

Security

Practice Exercises

- **17.1** What protection problems may arise if a shared stack is used for parameter passing?
- **17.2** Consider a computing environment where a unique number is associated with each process and each object in the system. Suppose that we allow a process with number n to access an object with number m only if n > m. What type of protection structure do we have?
- **17.3** Consider a computing environment where a process is given the privilege of accessing an object only *n* times. Suggest a scheme for implementing this policy.
- **17.4** If all the access rights to an object are deleted, the object can no longer be accessed. At this point, the object should also be deleted, and the space it occupies should be returned to the system. Suggest an efficient implementation of this scheme.
- **17.5** Why is it difficult to protect a system in which users are allowed to do their own I/O?
- **17.6** Capability lists are usually kept within the address space of the user. How does the system ensure that the user cannot modify the contents of the list?