Homework 3

Due: February 22, 2019 **Points:** 100

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.

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*) A publisher wishes to implement a DRM scheme for its digital books. Please explain why enciphering the contents of the books, and then distributing the appropriate cryptographic keys, is insufficient to provide a digital rights management scheme.

4. (*20 points*) The Rumpole policy requires the user to resubmit a request for break-the-glass access if the policy decision point returns a new set of obligations that the subject must accept. Why does the policy decision point simply check the obligations and, if they are a subset of the obligations in the request, grant the request?

5. (*20 points*) The system *plugh* has users Skyler, Matt, and David. Skyler cannot access David's files, and neither Skyler nor David can access Matt's files. The system *xyzzy* has users Holly, Sage, and Heidi. Sage cannot access either Holly's or Heidi's files. The composition policy says that Matt and Holly can access one another's files, and Skyler can access Sage's files. Apply the Principles of Autonomy and Security to determine who can read whose fles in the composition of *xyzzy* and *plugh*.