Pilot Study Web-Based Single Sign-On: Are We Giving Up Security and Privacy for Convenience?

Charles Scott and Devin Wynne
Faculty Advisor: Dr. Chutima Boonthum-Denecke
Department of Computer Science
Hampton University
Hampton, VA, USA 23668
{charles.c.scott26, devin.m.wynne}@gmail.com

ABSTRACT

Within our society we have seen a dramatic increase in the amount of individuals that have access to the World Wide Web 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 many 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 commercially adopted scheme raises concerns that could potentially allow users to give up on their privacy and security personal credentials for convenience. This paper describes the popular Web SSO system security posture. A survey is conducted as a part of this pilot study 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?

CCS Concepts

• Security and privacy→ Security services →Authorization

Keywords

Web-based single-sign-on; privacy; social media; security;

1. INTRODUCTION

Web Single-Sign-On's (SSO) 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 Figure 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 [1]. Additionally, many users are suffering from “password fatigue;” which is essentially the burden regular web-users face when managing an increase amount of accounts and passwords [2]. The described examples play a pivotal role in the use of Web SSO's, 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 SSO to be offered by websites and applications [3]. This percentage is proof to UX developers, industry, and users, that Web SSO's will continue to be utilized in the future. The push of Web SSO tools is deriving from the leading web technology companies that most web users are familiar with which include: Facebook, Google, Twitter, PayPal, and Yahoo. All of these companies offer Web 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 SSO's. Like any authentication scheme, their number one mission is to prevent an unauthorized party from gaining access to a legitimate users' account. Web SSO's 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 SSO's are just the beginning of authentication flaws that could expose critical personal assets to the unwanted individuals. In this paper we will take a look into the Web SSO implementation and its security vulnerabilities that may be associated. The research will aim to understand modern user point of views as it relates to these technology schemes. Ultimately the paper will seek to tackle issues associated with the

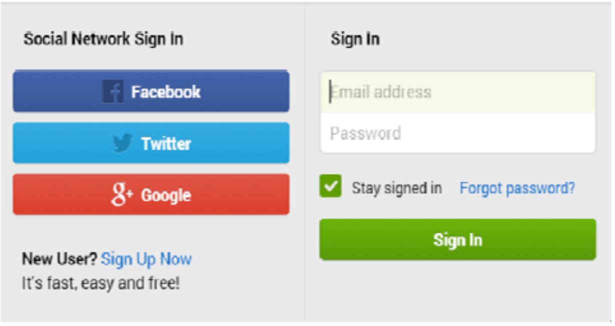


Figure 1. Real World Example of Web SSO

ADMI 2016, March 31-April 3, 2016, Winston-Salem, NC, USA.

trade-offs between the advancement of convenience technologies to a user's security and privacy desires.

2. MOTIVATION

The motivation behind this research stems from the ease of advanced technologies to lift the tensions off everyday 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 [15]. 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 vs. security is not a cut and dry choice but can be considered a sliding scale that requires finding the right balance between the two [16].

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 [16]. 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 [16]. 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 single sign-on's have 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 [17].

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 [17]. 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 SSO's: 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 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.

3. WEB SSO SECURITY VULNERABILITES

In order to discuss Web SSO's and its vulnerabilities, the tool must be broken down and understood. The frame-work behind these tools face a critical challenge because commercially deployed SSO systems are typically neither publish detailed specifications for their operations nor have their code of the RP and IdP sides accessible to the public [4].

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 SSO's that take place through 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 SSO's operate (shown in Figure 2). Additionally, these interactions are the beginning stages of how vulnerabilities may be associated with the widely used tool.

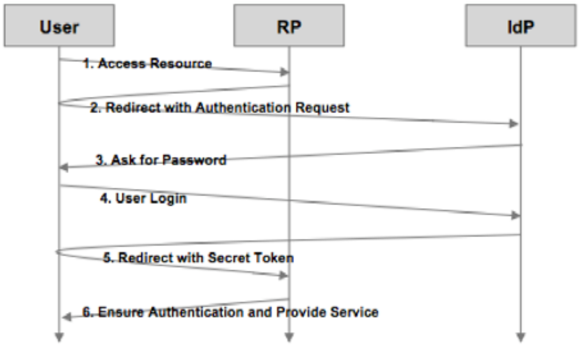

User
RP
IdP
1. Access Resource
2. Redirect with Authentication Request
3. Ask for Password
4. User Login
5. Redirect with Secret Token
6. Ensure Authentication and Provide Service

Figure 2. Web SSO Traffic Analysis

During the transaction Web SSO's are primary built upon the relying party (RP) integration of the web API's exposed by the IdP [4]. While using these API's the relying party virtually redirects the browser to the identity providers (IdP) to authenticate the user when he or she 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 [4]. This communication between HTTP responses and exchanging of tokens can be called browser-relayed message (BRM) (Low et al. 2014). Another associated tool used during these transactions includes OpenID. OpenID is an open and promising user-centric Web SSO solution [7]. 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 [7]. It is repeatedly discussed in related research that this process is riddled with logic flaws [4] [5] [7]. 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 [6].

