Office Use Only

MONASH University

Semester One 2018
Examination Period

Faculty of Information Technology

EXAM CODES:	**FIT3173**
TITLE OF PAPER:	**SOFTWARE SECURITY**
EXAM DURATION:	2 hours writing time
READING TIME:	10 minutes

THIS PAPER IS FOR STUDENTS STUDYING AT: (tick where applicable)

□ Caulfield □ Clayton □ Parkville □ Peninsula
□ Monash Extension □ Off Campus Learning □ Malaysia □ Sth Africa
□ Other (specify)

During an exam, you must not have in your possession any item/material that has not been authorised for your exam. This includes books, notes, paper, electronic device/s, mobile phone, smart watch/device, calculator, pencil case, or writing on any part of your body. Any authorised items are listed below. Items/materials on your desk, chair, in your clothing or otherwise on your person will be deemed to be in your possession.

No examination materials are to be removed from the room. This includes retaining, copying, memorising or noting down content of exam material for personal use or to share with any other person by any means following your exam.
Failure to comply with the above instructions, or attempting to cheat or cheating in an exam is a discipline offence under Part 7 of the Monash University (Council) Regulations.

<u>AUTHORISED MATERIALS</u>

OPEN BOOK	□ **YES**	✓ **NO**
CALCULATORS	□ **YES**	✓ **NO**
SPECIFICALLY PERMITTED ITEMS **if yes, items permitted are:**	□ **YES**	✓ **NO**

Candidates must complete this section if required to write answers within this paper

STUDENT ID: __ __ __ __ __ __ __ __ DESK NUMBER: __ __ __ __ __

Note: This is just a sample paper showing the structure of the final exam. The final exam will have different questions. Besides, there will be nine questions in total in the final exam. The students are expected to answer all of them.

Q1) What you mean by software security? Why or why not the principles of information security can be applied for software security?

(3 + 3 = 6 marks)

Sample answer:

Software security implies: SAFTEY, DEPENDABILITY, RELIABILITY (3 marks)

Security features are applicable to information objects that are stored in computer systems. Hence availability, confidentiality, integrity and repudiation need to be satisfied. They are different from that of the software security properties. Hence, Security features ≠ Secure features (of software). (3 marks)

Q2) Explain the purpose of the following three best practices in developing secure software: penetration testing, threat modelling, code review. For each, give an example of a threat or vulnerability that can be discovered by using this practice, and briefly describe the process that can be used to discover it. Explain in which order these three best practices should be used in the software development lifecycle.

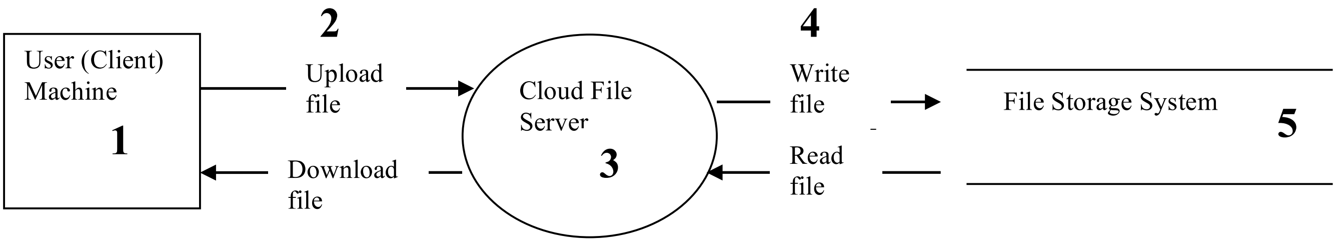
(4 + 4 + 4 = 12 marks)

Sample answer:

- Code Review: (4 marks)
    - Purpose: **Find implementation level vulnerabilities ("bugs" in code)**
    - Example vulnerability: buffer overflow in a copy operation
    - Process for discovery: Find a place in the code (wither manually or with a code review tool) where source length can exceed destination length but they have not been checked/validated in the code.
- Threat modelling: (4 marks)
    - Purpose: **Find design level threats or vulnerabilities ("flaws")**
    - Example threat: undetected manipulation of database contents
    - Process for discovery: perform threat modelling: decompose application into components, observe tempering threat on database component
- Penetration testing: (4 marks)
    - Purpose: **Test implemented system in its use environment**
    - Example vulnerability: malicious SQL code can be injected into SQL server via a web page user data entry field
    - Process for discovery: Test system response to malicious user input: insert SQL control characters and commands in each user input field and observe response

Q3) Consider the following data flow diagram for a personal cloud file storage system such as `Google Drive'. Select one of the five labelled elements in this diagram, and for the selected element consider one threat to the user's security. For the threat, write: (1) The threat target, (2) The threat category in terms of the STRIDE categories, (3) A brief description of the threat and the assumed identity/capability of the attacker, and (4) Proposed mitigation techniques for the threat.

(4 x 2 = 8 marks)



Sample solution:

User client Threat: Spoofing the client
(1) Target: Client machine (1) (2 marks)
(2) STRIDE category: S (2 marks)
(3) Attacker user Bob impersonates honest user Alice to the cloud file server to access Alice’s files. Attacker can observe data transferred from Alice’s client to cloud server, and manipulate authentication data sent to the server. (2 marks)
(4) Mitigation: Use strong authentication protocols like TLS/SSL and encrypt the communication between client and server. As long as attacker does not have access to client’s private keys and Alice’s password, he/she cannot impersonate Alice. (2 marks)

Q4) Consider the following C code that plans to perform copy operation. Review the code, and identify the vulnerability in it. Explain where it occurs in the code (and any assumptions you are making), how it could be exploited, and suggest a good practice for preventing it.

```
1   int copy_something(char *buf, int len){
2   char kbuf[800];
3   if(len > sizeof(kbuf)){
4       return -1;
5   }
6
7   memcpy(kbuf, buf, len);
8   return 1;
}
```

(4 marks)

Sample Solution:

Line 3: integer overflow, len could be negative number so that the check could be bypassed. Define len as unsigned int.

--- End of the Examination Paper ---