

Esecuzione di un processo

Tramite syscall, si fa:

- creazione del PCB: PID, registri, path, address space, stato, ...
- allocazione di memoria: trovare e/o liberare pagine;
- copia in memoria dell'eseguibile;
- allocazione dello stack;
- allocazione di spazio in kernel space per la gestione del processo (e.g. upcall);
- copia dei parametri passati: non basta un puntatore alla lista fornita dal chiamante, il nuovo processo non può accedere alla memoria del vecchio;
- esecuzione: impostazione di PC, SP, CPSR, ... Alternativamente, si segnala allo scheduler che il processo è pronto per l'esecuzione.

La lettura in memoria dell'eseguibile è un'operazione lenta di I/O, perciò viene eseguita in background tramite DMA. `exec` quindi non è una funzione monolitica, ma è interrotta e ripresa con interrupt.