

Comprehensive Intel 64 and IA-32 (x86) Architecture

Let MindShare Bring “Hands-On x86 Architecture” to Life for You

This course teaches the x86 architecture (both 32-bit and 64-bit) through a mix of lectures and hands-on programming labs. All topics are explained in lecture format first and then the students are given programming labs in Assembly Language to reinforce the concepts and to get hands-on experience working with x86 processors at a very low level.

You Will Learn:

- x86 architecture basics like an overview of the instruction set, register set and operating modes
- The behavior of segmentation, how it was originally intended to be used and how it is actually used by operating systems today (both 32-bit and 64-bit OSs)
- How to setup system calls using multiple methods (and what are benefits / side-effects of each)
- How to setup interrupt service routines for both software and hardware interrupts as well as exceptions
- How to implement paging in both the 32-bit environments as well as the 64-bit environments including using various page sizes
- What the concepts of virtualization are and the behavior of the x86 hardware extensions for virtualization (including benefits and side-effects)

Course Length: 5 Days (but can be customized to your needs / duration)

Course Outline:

- **x86 Instruction Set Background**
- **Intro to the Instruction Set**
 - General Purpose Instructions
 - Floating Point and SIMD Instructions
 - x87, MMX, SSE, AVX, AVX-2, AVX-512
 - Program Flow-related Instructions
 - Hardware-Related Instructions
- **Intro to the Register Set and Address Spaces**
 - General Purpose registers (GPRs)
 - x87 / MMX registers
 - XMM / YMM / ZMM registers
 - Segmentation registers
 - Control registers
 - Debug registers
 - Model-Specific registers (MSRs)
 - Memory, IO, and Configuration Spaces
- **Operating Modes**
 - Real Mode
 - Protected Mode
 - Virtual-8086 Mode
 - System Management Mode
 - Long (IA32e) Mode
 - 64-bit Mode
 - REX prefixes
 - Compatibility Mode
- **Real Mode Operation**
- **Introduction to Multitasking**

- **Segmentation (Protected Mode)**
 - Privilege Levels (Rings)
 - Code and Data Segment Descriptors
 - Segment Registers (CS, SS, DS, ES, FS, GS)
 - Global Descriptor Table (GDT)
 - Local Descriptor Table (LDT)
 - Flat memory model vs protected memory model
 - **HANDS-ON LAB:** covering Protected Mode Segmentation
 - Segmentation in Long Mode
- **Control Transfers**
 - Far Jumps and Calls
 - Call Gates
 - Optimized System Calls
 - SYSCALL / SYSRET
 - SYSENTER / SYSEXIT
 - Automatic Stack Switching
 - **HANDS-ON LAB:** covering system calls
 - Control Transfers in Long Mode
- **Task Management**
 - Software vs. Hardware task switching
 - Task State Segments (TSS)
 - Task Gates
- **Interrupts and Exceptions**
 - Hardware vs. Software interrupts
 - Vectors
 - Interrupt priorities
 - Exceptions and their classifications (faults, traps and aborts)
 - Interrupt Descriptor Table (IDT)
 - Interrupt Gates vs Trap Gates
 - Stack behavior on an interrupt / exception
 - Error codes
 - **HANDS-ON LAB:** covering interrupt handling
 - Interrupt handling in Long Mode
- **Paging**
 - Purpose of Paging
 - Paging Basics
 - Physical vs. Virtual (Linear) Address Space
 - Swap space (secondary storage)
 - x86 paging structures
 - Page Directory Entries (PDEs)
 - Page Table Entries (PTEs)
 - TLBs (Translation Lookaside Buffers)
 - Managing TLBs
 - Global pages
 - x86 Paging Modes (features)
 - Page Size Extensions (PSE)
 - Physical Address Extensions (PAE)
 - 3-level lookup: Page Directory Pointer Entries (PDPE)
 - IA32e (Long) Mode Paging
 - 4-level lookup: Page Map Level 4 Entries (PML4E)
 - Execute Disable functionality
 - **HANDS-ON LAB:** covering paging

- **Memory Types**
 - Intro to Caches
 - Memory Types
 - UC – Uncacheable (and UC-)
 - WC – Write Combining
 - WP – Write Protect
 - WT – Write Through
 - WB – Write Back
 - Assignment Mechanisms
 - Memory Type and Range Registers (MTRRs)
 - Page Attribute Table Register (PAT)
- **Intro to Virtualization Technology (Intel-VT)**
 - What is virtualization
 - Hardware extensions: Intel-VT_x
 - VMX Root Mode (Host Mode) vs VMX non-Root Mode (Guest Mode)
 - Virtual Machine Control Structure (VMCS)
 - Intel-VT instructions (VMLAUNCH, VMRESUME, etc.) and #VMEXIT
 - Memory Management with Virtualization
 - Shadow Page Tables
 - Extended (Nested) Page Tables
 - TLB Management with Virtualization
- **Data Protection Extensions**
 - Intel SGX (Software Guard eXtensions)
 - Intel MPX (Memory Protection eXtensions)
- **Performance Monitoring**
 - Precision Event Based Sampling (PEBS)
- **System Management Mode**

Recommended Prerequisites: None

Course Material:

1) MindShare's *x86 Instruction Set Architecture* textbook (1st Edition).

Author: Tom Shanley

Publisher: MindShare Press

Available through the MindShare Online Store and major bookstore outlets.

2) Students will be provided with the MindShare x86 debugger used for the labs in class and an electronic version of the slides.