The Devil is Phishing: Rethinking Web Single Sign-On Systems Security

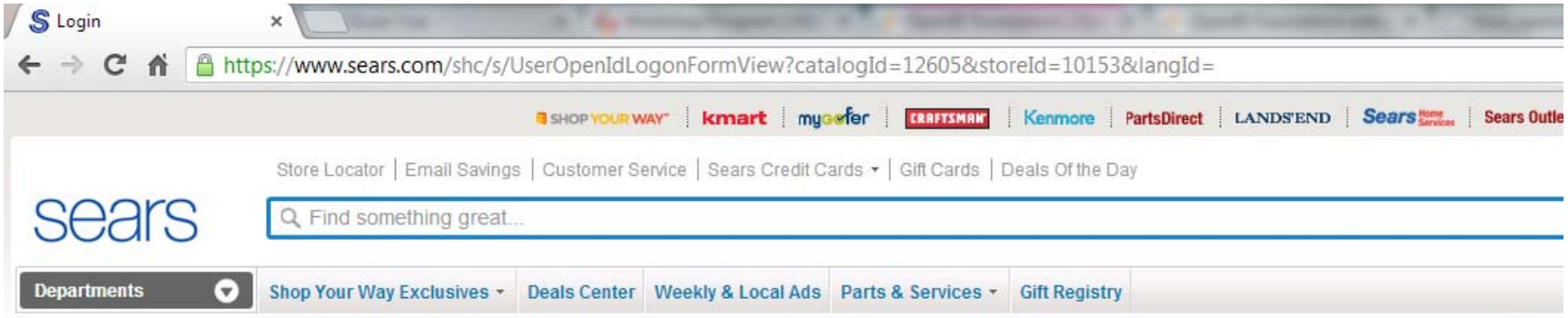
Chuan Yue

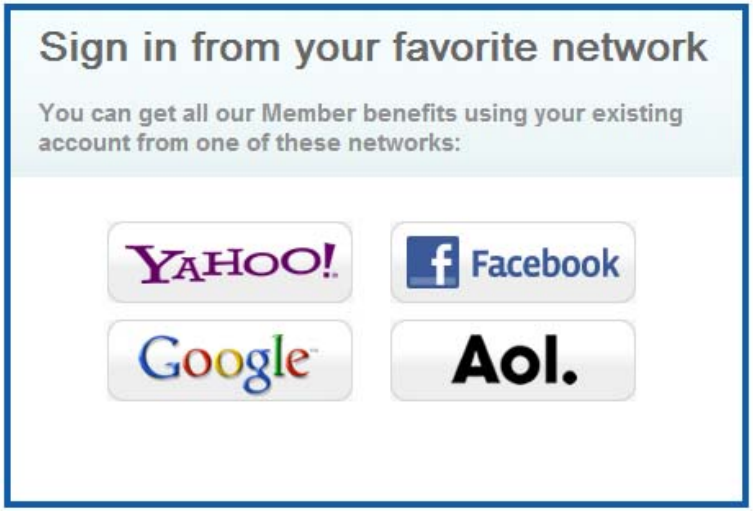
USENIX Workshop on Large-Scale Exploits
and Emergent Threats (LEET 2013)



University of Colorado
Colorado Springs

Web Single Sign-On (SSO) systems





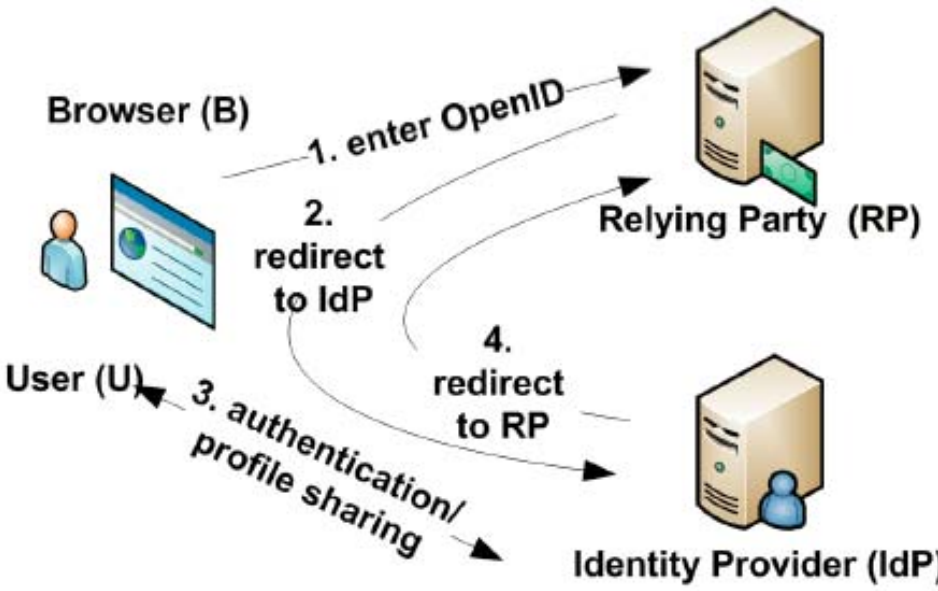
Sign in multiple relying party (RP) websites using one single identity provider (IdP) account.

