Questões - Trabalho 2

**1. No contexto do protocolo TLS:**

**1.1. Qual o material criptográfico (certificados e chaves) que têm de ser configurados no cliente caso seja necessário autenticação de cliente e de servidor?**

RSA🡪 dominante de key exchange

Diffie-Hellman 🡪 este key Exchange é usado para reduzir o risco de ser comprometido

**1.2. Qual o esquema simétrico usado no handshake do TLS e quais os objetivos da sua utilização?**

Protocolo de Handshake do TLS trata da criação de conexão segura e manuseamento, principalmente para assegurar os parâmetros do record protocol.

O esquema simétrico de encriptação (Symmetric encryption scheme), é usado para suportar os esquemas de bloco e de stream. São utilizados para transferir dados com a chave simétrica durante o key-exchange

Handshake Protocol

– Handles the secure connection creation and management, namely the secure establishment of the record protocol cryptographic parameters

**1.3. Qual a característica do record protocol que o torna suscetível a ataques baseados no de Vaudenay?**

Record protocol tem a característica de authenticate-then-encrypt que o torna vulnerável aos ataques baseados no de Vaudenay. O TLS utiliza o padding como maneira de chegar ao bloco correto ou incorreto fazendo downgrading. O servidor responde dizendo se o padding está correcto ou errado. Permitindo vários ataques poodle, podendo fazer um ataque a cada downgrade que acontece.

<https://www.us-cert.gov/ncas/alerts/TA14-290A>

Record Protocol

– Handles data fragmentation, compression, confidentiality and message authentication

– Requires a reliable transport protocol

<https://moxie.org/blog/the-cryptographic-doom-principle/>

<https://crypto.stackexchange.com/questions/202/should-we-mac-then-encrypt-or-encrypt-then-mac>

\*\*Fragment, Compress, Authenticate (MAC) then Encrypt • Two independent connection directions – Separate keys, IVs and sequence number (client write and server write)

The MAC protects the : sequence number, packet type, version and the payload

<https://technet.microsoft.com/pt-pt/library/cc783349(v=ws.10).aspx>

**2. No contexto da framework de autorização OAuth 2.0 :**

**2.1. Como é que o cliente/relying party especifica os recursos a que pretende ter acesso?**

Os clientes têm de se registar no servidor de autorização, sendo-lhes atribuído um client\_id. Para alguns é também atribuído um client\_secret, usado pelo cliente no servidor de autorização

Relying party guarda o client\_id e cliente\_secret.

O cliente/ relying party especifica os recursos a que pretende ter acesso indicando um access token. Para obtenção de um access token há quarto Grant flows: cliente credentials, resource owner password, authorization code and implicit.

**2.2. Quais as limitações da utilização deste protocolo para autenticação?**

**A utilização do protocolo para autenticação**

**3. No contexto do fluxo authorization code do protocolo OpenID Connect:**

**3.1. Para que serve o ID Token?**

OpenID Connect é uma camada de identidade simples criada com base no protocolo de OAuth 2.0. O ID Token é um token de segurança que contem os pedidos de autenticação de um utilizador através de um servidor de autenticação. Verifica a identidade do utilizador e fornece informações de perfil básicas sobre o utilizador.

O ID *token* guarda as informações sobre um utilizador autentificado e serve para transferir estas informações de forma segura do *identity provider* para o *relying party*.

**3.2. Qual destas duas entidades desempenha o papel de relying party: a aplicação cliente ou o resource server?**

O resource server desempenha o papel de relying party, sendo o *relying party* um servidor que estamos a aceder na qual irá direcionar para um servidor autentificador.

A aplicação cliente desempenha o papel de relying party, o OpenID Connect retorna o resultado da autenticaçao realizada pelo servidor ao cliente, de uma maneira segura de forma que o cliente possa confiar.