Operating Systems (COMP2006)

CURTIN UNIVERSITY
Computing Discipline
School of Electrical Engineering, Computing and Mathematical Sciences

Worksheet 10

1. What is the *need to know* principle? Why is it important for a protection system to adhere to this principle?

2. Why is the separation of mechanism and policy a desirable property?

3. What are the main differences between capability lists and access lists?

4. 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?

5. Buffer-overflow attacks can be avoided by adopting a better programming methodology or by using special hardware support. Discuss these solutions.

6. Attacks from inside the system (by somebody that has already been logged in, legally or illegally) can be, among the few, in the forms of Trojan Horses, Login Spoofing, Logic Bombs, and trap doors. Explain how each work, and ways to prevent them, if possible.

7. What is the purpose of using a "salt" along with the user-provided password? Where should the "salt" be stored, and how should it be used?

8. When a file is removed, its blocks are generally put back on the free list, but they are not erased. Do you think it would be a good idea to have the OS erases each block before releasing it? Consider both security and performance factors in your answer, and explain the effect of each.