Users are relieved from the huge burden of registering many online accounts and remembering many passwords.

Rapid Adoption of Web SSO systems

- Open Web SSO standards OpenID and OAuth.
  - one billion OpenID enabled user accounts and over 50,000 RP websites (http://openid.net/get-an-openid/what-is-openid/).
  - leading IT companies including Google, Facebook, Microsoft, and Yahoo are OpenID IdPs.
  - OAuth 2.0 authorization framework has also been widely supported by IdPs and adopted by a large number of RP websites (http://oauth.net/about/).

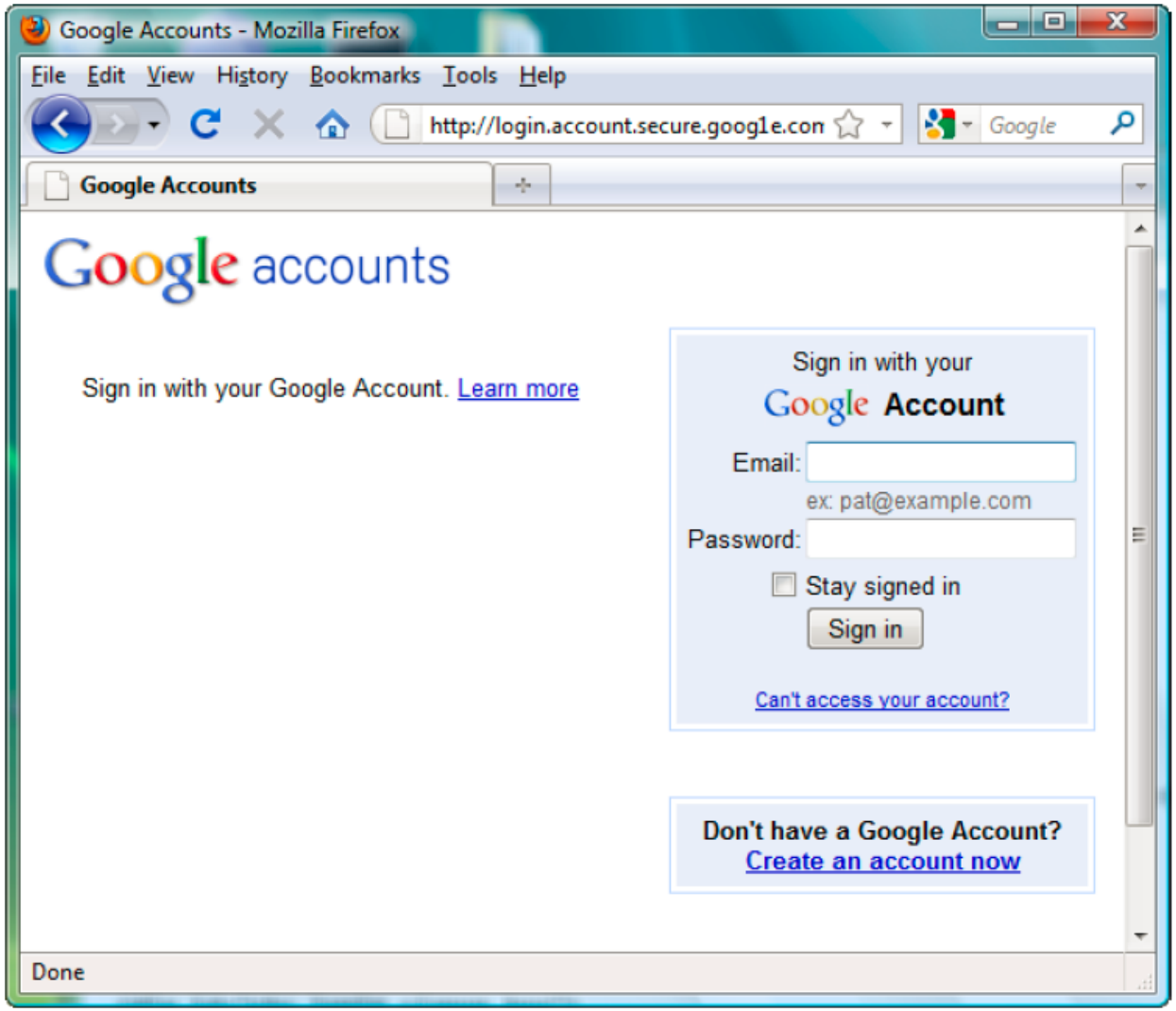
Security of Web SSO systems



This figure comes from Reference [10] Figure 1 (a): OpenID login flow

- Formal security analysis of some Web SSO protocols [1, 2]
- Logic flaws and implementation vulnerabilities of many deployed Web SSO systems [9, 11]
- Phishing attacks [10, 14, 17, 18]

An Example of Previous Web SSO Phishing Study



This figure comes from Reference [10] page 20 (the original OpenID phishing demo website http://idtheft.fun.de is not available now).

About 50% success rate in this particular case

Our Main Argument and Contributions

- Argument
  - large-scale threat from phishing attacks to real-world Web SSO systems has been significantly underestimated and insufficiently analyzed.

- Contributions
  - pinpoint what are really unique in Web SSO phishing
  - provide one example to illustrate how the IdPs of Web SSO systems can be spoofed with ease and precision
  - present a preliminary user study to demonstrate the high effectiveness of Web SSO phishing attacks

What are Really Unique in Web SSO phishing

- The value of IdP accounts is highly concentrated.
