DI/FCT/UNL
Mestrado Integrado em Engenharia Informática

Segurança de Redes e Sistemas de Computadores
2º Semestre, 2015/2016
(14/Abril/2016 T1A)

T1: Teste sobre tópicos teóricos do programa
Teste sem consulta, duração: 1h45m

Questão 1

a) De acordo com as noções, conceitos e terminologias na *framework* X.800 indique a diferença entre um ataque passive e um ataque ativo a um canal de comunicação.

b) Ainda com base na terminologia e tipologia de ataques às comunicações conforme a *framework* X.800, indique a seguir, nos espaços indicados, dois tipos de ataques passivos e cinco tipos de ataques ativos, descrevendo depois numa folha anexa, em que consistem os mesmos.

Tipologias de Ataques Passivos

P1 – _____

P2 – _____

Tipologias de Ataques Ativos

A1 – _____

A2 – _____

A3 – _____

A4 – _____

A5 - _____

c) A tabela seguinte permite representar a associação (nas posições Y) entre propriedades de segurança (nas linhas) e mecanismos de segurança (nas colunas), de acordo com a terminologia do modelo conceptual de segurança subjacente à *framework* OSI X.800.

Com base nesta tabela e nas tipologias de ataques que indicou em b), complete uma tabela similar (preenchendo os respetivos Ys) para mapear mecanismos concretos de segurança (nas colunas) como mecanismos base para suporte de contra-medidas face aos ataques (P1, P2, A1, A2, A3, A4, A5) indicados antes.

(**Nota:** *responda usando a tabela no enunciado*).

Table 1.4 Relationship Between Security Services and Mechanisms

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			

Mechanism		**Passive Attacks**		**Active attacks**				
		P1	**P2**	**A1**	**A2**	**A3**	**A4**	**A5**
M1	AES Algorithm							
M2	CMAC using symmetric crypto alg. 3DES and CBC mode							
M3	Switched LAN Access Control based on assigned fixed MAC addresses (in each switch port)							
M4	SHA-512 Algorithm							
M5	HMAC with SHA-1 or MD5							
M6	Introduction of random traffic padding in a data-stream message, before encryption							
M7	Encryption of a Message Digest (hash) of a message, encrypted with a private key using a asymmetric crypto algorithm (ex., RSA private Key)							
M8	Encryption with a RSA public key							
M9	PKCS#7 used in plaintext encrypted with AES and CBC Mode							
M10	Authentication auditable LOGs maintained by a KDC running the Needham-Schroeder Algorithm for Key-Distribution							
M11	Use of randomly generated nonces for challenges), controlled with appropriate responses in a communication protocol							
M12	Use of sequence numbers or timestamps, encrypted in messages exchanged by two principals.							

Questão 2

a) Em que circunstâncias deve privilegiar na utilização de um algoritmo criptográfico simétrico o uso do modo de cifra ECB em vez de CBC ? Justifique.

b) Em que circunstâncias deve privilegiar na utilização de um algoritmo criptográfico simétrico o uso do modo de cifra OFB ou CFB em vez de CBC ? Justifique.

c) Entre os diversos modos (CBC, ECB, OFB, CFB, CTR), qual o modo que considera à partida como susceptível de permitir uma implementação com maior desempenho ? Justifique.

d) Suponha que apenas tem à sua disposição uma implementação de um algoritmo criptográfico simétrico que implementa uma cifra segura por blocos, capaz de operar com chaves suficientemente grandes (ex., maiores de 128 bits) e blocos de pelo menos 128 bits (ex., RC6, AES, Twofish, Você precisa de implementar um algoritmo de cifar em cadeia, para ser usado como cifra de cadeias de bits (ou seja, como um método criptográfico implementando uma *stream-cipher*) de modo a poder conseguir cifrar "bit" a "bit" uma emissão de *streaming* codificado com constrangimentos de transmissão em tempo real (a fonte de dados plaintext debita informação real-time, bit a bit).

   Como se proporia conceber um método para realizar as operações de cifra (na emissão) e decifra (na recepção), usando como módulo base o algoritmo de cifra por blocos ? Apresente a sua proposta com base num diagrama de blocos de processamento, em que um deles é o algoritmo criptográfico simétrico a utilizar.

   Racional: para a sua proposta parta da estrutura básica (modular) de um algoritmo de cifra em cadeia (*stream-cipher*).

Questão 3

Responda Verdadeiro (V) ou Falso (F), justificando ou argumentando com fundamentação nos casos que considera FALSO.

a) Um algoritmo criptográfico simétrico que implementa uma cifra de blocos, pode usar qualquer modo de cifra (ex., ECB, CTR, OFB, CFB, CBC ou CTR) independentemente do tamanho do bloco base que opera e da dimensão da chave criptográfica que utiliza.

b) Um algoritmo criptográfico simétrico que implementa uma cifra em cadeia pode ser usado de forma a operar um modo ECB

c) Quando se usa um algoritmo criptográfico simétrico que possa operar com blocos e no modo CTR, a cifra e a decifra de mensagens apenas requer que se use a função de cifra (não sendo necessária a função de decifra).

d) Uma função de síntese que garanta a propriedade de resistência forte a colisões (*strong collision resistance*), garante também a propriedade de resistência fraca a colisões (*weak-collision resistance*).

e) Suponha que utiliza um protocolo seguro de transferência de mensagens, suportado sobre TCP para implementar um canal seguro, com garantias de autenticidade dos *endpoints* (*DNS names*, endereço IP e Porto), confidencialidade dos dados (apenas *payloads* dos segmentos TCP), integridade (com base numa prova materializada por um mecanismo do tipo MAC) e garantias contra *message-replaying* (com base em mecanismos do tipo random nonces/responses), que viajam cifrados, conjuntamente com o payload das mensagens TCP. Se esse protocolo garante essas propriedades entre dois principais A e B, continuará a garanti-las mesmo que existam proxies (TCP) entre A e B.

f) Nas mesmas condições de e), não será preciso incluir os mecanismos do tipo *random-nonces* / *reponses* cifrados conjuntamente com o *payload*, pois usando-se TCP este já garante o sequenciamento das mensagens, o que garante implicitamente proteção contra *message-replaying*.

Questão 4

a) Indique e defina as propriedades de segurança de um algoritmo de síntese segura de mensagens. (Nota: tal como estudado, tratam-se de 7 propriedades, mas no mínimo deve indicar cinco).

b) Qual a diferença entre confidencialidade de dados e confidencialidade de tráfego (*Data confidentiality* vs. *Traffic confidentiality*). Complete a sua resposta com dois exemplos sugestivos dessa diferença.

c) Um mecanismo para autenticidade e integridade de mensagens do tipo MAC (HMAC ou CMAC) pode ser usado como prova de autenticação de um principal que emitiu uma mensagem, tendo em vista ter uma prova base para garantia da propriedade de não-repudiação da origem dessa mensagem ? Justifique.