Introduction and Goals

Origins

For a long time, a group of us at PSU have been looking at the role that high-level programming languages can play in the construction of (very) low-level software.

- By using high-level languages, we can hope to increase programmer productivity, and improve software quality.
- By focussing on very low-level software, we hope to provide strong foundations for the complete software stack.

House (2005)

Kernel, GUI, drivers, network stack, and apps

Boots and runs in a bare metal environment

... all written in Haskell, a "purely functional" programming language

Why “House”?

“The Haskell User’s Operating System Environment”

You are more secure in a house …

than if you only have Windows …
Performance concerns

• By design, higher-level languages abstract away from the details of how the underlying machine works.
• Can we obtain the levels of performance and predictability that are typically required/expected in the systems programming domain?
• Can we write good systems software in a language that intentionally distances users from details of memory layout, representation, instruction selection, alignment, caching, etc.?
• Traditional approaches to building system software resort to using old, low-level languages like assembly and C.
• Do “modern” languages have anything to offer in this area?

The Habit programming language

• “a dialect of Haskell that is designed to meet the needs of high assurance systems programming”
• How do you design a programming language for a specific domain?
• Experiment with existing languages
• Understand the domain …

The seL4 experience

• In 2009, a group from NICTA, UNSW, and OK Labs in Australia announced seL4, as “the world’s first operating system kernel with an end-to-end proof of implementation correctness and security enforcement.”

The seL4 microkernel implementation (~8700 lines of C)

formal specification

proof of equivalence

~200K lines of Isabelle

• A landmark achievement for formal verification, and a strong foundation for building trustworthy systems

seL4 and capabilities

• Even without the verification result, the design of seL4 is interesting in its own right:
  • seL4 is a “capability enhanced” version of an earlier microkernel design called L4.
  • The “capability” abstraction in seL4 provides facilities for implementing “least privilege” security policies and novel mechanisms for controlling resource usage.

Safety properties for “free”?

• Security properties established in the seL4 verification include:
  • Absence of buffer overflows
  • Absence of null pointer dereferences
  • Absence of code injection attacks
  • …
• Many of these properties could be established for “free” if the implementation had been written in a “safer” language.
• How might things be different if we built something like seL4 in Habit?

The CEMLaBS project

• “Using a Capability-Enhanced Microkernel as a Testbed for Language-Based Security”
• Started October 2014, funded by The National Science Foundation
• Three main questions:
  • Feasibility: Is it possible to build an inherently “unsafe” system like seL4 in a “safe” language like Habit?
  • Benefit: What benefits might this have, for example, in reducing verification costs?
  • Performance: Is it possible to meet reasonable performance goals for this kind of system?
Course description

• An overview of conventional low-level programming techniques (1-5):
  • Bare metal programming
  • Fundamental programmable hardware components

• Case studies of practical microkernel implementations (6-8):
  • OS abstractions (address spaces, threads, capabilities, …)
  • The L4 and seL4 microkernels

• Reflections on the design of programming languages for this application domain (9-12):
  • Assembly, C, Rust, Habit, domain specific languages, …

Course learning objectives

Upon the successful completion of this course, students will be able to:

1. Write simple programs that can run in a bare-metal environment using low-level programming languages.
2. Discuss common challenges in low-level systems software development, including debugging in a bare-metal environment.
3. Explain how conventional operating system features (multiple address spaces, context switching, protection, etc.) motivate the desire for (and benefit from) hardware support.

Course learning objectives, continued

4. Develop code to configure and use programmable hardware components such as a memory management unit (MMU), interrupt controller (PIC), and interval timer (PIT).
5. Describe the key steps in a typical boot process, including the role of a bootloader.
6. Describe the motivation, implementation, and application of microkernel abstractions for managing address spaces, threads, and interprocess communication (IPC).
7. Explain the use and implementation of capabilities in access control and resource management.
8. Develop programs using a capability abstraction, like the one provided by the seL4 microkernel.

Course learning objectives, continued

9. Illustrate the use of a range of domain specific languages in the development of systems software.
10. Use practical case studies to evaluate and compare language design proposals.
11. Describe features of modern, high-level programming languages—including abstract datatypes and higher-order functions—and show how they can be leveraged in the construction of low-level software.
12. Explain how the requirements of low-level systems programming motivate the desire for (and benefit from) language-based support.

