CSE 303: Quiz #1  
Due Friday September 16th, 2022 at 11:59 PM

The quiz has THREE questions. Please submit your answer on CourseSite as a pdf whose name is exactly your user Id and the “pdf” extension (e.g., abc123.pdf) before the deadline.

**Question 1: “**Storing data permanently in a secondary storage device appears to be a *persistence* problem. However, a deeper view reveals that it is indeed related to all the five OS themes we discussed in lectures”. Briefly explain with clear examples to what extent you agree or disagree with this statement.

Please use the remainder of this page to provide your answer to the question. Give a detailed answer, but keep your entire response to a single side of an 8.5x11 page.

Five OS themes include virtualization, security, persistence storage, concurrency and resource management. The persistence is defined as a way to retrieve information and data after the machine is turn off. Secondary storage device refers to external storage device which will maintain the data and information even when we turn off the power. Comparing to those primary storage device, like RAM, storing in the secondary device may be a way to deal with persistence problem on the condition that the secondary device is reliable, durable and recoverable. However, storing every data permanently into the secondary storage device may raise the security problem. For example, we definite don’t want to store the sensitive and critical data into the secondary storage device, instead we should put them into the primary storage device, which give us frequent access and monitor for security issue like unauthorized access, and we also probably want those system security data goes always if we turn off the machine, for the reason that resource management require fairness and sharing which means multi-users can access the secondary storage device on a single machine. Also, if we store our data through external storage device like cloud, security issue may also raises at the process of sending and requiring data. I do agree with the statement for the reason that those 5 themes are interrelated to each other.

**Question 2:** The idea of separating mechanism and policy is widely used in OS designs. Briefly discuss two examples of this separation in two different themes of the five themes we cover in this course (clearly state which theme is related to each example you give).

Please use the remainder of this page to provide your answer to the question. Give a detailed answer, but keep your entire response to a single side of an 8.5x11 page.

1. Policy: who is allowed to access what data, and who can do what operation. Mechanism: dual-mode execution. This is the example of separation in security themes, which is a protection of system from improper usage and access. This separation is related to the security theme. The policy is a way we could achieve security, which recognize and distinguish the authorization of data accessing and performing operation. The mechanism that we used to enforce our policy is through dual-mode execution where we switch from user mode to kernel mode to access protected memory when encountering system call or interruption, and switch back to user mode after handling the system call.
2. Policy: depends on priority to switch program sharing CPU. Mechanism: time interrupt, which applies APIC to send a signal and invoke dual-mode execution to switch different program sharing the CPU. This example is related to the concurrency where we focus on the situation where we have multiple programs run on the CPU at the same time, and we want to switch between them and get the program with the highest priority done first.

**Question 3:** In P1 all messages are encrypted except req\_key and its response, which is claimed to be harmless since the public key sent in the response cannot be used to decrypt further messages. To what extent do you agree with that claim? Are there any other possible attacks a malicious third party can make if it is able to intercept this unencrypted req\_key message and/or its response? If yes, give an example of such attacks and briefly explain one way to protect against it. If not, briefly explain why.

Please use the remainder of this page to provide your answer to the question. Give a detailed answer, but keep your entire response to a single side of an 8.5x11 page.

Based on the idea from the course content, we use the Euler’s totient of n to generate public key and private key

e \* d = 1 mod ɸ(n) where e is public key and n is private key. We are sending e and n along the response, and client use them to encrypt message m. According to the course slide, there is actually 2 way of breaking it if someone intercept the response, but both way are hard. 1. Try to calculate d, but since we just send the n not the ɸ(n), it will be hard to factorize. 2. Try to reverse-engineer by encrypting all possible messages using e, which is also hard if m is long. Therefore, I do partially agree the statement, but it is still possible to break the encrypted messages, even it is hard. The way to avoid such attack might be: 1. Encrypt the response(public key), make it a lot more harder to break. 2. Make message long enough.