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

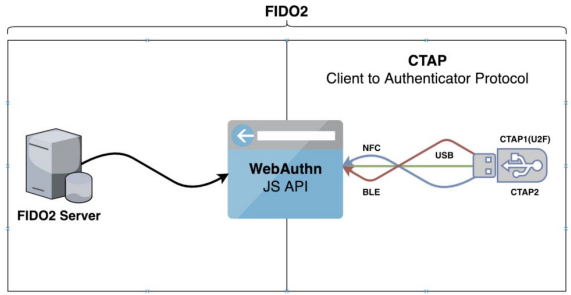
- Evolución de la tecnología y métodos de autenticación.
- Ataques a credenciales (Collection #1).
- Nuevo estándar de autenticación web, WebAuthn.
- Objetivos del TFM.

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.

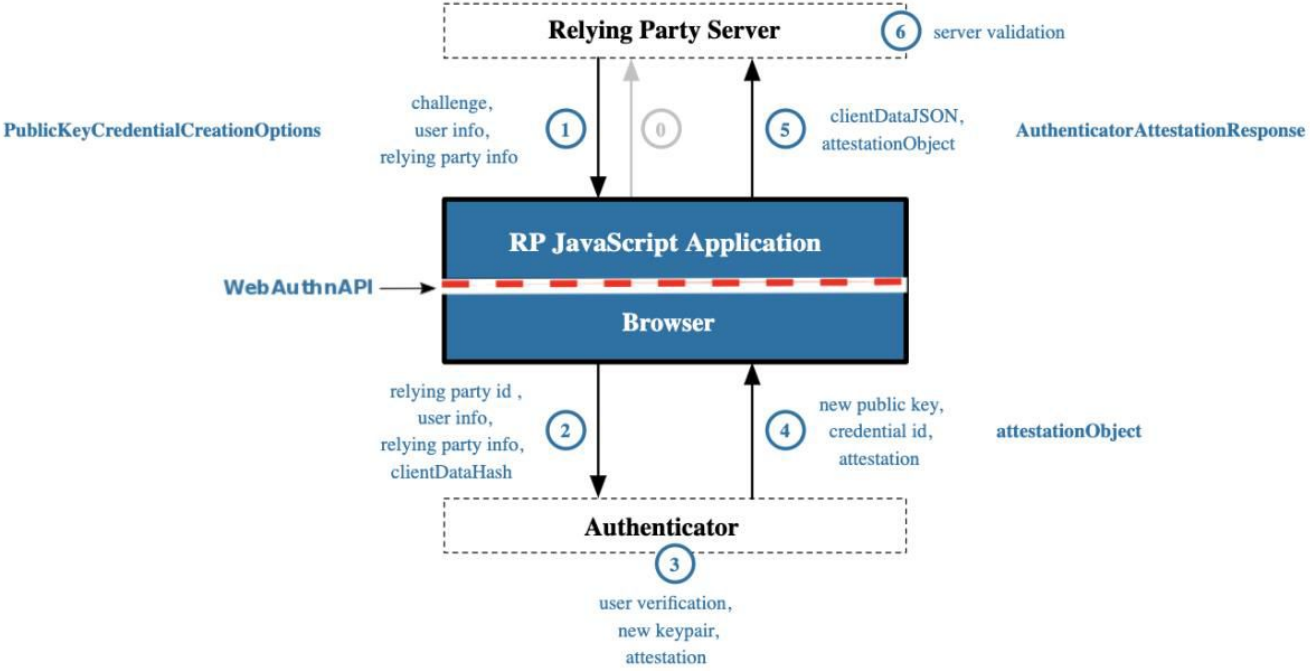
WebAuthn

- 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]