The “programming languages” perspective

• We will survey and evaluate a range of programming languages during this course:
  • Low-level machine and assembly languages
  • Systems programming languages (e.g., C, Rust, …)
  • Object-oriented languages (e.g., the seL4 API)
  • Domain specific languages
  • Functional languages (e.g., Habit, Haskell, …)
  • What are the driving needs of the systems domain?
  • How can a programming language design best meet those needs?

Context

• Basic Platform: Generic “IBM PC” compatible
  • 32 bits … not 64
  • IA32 … not x86_64 or ARM
  • BIOS … not EFI or UEFI
  • int and iret … not sysenter/sysexit
  • PIC … not APIC
  • No PAE, PCI, ACPI, MMX, SSE, SMM, SMP, VTx, …
  • etc., …
• Already complicated enough for our purposes!
• Well supported by current hardware, emulators, and tools
• Underlying concepts still very broadly applicable
Development environment

- Ubuntu Linux
  - Week 1: using the lab machines (others also an option)
  - Weeks 2+: using a VirtualBox virtual machine, preconfigured with appropriate development tools (can be used on Linux, Mac OS, or Windows)
- Bare metal emulation using the QEMU emulator

Rough schedule

<table>
<thead>
<tr>
<th>Week</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Assembly language programming</td>
</tr>
<tr>
<td>2</td>
<td>Bare metal programming</td>
</tr>
<tr>
<td>3</td>
<td>Hardware support for OS abstractions</td>
</tr>
<tr>
<td>4</td>
<td>Memory management &amp; protection</td>
</tr>
<tr>
<td>5</td>
<td>Case Study: L4 use &amp; implementation</td>
</tr>
<tr>
<td>6</td>
<td>Case Study 2: seL4 use &amp; implementation</td>
</tr>
<tr>
<td>7</td>
<td>Language design for low-level programming</td>
</tr>
</tbody>
</table>

What is IA32?

- We’ll be using the IA32 (x86) architecture as our main target:
  - A “32-bit” instruction set
  - Broadly adopted by:
    - processors from Intel, AMD, Via, ...
    - laptops, desktops, servers, gaming consoles, ...
    - Linux, Mac OS X, Windows, ...
  - Arguably, a bit dated … but still very relevant, and a good platform for learning and exploration
  - (… and one of the architectures supported by seL4)

An introduction to IA32 assembly language programming

Other architectures:

- Not to be confused with:
  - x86-64/AMD64: a 64 bit architecture supported (in addition to IA32) by more recent AMD/Intel designs
  - IA64: a completely different 64-bit Intel architecture (Itanium)
  - ARM: widely used in phones, tablets, and more
  - IBM Power: used in Xbox 360, PS3, Wii, servers, and more
  - SPARC: used by some of the college’s Unix servers
- Except for x86-64, you can’t run IA32 code directly on a machine that uses one of these alternative instruction sets!

Notes

- No prior or in-depth knowledge of IA32 programming will be assumed
- We will only use a small subset of the full instruction set
- If you’re looking to become an expert on IA32 programming, you’ll want to look for another class!
- We’ll be using the AT&T syntax for IA32 assembly language rather than the Intel syntax. This is the default syntax used by the free GNU tools in Linux, MacOS, and DJGPP or Cygwin on Windows, and others
A greatly simplified view of IA32 computing

CPU
- instruction pointer
- general purpose registers

Memory
- up to 4 GB (2^32 bytes)

ALU
- data / 8

Programming for IA32
- In concrete terms, an IA32 program is just a collection of byte values (machine code)
- Once it has been loaded into memory, the processor can execute a program by interpreting the byte values as instructions for the processor to act on
- For practical purposes, we will usually write IA32 programs in a textual format called assembly language that is easier to read than raw byte values
- The program that translates assembly language programs into machine code is called an assembler

The GNU assembler, as
- Assembly code goes in files with a .s suffix
- We will typically use gcc to invoke the assembler
  gcc -m32 -o outputAssemblyCode.s extras.c
- You can also invoke the assembler directly: detailed documentation is available from: http://sourceware.org/binutils/docs/as/
  For IA32 programming, look in particular at the section on “80386 Dependent Features”

An assembly code listing

```
.globl f
f:   pushl %ebp
    movl %esp,%ebp
    pushl $0
    subl %ebp, %esp
    test %ebp, %ebp
    cmpl $0, %eax
    jae .loop
    addl $4, %ebx
    # and move to next array element
    test:   movl (%ebx), %ecx
    cmpl $0, %ecx
    jae .test
    jmp .test
    popl %ebp
    movl %esp,%ebp
    popl %ebp
    ret
```

