

Homework 4

Due: March 8, 2019

Points: 100

1. (30 points) Revisit the example for $x := y + z$ in Section 17.1.1. 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. (20 points) Let $L = (S_L, \leq_L)$ be a lattice. Prove that the structure $IL = (S_{IL}, \leq_{IL})$ is a lattice, where:
 - (a) $S_{IL} = \{[a, b] \mid a, b \in S \wedge a \leq_L b\}$
 - (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) $\text{lub}_{IL}([a_1, b_1], [a_2, b_2]) = (\text{lub}_L(a_1, a_2), \text{lub}_L(b_1, b_2))$
 - (d) $\text{glb}_{IL}([a_1, b_1], [a_2, b_2]) = (\text{glb}_L(a_1, a_2), \text{glb}_L(b_1, b_2))$
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?
 - (b) Could access control lists be used to implement this? If so, how?
4. (30 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.