Announcements

- LA-8 due Tuesday
- LA-8 Challenge A edit
- OP Option
- Syllabus 1.7 posted

Last Time

- Passwords
  - Cracking
  - Entropy
- Info Security Best Practices
  - Personal Information
  - Financial Transactions
  - Security Questions
  - Browser Settings
  - Emails
  - Online Accounts
  - Networking
  - Computers
  - Devices

Today

- Password salt
- Computer Failures
  - lost time, lost money, injury, or even death
  - Studying failures a way to appreciate complexity of building reliable computerized systems
  - Data entry errors
  - Data interpretation errors
  - Software and billing errors
  - Notable software system failures
- Computer simulations
- Software engineering
- Software warranties and vendor liability

Password Salt

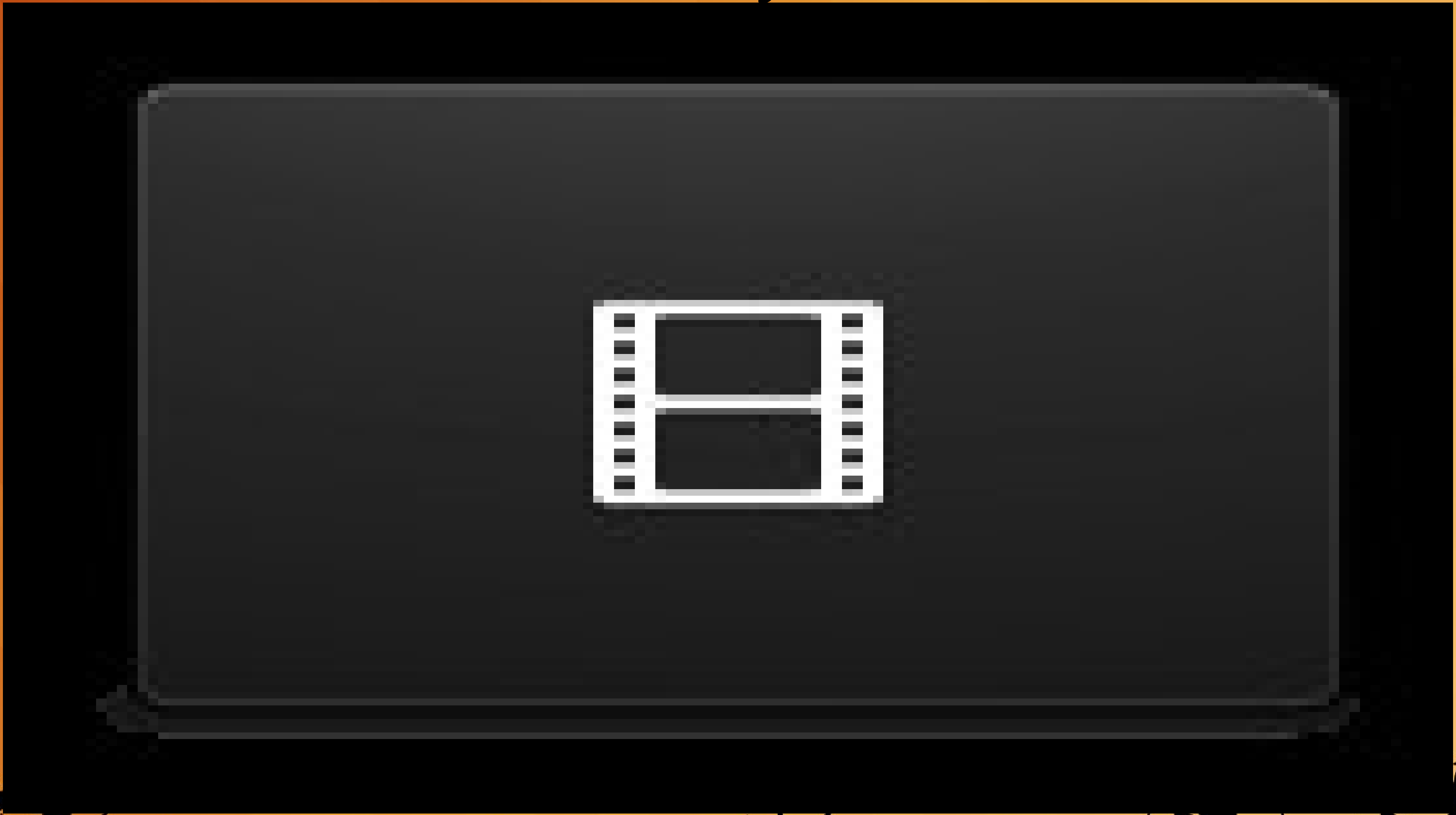
- Passwords stored as hashes
  - Vulnerable to dictionary and Rainbow Tables
- Salt is a random string added before hashing
  - Password: superman
  - Salt: T$3d
  - New password: supermanT$3d
- Salt added on the backend when the password is hashed
- User does not know about it
- Salt also added when challenging password
- Hash is now changed
  - Pre-computed tables worthless

