Teste e ficha de avaliação sobre o enquadramento do TRABALHO Nª 2.

SSRC – Segurança em Sistemas e Redes de Computadores

2º Semestre, 2007/2008

TESTE DE CONHECIMENTOS SOBRE O ENQUADRAMENTO E REALIZAÇÃO DO TRABALHO PRÁTICO Nº 2

Questão 1

Considere a norma SSL. Diga quais as opções de modos de autenticação e estabelecimento de chaves criptográficas que conhece e que estão normalizadas, para o estabelecimento de sessões seguras com base no protocolo SSL ou TLS. Apresente cada um desses modos e diga em que consistem do ponto de vista do suporte que propiciam.

Questão 2

De acordo com as suites criptográficas que encontrou na implementação JAVA (JSSE) na implementação do trabalho, relacione as mesmas com os modos de autenticação e estabelecimento de sessões seguras SSL que apresentou em 1.

Questão 3

De entre as anteriores opções (indicadas na questão 2.),

a) qual ou quais considera serem mais seguras. Justifique.
b) qual ou quais não consideraria como adequadas para suportar uma aplicação crítica do ponto de vista de segurança, em ambiente WEB (HTTPS) na rede Internet. Justifique a sua resposta.

Questão 4

De entre as suites associadas aos modos indicados em 2., quais as que não estão habilitadas ou não estão activadas (por default) na criação de sockets SSL entre clientes e servidores ?

Questão 5

Identifique os 4 sub-protocolos principais que fazem parte da norma SSL. Diga qual o papel de cada um deles.

Questão 6

Considere o suporte JSSE para suporte de sockets SSL em JAVA usado no trabalho e tenha em conta as observações que fez (com SSLDUMP ou SSLTAP) e o âmbito do Handshake Protocol em SSL.

a) Em que casos é enviada uma mensagem de certificate-request do servidor para o cliente ? Justifique.
b) A mensagem certificate-request é composta por uma parte com um tipo de certificado e outra parte que contém uma lista de certificados X509. Para que serve esta lista e qual o critério do servidor para preencher a mesma no ambiente JSSE ?
c) O estabelecimento de uma KEYSTORE com certificados de confiança por parte do servidor, pode mudar a estrutura e o conteúdo da mensagem certificate-request ? Justifique.
d) Considere o modo de autenticação mútua. Considere que o certificado do servidor foi gerado numa hierarquia de certificação directa com pelo menos dois certificados, sendo um o certificado raiz que contém a chave pública para reconhecimento do certificado usado pelo servidor. Este seria o caso do certificado do servidor ter sido emitido, por exemplo, por uma CA. No protocolo Handshake, qual dos dois anteriores certificados é enviado pelo servidor ao cliente na mensagem "Certificate" enviada a seguir à mensagem SERVER_HELLO ?
e) Em que fase do protocolo HANDSHAKE (isto é, após a recepção de quais mensagens por parte do cliente e do servidor), pode ter lugar a computação do PRE-MASTER-SECRET por parte do cliente e por parte do servidor? Isso é dependente do modo de autenticação e estabelecimento de chaves que esta a ser usado ? Justifique.

Questão 7

Considere a sua implementação do modo FIXED DIFFIE-HELLMAN

a) Como implementou o suporte FIXED DIFFIE-HELLMAN na sua implementação do trabalho nº 2 ?
b) A mesma é compatível ou transparente em relação à possibilidade de uso de autenticação bilateral (ou two-way) cliente/servidor ?
c) Em que é que a sua implementação difere, do ponto de vista do suporte de segurança, da utilização de uma suite como por exemplo: TLS_DHE_RSA_WITH_AES_128_CBC_SHA, já suportada na implementação da JSSE em JAVA ?

Questão 8

a) Qual o fluxo do HAND-SHAKE protocolo em SSL no caso de usar Autenticação e estabelecimento da sessão SSL com Certificados de Chave Pública (modo RSA) e autenticação unilateral apenas por parte do cliente perante o servidor.
b) Em que consiste o suporte de a) na implementação do seu trabalho ?

Questão 9

Os seguintes ecrãs foram obtidos com capturas do estabeleicmento de uma sessão SSL usando a ferramenta SSLDUMP.

a) A que modo de autenticação e estabelecimento da sessão SSL diz respeito o traço da alínea a) ? Indique o valor dos parâmetros da sessão SSL que foi estabelecida (pode indicá-los no próprio traço apresentado)

Suite / modo de autenticação e estabelecimento de chaves aceite pelo servidor:
SID: SessionID criado para a sessão cliente/servidor:
CR: Client Random para a computação PMS
SR: Server Random para a ocmputação PMS
CM: Compression Method
C: Algoritmo de Cifra simétrica a usar na sessão:
MAC: Algoritmo MAC a usar na sessão:
MODE: Tipo de cifra – blocos ou streams (cadeia)

b) A que modo de autenticação e estabelecimento da sessão SSL diz respeito o ecrã na alínea b) ? Indique o que possa ter ocorrido para ter acontecido esse traço. Justifique.