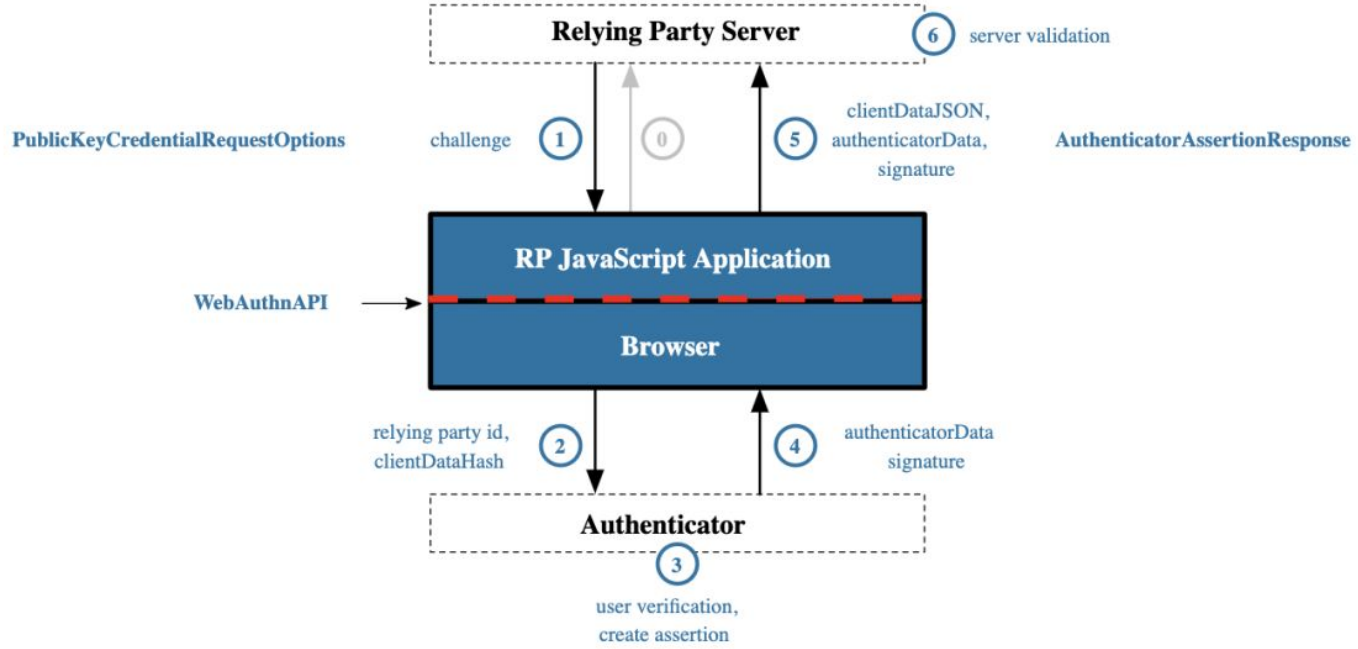
```
var publicKey = {
    'challenge': challenge,

    'rp': {
        'name': 'Example Inc.'
    },

    'user': {
        'id': id,
        'name': 'alberto@example.com',
        'displayName': 'Alberto Ruiz'
    },

    'pubKeyCredParams': [{
        'type': 'public-key',
        'alg': -7
    }, {
        'type': 'public-key',
        'alg': -257
    }]
}

navigator.credentials.create({
        'publicKey': publicKey
    })
    .then((newCredentialInfo) => {
        console.log('SUCCESS', newCredentialInfo)
    })
```

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.