An assembly code listing

```
0000 55
0001 89E5
0002 53
0003 8B5D08
0004 8B000000
0005 00
0006 C9
0007 80389000
0009 75F5
000A 5B
000B 89EC
000C 5D
0011 C3

Machine code
```

```
.globl f
f:   pushl %ebp
    movl %esp,%ebp
    pushl $0
    subl %ebp, %esp
    test %ebp, %ebp
    cmpl $0, %eax
    jae .loop
    addl $4, %ebx
    # and move to next array element
    test:   movl (%ebx), %ecx
    cmpl $0, %ecx
    jae .test
    jmp .test
    popl %ebp
    movl %esp,%ebp
    popl %ebp
    ret
```

```
0000 55
0001 89E5
0002 53
0003 8B5D08
0004 8B000000
0005 00
0006 C9
0007 80389000
0009 75F5
000A 5B
000B 89EC
000C 5D
0011 C3

Assembly code
```

```
0000 55
0001 89E5
0002 53
0003 8B5D08
0004 8B000000
0005 00
0006 C9
0007 80389000
0009 75F5
000A 5B
000B 89EC
000C 5D
0011 C3

Machine code
```

```
.globl f
f:   pushl %ebp
    movl %esp,%ebp
    pushl $0
    subl %ebp, %esp
    test %ebp, %ebp
    cmpl $0, %eax
    jae .loop
    addl $4, %ebx
    # and move to next array element
    test:   movl (%ebx), %ecx
    cmpl $0, %ecx
    jae .test
    jmp .test
    popl %ebp
    movl %esp,%ebp
    popl %ebp
    ret
```

```
0000 55
0001 89E5
0002 53
0003 8B5D08
0004 8B000000
0005 00
0006 C9
0007 80389000
0009 75F5
000A 5B
000B 89EC
000C 5D
0011 C3

Assembly code
```

```
0000 55
0001 89E5
0002 53
0003 8B5D08
0004 8B000000
0005 00
0006 C9
0007 80389000
0009 75F5
000A 5B
000B 89EC
000C 5D
0011 C3

Machine code
```

```
.globl f
f:   pushl %ebp
    movl %esp,%ebp
    pushl $0
    subl %ebp, %esp
    test %ebp, %ebp
    cmpl $0, %eax
    jae .loop
    addl $4, %ebx
    # and move to next array element
    test:   movl (%ebx), %ecx
    cmpl $0, %ecx
    jae .test
    jmp .test
    popl %ebp
    movl %esp,%ebp
    popl %ebp
    ret
```

```
0000 55
0001 89E5
0002 53
0003 8B5D08
0004 8B000000
0005 00
0006 C9
0007 80389000
0009 75F5
000A 5B
000B 89EC
000C 5D
0011 C3

Machine code
```

```
.globl f
f:   pushl %ebp
    movl %esp,%ebp
    pushl $0
    subl %ebp, %esp
    test %ebp, %ebp
    cmpl $0, %eax
    jae .loop
    addl $4, %ebx
    # and move to next array element
    test:   movl (%ebx), %ecx
    cmpl $0, %ecx
    jae .test
    jmp .test
    popl %ebp
    movl %esp,%ebp
    popl %ebp
    ret
```

```
0000 55
0001 89E5
0002 53
0003 8B5D08
0004 8B000000
0005 00
0006 C9
0007 80389000
0009 75F5
000A 5B
000B 89EC
000C 5D
0011 C3

Machine code
```

```
.globl f
f:   pushl %ebp
    movl %esp,%ebp
    pushl $0
    subl %ebp, %esp
    test %ebp, %ebp
    cmpl $0, %eax
    jae .loop
    addl $4, %ebx
    # and move to next array element
    test:   movl (%ebx), %ecx
    cmpl $0, %ecx
    jae .test
    jmp .test
    popl %ebp
    movl %esp,%ebp
    popl %ebp
    ret
```

```
0000 55
0001 89E5
0002 53
0003 8B5D08
0004 8B000000
0005 00
0006 C9
0007 80389000
0009 75F5
000A 5B
000B 89EC
000C 5D
0011 C3

Machine code
```

```
.globl f
f:   pushl %ebp
    movl %esp,%ebp
    pushl $0
    subl %ebp, %esp
    test %ebp, %ebp
    cmpl $0, %eax
    jae .loop
    addl $4, %ebx
    # and move to next array element
    test:   movl (%ebx), %ecx
    cmpl $0, %ecx
    jae .test
    jmp .test
    popl %ebp
    movl %esp,%ebp
    popl %ebp
    ret
```

```
0000 55
0001 89E5
0002 53
0003 8B5D08
0004 8B000000
0005 00
0006 C9
0007 80389000
0009 75F5
000A 5B
000B 89EC
000C 5D
0011 C3

Machine code
```
IA32 registers

