Bugs, errors, risks

CS 594 Special Topics/Kent Law School:
Computer and Network Privacy and Security: Ethical, Legal, and Technical Considerations

Even without black hats

- System designers make mistakes
- Data entry errors
- Murphy
- Software-based systems inherently daedal

Facts about Computer Errors

- Error-free software is not possible
  - But software can have very different rates of error
  - Errors can be reduced by following good software engineering procedures/practices
- Errors are often caused by more than one factor
- Line between tolerable and/or unavoidable errors versus careless software development blurry but exists

My opinions on software errors

- Discrete versus continuous math leads to fewer 9's of reliability.
- 1975 Bridge over roadway not crashing; POTS (Plain-old-telephone system): easily 0.99999 chance that if you picked up phone, you got a dial tone.
- Not true of Windows XP! Nor Mac OS X

Database entry and/or retrieval errors

- November 2000 general election Florida disqualified 1000s of voters charged with **misdemeanors**; **probably changing outcome of Presidential Election**
- False arrests because of errors among 40 million entries in National Crime Information Center (NCIC)
  - But 10,000s of recovered stolen cars too.

Database Error Causes

- Large population ⇒ Name collisions
- Human common sense not part of automated processing
- Errors in data entry
- Overconfidence in accuracy of data from a computer
- Information not updated or corrected
- Lack of accountability for errors

System Failures

- Communications: Telephone, online, broadcast
  - 1990: AT&T disrupted 9 hours; 50 million failed calls; bug in 4 million line program.
  - AT&T Official Report: “While the software had been rigorously tested in laboratory environments before it was introduced, the unique combination of events that led to this problem couldn’t be predicted.”

More Famous System failures

- Ariane 5 satellite launch vehicle (France) 1996; conversion of 64-bit float to 16-bit signed int oveflowed; exception not handled. (Code reused as-is from Ariane 4, where value was guaranteed to be small enough)
  - Loss: $500 million of satellites
- CTB/McGraw-Hill software error messing up NYC test score results—showed way down when up 5%
- Robot mission to Mars, 1999, metric-British clash

System failures: Airports

- Denver airport opening delayed 4 times, cost of $30 million/month of delay. Most of delay computer-controlled baggage system, $200 million of $3.2 billion airport.
  - Spec: outbound checked luggage in < 10 minutes on carts at 19 mph on 22 miles of underground tracks. Laser scanners tracking 4000 carts
  - Nobody expects software/hardware system of this complexity to work right first time

Denver fiasco

- Real-world problems: scanners got dirty, knocked out of alignment
- Problems in other systems: Airport electrical system could not handle power surges associated with baggage system; massive circuits blowing
- Software errors (needed carts routed to waiting pens)
- Overall: *Inadequate development and testing time; significant changes in specs after project start*

DIA final outcome

- In June 2005, United Airlines scrapped the trouble-plauged automated baggage system.
- Returned to manual baggage handling after having spent about $200 million
- Return to manual baggage handline estimated to save $1 million/month in system maintenance costs, and more in cossts of misdirected and damaged bags.

When will they ever learn?

- More ambitious plans for Hong Kong and Kuala Lumpur (Malaysia) airports
  - Ambitious, complex computer systems to manage *everything:* moving 20,000 pieces baggage/hour, coordinating and scheduling crews, gate assignments for flights, etc.
- Both failed spectacularly

Voting

- Almost 2 million ballots not counted in 2000 U.S. Presidential election because they registered no choice or multiple choices
- Minor dispute in Florida over exact count
- These problems demonstrated problems of traditional paper ballots
- Led to 2002 Help America Vote Act; replacement of punch cards

Direct Recording Electronic (DRE) Voting Machines

- Many states including IL used HAVA funds to buy DRE voting machines
  - Touch screen; *no paper audit trail*
- Numerous voting irregularities linked to DRE voting machines in 2002, 2004, 2006, some clearly due to programming errors; some cause unknown
- Machine makers code secret as valuable trade secret
- May 2007: Florida legislature voted to replace DRE with optical scan

System failure causes

- Insufficient testing and debugging time
- Significant changes in specifications (after project begun)
- Overconfidence in system
- Project mismanagement

Saftey-Critical Applications

- Aircraft; Trains
- Military
- Power plants
- Automated Factories
- Medicine
- Etc.

Causes of safety-critical failures

- Overconfidence
- Lack of override features
- Insufficient testing
- Sheer complexity of the system
- Mismanagement

Therac-25 overview

- Therac-25 was a software controlled radiation therapy machine used to treat people with cancer.
- Resulted in overdoses of radiation
  - Normal dosage 100–200 rads.
  - ≥6 people got estimated 13,000–25,000 rads
  - Three of the six known people died.
- Important to study to avoid repeating the errors
- Manufacturer, programmer(s), hospitals/clinics all share some of the blame

Therac-25: multiple causes

- Poor safety design
- Insufficient testing and debugging
- Software errors
- Lack of safety interlocks
- Overconfidence
- Inadequate reporting and investigation of accidents

Therac-25 Software & Design Problems

- Re-used software from older systems, unaware of bugs in previous software
- Weaknesses in design of operator interface
- Inadequate test plan
- Bugs in software
  - Allowed beam to deploy when table not in proper position
  - Ignored changes and corrections operators made at console

Therac-25: Why So Many Incidents?

- Hospitals had never seen such massive overdoses before, were unsure of the cause
- Manufacturer said the machine could not have caused the overdoses and no other incidents had been reported (which was untrue)
- The manufacturer made changes to the turntable and claimed they had improved safety after the second accident. The changes did not correct any of the causes identified later

Why So Many Incidents (cont.)?

- Recommendations were made for further changes to enhance safety; the manufacturer did not implement them
- The FDA declared the machine defective after the fifth accident
- The sixth accident occurred while the FDA was negotiating with the manufacturer on what changes were needed

What goes wrong in general?

- Computer Systems fail because:
  - The job they are doing is inherently difficult
  - The job is done poorly
- Compounding the reliability issue:
  - Developers and Users exhibit overconfidence in the system
  - Reused system software may not work in different environments

Professional Techniques

- Follow good software engineering practices
- Take human factors into account, especially construct well-designed user interfaces
- Incorporate self-checking where appropriate, redundancy in saftey/wealth-critical systems
- Follow good testing principals and techniques

A little better all the time?

"… large software project failures: it has been known for years that perhaps 30% of large development projects fail [24], and this figure does not seem to change despite improvements in tools and training: people just built much bigger disasters nowadays than they did in the 1970s."

Anderson, Crypto 07 Keynote

Vs. Standish Group, which tracks 1000s of IT Projects

1994: 31% failed (cancelled before completion); 16% on time & in budget

2006: 19% cancelled, 35% on time & in budget

Increasing Reliability?

- Would forced real warranties help?
  - When I was in law school in the Dark Ages, used to be something called UCC, and Magnusun-Moss.
- Professional Licensing of software engineers a current controversial discussion

For more info

- Peter G. Neumann's "Inside Risks" email/web site has been the source where sad and scary stories have been collected since the 1980s.