Computer Architecture

Friday, March 23, 2018 12:34 PM

Von Neumann diagram

- Program and data in same memory region, no clear distinction
- Vs. Harvard architecture

Control Flow

- Instruction Pointer (program counter) = register that stores address of next instruction
- Program counter need not move by +1
    - Direct branch: constant value to increase
    - Indirect branch (value fetched from memory)
    - Conditional branch

Call Stack

- Top = stack pointer
- Call stack will have a return address for previous process

Stack Smashing

- Modify code/ control flow (return address)
    - Cannot easily distinguish between malicious code and benign data
    - Buffer overflow to write to memory locations
    - Restrictive attack method: can only write to small part of memory/ sequence of consecutive bytes (surgical attack)
- Attack 1: Overwrite execution code with malicious code
- Attack 2: Overwrite control flow information
    - printf vulnerability
    - Buffer overflow