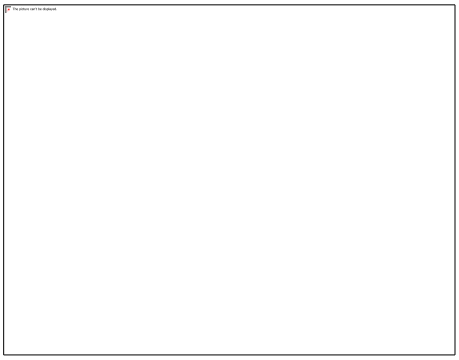
Erick Llanos Ríos

Informe sobre SSO y SAML



24/01/2023

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)

Single Sign-On (SSO) es una técnica de autenticación que permite a los usuarios acceder a varios sistemas o aplicaciones con un solo conjunto de credenciales. Con SSO, los usuarios solo tienen que ingresar sus credenciales una vez y luego pueden acceder a todos los sistemas o aplicaciones a los que tienen acceso sin tener que volver a ingresar sus credenciales. El objetivo de SSO es reducir la cantidad de veces que un usuario tiene que ingresar sus credenciales y mejorar la facilidad de uso de los sistemas. Además, también ayuda a mejorar la seguridad al reducir el número de contraseñas que un usuario debe recordar y minimizar el riesgo de que un usuario utilice la misma contraseña para varios sistemas.

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?

El funcionamiento de SSO depende del protocolo de autenticación utilizado, pero en general, funciona de la siguiente manera:

- El usuario intenta acceder a un sistema o aplicación protegido por SSO.
- En lugar de pedirle al usuario que ingrese sus credenciales directamente, el sistema o aplicación redirige al usuario a un servicio de autenticación centralizado (conocido como proveedor de identidad o IdP).
- El usuario ingresa sus credenciales en el IdP.
- El IdP verifica las credenciales del usuario y, si son válidas, emite un token de seguridad (como una cookie o un jetón de seguridad) que contiene información sobre la autenticación del usuario.
- El sistema o aplicación recibe el token de seguridad y lo utiliza para verificar la autenticación del usuario.
- Si la verificación es exitosa, el usuario es autorizado a acceder al sistema o aplicación.

En general, una vez que el usuario ha sido autenticado, el sistema o aplicación no requerirá que el usuario ingrese sus credenciales de nuevo para acceder a los sistemas o aplicaciones adicionales protegidos por SSO, en su lugar utilizara el token emitido por el IdP.

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.

Otra opción es implementar una solución SSO interna utilizando tecnologías como SAML o OpenID Connect. Estas tecnologías permiten a los desarrolladores crear un sistema de SSO personalizado que se integra con los sistemas y aplicaciones internos de la organización.

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.

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 "assertión" 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?

SAML (Lenguaje de Marcado para Confirmaciones de Seguridad) funciona a través de un intercambio de afirmaciones de seguridad entre un proveedor de identidad (IdP) y un proveedor de servicio (SP). El funcionamiento es el siguiente:

- El usuario intenta acceder a un servicio protegido por SAML.
- El servicio redirige al usuario al IdP para que el usuario pueda ingresar sus credenciales.
- El IdP verifica las credenciales del usuario y, si son válidas, genera una afirmación de seguridad en formato SAML.
- La afirmación de seguridad se envía de vuelta al servicio que el usuario intentaba acceder. La afirmación incluye información sobre la autenticación del usuario, como su nombre de usuario, su nombre completo, y su estado de sesión.
- El servicio valida la afirmación de seguridad, verificando la firma digital del IdP y la validez temporal de la afirmación. Si es válida, el servicio autoriza al usuario a acceder al servicio y acceder a los recursos que el usuario tiene permisos.
- Si el usuario intenta acceder a otro servicio protegido por SAML, el IdP valida su sesión y genera una nueva afirmación de seguridad.

Es importante destacar que SAML solo se encarga de la autenticación y autorización, no se encarga de la gestión de sesiones o de la gestión de credenciales. Es necesario que exista un mecanismo adicional para manejar estas tareas. SAML es compatible con diferentes protocolos de SSO, lo que permite a los usuarios acceder a varios sistemas y aplicaciones con un solo conjunto de credenciales.

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:

- Identificación de requisitos: Los programadores deben entender los requisitos del sistema, incluyendo los servicios que deben ser accedidos y los usuarios que los accederán.
- Selección de un proveedor de SSO: Los programadores deben elegir un proveedor de SSO que se integre con sus aplicaciones y cumpla con sus requisitos de seguridad.
- Configuración del proveedor de SSO: Los programadores deben configurar el proveedor de SSO para autenticar a los usuarios y emitir tokens de acceso.
- Integración de aplicaciones: Los programadores deben integrar sus aplicaciones con el proveedor de SSO, utilizando SAML para intercambiar información de autenticación entre las aplicaciones y el proveedor.
- 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

Los desarrolladores y programadores son clave en la implementación de SSO y SAML. Deben ser capaces de entender y aplicar los estándares SAML para garantizar una implementación segura y efectiva. Además, deben ser conscientes de las posibles amenazas de seguridad y cómo mitigarlas para garantizar la protección de los datos y la privacidad de los usuarios.

Los desarrolladores también deben ser capaces de integrar SSO con aplicaciones y sistemas existentes, lo que puede requerir una comprensión profunda de la arquitectura y los protocolos de autenticación. La habilidad de trabajar con diferentes tecnologías de autenticación y single sign-on es esencial para garantizar 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