3.1 Phishing Attacks

Web 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 associated with this tool if they are not properly implemented or used effectively. Yue from the University of Colorado Springs conducted a study on the idea behind how Web SSO's can be used in phishing attacks [8]. It is stated that Web SSO's can be spoofed with ease to even trick regular web users who are familiar with the idea of phishing attacks [8]. The study explains that the spoofed login page deceived 61% of the surveyed participants who have heard about phishing [8]. 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 [8]. In conclusion the paper explains that a collective solution must be thought of between IdP, RP, browser, and especially 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 [8].

3.2 BRM Traffic Analysis Vulnerability

It is also studied that the actual transactions commercially deployed by Web 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 8 serious logic flaws in identity providers such as Google ID, Facebook, and Sears.com just to name a few [4].

These logic flaws allow an attacker to sign in as the victim user. To complete their study, the researchers developed a "BRM analyzer" to provide differential analysis on BRM traces. The tool captured and parsed BRM traces and even modified/replayed HTTP requests. In the 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 [4]. The elaborate steps shown in this study exemplify serious logic flaws in Web 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. Although researchers have reported some flaws in web SSO's, they explain that there are plenty others that this study cannot cover. The BRM analyzer tool is available to the general public to allow developers and security analysts to conduct investigations similar to the ones conducted in their paper.

3.3 Covert Redirect

Another serious vulnerability that can be associated with Web SSO's involves the use of login standards OAuth and OpenID, found by Wang Jing a PhD student at the Nan-yang Technological University in Singapore. Symantec defines OAuth as an open protocol to allow secure authorization from web, mobile, and desktop applications [12]. This vulnerability is known as the "*Covert Redirect*" and is loosely derived from the existing Open Direct vulnerability [9]. The open direct is an application that takes a parameter and redirects a user to the parameter value without any validation [10].

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 [9]. A covert redirect vulnerability exists because of the website overconfidence in its partners, consequently giving leeway to the attacks [9]. In order for this flaw to be exploited it requires interaction from web users [15]. A user would physically have to grant permissions to a susceptible application in order for the access token to be compromised [12]. Only then can an attacker obtain user account data, which could be used for further malicious purposes [12].

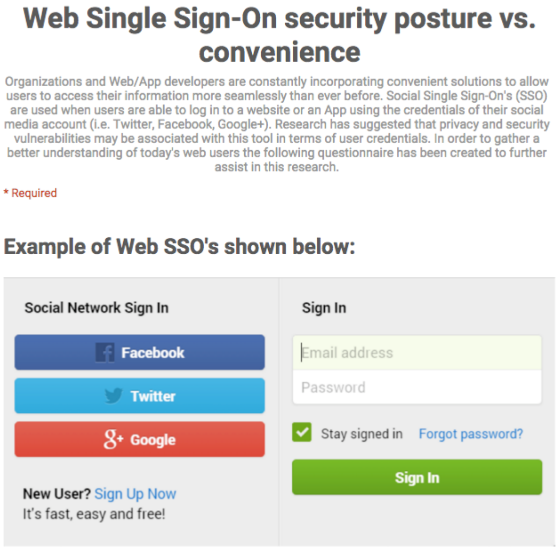
A popular online tech website titled CNET explains an example using Facebook. It explains that most malicious phishing links involving pop-ups use a fake domain name, but the Covert Redirect flaw uses the real site address for authentication [11]. If a user chooses to authorize the log in, personal data 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 [9]. His research has also expressed his concern about who is responsible for the vulnerability. There a number of parties that are associated with this scheme, which includes 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 don't feel the need to fix it [9]. Jing believes that the website should be responsible to fix the vulnerability because the attacks are mainly targeting them. Although 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.

