Instituto Superior de Engenharia de Lisboa

Licenciatura/Mestrado em Engenharia Informática e de Computadores

Segurança Informática

Teste final, primeira época, Semestre de Inverno, 08/09

Duração: 2 horas e 30 minutos

---

1. (2) Considere a existência de um ataque à função de *hash* SHA1, baseado num algoritmo eficiente para: dado x, obter $x' \neq x$ tal que $H(x') = H(x)$. Quais as implicações deste ataque caso esta função seja usada num esquema de assinatura digital.

2. (2) Na JCA (*Java Cryptography Architecture*) os *keystores* podem armazenar chaves e certificados. Qual a necessidade de indicar uma *password* para proteger um *keystore* apenas com certificados?

3. (2) Considere a infra-estrutura de certificados X.509.

   3.1. Como é que uma CA ao emitir o certificado C consegue impedir que uma cadeia seja considerada válida se o certificado C for usado nos certificados intermédios?

   3.2. Comente a seguinte frase: "Dada a natureza especial do certificado raiz (*trust anchor*) não faz sentido que este faça parte da cadeia de certificação de um certificado X.509".

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

   4.1. Indique quais os dois grandes sub-protocolos em que se divide o protocolo TLS. Descreva a funcionalidade de cada um.

   4.2. Descreva os mecanismos usados nos sub-protocolos para evitar ataques de *replay*.

5. (3) Considere um *site* para consulta das colocações dos alunos no concurso de acesso ao ensino superior. Um aluno pode consultar a sua colocação introduzindo o seu número de BI no *site*.

   Como é que se pode evitar que um atacante com acesso à base de dados do *site* consiga facilmente obter uma lista dos BIs de todos os alunos que concorreram? Descreva as limitações da sua solução.

v.s.f.f.

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

   - $U = u_1, u_2, u_3$
   - $R = r_0, r_1, r_2, r_3$
   - $P = p_0, p_1, p_2$
   - $\{r_0 \preceq r_1, r_0 \preceq r_2, r_2 \preceq r_3, r_1 \preceq r_3\} \subseteq RH$
   - $UA = \{(u_1, r_1), (u_2, r_2), (u_3, r_3)\}$
   - $RA = \{(r_0, p_0), (r_1, p_1), (r_2, p_2)\}$

   6.1. Sendo s_0 um identificador de sessão, e $user(s_0) = u_2$, é possível que $r_1 \in roles(s_0)$? E que $r_0 \in roles(s_0)$?

   6.2. Quais os utilizadores que podem aceder a um recurso que exija a permissão p_1.

   Justifique todas as respostas.

7. (3) Considere os seguintes certificados SDSI (*Simple Distributed Security Infrastructure*):

   a) $K_M\ InstituicoesES \rightarrow K_M\ Politecnico$

   b) $K_M\ InstituicoesES \rightarrow K_M\ Universidade$

   c) $K_M\ AlunoES \rightarrow K_M\ InstituicoesES\ Aluno$

   d) $K_M\ AlunoES \rightarrow K_M\ Politecnico\ Aluno$

   e) $K_M\ AlunoES \rightarrow K_M\ Universidade\ Aluno$

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

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

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

   i) $K_{IPL}\ Aluno \rightarrow K_{IPL}\ AlunoMestrado$

   j) $K_{IPL}\ AlunoMestrado \rightarrow K_{A456}$

   7.1. Quais dos certificados anteriores são redundantes? Demonstre esta redundância provando que são inferíveis a partir de outros certificados.

   7.2. Quais as chaves que fazem parte do nome local $K_M\ AlunoES$? Justifique.

   7.3. Se a chave do IPL (K_{IPL}) mudar quais os certificados que teriam de ser reemitidos?

8. (2) Em C e C++, os *buffers* presentes em *stack* são os únicos vulneráveis a ataques de *buffer overflow*?

24 de Janeiro de 2009