Single Sign-On with Multifactor Auth Via SAML and Navigate Multiple Systems

Gaurav Rohatgi
Sr Engineer (MCA)
43863 Hibiscus Drive Ashburn VA 20147

ABSTRACT

Single Sign-On (SSO) is a popular authentication mechanism used by organizations to provide users with seamless access to multiple applications using a single set of credentials. However, SSO systems are vulnerable to various security threats, such as phishing, man-in-the-middle (MITM) attacks, and password theft. To address these risks, it is essential to implement robust security measures, such as multiple authentication methods, to enhance the security of SSO systems. This research paper proposes a comprehensive solution for improving the security of SSO systems by using multiple authentication methods with Security Assertion Markup Language (SAML).

General Terms

Security, Authorization

Keywords

Single Sign-On, SSO, SAML

1. INTRODUCTION

Single Sign-On (SSO) is an authentication mechanism that enables users to access multiple applications using a single set of credentials. The primary benefits of SSO systems include increased convenience, productivity, and user satisfaction. However, SSO systems are exposed to various security risks, such as identity spoofing, replay attacks, and session hijacking. These vulnerabilities can be exploited by malicious actors to gain unauthorized access to sensitive data and systems. To mitigate these risks, it is essential to employ robust security measures that incorporate multiple authentication methods. Multiple authentication methods provide an additional layer of security that can significantly reduce the risk of unauthorized access. Multi-factor authentication (MFA) has gained significant attention in recent years as a means of enhancing security in digital systems (Dasgupta, Roy, & Nag, 2017). Furthermore, the use of SAML as a protocol for exchanging authentication and authorization data between parties can enhance the security of SSO systems.

2. SOLUTION

Our proposed solution involves the use of multiple authentication methods, such as username/password, smart card, biometric, and one-time passwords (OTP). These methods can be combined to provide stronger authentication for SSO systems. One aspect closely related to MFA is the concept of Single Sign-On (SSO) architectures, which aim to streamline user authentication processes across multiple applications (De Clercq, 2002). Additionally, we propose the use of SAML as the protocol for exchanging authentication and authorization data between the identity provider (IdP) and the service provider (SP). The proposed solution includes the following steps (see Figure 1)

1. The user initiates the authentication process by accessing an application that is part of the SSO system.
2. The application redirects the user to the IdP for authentication.
3. The IdP authenticates the user using one or more authentication methods like (OTP, Email, Phone App, Security Tokens etc)
4. Then IdP generates a SAML assertion that includes the user's identity information and authentication status.
5. The IdP sends the SAML assertion to the application.
6. The application verifies the SAML assertion and grants access to the user.
7. The user may navigate between the application and before providing the SAML assertions attributes to another app – it may or may not ask the MFA again.

3. IMPACT

Our proposed solution provides several benefits over traditional SSO systems:

3.1 Enhanced security: The use of multiple authentication methods provides stronger authentication for SSO systems, making them more resilient to security threats.

3.2 Flexibility: The use of multiple authentication methods gives users the flexibility to choose the authentication method that best suits their needs.

3.3 Usability: The use of SAML simplifies the authentication process for users, as they only need to provide their credentials once to access multiple applications.

4. USAGE

There are multiple usages for Multiple Authentication:

1. Company Portal Access with SSO & SAML with Multiple Authentication
2. Financial Industries Logins & Transactions
3. Sensitive/Confidential Data Access & Modifications.