- The attack surface area is highly enlarged.
- The difficulty of phishing detection (either by algorithms or by users) is highly increased.

These characteristics make Web SSO phishing more profitable and insidious, and very challenging to defend against.

Phishers have greater incentives to attack users' IdP accounts.

Highly Concentrated Value of IdP Accounts

- A few major IdPs such as Google, Facebook, and Microsoft.
- IdP accounts are already highly valuable by themselves.
- A compromised IdP account also allows attackers to impersonate the victim on a large number of RP websites.
- Phishing IdP accounts becomes more profitable than before.

Highly Enlarged Attack Surface Area

- Traditionally, phishers mainly use spoofed emails.
  - a spoofed email provides the first-level context (asking for account verification or update) to entice users to click a phishing URL
  - the spoofed phishing website further provides the second-level context (e.g., with look and feel similar to a targeted real website)

- In terms of this first-level context, the success of traditional phishing is limited by two main constraints:
  - phishing emails are suspicious, users would not visit phishing sites [3, 5]
  - a large number of phishing emails are captured by spam filters [12]

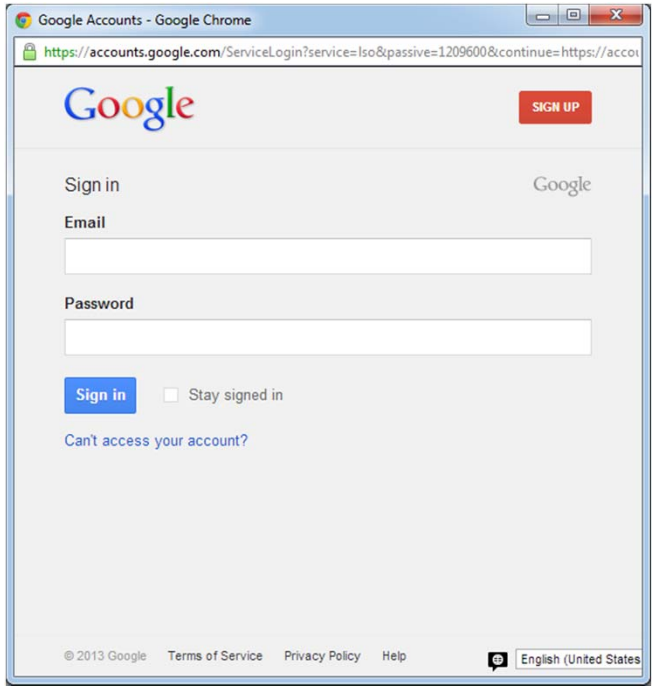
- In Web SSO, clicking a button that represents an IdP (e.g., Google or Facebook) to visit the IdP's login webpage is a common practice. Phishers are freed from these two constraints – they can host their own "legitimate" RP websites or webpages and post URLs everywhere (e.g., Web forums, blogs, and advertisements).

