THE UNIVERSITY OF AUCKLAND

SECOND SEMESTER, 2007
Campus: City

COMPUTER SCIENCE
Software Security
(Time allowed: TWO hours)

NOTE: Attempt **ALL** questions in the 12-page script book provided, using approximately **25** words to answer each 5-mark question, **50** words to answer each 10-mark question, and approximately **75** words to answer each 15-mark question. Total possible: **100 marks.**

This is an ungraded sample exam, which should take you about 25 minutes to complete.

A. The following questions refer to the CPRM system shown in Figure 4 of Myles *et al.*, "Content Protection for Games", *IBM Sys. J. 41:1*, pp. 119-143, 2006. This figure is reproduced below.

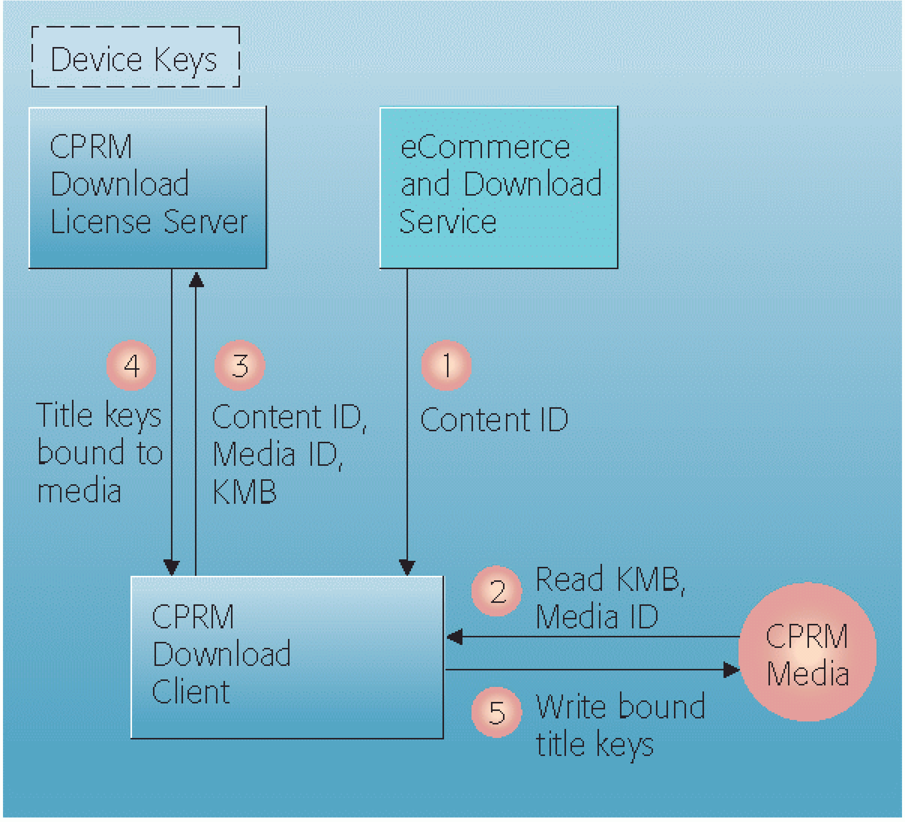
Device Keys
CPRM Download License Server
eCommerce and Download Service
4
Title keys bound to media
3
Content ID, Media ID, KMB
1
Content ID
CPRM Download Client
2
Read KMB, Media ID
CPRM Media
5
Write bound title keys

Figure 4
CPRM for network download

1. Redraw this system diagram, so that it shows an end-user, an attacker, and an author. To obtain full credit, your diagram must clearly show the following

i) the end-user attempting to make an authorised read access (6) to the CPRM-protected media,

ii) the attacker attempting to make an unauthorised read access (7) to this media,

iii) how the author is able to write their intended media content to this protection system. (The arc or arcs for these pre-publication steps should be assigned small numbers, e.g. 0, -1 etc. so that the time-sequence of your diagram is as clear as possible.)

iv) the “trust boundary” in the system, separating the trusted components (and people) from the untrusted components and people, and

v) the valuable item, information, or service which is being protected by this security system. (This should be labelled as “$$”.)

Your diagram must be accompanied by a brief explanation of each arc you have added to the original figure 4. **(15 marks)**

2. Butler Lampson, in his article “Computer Security in the Real World”, identifies four goals of security: Secrecy, Integrity, Availability, and Accountability. He identifies three basic mechanisms for implementing security: Authentication, Authorisation, and Auditing. His five defensive strategies are isolate, exclude, restrict, recover, and punish. Using Lampson’s terminology, identify and briefly describe the most important security goal, mechanism, and defensive strategy of the CPRM system shown in Figure 4. **(10 marks)**

C. (Other questions…). **[75 marks]**