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

Curso de Engenharia Informática (2º Ciclo)

Segurança em Sistemas e Redes de Computadores

SSRC-0809-EN-1.1.B

2º Semestre 2007/2008

Exame de Época Normal, 20/Junho/2008

Notas:

- O enunciado tem 7 questões, divididas em diversas alíneas.
- Podem utilizar-se 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 é considerada um factor de avaliação.
- A duração da prova é de 2h30min (máximo)

---------- 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 ----------

1)	2)	3)	4)	5)	6)	7)	TOTAL

INF Controlo:

Questão 1)
Considere a *framework* OSI X.800, nomeadamente no que diz respeito à definição dos **serviços de segurança** e **mecanismos de segurança** que estão na base desses serviços. Considere também a tipologia e terminologia de ataques de segurança estudados e sua caracterização, nomeadamente: release of message contents, traffic analysis, masquerading, replaying, tampering e DoS.
A tabela 0 (anexa) representa a relação entre os serviços de segurança e os mecanismos de segurança abordados no âmbito da *framework* X.800. Cada célula na tabela está preenchida com Y para indicar os mecanismos básicos de segurança que estão na base do suporte de cada um dos serviços.

a) Faça uma nova tabela, de forma similar, em que **nas colunas coloque os ataques** (classificados como passivos e activos) **e nas linhas coloque os mecanismos de segurança** usados na base dos serviços usados como contra-medidas para esses ataques.

b) Faça uma nova tabela, de forma similar, em que **nas colunas coloque a tipologia de ataques** (classificados como passivos e activos) e **nas linhas coloca os serviços de segurança** usados como contra-medidas para esses ataques.

Questão 2)

a) Sintetize quais as premissas fundamentais de um modelo adversarial do tipo Dolev-Yao.

b) Um ataque por intrusão devido a um vírus instalado através da execução de um conteúdo executável capturado a partir de um site Web, está contemplado no modelo de adversário de Dolev-Yao ? Justifique.

c) Um ataque do tipo ARP Spoofing está comportado pela definição de um ataque do tipo Dolev-Yao? Justifique.

d) Um ataque vulgarmente designado por *Phishing* para posterior captura de passwords ou segredos de um utilizador, que seja desencadeado através de E-Mail ou Instant Messaging, está contemplado no modelo de adversário de Dolev-Yao ? Justifique.

Questão 3)
Em SSL, usa-se HMAC como método expedito de síntese e autenticação de mensagens encapsuladas no sub-protocolo RLP (Record Layer Protocol).

a) No processamento SSL, se opcionalmente se estiver a usar compressão de dados, a ordem do processamento de cada fragmento é a seguinte: (1) compressão do fragmento, (2) concatenação da assinatura HMAC, (3) cifra com a chave de sessão. Diga se também seria adequado fazer-se a seguinte sequência: (1) concatenação da assinatura MAC ao fragmento *plaintext*, (2) cifra com a chave de sessão e (3) compressão apenas no fim.
b) Porque é que a assinatura de cada record RLP é um HMAC e não uma assinatura de chave pública, e em que medida isso é mais ou menos inseguro?
c) Dois processos P1 e P2 estão a usar comunicação suportada em sockets TCP, modo de autenticação unilateral e estabelecimento de chaves RSA. P1 estabelece a conexão, mas P2 é que actua em modo cliente no handshake SSL. Qual dos dois processos (P1 ou P2) é responsável por gerar a chave de sessão ? Justifique.

Questão 4)

a) Apresente comparativamente vantagens e desvantagens entre os modos de cifra simétrica seguintes, em termos do seguintes critérios: (1) recuperação de erros de cifra, (2) desempenho (*performance*) (3) recuperação face a erros de transmissão por troca de bits em blocos, (4) recuperação face a perda de bits em blocos, (5) incremento do tamanho da cifra produzida e (6) maior robustez de segurança, face à utilização dos seguintes modos de cifra: EBC, CBC, CFB, e CTR. Sugestão: organize a resposta numa tabela (numa página A4), com os modos por linha e os critérios indicados por coluna. Em cada célula da tabela indique com sinal "+" indicando modos mais vantajosos e "–" os modos mais desvantajosos. Use mais do que um sinal se quizer diferenciar ou reforçar a vantagem ou desvantagem de uns modos face a outros. Pode incluir na sua resposta uma pequena justificação em relação à sua visão comparativa.

b) Um algoritmo de cifra simétrica por blocos, operado no modo CBC, pode ser utilizado como bloco base para construir um método de cifra em cadeia, de modo a poder cifrar-se continuamente um fluxo de dados, quando esses dados têm que ser transmitidos bit a bit, para serem depois decifrados igualmente numa cadeia, bit a bit. Suponha por exemplo que se trata de um fluxo contínuo de dados, do tipo uma *stream* de vídeo transmitida e consumida em tempo real. Descreva uma solução de como isso pode ser feito, no pressuposto que o emissor e o receptor já possuem uma chave secreta partilhada.

Questão 5)

a) Em que consiste o princípio de assinaturas duais suportadas em assinaturas do tipo MAC ou HMAC ?

b) Conhece algum protocolo de segurança em que as assinaturas duais com HMACs sejam usadas de forma relevante para implementar requisitos de segurança entre a informação enviada por um principal a outros principais? Diga qual e explique os requisitos para uso dessas assinaturas duais com HMAC nesse mesmo protocolo.

Questão 6)

a) O protocolo Kerberos está imune a um ataque à autenticação de utilizadores que tem por base um ataque do tipo dicionário a *passwords* ? Justifique a sua resposta.

b) Uma das modificações do Kerberos entre a versão 4 e a versão 5 reside na optimização introduzida que evita que se façam desnecessariamente duas cifras encadeadas ou dupla encriptação, aspecto apontado como uma das deficiências da versão 4 do protocolo. Discuta essa melhoria em relação às suas vantagens e pressupostos de segurança.

Questão 7)

Diga se a suite IPSec (seus protocolos e serviços) suporta ou não as seguintes noções de serviços de segurança. Justifique a resposta descrevendo como e se considera essa protecção completa face às noções indicadas (estabelecidas a partir da terminologia OSI X.800):

7.1 Access Control
7.2 Connection and connectionless confidentiality
7.3 Connection and Connectioneless integrity
7.4 Traffic flow confidentialty
7.5 Data Origin Authentication
7.6 Peer-Authentication

TABELA 0

Service	Mechanism							
	Enciph-erment	Digital signature	Access control	Data integrity	Authenti-cation exchange	Traffic padding	Routing control	Notari-zation
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Non-repudiation		Y		Y				Y
Availability				Y	Y			