Single sign-on

Single sign-on (**SSO**) is an authentication scheme that allows a user to log in with a single ID to any of several related, yet independent, software systems.

True single sign-on allows the user to log in once and access services without re-entering authentication factors.

It should not be confused with same-sign on (Directory Server Authentication), often accomplished by using the Lightweight Directory Access Protocol (LDAP) and stored LDAP databases on (directory) servers.[1][2]

A simple version of single sign-on can be achieved over IP networks using cookies but only if the sites share a common DNS parent domain.[3]

For clarity, a distinction is made between Directory Server Authentication (same-sign on) and single sign-on: Directory Server Authentication refers to systems requiring authentication for each application but using the same credentials from a directory server, whereas single sign-on refers to systems where a single authentication provides access to multiple applications by passing the authentication token seamlessly to configured applications.

Conversely, **single sign-off** or **single log-out** (**SLO**) is the property whereby a single action of signing out terminates access to multiple software systems.

As different applications and resources support different authentication mechanisms, single sign-on must internally store the credentials used for initial authentication and translate them to the credentials required for the different mechanisms.

Other shared authentication schemes, such as OpenID and OpenID Connect, offer other services that may require users to make choices during a sign-on to a resource, but can be configured for single sign-on if those other services (such as user consent) are disabled.[4] An increasing number of federated social logons, like Facebook Connect, do require the user to enter consent choices upon first registration with a new resource, and so are not always single sign-on in the strictest sense.

Benefits

Benefits of using single sign-on include:

- Mitigate risk for access to 3rd-party sites ("federated authentication")[5] because user passwords are not stored or managed externally
- Reduce password fatigue from different username and password combinations
- Reduce time spent re-entering passwords for the same identity[5]
- Reduce IT costs due to lower number of IT help desk calls about passwords[6]
- **Simpler administration.** SSO-related tasks are performed transparently as part of normal maintenance, using the same tools that are used for other administrative tasks.

- **Better administrative control.** All network management information is stored in a single repository. This means that there is a single, authoritative listing of each user’s rights and privileges. This allows the administrator to change a user’s privileges and know that the results will propagate network wide.
- **Improved user productivity.** Users are no longer bogged down by multiple logons, nor are they required to remember multiple passwords in order to access network resources. This is also a benefit to Help desk personnel, who need to field fewer requests for forgotten passwords.
- **Better network security.** Eliminating multiple passwords also reduces a common source of security breaches—users writing down their passwords. Finally, because of the consolidation of network management information, the administrator can know with certainty that when he disables a user’s account, the account is fully disabled.
- **Consolidation of heterogeneous networks.** By joining disparate networks, administrative efforts can be consolidated, ensuring that administrative best practices and corporate security policies are being consistently enforced.

SSO shares centralized authentication servers that all other applications and systems use for authentication purposes and combines this with techniques to ensure that users do not have to actively enter their credentials more than once.

Criticism

The term *reduced sign-on* (RSO) has been used by some to reflect the fact that *single sign-on* is impractical in addressing the need for different levels of secure access in the enterprise, and as such more than one authentication server may be necessary.[7]

As single sign-on provides access to many resources once the user is initially authenticated ("keys to the castle"), it increases the negative impact in case the credentials are available to other people and misused. Therefore, single sign-on requires an increased focus on the protection of the user credentials, and should ideally be combined with strong authentication methods like smart cards and one-time password tokens.[7]

Single sign-on also makes the authentication systems highly critical; a loss of their availability can result in denial of access to all systems unified under the SSO. SSO can be configured with session failover capabilities in order to maintain the system operation.[8] Nonetheless, the risk of system failure may make single sign-on undesirable for systems to which access must be guaranteed at all times, such as security or plant-floor systems.