Traço da especificação SSL (referência e identificação das mensagens tipo)

Fase 1

C > S: Client Hello

S > C : Server_Hello

Fase 2

S > C: Certificate

S > C: Server_Key-Exchange

S > C: Certificate_Request

S > C: Server_Hello_Done

Fase 3

C > S: certificate

C > S: Client_Key-Exchange

C > S: Certificate_Verify

Fase 4

C > S: Change_Cypher_Spec

C > S: Finished

S > C: Change Cypher_Spec

S > C: Finished

Traço da especificação SSL

Questão 9 a)

```
New TCP connection #1: di163.di.fct.unl.pt(46232) <-> wwwbaytest1.microsoft.com(443)
1 1  1.0011 (1.0011)  C>S SSLv2 compatible client hello
  Version 3.1
  cipher suites
  TLS_RSA_WITH_RC4_128_MD5
  SSL2_CK_RC4
  TLS_RSA_WITH_RC4_128_SHA
  Unknown value 0x2f
  Unknown value 0x35
  Unknown value 0x33
  Unknown value 0x39
  Unknown value 0x32
  Unknown value 0x38
  TLS_RSA_WITH_3DES_EDE_CBC_SHA
  SSL2_CK_3DES
  TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
  TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
  TLS_RSA_WITH_DES_CBC_SHA
  SSL2_CK_DES
  TLS_DHE_RSA_WITH_DES_CBC_SHA
  TLS_DHE_DSS_WITH_DES_CBC_SHA
  TLS_RSA_EXPORT_WITH_RC4_40_MD5
  SSL2_CK_RC4_EXPORT40
  TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
  TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
  TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
1 2  1.3658 (0.3647)  S>C  Handshake
      ServerHello
        Version 3.1
        session_id[32]=
          d3 03 00 00 62 1b a9 6d 98 a3 bc ca 4a bb d4 64
          98 6e ec b8 d1 df f2 80 70 43 02 f5 b4 28 d1 b6
        cipherSuite         Unknown value 0x2f
        compressionMethod                   NULL
      Certificate
      ServerHelloDone
1 3  1.4395 (0.0736)  C>S  Handshake
      ClientKeyExchange
1 4  1.4567 (0.0172)  C>S  ChangeCipherSpec
1 5  1.6353 (0.1786)  C>S  Handshake
1 6  1.8133 (0.1780)  S>C  ChangeCipherSpec
1 7  1.8133 (0.0000)  S>C  Handshake
1 8  1.8196 (0.0062)  C>S  application_data
1 9  2.0015 (0.1819)  S>C  application_data
1 10 2.0066 (0.0050)  C>S  Alert
1    2.0068 (0.0002)  C>S  TCP FIN
1    2.1834 (0.1765)  S>C  TCP FIN
New TCP connection #2: di163.di.fct.unl.pt(46233) <-> wwwbaytest1.microsoft.com(443)
2 1  0.1792 (0.1792)  C>S  Handshake
      ClientHello
        Version 3.1
        resume [32]=
          d3 03 00 00 62 1b a9 6d 98 a3 bc ca 4a bb d4 64
          98 6e ec b8 d1 df f2 80 70 43 02 f5 b4 28 d1 b6
        cipher suites
        TLS_RSA_WITH_RC4_128_MD5
        TLS_RSA_WITH_RC4_128_SHA
```

```
        Unknown value 0x2f
        Unknown value 0x35
        Unknown value 0x33
        Unknown value 0x39
        Unknown value 0x32
        Unknown value 0x38
        TLS_RSA_WITH_3DES_EDE_CBC_SHA
        TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
        TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
        TLS_RSA_WITH_DES_CBC_SHA
        TLS_DHE_RSA_WITH_DES_CBC_SHA
        TLS_DHE_DSS_WITH_DES_CBC_SHA
        TLS_RSA_EXPORT_WITH_RC4_40_MD5
        TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
        TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
        TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
        compression methods
                  NULL
2 2  0.3562 (0.1770)  S>C  Handshake
      ServerHello
        Version 3.1
        session_id[32]=
          d3 03 00 00 62 1b a9 6d 98 a3 bc ca 4a bb d4 64
          98 6e ec b8 d1 df f2 80 70 43 02 f5 b4 28 d1 b6
        cipherSuite         Unknown value 0x2f
        compressionMethod                   NULL
2 3  0.3562 (0.0000)  S>C  ChangeCipherSpec
2 4  0.3562 (0.0000)  S>C  Handshake
2 5  0.3604 (0.0041)  C>S  ChangeCipherSpec
2 6  0.3613 (0.0008)  C>S  Handshake
2 7  0.5379 (0.1765)  C>S  application_data
2 8  1.2804 (0.7425)  S>C  application_data
2 9  1.6524 (0.3719)  S>C  application_data
2 10 1.8647 (0.2123)  S>C  application_data
2 11 11.8887 (10.0239)  C>S  Alert
2    11.8889 (0.0001)  C>S  TCP FIN
2    12.0677 (0.1788)  S>C  TCP FIN
```

