1 Security Models (2011 Paper 8 Question 11)

You are consulting for a large online service company which stores personal information on millions of users. Your clients are alarmed by the Wikileaks saga and are concerned about damage to their company’s reputation should a disaffected member of staff steal and publish personal information on a large number of customers.

Discuss the security policy options available to your client to minimise the damage that a member of staff could do.

2 Security Models (2012 Paper 8 Question 12)

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

a. Professor invents question.
b. Chief examiner sanity-checks it.
c. Professor amends it if necessary.
d. External auditor sanity-checks it.
e. Professor amends it again if necessary.
f. Chief examiner approves final version.
g. 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.
(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.

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.

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

3 De-anonymising Alice

Describe how you would de-anonymise Alice in the second last page of Dr Steven Murdoch’s Anonymity & Censorship lecture? Can you improve it with more time or other resources?

4 Anonymous Communications (2009 Paper 8 Question 11)

a. Give four uses of anonymous communication other than censorship resistance.

b. Explain the role of privacy in anonymous communications. What limits or costs does low latency impose?

c. Imagine you are a government censor, trying to identify which of your citizens are viewing forbidden websites through Tor. (i) If you are able to wiretap the Internet connections of any 1% of the population, what effective capability does this give against Tor users? (ii) If there are currently 1000 active Tor nodes, what extra capability would you acquire if you added a further 100 nodes under your control? Explain any assumptions you make.

d. If you are using Tor to escape censorship, how often should you change the circuit path you use? Explain your answer.

5 Anonymous Communication-Proxy

Consider two designs for an anonymizing proxy which seeks to avoid timing analysis of individual packets

- **Stop and Go** The proxy will wait until it receives $k$ packets, then send the $k$ packets out in a random order.
• **Pooling** The proxy will keep a pool of between $k$ and $2k$ packets at all times. When the pool gets to size $2k$, it will randomly select $k$ packets to send from its pool, then wait for $k$ more packets to arrive.

We will compare the properties of these two designs.

a. What are the performance implications of the two designs? How does their throughput compare? How does their latency, specifically how much longer do we expect a packet to wait in a Pooling proxy compared to a Stop and Go proxy?

b. How large is the anonymity set for each packet sent out from a Stop and Go proxy? How large is it for a Pooling proxy?

c. Is the absolute size of the anonymity set a “fair” comparison between the two designs? What might be a better way to compare the anonymity provided by the Pooling proxy?