Network Security and Cryptography

December 2015

Sample Examination Paper

Answer ALL questions.

Clearly cross out surplus answers.

Time: 3 hours

The maximum mark for this paper is 100.

Any reference material brought into the examination room must be handed to the invigilator before the start of the examination.

Answer ALL questions

Marks

Question 1

a) Briefly describe the processes of *encryption* and *decryption* in relation to cryptography. **5**

b) What is the difference between Symmetric and Asymmetric key encryption? **4**

c) Suppose you decide to use a 10-bit key. How many combinations are there? **1**

Total: 10 Marks

Question 2

a) James and Alexander are having a debate about Public Key Infrastructure (PKI). James says that it is simply a way of authenticating users. However, Alexander argues that it is a type of encryption algorithm. They have asked you to decide who is correct. **6**

Briefly outline the purpose of PKI. You should also explain what is meant by a certificate authority and digital certificate.

b) Are James's and Alexander's opinions about Public Key Infrastructure correct or incorrect? For **each** opinion, you should provide ONE (1) reason for why it is either correct or incorrect. **4**

Total: 10 Marks

Question 3

a) IPsec is a suite of protocols for securing networks. Briefly outline how it provides confidentiality, integrity and authentication. **3**

b) Briefly explain what is by an Authentication Header (AH) **and** an Encapsulating Security Payload (ESP). **6**

c) Draw a diagram to show where IPSec fits in the TCP/IP model. **1**

Total: 10 Marks

Questions continue on next page

Marks

Question 4

a) Explain what is meant by a digital signature **and** describe how it is generated. **6**

b) Does a digital signature ensure the entire message is encrypted? You should provide ONE (1) reason to support your answer. **2**

c) Name the IETF standard for email security **and** briefly outline what additional security it provides in addition to digital signatures. **2**

Total: 10 Marks

Question 5

a) Explain what is meant by the term *firewall* in network security **and** discuss how it is used in network architectures. **7**

b) Firewalls use Access Control Lists (ACL). Explain what is meant by an ACL and typical contents. **3**

Total: 10 Marks

Question 6

a) Employees are increasingly connecting to company networks remotely via mobile devices such as laptops, tablets and smartphones. Remote access needs to satisfy five essential requirements to be efficient and secure. Identify and briefly explain each of these FIVE (5) requirements. **5**

b) There are several methods of achieving secure remote access. One important method is to use a VPN. Explain if/ how a VPN achieves each of the requirements in part (a) **5**

Total: 10 Marks

Question 7

a) Confidentiality, Integrity and Availability are core attributes in security. Identify THREE (3) threats to a wireless network that could compromise security. You should state the security attribute that is compromised by each threat. **6**

b) Spell out the acronyms PSK and EAP. Briefly explain the difference between PSK and EAP for authenticating devices onto a Wireless network. **4**

Total: 10 Marks

Questions continue on next page

		Marks
Question 8		
a)	Briefly explain what is meant by a password audit.	**2**
b)	Explain what is meant by the term *salt* in relation to cryptography. You should discuss how it is used to make it more difficult to crack passwords.	**4**
c)	Discuss TWO (2) alternative methods of authentication **and** outline ONE (1) advantage or disadvantage of each method.	**4**
		Total: 10 Marks
Question 9		
a)	Briefly describe the term *vulnerability* in the context of network security **and** provide THREE (3) examples of vulnerabilities in a network.	**5**
b)	Explain what is meant by a *vulnerability assessment* in the context of network security **and** provide THREE (3) reasons why it is important.	**5**
		Total: 10 Marks
Question 10		
a)	James and Alexander are having another debate about computer and network security. James says that it is the job of security professionals to find all vulnerabilities and every threat and make sure the system is always 100% secure. Do you agree with James? You should explain your answer with NINE (9) reasons.	**10**
		Total: 10 Marks

End of Examination Paper