Instituto Superior de Engenharia de Lisboa

Licenciatura em Engenharia Informática e de Computadores

Segurança Informática

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

Duração: 2 horas e 30 minutos

---

1. (2) A função de cifra do esquema de cifra assimétrica definido na norma PKCS #1 v1.5 é não-determinística. Apresente um problema existente se esta função fosse determinística. O problema apresentado também existe no caso dos esquemas de cifra simétrica com funções de cifra determinísticas?

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

   2.1. Descreva a utilização destes certificados no protocolo TLS (*Transport Layer Security*).

   2.2. Porque é que a validação dum certificado implica a obtenção da chave pública do seu emissor? Como é que esta obtenção é normalmente realizada?

   2.3. Considere a autoridade de certificação CA, cuja chave pública é considerada *trust anchor* por uma comunidade de entidades (ex. autoridade de certificação do IPLNet). Considere que CA emite um certificado para a entidade E. Como é que CA pode impedir que E emita certificados aceites na mesma comunidade de entidades?

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 as vantagens decorrentes da não utilização de mecanismos assimétricos neste protocolo?

   3.2. Tendo em consideração que B recebe o bilhete de A, pode B autenticar-se como A perante uma terceira entidade?

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

4. (4) Considere o seguinte esquema para a manutenção do estado de autenticação duma aplicação *web*.

   - A autenticação dos utilizadores é baseada em palavras-chave. Para cada utilizador i, o servidor contém a informação de verificação $v_i = H^2(p_i)$, onde H é uma função de *hash* criptográfica e p_i é a palavra chave do utilizador i.
   - Após a correcta autenticação do utilizador i, o servidor emite um *cookie* contendo $(i, H(p_i))$.
   - Em cada pedido, o *browser* envia o *cookie* emitido pelo servidor. O servidor verifica se o cliente está correctamente autenticado através da comparação $H(c_2) = v_{c_1}$, onde (c_1, c_2) é o *cookie* enviado pelo *browser*.

   4.1. Qual a vantagem do *cookie* conter $H(p_i)$ e não p_i?

   4.2. Qual a vantagem do servidor armazenar, para cada utilizador i, $H^2(p_i)$ e não p_i ou $H(p_i)$?

   4.3. Apresente um problema deste esquema.

5. (1) Considere o esquema de cifra baseada em palavras-chave definido pela norma PKCS #5. Descreva o objectivo e a utilização do *salt*. Diga se o valor do *salt* pode ser constante?

6. (2) Descreva uma forma de implementação das regras de *enforcement* do modelo de Clark e Wilson usando os mecanismos de controlo de acesso ao código da plataforma .NET. Indique as limitações que a sua implementação apresenta.

7. (1,5) Considere o departamento identificado pela chave pública D e os seguintes *roles*, representados através de nomes locais SDSI *(Simple Distributed Security Infrastructure)*:

   - "D $responsavel\_projecto$" - responsável da disciplina de projecto
   - "D $orientador\_projecto$" - orientador de um projecto
   - "D $aluno\_projecto$" - aluno de um projecto

   Considere a seguinte política:

   - O departamento D delega no responsável de projecto a atribuição do *role* "D $orientador\_projecto$".
   - O departamento D delega nos orientadores a atribuição do *role* "D $aluno\_projecto$".

   Defina os certificados de nome SDSI necessários para implementar esta política.

8. (1,5) Um dos objectivos dum ataque de *buffer overflow* é a mudança da sequência de execução do programa a atacar. Uma forma de realização desta mudança é a alteração do endereço de retorno de funções. No contexto deste tipo de ataque, indique outras formas de alteração da sequência de execução.

ISEL, 2 de Fevereiro de 2007.