8-bit registers (holding a single byte, 0-255)

<table>
<thead>
<tr>
<th>accumulator</th>
<th>al</th>
<th>ah</th>
</tr>
</thead>
<tbody>
<tr>
<td>base</td>
<td>bh</td>
<td>bl</td>
</tr>
<tr>
<td>count</td>
<td>cl</td>
<td>ch</td>
</tr>
<tr>
<td>data</td>
<td>dh</td>
<td>dl</td>
</tr>
</tbody>
</table>

Introduced in 1978 as part of the 8086 architecture

16-bit registers (“word”)

<table>
<thead>
<tr>
<th>ax</th>
<th>ah</th>
<th>al</th>
</tr>
</thead>
<tbody>
<tr>
<td>bx</td>
<td>bh</td>
<td>bl</td>
</tr>
<tr>
<td>cx</td>
<td>ch</td>
<td>cl</td>
</tr>
<tr>
<td>dx</td>
<td>dh</td>
<td>dl</td>
</tr>
<tr>
<td>si</td>
<td></td>
<td></td>
</tr>
<tr>
<td>di</td>
<td></td>
<td></td>
</tr>
<tr>
<td>bp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sp</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Introduced in 1978 as part of the 8086 architecture

32-bit registers (“double word”)

<table>
<thead>
<tr>
<th>eax</th>
<th>ah</th>
<th>al</th>
</tr>
</thead>
<tbody>
<tr>
<td>ebx</td>
<td>bh</td>
<td>bl</td>
</tr>
<tr>
<td>ecx</td>
<td>ch</td>
<td>cl</td>
</tr>
<tr>
<td>edx</td>
<td>dh</td>
<td>dl</td>
</tr>
<tr>
<td>esi</td>
<td></td>
<td></td>
</tr>
<tr>
<td>edi</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ebp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>esp</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

“e” for extended sometimes referred to as “long word”

Introduced in 1985 as part of the 80386 architecture

Special vs. general purpose registers

- eip: the instruction pointer register
- esp: the stack pointer register
- eflags: the flags register, stores information about the results of the most recent arithmetic or logic instruction
- Other registers can typically be used for any purpose (although some instructions—division, for example—work only with specific registers)

IA32 instructions
**Instruction format**

- A typical IA32 instruction has the form:
  
  \[
  \text{opcode src, dst}
  \]

- A suffix on the opcode indicates the size of the data that is being operated on:
  - 32-bit values use the suffix \(l\) (ong)
  - 16-bit values use the suffix \(w\) (ord)
  - 8-bit values use the suffix \(b\) (yte)

**Addressing modes**

- **Register access**, \(\text{reg}\):
  - \(%eax\): the value in register \(eax\)
  - Can typically use any registers except \(eip\) and \(eflags\)

- **Memory access**, \(\text{mem}\):
  - \(\%\text{var}\): the value in memory at address \(\text{var}\)
  - \((\%eax)\): the value in memory at the address in \(eax\)
  - \(8(\%eax)\): the value in memory at the address given by adding 8 to the value in \(eax\)

- **Immediate**, \(\text{immed}\):
  - \$42: the constant value 42 (decimal; use \$0x2A for hex)
  - \$\text{var}: the address of memory location \text{var}

**Directives for “declaring” variables**

- \(.data\)
  - # put variables in the “data” section
  - # (code usually goes in .text)

- \(.align 4\)
  - # make sure address is multiple of 4

- \(.global days\)
  - # A globally accessible array of ints

- \(\text{myvar}\.long 42\)
  - # Simple variable, initialized to 42

- \(\text{scratch}.space 4*100\)
  - # reserve uninitialized space

- \(\text{medium}\.long 123\)
  - # a 32-bit integer (takes 4 bytes)

- \(\text{regular}.short 123\)
  - # a 16-bit integer (takes 2 bytes)

- \(\text{small}\.byte 123\)
  - # an 8-bit integer (takes 1 byte)

- \(\text{days}\.long 31, 28, 31, 30, 31, 30, 31\)

**How values are stored in memory**

- A double word holds 32 binary digits (“bits”) (i.e., 4 bytes)

- 0xBE1A3910 can be interpreted as -1,105,577,712 (signed) or 3,189,389,584 (unsigned)

