- Please indicate which of the following sites that you currently have an account with (Select all that apply): Facebook, Google, Twitter, Yahoo, and Microsoft.
- Have you heard of Web-based Single-Sign-On?
- How many smartphones, PDA, computers or other devices do you use to browse the web?
- When creating a new account, would you prefer to sign in using your social media credentials (i.e. Sign in with Twitter), or register for a new username and password?
- Please select your primary browser (Select all that apply): Safari, Google Chrome, Internet Explorer, Mozilla Firefox, or other (please indicate).
- Would you be willing to use a Web-based Single Sign-On tool (i.e. Sign in with Twitter) when accessing personal banking or stock trading information? Please explain your answer
- Are you aware that Single Sign-On implementations are being used by Hampton University's myCampus Portal and other universities?
- For Hampton's myCampus Portal: would you prefer registering for an entirely new account with a website or use a "Sign-in with Facebook" option?
- Prior to this questionnaire were you aware of the security vulnerabilities that lie within Web-based Single Sign-On schemes?
- Will you continue using Web-based Single Sign-On tools (i.e. Sign in with Facebook) after taking this questionnaire?

In order to learn the importance of this tool to users we even ask them if they are willing to use Web-based SSO when accessing personal banking or stock information. Each participant is asked to explain his or her answer in a textbox provided in the questionnaire. Some questions are to grasp the participant's understanding and thoughts on security vulnerabilities of Web-based SSO prior to the questionnaire.

Fig. 3. Survey Using Google Form



Web Single Sign-On security posture vs. convenience

Organizations and Web/App developers are constantly incorporating convenient solutions to allow users to access their information more seamlessly than ever before. Social Single Sign-On's (SSO) are used when users are able to log in to a website or an App using the credentials of their social media account (i.e. Twitter, Facebook, Google+). Research has suggested that privacy and security vulnerabilities may be associated with this tool in terms of user credentials. In order to gather a better understanding of today's web users the following questionnaire has been created to further assist in this research.

* Required

Example of Web SSO's shown below:

Lastly, if participants are aware of vulnerabilities existing in Web-based SSO, will they still continue to use this convenient scheme? These are sample questions taken from the survey questionnaire that will aid in answering the underlying questions that effect most if not all web users today: are we willing to give up security and privacy for the convenience of Web-based SSO tools and other technologies alike? If so, where will this lead us in the future as technology is being incorporated in almost all of our daily tasks to virtually make our lives easier.

B. *Survey Results*

The results of the survey consisted of 68 responses: 63% of the respondents are male while 37% are female. Almost 60% of the respondents have at least a college degree while 21% are still in college. Of the respondents, 99% use the internet daily while 54% indicated that they have six or more web accounts that require a username and password; 24% of respondents even indicated that they had upwards of 20 plus accounts (see Fig. 4). Memorizing all of these passwords daily can be an exhausting task. Because of this, users would be inclined to use the same passwords for multiple accounts or result to using Web-based SSO's. Users likely settle with these solutions in order to reduce the risk of forgetting a password and losing access to their accounts. Most of the respondents are mindful when it comes to using Web-based SSOs when accessing personal banking or stock trading information. Majority of the responses answered no (see Fig. 5) and briefly explained their answer. One respondent explains by saying "No, although it may be considered secure, it makes your information more vulnerable by using multiple gateways to access your account..."

Overall the responses reflect that users believe using SSOs would present an unnecessary risk to important information such as finances. With that being said, about 47% (see Fig. 6) indicated that prior to taking the questionnaire they were unaware of the security vulnerabilities that lie within Web-based SSO schemes and 42% indicated they would continue to use Web-based SSO tools even after taking the questionnaire (see Fig. 7).

About 42% of respondents stated that they are not going to continue to use Web-based SSO after taking the questionnaire. The remaining 16% were unable to answer the question and gave their responses accordingly. Many replied by saying they had never used the scheme or it strictly depends on what they are using the technology for. Although this survey reveals that many users would not continue to use Web-based SSO, there is still a large percentage of participants that will continue to use the tool despite the vulnerabilities that may be associated with them. The only explanation for this conduct is convenience.

IV. Conclusion

In this paper, we report an extensive security study relating to the regular use of Web-based SSO schemes. The study shows that although users are aware of the security vulnerabilities that may lie within Web-based SSO implementations, they are still willing to submit themselves to the technology. It is obvious to some users that the benefits outweigh the risks that are involved with the scheme.

