¡iClickers!

How many CS classes are you planning on taking in the fall?

A. 1
B. 2
C. 3
D. 4
E. none :(
Administrivia

- Review Session TONIGHT – 306 Soda, 6:30-9:30pm

- Homework 13 (last HW!) due TONIGHT – 11:59pm

- Wed/Thurs (8/12) Sections converted to office hours/general review

- Final THURSDAY 8/12, 155 Dwinelle, 7-10pm
Part I: Therac Case Study
Figure 9  Typical Therac-25 Facility
What happened?

• 6 accidents – serious burns

• 4 deaths

• Otherwise effective – saved hundreds of lives
Lesson to be learned

- Social responsibility in engineering
- First real incident of fatal software failure
- What is good software engineering?
Lesson in Ethics?

• Not that simple...

• There were no bad guys

• Honestly believed there were no issues

• But something was clearly wrong... 
  ...so why couldn't they see it?
“Software Rot”

• Other engineering fields: clear sense of degradation and decay

• Software doesn't become brittle or fractured... does it?

• Phenomenon of software degrading after time
A bigger picture

• All software is part of a bigger system

• Software degrades because:
  • Other piece of software changes
  • Hardware changes
Ex: Compatibility Issues

This program has known compatibility issues

Check online to see if solutions are available from the Microsoft website. If solutions are found, Windows will automatically display a website that lists steps you can take.

Publisher: Symantec
Location: C:\Users\laptop\AppData\Local\Temp\NIS15.5.0.23\Setup.exe

Norton Internet Security ver. 2007 and 2008 is incompatible with this version of Windows. For more information, contact Symantec.
A bigger issue

• The makers of the Therac did not fully understand the complexity of their software

• Characterized by intricate web of dependencies and relations

• Other engineering disciplines – complexity of their creations are more apparent
A “simple” program

• One of my favorites...

• Spider Solitaire
This program can delete any file you can.
Complexity and You

• Hyper-technological modern society

• Limitless reach of software complexity

• Is every piece of software lethal?
Problems with Therac-25

• No atomic test-and-set

• No more hardware interlocks

• Abundant user interface issues
UI Problems

- Cursor position and form entry
CalNet Login

Note: Your CalNet Passphrase is case sensitive.

CalNet ID: 

Passphrase: 

 Warn me before logging me into other applications. (?)

Authenticate

Have you personalized your CalNet ID yet?  
If not, you can do so by going to the 
CalNet Change ID Application (authentication required)

If you are having persistent problems authenticating using your CalNet ID and passphrase, please contact the CalCard Office at calnet@berkeley.edu, 180 Ceser Chavez Center, Lower Sproul, (510) 643-6839, (M-F, 9-5). For answers to general questions about using this service, please see the IST Knowledge Base section entitled CalNet Central Authentication Service (CAS).

Copyright © 2009 The Regents of the University of California. All rights reserved.
UI Problems

• Cursor position and form entry

• Default values
UI Problems

- Cursor position and form entry
- Default values
- Too many error messages
When you send information to the Internet, it might be possible for others to see that information. Do you want to continue?

☑ In the future, do not show this message.

Yes  No
When you see a dialog box like this, click ‘Yes’ to make it go away. If available, click the checkbox first to avoid being bothered by it again.

☑️ In the future, do not show this message.

[Yes] [No]
How would you solve these?

- Cursor position and form entry
- Default values
- Too many error messages
Problems with Therac-25

• No atomic test-and-set
• No more hardware interlocks
• Abundant user interface issues
• Bad documentation
• Organization Response
How do we solve these problems?

• One idea:
  • Responsible programming

• Big idea:
  • Redundancy
(define (mc-eval exp env)
  (cond ((self-evaluating?...
       ((variable?...
      
      
      
      (else
       (error "Unknown exp"...
How do we solve these problems?

- Redundancy
- Know your user
- Fail-Soft (or Fail-Safe)
- Audit Trail
- Correctness from the start
Correctness from the start

• Edsger Dijkstra: “On the Cruelty of Teaching Mathematics”

• CS students shouldn't use computers

• Rigorously prove correctness of program
Verification Techniques

• Correctness proofs

• Compilation (pre-execution) analysis
Debugging Techniques

• Black box debugging

• Glass box debugging

• Don't break what works

• And the golden rule of debugging...
“Debug by subtraction, not by addition”

Prof. Brian Harvey
Can you think of examples?

• Redundancy

• Know your user

• Fail-Soft (or Fail-Safe)

• Audit Trail

• Correctness from the start
Break
¡Clickers!

Which project was your favorite?

A. 1 – Twenty-one
B. 2 – Painter language
C. 3 – Adventure game
D. 4 – Logo interpreter
E. All of them! :)}
Big Ideas

• Redundancy
• Know your user
• Fail-Soft (or Fail-Safe)
• Audit Trail
• Correctness from the start
Flashback: MapReduce
Failure?

Is this even an issue?
Warehouse Scale Computing
Let's say you have... 50,000 servers. Each server has four disks. On average, how often do you get a disk failure?

A. Once per year
B. Once per month
C. Once per week
D. Once per day
E. Once per hour
Failure rate of disk is 2%-10% per year. Let's assume 4%. In one year, 4% of 200,000 disks fail = 8,000 disks. There are 8,760 hours in a year.

A. Once per year
B. Once per month
C. Once per week
D. Once per day
E. Once per hour
Warehouse Scale Computing

Google is estimated to have 900,000 servers.

Is failure even an issue? Yes.
Redundant redundancy

• How do they deal with a worker failing?

• Answer: redundancy

• When a worker fails, one of its “superiors” (a scheduler node) assigns a new worker to complete its task.
Redundant redundancy

• How do they know a worker has failed?

• Answer: redundancy

• Workers are programmed to periodically report to their superiors

• If a worker falls “silent”, it is no longer capable of operating
Redundant redundancy

• How can they always replace downed workers?

• Answer: redundancy

• Hundreds of thousands of possible replacements

• What is the result of all of this?
Redundant redundancy

• How can they always replace downed workers?

• Answer: redundancy

• Hundreds of thousands of possible replacements

• What is the result of all of this?

• Answer: When was the last time Google search was down?
Safe Browsing

• Let's say you visit some website... like Facebook

• How do you know it's really Facebook, and not some evil site that only looks like Facebook?
Safe Browsing

• Answer: Website certificates

• Verify through a trusted 3\textsuperscript{rd} party that website displays correct certificate

• What if website has been certified by 3\textsuperscript{rd} party that is not necessarily trusted?

• What if we can't receive the certification at all?
Fail-Safe Defaults

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

- Click here to close this webpage.
- Continue to this website (not recommended).
- More information
Questions?