

Username: Jeanne Chua **Book:** Computer Security: Art and Science. No part of any chapter or book may be reproduced or transmitted in any form by any means without the prior written permission for reprints and excerpts from the publisher of the book or chapter. Redistribution or other use that violates the fair use privilege under U.S. copyright laws (see 17 USC107) or that otherwise violates these Terms of Service is strictly prohibited. Violators will be prosecuted to the full extent of U.S. Federal and Massachusetts laws.

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 $\mathbf{H}(\mathbf{y}_{\mathbf{s}} \mid \mathbf{x}_{\mathbf{t}})$, $\mathbf{H}(\mathbf{y}_{\mathbf{s}})$, $\mathbf{H}(\mathbf{z}_{\mathbf{s}} \mid \mathbf{x}_{\mathbf{t}})$, and $\mathbf{H}(\mathbf{z}_{\mathbf{s}})$ and showing that $\mathbf{H}(\mathbf{y}_{\mathbf{s}} \mid \mathbf{x}_{\mathbf{t}}) < \mathbf{H}(\mathbf{y}_{\mathbf{s}})$ and $\mathbf{H}(\mathbf{z}_{\mathbf{s}} \mid \mathbf{x}_{\mathbf{t}}) < \mathbf{H}(\mathbf{z}_{\mathbf{s}})$.

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

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

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. $\text{lub}_{\mathbf{IL}}([\mathbf{a}_1, \mathbf{b}_1], [\mathbf{a}_2, \mathbf{b}_2]) = (\text{lub}_{\mathbf{L}}(\mathbf{a}_1, \mathbf{a}_2), \text{lub}_{\mathbf{L}}(\mathbf{b}_1, \mathbf{b}_2))$

d. $\text{glb}_{\mathbf{IL}}([\mathbf{a}_1, \mathbf{b}_1], [\mathbf{a}_2, \mathbf{b}_2]) = (\text{glb}_{\mathbf{L}}(\mathbf{a}_1, \mathbf{a}_2), \text{glb}_{\mathbf{L}}(\mathbf{b}_1, \mathbf{b}_2))$

3: Prove or disprove that the set \mathbf{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 $\text{lub}\{ \mathbf{i}, \mathbf{b}[\mathbf{i}] \} \leq \mathbf{a}[\mathbf{i}]$ 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 $\text{IFD}(\mathbf{b}_i)$ 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.)