# 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

### 2.2. SAML y OpenID Connect

### 2.3. Certificados de clientes

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

### 2.5. Claves API

### 2.6. Problema del reemplazo

## 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