SEMESTER 2 EXAMINATIONS 2017/18

PRINCIPLES OF CYBER SECURITY

Duration 120 mins (2 hours)

This paper contains 4 questions

Answer **ONE** question in **Section A** and **BOTH** questions in **Section B.**

Section A carries 1/3 of the total marks for the exam paper.

Section B carries 2/3 of the total marks for the exam 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.

5 page examination paper

SECTION A

Answer ONE question

A1

"BankPlus" is a small local bank that provides online-only banking services to their customers.

(a) Identify *four* possible attack scenarios that could target BankPlus. For each of your proposed scenarios discuss (with justifications) who is a possible attacker for the scenario, their motivation and required skills

[12 marks]

(b) For each of your identified scenarios discuss (with justifications) the risk represented by the scenario in terms of its impact and likelihood. Prioritize the scenarios based on their risk.

[12 marks]

(c) Propose (with justifications) a possible mitigation for the scenario that represents the highest security risk for BankPlus.

[9 marks]

A2

(a)   Explain what *ransomware* is and provide two detailed examples of recent ransomware attacks.

[5 marks]

(b)   Discuss in detail all the phases of the "kill chain" for a ransomware attack.

[20 marks]

(c)   Propose and discuss a set of security controls that could disrupt the "kill chain" for a ransomware attack.

[8 marks]

TURN OVER

SECTION B

Answer ALL questions

B1

"Genoma" is a new biobank that stores human biological samples related to lung cancer, the data derived from the analysis of the samples and the medical history of the patients from which the samples were collected.

a) Explain in detail the privacy threats that the patients whose data are stored by Genoma are subject to.

[10 marks]

b) Explain in detail what information stored by Genoma is subject to the new General Data Protection Regulation.

[8 marks]

c) Explain in detail the steps that Genoma must take to comply with the new General Data Protection Regulation.

[15 marks]

B2

"Famebook" is a social network, where online users share personal information such as relationship status, pictures, and comments with their friends. Alice is a registered user of Famebook. Each time Alice updates her friends list, she first connects to the social network's web portal. The portal communicates with the social network's server, and the friendship information of Alice and all other users of that social network is stored in a database.

a) Propose a security solution to ensure that i) only Alice's family members can access Alice's profile information; ii) that only her friends can access her photos and wall posts iii) that only her acquaintances can access her wall post. Explain how your solution can be implemented.

[13 marks]

b) Propose a security solution that protects the confidentiality of Famebook user information stored in the database. Explain how your solution can be implemented.

[9 marks]

c) Propose a security solution that provides mutual authentication between the client application and the social network's web portal. Explain how your solution can be implemented.

[11 marks]

END OF PAPER