Respostas

1 –

1. No *record protocol* a autenticidade nas mensagens é garantida pela utilização do MAC (*Message Authentication Codes*).
2. A deteção de inserção ou adulteração maliciosa da mensagem é realizada do seguinte modo:
3. Após a definição dos algoritmos de encriptação, o cliente gera um sequência confidencial (*pre master secret*) cifrada com a chave pública do servidor.
4. Numa faze seguinte, com a sua chave privada, o servidor irá decifrar essa sequência gerada pelo cliente, após a qual será calculada o algoritmo HMAC da mesma juntamente com todas as mensagens enviadas anteriormente.
5. Após receber o HMAC do servidor, o cliente poderá confirmar a sua integridade calculando o algoritmo HMAC por si próprio e comparar com a enviada pelo servidor.
6. Caso o resultado calculado pelo cliente for diferente do calculado e enviado pelo servidor, conclui-se que houve alguma inserção/adulteração das mensagens.
7. O estabelecimento da *pre master secret* apenas através da chaves pública e privada não garante o *perfect foward secrecy* uma vez que todo o processo é dependente da confidencialidade da chave privada do servidor, caso esta seja comprometida, é possível que o atacante aceda às chaves e aos IVs o que, por conseguinte, caso tenha acesso as sessões de *handshake* anteriores conseguirá decifrar as mensagens.

2 – Num cenário em que o atacante tenha acesso ao *hash* do utilizador e ao respetivo *salt*, o processo será totalmente dependente da robustez da palavra-passe e o número de tentativas será um fator inafetivo. Ou seja, neste caso especificamente, há duas possíveis vertentes:

1. Caso a palavra-passe do cliente seja robusta o suficiente para não estar presente no dicionário o ataque será inútil.
2. Caso a palavra-passe esteja no dicionário, é certo que o atacante através de uma procura exaustiva chegue a palavra-passe comparando o hash deste cliente com o hash de cada palavra-passe do dicionário juntamente com o *salt* deste mesmo utilizador, o que levará, consequentemente, a necessidade de apenas uma única tentativa no processo de autenticação.

3 –

1. Já pensado.