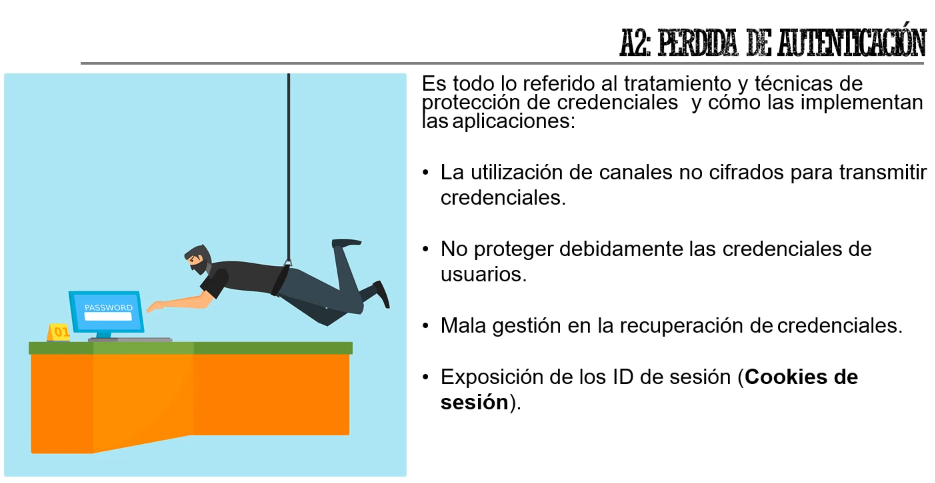
**Pérdida de Autenticación**

****

La pérdida de la autenticación se refiere al tratamiento y técnicas de protección de las credenciales. Además se analiza cómo viajan esas credenciales por la red y por Internet.

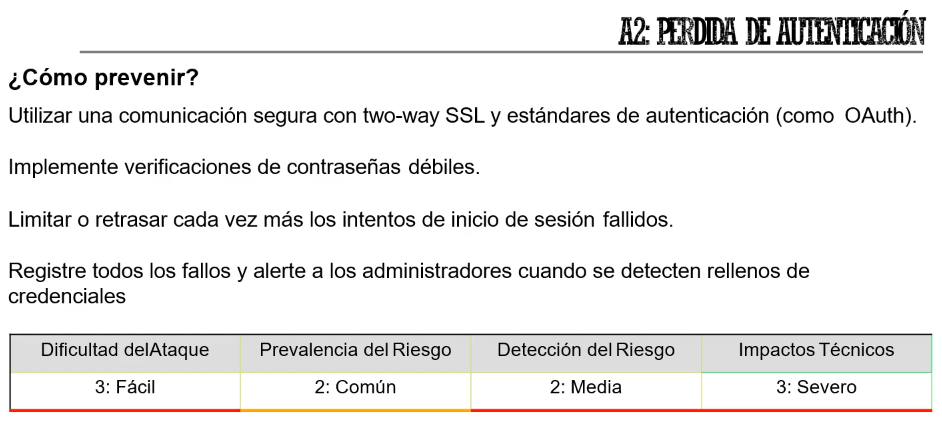
Uno de los riesgos es, por ejemplo, el uso de canales no cifrados para transmitir las credenciales y que estas viajen limpias por la red, por lo que si hubiera un ataque de "Man in the Middle" podría ver los password que están utilizando nuestros usuarios.

Otro caso es el de no proteger debidamente las credenciales de los usuarios, pudiendo ser accedido, por ejemplo, dentro de nuestra base de datos.

Otra vulnerabilidad es la mala gestión en la recuperación de credenciales, Por ejemplo, en numerosas páginas como aquellas que tienen la leyenda "me he olvidado la contraseña" y que directamente cuando se envía al email, viaje limpia.

También podemos mencionar los id de sesión y el robo, por ejemplo, de las cookies de sesión.

**Prevención**

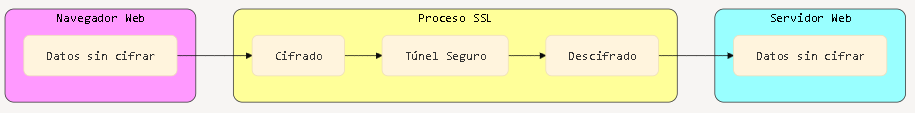


Para evitar el ataque de Man in the Middle podemos utilizar una comunicación segura, mediante two-way SSL o autenticación OAuth o JWT.

**SSL**

Según el diagrama:

* Los datos normales (como tu contraseña o información personal) comienzan en el navegador
* SSL los convierte en un código secreto (cifrado)
* Este código viaja por internet a través de un "túnel seguro"
* El servidor web puede descifrarlo para leer la información original

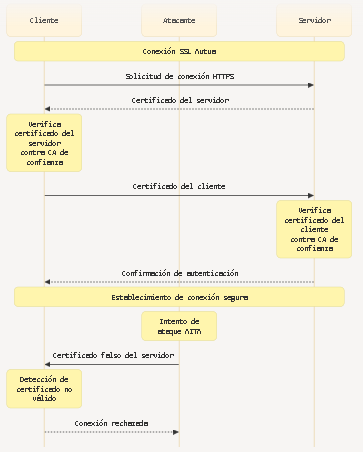


Cuando ves "https://" al principio de una dirección web, significa que esa conexión está protegida por SSL. Es especialmente importante cuando:

* Ingresas a tu banco en línea
* Compras por internet
* Te conectas a redes Wi-Fi públicas

**Two-way SSL**

El Two-way SSL (también conocido como SSL mutuo) es un mecanismo de autenticación que requiere que tanto el servidor como el cliente se autentiquen mutuamente antes de establecer una conexión segura.



