Instituto Superior de Engenharia de Lisboa

Licenciatura/Mestrado em Engenharia Informática e de Computadores

Segurança Informática

Teste final, primeira época, Semestre de Inverno de 07/08.

Duração: 2 horas e 30 minutos

---

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

   1.1. Qual o objectivo da utilização de esquemas de assinatura digital neste protocolo?

   1.2. Quais as chaves e certificados que têm de ser configurados do lado do servidor?

   1.3. Considere uma implementação errada do protocolo, em que o valor de *server hello random* é constante. Quais as consequências desse erro?

2. (2,5) Considere o esquema de autenticação em aplicações web, baseado em autenticadores presentes em *cookies* e *protegidos* atráves da utilização dum esquema MAC (*Message Authentication Code*).

   2.1. Descreva em detalhe a forma como o esquema MAC é usado para a *protecção* dos autenticadores.

   2.2. O esquema MAC pode ser substituído por um esquema de cifra simétrica? Se sim, quais as vantagens desta substituição?

   2.3. O esquema MAC pode ser substituído por um esquema de assinatura digital? Se sim, quais as vantagens desta substituição?

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

   3.1. Uma das sobrecargas do método `init` da class `Cipher` recebe um parâmetro do tipo `SecureRandom`. Qual a finalidade deste parâmetro? Em que situações deve ser usado?

   3.2. O carregamento duma instância de `KeyStore` (método `load`), requer uma *password* como parâmetro. Contudo, o acesso a uma chave privada (método `getKey`) também requer a passagem duma *password*. Descreva a utilidade destas duas *passwords*.

4. (4) Considere as infra-estruturas de chave pública baseadas na norma X.509.

   4.1. Seja C um certificado contendo a chave pública K. Qual o resultado da verificação da assinatura digital de C usando a chave K?

   4.2. Seja C um certificado auto-assinado (auto-emitido), contendo o nome N e a chave pública K. A verificação de que K é de facto a chave pública de N é condição suficiente para se utilizar C como *trust anchor*?

   4.3. Qual a diferença entre os certificados X.509 e os certificados de nome da SDSI (*Simple Distributed Security Infrastructure*).

5. (3) Considere a família RBAC (*Role Based Access Control*) de modelos de controlo de acesso.

   5.1. Qual a motivação para o conceito de *sessão*?

   5.2. Considere o cenário onde o administrador delega a definição da relação UA (*User Assignment*). Qual a importância da utilização de restrições (*constraints*) neste caso?

6. (1,5) Qual a razão da existência da regra *no read down* no modelo de Biba? Existe alguma regra análoga no modelo de Clark e Wilson?

7. (1,5) Qual o objectivo da componente *Code Access Security* (CAS) da plataforma Microsoft .NET? De que forma são atribuídas permissões a métodos?

8. (1,5) Descreva o que se entende por ataques de *SQL injection*. O tipo de vulnerabilidade explorada neste tipo de ataque é especifico da linguagem SQL?

ISEL, 2 de Fevereiro de 2008.