Atividade Redes

Mirela Mei - 11208392 - Turma 04
Alexandre Kenji Okamoto - 11208371
Fernanda Cavalcante Nascimento - 11390827
Gabriel Afonso Carnaiba Silva - 11270886
Karina Duran - 11295911

1. Quando você acessa uma página web com TLS, onde no seu dispositivo está implementado este protocolo?

O TLS está implementado na camada de aplicação. Do ponto de vista do desenvolvedor, ele é um protocolo de transporte que provê serviços do TCP aprimorados com serviços de segurança.

2. Explique quais são todas as mensagens do handshake do TLS (ou seja, que o cliente e o servidor trocam, após o cliente pedir uma conexão segura ao servidor, até que possam começar a enviar os dados da camada de aplicação). Essa resposta deve dizer quais dados são enviados em criptografia, quais usam criptografia de chave pública e quais de chave simétrica. Deve também incluir a negociação de algoritmos de criptografia e hash a serem utilizados; como e para que o certificado digital do servidor é usado; o que é o pre master secret gerado pelo cliente e quais segredos são gerados no cliente e no servidor a partir dele. Deve incluir, por fim, para evitar qual tipo de ataque serve a troca de resumos das mensagens anteriores feita nas mensagens finais do handshake.

1. O cliente envia uma lista de algoritmos criptográficos que ele suporta, junto com um nonce do cliente.
2. A partir da lista, o servidor escolhe um algoritmo simétrico (por exemplo, AES), um algoritmo de chave pública (por exemplo, RSA com um comprimento de chave específico) e um algoritmo MAC. Ele devolve ao cliente suas escolhas, bem como um certificado e um nonce do servidor.

3. O cliente verifica o certificado, extrai a chave pública do servidor, gera um Segredo Pré-Mestre (PMS), cifra o PMS com a chave pública do servidor e envia o PMS cifrado ao servidor.
4. Utilizando a mesma função de derivação de chave (conforme especificado pelo padrão SSL), o cliente e o servidor calculam independentemente o Segredo Mestre (MS) do PMS e dos nonces. O MS é então dividido para gerar as duas chaves de criptografia e duas chaves MAC. Além disso, quando a cifra simétrica selecionada emprega o CBC (como 3DES ou AES), então dois Vetores de Inicialização (IVs) — um para cada lado da conexão — são também obtidos do MS. De agora em diante, todas as mensagens enviadas entre o cliente e o servidor são cifradas e autenticadas (com o MAC).
5. O cliente envia um MAC de todas as mensagens de apresentação.
6. O servidor envia um MAC de todas as mensagens de apresentação.
   As duas últimas etapas protegem o handshake da adulteração.

3. Após o handshake, as mensagens trocadas entre cliente e servidor via TLS usam criptografia de chave pública ou simétrica? Usam resumos de mensagem? Se sim, como e para que?

Criptografia de chave simétrica.
Sim, para fornecer integridade. Para autenticação do servidor, o cliente utiliza a chave pública do servidor para criptografar os dados que são utilizados para calcular a chave secreta. O servidor poderá gerar a chave secreta somente se puder descriptografar esses dados com a chave privada correta. Para a autenticação do cliente, o servidor utiliza a chave pública do certificado do cliente para decriptografar os dados enviados pelo cliente pelo protocolo de reconhecimento. A troca de mensagens concluídas que são criptografadas com a chave secreta confirma que a autenticação está completa.

4. Explique como e para evitar que ataques são usados nonces e números de sequência no TLS.

Os nonces são usados para proteger o “ataque de repetição de conexão”. Eles são um número aleatório R que compõe o MAC e que só pode ser usado para

cada sessão TCP, fazendo com que as chaves de criptografia sejam diferentes.

Os números de sequência são usados para defender a repetição de pacotes individuais durante uma sessão em andamento. É um contador de números de sequência que se inicia no zero e vai aumentando para cada registro SSL, assim não é possível alterar a ordem, duplicar ou excluir.