SLH-2022

Test #2

15-12-2022

You have until the end of the semester to provide a report (in a pdf) answering the following questions. The goal of this test is to study the OAuth2 standard. You can use different resources to study the protocol. For instance :

— https://oauth.net/2/

— The following book : *OAuth 2 in Action* by Justin Richer and Antonio Sanso, available for free within the school network on http://go.oreilly.com/hes-so

1 Questions

1. You are developing a software that takes the Facebook friends of a user and displays a nice friendship graph out of it. For this, you need to somehow gain access to the Facebook account of the user. Why isn't it recommended in this case to use passwords ? Give all the reasons you can think of.
2. Let's suppose that you are using OAuth2 for managing the authorization of your Facebook friendship graph website. Draw a schema describing what are the interactions between your app, Facebook, and the user for a legitimate request (obtaining Facebook friends) and for an illegitimate request (e.g. obtaining the private messages of the user). Explain which mechanism will disallow the app to recover private messages.
3. Your Facebook friendship graph website runs only over HTTP. Although this is bad, you cannot change this. You decide to use the OAuth2 protocol for authorization. However, by default, the requests are not signed (unlike in OAuth1). What could an adversary do ? Be precise and provide an example. Provide also a detailed technical solution that would fix the problem. Don't forget to propose algorithms. Explain also how the keys are managed.
4. In our scenario, how would a user revoke access to his account ? Explain technically what it implies. What prevents a malicious application to reuse some previously generated tokens ?
5. In your Facebook friendship graph software, what information would typically contain all the JWTs used by OAuth2 ? Would you need to encrypt the token ? Justify. What expiration time would you typically set ?
6. PKCE is an extension to OAuth2 to make it more secure.
   (a) Draw a scheme describing the interactions between Facebook, your app and the user in the case PKCE is enabled. Be technically precise (e.g. use terms like "hash functions"...)
   (b) What type of attacks are prevented by PKCE in our scenario ? Explain how the attack works.
   (c) What are the differences between having PKCE enabled and using a client secret ? Are the attacks prevented by both mechanisms identical ?
7. JWT tokens can be
   — encrypted or not
   — Signed using a public key cryptography algorithm (digital signature)
   — Signed using a MAC algorithm (symmetric key cryptography)
   Give a real world example of each usage (encrypted, not encrypted, digital signature, MAC). Justify your answer.