The following scenario shows a successful authentication of a client using the mobile OTP solution.

The authentication is initiated when a user requests access to a service that requires authentication. The SP notifies the authenticator that a user needs to be authenticated. The session is redirected to the authenticator and the user is asked to enter a username. The username is sent to the AS which gets the secret key for this client and from this generates an OTP. The OTP is also based on a challenge. A different challenge is used every time so the generated OTP is always changing. At last a message authentication code (MAC) based on the secret key is calculated over the OTP. The AS sends the triplet (challenge, MAC, OTP) to the

AS has proved that it is in possession of the shared key. The client then sends the OTP back to the Authenticator. If the MAC is wrong the authentication is aborted. The Authenticator compares the OTP with the one received from the AS and if they match, notifies the SP that the client is authenticated. A mutual authentication of the client and server has been achieved and the session is redirected back to the SP which grants the user access to the service.

Draw a sequence diagram based on the above information.

The following scenario shows a successful authentication of a client using the mobile OTP solution.
The authentication is initiated when a user requests access to a service that requires authentication. The SP notifies the authenticator that a user needs to be authenticated. The session is redirected to the authenticator and the user is asked to enter a username. The username is sent to the AS which gets the secret key for this client and from this generates an OTP. The OTP is also based on a challenge. A different challenge is used every time so the generated OTP is always changing. At last a message authentication code (MAC) based on the secret key is calculated over the OTP. The AS sends the triplet (challenge, MAC, OTP) to the Authenticator which relays the challenge and the MAC to the client. Upon receiving the challenge the client calculates the OTP. Then it calculates the MAC and compares it to the one received from the Authenticator. If the values match the client can authenticate the AS since the AS has proved that it is in possession of the shared key. The client then sends the OTP back to the Authenticator. If the MAC is wrong the authentication is aborted. The Authenticator compares the OTP with the one received from the AS and if they match, notifies the SP that the client is authenticated. A mutual authentication of the client and server has been achieved and the session is redirected back to the SP which grants the user access to the service.
Draw a sequence diagram based on the above information.

There are 3 steps to solve this one.

Expert-verified

Share (0)

1st step | All steps | Answer only

Step 1

Sequence Diagram for Mobile OTP Authentication with Mutual Authentication

Actors:

- Client
- Authenticator
- Service Provider (SP)

Messages:

```
Client -> SP: Authentication request

SP -> Authenticator: Authentication request (with username)

Authenticator -> AS: Get secret key request

AS -> Authenticator: Secret key response

Authenticator -> Client: Challenge, MAC, OTP

Client -> Authenticator: MAC, OTP

Authenticator -> SP: Authentication response (with OTP)

SP -> AS: Verify OTP request

AS -> SP: Verify OTP response

SP -> Client: Authentication success
```

Explanation:

This step explains about the process of diagram I.E steps and the parts of the diagram.

Step 2

Sequence :

1. The client requests access to a service that requires authentication.
2. The SP notifies the authenticator that a user needs to be authenticated.
3. The authenticator redirects the session to the authenticator and prompts the user to enter a username.
4. The username is sent to the AS, which gets the secret key for this client and generates an OTP.
5. The AS also generates a challenge and a MAC based on the secret key and the OTP.
6. The AS sends the triplet (challenge, MAC, OTP) to the authenticator.
7. The authenticator relays the challenge and the MAC to the client.
8. Upon receiving the challenge, the client calculates the OTP and the MAC.
9. The client compares the calculated MAC to the MAC received from the authenticator. If the values match, the client authenticates the AS.
10. The client sends the OTP back to the authenticator.
11. The authenticator compares the OTP received from the client to the OTP received from the AS. If the OTPs match, the authenticator authenticates the client.
12. The authenticator notifies the SP that the client is authenticated.
13. The SP verifies the OTP with the AS.
14. If the OTP is valid, the SP authenticates the client and grants access to the service.

Explanation:

This is the sequence of events that happens before the successful authentication of a client using the mobile OTP solution.

Step 3

MutualAuthentication

Mutual authentication is achieved by the following steps:

1. The authenticator authenticates the AS by verifying the MAC that it sends with the challenge and OTP.
2. The AS authenticates the client by verifying the OTP that it sends back to the authenticator.

By mutually authenticating each other, the client and the AS can ensure that they are communicating with the correct entities. This helps to prevent man-in-the-middle attacks and other security threats.

Explanation:

The mutual authentication and the benefits of it are explained here.

Answer

Mobile OTP authentication with mutual authentication is a secure way to authenticate users by using a one-time password (OTP) generated by the user's mobile device. The authentication server verifies the OTP to ensure that the user is who they say they are.

Mutual authentication is achieved by the authenticator authenticating the service provider and the service provider authenticating the client. This helps to prevent man-in-the-middle attacks and other security threats.

Here is an example of how mobile OTP authentication with mutual authentication can be used:
Alice tries to log in to her online banking account. The bank's server sends a challenge and OTP to Alice's mobile device. Alice enters the OTP into her mobile device and sends it back to the bank's server. The bank's server verifies the OTP and authenticates Alice. Alice is then granted access to her online banking account.

Mobile OTP authentication with mutual authentication is a secure and convenient way to authenticate users and is used by a variety of online services.

Was this solution helpful? 1

What would you like to do next?

Send my question to an expert