Home Assignment 4

A-1 Explain the purpose of using a MAC instead of a digital signature in OTR.

One of the goals of the OTR protocol is *deniability*, i.e. that after a conversation, both parties can deny having sent messages. If digital signatures are used for authenticating messages, it is not possible to deny them at a later stage. This is because digital signatures provides non-repudiation. Therefore, MACs are used instead.

A-3 Why is the Socialist Millionaire Problem not useful in TLS? Or would it be?

The socialist millionaire problem is used for sharing and comparing values without actually revealing the value. This is done with the help of shared secrets which prohibits man-in-the-middle attacks.

TLS provides privacy and data integrity between two or more communicating parties. With the help of a TLS handshake which for example utilizes Diffie-Hellman key exchange, the two parties can know that their communication channel is well-protected. The Socialist Millionaire Problem can be useful in TLS if the two parties for example wants to control that their symmetric key is the same. However, since TLS is widely used and considered reliable, this "control" might not be useful.

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

The HTTP GET method is not allowed since the response is too big to fit within the maximum URL length. Alternatives are to send the authentication request as an HTTP POST binding or as an HTTP artifact binding for example.

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

In SAML, the *identity provider discovery profile* settles concepts such as: common domain and common domain cookie. In short, a discovery service in SAML is used to allow users to pick their own IdP. In OpenID, *discovery* is when the RP (relying party) uses the identifier to determine which OP (OpenID Provider) to use for authenticating a user. RP and OP corresponds to SP (service provider) respectively IdP (identity provider) in SAML. Therefore, in SAML, the users can choose IdP whereas in OpenId that is not the case.

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.

The types of communications in SAML are referred to as bindings. The three types of bindings are: HTTP POST binding, HTTP redirect binding and HTTP artifact binding. The HTTP redirect binding transfers data using HTTP redirects, while HTTP POST transfers data with HTTP POST forms. Artifact binding is instead used if the requester and responder needs to communicate using an HTTP user agent as an intermediary.

In OpenId the types of communication are *indirect* and *direct* communication. Direct communication can only be initiated by the RP. In comparison, indirect communication can be initiated by either the RP or the OP.

A-13 Describe two use cases — one where SAML and one where OpenID appears to be the best choice, respectively.

SAML is more static and requires that the IdP and SP know each other beforehand. This makes it more suitable when IdP wants to fully know who's accessing the data. A use case may be a communication between a bank and a customer where the bank may want to restrict the users to some predefined services.

OpenID is more lightweight and dynamic. It builds trust by sending HTTP calls. It is much easier to accept users from different providers. OpenID is therefore more common than SAML and used in for example consumer websites, web apps and mobile apps.

A-17 What is the purpose of the Yadis protocol?

The purpose of the Yadis protocol is to retrieve XRDS documents from URLs. It is used if the User-Supplied Identifier is a URL instead of an XRI.

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

A grant is a type of method for obtaining access tokens, which are used for authentication. Here are a few different types of grants:

Client credentials grant: The client uses his or her own credentials in order to obtain an access token. It is the simplest of all OAuth 2.0 grants.

Authorization code grant: The most common grant. Here the user and client exchange an authorization code for an access token.

Refresh token grant: Used when an access token has expired. The client can submit a refresh token grant and receive a new, fresh access token.