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

Curso de Mestrado em Engenharia Informática (2º Ciclo)

Segurança em Sistemas e Redes de Computadores

1º Semestre - 2011/2012

TESTE DE FREQUÊNCIA Nº 2 (16/Dezembro/2011)

Teste individual
Duração do teste: 2 horas

- **Questões do grupo I: sem consulta (1 hora)**
- **Questões do grupo II: com consulta (1 hora).**
  - Apenas podem ser consultados elementos individuais, não sendo permitida nenhuma forma de comunicação entre os alunos.

Nº de aluno	Nome:	
LEI/MEI:	Grupo (trabalho prático):	Nº de páginas entregues:

As páginas devem ser numeradas, no canto superior direito, na forma: Nº Página / Total de Páginas, não contando com esta página.

Tabela e critérios de avaliação (a ser preenchido pelo docente)

GRUPO 1 (respostas sem consulta)					

GRUPO 2 (respostas com consulta)					

GRUPO I – Questões para resposta sem consulta

Questão 1 (~20-25 minutos, 4 valores

a) Indique como se processa o protocolo de acordo para estabelecimento de uma chave simétrica a ser usada para estabelecimento de um canal confidencial entre dois principais A e B, usando o método de Diffie-Hellman. Deve ilustrar o protocolo de Diffie-Hellman com base num diagrama temporal, explicitando a troca de mensagens e o conteúdo das mesmas, na versão anónima do protocolo, ou seja, sem autenticação dos principais envolvidos. Deve ainda indicar em cada passo qual o cálculo (computação) realizada por cada principal até obter a chave partilhada final. A sua resposta deve ser apresentada com o detalhe necessário que descreva em cada passo as computações que têm lugar e as mensagens trocadas entre A e B.

b) Com base na sua resposta a a), diga como um atacante do tipo "*man in the middle*" pode atacar o acordo entre A e B e conseguir posicionar-se de tal forma que, no final do acordo, colocará em causa a confidencialidade de mensagens enviadas entre A e B.

c) Indique as dimensões (em bits) dos números de D-H gerados, que usaria nas computações, bem como as dimensões que escolheria para os restantes parâmetros necessários, para que se estabeleça no final do acordo uma chave K partilhada, de dimensão 256 bits. Justifique.

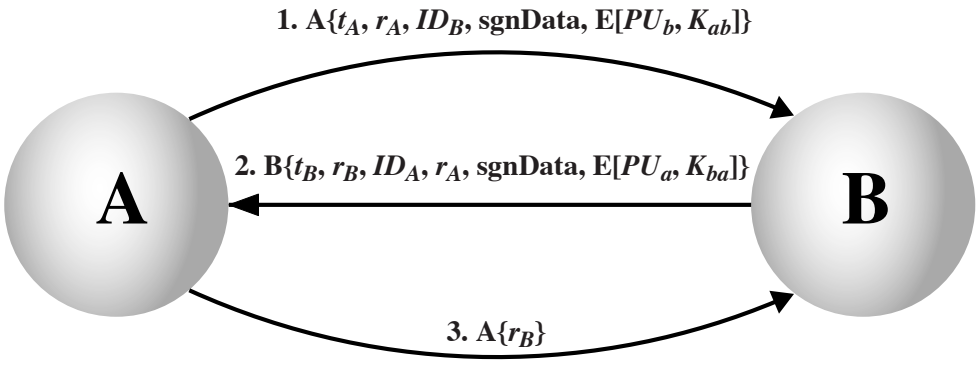
d) Tente fazer um cálculo manual (pode usar uma calculadora) que permita responder a esta questão teórica, que tem como base a utilização de números muito pequenos para o acordo:

Raiz primitiva = 3; valor a usar para módulo = 353
E1) Se o principal A usar um numero secreto DH = 97, qual será o numero público que A proporá a B no acordo ? Indique o cálculo utilizado e o resultado obtido.

E2) Se B gerar um numero secreto DH = 233, qual será o valor inteiro da chave partilhada no fim do acordo ? Indique o cálculo utilizado e o resultado obtido.

