Xi'anJiaotong-LiverpoolUniversity

西交利物浦大学

PAPER CODE	EXAMINER	DEPARTMENT	TEL
CSE108		Computer Science and Software Engineering	

2nd SEMESTER 2015/16 REGULAR EXAMINATIONS

BACHELOR DEGREE – Year 2

Operating Systems Concepts

TIME ALLOWED: 2 Hours

INSTRUCTIONS TO CANDIDATES

1、 Total marks available are 100.

2、 Answer all questions.

3、 The number in the column on the right indicates the marks for each question.

4、 Answershould be written in the answer booklet(s) provided.

5、 The university approved calculator - Casio FS82ES/83ES can be used.

6、 All the answers must be in English.

1. Explain the following terms:

1.1 Process state (also list the states). (10 marks)

1.2 Network-attached storage. (10 marks)

1.3 Principle of least privilege. (10 marks)

2. Assume in a system, there are:

- 3 processes P1 to P3;
- 3 resource types: A (9 instances), B (5 instances), and C (5 instances).

Below is a snapshot at time T:

	Allocation			Max		
	A	B	C	A	B	C
P1	0	1	1	6	5	3
P2	3	4	1	3	4	2
P3	3	0	2	9	0	2

2.1 Show that the system is in a safe state at time T. (10 marks)

2.2 Can request for (A: 2, B: 0, C: 0) by P1 be granted? Explain your answer. (10 marks)

3. Consider the following page reference string: 7, 0, 3, 1, 3, 5, 3, 4, 6, 5. Assuming demand paging with three frames, how many page faults would occur for the following replacement algorithms?

3.1 FIFO replacement. (10 marks)

3.2 LRU replacement. (10 marks)

4. A secure boot scheme adds cryptographic checks to each stage of the boot process. This process aims to assert the integrity of all software images that are executed, preventing any unauthorized or maliciously modified software from running. The most logical cryptographic protocol to apply is one based on a public-key signature algorithm. Design a public-key signature algorithm-based protocol to realize the secure boot scheme. Your answer should specify the usage of public and private keys; also, your answer should evaluate the following public key storing methods: (1) embed the public key in the ROM, (2) store the public key in One-Time-Programmable (OTP) hardware, and (3) store a hash of the public key. (30 marks)

END OF EXAM PAPER