CSSE 442: Computer Security **Homework 4** Due: January 12, 2016

Winter 2015-2016 SCORE: / 50

Name:

Start on this assignment early, it may take a while.

Write your answers on separate pieces of paper (handwritten or typed), staple to a printed copy of this page, and submit it in class. *The SSL video is the same one assigned earlier in class. It is about 50 minutes long, so budget for at least that amount of time for the SSL and PKI questions.*

SSL and PKI: Watch Moxie Marlinspike's talk on SSL (https://www.youtube.com/watch?v=Z7Wl2FW2TcA) and answer the following questions:

1. (3pts) What is the name of the tool Moxie created to perform man-in-the-middle attacks on SSL connections?
2. (5pts) Explain how the tool in problem 1 works.
   You may need to find additional information not available in the video to answer this.
3. (5pts) How can you modify or configure a web site to prevent Moxie's tool (problem 1) from working on that site?
4. (6pts) What are the two properties of **Trust Agility**?
5. (5pts) Describe one limitation of Moxie's proposed "Convergence" system.

PASSWORD Exercises:

6. (15pts) Install John the Ripper (jumbo free version 1.8 or later) and crack the password to the PDF linked from the course schedule page using "pdf2john" and "john" (or similar programs). **The answer to this question is in the PDF (requires password to read it). Decrypt that PDF and follow the instructions it contains.**

   > You can get John for windows here:
   > http://openwall.info/wiki/john/custom-builds#Compiled-for-Windows
   > The pre-compiled "2john" executables are more reliable than the python scripts.
   >
   > *(Note: you'll need John later in this class, so keep it installed!)*

(continues on next page)

7. (2pts) Was the “john” activity an Online or an Offline dictionary attack?

8. (3pts) Was the “john” activity a breach of attack on Confidentiality, Integrity, or Availability? Justify your answer.

9. (6pts) Describe ***two*** techniques the owner of that encrypted PDF could use to make it significantly more difficult to attack.