Departamento de Informática
Faculdade de Ciências e Tecnologia
UNIVERSIDADE NOVA DE LISBOA

Mestrado em Engenharia Informática

Segurança em Sistemas Informáticos Distribuídos

2º Semestre 2005/2006

Teste de Avaliação de Conhecimentos (Teste Nº 2 – 27/MAIO/2005)

Notas:

- O enunciado tem 5 questões, divididas em duas partes:
  - **Parte sem consulta** (Questões 1 e 2): 50 min
  - **Parte com consulta** (Questões 3 e 4) : 50 min
- Leia completamente e com atenção cada questão antes de responder. A interpretação do enunciado é um factor de avaliação.

---------- A preencher pelos alunos ----------

Nº de aluno: _____ Nome: _____

Nº Total de páginas entregues: _____ (numere as páginas na forma Pág / TOTAL)

Classificação (a preencher pelo docente):

PARTE 1 (sem consulta)	**PARTE 2 (com consulta)**

1)	**2)**	**3)**	**4)**
a)	a)	a)	
b)	b)	b)	
c)	c)	c)	
d)	d)	d)	
e)			
f)			
g)			
h)			

Questão 1) Considere as seguintes afirmações. Assinale as que considera verdadeiras e as que considera falsas. No caso da falsas corrija a afirmação de modo a justificar o que está incorrecto

a) O algoritmo DSA é um algoritmo criptográfico assimétrico de chave pública e, como tal, um utilizador possuir um par de chaves (pública e privada). O que se cifra com qualquer uma dessas chaves pode decifrar-se com a outra (ou seja: Se C={P}Kpriv => P={C}Kpriv Se C={P}Kpub => P={C}Kpriv

b) Suponha que Alice transmite uma mensagem cifrada com uma chave DES a Bob da seguinte forma. Alice e Bob estão a usar chaves RSA e, qualquer um deles (ou qualquer outro principal ou potencial atacante) podem obter as chaves públicas de Alice e Bob, como é normal.

   Alice gera a chave DES (Kdes) e envia a mensagem M a Bob:

   {Kdes}KpubBOB {{M}Kdes}

   Mesmo que um atacante que conhece a chave pública de BOB (actuando como man-in-the-middle) saiba que M está cifrada por uma chave Kdes não terá como produzir um ataque de modo a obter M

c) A vantagem de utilizar Padding em RSA com um método do tipo OAEP que adiciona padding aleatório a blocos plaintext é que se minimizam (ou tornam computacionalmente inviáveis) ataques do tipo "chossen-ciphertex-analysis" comparativamente à simples adopção do método RSA quando se cifram mensagens confidenciais sem usar padding ou usando padding constante, do tipo PKCS1.

d) O método D-H permite negociar uma chave (ou segredo partilhado) entre dois principais A e B, garantindo que quando A e B comunicarem usando essa chave (ou alguma chave gerada do segredo partilhado) estão implicitamente autenticados.

e) Um método do tipo HMAC permite cifrar e decifrar mensagens, de modo mais rápido que um algoritmo criptográfico assimétrico.

f) As assinaturas duais utilizadas nas mensagens enviadas pelo *cardholder* como são usadas no protocolo SET são calculadas utilizando criptografia assimétrica.

g) O modo de autenticação RSA no protocolo de handshake SSL torna o desempenho do protocolo handshake mais eficiente (mais rápido) do que o modo Ephemeral Diffie Hellman.

h) O protocolo SSL não garante o controlo de ordenação de menagens, a não ser que a conexão SSL dependendo este controlo do facto de ter que ser suportado em TCP (ao nível transporte).

Questão 2)

a) Diga, resumidamente, para cada um dos eventuais ataques que se referem, em que consiste o suporte de defesas do protocolo SSL:

A1) Message Reply de records SSL trocados anteriormente
A2) Man-In-the-Middle, com ataque a forçar que a chave de sessão estabelecida seja negociada entre o atacante e cada um dos extremos do canal para depois poder interceptar e decifrar mensagens entre os dois extremos
A3) IP Spoofing
A4) IP Hijacking com possibilidade de controlo da conexão SSL tomando o atacante o lugar do endereço IP a meio dessa conexão
A5) DoS provocado por um ataque do tipo SYN-flooding à conexão TCP subjacente ao protocolo SSL
A6) Tampering dos records SSL na conexão
A7) Ataque provocando desordenação de records SSL no meio de uma sessão SSL (se por exemplo esta estivesse suportada em UDP)

b) Em que consiste, porque e como são utilizadas as assinaturas duais no âmbito do protocolo SET ?

c) No protocolo SET o Merchant possui dois certificados de chave pública ? Qual o objectivo de utilização de dois e não apenas um certificado de chave pública emitido por uma CA ?

d) Em que consiste um esquema de assinatura do tipo CMAC ou CBC-MAC ? Responda apresentando um esquema de como se produz uma assintura deste tipo e quais os seus pressupostos.