Questão 2 (~10-15 minutos, 3 valores)

Num processo de autenticação com certificados de chave pública X509 v3, A e B vão autenticar-se perante B com base no seguinte protocolo:



tB, tA	são timestamps geradas por B e A
rA e rb	são valores aleatórios gerados por A e B
IDA e IDB	são identificadores únicos globais que representam A e B
E[PU, K]	significa um envelope da chave K cifrado com a chave pública P
PUa, PUb	são as chaves públicas de A e B
Kab e Kba	são chaves geradas por A e B para uso unidireccional emissor-receptor na confidencialidade entre esses principais
A{x}	significa o conteúdo x assinado com RSA por A
B{x}	significa o conteúdo x assinado com RSA por B
signData	é uma concatenação de outros valores que têm que ser autenticados nas mensagens trocadas enter A e B.

Antes de iniciar o protocolo, A e B não conhecem as chaves públicas um do outro. Por isso, A e B têm que explicitamente enviar nas mensagens 1 e 2 os seus certificados de chave pública, concatenados com as mensagens indicadas.

Assim, na mensagem 1, o principal A precisa de enviar uma cadeia de quatro certificados X509v3, isto é: Ca || Cca1 || Cca2 || Cca3 , formando uma cadeia de certificação, sendo Cca3 o certificado da raíz dessa cadeia e Ca é o certificado de A. Nesta cadeia, os certificados correspondem a certificados das CAs: CA1, CA2, CA3, CA4.

Na mensagem 2, de forma equivalente, B envia uma cadeia de 3 certificados, enviados na forma: Cb || Ccb1 || Ccb2, sendo Ccb2 o certificado raiz dessa cadeia e Cb é o certificado de B, e a cadeia possui os certificados das CAs: CB1 e CB2

Sabe-se que Cca3 é o único certificado reverso, de CA3 em relação a CB2.

a) Faça um esquema indicando como deve estar estabelecida a hierarquia de certificação para que seja possível que A e B se possam autenticar.
b) Na verdade, sobre certas condições, as mensagens 1 e 2 já bastariam para garantir autenticação mútua entre A e B. Qual o interesse ou importância da terceira mensagem ? Justifique.

Questão 3 (~15-20 minutos, 2 valores)
PODE USAR CALCULADORA PARA REALIZAR CÁLCULOS

Considere o seguinte exemplo teórico: um principal A envia a B uma mensagem cifrada com RSA com a chave pública de B. A mensagem cifrada (representação binária) corresponde ao valor inteiro 26. Esta mensagem cifrada é por si interceptada. De seguida, você obtém a chave pública de B e descobre que esta corresponde ao número inteiro 3, com módulo 33. Neste caso (com estes números pequenos), descubra:

- O valor da mensagem original que A mandou a B
- O valor da chave privada de B

GRUPO II – Questões para resposta com consulta

Questão 4 (~5-10 minutos, 4 valores)

Com o seu browser, aceda a https://www.google.com e obtenha o certificado de chave pública do servidor (Google). Como poderá verificar, esse certificado foi emitido pela CA Thawte SGC CA. De acordo com a inspeção do certificado, responda às seguintes questões:

a) Qual o tamanho em bits da chave pública RSA do servidor https://www.google.com ? Justifique.

b) Se verificar, o método de assinatura usado pela CA que emitiu o certificado para certificar a chave pública RSA do servidor www.google.com é uma assinatura RSA com síntese SHA-1. Esta síntese tem 160 bits. Porque é que o tamanho da assinatura da chave pública do certificado é de 128 bytes e não poderia ter outro valor ? Justifique.

c) Suponha que vai implementar um programa que vai abrir uma conexão SSL com www.google.com e precisa de validar o certificado para garantir autenticação unilateral do servidor. Certamente, nessa conexão SSL, irá receber uma cadeia de certificação do servidor composta por 3 certificados. Suponha que previamente já tinha obtido com confiança o certificado de chave pública da raiz dessa cadeia. Quando começa a inspecionar a cadeia de certificação, o que o levaria a aceitar que o 2º certificado da cadeia (número de série 805306370) tenha servido para emitir o certificado de www.google.com e seja verificado como válido pelo seu programa que estabeleceu a conexao? Indique de forma completa todos os campos do certificado que iria verificar nesse 2º certificado, como condições que o levam a aceitar o certificado de www.google.com.

Questão 5 (~15-20 minutos, 3 valores)

Considere o contexto e a sua análise para efeitos de especificações de implementação do Trabalho Prático nº 2.

