Tema 4: Mecanismos de autenticación, autorización y control de acceso

Los servicios REST/JSON gestionan eventos corporativos. Los conceptos que se estuduan son los aplicables a otro tipo de servicios como SOAP, Thrift, gRPC, etc… Un servicio REST es un servicio que implementa la lógica de negocio, pero que no tiene interfaz gráfica y es utilizado por un servicio o aplicación que si tiene interfaz gráfica. Un ejemplo de esto sería una aplicación para ver el tiempo en el móvil, la aplicación contactaría con un servicio REST por HTTP para solicitar la información climatológica y el REST devolvería la información en un formato estructurado como por ejemplo XML o JSON. Este mismo servicio rest podría ser utilizado por otras aplicaciones con una interfaz gráfica diferente.

Vamos a ver un ejemplo base. Normalmente dentro de estos servicios suelen haber roles como:

- User
- Manager

El servicio atiende a peticiones HTTP para:

- [Manager] Crear un evento
- [Manager] Manager
- [No autentciado] Buscar eventos
- [No autenticado]Obtener información de un evento
- [User]responder a un evento
- [User y Manager]Recuperar las respuestas de un usuario

Dependiendo de lo que se vaya viendo en cada apartado se analizará este ejemplo base o versiones extendidas de este.

Autenticación y Autorización

Muchas funcionalidades requieren que el usuario de la aplicación cliente se autentique. Se reciben el nombre de usuario y la contraseña. Normalmente, el punto de acceso de autenticación podría devolver un toquen que autoriza a esa aplicación cliente a hacer peticiones al servicio REST.El token debe ser seguro. Un atacante no debería tener forma de generar un token arbitrario válido.

Cuando el servicio recibe una petición debe comprobar que el token es válido y si lo es, comprobar que no esté caducado. Tras eso se revisa si el usuario que ha realizado la petición está autorizado.

Autenticación en HTTP

La cabecera debe ser ASCII estádar (7 bits, del 0 al 127) si hay simbolos extraños en la contraseña puede haber problemas, por ello normalmente se codifican las contraseñas en base 64.

JSON Web Token

OAuth

OpenID Connect

SAML

Kerberso y NPNEGO

Control de acceso

Impedir a otros usuarios que puedan acceder a funcionalidades como las de administrador.

Control de acceso basado en roles

Control de acceso basado en atributos

From:
https://knoppia.net/ - **Knoppia**

Permanent link:
https://knoppia.net/doku.php?id=app:tema4&rev=1731001056

Last update: **2024/11/07 17:37**