



Universitat Oberta
de Catalunya

WebAuthn

Alberto Gabriel Ruiz Pérez

Tutor: Pau del Canto Rodrigo

Máster Interuniversitario en Seguridad de las Tecnologías de la Información y de las
Comunicaciones (MISTIC)

Sistemas de autenticación y autorización

Junio, 2019

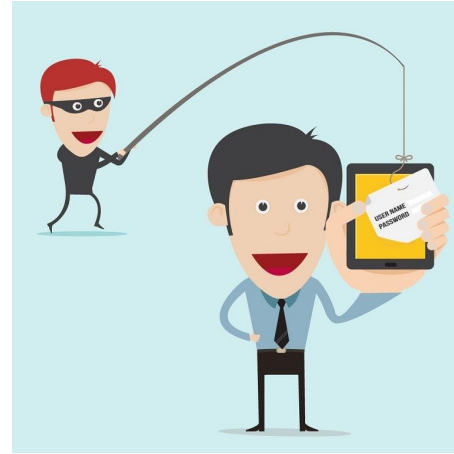
Índice

- ❖ Introducción
 - Estado actual
- ❖ WebAuthn
 - Registro
 - Autenticación
 - Operaciones del servidor
 - Posibles escenarios
 - Ventajas y desventajas
- ❖ Desarrollo
 - Esquema de funcionamiento
 - Demostración
- ❖ Conclusiones



Introducción

- Evolución de la tecnología y métodos de autenticación.
- Ataques a credenciales (Collection #1).
- Nuevo estándar de autenticación web, WebAuthn.
- Objetivos del TFM.



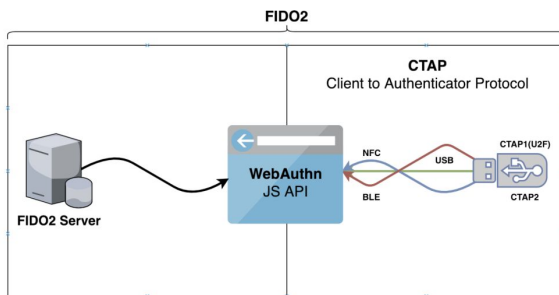
Introducción – Estado actual

- Robo y filtración de credenciales, phishing, robo de información, etc.
- Desarrollo de nuevos métodos de autenticación:
 - Credencial usuario + contraseña.
 - Autenticación mediante certificados.
 - Segundo factor (A2F) o multifactor (MFA).
 - etc.



