1a. Process order from parent to child: 1_init ->14806_sshd ->18691_sshd ->18694_sshd ->18695_tcsh

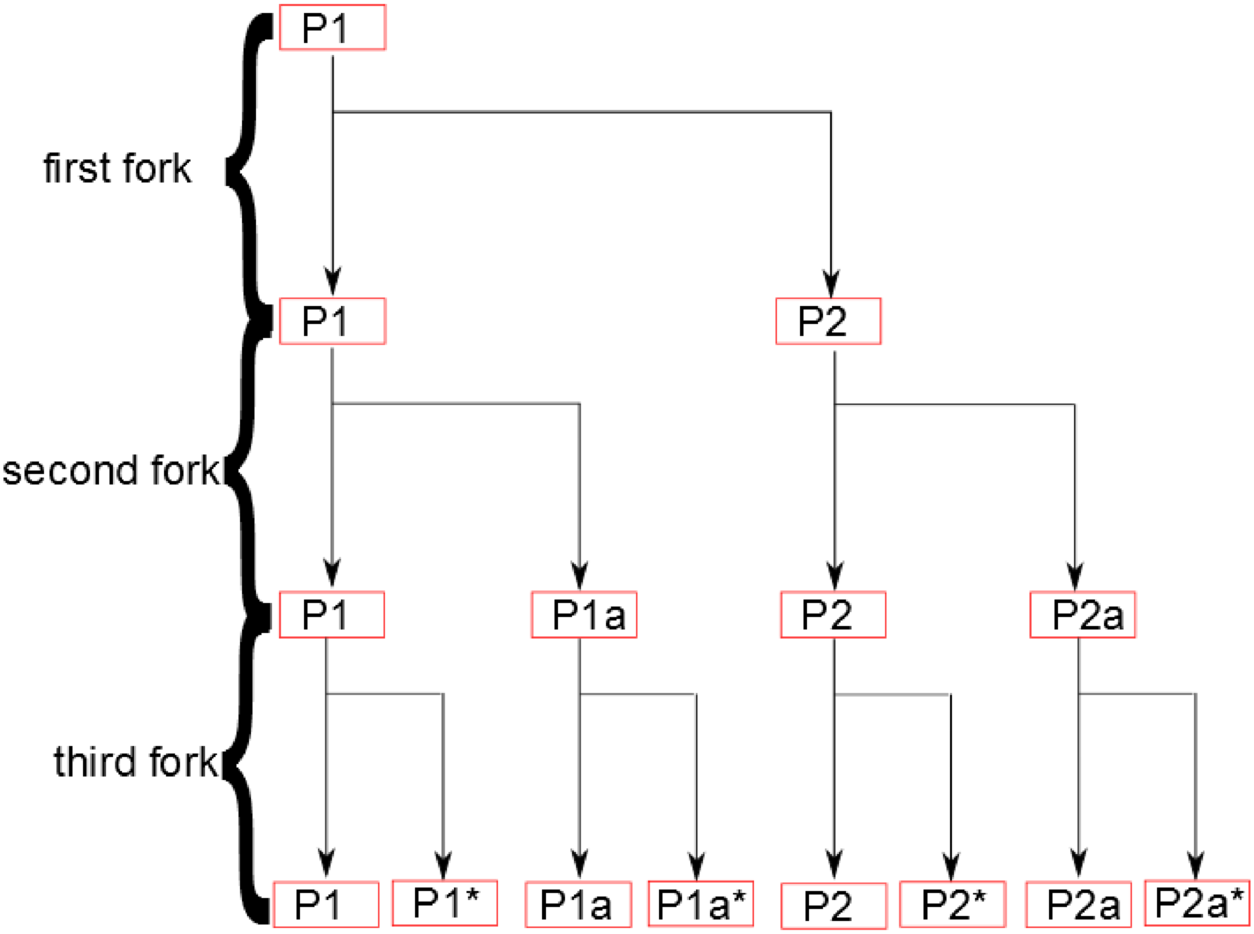
1b. these applications need to need to retain special privilege throughout their life-time and attacker can use programming error to gain special privilege.

