COMP435 In-Class Practice 9/29/25 Name: _____

Question 1: Trusted Computing Base It is better for the TCB to be big, encompassing most of the system, or small, encompassing very little of the system. Explain your answer.

Question 2: Honest, but Curious Adversaries It is instructive to consider an "honest, but curious" threat model because...

- ◯ It has the most powerful threat model.
- ◯ It can reveal information leaks in protocols.
- ◯ It is part of the trusted computing base.
- ◯ It is impossible to be honest and incurious.

Question 3: Race Conditions Suggest a fix to this race condition vulnerability.