Furthermore, the use of single-sign-on techniques utilizing social networking services such as Facebook may render third party websites unusable within libraries, schools, or workplaces that block social media sites for productivity reasons. It can also cause difficulties in countries with active censorship regimes, such as China and its "Golden Shield Project," where the third party website may not be actively censored, but is effectively blocked if a user's social login is blocked.[9][10]

Security

In March, 2012,[11] a research paper reported an extensive study on the security of social login mechanisms. The authors found 8 serious logic flaws in high-profile ID providers and relying party websites, such as OpenID (including Google ID and PayPal Access), Facebook, Janrain, Freelancer, FarmVille, and Sears.com. Because the researchers informed ID providers and relying party websites prior to public announcement of the discovery of the flaws, the vulnerabilities were corrected, and there have been no security breaches reported.[12]

In May 2014, a vulnerability named Covert Redirect was disclosed.[13] It was first reported "Covert Redirect Vulnerability Related to OAuth 2.0 and OpenID" by its discoverer Wang Jing, a Mathematical PhD student from Nanyang Technological University, Singapore.[14][15][16] In fact, almost all Single sign-on protocols are affected. Covert Redirect takes advantage of third-party clients susceptible to an XSS or Open Redirect.[17]

In December 2020, flaws in federated authentication systems were discovered to have been utilized by attackers during the 2020 United States federal government data breach.[18][19]

Due to how single sign-on works, by sending a request to the logged-in website to get a SSO token and sending a request with the token to the logged-out website, the token cannot be protected with the HttpOnly cookie flag and thus can be stolen by an attacker if there is an XSS vulnerability on the logged-out website, in order to do session hijacking. Another security issue is that if the session used for SSO is stolen (which can be protected with the HttpOnly cookie flag unlike the SSO token), the attacker can access all the websites that are using the SSO system.[20]

Privacy

As originally implemented in Kerberos and SAML, single sign-on did not give users any choices about releasing their personal information to each new resource that the user visited. This worked well enough within a single enterprise, like MIT where Kerberos was invented, or major corporations where all of the resources were internal sites. However, as federated services like Active Directory Federation Services proliferated, the user's private information was sent out to affiliated sites not under control of the enterprise that collected the data from the user. Since privacy regulations are now tightening with legislation like the GDPR, the newer methods like OpenID Connect have started to become more attractive; for example MIT, the originator of Kerberos, now supports OpenID Connect.[21]

Email address

Single sign-on in theory can work without revealing identifying information such as email addresses to the relying party (credential consumer), but many credential providers do not allow users to configure what information is passed on to the credential consumer. As of 2019, Google and Facebook sign-in do not require users to share email addresses with the credential consumer. "Sign in with Apple" introduced in iOS 13 allows a user to request a unique relay email address each time the user signs up for a new service, thus reducing the likelihood of account linking by the credential consumer.[22]

Common configurations

Kerberos-based

- Initial sign-on prompts the user for credentials, and gets a Kerberos ticket-granting ticket (TGT).
- Additional software applications requiring authentication, such as email clients, wikis, and revision-control systems, use the ticket-granting ticket to acquire service tickets, proving the user's identity to the mail-server / wiki server / etc. without prompting the user to re-enter credentials.

Windows environment - Windows login fetches TGT. Active Directory-aware applications fetch service tickets, so the user is not prompted to re-authenticate.

Unix/Linux environment - Login via Kerberos PAM modules fetches TGT. Kerberized client applications such as Evolution, Firefox, and SVN use service tickets, so the user is not prompted to re-authenticate.

Smart-card-based

Initial sign-on prompts the user for the smart card. Additional software applications also use the smart card, without prompting the user to re-enter credentials. Smart-card-based single sign-on can either use certificates or passwords stored on the smart card.

Integrated Windows Authentication

Integrated Windows Authentication is a term associated with Microsoft products and refers to the SPNEGO, Kerberos, and NTLMSSP authentication protocols with respect to SSPI functionality introduced with Microsoft Windows 2000 and included with later Windows NT-based operating systems. The term is most commonly used to refer to the automatically authenticated connections between Microsoft Internet Information Services and Internet Explorer. Cross-platform Active Directory integration vendors have extended the Integrated Windows Authentication paradigm to Unix (including Mac) and Linux systems.

