Erick Llanos Ríos

Informe sobre SSO y SAML

03/02/2023

Índice

Introducción

El Single Sign-On (SSO) y el Security Assertion Markup Language (SAML) son tecnologías de autenticación y autorización que tienen como objetivo facilitar el acceso de los usuarios a diferentes aplicaciones y servicios en línea. En el mundo digital actual, los usuarios a menudo tienen que administrar muchas credenciales diferentes para acceder a diferentes aplicaciones y servicios en línea, lo que puede ser un proceso tedioso y propenso a errores. SSO y SAML buscan resolver este problema al permitir que los usuarios accedan a múltiples aplicaciones y servicios con una sola credencial.

El SSO es una técnica que permite a los usuarios iniciar sesión en un sistema centralizado y, a partir de allí, acceder a diferentes aplicaciones y servicios sin tener que proporcionar credenciales adicionales. SAML es un protocolo de autenticación que permite la interacción segura entre diferentes aplicaciones y servicios, lo que permite una experiencia de SSO sin interrupciones para los usuarios.

Este informe brindará una descripción detallada de SSO y SAML, así como un análisis de su implementación y relación con los desarrolladores y programadores. Además, se presentará una conclusión sobre la importancia y las implicaciones de estas tecnologías en la autenticación y autorización en línea. En resumen, este informe proporcionará una comprensión completa y profunda de SSO y SAML y su impacto en la seguridad y la experiencia de usuario en línea.

Descripción

¿Qué es SSO y SAML?

Single Sign-On (SSO)

Significa ‘inicio de sesión único’, ‘unificado’ o ‘autenticación única’. SSO es un procedimiento de autenticación donde se habilita al usuario para que pueda acceder a múltiples sistemas, recursos o aplicaciones con una sola identificación en base a un único "usuario" y "contraseña". Esto facilita y agiliza el inicio de sesión de los usuarios, lo que permite aumentar la comodidad en el uso de los recursos electrónicos.

Security Assertion Markup Language (SAML)

SAML (Lenguaje de Marcado para Confirmaciones de Seguridad) es un estándar abierto que permite intercambiar información de autenticación y autorización entre sistemas. Es ampliamente utilizado para implementar SSO (Single Sign-On) en entornos empresariales. Con SAML, un proveedor de identidad (IdP) puede emitir afirmaciones sobre el usuario y enviarlas a un proveedor de servicio (SP) para que el usuario pueda acceder a los servicios del SP. Estas afirmaciones pueden incluir información como el nombre de usuario, el nombre completo del usuario, el estado de la sesión y los roles o grupos a los que el usuario pertenece.

Análisis

¿Cómo funciona SSO?

Cada vez que un usuario se registra en un servicio SSO, el servicio crea un token de autenticación que recuerda que el usuario está verificado. Un token de autenticación es una pieza de información digital almacenada en el navegador del usuario o en los servidores del servicio SSO, como una tarjeta de identificación temporal emitida al usuario. Cualquier aplicación a la que el usuario acceda se verificará con el servicio SSO. El servicio SSO pasa el token de autenticación del usuario a la aplicación y el usuario tiene entonces permiso para entrar. Sin embargo, si el usuario todavía no ha iniciado la sesión, se le pedirá que lo haga a través del servicio SSO.

Un servicio SSO no recuerda necesariamente quién es un usuario, ya que no almacena las identidades de los usuarios. La mayoría de los servicios SSO funcionan mediante la comprobación de las credenciales de los usuarios con un servicio de gestión de identidades independiente.

Pensemos que el SSO es como un intermediario que puede confirmar si las credenciales de inicio de sesión de un usuario coinciden con su identidad en la base de datos, sin gestionar ellos mismos la base de datos, algo así como cuando un bibliotecario busca un libro en nombre de otra persona basándose en el título del libro. El bibliotecario no tiene memorizado todo el catálogo de la biblioteca, pero puede acceder al mismo con facilidad.