Many experts think that the problem is associated with how the framework is implemented by web site developers [12] [13] [14]. 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 [12] [13] [14]. Whether this is a security flaw or vulnerability, it is clear that this issue does exist 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 SSO's. Each of them is unique in their own ways but all of them can be dangerous to a creditable user if not used properly.

4. STUDY PROTOCOL

The survey was created and issued out via Google Forms for easy accessibility for study participants. The target audiences for this pilot study were college students and recent graduate from ages 16-30. Each of the participants was provided with a brief description of what Web 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.



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:

Figure 3. Google Form

Additionally, the survey provides individuals with a screenshot showing an example of a traditional Web SSO may look like on the web. All of this information is conveniently provided before the questionnaire is started by the participants. A live view is shown in Figure 3.

5. SURVEY QUESTIONS

The questionnaire is no longer than 20 questions in order to be transparent with the participant. Some of the 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 SSO tools. Additionally, we want to understand the participants' average web use and how many web accounts they own that may require the use of username and passwords. This can lead us into concluding how often they may use Web SSO technology schemes. Regardless if users are using this technology the survey will ask questions about if they prefer the use of Web 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. 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 the following sites that you use of currently have an account with (Select all that apply): Facebook, Google, Twitter, Yahoo, and Microsoft.
- Have you heard of Web Single-Sign-On's?
- 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 SSO 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 Single-Sign-On's (SSO) schemes?
- Are you still going to continue to use Web SSO 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 SSO's when accessing personal banking or stock information (Shown in the questions above). We ask that each participant explain his or her answer in a textbox provided in the questionnaire. We will also ask questions to grasp the user's mindset of security vulnerabilities of Web SSO's prior to the questionnaire. Finally, if users are aware of vulnerabilities that may lie in Web SSO's, will they still continue to use this convenient scheme? All of these sample questions taken from the questionnaire 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 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?

6. SURVEY RESULTS

The results of a preliminary survey consist of 30 responses. All but seven of the respondents are between the ages of 16 and 25 years of age. All but four of the respondents have obtained a college degree and the other four either had recently or are currently taking college courses. The results show that 97% percent of the respondents use the internet daily while 70% indicated that they have six or more web accounts that require a username and password. Memorizing six or more passwords can be a difficult task.

Users with this many accounts would be inclined to use the same passwords for multiple accounts or result to using Web SSO's. Users likely settle with these solutions in order to reduce the risk of forgetting a password and losing access. Most of the initial respondents are mindful of using SSO's when accessing personal banking or stock trading information.

Half of the respondents answered "No" when questioned if they would use SSO when accessing personal banking or stock trading information for a variety of reasons. However, the outlook of the responses reflects that users believe using SSOs would present an unnecessary risk to important information such as financial applications. With that being said, about 62% (Shown in Figure 4) indicated that prior to taking the questionnaire they were unaware of the security vulnerabilities that lie within SSO's schemes and 39% indicated that they would continue to use SSO tools after taking the questionnaire (shown in Figure 5). About 25% of the participants responded by saying they are not going to continue to use Web SSO's after taking the questionnaire. The rest 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 scheme for. These statistics are found in figures three and four. This survey reveals that the majority of users will continue to use SSO tools despite the vulnerabilities associated with them. The only explanation for this conduct is convenience.

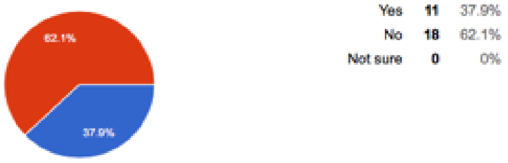


Figure 4. Familiarity with Web SSO's Vulnerabilities

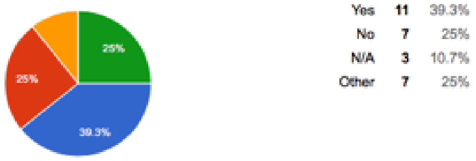


Figure 5. Continued use of Web SSO schemes

7. CONCLUSION

In this paper, we reported an extensive security study relating to the regular use of Web SSO schemes. The pilot study shows that although users are aware of the security vulnerabilities that may lie within Web SSO implementations, they are still willing to submit themselves to the technology. It's clear to the users that the benefits outweigh the risks that are involved with the scheme. 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+ online accounts. When utilizing Web SSO's, users are clearly relived from the huge burden of registering for many online accounts and remembering passwords. The convenience that this type of authentication scheme provides to our digitally-centric lives is unparalleled. It's no question that tools like these are being developed more each and every day.

