Homework 1

Due: October 6, 2021 **Points:** 100

1. (*20 points*) In addition to mathematical and informal statements of policy, policies can be implicit (not stated). Why might this be done? Might it occur with informally stated policies? What problems can this cause?

2. (*20 points*) The PostScript language describes page layout for printers. Among its features is the ability to request that the interpreter execute commands on the host system.

   (a) Describe a danger that this feature presents when the language interpreter is running with administrative or root privileges.

   (b) Explain how the principle of least privilege could be used to ameliorate this danger.

3. (*20 points*) Definition 19–2 defines assurance in terms of "confidence." A vendor advertises that its system was connected to the Internet for three months, and no one was able to break into it. It claims that this means that the system cannot be broken into from any network.

   (a) Do you share the vendor's confidence? Why or why not?

   (b) If a commercial evaluation service had monitored the testing of this system and confirmed that, despite numerous attempts, no attacker had succeeded in breaking into it, would your confidence in the vendor's claim be increased, decreased, or left unchanged? Justify your answer.

4. (*20 points*) Given the security levels TOP SECRET, SECRET, CONFIDENTIAL, and UNCLASSIFIED (ordered from highest to lowest), and the categories A, B, and C, specify what type of access (read, write, both, or neither) is allowed in each of the following situations. Assume that discretionary access controls allow anyone access unless otherwise specified.

   (a) Paul, cleared for (TOP SECRET, { A, C }), wants to access a document classified (SECRET, { B, C }).

   (b) Anna, cleared for (CONFIDENTIAL, { C }), wants to access a document classified (CONFIDENTIAL, { B }).

   (c) Jesse, cleared for (SECRET, { C }), wants to access a document classified (CONFIDENTIAL, { C }).

   (d) Sammi, cleared for (TOP SECRET, { A, C }), wants to access a document classified (CONFIDENTIAL, { A }).

   (e) Robin, who has no clearances (and so works at the UNCLASSIFIED level), wants to access a document classified (CONFIDENTIAL, { B }).

5. (*20 points*) The relations *certified* (see ER1) and *allowed* (see ER2) can be collapsed into a single relation. Please do so and state the new relation. Why doesn't the Clark-Wilson model do this?

Extra credit

6. (*20 points*) A cryptographer once claimed that security mechanisms other than cryptography were unnecessary because cryptography could provide any desired level of confidentiality and integrity. Ignoring availability, either justify or refute the cryptographer's claim.