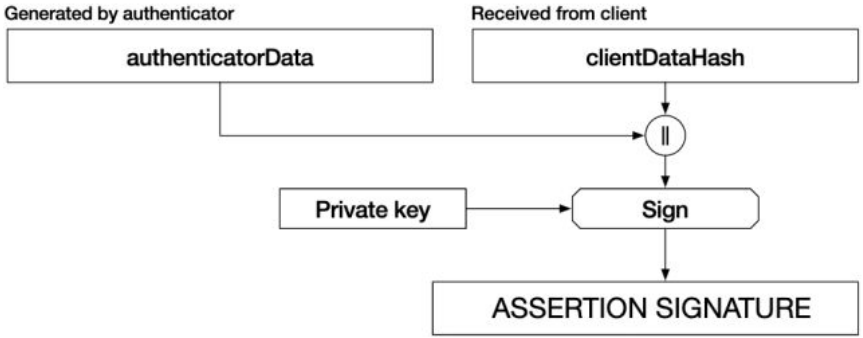
```
var publicKey = {
    challenge: challenge,

    allowCredentials: [
        { type: "public-key", id: credentialId }
    ]
}

navigator.credentials.get({ 'publicKey': publicKey })
  .then((getAssertionResponse) => {
      alert('Assertion recibida')
      console.log(getAssertionResponse)
  })
```

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

- WebAthn 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

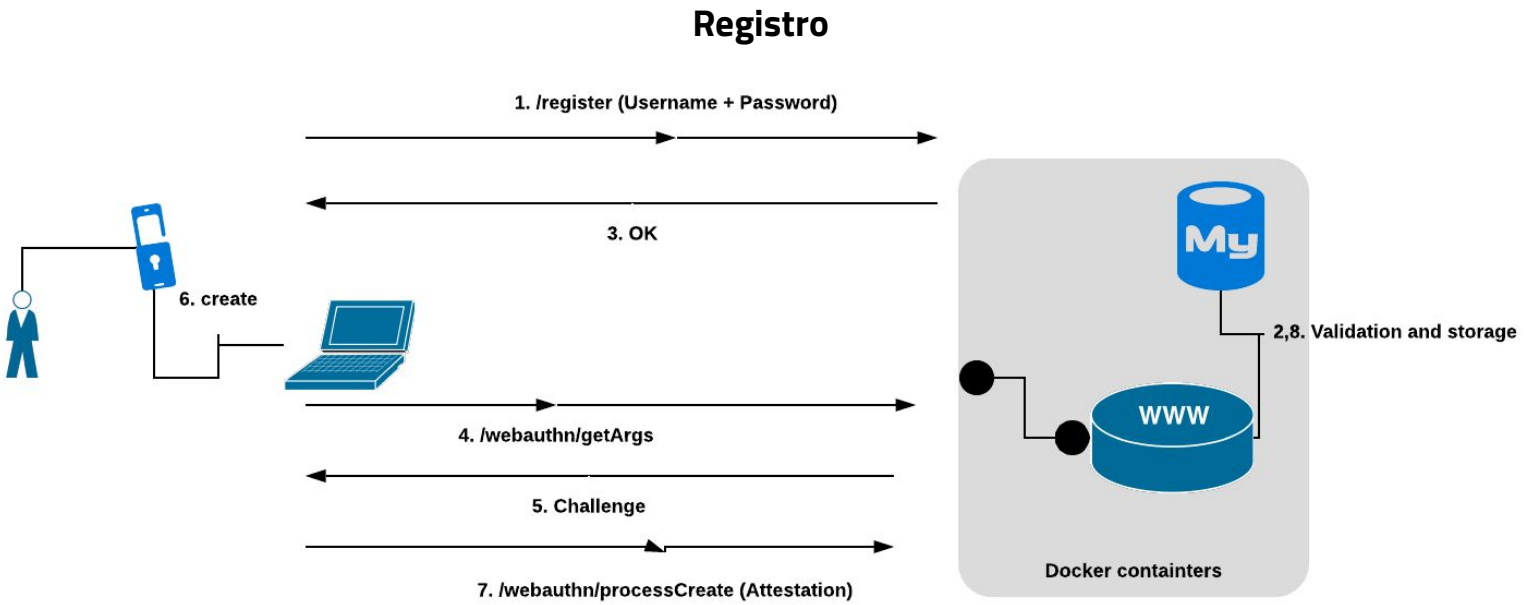
- Se elimina la importancia de las contraseñas (longitud, caracteres especiales, significado, etc).
- Se elimina la necesidad de depositar confianza en los navegadores.
- Se eliminan los tradicionales ataques y vulnerabilidades (MiTM, phising, etc).
- Liberación por parte de los desarrolladores.
- Se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

- Necesidad de un dispositivo adicional.

