CORK INSTITUTE OF TECHNOLOGY
INSTITIÚID TEICNEOLAÍOCHTA CHORCAÍ

Semester 1 Examinations 2017/18

Module Title:	**Computer Security Principles**

Module Code: **COMP 6035**

School: Computer Science & Mathematics

Programme Title: **B.Sc. (Hons) in Software Development Y1**
B.Sc. (Hons) in IT Management Y1
B.Sc. (Hons) in Web DevelopmentY1
B.Sc. in Information Technology Y1
B.Sc. (Hons) in Computer Systems Y1
B.Sc. in Software Development Y1

Programme Code: **KSDEV_8_Y1**
KDNET_8_Y1
KCOMP_7_Y1
KITMN_8_Y1
KITSP_7_Y1
KWEBD_8_Y1

External Examiner(s):   **Prof Gregory O'Hare**
Internal Examiner(s):   **Dr. S. Abdi, Dr. Vincent Emeakaroha, Dr. P. Reynolds,**
Mr. Roland Katona, Mr. D. Smyth.

Instructions: Answer **Q1** (mandatory) and any **two** questions from the other three.
Q1 is worth 40 marks. All other questions are worth 30 marks each.

Duration: 2 hours

Sitting: Winter 2017

Requirements for this examination:

Note to Candidates: Please check the Programme Title and the Module Title to ensure that you are attempting the correct exaination. If in doubt please contact an Invigilator.

Q1.

   (a) Explain, using examples, what is a virus, a worm, a botnet, and a rootkit.

        (8 marks)

   (b) What is Social Engineering? List four Social engineering techniques.

        (7 marks)

   (c) Illustrate and explain the generation of a digital signature.   *(6 marks)*

   (d) List five steps you could take to protect a home wireless network. *(5 marks)*

   (e) Illustrate or explain the encryption process in PGP.   *(6 marks)*

   (f) List eight ways to secure an Android mobile phone.   *(8 marks)*

Q2.

   (a) Explain with the aid of an example or a diagram the anatomy of a Cross-Site scripting (XSS) attack?   *(8 marks)*

   (b) What is Sandboxing? Where is it used?   *(5 marks)*

   (c) List five steps you can take to protect PC against worm or virus infections.

        (5 marks)

   (d) List five steps you can take to protect against social engineering.   *(5 marks)*

   (e) What is a firewall? Distinguish between the three modes of operation of a firewall.   *(7 marks)*

Q3.

(a) List five common web browsers. Explain the purpose of each of the following browser security add-ons:
1) Web of Trust
2) AdBlock Plus
3) Ghostery
4) Better Privacy   *(8 marks)*

(b) Explain Biometric authentication.   *(5 marks)*

(c) Explain the potential paths for information flow and leakage from a PC.
                                                                        (6 marks)

(d) Describe the difference between wireless security protocols WEP, WPA and WPA2. Which of these protocols should never be used on a wireless networks and why?   *(5 marks)*

(e) Briefly explain the difference between signature and heuristic analysis for Anti-Virus software.   *(6 marks)*

Q4.

(a) Explain the difference between multi-class and multi-factor authentication.
                                                                        (5 marks)

(b) List and describe five safe browsing practices that should be adopted.
                                                                        (5 marks)

(c) Explain with the aid of an illustration Cross-Site tracking.   *(7 marks)*

(d) What is the difference between a polymorphic and metamorphic worm?
                                                                        (5 marks)

(e) Comment with the aid of examples on the following statement "The human has become the weak link in Computer Security ".   *(8 marks)*