**CSE 484 In-class Worksheet #0xAAAAARGH (Fall 2016)**

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ UWNetID: \_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Email address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Student ID #: \_\_\_\_\_\_\_\_\_\_\_

Partner names for this activity: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Q1.** What problems might arise due to the fact that the initial handshake in SSL is not encrypted? Imagine you’re a person-in-the-middle (say, a router).

**Q2.** How could SSL/TLS deal with the danger of a version rollback? How can a server and client ensure that they actually agreed upon the highest version of the protocol they support?

**Q3.** What makes web security different from software security? What similarities do they have?