Fig. 4. Number of Web Accounts

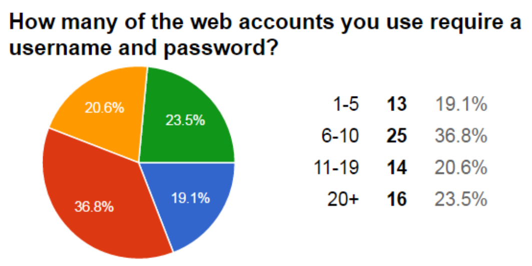


Fig. 5. Preference on Sign-in with Facebook

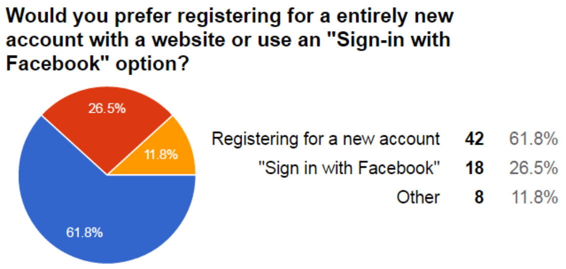


Fig. 6. Familiarity with Web-based SSO's Vulnerabilities

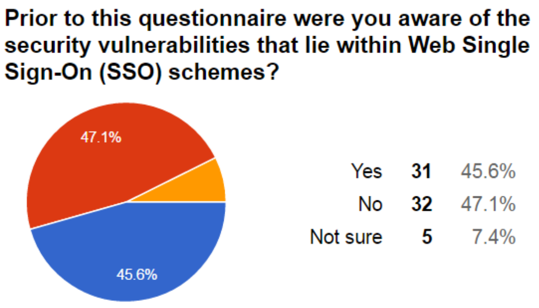
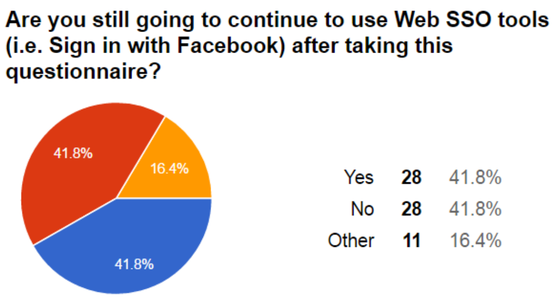


Fig. 7. Continued Use of Web-based SSO Schemes



These benefits could include minimizing the amount of passwords and usernames, and the ease in signing up for new websites and apps. Simplicity and convenience are both attributes that users and UX developers aim to provide. Many of the participants have recorded that they have upwards of 20 plus online accounts. Users are clearly relieved from the huge burden of registering many online accounts and remembering passwords. The convenience that this type of scheme brings to our digitally-centric lives is unparalleled. It is no question that tools like these are being developed more each and every day. Even though this may be true our society must understand that the same tools that make our lives more convenient also tend to be less secure. As we become more technologically advanced, it is becoming evident that we must think carefully about the schemes and devices used on a daily basis. If we are so willingly able to submit our information to tools like Web-based SSOs, knowing the potential security vulnerabilities, what else are we willing to submit ourselves to?

ACKNOWLEDGMENT

This research is supported by the National Science Foundation Award DGE-1303409 (CyberCorps Scholarship for Service: Hampton University Graduate Education and Training Scholarship in Information Assurance (HU GETS-IA) Program and by the National Security Agency H98230-15-1-0285 (CAE Cyber Security Research: Intelligent Secured Programming and Cloud-based Computing System.

REFERENCES

[1] K. Scarfone, and M. Souppaya, "Guide to Enterprise Password Management," 2009, http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf.

[2] TechoPedia, "Single Sing-On (SSO): Definition," 2016, https://www.techopedia.com/definition/4106/single-sign-on-sso

[3] D. Florencio, and C. Herley, "A large-scale study of web password habits," Proceedings of the 16th Inter-national Conference on World Wide Web, New York, NY, USA ACM, 2007, pp. 657-666.

[4] L. Klingbeil, "Password Fatigue: Why Users Hate Your Site," 2014, http://blog.loginradius.com/2014/12/password-fatigue-why-users-hate-your-site/

[5] P. Abel, "Consumer Perceptions of Online Registration and Social Sign-In," 2011, http://www1.janrain.com/rs/janrain/images/Industry-Research-Consumer-Perceptions-of-Online-Registration-and-Social-Sign-In-2011.pdf

[6] C. Spain, "The Technology of Convenience," 2015, http://newsroom.cisco.com/feature-content?type=webcontent&articleId=1648482

[7] D. Jeffers, "Why Convenience Is the Enemy of Security," 2013, http://www.pcworld.com/article/257793/why_convenience_is_the_enemy_of_security.html

[8] P. Abel, "Consumer Perceptions of Online Registration and Social Login," 2012, http://www1.janrain.com/rs/janrain/images/Industry-Research-Consumer-Perceptions-of-Online-Registration-and-Social-Login-2012.pdf.

[9] R. Wang, S. Chen, and X. Wang, "Signing Me onto Your Accounts through Facebook and Google: a Traffic-Guided Security Study of Commercially Deployed Single-Sign-On Web Services," Proceedings of the 2012 IEEE Symposium on Security and Privacy, Washington DC, USA, IEEE, 2012, pp. 365-379.

[10] A. Low, and S. Rosenblatt, "Serious security flaw in OAuth, OpenID discovered," 2014, http://www.cnet.com/news/serious-security-flaw-in-oauth-and-openid-discovered/

[11] L. Xing, Y. Chen, X. Wang., and S. Chen, "InteGuard: Toward Automatic Protection of Third-Party Web Service Integrations," 2013, http://www.internetsociety.org/sites/default/files/Presentation04_1.pdf

[12] S. 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," Symposium on Usable Privacy and Security (SOUPS), July 20–22, 2011, Pitts-burgh, PA USA.

[13] C. Yue, "The Devil is Phishing: Rethinking Web Single Sign-On Systems Security," the 6th USENIX Workshop on Large Scale Exploits and Emergent Threats (LEET), August 12, 2013, Washington DC, USA.

[14] Symantec, "Convert Redirect Flaw in OAuth is Not the Nextbleed," 2014, http://www.symantec.com/connect/blogs/covert-redirect-flaw-oauth -not-next-heartbleed

[15] W. Jing, "Convert Redirect Vulnerability," 2014, http://tetraph.com/covert_redirect/

[16] OWASP, "Open Redirect," 2012, https://www.owasp.org/index.php /Open_redirect

[17] S. Ragan, "Convert Redirect isn't a vulnerability, and it's nothing like Heartbleed," 2014, http://www.csoonline.com/article/2150983/application-security/covert-redirect-isnt-a-vulnerability-and-its-nothing-like-heartbleed.html

[18] D. Thorpe, "Tech Analysis of Serious security flaw in OAuth, OpenID Discovered," 2014, http://dannythorpe.com/2014/05/02/tech-analysis-of-serious-security-flaw-in-oauth-openid-discovered/