The University of Nottingham

SCHOOL OF COMPUTER SCIENCE

A LEVEL 3 MODULE, AUTUMN SEMESTER 2009-2010

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) What are the main limitations of GSM from security perspective?

(3)

c) What does "layer below attack" refer to? Give one example.

(5)

d) What is "tampering"? Describe four major tampering mechanisms?

(4)

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

(3)

f) How does Mobile IPv6 advance GSM and UTMS? Can firewalls be deployed on host computers? Give example of a firewall that is used in the internal network? Give an example of a firewall that is used in the external network?

(4)

2. Question Two (20 marks)

a) With the help of a diagram, explain "Chip and PIN relay" attack?

(5)

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 are the four types of threat vectors? Describe them and give examples for each type.

(*6)*

3. Question Three (20 marks)

a) Describe what "hardware security modules" are and give examples of how they can be used.

(3)

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

(2)

c) What are intrusion detection systems? Compare host based and network based intrusion detection systems.

(3)

d) Describe and compare "accountability" and "nonrepudiation"?

(4)

e) What is "denial of service attack"? Give an example?

(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) Describe the security problems associated with RFID?

(2)

c) What is vulnerability? Give an example.

(2)

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

(4)

e) With the aid of a diagram, describe TCP SYN flooding attack.

(5)

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

(3)

END OF EXAM