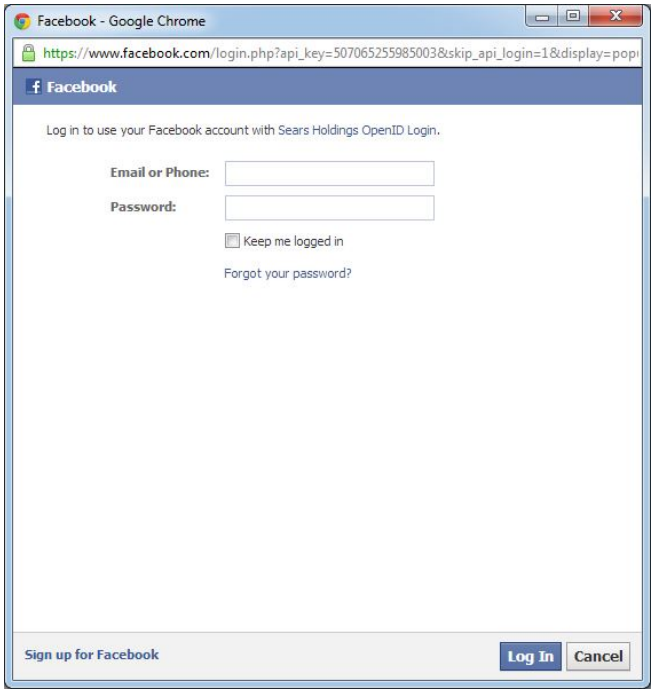
Highly Increased Phishing Detection Difficulty

