Name:_____

CS 600.443 Final Exam

This exam is closed book and closed notes. **You are required to do this completely on your own without any help from anybody else.** Feel free to write on the back of any page to continue an answer, and indicate (over) when doing so.

Short answer. (use the back if necessary) (4 points each)

1. Give 3 advantages of IPsec over SSL. Give one advantage of SSL over ISsec.

2. Explain what Nessus is. Describe a defense mechanism against such tools.

3. Today's commercial web browsers often have over 100 root certificates in them. Does that increase or decrease security? (pick one, no hedging) Justify your answer.

4. ECB and CBC are both modes of operation of block ciphers that allow for random access decryption in long ciphertexts. Explain how and why this works for each of ECB and CBC. Why does random access decryption not work for OFB mode?

5. Given a network of n mixes, how many of the mixes (in terms of n) must collaborate to compromise the linkability between sender and receiver in synchronous communications? Justify your answer. Why does the attack not work in asynchornous communication?

6. According to Dr. Gary McGraw, most security problems in software are caused by what 2 things? What is the ratio of the two things to each other?

7. Does having a patent on an encryption algorithm give you the right to develop and sell a software product that utilizes that algorithm? Explain your answer.

8. Explain why the Rob Harris case is relevant to the discussion of electronic voting. What threat does it exemplify?

9. Describe the primary flaw in the Needham and Schroeder protocol and how to fix it.

10. Alice and Bob wish to share a symmetric key. One way to do this is for them to run Diffie Hellman. Another way, if they already have each others' public RSA keys, is simply for them to use public key encryption to exchange a key. Compare and contrast these two approaches. Which one is more secure? Is there a way to make the RSA scheme more secure than the naive approach of just having Alice encrypt a random key with Bob's public key and sign it? If so, give a protocol for that. (8 points)