**CSE 484 In-class Worksheet #2**

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

Email address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Student Number: \_\_\_\_\_\_\_\_\_\_\_\_

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

Q1: Defense in depth can help alleviate the asymmetry of security. Name an instance where you’ve seen defense in depth used OR an instance where it wasn’t used but might have helped.

Paperless electronic voting machines are designed to allow voters to vote without needing to use paper, which some argue is more cost effective and also easier and less error-prone than previous paper-based methods.

Q2: What potential security problems do you see with electronic voting systems? What are the security goals for an electronic voting system? What **assets** must be protected? Who are the **adversaries** who might try to attack an electronic voting system? What resources / capabilities / level of access / goals might the attacker have?

Q3: Now we’ve discussed the specific design of a particular electronic voting machine. Does knowing the particulars of the system make you think of any new, **assets**, **adversaries, or threats?** Does it make you think of goals that the adversary might have, which you didn’t think of before?