International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 09 | Sep 2020 www.irjet.net p-ISSN: 2395-0072

Security in SSO

Pritha Maurya[1], Prof. Vaishali Gatty[2]

[1]PG Student, Dept. of MCA, Vivekanand Education Society's Institute of Technology, Mumbai, India.
[2]Assistant professor, Dept. of MCA, Vivekanand Education Society's Institute of Technology, Mumbai, India

---

Abstract - *Single sign-on (SSO) is a centralized user authentication and session service in which one set of login credentials can be used to access multiple applications. [1] Single sign-on (SSO) is an important element in the complex structure of an effective security program. It is a service that gives a user access to multiple network destinations by entering only one username, one login and one password. It simplifies the login process streamlines workflow and adds a layer of safety by reducing the likelihood of error. For example, if a user typically accesses two or more applications during a work session, going through multiple login routines multiplies the possibility of mistakes which consumes more time. While SSO enhances ease of access, however it also presents some risk.*

For example, there are many applications and websites that provide the option to login with your google, google+ and Facebook accounts. The user does not have to register for a new account for each website. Which makes the process easy and it saves a lot of time too but there comes so many security risks with that single click.

Key Words: Authentication, Security risks, Single sign-on, phishing, data breaching

1. INTRODUCTION

Without SSO how does authentication works?

Each website maintains its own database of users and user credentials.

1. Website checks if you have already been authenticated. If you are already authenticated it gives you the access of their site.
2. If you are not authenticated then it checks your username and password in their database.
3. The site passes the authentication data to verify that you are authenticated every time you go to the new page after you login.[9]

Figure 1- Without SSO authentication [8]

How does authentication work with SSO?

Web development teams usually face one problem during implementing the SSO. You have developed a website or application at one domain D1 and now you want to deploy on a new domain D2 to use the same login details or information as the other domain. Or you want users who are already registered and logged in at domain D1 to be already logged in at domain D2.
So, this is solved by sharing the session information across different domains. And for its security, browsers enforce a "same origin policy". The same origin policy dictates that cookies and other stored local data can be accessed by its creator or user only.
There are many SSO protocols and different SSO protocols share session information in different ways. But the concept is the same which is the central domain through which authentication process is performed and then session is shared between domains.

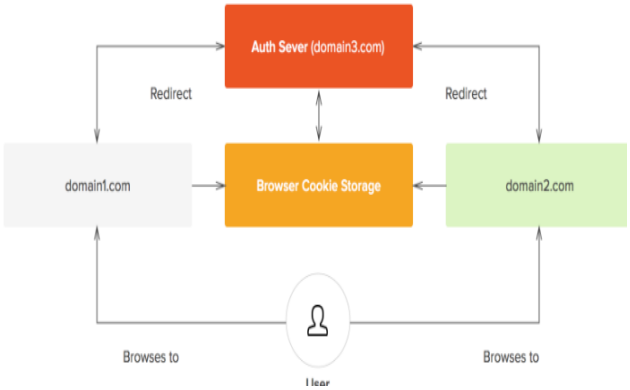

Figure 2- Using a central authentication domain [7]

Whenever users go to a domain that requires authentication, they are redirected to the authentication domain. As users are already logged-in at that domain, they can be immediately redirected to the original domain with the necessary authentication token.

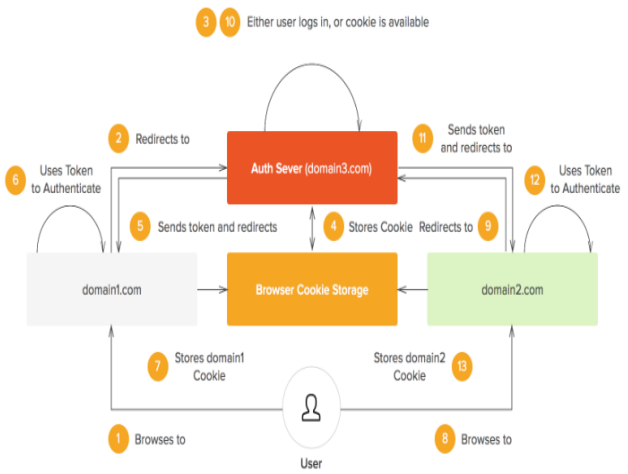

Figure 3- TYPICAL SSO [7]

2. Advantages of SSO:

1. **Reduces hassle of remembering passwords**: Remembering one password instead of many makes users' lives easier. As a tangential benefit, it gives users greater incentive to come up with strong passwords.
2. **Management of username and password is made easy**: When changes of personnel take place, SSO reduces both IT effort and opportunities for mistakes. Employees leaving the organization relinquish their login privileges.
3. **Improves user security:** With SSO, companies can strengthen identity security with techniques such as two-factor authentication (2FA) and multifactor authentication (MFA).
4. **Saves Time:** In settings such as hospitals, defence industries, and emergency services, where large numbers of people and departments demand rapid and unfettered access to the same applications, SSO is especially helpful. In such cases, preventing errors and malware intrusion can be the difference between life and death.
5. **Reduces Workload**: Fewer users calling for help with lost passwords saves money and improves security. Security risks are reduced for your customers, vendors, and partner entities. Connections between allied companies always present vulnerabilities, which SSO can reduce.
6. **Easy to integrate:** There is no reason for any organization to create its own system or to develop deep SSO expertise.[3]

3. SSO's challenges:

1. **Password policies:** Other accounts under the same authentication can also be endangered, if an SSO account is cracked.