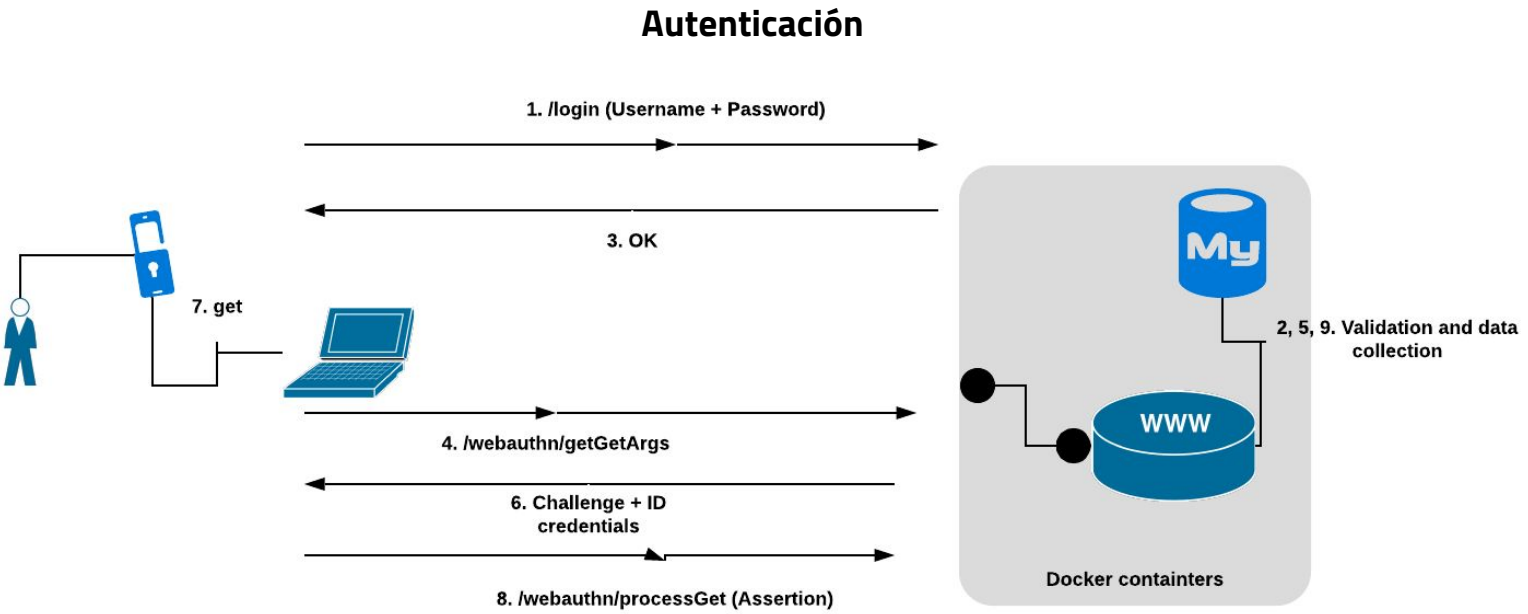
Desarrollo

- 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.
- lbuchs/WebAuthn Para la verificación de WebAuthn en el servidor.
- OpenSSL.
- Docker.

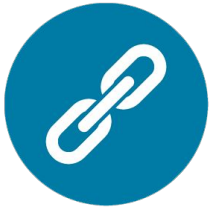
Desarrollo - Esquema de funcionamiento



Desarrollo - Esquema de funcionamiento



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.

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