Instituto Superior de Engenharia de Lisboa

Licenciatura/Mestrado em Engenharia Informática e de Computadores

Segurança Informática

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

Duração: 2 horas e 30 minutos

---

1. (2) Considere um modo de operação, para esquemas simétricos de cifra, definido por:

   - Seja $x = x_1, \ldots, x_L$ a divisão nos blocos x_i do texto em claro x.
   - Seja $y_i = E(k)(x_i) \oplus y_{i-1}$, para $i = 1, \ldots, L$, onde E é a operação de cifra, $\oplus$ denota a operação de ou-exclusivo bit a bit e y_0 é o vector inicial.
   - O criptograma resultante da cifra da mensagem x é $y = y_1, ..., y_L$.

   1.1. Defina o algoritmo de decifra para este modo de operação.

   1.2. Quais os principais problemas do modo ECB? O modo de operação proposto resolve estes problemas?

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

   2.1. Um código PIN (4 dígitos decimais) foi cifrado com um esquema assimétrico, tendo sido usada uma instância da *engine class* `Cipher`. Para iniciar essa instância foi utilizado um objecto `SecureRandom` cujo método `nextBytes` retorna sempre a mesma sequência de bytes. Descreva uma forma de determinar o código PIN, dado o criptograma obtido.

   2.2. Que tipo de chaves (*Public Key* ou *Private Key*) são usadas nos métodos `initSignature` e `initVerify` da classe `Signature`.

3. (3) Considere as infra-estruturas de chave pública baseadas em certificados X.509.

   3.1. Qual a motivação para a existência de autoridades de certificação intermédias?

   3.2. Qual o papel dos certificados X.509 na autenticação do cliente e do servidor no protocolo SSL (*Secure Socket Layer*)?

4. (3) Considere o protocolo Kerberos.

   4.1. Assumindo que a autenticação dos clientes é baseada em *passwords*, de que forma esta informação é usada no protocolo?

   4.2. Porque razão o mesmo bilhete não pode ser utilizado para o cliente estabelecer ligações seguras com dois ou mais servidores distintos?

5. (2) Considere a seguinte afirmação

   > No user of the system, even if authorized, may be permitted to modify data items in such a way that assets or accounting records of the company are lost and corrupted

   presente em: D. Clark, D. Wilson, "A Comparison of Commercial and Military Computer Security Policies", IEEE Symposium on Security and Privacy, 1987. Quais os conceitos do modelo de Clark e Wilson que contribuem para a obtenção do requisito descrito nesta afirmação?

6. (2) Qual a motivação para o conceito de *sessão* existente na família de modelos de controlo de acesso RBAC (*Role Based Access Control*)?

7. (3) Considere a plataforma Microsoft.NET e o modelo de segurança *Code Access Security* (CAS).

   7.1. Considere a classe W e os seus métodos $M1$ e $M2$. $M1$ e $M2$ podem exigir permissões diferentes? Os métodos $M1$ e $M2$ podem ter permissões diferentes?

   7.2. Identifique o *Policy Decision Point* (PDP) e o *Policy Enforcement Point* (PEP) neste modelo de controlo de acessos. Explique o funcionamento do PEP.

8. (2) Relacione as técnicas de ataque *cross site scripting* e *SQL injection*. Que medida genérica pode ser tomada para prevenir ambos os ataques?

9 de Fevereiro de 2009