When an SSO is down, the access to its all connected sites are also stopped. This is a big reason to exercise great care in choosing an SSO system. The SSO system must be exceptionally reliable and there should be plans for dealing with breakdowns and other security risks.

SSO get affected too, when your identity provider goes down. The identity provider's vulnerability to any kind of interruption becomes the user's vulnerability as well, and it is mostly beyond user's control. This is why the choice of vendors is critical. Extra-strong passwords must be enforced.[3]

If a hacker cracks your identity provider user account, all linked systems to it could be open to attack. This will become classic single point of failure and should be headed off in the planning process. High quality identity providers have top-notch security on the plus side.

SSO is risky for multi-user computers. What happens when one user is logged in and another needs to use the machine? To accommodate different levels of access, reduced sign-on (RSO) may be needed. Additional authentication servers may be required with reduced sign-on.

Using SSO for social networking services can encounter many problems. Some workplaces have censorship where the government connections and social media sites are blocked.

There are some SSO-linked sites who may give their user data to third party entities. This is an area requiring careful attention.

An SSO can take plenty of time to set up than expected. Each environment is different, so added steps in implementation can crop up. One example is the task linking the identity provider to the service provider.

2. **Instant Access to More Than Just the Endpoint:**

User credentials are a major focus for external attackers (81% of data breaches involve credential misuse). Once a malicious user has prime access to an authenticated SSO account, they automatically have access to all linked data sets, applications, systems and environments the authenticated user is provisioned for. Most SSO environments leverage a portal of some kind that facilitates access without requiring additional passwords. It is user friendly for sure but on the other hand it's dreadful for security.

External attacks using malware to govern over an endpoint would have post-logon access to everything connected via SSO immediately after infection, increasing an attacker's footprint within the organization.[3]

3. Less-Than-Perfect Control over Access Once Granted:

When a user has successfully logged on via SSO and is granted access to other external applications too in the cloud. Then the user falls prey to a phishing attack, giving an attacker access to the endpoint. The account certainly can be disabled if it's detected but the way Windows works, the user remains logged on and it is possible for the attacker to remain logged on with access to a given application, depending on the SSO solution in place and the linked application's security model.[2]

4. Little-to-No Adherence to the Principle of Least Privilege:

The principle of least privilege dictates that users should have access to the minimum data, applications and systems necessary to do their job, and usually involves requiring separate credentials for elevated access. It runs contrary to the idea of requiring the user to authenticate each and every time they need to access something new because SSO is all about giving users access with a single authentication. And humans do like the easy access to everything. Organizations like the benefit of the improvement in productivity and reduction in support costs even if there are risks. [2]

4. CONCLUSIONS

It is quite possible for an SSO server to get hacked or breached, which may lead to data loss. It has major risk of phishing attack. Furthermore, all of the crucial and confidential data of a user may get compromised in just a single shot, as all of the authentication credentials are in the same basket and the key to the basket may get revealed if the coupled usage of SSO and MFA is not implemented. Thus, it cannot be considered a total security tool. Sharing of user data with a third party is another underlying factor which enhances the risk factor of SSO usage. In order to cover a good portion of potential users, the right choice of Identity provider is vital. Hence, the disadvantages of relying on a third party is overwhelming and needs to be addressed to minimize the risk factor involved in SSO.

REFERENCES

[1] DougDrinkwater experienced technology and security journalist 2018 "What is single sign-on? How SSO improves security and the user experience. Password fatigue, cloud sprawl and developer simplicity are pushing the rise of SSO." https://www.csoonline.com/article/2115776/what-is-single-sign-on-how-sso-improves-security-and-the-user-experience.html

[2] Verizon, Data Breach Investigations Report (2017) https://www.isdecisions.com/single-sign-on-active-directory-security-issues/

[3] The Pros and Cons to Single Sign-On (SSO) By RenovoData https://www.renovodata.com/blog/2019/01/17/single-sign-on

[4] Li, B., Ge, S., Wo, T. Y. and Ma, D.F. 2004. Research and Implementation of Single Sign-On Mechanism for ASP Pattern. In Proceedings of the Third International Conference on Grid and Cooperative Computing.

[5] Villanueva, J. 2014 "5 Big Business Benefits of Using SSO (Single Sign-On)" Managed File Transfer and Network Solutions.

[6] Davis, M. 2013 "The Pros And Cons Of Single Sign-On for Web Services", Future Hosting, [Online] https://www.futurehosting.com/blog/the-pros-and-consof-single-sign-on-for-web-services/

[7] "Why Federated Identity Management Matters" by Martin Gontovonikas, 2016 https://auth0.com/blog/why-identity-federation-matters/

[8] "How does single sign-on works", onelogin https://www.onelogin.com/learn/how-single-sign-on-works