Access Controls: Single Sign-On (SSO)

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

CYSE 300 – Introduction to Cybersecurity

October 05, 2025

Instructions:

(1) What are the benefits and risks of the use of SSO?

(2) Specify measures that can be taken to better secure an SSO system.

Access Controls: Single Sign-On (SSO)

Single Sign-On (SSO) is a method of access that enables users to securely log in to multiple devices, applications, and websites using a single set of credentials (e.g., a username and password). The purpose of SSO is to streamline and reduce administrative login credential management or overhead without sacrificing security (Kim & Solomon, 2021).

Benefits of Using SSO (Cloudflare, 2025)

1. **Improved User Experience:** Users only need to remember one password or set of credentials to log in and access all their work-related apps. Remembering one set of complex credentials is more convenient and efficient (i.e., fewer human errors) for a user than remembering multiple complex credentials.
2. **Enhanced Security:** Centralized authentication allows for tighter security controls over an organization's environment. It is simpler to enforce strong passwords and multi-factor authentication (MFA) at a single point of entry rather than across dozens of different applications that use various authentication methods and login credentials. Applying account login thresholds and lockouts after multiple failed attempts is an added and ideal feature to prevent unauthorized login attempts as an effective technical "failsafe" feature.
3. **Simplified Administration:** Administrators can manage user access from a single location. For example, when an employee joins or leaves the company, their access to all integrated applications can be granted or revoked in a single step. Centralization reduces the complexity of tracking devices and user accounts, thereby reducing the risk of unauthorized access to hardware and company data from insider threats and former employees.

Risks of Using SSO (Yambari, 2022)

1. **Single Point of Failure:** If an attacker compromises a user's SSO credentials, they typically gain access to all applications connected to it. That leads to a "one key to rule them all" scenario. Also, suppose there is a bug or vulnerability in an automation coding script. In that case, an attacker may exploit it by applying different approaches to "wedge" themselves into the secure network (i.e., injection attacks against SQL databases or within host Command Lines, cross-site scripting (XSS)).
2. **Difficult to Implement:** Implementing SSO is typically complex and costly for most organizations, especially when integrating with unique computer systems, legacy devices, and networks. The ability to organize and unify all networks under a single "umbrella" platform can prove too demanding or inefficient for some institutions.
3. **Provider Outage:** If the SSO service provider (e.g., Okta, Google, or Microsoft) experiences an outage, the outage can lock all users out of all their connected applications, bringing production to a halt until the service provider is back online.

Measures to Secure an SSO System

1. **Multi-Factor Authentication (MFA):** Layering network security by requiring users to provide at least one more form of verification (e.g., a software code from a phone app or a physical security key) in addition to a complex password makes it harder for attackers to gain unauthorized access to sensitive data. Multiple forms of authentication are preferable to relying on a single SSO password.
2. **Strong Password Policies:** Enforce complex password requirements with reuse or recycle restrictions for a user's master SSO password, preventing the use of easily guessable or previously breached passwords by threat actors performing Brute-Force attacks using Dictionaries and Rainbow Tables.
3. **Principle of Least Privilege:** Use Role-Based Access Control (RBAC) and network segmentation to ensure that users are only granted access to the applications and data they absolutely need to perform their jobs.
4. **User Training:** Educate users on how to identify and report phishing attempts, which are often designed to steal SSO credentials using fake login pages, captive portals, and keyloggers.
5. **Regular Monitoring and Auditing:** Organizations should regularly monitor their users' login activity for any suspicious or anomalous behavior to identify and mitigate potential threats quickly. Examples of such anomalies include login attempts from unexpected geographic locations and unusual times of day (e.g., after normal business or work hours for the location or outside the employee/user's normal working hours).

References

Cloudflare. (2025, September 2). *What is SSO? | How single sign-on works*. Cloudflare. Retrieved September 30, 2025, from https://www.cloudflare.com/learning/access-management/what-is-sso/

Kim, D., & Solomon, M. G. (2021). Fundamentals of information systems security (4th ed.). Jones & Bartlett Learning.

Yambari, C. (2022, March 14). *The 5 big security risks of single sign-on (SSO)*. Zluri. Retrieved September 30, 2025, from https://www.zluri.com/blog/sso-security-risks