Technological Institute of the Philippines
Manila Campus
CBS402A – Data and Application Security

Name	Sharmaine R. Panayas
Section	IT32S2

Intended Learning Outcomes

At the end of the laboratory, the student is expected to:

1. Learn what is SSO.
2. Identify the different types of SSO.
3. Explain the flow of an SSO.

Instructions

1. Do not change the format.
2. Put your answers in the spaces provided for each question.
3. Make sure to add references in APA format. At least 3 references for this activity.
4. Filename upon submission: Lab1_Lastname_Firstname.pdf

Activity

1. What is a single sign-on?

   Single sign-on (SSO) uses one set of credentials such as username and password to login to multiple applications and websites. This type of authentication service is commonly used by businesses and organization to ease the management on managing many login credentials.

   An example of Single sign-on (SSO) is that if a user logs in using their Google Account, automatically they will be signed into other applications that Google is linked to such as Gmail, Google Drive, and YouTube.

2. Describe the process or flow of SSO

   Single sign-on works when a user sign into a website or application which is known as the Service Provider, that service will generate an authentication token that will serve as an identification and verification of the user, which contains some of the user’s information such as email. The authentication token of the user will be stored on either the user’s browser or within the SSO service's servers. The SSO service will pass the authentication token of the user to the application or website that the user will sign in to. And if the token is validated, the user will be granted an access to the Service Provider.

   If the user has not yet signed in, they will be prompted to do so by providing the credentials needed by the SSO Service.

3. What are the different types of SSO?
   The types of SSO are Federated Identity Management (FIM), OAuth (specifically OAuth 2.0 nowadays), OpenID Connect (OIDC), and Security Access Markup Language (SAML).

   - **Federated Identity Management (FIM)** refers to the created trust relationship between two or more domains. Single sign-on is a part of FIM architecture, it is a feature of it.

   - **OAuth (Open Authorization)** is also a framework within the FIM architecture, its focus is on the trusted relationship that allows user identification information to be transferred or shared between domains.

   - **OpenID Connect (OIDC)** is an authentication mechanism that allows the clients to utilize authentication through an authorization server to validate an end user's identity. It is developed on OAuth 2.0 to provide Single Sign-on mechanism.

   - **Security Access Markup Language (SAML)** is a protocol that enables the exchange of user authentication and authorization data within secure domains.

4. Is SSO good or bad? Reflect on your answer based on our discussion regarding authentication where best practices say we maintain different passwords in each of our accounts.

   For me Single sign-on (SSO) is not good for a standard user like me but when it comes to business environments, using SSO is suitable since it will lessen the complaints of the employee regarding credential issues such as passwords and it is an advantage for the IT help desks. For a student like me it is preferable to have different passwords in different accounts, my personal account and school account has different passwords.

   Having the same credentials in multiple applications is risky, if the user forgot their username and password or if they got locked out, they will not have access to their accounts that is linked to the SSO. For example, in Google account if you forgot your password or your account has been locked, you cannot access other google related applications such as Gmail and Google Meet, it also applies when you use your social media accounts such as Facebook and Twitter to sign to an application or website. Another negative thing about SSO is that if an attacker got your credentials, they could also have access to other applications that is linked to that account.

   In conclusion, using SSO has an advantage to an enterprise and employees since on what I have stated, it will lessen the account credential complaints which lowers the IT costs, and it will improve the usability and satisfaction of employees. However, for a standard user it is not required to use SSO, for me having different passwords for multiple accounts will prevent my account to be hacked. Also add extra layer of protection such as OTP and email verification, always follow the best practices to avoid attackers and unauthorized users from accessing your accounts.

References

How Does Single Sign-On (SSO) Work? | OneLogin. (n.d.). One Login.
https://www.onelogin.com/learn/how-single-sign-on-works

Teravainen, T. (2020, April 16). *single sign-on (SSO)*. SearchSecurity.
https://www.techtarget.com/searchsecurity/definition/single-sign-on

What is SSO? | How single sign-on works. (n.d.). Cloudflare.
https://www.cloudflare.com/learning/access-management/what-is-sso/

Honor Pledge:

"I affirm that I have not given or received any unauthorized help on this assignment and that this work is my own."

Panayas, Sharmaine R.