Aston University

School of Engineering and Applied Science
DC3190 – Information Security
Final Examination

CLOSED BOOK

Date: TBA August 2018

Time: TBA

Duration: 2 hours

Instructions to Candidates

1. This exam paper contains FIVE questions worth 25 marks EACH.
2. Answer FOUR questions ONLY
3. Use of Casio fx-85ms OR Hewlett Packard HP10S Scientific calculators IS allowed

Materials provided

1. Answer booklets

Please note that the exam questions are printed on both sides of the exam paper.

This exam paper cannot be removed from the exam room.

Show your working in all calculations.

This examination is subject to the Examination Regulations for Candidates

1.

a) List and define the THREE key goals of Information Security.

(6 marks)

b) Analyse the security attack described in the News article in the box below. Briefly discuss the **vulnerabilities** that enable such a **denial-of-service attack**. Briefly discuss the **security controls** that can be used to mitigate the negative effects of such attacks for any TWO of: (i) the affected computers, (ii) their Internet Service Providers (ISPs) and (iii) the affected websites.

(7 marks)

> .CN websites come under attack (August 26, 2013 at 1:00 pm by Paul Bischoff)
>
> China's national registry of websites ending in ".cn" was hit by a denial-of-service attack yesterday. Several websites with the .cn suffix were either inaccessible or extremely slow, including the popular Twitter-like Sina Weibo, Amazon.cn, and the Bank of China. Many Weibo users were unable to log on during the attack.
>
> About 30 minutes after midnight on Sunday, the attacks crippled the registry for more than 13 hours until 2 p.m. Then, just two hours later at around 4 p.m., another wave of attacks struck. CNNIC did not specify where the attacks originated from, but it did say it was the largest denial of service attack it's ever underwent. As of the latest announcement, the registry is still recovering.
>
> Although it's unclear whether or not the attack originated in China, antivirus software vendor Symantec's 11th Internet Security Threat Report says the mainland accounted for 26 per cent of more than six million computers worldwide found to be infected by bots – programs covertly installed in a computer to allow an unauthorised user to remotely control the machine. These bots are brought online to conduct this type of attack.

c) An **authentication system** is composed of THREE main components. What are these components? Give a brief description and ONE example of each of these components.

(6 marks)

d) Describe EACH of the THREE classic programming error types: **buffer overflows**, **incomplete mediation**, **time-of-check to time-of-use** errors.

(6 marks)

2.

a) Explain the relationship between the **Caesar cipher** and the **shift cipher**.

(2 marks)

b) Is the **shift cipher** a symmetric or asymmetric cryptosystem? Justify your answer.

(3 marks)

c) Encrypt the Shakespeare quotation below using the **shift cipher** and a valid encryption key of your choice. Ignore punctuation marks and white space characters. Show every step in the encryption process.

"To be, or not to be: that is the question."

The numerical representation of the letters from the English alphabet is given below for convenience.

a **0**	**b** **1**	**c** **2**	**d** **3**	**e** **4**	**f** **5**	**g** **6**	**h** **7**	**i** **8**	**j** **9**	**k** **10**	**l** **11**	**m** **12**
n **13**	**o** **14**	**p** **15**	**q** **16**	**r** **17**	**s** **18**	**t** **19**	**u** **20**	**v** **21**	**w** **22**	**x** **23**	**y** **24**	**z** **25**

(8 marks)

d) The table below shows the average character frequencies for typical English plaintext.

Based on the information in this table, analyse the **ciphertext** "WJJQJHYNTS", which was produced by encoding a message using the **shift cipher**.

Explain how you can find out the most likely encryption key used in the encoding, state the value of this encryption key and use it to decode the **ciphertext** to find the **plaintext**.

(12 marks)

a 0.080	h 0.060	o 0.080	v 0.010
b 0.015	i 0.065	p 0.020	w 0.015
c 0.030	j 0.005	q 0.002	x 0.005
d 0.040	k 0.005	r 0.065	y 0.020
e 0.130	l 0.035	s 0.060	z 0.002
f 0.020	m 0.030	t 0.090	
g 0.015	n 0.070	u 0.030	

3.

a) The complete set of access control lists for a computer system is given below:

File-1: ((Alice, rw), (Bob, r), (Cathy, r))
File-2: ((Alice, r), (Bob, orw))
File-3: ((Alice, orw), (Bob, r), (Cathy, orw), (Dan, orw))
File-4: ((Alice, r), (Bob, r), (Cathy, orw))
File-5: ((Alice, r), (Bob, r), (Cathy, r))

i) Draw the **access control matrix** for this computer system.

(6 marks)

ii) Identify TWO potential **covert channels** for this computer system.

(2 marks)

b) Consider the scenario in which an attacker steals the ID card of a company employee and attempts to use it to gain unauthorised access to the company's office. The office door is protected by a swipe-card security system that uses six-digit personal codes to authenticate ID card owners. The attacker tries to guess the six-digit code associated with the stolen ID card by repeatedly swiping the card and trying one code at a time. Assume that each try takes six seconds and that the attacker starts at 1:30am.

i) Calculate the minimum probability for the attacker to break in by 6:30am on the day when the attack started.

(6 marks)

ii) Calculate the latest time by which the attacker can guess the entry code with probability 0.7.

(6 marks)

iii) Explain why a six-digit code might be sufficient for the swipe-card system described above, but might not be for an online log-in system for which no physical action (swiping the card) is needed. Suggest a control to mitigate the issue in an online log-in system.

(5 marks)

4.

a) Present the steps of the **challenge-response authentication mechanism** and illustrate their execution using a simple example.

(8 marks)

b) The security levels for several subjects and objects of an information system are shown in the following table:

Security Class	**Subject**	**Object**
5 - Top Secret	Alice	Personal Files
4 - Secret	Bob	E-mail Files
3 - Confidential	Cathy	System Logs
1 - Unclassified	Dan	Blog Files

Describe the **Bell-LaPadula model** of security and classify each of the following operations as permitted or prohibited by the Bell-LaPadula model and explain why:

i) Cathy reads the Blog files;
ii) Bob updates the E-mail files based on information from the Personal files;
iii) Dan updates the System Logs;
iv) Alice copies information from a Blog file to Personal files.

(10 marks)

c) Describe the operation of **computer worms**. Give an example of a worm and its effect. What is the difference between computer worms and computer viruses?

(7 marks)

5. a) Describe the role of a **firewall** within an IT system, giving examples of TWO simple **security policies** that firewalls can implement.

(5 marks)

b) Explain in detail the operation of a **packet filtering gateway**.

(5 marks)

c) Draw a diagram to illustrate the use of a packet filtering gateway to block all traffic from a specific remote network and all telnet traffic, but to allow all other traffic (such as HTTP traffic) through.

(5 marks)

d) Give brief definitions of **port scans** and **social engineering attacks**, compare and contrast how they operate as precursors of a network attack and suggest a set of controls that, when combined, would provide protection against them both.

(10 marks)

END OF EXAMINATION PAPER