Home Assignment 4 - EITN41

A-2 What problem in OTR is solved using the Socialist Millionaire Problem?

Answer: In the first scenario (section 1.4 in the lecture notes) it is assumed that Alice and Bob knows each other's public keys, mitigating the risk for a potential MitM attack. The problem solved by SMP is the agreement on keys, here Alice and Bob does not need to know each other's public keys in advance 1/1 - True, the adaption of SMP in OTR is used to limit the chance of a MITM attack to one chance during the AKA according to page 3 in the OTR lecture notes.

A-4 How is perfect forward secrecy solved in OTR?

Answer: A MAC is calculated on each message, after every message the MAC key used for that message is released and a new one is calculated/agreed upon for the next message. This means that the MAC keys are 'fresh' for only one message and that any later use of it directly gives the attacker away 1/1 - True, a new key is agreed on for each message which in turn makes every message a new session and provides perfect forward secrecy. Source: pages 4-5 in the OTR lecture notes.

A-7 Why does not an IdP send a response to an authentication request with the HTTP GET method? What alternatives are there?

Answer: Partly because a GET is an insecure method, all parameters are included in the URL and GETs can be cached and also stored in browser history potentially enabling someone to use an earlier authentication without doing a present authentication, partly because the parameters are included in the URL, and the size of the response is usually larger than the Subjects user-agent (e.g. browser) can handle. An alternative is an artifact binding. 1/1 - True according to HTTP GET specification and pages 4-5 in the SSO lecture notes.

A-9 Name and describe four problems in SAML. You should be able to provide a more detailed description for one of them.

Answer:

- SAML requires a trust relationship between IdP and SP
- ?
- ?
- ?

0.25/1 - The given answer is true according to page 10 in the SSO lecture notes.

A-11 Describe and compare "discovery" in SAML and OpenID

Answer: "Discovery" is in the lecture notes defined as a method for an SP/RP "to get information about how to proceed with the authentication request."

OpenID: this can be done either by finding an XRDS document with the necessary information or by finding an HTML page that holds the information. SAML: does not specify how to do this. There exists a SAML profile called "SAML identity provider discovery profile" that can be used for this. The SP can also use another service for this. 1/1 - True according to page 4 and 8 in the SSO lecture notes.

A-12 In a certain sense, there are three different types of communication in SAML and two in OpenID. Describe them and explain the difference

Answer:

- OpenID
  - Direct Communication: can only be initiated by RP. RP sends direct requests to OP
  - Indirect Communication: can be initated by RP or OP. Messages are passed through the user-agent.
- SAML
  - IdP initiates communication.

– SP initiates communication.

– ?

0.8/1 - True according to page 3 and 7 in the SSO lecture notes.

A-18 In OAuth, explain why the access token must not be cached, and how this is achieved

Answer: The Authorisation Server returns an access token with a 200, the data in JSON format. The 200 has header options telling the receiver (Client) to not cache the token (and data). Cache-Control: no-store, this is the don't cache command, if you will. `https://tools.ietf.org/html/rfc7234#section-5.2.1.5` Pragma: no-cache, this is mostly used for backwards compatibility, `https://tools.ietf.org/html/rfc7234#section-5.4`. If HTTP 1.0 is used, CacheControl is not understood, in this case Pragma specifies don't cache. If CacheControl is understood, Pragma is ignored. 0.5/1 - True according to pages 13-14 in the SSO lecture notes. -0.5 due to lack of reasoning of why the token must not be cached..

A-20 What is a grant? Name and describe a few different grants

Answer: It is a sort of attestation, or authorisation promise. The Resource Owner grants a Client access to certain resources the Owner owns. This can be used by the Client to request an Access Token from the Authorisation Server. The process for this can be different for different types of grants. The four types / classes described in the lecture notes are:

- **Authorisation code -** the Client receives a code, which is used when they request access from Authorisation Server.
- **Implicit grant -** the Client receives a token directly from the Authorisation Server
- **Resource Owner Password Credentials grant -** Resource Owner gives Client their own login credentials for the Authorisation Server. Using these, the Client receives a token from the server.
- **Client Credentials grant -** Here the Resource Owner is not involved. The Client directly from Authorisation Server after provding their own credentials

1/1 - True according to pages 11-12 and page 14 in the SSO lecture notes.