- Stored in memory with the least significant byte at the lowest address (“little endian”):

- Copy data from a source to a destination (where \(X\) is one of the size suffixes: \(b, w, l\)):

  \[
  \text{movX src, dst}
  \]

- Any of the following combinations of arguments is allowed:

  \[
  \text{movX reg, (reg | mem)}
  \]

  \[
  \text{movX mem, reg}
  \]

  \[
  \text{movX immed, (reg | mem)}
  \]

- Note that you can’t move \(\text{mem to mem}\) in one instruction

**IA32 instructions: data movement**
Examples

Suppose that the memory (starting at address 0) contains the following (four byte) values:

<table>
<thead>
<tr>
<th>8 6 2 8 0 2 4 1 7 3 4 5 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>0  4  8 12 16 20 24 28 32 36 40 44 48</td>
</tr>
</tbody>
</table>

Then

<table>
<thead>
<tr>
<th>instruction</th>
<th>contents of eax</th>
</tr>
</thead>
<tbody>
<tr>
<td>movl $12, %eax</td>
<td>12</td>
</tr>
<tr>
<td>movl (%eax), %eax</td>
<td>8</td>
</tr>
<tr>
<td>movl 8(%eax), %eax</td>
<td>0</td>
</tr>
</tbody>
</table>

Zero and sign-extension

- Suppose we want to copy a value from a 16-bit register in to a 32-bit register:

```
stu ....... xyz          
```

<table>
<thead>
<tr>
<th>ax</th>
<th>eax</th>
</tr>
</thead>
<tbody>
<tr>
<td>ax</td>
<td>eax</td>
</tr>
</tbody>
</table>

- Two common strategies:

  - Zero extension: for unsigned values

```
stu ....... xyz          
```

<table>
<thead>
<tr>
<th>ax</th>
<th>eax</th>
</tr>
</thead>
<tbody>
<tr>
<td>ax</td>
<td>eax</td>
</tr>
</tbody>
</table>

  - Sign extension: for signed values

```
stu ....... xyz          
```

<table>
<thead>
<tr>
<th>ax</th>
<th>eax</th>
</tr>
</thead>
<tbody>
<tr>
<td>ax</td>
<td>eax</td>
</tr>
</tbody>
</table>

Move with sign, move with zero extension

- Copy from source to larger destination with sign extension:

```
movsFT src, dst
```

- Copy from source to larger destination with zero extension:

```
movzFT src, dst
```

- F and T are the “from” and “to” sizes (either b, w, or l)
- Valid combinations: bw, bl, or wl
- Examples:

  - Copy from source to larger destination with sign extension:

```
movsbw %al, %dx # byte to word
movzwl %ax, %edx # word to long
```
The exchange instruction

• Exchange data between two locations
  \[ \text{xchg}(\text{reg} | \text{mem}), \text{reg} \]

• Consider the following instructions in a high-level language:
  \[
  \text{int tmp = x;}
  \]
  \[
  \text{x = y;}
  \]
  \[
  \text{y = tmp;}
  \]

• If \(x\) and \(y\) are held in registers, then a “clever enough”
  compiler can translate this code into a single \text{xchg} instruction

The instruction pointer, \(\text{eip}\)

• The \(\text{eip}\) register holds the address of the next instruction to
  be executed

• As the processor reads each instruction, it increments the
  value in \(\text{eip}\) by the appropriate number of bytes to point to
  the following instruction

• This mechanism allows the processor to execute a sequence
  of instructions stored in contiguous locations in memory

• What would happen if we “move” a different value in to \(\text{eip}\)?

Jumping and labels

• We can transfer control and start executing instructions at
  address \(\text{addr}\) by using a jump instruction
  \[
  \text{jmp} \ \text{addr}
  \]

• Labels can be attached to instructions in an assembly language
  program:
  
  ```
  a:     \text{jmp} \ b
  b:     \text{jmp} \ a
  c:     ...
  ```

• Modern, pipelined machines work well with sequences of
  instructions that appear in consecutive locations. Jumps can
  be expensive: one of the goals of an optimizing compiler is to
  avoid unnecessary jumps.