Sign-in to your shopping account using

Google facebook

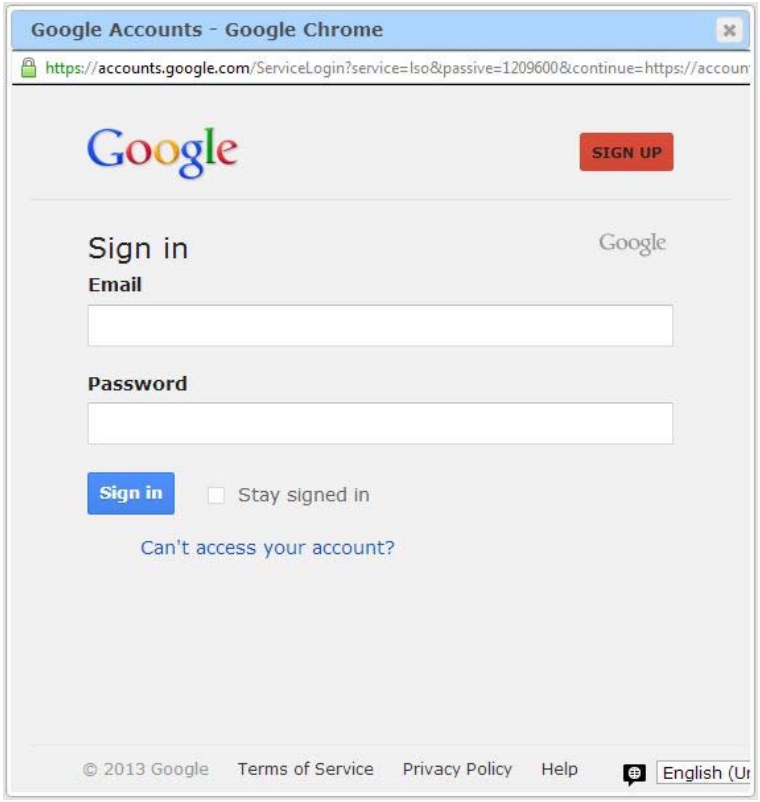
JavaScript window.open() method

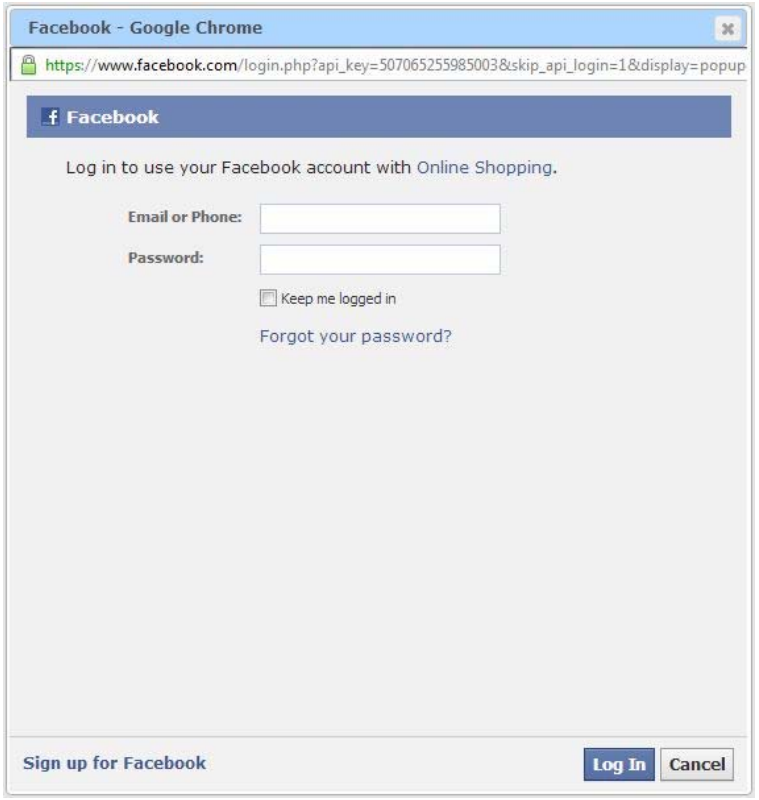




- The click-and-popup user interaction style is the root cause of the difficulty.
  - a popup IdP login window, although displaying the EV-SSL (Extended Validation SSL) icon and an HTTPs URL address, can be spoofed with ease and precision.
  - a spoofed popup login window does not need to correspond to a real URL address, thus can make the results of a large number of URL-heuristics-based automatic phishing detection algorithms (e.g., [4, 6, 7, 12, 13]) either inaccurate or incorrect.
  - the look and feel of a spoofed popup login window can also deceive many users.