Unfortunately, the same tools that make users' lives more convenient also tend to be less secure. As we become technologically more advanced it is becoming evident that we must think carefully about the schemes and devices we are using on a constant basis. If we are so willingly able to submit ourselves to technology like Web SSO's, even knowing the potential security vulnerabilities, what else are we willing to submit ourselves to?

8. ACKNOWLEDGEMENTS

This work is partly supported by the National Science Foundation, CyberCorps: Scholarship for Service Program under grant no. DGE-1303409 (PI/co-PI: Dr. Chutima Boonthum-Denecke, Dr. Jean Muhammad).

9. REFERENCES

[1] Florencio, D. and Herley, C. 2007. A large-scale study of web password habits. In WWW '07: Proceedings of the 16th International Conference on World Wide Web, pages 657–666, New York, NY, USA, 2007. ACM.

[2] Klingbeil, L. Password Fatigue: Why Users Hate Your Site. 2014. Retrieved from http://blog.loginradius.com/2014/12/password-fatigue-why-users-hate-your-site/ [November 8, 2015]

[3] Abel, P. Consumer Perceptions of Online Registration and Social Sign-In.2011.Retrievedfrom http://www1.janrain.com/rs/janrain/images/Industry-Research-Consumer-Perceptions-of-Online-Registration-and-Social-Sign-In-2011.pdf [November 4, 2015]

[4] Wang, R., Chen, S. and Wang, X. 2012. Signing Me onto Your Accounts through Facebook and Google: a Traffic-Guided Security Study of Commercially Deployed Single-Sign-On Web Services. SP '12 Proceedings of the 2012 IEEE Symposium on Security and Privacy Pages 365-379. Washington DC, USA, 2012. IEEE.

[5] Xing, L., Chen, Y., Wang, X. and Chen, S. 2013. InteGuard: Toward Automatic Protection of Third-Party Web Service Integrations. Retrieved from http://www.internetsociety.org/sites/default/files/Presentation04_1.pdf [November 16, 2015]

[6] Low, A. and Rosenblatt, S. 2014. Serious security flaw in OAuth, OpenID discovered. Retrieved from http://www.cnet.com/news/serious-security-flaw-in-oauth-and-openid-discovered/ [November 3, 2015]

[7] Sun, S., Pospisil, E., Muslukhov, I., Dindar, N., Hawkey, K., and Beznosov, K. 2011. What Makes Users Refuse Web Single Sign-On? An Empirical Investigation of OpenID. Symposium on Usable Privacy and Security (SOUPS) 2011, July 20–22, 2011, Pittsburgh, PA USA.

[8] Yue, C. 2013. The Devil is Phishing: Rethinking Web Single Sign-On Systems Security. Large Scale Exploits and Emergent Threats. Washington DC, USA.

[9] Jing, W. 2014. Convert Redirect Vulnerability. Retrieved from http://tetraph.com/covert_redirect/ [November 8, 2015]

[10] OWASP. 2012. Open Redirect. Retrieved from https://www.owasp.org/index.php/Open_redirect

[11] Symantec Security Response {Symantec Employee}.. 2014. Convert Redirect Flaw in OAuth is Not the Nextbleed. Retrieved from http://www.symantec.com/connect/blogs/covert-redirect-flaw-oauth-not-next-heartbleed [November 16, 2015]

[12] Ragan, S. 2014. Convert Redirect isn't a vulnerability, and it's nothing like Heartbleed. Retrieved from http://www.csoonline.com/article/2150983/application-security/covert-redirect-isnt-a-vulnerability-and-its-nothing-like-heartbleed.html [November 13, 2015]

[13] Thorpe, D. 2014.Tech Analysis of Serious security flaw in OAuth, OpenID Discovered. Retrieved from http://dannythorpe.com/2014/05/02/tech-analysis-of-serious-security-flaw-in-oauth-openid-discovered/ [November 3, 2015]

[14] Spain, C. 2015. The Technology of Convenience. Retrieved from http://newsroom.cisco.com/feature-content?type=webcontent&articleId=1648482 [November 13, 2015]

[15] Jeffers, D. 2013.Why Convenience Is the Enemy of Security. Retrieved from http://www.pcworld.com/article/257793/why_convenience_is_the_enemy_of_security.html [November 16, 2015]

[16] Abel, P. 2012.Consumer Perceptions of Online Registration and Social Login. Retrieved from http://www1.janrain.com/rs/janrain/images/Industry-Research-Consumer-Perceptions-of-Online-Registration-and-Social-Login-2012.pdf [November 4, 2015]