CPSC 457/557 // Exam 2 // December 5, 2013

Answer all of the questions. Please remember to write your name, the course number, and today's date on all blue books that you submit.

You need not justify your answers to True-False questions **unless you are explicitly instructed to do so**.

This is a closed-book exam; please do not refer to any books or notes, and please do not talk to any of the other students.

Question 1 (12 points):

a) (6 points) What are *hidden services* in Tor? Give an example of a scenario in which hidden services are useful.

b) (6 points) Briefly explain one way in which website or network operators can block Tor traffic.

Question 2 (24 points):

a) (12 points) Recall that GMail uses both the *internal data* and the *external data* of an email message to decide which ads to display. For two points each, give three examples of internal data and three examples of external data.

b) (4 points) Define the term *personal information* as it is used in Google Privacy Policy.

c) (2 points) True or False: Google shares personal information about all of its users with other companies.

d) (6 points) What is *wardriving*, and why is it a good example of the inherent difficulties that Google faces in its role as a steward of sensitive information?

Question 3 (10 points):

Recall that the *subject* field of an X.509 certificate contains a *distinguished name* (DN) of the owner of that certificate, *i.e.*, the person or organization to which the certificate was issued.

a) (3 points) True or False: A DN can occur in the subject field of at most one certificate. Briefly justify your answer.

b) (3 points) True or False: If a person has multiple certificates, the same DN must appear in the subject field of all of them. Briefly justify your answer.

c) (2 points) True or False: If I succeed in obtaining an X.509 certificate with PK in its public-key field, then the CA that issued the certificate has implicitly claimed that there is a secret key SK that corresponds properly to PK (with respect to the public-key system that appears in the *Signature Algorithm* field of the certificate).

d) (2 points) True or False: If I succeed in obtaining an X.509 certificate with "Joan Feigenbaum" in the subject field, then the CA that issued that certificate must have verified that I am in fact Joan Feigenbaum.

Question 4 (20 points):

a) (9 points) For 3 points each, give three characteristics that are common to developing-world environments in which M-payment systems have flourished.

b) (5 points) As discussed in class and in assigned readings, M-payment systems are plagued by breakable encryption. Briefly explain one reason that it is difficult to upgrade the encryption in these systems.
c) (6 points) Briefly explain why Universal Software Radio Peripherals (USRPs) pose a threat to the security of M-payment systems.

Question 5 (14 points):
a) (6 points) Briefly explain what a *Deep Packet Inspection (DPI) engine* is and how it differs from a firewall.
b) (8 points) For two points each, give two uses of DPI that are clearly potentially beneficial and two that are controversial.

Question 6 (8 points):
What does Schneier mean by the term *feudal internet*?

Question 7 (12 points):
For 3 points each, answer True or False for each of parts a) through d).

a) Information goods are typically priced in proportion to their marginal cost.

b) E-bay's feedback mechanisms have more impact on high-value transactions than on low-value transactions.

c) Pinterest has taken more care than most website operators to make its privacy policy understandable.

d) Journalist "shield laws" currently apply to citizen journalists.