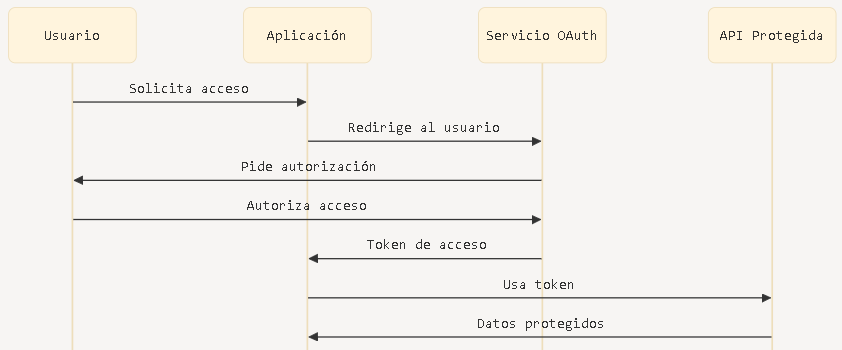
*Los componentes clave del proceso son:*

* Certificado del servidor: El servidor presenta su identidad mediante un certificado digital firmado por una Autoridad de Certificación (CA) de confianza
* Certificado del cliente: El cliente también debe presentar su certificado, lo que permite al servidor verificar su identidad
* Verificación mutua: Ambas partes verifican los certificados contra sus CA de confianza antes de establecer la conexión

Este mecanismo previene los ataques MITM porque incluso si un atacante intercepta la comunicación, no podrá establecer una conexión válida sin los certificados correctos

**Autenticación OAuth**

OAuth es un protocolo de autenticación que permite a las aplicaciones acceder a servicios de otras plataformas sin compartir contraseñas. Es como cuando autorizas a una aplicación a usar tu cuenta de Facebook para iniciar sesión, sin darle tu contraseña de Facebook.



Como podes ver en el diagrama, el proceso es similar a cuando:

* Una aplicación (como Spotify) te pide acceso a tu cuenta de Facebook
* Facebook te pregunta si aceptas darle permisos a Spotify
* Si aceptas, Facebook le da un "pase temporal" (token) a Spotify
* Spotify usa ese pase para acceder a tu información, sin necesitar tu contraseña

Este sistema es más seguro que compartir contraseñas porque:

* Nunca compartes tu contraseña real
* Puedes revocar el acceso cuando quieras
* Controlas exactamente qué información comparte cada aplicación

La dificultad de este ataque es bastante fácil porque los hackers están probando los distintos passwords o están detectando el password que está viajando y lo están usando.

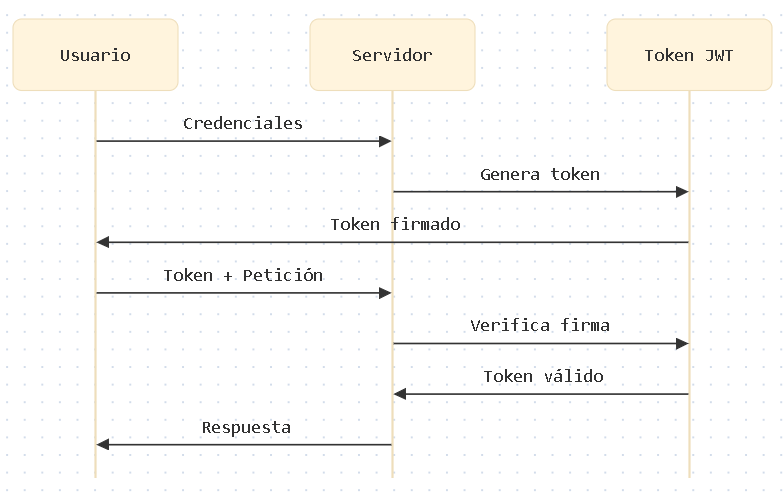
La prevalencia de riesgo es común, ya que son muchos los hackers que intentan descubrir las contraseñas de las cuentas, por ejemplo, de diferentes plataformas o incluso cuentas bancarias.

La detección de riesgo es media.

En cambio, el impacto técnico es severo, ya que puede suponer un gran perjuicio para el usuario que está siendo hackeado.

**JWT**

JWT (JSON Web Token) es un método de autenticación que utiliza un token digital firmado para verificar la identidad de un usuario. Es como un boleto de avión digital que contiene toda tu información de viaje de manera segura y verificable.



Como puedes ver en el diagrama, el proceso funciona así:

* Cuando te autenticas, el servidor crea un token JWT que contiene tu información
* Este token está firmado digitalmente, como un sello que garantiza que no ha sido modificado
* Cada vez que haces una petición, el servidor verifica el token sin necesidad de consultar la base de datos

Es más eficiente que las sesiones tradicionales porque:

* No necesita almacenar información en el servidor
* El token contiene toda la información necesaria
* Es más seguro y escalable para aplicaciones modernas