Homework #3

Due: May 11, 2026 **Points:** 100

Questions

1. (*20 points*) Consider the KeyNote example for the company's invoicing system. The assertion requires 2 signatures on any invoice under $10,000. If the invoice is under $500, the chief financial officer believes this is unnecessary; one signature should suffice. Write a KeyNote assertion that says only one signature is needed if the amount of the invoice is under $500. For your assertion, the evaluator is to return _MAX_TRUST.

2. (*20 points*) Consider countermeasures for the SYN flood attack that are present on intermediate systems and are designed to allow only legitimate handshakes reach the destination system (see Section 7.4.2). Is the focus of this type of countermeasure the waiting time policy, the user agreements, or both? Why?

3. (*20 points*) Consider the systems Louie and Dewey in Section 9.2.4.

   (a) Suppose the sends and receives for the buffers are non-blocking. Is the composition of Hughie, Dewey, and Louie still noninterference-secure? Justify your answer.

   (b) Suppose all buffers are unbounded. Is the composition of Hughie, Dewey, and Louie still noninterference-secure? Justify your answer.

4. (*20 points*) A company develops a new security product using the agile programming software development methodology. Programmers code, then test, then add more code, then test, and continue this iteration. Every day, they test the code base as a whole. The programmers work in pairs when writing code to ensure that at least two people review the code. The company does not adduce any additional evidence of assurance. How would you explain to the management of this company why their software is in fact not "high assurance" software?

5. (*20 points*) Prove that for $n = 2$, $H(X)$ is maximal when $p_1 = p_2 = \frac{1}{2}$.

Extra Credit

Remember that extra credit scores are *not* added to your homework score. They are recorded separately and used to determine whether to boost your grade if the score is on a borderline.

1. (*40 points*) Prove that the system resulting from the composition of two restrictive systems is itself restrictive.