Existen diferentes protocolos de SSO como SAML, OAuth2, OpenID Connect, entre otros. Cada uno de ellos tiene su propia forma de funcionar pero en general cumplen con el objetivo de SSO.

Existen varios beneficios para implementar SSO en una organización. En primer lugar, SSO mejora la seguridad, ya que los usuarios no están expuestos a la posibilidad de utilizar contraseñas débiles o compartirlas entre diferentes servicios. Además, SSO reduce los costos de administración de contraseñas y mejora la eficiencia, ya que los usuarios no tienen que recordar y gestionar varias contraseñas diferentes.

SSO también mejora la experiencia del usuario al permitirles acceder a los servicios que necesitan sin tener que iniciar sesión varias veces. Esto ayuda a aumentar la productividad y reduce la frustración del usuario.

Hay varias opciones disponibles para implementar SSO en una organización. Una de las opciones más populares es utilizar un proveedor de SSO de terceros, como Okta o OneLogin. Estos proveedores proporcionan una plataforma centralizada para gestionar los inicios de sesión de los usuarios y integrarse con diferentes sistemas y aplicaciones.

En resumen, SSO es una tecnología valiosa para mejorar la seguridad, eficiencia y experiencia del usuario en una organización. Existen varias opciones disponibles para implementar SSO, incluyendo proveedores de terceros y soluciones internas. Es importante evaluar las necesidades de la organización y seleccionar la opción adecuada para implementar SSO.

¿Cómo funcionan los tokens de autenticación del SSO?

La capacidad de pasar un token de autenticación a aplicaciones y servicios externos es fundamental en el proceso de SSO. Esto es lo que permite que la verificación de la identidad tenga lugar por separado de otros servicios en la nube, haciendo posible el SSO.

Piensa en un evento exclusivo al que solo pueden entrar unas pocas personas. Una forma de indicar que los guardias de la entrada al evento han comprobado y aprobado a un invitado es poniendo un sello en la mano de cada uno de ellos. El personal del evento puede comprobar los sellos de cada invitado para asegurarse de que está autorizado a estar allí. Sin embargo, no sirve cualquier sello; el personal del evento conocerá la forma y el color exactos del sello utilizado por los guardias de la entrada.

Al igual que cada sello tiene que tener el mismo aspecto, los tokens de autenticación tienen sus propios estándares de comunicación para garantizar que sean correctos y legítimos. El principal estándar de tokens de autenticación se llama SAML (Lenguaje de marcado para confirmaciones de seguridad). Al igual que las páginas web se escriben en HTML (Lenguaje de hipertexto de marcado), los tokens de autenticación se escriben en SAML.

SAML

SAML se basa en el intercambio de "assertiones" de seguridad entre un proveedor de identidad (IdP) y un proveedor de servicios (SP). Una vez que un usuario ha sido autenticado en el IdP, este emite una "assertión" que contiene información de autenticación y autorización. El SP, a su vez, valida la "assertión" para permitir el acceso a la aplicación o servicio.

SAML permite una autenticación segura y SSO sin que el usuario tenga que compartir sus credenciales con el SP. Además, SAML permite la interoperabilidad entre diferentes proveedores de identidad, lo que significa que un usuario puede acceder a diferentes aplicaciones y servicios con un único conjunto de credenciales.

SAML también permite la personalización de la autorización, ya que los atributos incluidos en la "assertion" pueden ser utilizados para determinar el nivel de acceso del usuario a una aplicación o servicio.

La implementación de SAML en una organización se puede realizar mediante el uso de un software de terceros o mediante el desarrollo de una solución personalizada. Existen varios proveedores de software que ofrecen soluciones de SAML listas para usar, como Okta o OneLogin. También existen bibliotecas de software libre como SAML2 int libraries, que permite a los desarrolladores implementar SAML en sus propias aplicaciones.

En conclusión, SAML es un estándar de seguridad abierto que permite la interoperabilidad entre sistemas de seguridad de diferentes proveedores. Permite una autenticación segura y SSO sin que el usuario tenga que compartir sus credenciales con el SP, y también permite la personalización de la autorización. La implementación de SAML puede ser realizada mediante el uso de un software de terceros o mediante el desarrollo de una solución personalizada.

