Instituto Superior de Engenharia de Lisboa

Licenciatura em Engenharia Informática e de Computadores

Segurança Informática

Teste final, época especial, Semestre de Inverno de 06/07.

Duração: 2 horas e 30 minutos

---

1. (2) Qual a utilização das funções de *hash* nos esquemas de assinatura digital? Quais as propriedades que estas funções devem possuir para serem utilizadas nestes esquemas?

2. (4) Considere os certificados definidos na norma X.509.

   2.1. Um certificado contém chave privada?

   2.2. Qual a vantagem da existência de autoridades de certificação intermédias (não raízes)? Estas autoridades têm de ser *trust anchors*?

   2.3. Qual a função e conteúdo da extensão *basic constraints*?

3. (4) 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. Quais os mecanismos existentes neste protocolo para a protecção contra ataques de *replay*?

   3.2. A utilização da cifra no $authenticator_A$ pode ser substituída por um esquema MAC (*Message Authentication Code*)? Se sim, indique como.

   3.3. Considere um cenário de aplicação deste protocolo em que a chave partilhada entre A e T (kAT) é derivada da palavra-chave de A. Descreva um ataque de dicionário para a obtenção desta palavra-chave. Assuma que o atacante tem acesso a todas as mensagens trocadas entre A, T e B.

4. (2) Considere o esquema de cifra baseado em palavras-chave, definido pela norma PKCS #5. Descreva o objectivo e a utilização da função de *hash*. Descreva o objectivo e a utilização do *iteration count*.

5. (2) O modelo $RBAC_2$ acrescenta ao modelo $RBAC_0$ o suporte para o conceito de *separation of duty*. Descreva este conceito e a forma como é implementado no $RBAC_2$.

6. (2) Descreva a forma utilizada pelo modelo de *Clark e Wilson* para implementar o conceito de *separation of duty*.

7. (2) Na plataforma .NET, o *strong name* dum *assembly* contém uma chave pública. Qual a utilização dada a esta chave pública?

8. (2) A utilização das funções da biblioteca normalizada da linguagem C para manipulação de blocos de memória e de *strings* (ex. `memcpy e strcpy`) apresenta riscos para a segurança. Quais são estes riscos e quais as técnicas existentes para os mitigar?

ISEL, 2 de Abril de 2007.