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

Curso de Engenharia Informática (2º Ciclo)
Teste nº 2 (frequência), 05/Jan/2010

# Segurança em Sistemas e Redes de Computadores

SSRC-0910-EN-2.2.A

Notas:

- O enunciado tem duas partes: uma parte sem consulta e outra com consulta. Cada uma destas partes deve ser respondida no máximo em 1h30 min.
- Podem utilizar-se na parte com consulta quaisquer elementos de consulta excepto computadores ligados em rede ou quaisquer outros dispositivos de comunicações.
- As respostas a entregar devem estar escritas a tinta.
- Deve ler-se completamente e com atenção cada questão e as suas alíneas antes de responder. A interpretação do enunciado ou justificação e argumentação das respostas face às perguntas é considerado um factor de avaliação.
- A duração da prova é de 2h00min

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

Nº de aluno: _____ Nome: _____

Nº TOTAL de páginas entregues (excepto esta capa): _____
(numere as páginas na forma nº da página /Nº TOTAL e coloque o nº e nome em cada página.)

---

---------- A preencher pelo docente ----------

| | | | | | | | **TOTAL** |
|---|---|---|---|---|---|---|---|
| | | | | | | | |

**INF Controlo:**

| |
|---|
| |

**Questão 1 (Sem consulta)**

a) Apresente pelo menos 4 vantagens na utilização do modo de cifra simétrica CTR comparativamente aos modos OFB ou CFB ? Indique, justificando, uma aplicação em que considere ser indicada a utilização deste modo.

b) No modo OFB (Output Feedback Mode), pode representar-se a operação de cifra da seguinte forma, para o primeiro bloco P1 (de m conjunto de blocos P1, P2, … Pi, … Pn):

C1 = P1 XOR { Ss(IV)}K

IV representa um vector de inicialização e Ss() representa uma operação de deslocamento de s bits, num registo de deslocamento (*shift register*).

Indique as expressões para a cifra de um bloco arbitrário Pi, bem como a recuperação do bloco inicial P1 e de um bloco de texto arbitrário Pi a partir de um bloco de cifra

P1 =

Ci =

Pi =

c) Qual o propósito e que vantagem tem a utilização de um modo do tipo CTS (Ciphertext Stealing) comparativamente ao modo CFB ? Justifique.

**Questão 2)  (sem consulta)**
Apresente quais são os métodos de troca (ou estabelecimento) de chaves de sessão normalizados em TLS e indique quais os que considera serem mais seguros e de menor complexidade para efeitos de melhor desempenho.

**Questão 3 (sem consulta)**

Apresenta-se a especificação do protocolo Kerberos Versão 5.

(1) C → AS Options || $ID_c$ || $Realm_c$ || $ID_{tgs}$ || $Times$ || $Nonce_1$

(2) AS → C $Realm_c$ || $ID_C$ || $Ticket_{tgs}$ || $E(K_c, [K_{c,tgs} || Times || Nonce_1 || Realm_{tgs} || ID_{tgs}])$

$Ticket_{tgs} = E(K_{tgs}, [Flags || K_{c,tgs} || Realm_c || ID_C || AD_C || Times])$

**(a) Authentication Service Exchange to obtain ticket-granting ticket**

(3) C → TGS Options || $ID_v$ || $Times$ || || $Nonce_2$ || $Ticket_{tgs}$ || $Authenticator_c$

(4) TGS → C $Realm_c$ || $ID_C$ || $Ticket_v$ || $E(K_{c,tgs}, [K_{c,v} || Times || Nonce_2 || Realm_v || ID_v])$

$Ticket_{tgs} = E(K_{tgs}, [Flags || K_{c,tgs} || Realm_c || ID_C || AD_C || Times])$

$Ticket_v = E(K_v, [Flags || K_{c,v} || Realm_c || ID_C || AD_C || Times])$

$Authenticator_c = E(K_{c,tgs}, [ID_C || Realm_c || TS_1])$

**(b) Ticket-Granting Service Exchange to obtain service-granting ticket**

(5) C → V Options || $Ticket_v$ || $Authenticator_c$

(6) V → C $E_{K_{c,v}}$ [ $TS_2$ || Subkey || Seq# ]

$Ticket_v = E(K_v, [Flags || K_{c,v} || Realm_c || ID_C || AD_C || Times])$

$Authenticator_c = E(K_{c,v}, [ID_C || Realm_c || TS_2 || Subkey || Seq\#])$

**(c) Client/Server Authentication Exchange to obtain service**

a) Em que se baseia o suporte do protocolo quando se exige autenticação mútua entre clientes e servidores ?

b) Suponha que este protocolo é implementado em UDP num ambiente de grande escala (ex., Internet), isto é, os clientes, servidores Kerberos e servidores finais estão distribuídos num ambiente Internet, não sendo possível esperar que haja condições de sincronização de relógios nem de ordenação de mensagens.

   Indique se considera existirem limitações, nesse caso, para o funcionamento correcto do protocolo e garantia das suas propriedades de segurança.

**Questão 4 (com consulta)**

Tome como referência a estrutura dos chaveiros de chaves públicas e chaves privadas tal como estão especificados no sistema PGP.

a) Qual a razão do campo designado por "*filename*" na estrutura de uma mensagem PGP e como é esse campo utilizado? Justifique.

**b)** Suponha que pretende utilizar autenticação X509 para autenticação de clientes no sistema Kerberos, substituindo o sistema de passwords subjacente ao protocolo. Diga como proporia uma modificação do protocolo (com base na versão 6) para esse efeito. Apresente o protocolo com base na mesma notação da especificação anteriormente indicada.

**Questão 5 (com consulta)**

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 com sucesso diga que algoritmo simétrico está subjacente ao suporte 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?

d) Usando a numeração dos traços (números de sequência das mensagens à esquerda) em quais dos traços e entre que mensagens o cliente e o servidor procedem à geração da chave simétrica de sessão para uso no canal.

e) 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.

f) Indique possíveis razões que podem explicar os casos dos traços em que a sessão SSL não foi concluída com sucesso. Justifique bem essas possíveis razões.

**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
```

**Questão 6 (com consulta)**

Diga como é que o protocolo SET e pressupostos da sua especificação formal garantem a um consumidor (*Cardholder*) o seguinte:

a) Que o valor de uma aquisição não possa ser cobrado duas vezes por um comerciante (*Merchant*) fraudulento ou incorrecto.

*b)* Que um comerciante não proceda a uma cobrança múltipla de um mesmo produto adquirido por um mesmo consumidor através de dois *Payment Gateways* de duas entidades *Acquirer*.

c) Que um comerciante não cobra o crédito de uma compra, sem poder exibir uma garantia de não-repudiação que prove que o consumidor já recebeu e aceitou o produto de uma compra.