Computer Failures

- Lost time, lost money, injury, or even death
- Studying failures a way to appreciate complexity of building reliable computerized systems
- Data Failures
  - Incorrect data entry
  - Incorrect data interpretation

Data Entry Errors

Data Entry Errors



Disenfranchised Voters

- November 2000 general election
- Florida disqualified thousands of voters
- Reason: People mistakenly identified as felons
- Cause: Incorrect records entered in voter database
- Consequence: May have affected outcome of national presidential election

False Arrests

- Sheila Jackson Stossier mistaken for Shirley Jackson
  - Arrested and spent five days in detention
- Roberto Hernandez mistaken for another Roberto Hernandez
  - Arrested twice and spent 12 days in jail
- Terry Dean Rogan arrested after someone stole his identity
  - Arrested five times, three times at gun point

Accuracy of NCIC Records

- March 2003: Justice Dept. announces FBI not responsible for accuracy of NCIC information
- Exempts NCIC from some provisions of Privacy Act of 1974
- Should government take responsibility for data correctness?

Dept. of Justice Position

- Impractical for FBI to be responsible for data's accuracy
- Much information provided by other law enforcement and intelligence agencies
- Agents should be able to use discretion
- If provisions of Privacy Act strictly followed, much less information would be in NCIC
- Result: fewer arrests

Position of Privacy Advocates

- Number of records is increasing
- More erroneous records → more false arrests
- Accuracy of NCIC records more important than ever

Act Utilitarian Analysis: Database of Stolen Vehicles

- Over 1 million cars stolen every year
- Just over half are recovered, say 500,000
- Assume NCIC is responsible for at least 20%
- 100,000 cars recovered because of NCIC
- Benefit of $5,000 per car (owner gets car back; effects on national insurance rates; criminal doesn’t profit)
- Total value of NCIC stolen vehicle database: $500 million/year

Act Utilitarian Analysis: Database of Stolen Vehicles

- Only a few stories of false arrests
- Assume 1 false arrest per year (probably high)
- Assume harm caused by false arrest $55,000 (size of award to Rogan)
- Benefit surpasses harm by $499,945,000/year
- Conclusion: Good to have NCIC stolen vehicles database

Errors When Data Are Correct

- Assume data correctly fed into computerized system
- System may still fail if there is an error in its programming

Errors Leading to System Malfunctions

- Qwest sent incorrect bills to cell phone customers
- Faulty USDA beef price reports
- U.S. Postal Service returned mail addressed to Patent and Trademark Office
- Spelling and grammar error checkers increased errors
- New York City Housing authority overcharged renters
- About 450 California prison inmates mistakenly released

Errors Leading to System Failures

- Ambulance dispatch system in London
- Japan’s air traffic control system
- Los Angeles County + USC Medical Center laboratory computer system
- Boeing 777 (Malaysia Airlines flight)
- NASDAQ stock exchange shut down
- Insulin pump demo at Black Hat conference
- Jeep Cherokee

Analysis: E-Retailer Posts Wrong Price, Refuses to Deliver

- Amazon.com in Britain offered iPaq for £7 instead of £275
- Orders flooded in
- Amazon.com shut down site, refused to deliver unless customers paid true price
- Was Amazon.com wrong to refuse to fill the orders?

