cse30 discussion 7

Ibrahim Awwal

July 20, 2015

arm assembly review

conditional execution

- CMP instruction: compares register(s) and/or immediates
- equivalent to SUBS without storing result of subtraction
- Why is this?
- After performing comparison, we can conditionally execute any instruction

conditional execution - examples

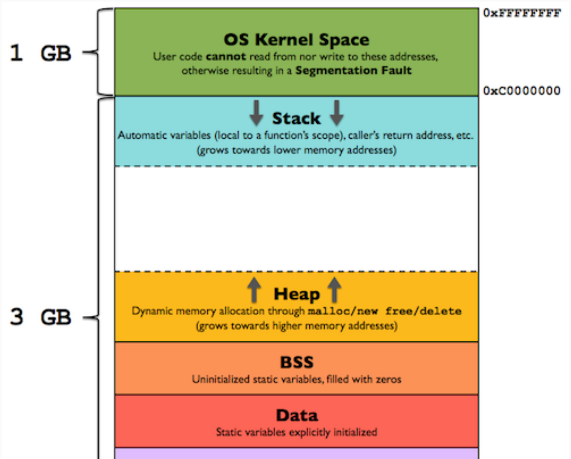
control flow

control flow: c to arm

function calls

the stack

- Stores automatic variables, return address, any registers we need to save before ## Memory Layout


0xFFFFFFFF
1 GB
OS Kernel Space
User code cannot read from nor write to these addresses, otherwise resulting in a Segmentation Fault
0xC0000000
Stack
Automatic variables (local to a function's scope), caller's return address, etc. (grows towards lower memory addresses)
3 GB
Heap
Dynamic memory allocation through malloc/new free/delete (grows towards higher memory addresses)
BSS
Uninitialized static variables, filled with zeros
Data
Static variables explicitly initialized

stack nomenclature

- **Ascending** stack grows upwards, i.e. memory addresses go from low to high
- **Descending** stack grows downwards, i.e. memory addresses go from high to low
- **Empty** stack, the stack pointer points to the next free (empty) location on the stack
- **Full** stack, the stack pointer points to the topmost item in the stack

stack nomenclature

- **Ascending** stack grows upwards, i.e. memory addresses go from low to high
- **Descending** stack grows downwards, i.e. memory addresses go from high to low
- **Empty** stack, the stack pointer points to the next free (empty) location on the stack
- **Full** stack, the stack pointer points to the topmost item in the stack

- The ARM Linux stack convention is to use a full descending stack
- That is, addresses grow downwards, and `$sp` points to the last item pushed onto the stack

push and pop instructions

- Push registers onto, and pop registers off a full descending stack.
- PUSH{cond} reglist
- POP{cond} reglist
- reglist is a non-empty list of registers, enclosed in braces. It can contain register ranges. It must be comma separated if it contains more than one register or register range.
- PUSH and POP are synonyms for STMDB and LDM (or LDMIA), with the base register sp (r13), and the adjusted address written back to the base register
- source

system calls: leveraging the os

exercises

linked lists

tree recursion

int to string