Security Assertion Markup Language

Security Assertion Markup Language (SAML) is an XML-based method for exchanging user security information between an SAML identity provider and a SAML service provider. SAML 2.0 supports W3C XML encryption and service-provider–initiated web browser single sign-on exchanges.[23] A user wielding a user agent (usually a web browser) is called the subject in SAML-based single sign-on. The user requests a web resource protected by a SAML service provider. The service provider, wishing to know the identity of the user, issues an authentication request to a SAML identity provider through the user agent. The identity provider is the one that provides the user credentials. The service provider trusts the user information from the identity provider to provide access to its services or resources.

Emerging configurations

Mobile devices as access credentials

A newer variation of single-sign-on authentication has been developed using mobile devices as access credentials. Users' mobile devices can be used to automatically log them onto multiple systems, such as building-access-control systems and computer systems, through the use of authentication methods which include OpenID Connect and SAML,[24] in conjunction with an X.509 ITU-T cryptography certificate used to identify the mobile device to an access server.

A mobile device is "something you have," as opposed to a password which is "something you know," or biometrics (fingerprint, retinal scan, facial recognition, etc.) which is "something you are." Security experts recommend using at least two out of these three factors (multi-factor authentication) for best protection.

See also

- Account pre-hijacking
- Central Authentication Service

- Identity management
- Identity management systems
- List of single sign-on implementations
- Password manager
- Security Assertion Markup Language
- Usability of web authentication systems

References

1. "What's the Difference b/w SSO (Single Sign On) & LDAP?" (https://jumpcloud.com/blog/sso-vs-ldap). *JumpCloud*. 2019-05-14. Retrieved 2020-10-27.
2. "SSO and LDAP Authentication" (https://archive.today/20140523114521/http://www.authenticationworld.com/Single-Sign-On-Authentication/SSOandLDAP.html). Authenticationworld.com. Archived from the original (http://www.authenticationworld.com/Single-Sign-On-Authentication/SSOandLDAP.html) on 2014-05-23. Retrieved 2014-05-23.
3. "OpenID versus Single-Sign-On Server" (http://alleged.org.uk/pdc/2007/08/13.html). alleged.org.uk. 2007-08-13. Retrieved 2014-05-23.
4. "OpenID Connect Provider - OpenID Connect Single Sign-On (SSO) - OIDC OAuth Authentication" (https://www.onelogin.com/pages/openid-connect). *OneLogin*.
5. "Single sign-on and federated authentication" (https://kb.iu.edu/d/bbrl). *kb.iu.edu*.
6. "Benefits of SSO" (https://www.uoguelph.ca/ccs/security/internet/single-sign-sso/benefits). University of Guelph. Retrieved 2014-05-23.
7. "Single Sign On Authentication" (https://archive.today/20140315095827/http://www.authenticationworld.com/Single-Sign-On-Authentication/). Authenticationworld.com. Archived from the original (http://www.authenticationworld.com/Single-Sign-On-Authentication/) on 2014-03-15. Retrieved 2013-05-28.
8. "Sun GlassFish Enterprise Server v2.1.1 High Availability Administration Guide" (http://docs.oracle.com/cd/E19879-01/821-0182/abdln/index.html). Oracle.com. Retrieved 2013-05-28.
9. Laurenson, Lydia (3 May 2014). "The Censorship Effect" (https://web.archive.org/web/20200807161234/https://techcrunch.com/2014/05/03/business-and-censorship/). *TechCrunch*. Archived from the original (https://techcrunch.com/2014/05/03/business-and-censorship/) on August 7, 2020. Retrieved 27 February 2015.
10. Chester, Ken (12 August 2013). "Censorship, external authentication, and other social media lessons from China's Great Firewall" (https://web.archive.org/web/20140326175137/http://www.techinasia.com/china-social-media-lessons-from-great-firewall/). *Tech in Asia*. Archived from the original (https://www.techinasia.com/china-social-media-lessons-from-great-firewall/) on March 26, 2014. Retrieved 9 March 2016.
11. Wang, Rui; Chen, Shuo; Wang, XiaoFeng (2012). "Signing Me onto Your Accounts through Facebook and Google: A Traffic-Guided Security Study of Commercially Deployed Single-Sign-On Web Services" (https://ieeexplore.ieee.org/document/6234424). *2012 IEEE Symposium on Security and Privacy*: 365–379. doi:10.1109/SP.2012.30 (https://doi.org/10.1109%2FSP.2012.30). ISBN 978-1-4673-1244-8. S2CID 1679661 (https://api.semanticscholar.org/CorpusID:1679661).
12. "OpenID: Vulnerability report, Data confusion" (http://openid.net/2012/03/14/vulnerability-report-data-confusion/) - OpenID Foundation, March 14, 2012
13. "Facebook, Google Users Threatened by New Security Flaw" (http://www.tomsguide.com/us/facebook-google-covert-redirect-flaw,news-18726.html). Tom's Guide. 2 May 2014. Retrieved 11 November 2014.