¿Cómo funciona SAML?

Un proceso típico de autenticación de SSO involucra a estas tres partes:

- Principal (también conocido como el "sujeto")
- Proveedor de identidad
- Proveedor de servicios

Principal/sujeto: se trata casi siempre de un usuario humano que intenta acceder a una aplicación alojada en la nube.

Proveedor de identidad: un proveedor de identidad (IdP) es un servicio de software en la nube que almacena y confirma la identidad del usuario, normalmente a través de un proceso de inicio de sesión. Básicamente, el papel de un IdP es decir: "Conozco a esta persona y esto es lo que tiene permiso para hacer." Un sistema de SSO puede estar separado del IdP, pero en esos casos el SSO actúa esencialmente como representante del IdP, así que a todos los efectos son lo mismo en un flujo de trabajo SAML.

Proveedor de servicios: se trata de la aplicación o servicio alojado en la nube que el usuario desea utilizar. Algunos ejemplos típicos son las plataformas de correo electrónico en la nube, como Gmail y Microsoft Office 365, los servicios de almacenamiento en la nube, como Google Drive y AWS S3, y las aplicaciones de comunicación, como Slack y Skype. Normalmente, un usuario simplemente iniciaría sesión en estos servicios directamente, pero cuando se utiliza el SSO, el usuario inicia la sesión en el SSO, y se utiliza SAML para darle acceso, en lugar de utilizar un inicio de sesión directo.

Este es el aspecto de un flujo típico:

- El principal realiza una solicitud al proveedor de servicios. A continuación, el proveedor de servicios solicita la autenticación al proveedor de identidad. El proveedor de identidades envía una aserción SAML al proveedor de servicios, y el proveedor de servicios puede entonces enviar una respuesta al principal.
- Si el principal (el usuario) todavía no ha iniciado la sesión, el proveedor de identidad puede pedirle que inicie la sesión antes de enviarle una aserción SAML.

Para establecer un sistema de Single Sign-On (SSO) y Lenguaje de Marcado para Confirmaciones de Seguridad (SAML), se requiere tanto hardware como software específicos.

Hardware:

- Servidores: necesarios para procesar las solicitudes de autenticación y manejar la información de seguridad.
- Almacenamiento: para almacenar los datos de usuarios y configuraciones.

Software:

- Proveedor de identidad (IdP): encargado de autenticar a los usuarios y emitir tokens de seguridad.
- Servicios de aplicación (SP): destinatarios de las solicitudes de autenticación que usan los tokens emitidos por el IdP para autenticar al usuario.
- Metadatos del IdP: describen la configuración del IdP y se comparten con los SP para establecer una comunicación segura.
- Protocolo SAML: utilizado para el intercambio de información de seguridad entre el IdP y el SP.
- Software de gestión de identidades: para gestionar y administrar los usuarios y permisos en el sistema.

Estos componentes deben ser configurados y puestos en marcha para crear un sistema de SSO y SAML que brinde autenticación segura y cómoda para los usuarios.

Implementación

Para implementar SSO (Single Sign-On) y SAML (Security Assertion Markup Language), los programadores pueden seguir los siguientes pasos:

- Seleccionar un proveedor de identidad (IdP) y servicios de aplicación (SP) compatibles con el protocolo SAML.
- Configurar los servidores y el almacenamiento necesarios para el funcionamiento del sistema.
- Configurar el IdP y el SP para que trabajen juntos y establezcan una comunicación segura utilizando los metadatos del IdP.
- Configurar los usuarios y permisos en el software de gestión de identidades.
- Probar y depurar el sistema para asegurarse de que funcione correctamente.
- Pruebas: Finalmente, los programadores deben probar la implementación de SSO y SAML para asegurarse de que funcione correctamente y cumpla con sus requisitos de seguridad.

