CS526 Information Security
Assignment 4 Solutions

ZHONGSHU GU
CAREER:GU16

1 Answer

(a) False. [redacted]

(b) The choice is iv. According to definition 5-5, a system is secure if it satisfies the simple security condition, the *-property, and the discretionary security property. i,ii and iii do not mention the discretionary security property.

[redacted]

3 Answer

(1) release-write Represent this request as r = (release, s, o, $\underline{w}$) $\in R^{(1)}$, and let the current state of the system be v = (b, m, f, h). The release-write is the rule ρ_5(r, v):

if(r $\notin \Delta(\rho_5)$)
    then ρ_5(r, v) = ($\underline{i}$, v);
else
    ρ_5(r,v) = ($\underline{y}$,(b - {s, o, $\underline{w}$}, m, f, h));

Proof: Let v satisfy the ssc, the *-property and the ds-property. Let ρ_5(r, v) = (d, v'). Either v = v' or v' = (b - (s, o, $\underline{w}$), m, f, h) by the release-write rule. In the former case, because v satisfies the simple security condition, the *-property, and the ds-property, so does v'. So let v' = (b - (s, o, $\underline{w}$), m, f, h) in which b' = b - (s, o, $\underline{w}$). We can infer that b' $\subseteq$ b, f' = f and m'[s,o] = m[s,o] for all
According to Theorem 5-13

a. Because b' $\subseteq$ b, f' = f, and v satisfies the ssc, then v' satisfies the ssc.
b. Because b' $\subseteq$ b, f' = f, and v satisfies the *-property, then v' satisfies the *property.
c. Because b' $\subseteq$ b, m'[s,o] = m[s,o], and v satisfies the ds-property, then v' satisfies the ds-property.
Hence, the release-write rule preserves the security of the system.

4 Answer

(a)

process scheduler In wSecureOS, if the scheduler is preemptive, the timer which trigger the scheduling should be consistent with the time window, i.e. the scheduling can not happen inside the time window. In SecureOS, there is no restriction on when the schedule can happen.

interrupt handler In wSecureOS, if there are two interrupts happened in the gap of the time window, it should be ordered in a interrupt queue and processed at the interval of the time window. In SecureOS, the interrupt handler can process interrupts that happened arbitrarily.

system call interface System call is like a soft interrupt. In wSecureOS, the system call should also be ordered and processed according to the time window, i.e. we should delay some of the system call handler. In SecureOS, it can process the system call from user level program at arbitrary time.

loader In wSecureOS, when loader loads a new program image, the function to copy the text segment and data segment into the new allocated address space should be consistent with the time window, otherwise the image that is loaded will be modified during the time window. In SecureOS, it can keep the consistency of the process image when loading it into process address space.

(b) Such kind of operating system can be used in the embedded control system like microwave oven, refrigerator or vending machine. It only needs to process the input from human being which will have a longer time window than the time window which is pre-defined by the wSecureOS.