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 3 – 7/JUNHO/2006)

Notas:

- O enunciado tem 5 questões, divididas em duas partes:
  - **Parte sem consulta** (Questões 1): 50 min
  - **Parte com consulta** (Questões , 2 e 3) : 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)**
a)	a)	a)
b)	b)	b)
c)	c)	c)
d)		
e)		
f)		
g)		

Questão 1)

a) Pode dizer-se que no sistema PGO a confidencialidade é assegurada com base numa chave simétrica do tipo One Time Key ? Justifique a resposta.

b) A suite criptográfica adoptada pelo sistema PGP bem como os mecanismos complementares usados pelo protocolo no processamento e formatação de mensagens, envolve: DSS/SHA, RSA/SHA, CAST, IDEA, 3DES (com tripla chave), Diffie-Hellman, RSA, ZIP e RADIX 64 bem como controlo de segmentação. Diga qual o papel de cada um destes componentes em termos das propriedades de segurança contempladas pelo suporte do sistema PGP.

c) Porque é que é necessário enviar em cada mensagem PGP um identificador constituído por 16 bits menos significativos associados às chaves públicas do emissor e do receptor e não basta usar como identificador o próprio identificador associado aos principais emissor e receptor ?

d) Descreva o cenário tipo de um ataque "homem-no-meio" durante o protocolo de D-H entre duas entidades A e B. Sugestão: represente o ataque com base num diagrama temporal ou de sequência descrevendo a troca de mensagens entre A e B e a actuação-tipo do atacante para no final obter a mesma chave criptográfica simétrica que A e B pretendem partilhar. Com base nesse diagrama diga como a solução que avançou em c) evita esse problema.

e) Um possível esquema de MAC pode basear-se num algoritmo criptográfico simétrico de desempemnho rápido e uma sequência de blocos obtidos de amostras de relógio (uma stream obtida por concatenação de *timestamps* parciais). Em que consiste genericamente a obtenção de um MAC deste tipo ?

f) Em que consistem as propriedades de "*weak collision resistance*" e "*strong collision resistance*" num método de síntese ?

g) Refira as variantes de modos de autenticação em SSL que podem ser usados tanto em autenticação unilateral como bilateral (ou mútua) e indique qual o que considera mais seguro. Justifique.

Questão 2)

a) Porque é que o campo "signature-trust-field" tende a ter informação replicada (sendo na prática uma cópia) que pode ser usada como uma cópia cache do campo "owener-trust-field" durante o processamento da gestão de confiança subjacente às entradas de um chaveiro de chaves públicas por parte de um principal que utiliza o sistema PGP ? Sendo assim, qual o interesse que vê em ter essa informação duplicada ? Justifique adequadamente e claramente a sua resposta.

b) Pedem-lhe para utilizar o sistema PGP para suportar o envio de correio electrónico para listas de mail que podem conter potencialmente um número muito elevado de subscritores (da ordem de centenas de milhares).

   B1) Diga como proporia uma solução para que o sistema fosse usado para enviar mensagens autênticas e íntegras mas não confidenciais para essas listas.

   B1) Diga como proporia uma solução para que o sistema fosse usado para enviar mensagens autênticas, íntegras e confidenciais para essas listas.

   A ideia subjacente às repostas não pode modificar o PGP tal como está definido. A solução deve usar o PGP tal como está normalizado, referindo apenas como conceberia e proporia uma solução para a utilização do PGP tendo em vista os requisitos enunciados.

c) Os 16 bits prévios à síntese e que "viajam" no campo de assinatura de uma mensagem PGP são passados em claro. Diga em que medida isso compromete ou não a segurança do sistema e qual o interesse em que essa informação passe em claro. Tal poderia ser evitado ? Como ? O que se ganharia ?

Questão 3)

a) Na evolução do sistema Kerberos, a evolução da versão 4 para a versão 5 procedeu a melhorias interessantes entre as quais a optimização do protocolo evitando situações de duplas operações criptográficas sem necessidade nenhuma do ponto de vista de segurança efectiva. Mostre, justificando, o caso (ou casos) em que essa melhoria introduzida é vantajosa.

b) Duas noções interessantes no sistema Kerberos possuem um papel importante na versão 5 do protocolo: as noções de sub-chave e de número de sequência. Tente indicar as vantagens de exploração destas duas novidades introduzidas na versão 5 face à versão 4 do protocolo Kerberos.

c) Indique em que condições e como um servidor Kerberos tanto pode ser usado como proxy (ou relay), numa cadeia de *proxying* até um servidor Kerberos, final, de modo que o cliente pode assim delegar sucessivamente o seu processo de autenticação na instância do servidor Kerberos final. Diga como e porque pode isso ser suportado.