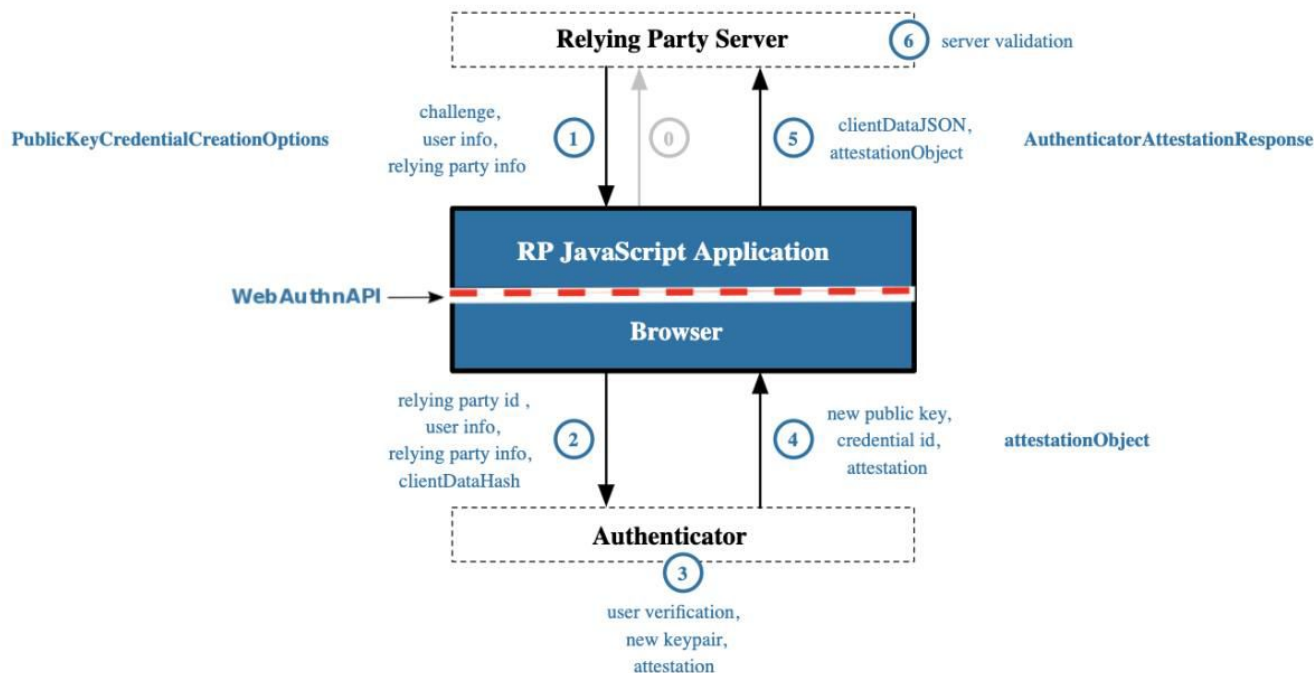
WebAuthn

- Robo y filtración de credenciales, phishing, robo de información, etc.
- W3C y Alianza FIDO, publicación el 4 de marzo de 2019.
- Estándar navegador-plataforma (API javascript, librerías lado del servidor).
- Provee un sistema simple y fuerte de autenticación (Criptografía asimétrica y autenticadores (plataforma o de itinerancia)).
- Elimina el uso de credenciales (y con ello las vulnerabilidades/ataques).



WebAuthn – Registro [1]

- Proceso donde el usuario registra una nueva credencial (asimétrica) en la plataforma.



WebAuthn – Registro [2]

```
7  var publicKey = {
8    'challenge': challenge,
9
10   'rp': {
11     'name': 'Example Inc.'
12   },
13
14   'user': {
15     'id': id,
16     'name': 'alberto@example.com',
17     'displayName': 'Alberto Ruiz'
18   },
19
20   'pubKeyCredParams': [{
21     'type': 'public-key',
22     'alg': -7
23   }, {
24     'type': 'public-key',
25     'alg': -257
26   }]
27 }
28
29 navigator.credentials.create({
30   'publicKey': publicKey
31 })
32 .then((newCredentialInfo) => {
33   console.log('SUCCESS', newCredentialInfo)
34 })
```

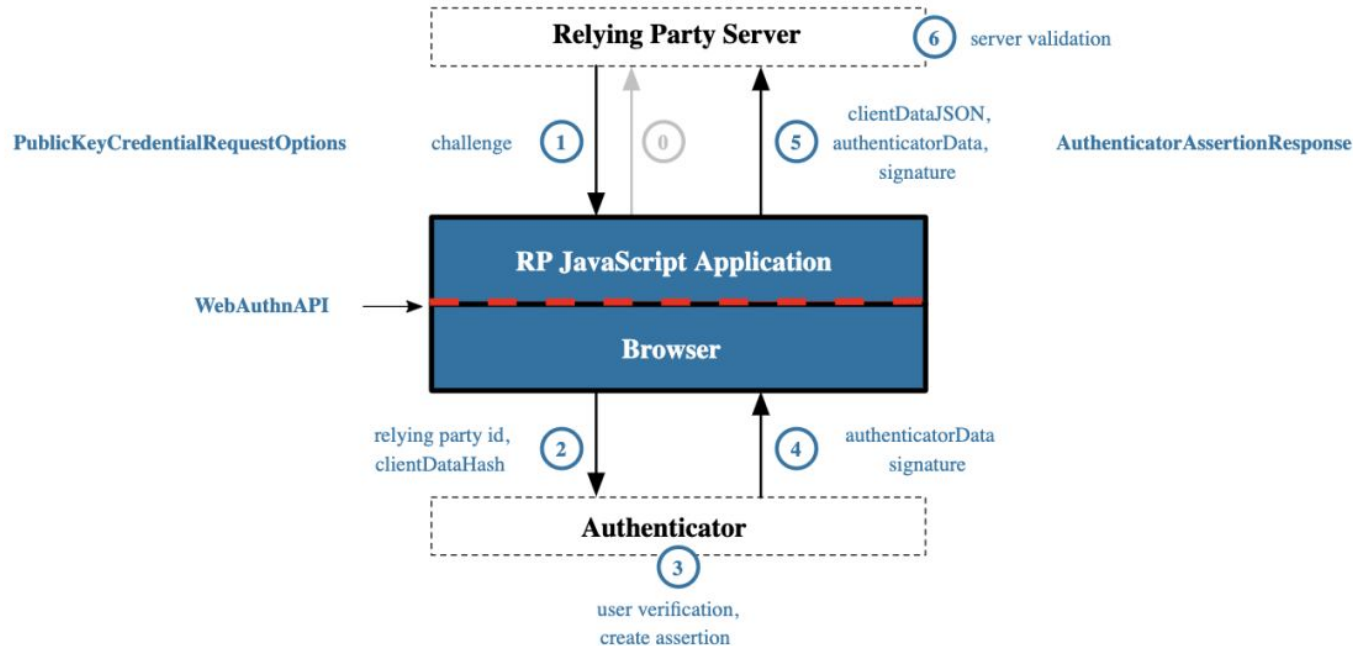


Información devuelta por el autenticador

- CredentialID
- clientDataJSON
- attestationObject
 - authData
 - fmt
 - attStmt

WebAuthn – Autenticación [1]

- Proceso donde el usuario se autentica en la plataforma utilizando una clave (asimétrica) anteriormente creada/registrada.



