14 - Debugging

Kernel vs. User-Mode
Debugger Functionality
Exceptions
Modifying Execution
Kernel vs. User-Mode Debugging

- **User mode:**
  - Debugger runs on same system as program being debugged.
  - Debugging a single executable.
  - OllyDbg or WinDbg can be used.

- **Kernel mode:**
  - Debugging performed on two systems
    - One system runs code being debugged.
    - One system runs debugger.
  - OS must be configured for its kernel to be debugged.
  - WinDbg must be used.
Debugger Functionality

• Single Stepping
• Stepping-over vs. Stepping-into
• Pausing Execution with Breakpoints
  – Software execution
    Debugger replaces first byte of instruction with 0xCC (INT 3) and rewrites instruction after reaching that point.
  – Hardware execution
    • Four hardware breakpoint registers store bkpt addr.
    • Can set breakpoint on access as well as execution. (DR7)
    • Running program can modify these registers.
  – Conditional Breakpoints (always software)
Exceptions

• After the debugger takes control, if an exception occurs, the debugger gets the first chance to handle it (program breaks at an exception).

• If a debugged program is allowed to handle an exception and there is no handler, the debugger gains control again.

• Common types:
  - INT 3
  - Trap flag
  - Memory access violation
  - Privileged mode instruction execution
Modifying Execution

- You can change the execution order of a program by
  - Modifying the instruction pointer register.
  - Modify the values in registers that will be arguments to `cmp` or `test`.
  - Modify the values of memory addresses.