Spoofing IdPs with Ease and Precision

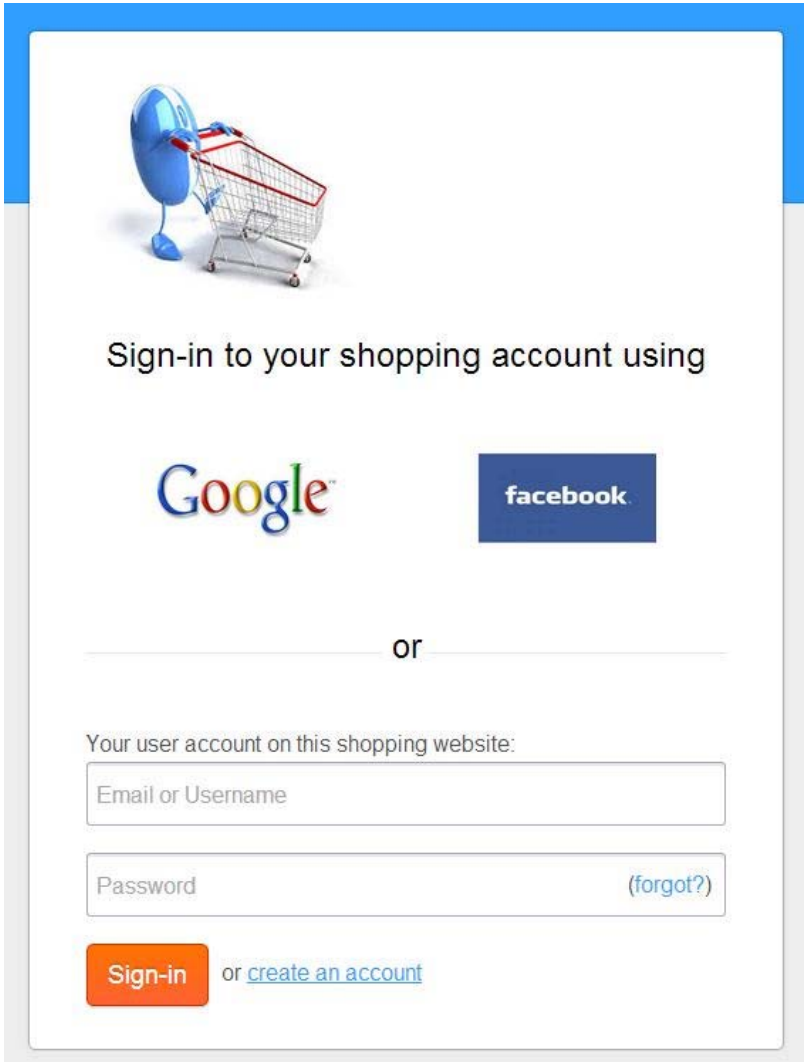




- We use HTML, CSS (Cascading Style Sheets), and JavaScript.
  - the essential trick is that such a spoofed login webpage is not contained in a real popup browser window – it is indeed contained in an HTML (i.e., division) element, which is supported in all major browsers.
  - the EV-SSL icon and the HTTPs URL address in the element are spoofed by copying a complete snapshot of the icon and the URL address from a real IdP login window.

A Preliminary User Study

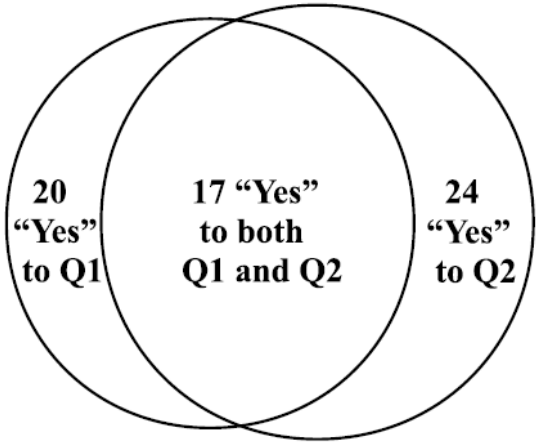
- Participants and Procedure
  - 28 (offers a reasonably tight confidence interval [19]) adults, 14 females and 14 males, participated in our study.
  - each participant logs into our shopping website using either a Google or a Facebook test account, and using one of the three browsers (i.e., Google Chrome, Firefox, and IE).



User Study Results and Analysis

- Pre-procedure Questionnaire
  - by looking at the Web SSO example webpage of one RP website (sears.com), 22 participants answered that they have Web SSO experience and have logged into some other websites using their Gmail or Facebook account before.

- Post-procedure
  - Q1: “Is that Gmail or Facebook login page a genuine one?”
  - Q2: “Have you heard about phishing attacks?”.

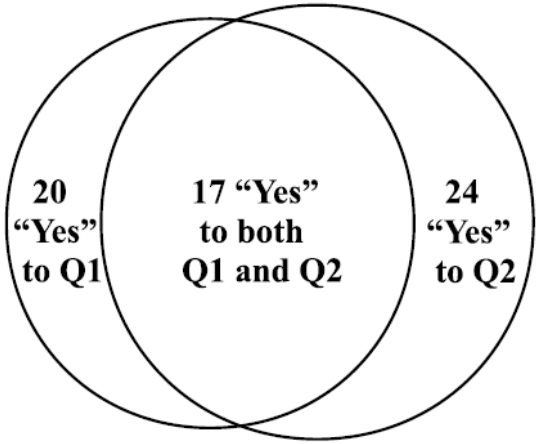


8 participants answered “No” to Q1: one explained that asking for Google/Facebook information is suspicious, and this participant indeed did not use Web SSO before; another explained that the shopping website is too simple and suspicious; the third explained the test Gmail account is suspicious; the other 5 mainly explained that the color and menu bar on the login webpages are suspicious.

User Study Results and Analysis

- Pre-procedure Questionnaire
  - by looking at the Web SSO example webpage of one RP website (sears.com), 22 participants answered that they have Web SSO experience and have logged into some other websites using their Gmail or Facebook account before.