WebAuthn – Autenticación [2]

- Proceso donde el usuario se autentica en la plataforma utilizando una clave (asimétrica) anteriormente creada/registrada.

```
1 var publicKey = {
2   challenge: challenge,
3
4   allowCredentials: [
5     { type: "public-key", id: credentialId }
6   ]
7 }
8
9 navigator.credentials.get({ 'publicKey': publicKey })
10 .then((getAssertionResponse) => {
11   alert('Assertion recibida')
12   console.log(getAssertionResponse)
13 })
```

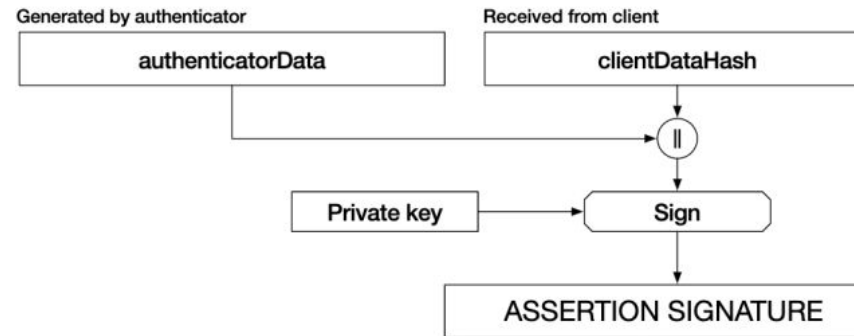


Información devuelta por el autenticador

- authenticatorData
- clientDataJSON
- signature
- userHandle

Operaciones del servidor

- Registro de una nueva credencial
- Verificación de la identidad del usuario



WebAuthn – Posibles escenarios

- WebAuthn como segundo factor de autenticación (A2F).
- WebAuthn sin envío de contraseñas (solo con username).
- WebAuthn como único factor de autenticación (sin usuario ni contraseña).
- Pérdidas o eliminación de credenciales.
- etc.

WebAuthn – Ventajas y desventajas

- Se elimina la importancia de las contraseñas (longitud, caracteres especiales, significado, etc).
- Se elimina la necesidad de depositar confianza en los navegadores.
- Se eliminan los tradicionales ataques y vulnerabilidades (MiTM, phishing, etc).
- Liberación por parte de los desarrolladores.
- Se podrá utilizar cualquier autenticador compatible (FIDO2, U2F).
- Compatibilidad con navegadores.
- Necesidad de un dispositivo adicional.

