

**Instituto Superior de Engenharia**

**de Lisboa**

**Engenharia Informática e de Computadores**

***SEGURANÇA INFORMÁTICA***

***2ºSÉRIE***

Docente: José Simão

Filipe Fé nº 42141

Inês Gomes nº 42160 José Cunha nº 43526

**Índice**

**Exercício 1** ..................................................................................................................................... 2

[**1.1** 4](#_Toc6200)

[**1.2** 7](#_Toc6201)

[**1.3** 7](#_Toc6202)

[**Exercício 2** 8](#_Toc6203)

**Exercício 1**

**1.1)**

Estamos perante o caso em que tanto o cliente como o servidor se querem autenticar, ou seja, existe uma autenticação mútua. No contexto do protocolo TLS, os materiais criptográficos necessários que têm de ser configurados no cliente são:

* Um conjunto de certificados de raiz de forma a verificar se o certificado enviado pelo servidor é válido.
* O seu próprio certificado com um par de chaves associado, que será enviado ao servidor que futuramente irá validar esse mesmo certificado junto dos seus conjuntos de certificados de raiz.

**1.2)**

O esquema simétrico usado no handshake do TLS é o de cifra simétrica, onde o cliente cifra com a chave pública do servidor uma mensagem com um número aleatório “ R ” (desafio). O servidor, se tiver na posse da mesma chave que foi usada na cifra consegue desencriptar o desafio lançado pelo cliente e devolver uma resposta a comprovar a posse desse número aleatório.

Os objetivos deste protocolo de handshake do TLS é garantir que primeiramente são negociados os parâmetros a usar no processo de encriptação para que depois exista uma autenticação do lado do servidor e/ou do lado cliente.

Depois de ser estabelecida uma chave segura a ser usado por ambos é garantido que o canal de comunicação é seguro.

**1.3)**

O record protocol é responsável pela transferência de blocos de dados entre os dois intervenientes na comunicação. Através dos parâmetros negociados no handshake, é gerada uma marca de autenticidade (através do MAC) e os dados são encriptados para futuramente serem enviados ao cliente ou ao servidor.

O problema é que um atacante pode dedicar-se a tentar descobrir o padding válido usado nas mensagens encriptadas por um desses intervenientes, como é descrito em ataques baseados no de Vaudenay. Para esse efeito basta guardar as mensagens que foram trocadas entre o cliente e o servidor e mais tarde usar a técnica descrita. Desta forma consegue obter a chave usada no processo de cifra. Caso o servidor tenha essa chave do seu lado e esta seja de longa duração, neste momento é possível ao atacante decifrar as mensagens que são enviadas nesse canal de comunicação (até a chave ser alterada).