Kernel Control Flaw
(1) Red boot hands control to intmain()
2) main sots the jump instruction in
the jump table in low memory.
the jump table in low memory. The jump table in low memory. *(0x8) = 0x0E51FF004 j LDR RC [PC, #4] 3 per next word into PC *(0x8) = 2 asm_SwiCall Entry * (0x0) = 2 asm_SwiCall Entry
*(0×10) = 2 asm_ SwiCall Entry
TODO; revise this step because it does some bod things
3 Main calls Init kernel & Public interface 4 Int Kernel colls osm-Internel Entry & Swi Interface 5 That Kernel Colls osm-Internel Entry & Swi Johns process state
4) Int Kernol colls orm-Inthernel Entry & Swissmen process state B) asm_Init Kernol Entry calls SWI O after nushing process state D) 11 - 0×8; 10 = 2 asm-swiColl Entry
Q PC = 0x8; SE = 2 asm-swiCall Entry
hd Mat = 1 (feet 1 CFN / 1)
Jang toble saw # 0 for svicull jumps to K_Internel
- 11- first tas/s , in L. schedaled ""C
asm ternelexit moses saved mode, 16 for user proc
asm ternelexit mes sets spand LR la source proc Description of the start saved mode, 16 for user proc Description of the start of the suite of the suite of the security of
(3) execute + rest ("
13 last task does exit (3) last task does exit (all schedule of next proc, but none
- TUNISION OF SUITED TO SU
13 Last task does exit (3) Last task does exit (9) In exit function, call schedule at next proc, but none 19) In exit function, call schedule at next proc, but none 19) In exit function, call schedule at next proc, but none 19) In exit function, call schedule at next proc, but none 19) In exit function, call schedule at next proc, but none 19) In exit function, call schedule at next proc, but none 19) In exit function, call schedule at next proc, but none 19) In exit function, call schedule at next proc, but none 19) In exit function, call schedule at next proc, but none 19) In exit function, call schedule at next proc, but none 19) In exit function, call schedule at next proc, but none 19) In exit function, call schedule at next proc, but none 19) In exit function, call schedule at next proc, but none 10) In exit function, call schedule at next proc, but none 10) In exit function, call schedule at next proc, but none 10) In exit function, call schedule at next proc, but none 10) In exit function, call schedule at next proc, but none 10) In exit function, call schedule 11) In exit function, call schedule 12) In exit function, call schedule 13) In exit function, call schedule 14) In exit function, call schedule 15) In exit function, call schedule 16) In exit function, call schedule 17) In exit function, call schedule 18) In exit function, call schedule 19) In exit function, call schedule 19) In exit function, call schedule 19) In exit function, call schedule 10) In exit function, call schedule 11) In exit function, call schedule 12) In exit function, call schedule 13) In exit function, call schedule 14) In exit fun
(16) 0.5 $M = 110$ M
Internal () in rivers (a) Main method returns control to red post
(16) Main method