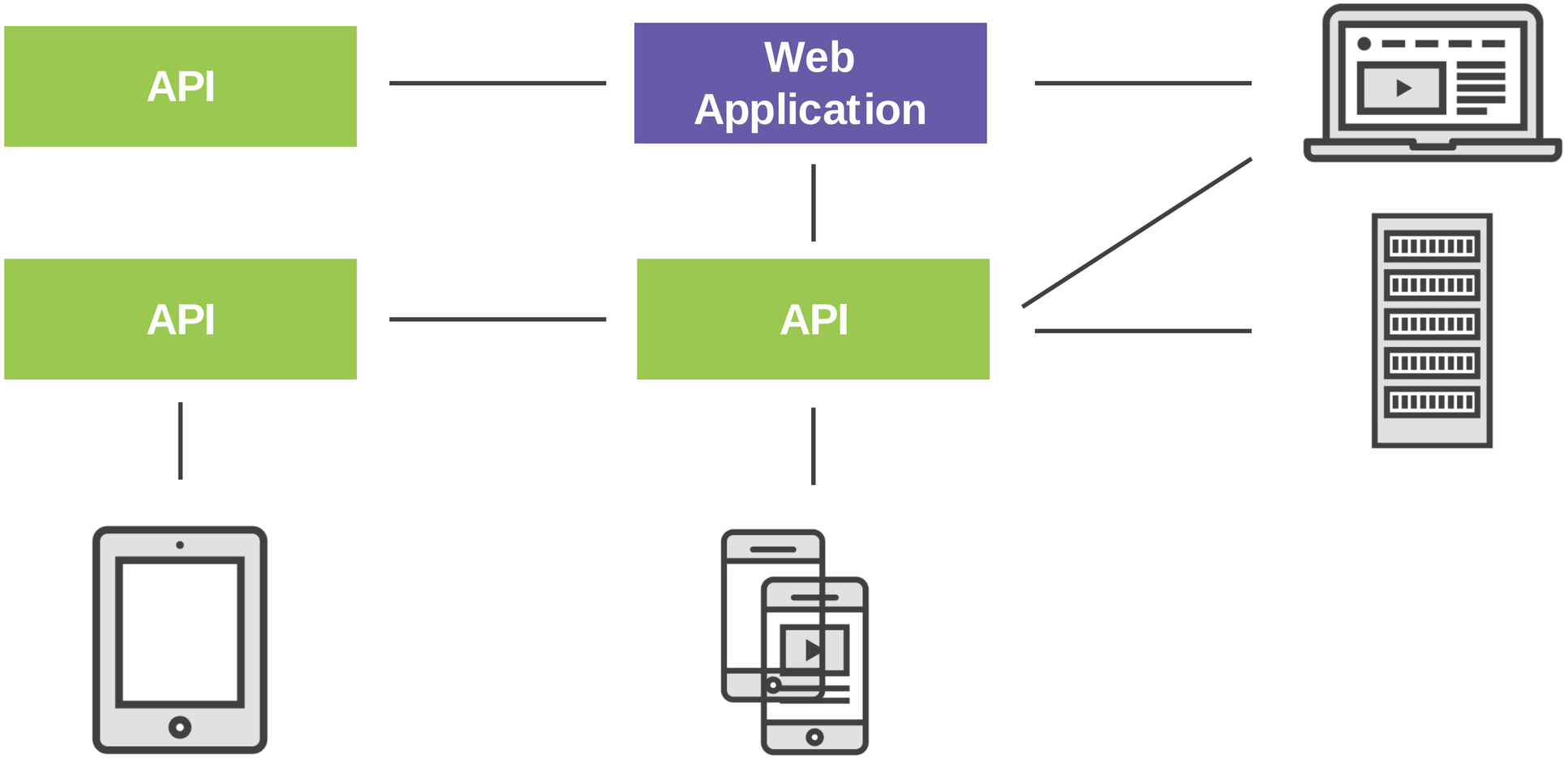
Seguridad en APIs

Resumen

Unas palabras sobre la seguridad de las API
Seguridad basada en tokens
Trabajar con directivas de autorización
OAuth2 y OpenID Connect

Unas palabras sobre la seguridad de las API



Unas palabras sobre la seguridad de las API

¿Qué entidad (usuario/aplicación) está intentando acceder a la API?

- ¿Cómo podemos verificar esto?

Una vez que sabemos quién/qué es la entidad, ¿cómo comprobamos si debe concederse el acceso?

Enviar nombre de usuario/contraseña en cada solicitud ha resultado ser una mala idea...

