CPSC 156 Exam
April 26, 2007

Answer all parts of all six questions. Each question is worth 16 points, for a total of 96; everyone gets 4 points for free. You do not have to justify your answers to True/False questions.

Please remember to write your name, CPSC 156, and today's date on the covers of all blue books you submit.

Question 1 (Open Source):

(a) (8 points) The *Free Software Foundation* defines "free software" in terms of "the four freedoms" that all users must have. For two points each, what are these four freedoms?

(b) (4 points) What is the *copyleft* principle that is exemplified by the GNU Public License?

(c) (4 points) For two points each, give two ways in which a company can make money distributing open-source software.

Question 2 (Cryptographic Primitives):

(a) (5 points) In the context of public-key encryption and public-key digital signatures, what are *certified keys*, and what problem do they solve?

(b) (5 points) Recall that one user's signatures on two different digital documents will be different; in this way, digital signatures are fundamentally different from paper signatures. Why is this property of digital-signature schemes necessary for their security?

(c) (6 points) As observed by Marx, Solove, and others, computers and networks have led to a proliferation of databases that contain sensitive information about people and to great social, political, and economic concern about potential misuse of these databases. Why doesn't encryption solve this problem? That is, why is it insufficient simply to require database owners to store all sensitive information in encrypted form?

Question 3 (Spam and viruses):

(a) (6 points) What is a CAPTCHA, and how are CAPTCHAs *currently* used to combat spam?

(b) (6 points) How are digital signatures currently used to combat virus propagation?

(c) (2 points) True or False: A WORD document cannot contain a virus.

(d) (2 points) True or False: A user can infect his computer with a virus simply by viewing a webpage.

Question 4 (Public Records and Marx's Identity-Knowledge Taxonomy):

(a) (6 points) What is the definition of "public records," and why is the migration of these records to public webpages socially disruptive?

(b) (6 points) What does Marx mean by "identification by certification of possession of knowledge, artifacts, or skills," and why is this form of identification relevant to Internet-based human interaction?

(c) (4 points) Suppose that Alice generates a public-key, secret-key pair (pk_A, sk_A), successfully identifies herself to certifying authority CA, and then publishes her certified public key under the pseudonym RanchHand (after telling the CA that this is what she plans to do). That is, her certificate is (RanchHand, pk_A, Sign((RanchHand, pk_A), gk_{CA})), where gk_{CA} is the signing key of the certifying authority. In Marx's taxonomy, what type of identity knowledge does this certificate exemplify? (You need not justify your answer; just give the type.)

Question 5 (Solove's Privacy Taxonomy):

(a) (6 points) What does Solove mean by the "secrecy paradigm," and why is its relevance to privacy norms increasing as computers and networks become more prevalent in daily life?

(b) (6 points) What does Solove mean by "increased accessibility," and why is this type of privacy violation relevant to Internet access to public records?

(c) (4 points) In Solove's taxonomy, what type of privacy violation does spam exemplify? (You need not justify your answer; just give the type.)

Question 6 (Browser-based Security and Privacy Tools):

(a) (6 points) What is the "same-origin principle"?

(b) (5 points) The PwdHash browser plug-in creates site-specific passwords by computing the expression $HMAC_{pwd}$(domain-name), where "domain-name" is the specific site for which a password is needed and "pwd" is the user's master password. What type of cryptographic primitive is the function HMAC?

(c) (3 points) Give one indication visible in the browser window that the webpage currently being viewed is a spoof.

(d) (2 points) Give one reason that, despite the indication you gave in part (c), spoofed websites still succeed in fooling users.