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)

Usando a caracterização da framework OSI X.800, que diferença existe entre as seguintes noções, dando exemplos concretos das mesmas no que diz respeito a protecção por parte de protocolos e serviços de segurança à sua escolha que protejam face a cada uma das noções. Nota: pode utilizar exemplos de serviços e protocolos de segurança, a diferentes níveis da pilha TCP/IP (nível rede até nível aplciação).

a) ***Peer Entity Authentication*** **vs.** ***Data Origin Authentication***
b) ***Connection Confidentiality*** vs. ***Selective-Field Confidentiality***
c) ***Connection Integrity without recovery*** **vs.** ***Connection Integrity with recovery***

Questão 2)

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 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.

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.

Questão 3)

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 e CTR.

b) Um algoritmo de cifra simétrica por blocos, operado no modo CBC, pode ser utilizado como componente 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

c) Porque é que a solução em b) é mais ou menos adequada comparativamente a usar cifra de blocos OFB, CFB ou CTR.

Questão 4)

a) Um método de distribuição de chaves como o método de Diffie Hellman é melhor ou pior do que o modelo de Needham-Schroeder com criptografia simétrica do ponto de vista de critérios e garantias de segurança futura perfeita? Justifique a sua resposta**.**

b) Quando em SSL se usam os modos de autenticação Ephemeral Diffie Hellman, Fixed Diffie Hellman ou RSA, qual deles apresenta melhores condições do ponto de vista de segurança futura perfeita ? Justifique a sua resposta.

Questão 5

Diga, para cada um dos eventuais ataques indicados, em que consiste o suporte de defesas no protocolo SSL:

A1) Message Replaying de records SSL
A2) Man-In-the-Middle, com ataque à autenticação, seja do tipo "peer-entity authentication" seja do tipo "data-origin authentication"
A3) IP Spoofing
A4) IP Hijacking com possibilidade de controlo da conexão SSL tomando o atacante o lugar do endereço IP de um dos extremos da sessão, após o estabelecimento da sessão.
A5) DoS provocado por um ataque do tipo SYN-flooding à conexão TCP subjacente ao protocolo SSL
A6) Tampering dos records SSL (RLP)
A7) Ataque provocando desordenação de records SSL no meio de uma sessão SSL (note que o transporte subjacente seja TCP ou UDP)

Questão 6)

a) Diga como proporia uma solução baseada em PGP para que o sistema fosse usado para enviar mensagens autênticas assinadas pelo emissor, íntegras e confidenciais para *mailing lists* (listas de distribuição de Email) constituídas por um número muito grande de subscritores individuais.

b) Porque é que é necessário enviar explicitamente em cada mensagem PGP um identificador constituído pelos 16 bits menos significativos associados às chaves públicas do emissor e do receptor e não basta estarem contidos nas mensagens os endereços de Email que identificam os mesmos ? Justifique.

Questão 7)

a) Comparando a versão 4 com a versão 5 do protocolo Kerberos, uma das inovações é a introdução das noções de sub-chave e de número de sequência. Tente ilustrar um cenário de utilização do sistema em que este suporte seja útil do ponto de vista de segurança. Justifique a sua resposta.

b) Na análise da especificação do protocolo AH em IPSec, refere-se que nem todos os campos do cabeçalho IP (seja IPV4 ou IPV6) são incluídos no cálculo de uma assinatura MAC para autenticação do pacote. Suponha que está a utilizar AH com adjacência, transporte + túnel, com IPV4 (end-systems) e IPV6 (entre routers).

B1) Que tipo de campos do cabeçalho não podem ser incluídos na assinatura MAC que cobre os pacotes IPV4 dos sistemas finais ?

B2) Idem para pacotes IPV6 do túnel adjacente.

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			