1c. The principle name is: least privilege.
Another definition: "Process isolation is the principle that each process should have no capability beyond what is required to perform its task."
Denning, Peter J. "Fault tolerant operating systems." ACM Computing Surveys (CSUR) 8.4 (1976): 359-389.

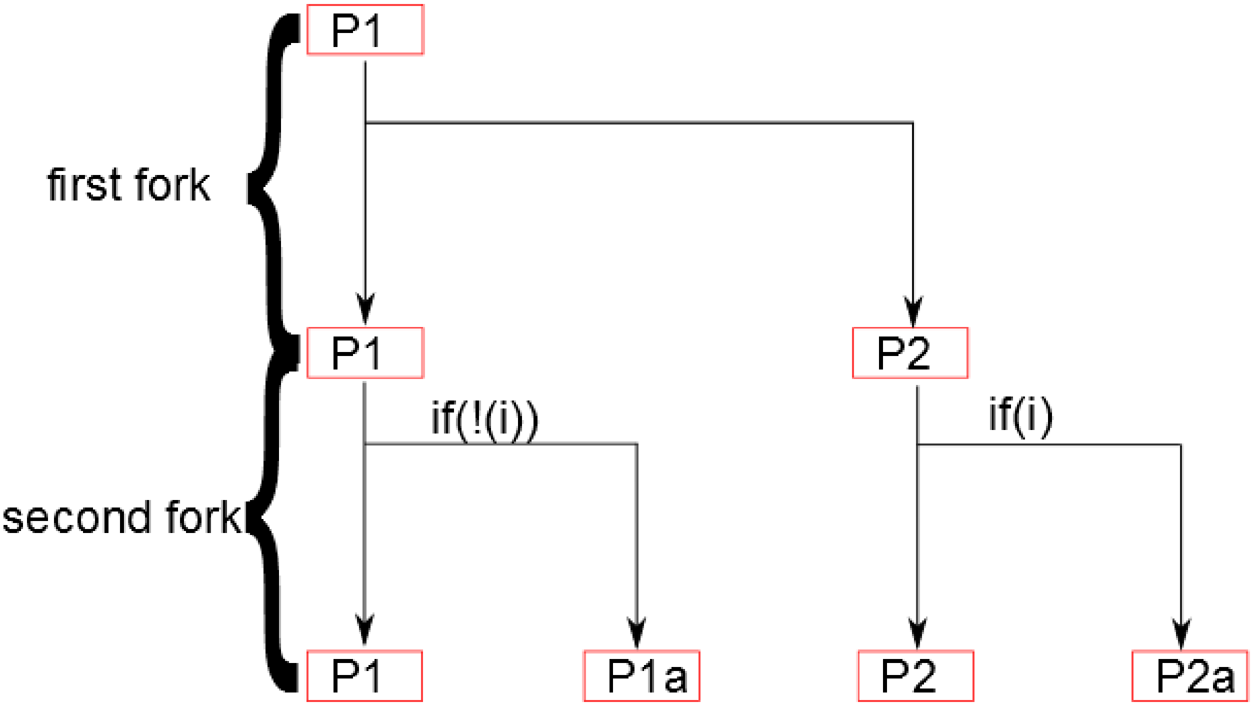
1d. privileged parent process: monitor
unprivileged child process: slave

1e. Since OpenSSH have only twenty five percent of the source code require privilege whereas the remaining seventy five percent are executed without special privilege.
It is assuming the error is uniformly distributed, so 75% of errors will not be attacked.

2a.



2b.



3. copy on write: when multiple separate tasks use initially identical copies of some information, only copy the information for the task if the task is going to modify it. So instead of doing many copy for multiple task(which will cause overhead), the system only copy information when necessary.