Questão 3)

a) Contrariamente ao SSL v3**,** em que o *padding* usado nos *records* SSL (do protocolo Record Layer) que se passam cifrados na sessão é o mínimo necessário para cada record poder ser cifrado e decifrado de acordo com a dimensão do bloco de cifra que estiver a ser usado, a norma TLS refere que esse *padding* pode ter qualquer tamanho desde que o record SSL seja múltiplo do tamanho do bloco. Que vantagens o TLS exibe face ao SSL devido a este facto ?

b) Em que consiste a propriedade conhecida como resistência computacional a uma assinatura do tipo HMAC e porque é que no caso de métodos de assinaturas baseadas em HMAC é muito mais complicado produzir ataques explorando resistência a colisões (fortes ou fracas) quando comparado com um vulgar método de síntese?

c) Responda novamente à alínea a) da questão 2, consultando agora a bibliografia ou especificações do protocolo SSL v.3.

d) Suponha que tem uma aplicação composta por 4 processos que executam em quatro hosts distintos ligados à Internet através de routers convencionais. Cada host utiliza endereçamento privado (por detrás do respectivo router). Os processos precisam de partilhar uma chave simétrica (ex: AES) para mandarem mensagens cifradas entre si na rede Internet. Diga como proporia uma solução de partilha da chave se só puder usar o método de D-H tal como o estudou e dispõe de certificados do tipo dos que estão subjacentes ao modo de autenticação Fixed Diffie Hellman, tal como existe no protocolo SSL.

Questão 4)

Suponha os seguintes traços observados numa interacção tipo entre um browser e um servidor WEB em HTTPS sobre conexão SSL. Em alguns dos traços da execução a conexão SSL não foi estabelecida. Com base nos traços indique:

a) Em que traços se verifica "autenticação one-way ou unilateral do servidor", "autenticação one-way ou unilateral do cliente" e "autenticação mútua cliente-servidor" ?

b) No traço ou nos traços que estabeleceram efectivamente a conexão SSL, diga que algoritmo simétrico estará subjacente ao suporet de confidencialidade da comunicação.

c) O que deveria ter feito o cliente se pretendesse usar a suite SSL_RSA_WITH_3DES_EDE_CBC_SHA ? Tente ersumir em que consistiria na prática esta suite do ponto de vista das várias operações criptográficas do processamento SSL?

e) Usando a numeração do trace (números de sequência das mensagens à esuqerda) em quais dos traços e em que passo o cliente iniciou o processo de geração da chave simétrica para uso no canal.

f) No traço (ou traços) em que ocorre autenticação mútua o que aconteceria se o cliente enviasse um certificado de chave pública do cliente em que a chave pública emitida por uma CA oficial (ex: Verisign) do cliente fosse assinada não por RSA mas pelo método DSA, isto é, um certificado emitido pela Verisign em que a assinatura da CA do certificado foi emitida com base no método DSA.

g) Indique possíveis razões que podem explicar os casos em que a sessão SSL que não foi concluída com sucesso tendo sido terminada antes que o canal SSL estivesse estabelecido.

TRACE 1

```
New TCP connection #1: guest-e-U-di-
10.171.96.43.in.di.fct.unl.pt(2762) <-> di157(443)
1 1  0.0376 (0.0376)  C>S SSLv2 compatible client hello
  Version 3.0
  cipher suites
  SSL_RSA_WITH_RC4_128_MD5
  SSL_RSA_WITH_RC4_128_SHA
  SSL_RSA_WITH_3DES_EDE_CBC_SHA
  SSL2_CK_RC4
  SSL2_CK_3DES
  SSL2_CK_RC2
  SSL_RSA_WITH_DES_CBC_SHA
  SSL2_CK_DES
  SSL_RSA_EXPORT1024_WITH_RC4_56_SHA
  SSL_RSA_EXPORT1024_WITH_DES_CBC_SHA
  SSL_RSA_EXPORT_WITH_RC4_40_MD5
  SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5
  SSL2_CK_RC4_EXPORT40
  SSL2_CK_RC2_EXPORT40
  SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
  SSL_DHE_DSS_WITH_DES_CBC_SHA
  SSL_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA
1 2  0.0382 (0.0006)  S>C  Handshake
      ServerHello
        Version 3.0
        session_id[32]=
          61 fe 04 a1 a6 37 98 3a bd 14 3d aa 38 11 2e 19
          ce c2 e8 a4 75 f6 5b a3 74 72 0c 3b 09 fe 23 f2
        cipherSuite         SSL_RSA_WITH_RC4_128_MD5
        compressionMethod                     NULL
1 3  0.0382 (0.0000)  S>C  Handshake
      Certificate
1 4  0.0382 (0.0000)  S>C  Handshake
      ServerHelloDone
1 5  0.0515 (0.0132)  C>S  Handshake
      ClientKeyExchange
1 6  0.0515 (0.0000)  C>S  ChangeCipherSpec
1 7  0.0515 (0.0000)  C>S  Handshake
1 8  0.2498 (0.1982)  S>C  ChangeCipherSpec
1 9  0.2498 (0.0000)  S>C  Handshake
```

