

CSE 240

Retrospective

Fall 2006

Big Picture

Hardware

- Representing data, transistors, digital logic structures, von Neumann machine model

Assembly language

- Instructions, (structured) programming, input/output, *relationship to hardware*

C programming

- Syntax, operators, control structures, functions, pointers, data structures, *relationship to assembly language*

Today's Agenda

Course retrospective

- Revisit our bottom-up journey

Format and content of final exam

- Comprehensive, open book, similar format as midterm

Course evaluations

- Tells me what worked; what to improve for next time

Pizza!

Friday: four big concepts in processor design

- Caches, virtual memory, pipelining, multi-threading/-processing

CSE 240

2

We've Come a Long Way...

How do computers work?

- Now you know!

Bottom-up approach

- Bits are bits
- Transistors
- Digital circuits (gates, latches, memories, state machines)
- Processor datapath
- Instructions
- Assembly programming
- C programming
 - Relationship to assembly
 - General non-safety of C

CSE 240

3

CSE 240

4

Beyond the Book

Transistors as pneumatic valves

Datapath

- Single-cycle datapath

New LC-3 simulator

New I/O devices

- Video output
- Timer

Operating system (SnakeOS)

- Unix history
- Input/output
- Trap table
- Memory protection with Memory Protection Register (MPR)

C Programming

- Comparisons to Java
- More function call stack discussion
- Security ramifications of C (smashing the stack example)
- Heap management discussion (malloc/free & garbage collection)

CSE 240

5

Microsoft TechNet

[TechNet Home](#) > [TechNet Security](#) > [Security Advisories](#)

Microsoft Security Advisory (929433)

Vulnerability in Microsoft Word Could Allow Remote Code Execution

Published: December 5, 2006

[Top of section](#)

Microsoft is investigating a new report of limited "zero-day" attacks using a vulnerability in Microsoft Word 2000, Microsoft Word 2002, Microsoft Office Word 2003, Microsoft Word Viewer 2003, Microsoft Word 2004 for Mac, and Microsoft Word 2004 v. X for Mac, as well as Microsoft Works 2004, 2005, and 2006.

In order for this attack to be carried out, a user must first open a malicious Word file attached to an e-mail or otherwise provided to them by an attacker.

What causes the vulnerability?

When a user opens a specially crafted Word file using a malformed string, it may corrupt system memory in such a way that an attacker could execute arbitrary code.

CSE 240

6

The New York Times
nytimes.com

PRINTED FROM THE NEW YORK TIMES
SPONSORED BY
GERCH BLANCHETT
WRESTLING

December 6, 2006

Spam Doubles, Finding New Ways to Deliver Itself

By BRAD STONE

Hearing from a lot of new friends lately? You know, the ones that write "It's me, Esmeralda," and tip you off to an obscure stock that is "poised to explode" or a great deal on prescription drugs.

Spammers have effectively foiled the first strategy — analyzing the reputation of the sender — by conscripting vast networks of computers belonging to users who unknowingly downloaded viruses and other rogue programs. The infected computers begin sending out spam without the knowledge of their owners. Secure Computing, an antispam company in San Jose, Calif., reports that 250,000 new computers are captured and added to these spam "botnets" each day.

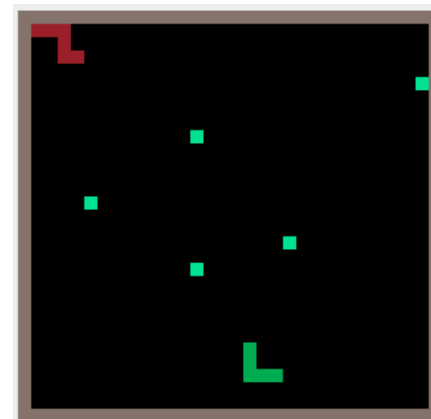
CSE 240

7

Remember the Demo the First Class?

Homework 6 & 7

- Build Snake in assembly language!



CSE 240

8

Course Assignments

Hardware

- HW#1: Data types
- HW#2: Digital logic
- HW#3: Hardware state machines
- HW#4: LC-3 instructions

Assembly Programming

- HW#5: Basic assembly
- HW#6: BreakOS
- HW#7: BreakOut

C Programming

- HW#8: LC-3 Disassembler
- HW#9: LC-3 Assembler

This year's CSE240

3rd time for "new" CSE240

- New textbook
- New lectures
- New assignments
- *etc.*

Course statistics

- ~90 students
- 37 lectures (Thanks to Professor Lewis for three of them)
- 100+ hours of "office hours" (TAs and instructors)
- 1100+ e-mail messages in my "cse240" folder
 - 11+ e-mails per day!
- 300+ messages on the forum

Final Exam Format

Similar format as midterm exam

- Questions that span multiple concepts
- Synthesis of knowledge

...but relatively shorter

- Slightly longer exam, but 120 minute final vs 50 minute midterm

Open book/open note

- But study like it is not open book
- Use only as a reference and safety net

Final Exam Topics

Comprehensive

- With more of a focus on assembly and C
 - Especially relationship between assembly and C
 - Especially *pointers, structs, function calls, and runtime stack*
- Relationship between assembly/C and hardware

Types of questions

- Write an assembly or C function to do something
- Translating C to LC-3 assembly
 - Much like HW#6 & HW#7, but using C for pseudocode
- Translating LC-3 assembly to C code
- C to C translation
 - Convert a `while` loop to a `for` loop
- What does this code/circuit do? (circuit, assembly, C code)
- State machines (saw them in hardware & a C code example)
- Some second-chance questions from midterm exam
 - Example: datapath question from midterm

Preparing for Exam

Review material

- Book (don't forget Ch. 19!)
- Notes
- Midterm
- Homeworks

Work example questions

- End of chapter exercises (some answers online)
- Exam from last two years

Optional review session

- Time and place TBD (although I've tried...)

What's Next? Courses Beyond CSE240

Perhaps, nothing...

- An explicit course goal:
 - broad overview for students not continuing
- Touch on big ideas, bottom-up, no magic

CSE371/372: Computer Architecture

- Focus on performance and design of processors
- Caching, pipelining, parallelism, I/O devices, virtual memory
- Lab: design a processor in a hardware description language (HDL)

CSE380/381: Operating Systems

- Concepts of operating systems: threading, protection, file system, etc.
- Lab: write a Unix "shell", implement parts of an operating system

CSE341: Compilers

- Translating a Java-like language to a real assembly language
- Automating much of what we talked about
- Techniques for parsing, translating, and optimizing code

Many other courses build on this course

- For example: networking, security, databases, embedded systems, etc.

Remainder of Today and Friday

Course evaluations

- Give us your feedback
- New-ish format
 - We spent a lot of effort to try avoid rough edges
 - Tell us what to do better next time!

Pizza!

Friday:

- One lecture on the fundamental issues in processor design
- Caches, virtual memory, pipelining, multi-threading/-processing
- For those continuing *and* those not continuing in CSE