5. WORKFLOW

Below is the workflow for MFA with SSO

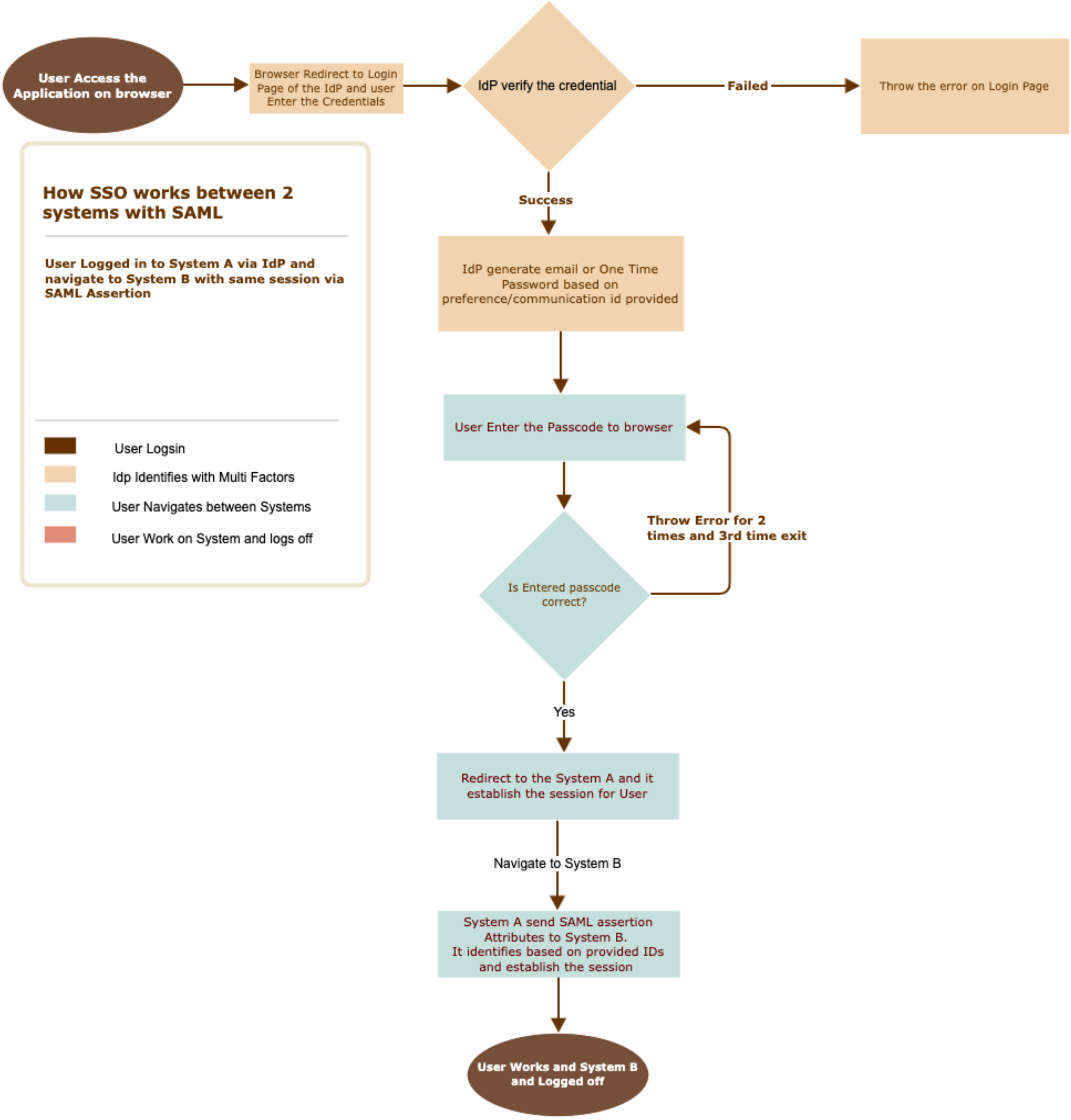
User Access the Application on browser
Browser Redirect to Login Page of the IdP and user Enter the Credentials
IdP verify the credential
Failed
Throw the error on Login Page
How SSO works between 2 systems with SAML
User Logged in to System A via IdP and navigate to System B with same session via SAML Assertion
User Logsin
Idp Identifies with Multi Factors
User Navigates between Systems
User Work on System and logs off
Success
IdP generate email or One Time Password based on preference/communication id provided
User Enter the Passcode to browser
Throw Error for 2 times and 3rd time exit
Is Entered passcode correct?
Yes
Redirect to the System A and it establish the session for User
Navigate to System B
System A send SAML assertion Attributes to System B. It identifies based on provided IDs and establish the session
User Works and System B and Logged off

Figure 1

6. SCOPE

It can be implemented for any Authentication Mechanism.

7. CONCLUSION

In conclusion, our research proposes a comprehensive solution for enhancing the security of SSO systems by using multiple authentication methods with SAML. The proposed solution provides enhanced security, flexibility, and usability for SSO systems. Further research can be done to evaluate the effectiveness of the proposed solution in real-world scenarios. By implementing the proposed solution, organizations can significantly reduce the risk of unauthorized access to sensitive data and systems, thereby ensuring the confidential reference and availability of their resources. The future scope of Single Sign-On (SSO) coupled with Multi-Factor Authentication (MFA) using the Security Assertion Markup Language (SAML) holds immense potential for advancing security, user experience, and interoperability in digital authentication systems.

8. REFERENCES

[1] Dasgupta, D., Roy, A., & Nag, A. K. (2017). Multi-Factor Authentication. In *Infosys science foundation series* (pp. 185–233). https://doi.org/10.1007/978-3-319-58808-7_5

[2] De Clercq, J. (2002). Single Sign-On Architectures. In *Lecture Notes in Computer Science* (pp. 40–58). https://doi.org/10.1007/3-540-45831-x_4

[3] Wilson, Y., & Hingnikar, A. (2019). SAML 2.0. *Apress eBooks*, 99–111. https://doi.org/10.1007/978-1-4842-5095-2_7