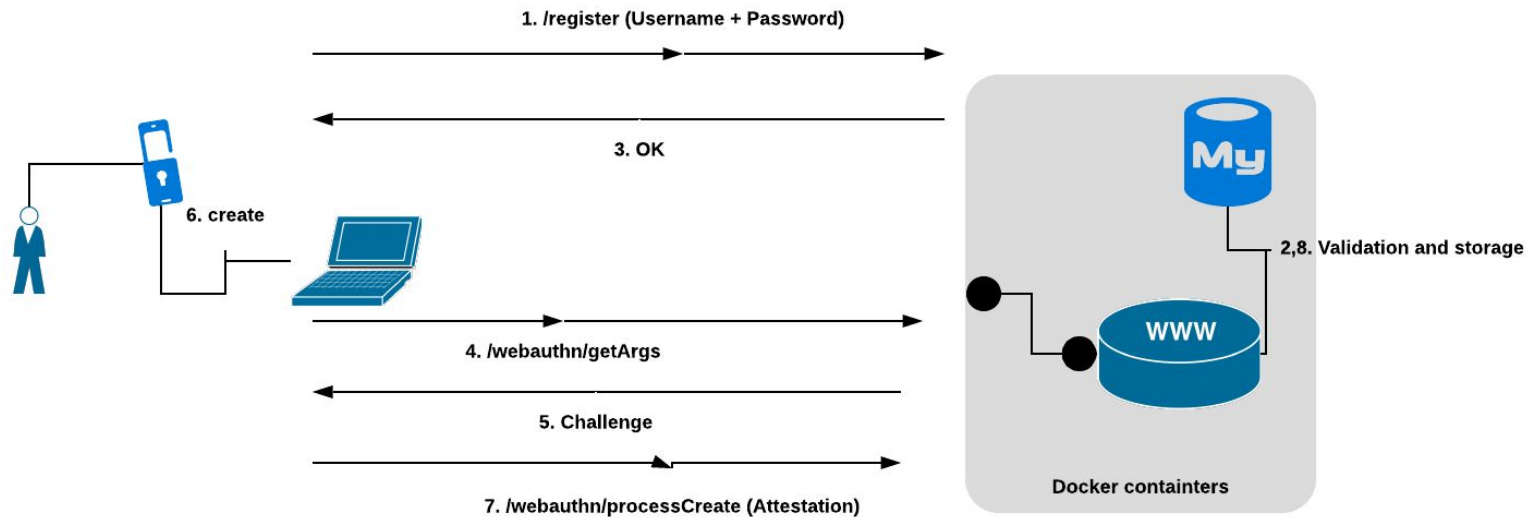
Desarrollo

- Plataforma web para el testeo de WebAuthn en un entorno de prueba.
- Utilización del framework Symfony 4.
- MySQL para almacenar la información de los usuarios.
- [Ibuchs/WebAuthn](#) Para la verificación de WebAuthn en el servidor.
- OpenSSL.
- Docker.



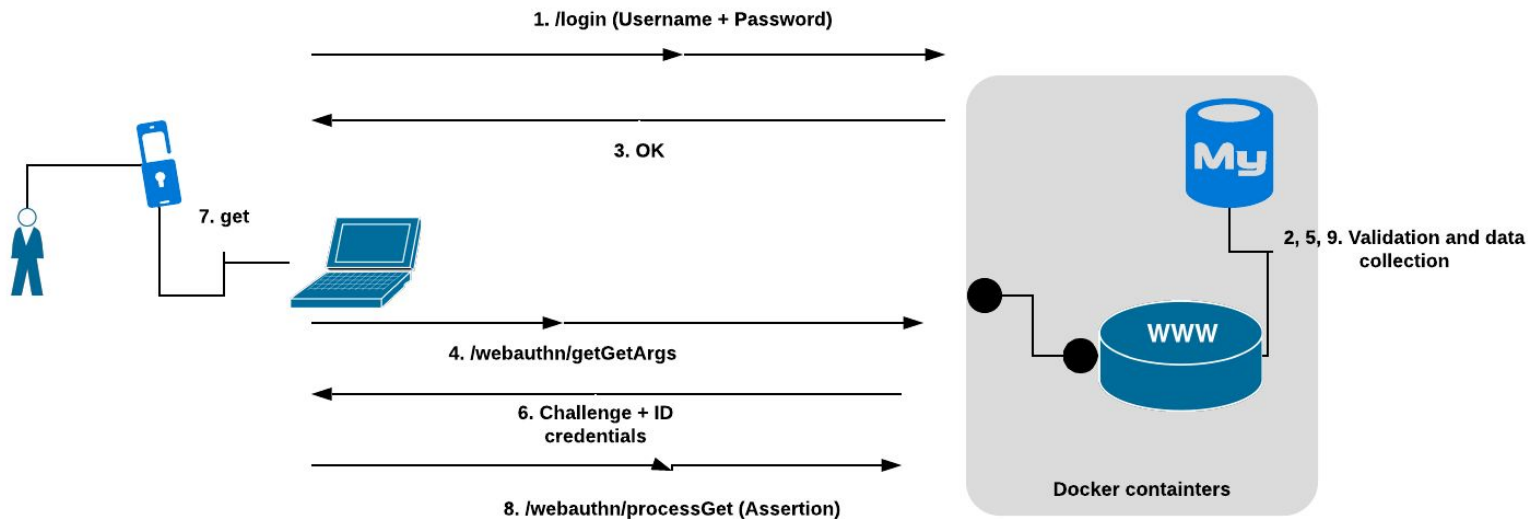
Desarrollo – Esquema de funcionamiento

Registro

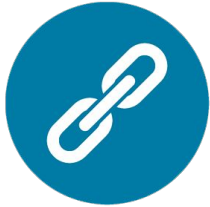


Desarrollo – Esquema de funcionamiento

Autenticación



Desarrollo - Demostración



<https://github.com/alber7rp/TFM-WebAuthn/tree/master/code>

Conclusiones

- Estándar de autenticación web que revoluciona el panorama actual.
- Con el tiempo se deberá aumentar la compatibilidad con lenguajes de programación, frameworks, navegadores, plataformas de desarrollo, etc.





Universitat Oberta
de Catalunya

Gracias por su atención

Alberto Gabriel Ruiz Pérez
Tutor: Pau del Canto Rodrigo

Máster Interuniversitario en Seguridad de las Tecnologías de la Información y de las
Comunicaciones (MISTIC)

Sistemas de autenticación y autorización

Junio, 2019