IA32 instructions:

arithmetic and logic operations

Arithmetic instructions

• Combine a given \(\text{src}\) with a given \(\text{dst}\) value and leave the
  result in \(\text{dst}\):

  \[
  \begin{array}{l}
  \text{addX} \ \text{src}, \ \text{dst} \\
  \text{subX} \ \text{src}, \ \text{dst} \\
  \text{imulX} \ \text{src}, \ \text{dst} \\
  \text{andX} \ \text{src}, \ \text{dst} \\
  \text{orX} \ \text{src}, \ \text{dst} \\
  \text{xorX} \ \text{src}, \ \text{dst}
  \end{array}
  \]

• Similar to \(\text{dst} += \text{src}\), \(\text{dst} -= \text{src}\), etc., in C/C++

Examples

• To compute \(x^2 + y^2\) and store the result in \(z\):

  ```
  \begin{array}{l}
  \text{movl} \ x, \ %eax \\
  \text{imull} \ %eax, \ %eax \\
  \text{movl} \ y, \ %ebx \\
  \text{imull} \ %ebx, \ %ebx \\
  \text{addl} \ %ebx, \ %eax \\
  \text{movl} \ %eax, \ z
  \end{array}
  ```

  .data

  ```
  \begin{array}{|c|c|}
  \hline
  \text{register} & \text{contents} \\
  \hline
  \text{eax} & x^2+y^2 \\
  \text{ebx} & y^2 \\
  \hline
  \end{array}
  ```

  x: .long 4
  y: .long 3
  z: .long 0
IA32 instructions: conditional execution

Flags
- In addition to performing the required operation, arithmetic instructions also change bits in the eflags register

<table>
<thead>
<tr>
<th>OP</th>
<th>DF</th>
<th>IF</th>
<th>SF</th>
<th>ZF</th>
<th>AF</th>
<th>PF</th>
<th>CF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overflow</td>
<td>Direction</td>
<td>Interrupt</td>
<td>Zero</td>
<td>Adjust</td>
<td>Parity</td>
<td>Carry</td>
<td></td>
</tr>
</tbody>
</table>

(Not to scale. Shaded areas indicate reserved or system fields.)

- The flags record details about the last operation, such as:
  - Was the result zero?
  - Was the result positive?
  - Did a carry occur?
  - etc...

Conditional jumps, jCC

We can test these flags in conditional jump instructions

- jz addr (jump to addr if the zero flag is set)
- jnz addr (jump to addr if the zero flag is not set)
- je addr (jump to addr if equal; same as jz)
- jne addr (jump to addr if not equal; same as jnz)
- jl addr (jump to addr if less than)
- jle addr (jump to addr if not less than)
- jg addr (jump to addr if greater than)
- jge addr (jump to addr if not greater than)

Examples

```
subl %eax, %ebx
jz addr
jnz addr
je addr
jne addr
jl addr
jle addr
jg addr
jge addr
jl addr
```

If the specified condition does not apply, then execution just continues with the next instruction ...

The compare instruction

- The cmpX instruction behaves like subX except that the result is not saved; only the flags are changed
- For example:  `cmpl %eax, %ebx  jl addr`

will jump to addr if the value in ebx is less than the value in eax, but it will not change the values in either register

Other conditional instructions

- There are some other instructions that perform an action based on the conditional flags without the cost of a jump
- `setCC reg8` sets the value in a specified 8-bit register to 0 or 1, based on the condition specified by CC:

  ```
  cmpl %ecx, %ebx # set eax to 1 if
  setl %al      # ebx < ecx, or
  movzl %al, %eax # else to 0
  ```

- `cmovCC src, dst` copies data from the specified src to dst, but only if the condition specified by CC holds:

  ```
  cmpl %ebx, %eax # set eax to the max of
cmovl %ebx, %eax # eax and ebx
  ```

  condition code; no size suffix here!
IA32 instructions: more arithmetic

Unary operations

- The following arithmetic operations have only one argument (which serves as both source and destination)
  - `negX` (reg | mem) negate
  - `notX` (reg | mem) complement
  - `incX` (reg | mem) increment
  - `decX` (reg | mem) decrement

- Like the binary operators, these instructions also set the flags for subsequent testing.

Bitwise shift operations

- Shift operations are handled using instructions of the form:
  - `op count, (reg | mem)`

  - `shl/sal` `cf` shift (logical/arithmetic) left
  - `shr` `cf` shift logical right
  - `sar` `cf` shift arithmetic right

- `count` is either a constant or else the `%cl` register
- In all cases, the `count` value will be masked to 5 bits (0-31)

Example

- Given two 32 bit input values:
  - `base`:
  - `limit`:

- Calculate a 64 bit descriptor:

- (Needed for the calculation of “GDT entries”)

Bitwise rotate operations

- Rotate operations use the same instruction format:

  - `rol` `cf` rotate left
  - `rcl` `cf` rotate left with carry
  - `ror` `cf` rotate right
  - `rcr` `cf` rotate right with carry

- [Aside: Curiously, “higher level” languages often include shift operators, but not rotates, even though the latter have more interesting/uniform behavior …]
Division

• Divide implicit destination (edx:eax) (a 64-bit quantity) by a specified argument with result in eax and remainder in edx

  idivl (reg | mem)

• Often used in conjunction with the cltd instruction (“convert long to double”, a.k.a. cdq), which converts a signed 32-bit value in eax into the corresponding signed 64-bit value in edx:eax.

