Instituto Superior de Engenharia de Lisboa

Licenciatura/Mestrado em Engenharia Informática e de Computadores

Segurança Informática

Segunda série de exercícios, Semestre de Inverno de 13/14

Data de entrega: 18 de Novembro de 2014

---

1. Qual a utilidade de garantir a integridade de um *key store* onde apenas são guardados certificados auto-assinados?

2. No contexto do protocolo SSL/TLS

   2.1. Considere que o servidor malicioso S_1 realiza uma instância do protocolo *handshake* com o cliente C. Como é que este protocolo impede que S_1 se possa autenticar como C perante um outro servidor S_2, nomeadamente através do reenvio das mensagens que C enviou para S_1.

   2.2. Em que contexto e com que objectivo são usados esquemas de assinatura digital?

   2.3. O que é e qual a importância da propriedade *Perfect Forward Secrecy*?

3. No contexto do armazenamento de informação de verificação para esquemas de autenticação baseados em *passwords*:

   3.1. O *salt* deve ser armazenado cifrado?

   3.2. Quais as consequências de usar um *salt* constante?

4. No contexto da norma OAuth 2.0

   4.1. Qual a diferença entre o *Resource Owner* e o cliente?

   4.2. Qual a razão pela qual o cliente não se autentica quando realiza o pedido de *authorization request* ao *Authorization Endpoint* (fluxo *Authorization Code Grant*)?

   4.3. Quais os problemas dos *bearer tokens*?

5. Realize um programa que, dado o *hostname* para um *site* com suporte HTTPS, apresenta:

   - Informação sobre a validade do certificado do servidor (e.g. validade temporal, cadeia de certificados, adequação ao *hostname*).
   - A cadeia de certificados do servidor.
   - A menor data de expiração dos certificados do servidor.
   - As versões dos protocolos SSL e TLS suportadas (de entre as disponíveis na plataforma Java).

6. Realize uma aplicação Web com a seguinte funcionalidade:

   - Autenticação baseada no fornecedor de identidade social da Google, usando o protocolo OpenID Connect.
   - Apresentação de *issues* do GitHub.
   - Criação de *tasks* Google a partir de *issues* do GitHub.

ISEL, 21 de Outubro de 2014.