Relación del tema con el módulo

El inicio de sesión único (SSO) y el lenguaje de marcado de aserción de seguridad (SAML) son tecnologías utilizadas en el mundo de la programación para la autenticación y autorización.

SSO permite a los usuarios acceder a múltiples aplicaciones usando una sola cuenta sin tener que ingresar sus credenciales varias veces, mientras que SAML es un protocolo de seguridad que permite la autenticación y autorización de usuarios en sistemas distribuidos.

Al implementar los sistemas SSO y SAML, los desarrolladores deben trabajar para integrar los servicios de autenticación y autorización en las aplicaciones y los sistemas de administración de identidad. También deben tener conocimientos de lenguajes de programación, seguridad de la información y protocolos de comunicación para implementar adecuadamente estas tecnologías.

Los desarrolladores y programadores son clave para implementar SSO y SAML. Deben poder comprender y aplicar el estándar SAML para garantizar una implementación segura y eficiente. Además, deben comprender las posibles amenazas a la seguridad y cómo pueden mitigarse para garantizar la protección de datos y la privacidad del usuario.

Los desarrolladores también deben poder integrar SSO con aplicaciones y sistemas existentes, lo que puede requerir un conocimiento profundo de los protocolos y arquitecturas de autenticación. La capacidad de usar diferentes tecnologías de autenticación e inicio de sesión único es esencial para una implementación exitosa.

Conclusión

En conclusión, el Single Sign-On (SSO) y el Security Assertion Markup Language (SAML) son tecnologías clave en la autenticación y autorización en línea que tienen como objetivo mejorar la experiencia del usuario y la seguridad. SSO permite a los usuarios acceder a múltiples sistemas y aplicaciones con un solo conjunto de credenciales, mientras que SAML es un estándar abierto que permite la interacción segura de información de autenticación y autorización entre sistemas. Juntos, SSO y SAML brindan una solución eficaz para reducir la cantidad de veces que los usuarios tienen que ingresar sus credenciales y mejorar la seguridad al reducir el número de contraseñas y riesgos asociados. Este informe proporciona una comprensión detallada de SSO y SAML y su impacto en la autenticación y autorización en línea.

Bibliografía

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

Single sign-on and federated authentication. (s. f.). Copyright 2023, The Trustees of Indiana University. https://kb.iu.edu/d/bbrl

Chakray_Admin, C. (2022, 12 diciembre). *¿Qué es el Single Sign on (SSO)? Características y ventajas*. https://www.chakray.com/es/que-es-el-single-sign-on-sso-definicion-caracteristicas-y-ventajas/

Â¿QuÃ© es SAML? (s. f.). Entrust. https://www.entrust.com/es/resources/faq/what-is-saml

Autenticación SAML. (s. f.). https://cpl.thalesgroup.com/es/access-management/saml-authentication

Herramientas de SSO (inicio de sesión único). (s. f.). GetApp. https://www.getapp.es/directory/573/single-sign-on-sso/software

Ingalls, S. (2022, 13 julio). *SAML (Security Assertion Markup Language)*. Webopedia. https://www.webopedia.com/definitions/saml/

Khalid, T. (2022, 18 julio). *Guía del desarrollador para la autenticación SAML [3 herramientas en línea]*. Geekflare. https://geekflare.com/es/saml-authentication-guide-tools/

Lorena, L. (2021, 2 julio). *Qué es Single Sign-On*. Kimaldi. https://www.kimaldi.com/blog/single-sign-on/

luisclausin@gmail.com. (2022, 28 septiembre). *¿Qué es SAML? ¿Qué novedades aporta SAML 2.0?* NTS SEIDOR. https://www.nts-solutions.com/blog/saml-que-es.html

¿Qué es SSO? - Single Sign-On - AWS. (s. f.). Amazon Web Services, Inc. https://aws.amazon.com/es/what-is/sso/

SSO: Qué es SSO | Servicio de Informática y Comunicaciones. (s. f.). https://sic.us.es/servicios/cuentas-y-accesos-los-servicios/integracion-con-sso/que-es-sso