Instituto Superior de Engenharia de Lisboa

Licenciatura/Mestrado em Engenharia Informática e de Computadores

Segurança Informática

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

Duração: 2 horas e 30 minutos

---

1. (4) Considere o contexto dos esquemas criptográficos e da *Java Cryptography Architecture*

   1.1. Considere uma função de *hash* h definida da seguinte forma:

   - Seja $m = m_1, \ldots, m_L$ a divisão da mensagem m nos blocos m_i, onde cada bloco tem 256 bits de dimensão ($m_i \in \{0,1\}^{256}$) e o último bloco resulta do *padding* da mensagem com bits de valor 0.
   - Seja $h_i = m_i \oplus h_{i-1}$, para $i = 1, \ldots, L$, onde $\oplus$ denota a operação de ou-exclusivo bit a bit e $h_0 = 0$ é o vector inicial.
   - O valor de *hash* é definido por $h(m) = h_L$.

   Esta função de *hash* é uma função de *hash* criptográfica?

   1.2. Quais os aspectos a considerar na decisão de escolha entre a utilização de esquemas MAC (*Message Authentication Codes*) ou esquemas de assinatura digital?

   1.3. Descreva o objectivo dos métodos `init`, `update` e `doFinal` pertencentes à classe `Cipher`, especialmente a diferença entre os métodos `update` e `doFinal`.

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

   2.1. Quais os certificados que têm de ser configurados num servidor HTTPS?

   2.2. A classe `Certificate` possui um método para a obtenção da chave pública mas não possui nenhum método para a obtenção da chave privada. Porquê?

   2.3. Na parametrização da construção duma cadeia de certificados, através da classe `PKIXParameters`, quais são os certificados fornecidos através de objectos `KeyStore` e quais são fornecidos através de objectos `CertStore`? Justifique esta utilização de tipos diferentes para conter certificados.

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

   3.1. 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.

   3.2. Quando o protocolo SSL é usado sem autenticação de cliente, o protocolo *record* também usa um esquema MAC (*Message Authentication Code*) na protecção das mensagens enviadas pelo cliente?

   3.3. O protocolo SSL pode usar certificados X.509 para autenticar o servidor e o cliente. Contudo, o *key usage* requerido para o certificado do cliente e para o certificado do servidor não são iguais. Porquê?

4. (2) Considere a plataforma .NET e o modelo de segurança CAS (*Code Access Security*).

   4.1. A declaração dum *assembly* com *strong name* inclui sempre uma chave pública. Contudo, a referência para um *assembly* com *strong name* pode incluir apenas o *hash* desta chave e não a chave completa. Este facto não representa um problema de segurança?

   4.2. A exigência duma permissão pode implicar ou não um percurso no *stack* da *thread* onde foi realizada esta exigência. Em que circunstâncias é necessário este percurso?

5. (2) Pretende-se implementar uma política de controlo de acesso, baseada no modelo de Bell-LaPadula, sobre um mecanismo que suporta o modelo $RBAC_1$. A política de Bell-LaPadula é caracterizada por:

   - Reticulado constituído pelo seguinte conjunto de etiquetas $\{l_0, l_1, l_2, l_3\}$, onde $l_0 \leq l_1 \leq l_2 \leq l_3$.
   - Conjunto de utilizadores constituído por $\{u_0, u_1, u_2, u_3\}$ onde o *clearance* do utilizador u_i é igual a l_i.
   - Conjunto de recursos constituído por $\{r_0, r_1, r_2, r_3\}$ onde a etiqueta do recurso r_i é l_i. Estes recursos apenas suportam duas operações: escrita e leitura.

   Defina a política $RBAC_1$ que implemente a política de Bell-LaPadula descrita anteriormente. Esta definição deve incluir: o conjunto de permissões, o conjunto de *roles*, o conjunto de utilizadores e as relações RH, PA, UA.

6. (3) Considere o modelo de certificados definido pela SDSI (*Simple Distributed Security Infrastructure*) e as seguintes entidades e nomes locais:

   a) $K_M\ Escola \rightarrow K_M\ Politecnico$

   b) $K_M\ Escola \rightarrow K_M\ Universidade$

   c) $K_M\ Aluno \rightarrow K_M\ Politecnico\ Aluno$

   d) $K_M\ Aluno \rightarrow K_M\ Universidade\ Aluno$

   f) $K_M\ Politecnico \rightarrow K_M\ IPL$

   g) $K_M\ IPL \rightarrow K_{IPL}$

   h) $K_{IPL}\ Discente \rightarrow K_{A123}$

   6.1. Mostre como K_M pode substituir os certificados c) e d) por um único certificado.

   6.2. Qual ou quais certificados têm de ser emitidos por K_{IPL} de forma a que todos as entidades que pertencem ao nome $K_{IPL}\ Discente$ também pertençam ao nome $K_M Aluno$. Usando este novo conjunto de certificados, prove que K_{A123} pertence ao nome $K_M\ Aluno$.

7. (2) No contexto dos ataques baseados em *buffer overflow*, uma das formas de protecção existentes é a proibição da execução de código localizado no *stack* ou no *heap*. Contudo, esta protecção não impede todos os ataques. Porquê?

8 de Fevereiro de 2010