Traço da especificação SSL

Questão 9 b)

```
New TCP connection #1: di163.di.fct.unl.pt(48470) <-> clip.unl.pt(443)
1 1  0.8170 (0.8170)  C>S SSLv2 compatible client hello
  Version 3.1
  cipher suites
  TLS_RSA_WITH_RC4_128_MD5
  SSL2_CK_RC4
  TLS_RSA_WITH_RC4_128_SHA
  Unknown value 0x2f
  Unknown value 0x35
  Unknown value 0x33
  Unknown value 0x39
  Unknown value 0x32
  Unknown value 0x38
  TLS_RSA_WITH_3DES_EDE_CBC_SHA
  SSL2_CK_3DES
  TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
  TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
  TLS_RSA_WITH_DES_CBC_SHA
  SSL2_CK_DES
  TLS_DHE_RSA_WITH_DES_CBC_SHA
  TLS_DHE_DSS_WITH_DES_CBC_SHA
  TLS_RSA_EXPORT_WITH_RC4_40_MD5
  SSL2_CK_RC4_EXPORT40
  TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
  TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
  TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
1 2  0.8183 (0.0013)  S>C  Handshake
      ServerHello
        Version 3.1
        session_id[32]=
          76 18 3a 1b 13 f6 dc e9 f5 98 d6 6a ad a5 af a6
          ec 8a 78 1d d0 03 bd 7b e9 a0 98 18 50 5a fc 09
        cipherSuite         TLS_RSA_WITH_RC4_128_MD5
        compressionMethod                   NULL
1 3  0.8191 (0.0008)  S>C  Handshake
      Certificate
1 4  0.8191 (0.0000)  S>C  Handshake
      ServerHelloDone
1 5  0.8518 (0.0327)  C>S  Alert
    level           fatal
    value           certificate_unknown
1    0.8528 (0.0009)  S>C  TCP FIN
1    0.8530 (0.0002)  C>S  TCP FIN
```

Traço da especificação SSL

Questão 9 b

FICHA DE REALIZAÇÃO DO TRABALHO PRÁTICO Nº 2

GRUPO: _____

Nº _____ Nome: _____

Nº _____ Nome: _____

Demonstração: DATA ESCOLHIDA _____

Tenha em conta os requisitos que tinham sido colocados no enunciado do trabalho nº 2. Nas alíneas da ficha que se encontram indicadas a seguir, coloque:

SIM:

em todas as alíneas que estejam suportadas na implementação e que podem ser apresentadas e demonstradas na sessão de demonstração e discussão do trabalho:

NÃO :

em todas as alíneas que não se encontram implementadas ou não podem ser demonstradas por não estarem correctamente suportadas na implementação.

Caso pretenda esclarecer o sentido da sua resposta, pode usar o verso de cada página com alguma justificação ou explicação complementar.

FASE 1 (> 2)

a1) Cliente/Servidor (Browser / Servidor HTTPS) com autenticação e estabelecimento da sessão SSL (modo RSA), só com autenticação do servidor e verificação do fluxo do protocolo com SSLTAP (ou SSLDUMP): _____

a2) Cliente/Servidor (ClienteSocketSSLGrab e ClienteURLGrab) com qualquer suite Anonymous DH, RSA ou EDH, só com autenticação do servidor e verificação do fluxo do protocolo com SSLTAP (ou SSLDUMP): _____

FASE 2 (2 > 3)

b1) ClienteSocketSSLGrab foi implementado e funciona com autenticação bilateral em pelo menos dois modos : EDH e RSA ? _____

b2) ClienteURLGrab foi implementado e funciona com autenticação bilateral em pelo menos dois modos : EDH e RSA ? _____

b3) ClienteURLGrab e ClienteSocketSSLGrab foram implementados e funcionam com autenticação bilateral com modos RSA, EDH e Anonymous DH ? _____

b4) Cliente (as duas versões) / Servidor (HTTPS) com autenticação unilateral do servidor, em todos os modos de autenticação incluindo Fixed DH: _____

FASE 2 (3 > 4):

c1) Modos RSA, EDE, Anonymous e Fixed DH (one-way cliente): _____

c2) Fixed DH com autenticação bilateral (two-way): _____

c3) Uso de certificados com geração numa cadeia de certificação (ex., simulação de um certificado emitido por uma CA)

FASE 3 (4 > 5):

Demonstração de RMI/SSL

d1) Implementação e demonstração com pelo menos modo RSA e autenticação do servidor: _____

d2) Implementação e demonstração com pelo menos modo RSA e autenticação mútua: _____

d3) Implementação e demonstração com pelo menos modo RSA e autenticação unilateral só do cliente: _____

d4) Suporte para todos os modos de autenticação e estabelecimento da sessão e demonstrável em qualquer um dos modos one-way (cliente ou servidor) ou two-way (cliente e servidor): _____