Instituto Superior de Engenharia de Lisboa

Licenciatura/Mestrado em Engenharia Informática e de Computadores

Segurança Informática

Teste final, primeira época, Semestre de Inverno, 09/10

Duração: 2 horas e 30 minutos

---

1. (3) No contexto dos esquemas criptográficos

   1.1. O conceito de *modo de operação* aparece tipicamente associado aos esquemas de cifra simétricos mas não aos assimétricos. Porquê?

   1.2. Na JCA (*Java Cryptography Architecture*), existe uma sobrecarga do método `Signature.initSign` que recebe um `SecureRandom`. Contudo, porque é que não existe nenhuma sobrecarga do método `Signature.initVerify` que receba também um `SecureRandom`.

2. (4) Considere os certificados definidos pela norma X.509 e a *Java Certification Path API*.

   2.1. Descreva, de forma resumida, o processo de validação dum certificado?

   2.2. Qual a informação que tem de ser parametrizada na construção de cadeias de certificados?

   2.3. Ambas as *engine classes* `KeyStore` e `CertStore` podem armazenar certificados. Quais os aspectos a considerar para a utilização de uma ou de outra classe?

3. (4) Considere o protocolo *Secure Socket Layer* (SSL).

   3.1. Quais seriam as consequências para a segurança do protocolo se a mensagem `ClientHello` não contivesse um *nounce*?

   3.2. Qual o propósito da lista de *trust anchors* enviada pelo servidor para o cliente?

   3.3. De que forma é realizada a autenticação do servidor?

4. (4) Considere a família de modelos de controlo de acesso RBAC (*Role Based Access Control*)

   4.1. Descreva o que é e qual a motivação para o conceito de *role hierarchy*?

   4.2. Quais as vantagens do modelo $RBAC_2$, em relação ao modelo $RBAC_0$, na implementação do princípio de *separation of duty*?

   4.3. A plataforma .NET possui suporte parcial para o modelo $RBAC_0$. Neste contexto, de que forma é implementada a relação *Permission Assignment*?

5. (1) Considere a plataforma .NET e o modelo de segurança CAS (*Code Access Security*). O objectivo da assinatura digital dos *assemblies* é a associação destes a nomes não forjáveis. Uma alternativa seria o nome do *assembly* conter o valor de *hash* do seu conteúdo, em vez da chave pública de verificação da assinatura. Quais as desvantagens desta alternativa?

6. (2) Considere o seguinte conjunto de certificados SDSI.

   a) $K_{IPL}\ aluno \longrightarrow K_{IPL}\ departamento\ \ aluno$
   b) $K_{IPL}\ departamento \longrightarrow K_{IPL}\ escola\ \ departamento$
   c) $K_{IPL}\ escola \longrightarrow K_{ISEL}$
   d) $K_{IPL}\ escola \longrightarrow K_{ISCAL}$
   e) $K_{ISCAL}\ aluno \longrightarrow K_{123}$
   f) $K_{ISEL}\ departamento \longrightarrow K_{DEETC}$
   g) $K_{ISEL}\ aluno \longrightarrow K_{456}$
   h) $K_{DEETC}\ aluno \longrightarrow K_{789}$

   Quais as chaves que pertencem ao nome $K_{IPL}\ aluno$? Para cada chave, apresente a prova desta pertença.

7. (2) Caracterize o tipo de erro de programação que possibilita os ataques do tipo *SQL injection*? De que forma a implementação do princípio de *least privilege* minimiza as consequências dum ataque deste tipo?

16 de Janeiro de 2010