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

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

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

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

**Q1.** Why is this strawman certificate authority design a bad idea?

**Q2.** Assuming you pwn a CA and make yourself a fake cert for a major website (say, mail.yahoo.com), how can you use it to fool users and steal their data? Think about a man-in-the-middle attack. Who is in a position to execute such an attack?

**Q3.** Revocation refers to making clients aware of the fact that they should no longer trust a particular certificate or key. What are some circumstances in which revocation might be necessary?