14. "Covert Redirect Vulnerability Related to OAuth 2.0 and OpenID" (http://tetraph.com/covert_redirect/oauth2_openid_covert_redirect.html). Tetraph. 1 May 2014. Retrieved 10 November 2014.
15. "Math student detects OAuth, OpenID security vulnerability" (http://techxplore.com/news/2014-05-math-student-oauth-openid-vulnerability.html). Tech Xplore. 3 May 2014. Retrieved 10 November 2014.
16. "Facebook, Google Users Threatened by New Security Flaw" (https://news.yahoo.com/facebook-google-users-threatened-security-192547549.html). Yahoo. 2 May 2014. Retrieved 10 November 2014.
17. "Covert Redirect Flaw in OAuth is Not the Next Heartbleed" (http://www.symantec.com/connect/blogs/covert-redirect-flaw-oauth-not-next-heartbleed). Symantec. 3 May 2014. Retrieved 10 November 2014.
18. "VMware Flaw a Vector in SolarWinds Breach? — Krebs on Security" (https://krebsonsecurity.com/2020/12/vmware-flaw-a-vector-in-solarwinds-breach/).
19. Kovacs, Eduard. "Group Behind SolarWinds Hack Bypassed MFA to Access Emails at US Think Tank" (https://www.securityweek.com/group-behind-solarwinds-hack-bypassed-mfa-access-emails-us-think-tank). *Security Week*. Security Week. Retrieved 19 December 2020.
20. "What Is Session Hijacking?" (https://www.netsparker.com/blog/web-security/session-hijacking/). 22 August 2019.
21. MIT IST. "OpenID Connect Authorization" (https://ist.mit.edu/oidc).
22. Goode, Lauren (2019-06-15). "App Makers Are Mixed on 'Sign In With Apple' " (https://www.wired.com/story/sign-in-with-apple-mixed-reactions/). *Wired*. ISSN 1059-1028 (https://www.worldcat.org/issn/1059-1028). Retrieved 2019-06-15.
23. Armando, Alessandro; Carbone, Roberto; Compagna, Luca; Cuéllar, Jorge; Pellegrino, Giancarlo; Sorniotti, Alessandro (2013-03-01). "An authentication flaw in browser-based Single Sign-On protocols: Impact and remediations" (https://linkinghub.elsevier.com/retrieve/pii/S0167404812001356). *Computers & Security*. **33**: 41–58. doi:10.1016/j.cose.2012.08.007 (https://doi.org/10.1016%2Fj.cose.2012.08.007).
24. "MicroStrategy's office of the future includes mobile identity and cybersecurity" (https://www.washingtonpost.com/business/capitalbusiness/microstrategys-office-of-the-future-includes-mobile-identity-and-cybersecurity/2013/04/13/eb82e074-a1e3-11e2-be47-b44febada3a8_story.html). *The Washington Post*. 2014-04-14. Retrieved 2014-03-30.

External links

- Single sign-on intro with diagrams (https://pubs.opengroup.org/onlinepubs/008329799/chap1.htm)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Single_sign-on&oldid=1156602271"