The rise of SSO and MFA

Most companies help keep their data safely locked up behind authentication systems. Usernames and passwords are the keys that unlock information for most organizations. But are those credentials enough? Information security often focuses on managing a user's access of, and authorization to, information.

Previously, you learned about the three factors of authentication: knowledge, ownership, and characteristic. Single sign-on (SSO) and multi-factor authentication (MFA) are two technologies that have become popular for implementing these authentication factors. In this reading, you'll learn how these technologies work and why companies are adopting them.

A better approach to authentication

Single sign-on (SSO) is a technology that combines several different logins into one. More companies are turning to SSO as a solution to their authentication needs for three reasons:

1. **SSO improves the user experience** by eliminating the number of usernames and passwords people have to remember.
2. **Companies can lower costs** by streamlining how they manage connected services.
3. **SSO improves overall security** by reducing the number of access points attackers can target.

This technology became available in the mid-1990s as a way to combat *password fatigue*, which refers to people's tendency to reuse passwords across services. Remembering many different passwords can be a challenge, but using the same password repeatedly is a major security risk. SSO solves this dilemma by shifting the burden of authentication away from the user.

How SSO works

SSO works by automating how trust is established between a user and a service provider. Rather than placing the responsibility on an employee or customer, SSO solutions use trusted third-parties to prove that a user is who they claim to be. This is done through the exchange of encrypted access tokens between the identity provider and the service provider.

Similar to other kinds of digital information, these access tokens are exchanged using specific protocols. SSO implementations commonly rely on two different authentication protocols: LDAP and SAML. LDAP, which stands for Lightweight Directory Access Protocol, is mostly used to transmit information on-premises; SAML, which stands for Security Assertion Markup Language, is mostly used to transmit information off-premises, like in the cloud.

Note: LDAP and SAML protocols are often used together.

Here's an example of how SSO can connect a user to multiple applications with one access token:
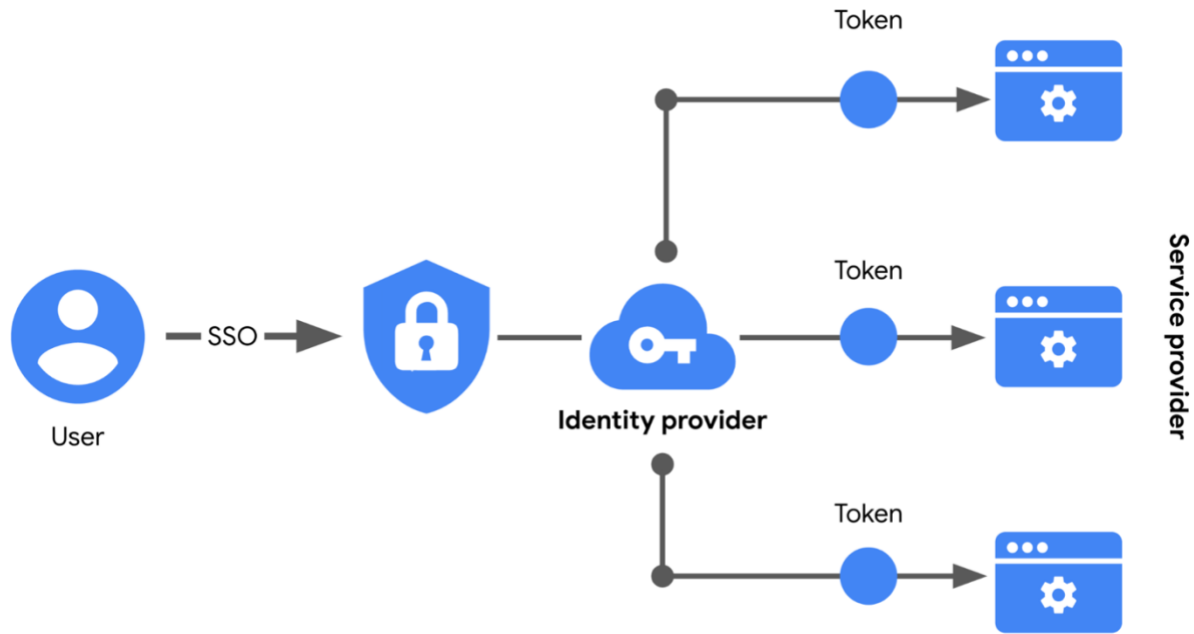
Limitations of SSO

Usernames and passwords alone are not always the most secure way of protecting sensitive information. SSO provides useful benefits, but there's still the risk associated with using one form of authentication. For example, a lost or stolen password could expose information across multiple services. Thankfully, there's a solution to this problem.

MFA to the rescue

Multi-factor authentication (MFA) requires a user to verify their identity in two or more ways to access a system or network. In a sense, MFA is similar to using an ATM to withdraw money from your bank account. First, you insert a debit card into the machine as one form of identification. Then, you enter your PIN number as a second form of identification. Combined, both steps, or factors, are used to verify your identity before authorizing you to access the account.

Strengthening authentication

MFA builds on the benefits of SSO. It works by having users prove that they are who they claim to be. The user must provide two factors (2FA) or three factors (3FA) to authenticate their identification. The MFA process asks users to provide these proofs, such as:

- **Something a user knows:** most commonly a username and password
- **Something a user has:** normally received from a service provider, like a one-time passcode (OTP) sent via SMS
- **Something a user is:** refers to physical characteristics of a user, like their fingerprints or facial scans

Requiring multiple forms of identification is an effective security measure, especially in cloud environments. It can be difficult for businesses in the cloud to ensure that the users remotely accessing their systems are not threat actors. MFA can reduce the risk of authenticating the wrong users by requiring forms of identification that are difficult to imitate or brute force.

Key takeaways

Implementing both SSO and MFA security controls improves security without sacrificing the user experience. Relying on passwords alone is a serious vulnerability. Implementing SSO means fewer points of entry, but that's not enough. Combining SSO and MFA can be an effective way to protect information, so that users have a streamlined experience while unauthorized people are kept away from important information.

Mark as completed