Trust, Safety and Reliability

CS 340, Fall 2014
Ch. 5 in Ethics in a Computing Culture

Ch. 5 Topics

• Computer reliability can be a matter of life or death
• Exploring the various ways people trust computer and technology to perform tasks for them & the things that can go wrong.
• Examining failures
• Approaches to minimize risks

The Apocalypses That Might Have Been

Lt. Colonel Stanislav Petrov
Overview: Causes of Computer Failure
• A computer might fail to meet expectations by:
  – Hardware errors (malfunction)
  – Software errors (bugs)
  – Being programmed to solve the wrong problem (programmers fail to deliver client expectations)
  – Misuse (a computer is provided erroneous data)
  – Communication failure (human misunderstands a computer prompt)
  – Malice (hackers)

Has a part in your computer (or your close family member’s) ever failed?
A. Yes, hard drive
B. Yes, battery
   wouldn’t charge / power supply issue
C. Yes, motherboard
D. Yes, input device
E. Nope, nothing has ever failed us.

Hardware errors
• Physical components of the system
Software Errors

- “Bugs”

- Bug v. mistake debate

Bugs and Public Safety

- **Safety-critical software**: software that may affect someone’s safety if it fails to work properly
- **Decision point**: a place in computer code where the next instruction executed depends on input data
- **Control programs**: programs that control some sort of machinery
- **Real time**: a program must do something within a specific amount of time
- **Multi-process**: programs that execute at the same time as one or more other programs

Software errors

- Pages 152-154
  - In 2005, Ariane 5
    - [Ariane 5 explosion – YouTube](#)
    - Floating point number storage
      - Arithmetic overflow
  - Pages 155-156
    - In 1994, Intel Pentium chip
      - Certain floating point numbers when divided produced invalid results

- Did Intel have a moral obligation to replace the defective Pentium 5 chips, even for those users who had no need for high precision?
- When employees of Intel first discovered the bug, did they have an ethical responsibility to make the problem public?
Computer Solves the Wrong Problem

- Complexity of programming: garbage in, garbage out
- Gemini 5, 105 miles off landing target:
  - Earth’s rotation is not 360° in 24 hr but 360.98°
- Friendship 7, 40 miles off landing target:
  - Failure to take into account weight loss in aircraft due to use of consumables

Suppose two records for individuals in a database, indicate that share the same last name, birthday, height and weight, similar tattoo and placement, and their reported SSN are off by only 1 digit. Once individual’s first name is Enrique and the other is Emiliano.

Would you think it was possible that the computer system had a error, and that these two people were actually the same person?

A. Yes
B. No

Misuse

The Hernandez situation:
- Emiliano Hernandez was pulled over running a stop sign
- When the officer ran his license the officer was convinced that he was dealing with a wanted man, “Enrique” Hernandez
- Shared same birthday, similar height/weight, tattoo. SSN numbers different by 1 digit...
- Officer was convinced that the name difference was a mistake in the system. It was not.
Communication Failure

• Misunderstandings
  – Of what the system is capable of or how it works
    • Book example – airplane computer monitoring
    • http://en.wikipedia.org/wiki/Gimli_Glider

Review: In the airliner situation, the communications failure related to
A. Airplane weight and balance
B. Airspeed indicator
C. Unit of measurement of jet fuel
D. Planned trip time
E. All of the above

Malice

• With ill intent people destroy or modify computer systems.
• Can be for-profit crime, terrorism, or warfare

• Ex. Target data stolen in Nov/Dec 2013
Malware

- **Malware**: short for “malicious software”
- **Hackers**: people who write and deploy malware
- **Worm**: program that makes copies of itself and propagates those copies through a network to infect other computers
- **Virus**: similar to a worm, but resides in another program (program that must execute in order for the virus to propagate)

Malware (continued)

- **Spyware**: program that is secretly installed for the purpose of collecting information about the computer’s user or users
- **Trojan horse**: software that masquerades as an innocent or useful program, but that is actually designed for a malicious purpose
- **Rootkit**: program that embeds itself into a computer’s operating system and acquires special privileges that would normally be available to the operating system

Intrinsic & Extrinsic software

- **Intrinsic**:
  - Software that is part of a completed product
- **Extrinsic**:
  - Loaded onto the computer or machine of the user, user directly encounters
Important Case Study: The Therac-25

- Radiation therapy machine
- Typical system malfunctions number 40x day

The Therac-25 case cont’d

- 20 month period, overdoses to 6 patients, directly killing 3.
- Previous models, 6 & 20
  - Differences to the 25?
- Chronology of accidents
  - Please see http://computingcases.org/case_materials/therac/supporting_docs/therac_case_narr/therac_toc.html

What was wrong with the Therac-25 programming?

- 2 modes
  - X-ray: high intensity beam deflected by tungsten target
  - Electron: removes tungsten & reduces beam intensity by factor of 100
- Quickly changing* (data entry editing) between mode resulted in electron mode not dropping the beam intensity
  - *If the operator was able to edit and start < 8 seconds
- Use of a Race condition – 2 or more tasks sharing a variable, order that each is encountered can affect behavior of the program
  - The Therac-25 no longer had the hardware safety feature
The software used by the Therac 25 was
A. Intrinsic
B. Extrinsic

Therac 25

- Problems
  - No fail safe
  - No dose reporting
  - Complicated programming
  - Re-use of code

Why were these software problems not detected in the Therac 20 system?
A. The Therac 20 was never used
B. The Therac 20 had a hardware control safeguard that engaged
C. The Therac 20 had different software that did not have the error
Who had moral and/or legal responsibility?

- Harm clearly shown. Was there intent? No
  - So we consider tort of negligence
- Defining negligence from law.com
  - n. failure to exercise the care toward others which a reasonable or prudent person would do in the circumstances, or taking action which such a reasonable person would not
- Must prove:
  - "(a) that the party alleged to be negligent had a duty to the injured party—specifically to the one injured or to the general public, b) that the defendant’s action (or failure to act) was negligent—not what a reasonably prudent person would have done, c) that the damages were caused ("proximately caused") by the negligence. An added factor in the formula for determining negligence is whether the damages were "reasonably foreseeable" at the time of the alleged carelessness"

Opinion: Do you think the manufacturer (AECL) was legally negligent?
A. Yes
B. No
C. Unsure

Opinion: Do you think the operators of the machines (nurses) were legally negligent?
A. Yes
B. No
C. Unsure
Opinion: Do you think the hospitals (such as the East Texas Cancer Center) were legally negligent?
A. Yes
B. No
C. Unsure

Opinion: Do you think the FDA was legally negligent?
A. Yes
B. No
C. Unsure

Opinion: Which of these bear moral/ethical responsibility?
A. AECL (mfr.)
B. Nurses/operators
C. Some of the hospitals
D. FDA
E. All of the above
Extrinsic Software Failures

- With these examples, companies or individuals are buying software for what it can do for them.
  - Disclaiming liability for problems through warranties

Software Warranties

- Limiting liability to:
  - A refund of the purchase price
  - Repair of the software product
- Accepting no liability for
  - Business losses arising out of the use of the product
- Enforceability of these disclaimers?
  - UCC & the Magnuson-Moss Warranty Act
  - Mix of case law

Mortenson v. Timberline Software

- Precision Bid software
- Used it and created bid $1.95 million too low
- Licensing disclaimed business losses related to use of the software in excess of licensing fee
- Timberline was aware of bug, did not send fix to Mortenson.
- Ct. found the Timberline was not liable b/c licensing agmt. properly limited liability.
Does it bother you that software companies can more easily waive liability than other product manufacturers?

A. Yes
B. No