Instituto Superior de Engenharia de Lisboa

Licenciatura/Mestrado em Engenharia Informática e de Computadores

Segurança Informática

Teste final, época especial, Semestre de Inverno de 07/08.

Duração: 2 horas e 30 minutos

---

1. (2) Considere a JCA (*Java Cryptography Architecture*).

   1.1. A criação de uma instância de classe derivada de `Cipher`, através do método estático `getInstance`, requer a definição duma *transformação*. No caso do esquemas de cifra simétricos, essa transformação é definida por três componentes. Descreva cada uma dessas componentes.

   1.2. A criação de uma instância de classe derivada de `KeyGenerator` também requer a definição das três componentes referidas na alínea anterior?

2. (3) Considere a variante do protocolo SSL (*Secure Socket Layer*) com autenticação de cliente.

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

   2.2. De que forma é realizada a autenticação do cliente?

3. (2) Considere a versão simplificada do protocolo *Kerberos* apresentada em seguida

   1. $A \rightarrow T : A, B, N_A$
   2. $A \leftarrow T : ticket_B, E_{kAT}(k, N_A, L, B)$
   3. $A \rightarrow B : ticket_B, authenticator_A$
   4. $A \leftarrow B : E_k(T_A)$

   onde $ticket_B = E_{kBT}(k, A, L)$, $authenticator_A = E_k(A, T_A)$; L é a validade de $ticket_B$ e T_A é a marca temporal de A.

   3.1. Qual a função da componente $authenticator_A$, presente na mensagem 3?

   3.2. Qual a necessidade da presença de N_A na componente $E_{kAT}(k, N_A, L, B)$ da mensagem 2?

4. (3) Considere as infra-estruturas de chave pública baseadas na norma X.509.

   4.1. Um certificado é uma estrutura de dados assinada. Quem produziu esta assinatura? Como é que esta assinatura deve ser verificada?

   4.2. Quais as componentes dum certificado que estão cifradas?

   4.3. Como são localizadas as *Certificate Revocation Lists*?

5. (2) Considere uma extensão ao modelo $RBAC_1$, na qual passa a existir o conceito de grupo de permissões:

   - Um grupo de permissões é um conjunto de permissões.
   - Um grupo de permissões pode ser associado a um ou mais *roles*.

   Mostre como implementar este modelo sobre um mecanismo que suporte o modelo $RBAC_1$.

6. (2,5) Considere a plataforma *Microsoft.NET* e o modelo de segurança *Code Access Security* (CAS).

   6.1. Qual a finalidade da interface `IPermission` e da classe `PermissionSet`?

   6.2. Qual a função da interface `IPrincipal`?

7. (2) Considere os ataques do tipo *buffer overflow*.

   7.1. Para que servem e como são usadas as *guardas* ("canários")?

   7.2. O valor da guarda pode depender do valor a proteger. Porquê?

ISEL, 7 de Abril de 2008.