TRACE 2

```
New TCP connection #1: guest-e-U-di-
10.171.96.43.in.di.fct.unl.pt(2794) <-> di157(443)
1 1  0.0445 (0.0445)  C>S SSLv2 compatible client hello
  Version 3.0
  cipher suites
  SSL_RSA_WITH_RC4_128_MD5
  SSL_RSA_WITH_RC4_128_SHA
  SSL_RSA_WITH_3DES_EDE_CBC_SHA
  SSL2_CK_RC4
  SSL2_CK_3DES
  SSL2_CK_RC2
  SSL_RSA_WITH_DES_CBC_SHA
  SSL2_CK_DES
  SSL_RSA_EXPORT1024_WITH_RC4_56_SHA
  SSL_RSA_EXPORT1024_WITH_DES_CBC_SHA
  SSL_RSA_EXPORT_WITH_RC4_40_MD5
  SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5
  SSL2_CK_RC4_EXPORT40
  SSL2_CK_RC2_EXPORT40
  SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
  SSL_DHE_DSS_WITH_DES_CBC_SHA
  SSL_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA
1 2  0.0452 (0.0006)  S>C  Handshake
      ServerHello
        Version 3.0
        session_id[32]=
          25 a7 27 e5 12 68 94 38 17 84 ad 8a 83 52 5e c0
          5e eb 97 df d7 ce 7a 5d d1 dc 5b 36 52 e8 57 bb
        cipherSuite         SSL_RSA_WITH_RC4_128_MD5
        compressionMethod                     NULL
1 3  0.0452 (0.0000)  S>C  Handshake
      Certificate
1 4  0.0452 (0.0000)  S>C  Handshake
      CertificateRequest
        certificate_types                   rsa_sign
        certificate_types                   dss_sign
      ServerHelloDone
1    0.2257 (0.1805)  C>S  TCP FIN
1    0.2259 (0.0002)  S>C  TCP FIN
New TCP connection #2: guest-e-U-di-
10.171.96.43.in.di.fct.unl.pt(2795) <-> di157(443)
2    0.5285 (0.5285)  C>S  TCP FIN
2    0.5288 (0.0002)  S>C  TCP FIN
```

TRACE 3

```
New TCP connection #1: guest-e-U-di-
10.171.96.43.in.di.fct.unl.pt(2825) <-> di157(443)
1 1  0.0031 (0.0031)  C>S  Handshake
      ClientHello
        Version 3.0
        resume [32]=
          1a b9 e3 fe f5 fb ad b4 df ed 00 19 3b 8e 9f b2
          9a 6a 40 3f 2e ec c8 53 7d 5b f9 0e d3 3c 2c 20
        cipher suites
        SSL_RSA_WITH_RC4_128_MD5
        SSL_RSA_WITH_RC4_128_SHA
        SSL_RSA_WITH_3DES_EDE_CBC_SHA
        SSL_RSA_WITH_DES_CBC_SHA
        SSL_RSA_EXPORT1024_WITH_RC4_56_SHA
        SSL_RSA_EXPORT1024_WITH_DES_CBC_SHA
        SSL_RSA_EXPORT_WITH_RC4_40_MD5
        SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5
        SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
        SSL_DHE_DSS_WITH_DES_CBC_SHA
        SSL_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA
        compression methods
                  NULL
1 2  0.0038 (0.0006)  S>C  Handshake
      ServerHello
        Version 3.0
        session_id[32]=
          1a b9 e3 fe f5 fb ad b4 df ed 00 19 3b 8e 9f b2
          9a 6a 40 3f 2e ec c8 53 7d 5b f9 0e d3 3c 2c 20
        cipherSuite         SSL_RSA_WITH_RC4_128_MD5
        compressionMethod                     NULL
1 3  0.0038 (0.0000)  S>C  ChangeCipherSpec
1 4  0.0038 (0.0000)  S>C  Handshake
1 5  0.0096 (0.0058)  C>S  ChangeCipherSpec
1 6  0.0096 (0.0000)  C>S  Handshake
1    0.0537 (0.0441)  C>S  TCP FIN
1    0.0538 (0.0000)  S>C  TCP FIN
```