SEMESTER 2 EXAMINATIONS 2018/2019

PRINCIPLES OF CYBERSECURITY

Duration 120 mins (2 hours)

This paper contains five questions.

Answer **THREE** questions **ONLY**

Each question carries 1/3 of the total marks for the examination paper and you should plan to spend about 40 minutes on it.

An outline marking scheme is shown in brackets to the right of each question.

A maximum of 99 marks are available for the paper.

Only University approved calculators may be used.

A foreign language dictionary is permitted ONLY IF it is a paper version of a direct 'Word to Word' translation dictionary AND it contains no notes, additions or annotations.

6 page examination paper

Question 1

An attack against a government data centre has resulted in a data breach. Several confidential documents were stolen from a database and published online, with the clear intention of disclosing compromising information publicly. A preliminary forensics analysis established that attackers broke into the data centre by taking advantage of a known vulnerability of the data centre software used to provide Internet web services, which was exposed to the Internet. This vulnerability allowed the execution of arbitrary code on the machine running that software.

The government has commissioned a more detailed analysis, based on the *kill chain* model, to identify the attacker profile and the strategy used.

(a) Explain the *"kill chain"* model in general terms and how the model can be used. Describe each of the seven attack phases and how more complex attacks can use multiple phases.

[10 marks]

(b) Analyse the attack by using the kill chain model by firstly identifying the phases used in this attack. Then, for each phase, briefly explain what might have happened. When no detailed information is available for a specific phase, suggest and justify possible actions the attacker might have taken. Explain and justify any phase that is not considered relevant for this attack.

[14 marks]

(c) The attackers could be classified as Cybercriminals, Nation States or Hacktivists. For each of these categories, discuss whether they might be responsible for the attack, in terms of attack strategy and motivation.

[9 marks]

Question 2

(a) Serial numbers (such as the ISBN) often incorporate a *check digit* to detect transmission errors. Explain how this concept can be extended to a *message digest* (or *message hash*) capable of detecting transmission errors in an entire message and discuss in detail the properties necessary for such a digest.

[7 marks]

(b) Explain in detail how such a message digest can be extended to provide a *digital signature* capable of detecting any attempt to compromise the integrity of a message.

[7 marks]

(c) Alice wishes to communicate a message consisting of a sequence of decimal digits to Bob, using the Internet. While the message is not confidential, it is important to check the integrity of the message. Alice and Bob have agreed to use a simple message digest, consisting of the addition of all message digits, modulo 31. They have also agreed on a simple monoalphabetic substitution cipher, where each digit n is replaced by (n+3) modulo 10.

Using the message 71306422649825 as an example, write down the transmission that Alice needs to send, explaining every step of the process in detail.

Then show how Bob can have confidence in the integrity of the message, again explaining every step in detail.

[12 marks]

(d) Discuss the deficiencies in the simple scheme that Alice and Bob are using and explain in detail how it can be improved.

[7 marks]

TURN OVER

Question 3

"NoName plc" is a large e-commerce company, which handles a significant amount of customer personal information, complies with all the required cybersecurity standards and has no security-critical business-processing tasks. "NoName" wishes to strengthen its cybersecurity defences and requires advice on which additional cyber controls should be deployed.

(a) The U.K. Government *Cyber Essentials* scheme identifies five different recommendations: boundary firewalls, secure configuration, user access control, malware protection and patch management.

Describe each of these recommendations and explain in detail the likely effectiveness of the *Cyber Essentials* approach in the context of the "NoName" requirements.

[10 marks]

(b) Identify three advanced cyber defences that "NoName" can adopt to enhance its cybersecurity. For each of them, explain the operation and discuss in detail how they operate to improve security.

[15 marks]

(c) "NoName" is particularly concerned about ransomware attacks. Among the three advanced cyber defences identified in (b) above, select the one you consider most effective against ransomware and justify your choice. Explain exactly why it is more effective than the others and to what extent it can prevent ransomware attacks. What else can "NoName" do to strengthen its protection against ransomware attacks?

[8 marks]

Question 4

(a) Explain in detail the advantages, disadvantages and difficulties of *data anonymisation*. One approach that is sometimes used is *data reduction* - describe with examples *two* specific techniques to achieve this.

[10 marks]

(b) The dataset below

Forename	Surname	Age	Value #1	Value #2
Leo	Aniello	21	68	58
Federico	Lombardi	19	75	84
Sarah	Martin	23	55	82
Andrea	Margheri	25	71	78
Shorouq	Alansari	20	46	68
Julian	Rathke	27	83	78
Minnie	Mouse	24	74	68
Vladimiro	Sassone	20	100	100
Salman	Rushdie	25	88	82

is to be anonymised using *micro-aggregation* (with every k-partition containing three records). Explain in detail how this technique provides anonymity and describe the precise procedure to be followed, complete with the replacement dataset.

[12 marks]

(c) Explain in detail the concept of *differential privacy*, complete with appropriate examples.

[11 marks]

TURN OVER

Question 5

Effective cybersecurity requires a multidisciplinary approach, considering not just technical measures and defences but also the interaction with other subject areas such as

- management and business aspects
- law enforcement and cyber crime
- economic factors
- social factors
- human factors

For each of these different subject areas, provide a short analysis discussing the key issues affecting cybersecurity, complete with examples as appropriate to demonstrate the importance of a multidisciplinary approach.

[33 marks]

END OF PAPER

