

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.

2,

4.11. Exercises

1:In [Figure 4-1](#), suppose that edge t_3 went from s_1 to s_4 . Would the resulting system be secure?

2:Revisit the example of one student copying another student's homework assignment. Describe three other ways the first student could copy the second student's homework assignment, even assuming that the file access control mechanisms are set to deny him permission to read the file.

3:A noted computer security expert has said that without integrity, no system can provide confidentiality.

- a. Do you agree? Justify your answer.
- b. Can a system provide integrity without confidentiality? Again, justify your answer.

4: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.

5:Classify each of the following as an example of a mandatory, discretionary, or originator controlled policy, or a combination thereof. Justify your answers.

- a. The file access control mechanisms of the UNIX operating system
- b. A system in which no memorandum can be distributed without the author's consent
- c. A military facility in which only generals can enter a particular room
- d. A university registrar's office, in which a faculty member can see the grades of a particular student provided that the student has given written permission for the faculty member to see them.

6:A process may send a message to another process provided that the recipient is willing to accept messages. The following class and methods are relevant:

```
class Messages {  
    public deposit(int processid, String message);  
    public int willaccept(int processid);  
    ...  
}
```

The method **willaccept** returns 1 if the named process will accept messages, and 0 otherwise. Write a constraint for this policy using Pandey and Hashii's policy constraint language as described in the first example in [Section 4.5.1](#).

7: Use DTEL to create a domain **d_guest** composed of processes executing the restricted shell **/usr/bin/rexsh**. These processes cannot create any files. They can read and execute any object of type **t_sysbin**. They can read and search any object of type **t_guest**.

8: Suppose one wishes to confirm that none of the files in the directory **/usr/spool/lpd** are world-readable.

- a. What would the fourth field of the **tripwire** database contain?
 - b. What would the second field of the RIACS database contain?
 - c. **Tripwire** does not provide a wildcard mechanism suitable for saying, "all files in the directory **/usr/spool/lpd** beginning with **cf** or **df**." Suggest a modification of the **tripwire** configuration file that would allow this.
-

9: Consider the UC Davis policy on reading electronic mail. A research group wants to obtain raw data from a network that carries all network traffic to the Department of Political Science.

9

- a. Discuss the impact of the electronic mail policy on the collection of such data.
 - b. How would you change the policy to allow the collection of this data without abandoning the principle that electronic mail should be protected?
-

10: Prove Theorem 4-1. Show all elements of your proof.

11: Expand the proof of Theorem 4-2 to show the statement, and the proof, of the induction.
