COMPUTER SCIENCE TRIPOS Part II – 2012 – Paper 8

12 Security II (FMS)

The lifecycle of an exam question in a fictitious university includes at least the following stages, which take place over several months:

1. Professor invents question.
2. Chief examiner sanity-checks it.
3. Professor amends it if necessary.
4. External auditor sanity-checks it.
5. Professor amends it again if necessary.
6. Chief examiner approves final version.
7. Clerk prints question in required number of copies.

Following a scandal whereby some dishonest candidates got hold of questions ahead of time, thus forcing the whole exam to be invalidated and repeated to the dismay of the honest participants, the university has put pressure on its departments to ensure this will not happen again.

(a) The Head of Department A, where the leak occurred, is now paranoid about computer networks and insists that no exam question shall ever reside on any networked computer system until after the corresponding exam takes place.

(i) Describe four ways that a determined undergraduate might nonetheless get hold of exam questions before the exam even if that requirement were observed. [4 marks]

(ii) Describe a security policy suitable for department A, taking into account the head-of-department's requirements and the staff workflow. Discuss it thoroughly, including requirements analysis, incentives and technical mechanisms. [4 marks]

(b) The Head of Department B finds that A's requirement would impose an excessive penalty on the productivity of her staff. At the same time, she certainly does not want to be blamed for the next leak.

(i) Describe a security policy suitable for department B, taking into account the head-of-department's requirements and the staff workflow. Discuss it thoroughly, including requirements analysis, incentives and technical mechanisms. [6 marks]

(ii) Describe three trade-offs between security and usability that you considered in devising the policy in (b)(i) and justify the choices you made.

[6 marks]