Example 1

Divide 4,660 (i.e., 0x1234) by 25:

  movl $0x1234, %eax  
  cltd  
  movl $25, %ecx  
  idivl %ecx

Results:

  eax = 0xBA (186)  
  edx = 0xA (10)

Sure enough: 186*25 + 10 = 4,660

Complications of division

• Division produces multiple results: a quotient and a remainder

• Division uses special registers: we’d better not store any other values in eax or edx if there’s a chance that a division instruction might be executed

• Doesn’t set flags: requires separate tests, for example, to determine whether quotient or remainder was zero

• Division can raise an exception if the src is zero (or -1)

IA32 instructions: using the stack

• The IA32 includes features that allow the programmer to use a region of memory as a simple stack:
  • the esp (stack pointer) register
  • special instructions like push, pop, call, ret, ...

• There is no obligation for the programmer to use these features, but it is often convenient to do so:
  • for temporary/scratch storage when a calculation needs more storage than the CPU registers can provide
  • to support calling and returning from functions
A typical memory layout

- A typical operating system reserves an area of scratch memory for each program, and sets the esp register to point to the end of this region when the program begins.

<table>
<thead>
<tr>
<th>program</th>
<th>data</th>
<th>stack</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>esp</td>
</tr>
</tbody>
</table>

- The stack pointer moves:
  - down (decreases) as values are pushed on to the stack
  - up (increases) as values are popped off of the stack

- So long as they never overlap, the data and stack areas can grow or shrink as necessary as the program runs.

Stack operations

- Push a value onto the stack
  \[ \text{pushl } (\text{reg} | \text{mem} | \text{immed}) \]

- Pop a value of the stack
  \[ \text{popl } (\text{reg} | \text{mem}) \]

- Roughly speaking:
  \[
  \begin{align*}
  \text{pushl } \text{src} & = \text{subl } \$4, \%esp; \quad \text{movl } \text{src}, (\%esp) \\
  \text{popl } \text{dst} & = \text{movl } (\%esp), \text{dst}; \quad \text{addl } \$4, \%esp
  \end{align*}
  \]

Spilling temporaries on the stack

- The stack is often used for saving the contents of a register on the stack (“spilling”) so that the register can be used, temporarily, for some other reason.

- For example:
  \[
  \begin{align*}
  \text{pushl } \%eax & \\
  \text{pushl } \%edx & \\
  \text{... code that changes eax and/or edx ...} & \\
  \text{popl } \%edx & \\
  \text{popl } \%eax &
  \end{align*}
  \]

- Note that values on the stack can still be accessed, from memory, using \((\%esp), 4(\%esp), 8(\%esp), 12(\%esp), \ldots\)

Call and return

- There is a special instruction for calling a function
  \[
  \begin{align*}
  \text{call } \text{addr} & = \text{pushl } \$\text{lab} \\
  & \quad \text{jmp } \text{addr} \\
  & \quad \text{lab: ...}
  \end{align*}
  \]

- And a special instruction for returning from a function
  \[
  \begin{align*}
  \text{ret} & = \text{popl } \%eax \\
  & \quad \text{jmp } \star\%eax
  \end{align*}
  \]

- In practice, additional instructions are often needed to deal with parameter passing, etc.

Implementing functions

- How do we pass arguments to a function?
- How does a function return a result?
- How do we handle local variables?

- In principle, especially in a bare metal setting, we can implement these features any way we like, using the basic tools that the IA32 instruction set provides.

- But there are some existing standards we can follow, notably the “System V IA32 Application Binary Interface (ABI)”: http://www.sco.com/developers/devspecs/abi386-4.pdf particularly Section 3-9.

