Security Protocols and Application — Final Exam

Philippe Oechslin and Serge Vaudenay

19.6.2018

Family Name: . . . .

Given Name: . . . .

SCIPER: . . . .

- duration: 3h00
- no document allowed
- a pocket calculator is allowed
- communication devices are not allowed
- the exam invigilators will not answer any technical question during the exam
- the answers to each exercise must be provided on separate sheets
- readability and style of writing will be part of the grade
- do not forget to put your name on every sheet!

1 Attacks on GCM

Q.1 Explain the following acronyms: GCM, TLS, AEAD.
Briefly explain what they are and what they are used for.

Q.2 Where did the BlackHat 2016 speakers got their slides from?

Q.3 In GCM, there is an algorithm $\mathsf{GHASH}_L(A,C)$ with key L, associated data A, and ciphertext C which first encodes A and C into a sequence $X_1,\ldots,X_\ell$ then compute

$$\mathsf{GHASH}_L(A,C) = \sum_{i=1}^{\ell} L^{\ell-i+1} X_i$$

How additions and multiplications are performed?
Explain how GHASH is used and how is L computed in GCM.

Q.4 Take two random messages (A,M) and (A',M') which are encrypted with the same IV into (C,T) and (C',T'), respectively.
Give an efficient algorithm to produce a short list containing L.
What can an attacker do with this?

Q.5 We assume that the IV in GCM is composed of a 32-bit salt which is constant, a 64-bit random nonce, and a 32-bit counter for the blocks of the message.
If we encrypt n messages, what is the probability to have a repeating IV?
How large should n be to have good chances?

Family Name: . . . .

Given Name: . . . .

SCIPER: . . . .

2 Oauth

Q.1 In OAuth1, when a third party application registers on a service provider, it gets a Consumer Key (App ID) and a Consumer Secret.

- What is the Consumer Secret used for ?
- In which of the messages shown in Figure Q.1 is it used ?

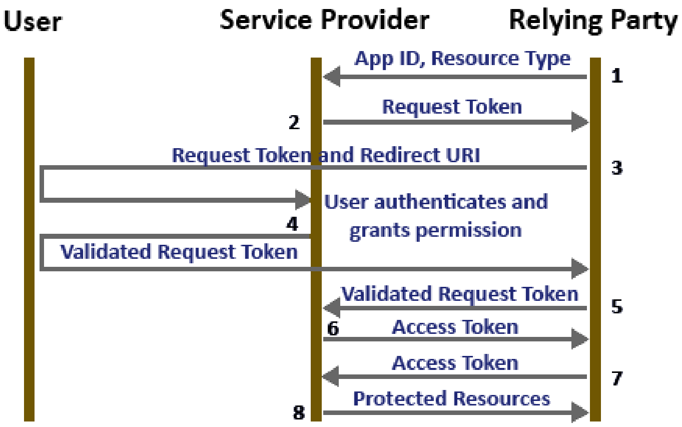

Fig. 1. Oauth1 messages

Q.2 In some version of the Pinterest mobile application the Consumer Secret could be extracted from the application.

- Describe a scenario starting with a hacker extracting the Consumer Secret from the Pinterest app on his phone and ending with the hacker accessing the photos of a victim's Facebook account

Q.3 In Oauth2 implicit flow, the relying party uses an App ID but no secret key. Also, the access token is not bound to a relying party. It can be used by anybody to access the data.

- What is the App ID used for ?
- Give an argument why it could be a good idea to not use a secret
- Describe an attack that would allow a malicious app to access a victim's Facebook account when the victim logs into Spotify using Facebook as service provider.

Q.4 The Oauth2 authentication flow can prevent some attacks that are possible with Oauth2 implicit flow.

- In the case of **implicit flow**, describe an attack that would allow a malicious app to access a victim's Spotify account when the victim logs into the malicious app using Facebook as service provider.
- Explain how **authentication flow** can prevent this attack.
- In particular, explain what verification the service provider must carry out to prevent this type of attacks.

Q.5 What are the two most important information that the service provider should display in the consent form ?

Q.6 Some mail clients, e.g. Thunderbird, have the option to use Oauth2 to authenticate to the mail server. Google recommends this method instead of authentication with username and password.

- Explain why it is safer to use Oauth2 authentication than username/password authentication.

Q.7 One way to redirect a user to a service provider from within a mobile application is to embed a browser into the application (a so-called *webview*. When the user clicks on “authenticate with Facebook”, the embedded browser is opened and loads the Facebook consent page.

- Explain why using a webview is dangerous. What risk is the user exposed to ?
- Describe another redirection mechanism that exist on mobile phones that does not require a webview.
- Describe a how this mechanism can verify that the redirections are not being intercepted.