Capítulo 9: Seguridad

Víctor Iranzo

30 de mayo de 2018

1. Autenticación y autorización

La autenticación es el proceso por el cual confirmamos que una entidad es quien dice ser. Generalmente, un usuario se autentica mediante un nombre de usuario y una contraseña.

La autorización es el mecanismo por el cual relacionamos una entidad autenticada con las acciones que puede llevar a cabo.

En las aplicaciones basadas en microservicios hace falta definir un mecanismo para que los usuarios no tengan que autenticarse en cada uno de los microservicios de forma separada.

1.1. Proveedor de identidades

Una aproximación para ofrecer estas características son las soluciones single sing-on (SSO). Entre ellas podemos mencionar SAML y OpenID Connect. SAML es un estándar basado en SOAP con el que es bastante complejo trabajar. OpenID Connect es un estándar que surge como una implementación específica de OAuth 2.0 que imita la manera en que organizaciones como Google gestionan sus soluciones SSO. Por su facilidad de uso, se espera que OpenID Connect sea en un futuro acogido por cada vez más organizaciones.

Cuando una entidad trata de acceder a un recurso o realizar una operación, es redirigido a un proveedor de identidades para que se autentique. Una vez autenticados, el proveedor de identidades responderá al servicio que lo ha invocado indicando los permisos que tiene la entidad sobre la operación o recurso solicitados.

El proveedor de identidades puede ser un servicio externo, como el de Google. Sin embargo, la mayoría de empresas emplear su propio servicio

de directorio (similar a Active Directory) donde se almacena información sobre las entidades conocidas, sus roles y permisos. Los permisos efectivos para un microservicio no se pueden almacenar de forma centralizada ya que esta información pertenece al servicio en si y puede suponer un punto de acoplamiento. Además, los roles que se modelan deben ser lo más similares a los existentes en el mundo real donde se ejecuta el sistema.

Para centralizar el contacto entre los servicios del sistema y el proveedor de identidades se puede emplear un SSO gateway. Este mecanismo consiste en un proxy situado entre los servicios y el mundo exterior, lo que puede suponer un único punto de fallo. Además, al ser una capa intermedia puede tender a ir aumentando progresivamente en las funcionalidades que ofrece hasta convertirse en un punto de acoplamiento.

2. Seguridad en tránsito

2.1. HTTP y HTTPS

No sólo se deben autenticar los usuarios para realizar una acción, otros servicios también se pueden modelar para saber si se les da acceso a un recurso o funcionalidad.

Una posible opción es hacer que cualquier invocación a un servicio hecha desde el propio servicio se considera autorizada. Esta solución puede ser peligrosa ante atacantes que penetren en la red, pero puede ser adecuada si los datos almacenados no son de alta sensibilidad.

La autorización HTTP permite a un cliente enviar un nombre de usuario y una contraseña en la cabecera del mensaje. Aunque es un protocolo muy extendido, puede ser peligroso porque estos datos son enviados sin ninguna seguridad. Por este motivo se suele emplear el protocolo de HTTPS.

Entre los problemas de usar HTTPS están que el tráfico en este protocolo no puede ser capturado por proxies inversos, aunque en caso de necesidad se puede capturar en alguno de los extremos o en un balanceador de carga. Además, se deben gestionar los certificados SSL, que puede resultar un problema cuando el sistema se distribuye entre múltiples máquinas, y se puede aumentar el tiempo de entrega de los mensajes.

2.2. Certificados de clientes

Con esta aproximación cada cliente emplea un certificado en su interacción con el servidor. Esta solución es aconsejable si la sensibilidad de los datos que se envían es muy alta. Sin embargo, puede traer dificultades a la hora de revocar y emitir certificados.

2.3. Códigos de autentificación de mensajes en clave-hash (HMAC)

El tráfico a través de HTTPS puede afectar al rendimiento del sistema. Una solución a este problema pasa por, en lugar de usar este protocolo, usar mensajes cifrados con claves hash y enviarlos a través de HTTP.

Con HMAC, el cuerpo de una petición es convertido en un hash empleado una llave privada y es enviado junto con la petición. El servidor, cuando recibe una petición, usa la misma llave privada que comparten para generar el hash con el cuerpo del mensaje recibido y compararlo con el hash del mensaje.

Este mecanismo cuenta con 3 desventajas. Primero, entre servidor y cliente tiene que existir un secreto compartido, que debe ser enviada usando un protocolo seguro. Segundo, este mecanismo no es un estándar y existen muchas implementaciones distintas disponibles que deben ser evaluadas. Tercero, un atacante pueda interceptar y leer una petición, pero no puede modificar esta porque si lo hace el hash que genera el servidor y el de la petición no coincidirían.

2.4. Claves API

Muchas APIs públicas emplean este mecanismo para ofrecer sus servicios a terceros. Se pueden emplear para identificar quién hace una llamada y limitar las que puede hacer para que no sobrecargue el servicio. Entre sus ventajas podemos nombrar su facilidad de uso.

2.5. Problema del reemplazo

Una entidad autenticada puede invocar a un servicio que a su vez tenga que invocar a un tercero. En esta segunda petición, si aceptamos la aproximación de que cualquier petición hecha desde dentro del sistema es válida, podemos incurrir en un problema de reemplazo de identidades.

Por ejemplo, un atacante que haya conseguido acceso a la red puede obligar a un servicio a hacer peticiones a otro y obtener los datos del servicio atacado. Este problema es grave de acuerdo a la sensibilidad de los datos. Una posible solución es solicitar que en cada petición sean provistas las credenciales de la entidad que comienza la interacción.

3. Seguridad en los datos

4. Seguridad en profundidad: otras medidas de protección

4.1. Cortafuegos

4.2. Logging

4.3. Sistemas de detección de intrusos

4.4. Segregación de redes

4.5. Sistemas operativos

5. Caso de estudio

6. Otros factores de la seguridad