16.9. Exercises

1: Revisit the example for $\mathbf{x} := \mathbf{y} + \mathbf{z}$ in Section 16.1.1. Assume that $\mathbf{x}$ does not exist in state $\mathbf{s}$. Confirm that information flows from $\mathbf{y}$ and $\mathbf{z}$ to $\mathbf{x}$ by computing $\mathbf{H}(\mathbf{y_S} \mid \mathbf{x_t})$, $\mathbf{H}(\mathbf{y_S})$, $\mathbf{H}(\mathbf{z_S} \mid \mathbf{x_t})$, and $\mathbf{H}(\mathbf{z_S})$ and showing that $\mathbf{H}(\mathbf{y_S} \mid \mathbf{x_t}) < \mathbf{H}(\mathbf{y_S})$ and $\mathbf{H}(\mathbf{z_S} \mid \mathbf{x_t}) < \mathbf{H}(\mathbf{z_S})$.

2: Let $\mathbf{L} = (\mathbf{S_L}, \leq_\mathbf{L})$ be a lattice. Prove that the structure $\mathbf{IL} = (\mathbf{S_{IL}}, \leq_\mathbf{IL})$, where each of the following is a lattice.

a. $\mathbf{S_{IL}} = \{ [\mathbf{a}, \mathbf{b}] \mid \mathbf{a}, \mathbf{b} \in \mathbf{S_L} \wedge \mathbf{a} \leq_\mathbf{L} \mathbf{b} \}$

b. $\leq_\mathbf{IL} = \{ ([\mathbf{a}_1, \mathbf{b}_1], [\mathbf{a}_2, \mathbf{b}_2]) \mid \mathbf{a}_1 \leq_\mathbf{L} \mathbf{a}_2 \wedge \mathbf{b}_1 \leq_\mathbf{L} \mathbf{b}_2 \}$

c. $\mathbf{lub_{IL}}([\mathbf{a}_1, \mathbf{b}_1], [\mathbf{a}_2, \mathbf{b}_2]) = (\mathbf{lub_L}(\mathbf{a}_1, \mathbf{a}_2), \mathbf{lub_L}(\mathbf{b}_1, \mathbf{b}_2))$

d. $\mathbf{glb_{IL}}([\mathbf{a}_1, \mathbf{b}_1], [\mathbf{a}_2, \mathbf{b}_2]) = (\mathbf{glb_L}(\mathbf{a}_1, \mathbf{a}_2), \mathbf{glb_L}(\mathbf{b}_1, \mathbf{b}_2))$

3: Prove or disprove that the set **P** formed by the dual mapping of a reflexive information flow policy (as discussed in Definition 16–5) is a lattice. 不用

4: Extend the semantics of the information flow security mechanism in Section 16.3.1 for records (structures). 4

5: Why can we omit the requirement $\mathbf{lub}\{ \underline{\mathbf{i}}, \underline{\mathbf{b}}[\underline{\mathbf{i}}] \} \leq \underline{\mathbf{a}}[\underline{\mathbf{i}}]$ from the requirements for secure information flow in the example for iterative statements (see Section 16.3.2.4)?

6: In the flow certification requirement for the **goto** statement in Section 16.3.2.5, the set of blocks along an execution path from $\mathbf{b_i}$ to IFD($\mathbf{b_i}$) excludes these endpoints. Why are they excluded?

7: Prove that Fenton's Data Mark Machine described in Section 16.4.1 would detect the violation of policy in the execution time certification of the **copy** procedure. 不用

8: Discuss how the Security Pipeline Interface in Section 16.5.1 can prevent information flows that violate a confidentiality model. (**Hint:** Think of scanning messages for confidential data and sanitizing or blocking that data.)