Considere também os métodos variantes de autenticação e distribuição de chaves que são suportados no protocolo SSL, nomeadamente: RSA, ADH (*Anonymous Diffie-Hellman*), EDH (*Ephemeral DH)* e FDH (*Fixed DH*). Como se estudou estas variantes apresentam diferentes condições e garantias relativas às propriedades de autenticação, confidencialidade e integridade, para efeitos do protocolo de Handshake SSL e estabelecimento de chaves de sessão, para setup de conexões SSL entre clientes (browsers de utilizadores) e servidores HTTPS.

a) Considere os requisitos e soluções para o protocolo de entrada de utilizadores nas sessões de CHAT, tal como o perspectivou na sua aproximação inicial à respectiva especificação, nomeadamente no que diz respeito a garantias de autenticação, confidencialidade e integridade, no protocolo de entrada (junção ao grupo de CHAT) e estabelecimento de chaves. Tendo em conta as variantes acima referidas para o protocolo SSL (Handshake), qual das variantes mais se aproxima, do ponto de vista das garantias e propriedades de segurança enunciadas, da solução preconizada para o protocolo de entrada nas sessões ? Justifique.

b) Considerando as variantes do protocolo SSL indicadas, qual a variante que considera mais segura ? Justifique.

Questão 6 (4 valores)

Considere o programa:
http://asc.di.fct.unl.pt/ssrc/classes/labmaterials/SSRC/aprat/criptografia-assimetrica/KeyExchangeRef/RSAKeyExchangeExample.java

Este programa implementa no essencial um exemplo de como se poderia implementar um processo que se poderia representar com base na seguinte notação para cifrar uma mensagem M que A enviaria a B:

A>B: {k, iv}KpubB {M}k

em que M (mensagem na variável input) é cifrada com uma chave k de 256 bits, com AES e em modo CTR. De acordo com o exemplo, B (representado no processamento final do programa), abrirá o envelope da chave usando a respectiva chave privada, e depois de retirar a chave da cifra simétrica, acabará por decifrar a mensagem enviada por A.

A>B: {MD(k,iv)}KprivA {k, iv}KpubB {M}k

Isto é, neste protocolo, A assinará a informação do envelope que distribuir a chave, garantindo a autenticidade da mensagem como tendo vindo de A.

a) Com base neste programa, concretize no mesmo tipo de exemplificação, a modelação do protocolo seguinte

A>B: {MD(k,iv)}KprivA {k, iv}KpubB {M}k

Isto é, neste protocolo, A assinará a informação do envelope que distribuir a chave, garantindo a autenticidade da mensagem como tendo vindo de A.

b) Faça uma medida dos tempos de execução para verificar o custo computacional de cada uma das partes da mensagem no custo total de computação do processamento da mensagem enviada (processamento de envio) e o custo total de computação da mensagem recebida (processamento de recepção). Faça um gráfico que mostre o impacto da computação das mensagens e cada uma das suas componentes (assinatura, envelope e cifra da mensagem).

c) Verifique, no tempo total do processamento, o impacto de substituir chaves RSA de 1024 bits por chaves de 2048 bits.

d) Verifique, se nota diferenças significativas, quando a componente de cifra passa a usar outro algoritmo simétrico (por exemplo, Blowfish com 448 bits).

ENVIAR SOLUÇÃO POR E-MAIL, COM ARQUIVO CONTENDO A IMPLEMENTAÇÃO DE a) e d). Deve também enviar anexo os gráficos correspondentes às observações de b) e c).

Questão 7 (4 valores)
Considere o programa:
http://asc.di.fct.unl.pt/ssrc/classes/labmaterials/SSRC/aprat/DH/ThreeWayDHExample.java

Este progarama demonstra a implementação de um modelo e acordo de Diffie-Hellman entre 3 entidades.

a) Porque é que em diferentes execuções do programa, as chaves que as chaves que resultam do acordo tripartido são sempre iguais ? Justifique.

b) Altere o programa de modo a que em diferentes corridas do programa as chaves sejam sempre diferentes.

c) Com base em b), tente produzir um programa que implemente um modelo estendido a 4 entidades.

d) Depois de fazer o programa, meça o impacto temporal provocado pelo custo computacional que envolva apenas 2 entidades, 3 entidades e 4 entidades e faça um gráfico do tempo de execução e tente justificar o gráfico obtido em função da complexidade do custo computacional quando o acordo é estendido de 2 a 4 entidades.

ENVIAR SOLUÇÃO POR E-MAIL, COM ARQUIVO CONTENDO EM DIRECTORIAS SEPARADAS AS IMPLEMENTAÇÕES DE b) e c) e anexando o gráfico para suporte da resposta a d).