The University of Nottingham

SCHOOL OF COMPUTER SCIENCE

A LEVEL 3 MODULE, AUTUMN SEMESTER 2008-2009

COMPUTER SECURITY

Time allowed ONE AND A HALF hours
Answer Question ONE (compulsory) and TWO OTHER questions

Candidates must NOT start writing their answers until told to do so

Answer Question ONE (compulsory) and TWO other questions

Marks available for sections of questions are shown in brackets in the right-hand margin

Only silent, self-contained calculators with a single-line display are permitted in this examination.

Dictionaries are not allowed with one exception. Those whose first language is not English may use a dictionary to translate between that language and English provided that neither language is the subject of this examination.

No electronic devices capable of storing and retrieving text, including electronic dictionaries, may be used.

DO NOT turn your examination paper over until instructed to do so

1. Question One – COMPULSORY (20 marks)

a) Describe and compare at least 3 different Authentication mechanisms.

(5)

b) Describe the difference between Authentication and Identification.

(3)

c) What is the difference between a subject and an object in access control?

(2)

d) Why software piracy was not an issue before personal computers appeared?

(3)

e) In hardware security how can EM be used to launch attack against devices?

(3)

f) Explain how firewall can improve network security and what their main limitations are.

(4)

2. Question Two (20 marks)

a) "*Our system is 100% secure.*" Discuss this statement.

(3)

b) In GMS networks what is TSMI, and what can it be used for?

(2)

c) What is an "*one-way*" function and how is it used in access control? Give an example.

(3)

d) What security mechanisms and vulnerabilities does Bluetooth have?

(2)

e) What security protocols exist for WiFi? Describe and compare them briefly.

(4)

f) What is the difference between invasive, semi-invasive, and non-invasive attacks and how do they differ? Give examples.

(6)

3. Question Three (20 marks)

a) Describe and compare at least three different Authentication mechanisms.

(3)

b) Describe the difference between *Unlinkability* and *Anonymity*.

(2)

c) Explain what "*TOCTTOU*" stands for and describe using an example.

(3)

d) Define "Trusted Computing Base", naming all its components.

(3)

e) Describe the issues with audio piracy and protection mechanisms against it

(5)

f) What is an Access Control List (ACL), where is it used and what are its disadvantages?

(4)

4. Question Four (20 marks)

a) Describe or represent diagrammatically the relationship between a subject and an object in access control including their function.

(4)

b) *Confidentiality*, *Integrity* and *Availability* are the three classical definitions of computer security. Define two additional properties that some argue should also be included in the definition of computer security.

(2)

c) What is vulnerability? Give an example.

(2)

d) What is a "*Man-in-the-middle*" attack? Give an example.

(4)

e) Describe the difference between active and passive network attacks and give examples.

(5)

(f) Describe the two major security mechanisms that *IP Security* is based on.

(3)

END OF EXAM