Tutorial 11
Protection and Security (Chapter 16 and 17)
Operating Systems CS 3SH3 Term 2, Winter 2022
Prof. Neerja Mhaskar

Tutorials are not mandatory. They are simply a tool for you to understand the course concepts better.

Tutorial Format: The questions will be posted a day before or on the day of the tutorial on the course website. You can choose to solve these problems before hand and come in with your solutions. I or one of the TAs helping me will check your solutions. If you have all of the questions correct you can choose to leave. If you have any of them incorrect, it is recommended that you stay and understand the solutions.

Solutions to the tutorial will not be posted online.

Question 1: Consider the following I/O scenarios on a single-user PC:
a. A mouse used with a graphical user interface
b. A tape drive on a multitasking operating system (with no device pre allocation available)
c. A disk drive containing user files
d. A graphics card with direct bus connection, accessible through memory-mapped I/O

For each of these scenarios, would you design the operating system to use buffering, spooling, caching, or a combination? Would you use polled I/O or interrupt-driven I/O? Give reasons for your choices.

Question 2:
The RC4000 system, among others, has defined a tree of processes (called a process tree) such that all the descendants of a process can be given resources (objects) and access rights by their ancestors only. Thus, a descendant can never have the ability to do anything that its ancestors cannot do. The root of the tree is the operating system, which has the ability to do anything. Assume the set of access rights is represented by an access matrix, *A*. *A*(*x*, *y*) defines the access rights of process *x* to object *y.* If *x* is a descendant of *z,* what is the relationship between *A*(*x, y*) and *A*(*z, y*) for an arbitrary object *y*?

Question 3: 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?

Question 4:
The access-control matrix could be used to determine whether a process can switch from, say, domain A to domain B and enjoy the access privileges of domain B. Is this approach equivalent to including the access privileges of domain B in those of domain A?

Question 5: What is the difference between symmetric and asymmetric encryption algorithms?

Question 6: Consider the RSA encryption algorithm. Given p = 5, q = 11, k_e= 3, k_d= 27, compute the following:

1. What are the public and private keys used?
2. Given message m = 9. Compute the ciphertext 'C' using the encryption algorithm.
3. Compute the message from the ciphertext 'C' using the decryption algorithm.