Instituto Superior de Engenharia de Lisboa

Licenciatura em Engenharia Informática e de Computadores

Segurança Informática

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

Duração: 2 horas e 30 minutos

---

1. (2) Considere os esquemas de cifra simétrica baseados em modos de operação em *stream*. Qual a razão para não se utilizar a mesma chave e o mesmo *vector inicial* (*Initialization Vector*) para cifrar dois ou mais textos em claro diferentes.

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

   2.1. As mensagens enviadas pelo cliente através do *Record Protocol* são protegidas por um esquema MAC (*Message Authentication Code*)? Justifique a resposta.

   2.2. Quais os certificados que têm de ser configurados no cliente?

   2.3. O *Handshake Protocol* utiliza um esquema de cifra assimétrica. O *Record Protocol* utiliza um esquema de cifra simétrica. Descreva a utilização destes dois tipos de esquema de cifra. Justifique a adopção de tipos de esquemas diferentes para os dois sub-protocolos.

3. (3) Considere os ataques de dicionário apresentados no contexto da autenticação baseada em *passwords*. Descreva a utilização desta técnica para a realização dum ataque do tipo *Known Plain Text* contra um esquema de cifra baseada em *passwords*. Quais as técnicas utilizadas nos esquemas de cifra baseada em *passwords* para protecção contra este tipo de ataque?

4. (2) As ACL (*Access Control Lists*) são um mecanismo que pode ser utilizado para proteger a confidencialidade da informação armazenada no sistema de ficheiros do sistema operativo *Windows XP*. A utilização de esquemas criptográficos de cifra constitui outra técnica para o mesmo objectivo. Compare estas duas técnicas.

5. (2) Qual a justificação para a regra *no-write-down* existente no modelo de Bell-LaPadula?

6. (3) O modelo $RBAC_1$ acrescenta ao modelo $RBAC_0$ o conceito de hierarquia de *roles*. Descreva em que consiste e como é utilizada esta hierarquia. Quais as vantagens resultantes da sua introdução no modelo $RBAC_1$?

7. (2) Considere o modelo de controlo de acesso ao código existente na plataforma .NET. A exigência duma permissão não requer sempre um percurso no *stack*. Quais as permissões em que este percurso é necessário e quais as permissões em que este percurso não é necessário?

8. (2) Considere a seguinte frase presente em H. Shacham, M. Page, B. Pfaff, E. Goh, N. Modadugu, D. Boneh, "On the Effectiveness of Address-Space Randomization", 11th ACM Conference on Computer and Communications Security.

   > It is widely believed that randomizing the address-space layout of a software program prevents attackers from using the same exploit code effectively against all instantiations of the program containing the flaw"

   Qual o tipo de ataques que a técnica referida (*randomizing the address-space layout*) visa impedir ou limitar? Justifique a resposta.

ISEL, 8 de Janeiro de 2007.