Instituto Superior de Engenharia de Lisboa

Licenciatura/Mestrado em Engenharia Informática e de Computadores

Segurança Informática

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

Duração: 2 horas e 30 minutos

---

1. (2,5) Considere a variante do protocolo SSL (*Secure Socket Layer*) com autenticação de cliente.

   1.1. Qual o objectivo da utilização de esquemas de cifra assimétrica neste protocolo?

   1.2. Quais as chaves e certificados que têm de ser configurados do lado do cliente?

2. (2) Quais as vantagens apresentadas pelos esquemas MAC (*Message Authentication Code*), quando comparados com esquemas de assinatura digital? No sub-protocolo *Handshake* do protocolo SSL, o esquema de assinatura digital pode ser substituído por uma esquema MAC?

3. (2,5) 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 do *nounce* N_A, presente nas mensagens 1 e 2?

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

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

   4.1. Descreva a utilização da classe `Cipher` na realização incremental (*multi-part*) das operações de cifra e decifra de esquemas simétricos de cifra.

   4.2. Considere a utilização da *engine class* `CertPathValidator` usando o algoritmo "PKIX". A parametrização desta classe, através de instâncias de `PKIXParameters`, usa uma *key store* como parâmetro. Para que serve esta *key store*?

5. (2,5) Considere as infra-estruturas de chave pública baseadas na norma X.509.

   5.1. O que é uma cadeia de certificados (*certificate path*)? Qual a relação entre os sujeitos e os emissores dos certificados presentes numa cadeia válida?

   5.2. Qual a vantagem da existência de autoridades de certificação intermédias?

6. (2) Considere a seguinte política definida sobre o modelo $RBAC_1$:

   - $U = \{u_0, u_1, u_2\}$
   - $R = \{r_0, r_1, r_2\}$
   - $P = \{p_0, p_1, p_2\}$
   - $\{r_0 \preceq r_1, r_1 \preceq r_2\} \subseteq RH$
   - $UA = \{(u_0, r_0), (u_1, r_1), (u_2, r_2)\}$
   - $RA = \{(p_0, r_0), (p_1, r_1), (p_2, r_2)\}$

   Sejam s_0 e s_2 duas sessões tais que $user(s_0) = u_0$ e $user(s_2) = u_2$.

   6.1. É possível que $r_1 \in roles(s_0)$?

   6.2. É possível que $r_1 \in roles(s_2)$?

   6.3. Assumindo que $r_0 \in roles(s_0)$, quais as permissões concedidas a s_0?

   6.4. Assumindo que $r_2 \in roles(s_2)$, quais as permissões concedidas a s_2?

   Justifique todas as respostas.

7. (2) Considere o modelo ACL (*Access Control List*). Neste contexto, os conceitos de *grupo de utilizadores* e de *grupo de objectos* podem ser usados para simplificar a definição de políticas. Por exemplo:

   - Se todos os utilizadores do grupo de utilizadores G_u podem realizar a acção A sobre o objecto O, então apenas é necessário criar uma entrada na ACL de O, concedendo a permissão para realizar A ao grupo G_u.
   - Se o utilizador U pode realizar a acção A sobre qualquer objecto do grupo de objectos G_o, então apenas é necessário criar uma entrada na ACL de G_o, concedendo a permissão para realizar A ao utilizador U.

   Na implementação deste modelo no sistema operativo *Windows*, de que forma são concretizados estes conceitos de *grupo de utilizadores* e de *grupo de objectos*.

8. (2,5) Considere a plataforma *Microsoft.NET* e o modelo de segurança *Code Access Security* (CAS).

   8.1. Qual a finalidade do método `Assert` da interface `IStackWalk`?Justifique a inexistência deste método `Assert` na classe `PrincipalPermission`.

   8.2. Dois *assemblies* com a mesma *strong name evidence* são iguais (têm o mesmo conteúdo)? Dois *assemblies* com a mesma *hash evidence* são iguais?

9. (2) Descreva o que se entende por ataques de *cross site script* (XSS). Quais os objectivos típicos deste tipo de ataque? Que tipo de vulnerabilidades são exploradas?

ISEL, 19 de Fevereiro de 2008.