Série nº2 Segurança Informática

Realizado por:

Diogo Leandro nº 44868

João Barata nº 44857

Questão 1:

1. Considere o sub-protocolo handshake do TLS:

1.1.  Em que situação é usado um esquema de assinatura digital? Poderia ser substituído por um esquema MAC?

R: TLS é um protocolo de encriptação desenhado para garantir comunicações seguras na internet. Um aperto de mão TLS é o processo que sinaliza o começo da sessão de comunicação. Durante o aperto de mão os dois intervenientes na comunicação trocam mensagens garantindo reconhecimento entre si, verificam identidades, estabelecem os algoritmos q irão utilizar e acordam as chaves de sessão.

Na autenticação do servidor é utilizado um esquema de chaves públicas nomeadamente um esquema de assinatura digital. Não poderia ser substituído por um MAC, devido ao problema de non repudiation em que o emissor não consegue confirmar que foi o mesmo quem mandou a mensagem o que faz com que a autenticação seja impossível.

1.2.  No excerto de texto ≪[...] perfect forward secrecy prevents the recovery of information that was encrypted with older session keys≫, presente no RFC 7525 sobre recomendações para uso seguro do TLS, quais são as chaves de sessão referidas e como poderiam ser obtidas pelo atacante?

R: São as chaves de longo termo que tornam possível a desencriptação da chaves de sessão e posteriormente de todas as mensagens trocadas.

Podemos obter essas chaves através de:

* O cliente ou o servidor serem atacados por uma Terceira parte e a chave privada ser alcançada.
* Uma chave de longo termo ser obtida através de um dispositivo que foi vendido e que não foi limpo apropriadamente.
* Uma chave de longo termo ser utilizada num dispositivo como chave padrão.
* Uma chave gerada por uma trusted party como a CA, mas que mais tarde é obtida através de extorsão ou compromisso.
* O uso de chaves assimétricas com tamanhos insuficientes.
* Ataques contra administradores de sistema.
* Coleção de chaves privadas provenientes de backups mal protegidos.

Questão 2:

1. O RFC 8018, Password-Based Cryptography Specification, especifica um algoritmo para transformar uma password numa chave simétrica. Qual o papel do salt nesse processo?

R: O Salt é uma string de 8 bits gerada aleatoriamente e é usado para proteger as senhas no seu armazenamento, permite a defesa contra ataques de dicionário porque é especifica para cada utilizador. O papel do salt no processo de transformação de uma password numa chave simétrica é de dificultar bastante o processo de descoberta da chave por parte do atacante, isto acontece porque basta o salt ter um tamanho de 64 bits para existirem 2^64 chaves para cada password.

Questão 3:

1. Descreva como pode uma aplicação web garantir a autenticidade dos cookies que usa para manter estado de sessão, desde a geração à verificação.

R: O cookie de sessão contém um identificador de números aleatórios que é utilizado para indexar o cookie no cache de sessão do servidor, nenhuma outra informação é exposta no cookie de sessão. Esse cookie de sessão não pode prejudicar o critério de segurança.

Além disso o cookie de sessão não pode ser transmitido a nenhuma máquina diferente da que gerou esse cookie.

Questão 4:

No contexto da framework de autorização OAuth 2.0:

4.1.  Qual o objetivo do parâmetro scope

R: O objetivo do parâmetro scope é de limitar o acesso da aplicação aos dados do utilizador, para isso é apresentado um ecrã onde o utilizador tem de dar o seu consentimento para a aplicação utilizar os seus dados.

4.2.  Admitindo que um atacante consegue ver toda a informação de e para o browser da vítima, é possível saber o client secret de uma determinada aplicação web cliente? E o client id?

R: O client\_id é o identificador do utilizador para a aplicação. É um código único e é suposto ser difícil descobrir este identificador. Ao contrário do client\_id que é um identificador público, o client\_secret é um identificador secreto que só a aplicação conhece.

Desta forma podemos concluir que o client\_id é possível ser descoberto pelo atacante, mas no entanto, o client\_secret não tem estas propriedades.

4.3.  No contexto de um pedido de autorização desencadeado por uma aplicação cliente, depois do utilizador se autenticar no servidor de autorização e dar consenso, é enviado à aplicação cliente a identidade do utilizador?

R: Não, é dado um code que mais tarde irá ser substituído por um access\_token que permite à aplicação pesquisar dados referentes ao utilizador autenticado.

Questão 5:

1. No contexto do fluxo authorization code do protocolo OpenID Connect, para que serve o ID Token?

R: O id\_token é usado para guardar em cache informações acerca do perfil do cliente (claims) e disponibilizá-las para as aplicações permitindo uma melhor performance.