- Post-procedure
  - Q1: “Is that Gmail or Facebook login page a genuine one?”
  - Q2: “Have you heard about phishing attacks?”.



16, 6, and 6 participants used Google Chrome, Firefox, and IE to perform the Web SSO procedure, respectively. 23 and 5 participants interact with the spoofed Google and Facebook login webpages, respectively. None of the 28 participants clicked the spoofed EV-SSL icon and the HTTPS URL address, indicating that users rely more on look than feel to identify the credibility of websites.

Discussion and Conclusion

- Web SSO phishing is more profitable and insidious than traditional phishing, and is very challenging to defend against.
- The click-and-popup user interaction style is the root cause of the highly increased phishing detection difficulty for algorithms and users. We are exploring some smooth Web content and context switching techniques to address this root cause.
- IdPs should further improve their phishing protection capabilities. For example, they may need to actively adopt two-factor authentication techniques and incentivize users.
- Users should be educated and trained to understand and identify Web SSO phishing.

Thank You!

References

[1] ARMANDO, A., CARBONE, R., COMPAGNA, L., CUELLAR, J., AND TOBARRA, L. Formal analysis of saml 2.0 web browser single sign-on: breaking the saml-based single sign-on for google apps. In *ACM FMSE* (2008).

[2] BANSAL, C., BHARGAVAN, K., AND MAFFEIS, S. Discovering concrete attacks on website authorization by formal analysis. In *IEEE CSF* (2012).

[3] DOWNS, J. S., HOLBROOK, M. B., AND CRANOR, L. F. Decision strategies and susceptibility to phishing. In *SOUPS* (2006).

[4] GARERA, S., PROVOS, N., CHEW, M., AND RUBIN, A. D. A framework for detection and measurement of phishing attacks. In *WORM* (2007).

[5] JAKOBSSON, M., AND RATKIEWICZ, J. Designing ethical phishing experiments: a study of (ROT13) rOnl query features. In *WWW* (2006).

[6] LUDL, C., MCALLISTER, S., KIRDA, E., AND KRUEGEL, C. On the effectiveness of techniques to detect phishing sites. In *DIMVA* (2007).

[7] MA, J., SAUL, L. K., SAVAGE, S., AND VOELKER, G. M. Beyond blacklists: learning to detect malicious web sites from suspicious urls. In *SIGKDD* (2009).

[8] RACHNA DHAMIJA, J.D.TYGAR, AND MARTI HEARST. Why phishing works. In *CHI* (2006).

[9] SUN, S.-T., AND BEZNOSOV, K. The devil is in the (implementation) details: an empirical analysis of oauth sso systems. In *CCS* (2012).

10] SUN, S.-T., POSPISIL, E., MUSLUKHOV, I., DINDAR, N., HAWKEY, K., AND BEZNOSOV, K. What makes users refuse web single sign-on?: an empirical investigation of openid. In *SOUPS* (2011).

[11] WANG, R., CHEN, S., AND WANG, X. Signing me onto your accounts through facebook and google: A traffic-guided security study of commercially deployed single-sign-on web services. In *the IEEE Symposium on Security and Privacy* (2012).

[12] WHITTAKER, C., RYNER, B., AND NAZIF, M. Large-scale automatic classification of phishing pages. In *NDSS* (2010).

[13] ZHANG, Y., HONG, J., AND CRANOR, L. CANTINA: A content-based approach to detecting phishing web sites. In *WWW* (2007).

[14] OAuth 2.0 Threat Model and Security Considerations. `http://tools.ietf.org/html/rfc6819`.

[15] OAuth Introduction. `http://oauth.net/about/`.

[16] OpenID Authentication 2.0 - Final. `http://openid.net/specs/openid-authentication-2_0.html`.

[17] OpenID Phishing Brainstorm. `http://wiki.openid.net/w/page/12995216/OpenID_Phishing_Brainstorm`.

[18] OpenID: Phishing Heaven. `http://www.links.org/?p=187`.

[19] Quantitative Studies: How Many Users to Test? `http://www.nngroup.com/articles/quantitative-studies-how-many-users/`.

[20] The OAuth 2.0 Authorization Framework. `http://tools.ietf.org/html/rfc6749`.

[21] What is OpenID? `http://openid.net/get-an-openid/what-is-openid/`.