- Gran vector de ataque

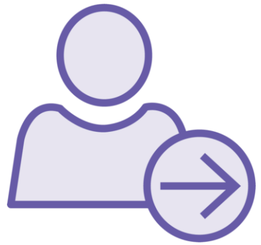
Unas palabras sobre la seguridad de las API

Seguridad basada en tokens

- Enviar un token en cada solicitud
- Un token representa el consentimiento
- Validar el token a nivel de la API

Este enfoque sirve para casi todos los tipos de aplicaciones actuales

Implementar seguridad basada en tokens



Endpoint "login" de la API que acepta un nombre de usuario/contraseña

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c
```

```
{
  "sub": "1234567890",
  "name": "John Doe",
  "iat": 1516239022
}
```

Payload

Por ejemplo: algún JSON que contenga información genérica del token, como cuándo se creó el token, y alguna información sobre el usuario.

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c

Signature

Un hash de la carga útil, utilizado para garantizar que los datos no han sido manipulados.

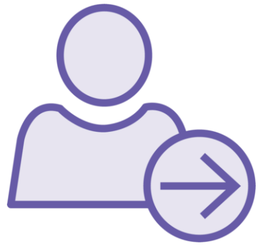
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c


```
{
  "alg": "HS256",
  "typ": "JWT"
}
```


Header

Información esencial sobre los tokens, como el algoritmo de clave utilizado para la firma.

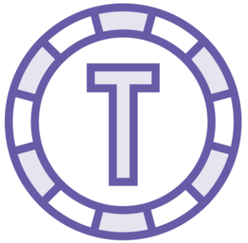
Implementar seguridad basada en tokens



Endpoint "login" de la API que acepta un nombre de usuario/contraseña

```
POST api/login
```

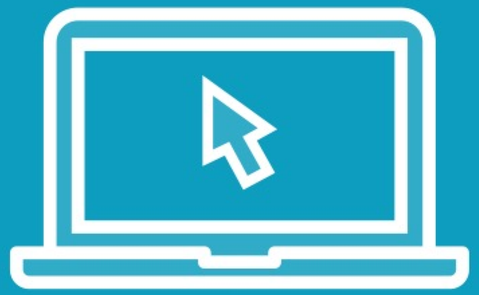
Asegúrate de que sólo se puede acceder a la API con un token válido



Pasar el token del cliente a la API como token de portador en cada solicitud.

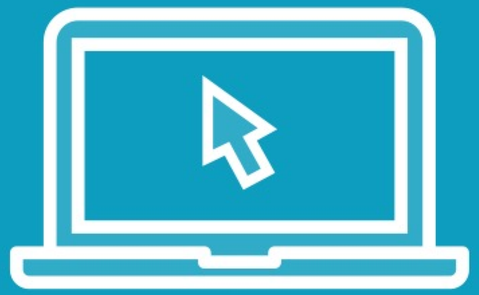
```
Authorization: Bearer mytoken123
```

Demo



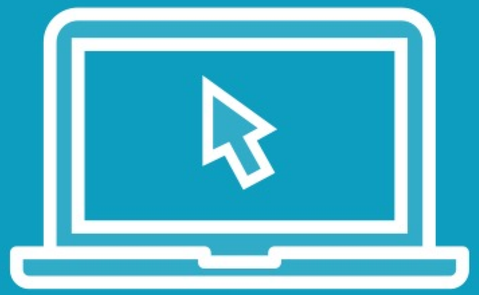
Crear un token

Demo



Solicitar y validar un token

Demo



Uso de la información del token en el controlador

Trabajar con directivas de autorización

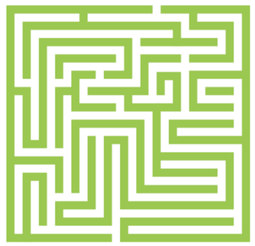
Las directivas de autorización ayudan a crear una capa de autorización completa

- Evita tener que entrar en la acción real del controlador

ABAC/CBAC/PBAC

Derechos de acceso concedidos mediante directivas

Una directiva combina un conjunto de atributos (claims)

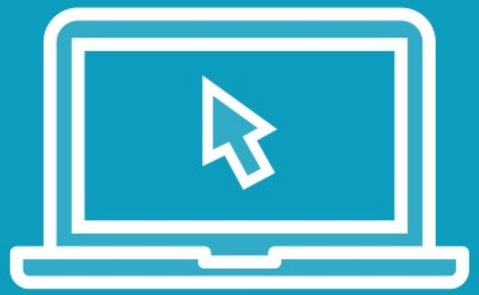


Permite reglas mucho más complejas que RBAC (Role-based Access Control)

“Si un usuario es del país A, vive en una ciudad con más de medio millón de habitantes y nació entre 1980 y 1985, puede realizar la acción X“

Ejemplo de directiva

Demo



Uso de la información del token en una directiva de autorización

Mejora de la seguridad basada en tokens con OAuth2 y OpenID Connect

La seguridad es un tema amplio y en rápida evolución

- Hemos implantado una forma básica y rudimentaria de seguridad basada en token.
- Existen normas que lo mejoran

OAuth2

OAuth2 es un protocolo abierto que permite la autorización segura en un método simple y estándar desde aplicaciones web, móviles y de escritorio.

OpenID Connect

OpenID Connect es una capa de identidad sencilla sobre el protocolo OAuth2.

Resumen

Existen múltiples formas de proteger las API

- La seguridad basada en tokens es el enfoque aconsejado

A continuación:
Versionado y documentación de la API