Functions and the System V ABI
Stack frames

The code for any given function/procedure call runs in the context of a stack frame of the form:

```
<table>
<thead>
<tr>
<th>l_n</th>
<th>...</th>
<th>l_1</th>
<th>old</th>
<th>retn</th>
<th>a_1</th>
<th>...</th>
<th>a_n</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>esp</td>
<td>-4</td>
<td>ebp</td>
<td>4</td>
<td>8</td>
<td>12</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

- **Frame (base) pointer**: ebp points to the stack frame; the caller’s frame pointer is stored in old (i.e., (%ebp))
- **Return address**: retn is the return address
- **Actual parameters**: a_1, ..., a_n are the function’s arguments. We can access a_1 as 8(%ebp), etc...
- **Local variables**: l_1, ..., l_m are the function’s local variables. We can access l_1 as -4(%ebp), etc...

Building the stack frame … in the caller

```
<table>
<thead>
<tr>
<th>a_1</th>
<th>...</th>
<th>a_n</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>esp</td>
<td>ebp</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

- The **caller** starts by pushing the arguments:
- Then it executes a call instruction, which pushes the return address:
- ... and jumps to the code for the callee ...

Building the stack frame … in the callee

```
<table>
<thead>
<tr>
<th>retn</th>
<th>a_1</th>
<th>...</th>
<th>a_n</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>esp</td>
<td>ebp</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

- The **callee** saves the old frame pointer, and sets a new value:
- Then it decrements the stack pointer to reserve space for any local variables:
- ... and now the callee can start work ...

Function prologue

The code that builds the stack frame at the start of a function body is called the prologue:

- At the beginning of a function body, the parameters and return address have already been pushed on to the stack. We need to:
  - pushl %ebp       # save old frame pointer
  - movl %esp, %ebp  # and set new value
- If local variables taking M bytes of storage are required, then we need to reserve space for them:
  - subl $M, %esp    # allocate space for locals (skip if M=0)

Function epilogue

When a function completes, we must dismantle the stack frame and return the machine to the state it was in before the call. The code to do this is called the epilogue:

- Running the previous process in reverse:
  - movl %ebp, %esp # discard locals/temps
  - popl %ebp # restore frame pointer
  - ret # return to caller
- The first two instructions here can be replaced with the more efficient, but otherwise equivalent leave instruction

Removing the parameters

- Once we return to the caller, the result of the function is in eax, but the parameters are still on the stack:
- We restore the stack pointer to its original value by adding on the number of bytes that are used by the parameters:
  - addl $N, %esp
- If no parameters were passed, then this step can be omitted
Example: a leaf function

```c
int g(int u) {
    return u*u;
}
```

Example: multiple parameters + call

```c
int f(int x, int y, int z) {
    return g(x+y);
}
```

Example: spilling

```c
int h(int x, int y, int z) {
    return g(x)+g(y);
}
```

Observations

- There is a four instruction overhead for each function that uses the frame pointer
  - Increases execution time
  - Prevents use of ebp as a general purpose register
  - For larger functions, the four instruction overhead is less of an issue
  - For small functions, we would prefer to inline rather than copy
  - Nevertheless, it is common to produce code that doesn’t use ebp as a frame pointer (e.g., `-fomit-frame-pointer` in gcc)

Caller and callee saves

We (System V) can designate some registers as:

- **caller saves** (eax, ecx, and edx)
  - can be freely used by the callee
  - the caller is responsible for saving (and later restoring) the value of a caller save register before a call

- **callee saves** (ebp, ebx, esi, and edi)
  - can be freely used by the caller
  - the callee is responsible for saving (and later restoring) the value of a callee saves register before using it to store temporary values

Revisiting the previous example: `h`

```c
int h(int x, int y, int z) {
    return g(x)+g(y);
}
```
Revisiting the previous example: h

```c
int h(int x, int y, int z) {
    return g(x)+g(y);
}
```

...we can move it to a callee saves register, esi
g will preserve the value in esi, if necessary
so it will still contain the correct value here...

Assembly “Language”?

• Highly imperative, primitive instructions, no expressions

• No high-level abstractions, but all the building blocks:
  • No arrays, records, variants, objects, closures, …
  • No loops, switch statements, functions, local variables, …

• Type System?
  • Values classified by size (e.g., 8 vs 32 bits) and storage class
    (e.g., memory, flag, integer register, floating point register, …)
  • Limited protection against common programming mistakes
  • Programmer has full control over data representation

Summary

• IA32 provides a very basic programming language:
  • A fixed set of registers
  • Instructions for moving and operating on data
  • Instructions for testing and control transfer

• In programming language terms:
  • Low-level, primitive instructions, loosely typed
  • No high-level abstractions, but all the building blocks
  • Very close to the metal, low-level control, “predictable” performance

• Let’s write some programs!