Homework #4

Due: May 29, 2026 **Points:** 100

Questions

1. (*25 points*) Revisit the example for $x := y + z$ in Section 16.1.1. Assume that x does not exist in state s. Confirm that information flows from y and z to x by computing $H(y_s|x_t)$, $H(y_s)$, $H(z_s|x_t)$, and $H(z_s)$ and showing that $H(y_s|x_t) < H(y_s)$ and $H(z_s|x_t) < H(z_s)$.

2. (*25 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.

   (a) Apply the Principle of Autonomy (all accesses that are not explicitly disallowed are allowed) to determine who can read whose files in the composition of *xyzzy* and *plugh*.

   (b) Apply the Principle of Security (only those accesses explicitly granted are allowed) to determine who can read whose files in the composition of *xyzzy* and *plugh*.

3. (*20 points*) Consider the rule of transitive confinement. Suppose a process needs to execute a subprocess in such a way that the child can access exactly two files, one only for reading and one only for writing.

   (a) Could capabilities be used to implement this? If so, how? If not, why not?

   (b) Could access control lists be used to implement this? If so, how? If not, why not?

4. (*30 points*) Section 18.3.2.3 derives a formula for $I(A;X)$. Prove that this formula is a maximum with respect to p when $p = \frac{M^{\frac{1}{m}}}{1+mM^{\frac{1}{m}}}$ (this is different than what is in the text).

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. (*20 points*) Let $L = (S_L, \leq_L)$ be a lattice. Define:

   (a) $S_{IL} = \{[a,b] \mid a,b \in S_L \wedge a \leq_L b\}$

   (b) $\leq_{IL} = \{([a_1,b_1],[a_2,b_2]) \mid a_1 \leq_L a_2 \wedge b_1 \leq_L b_2\}$

   (c) $lub_{IL}([a_1,b_1],[a_2,b_2]) = (lub_L(a_1,a_2), lub_L(b_1,b_2))$

   (d) $glb_{IL}([a_1,b_1],[a_2,b_2]) = (glb_L(a_1,a_2), glb_L(b_1,b_2))$

   Prove that the structure $IL = (S_{IL}, \leq_{IL})$ is a lattice.