Rule-Utilitarian Analysis

- Imagine rule: A company must always honor the advertised price
- Consequences
  - More time spent proofreading advertisements
  - Companies would take out insurance policies
  - Higher costs → higher prices
  - All consumers would pay higher prices
  - Few customers would benefit from errors
- Conclusion
  - Rule has more harms than benefits
  - Amazon.com did the right thing

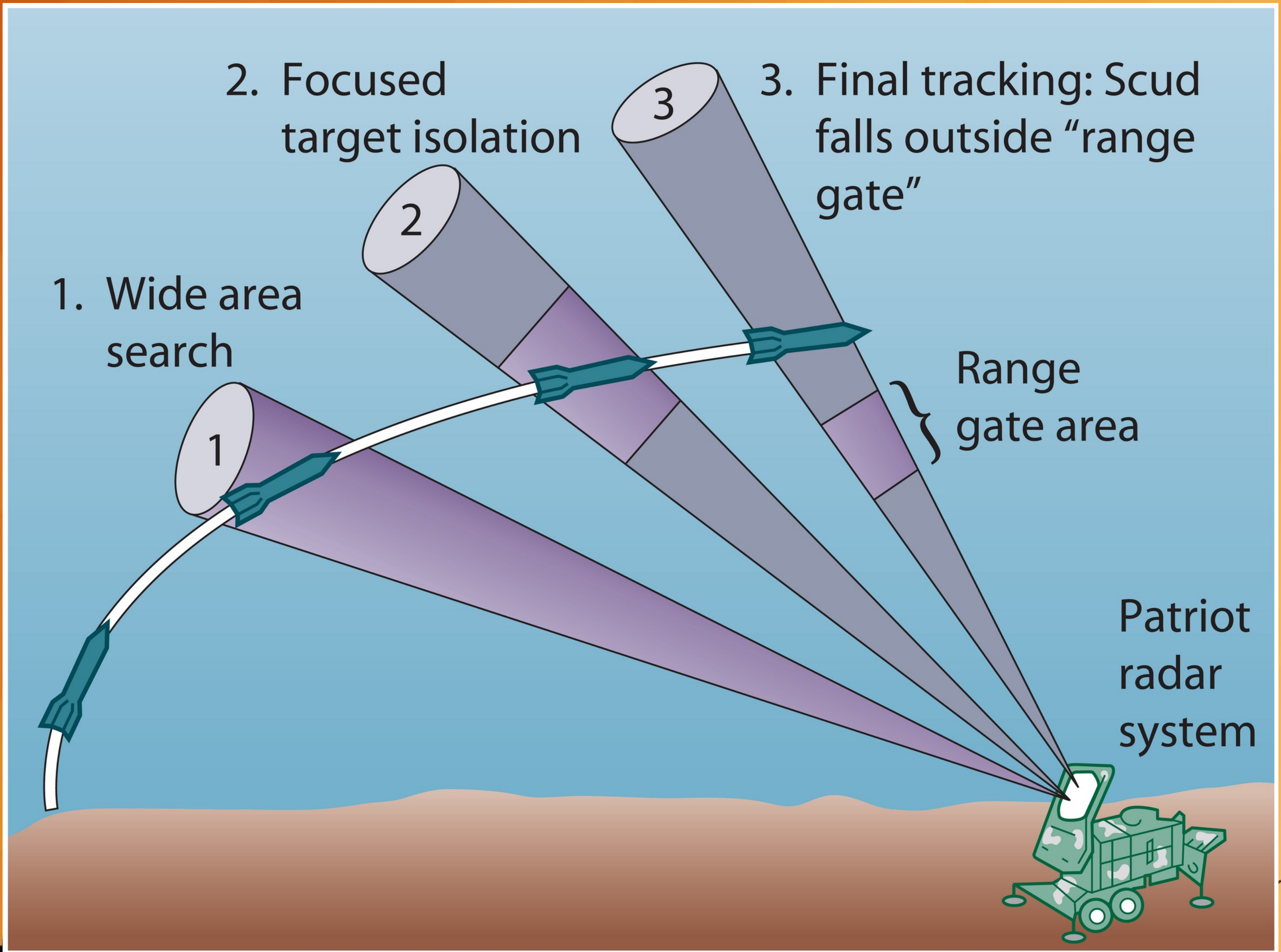
Kantian Analysis

- Buyers knew 97.5% markdown was an error
- They attempted to take advantage of Amazon.com's stockholders
- They were not acting in "good faith"
- Buyers were in the wrong, not Amazon.com

Patriot Missile

- Designed as anti-aircraft missile
- Used in 1991 Gulf War to intercept Scud missiles
- One battery failed to shoot at Scud that killed 28 soldiers
- Designed to operate only a few hours at a time
- Kept in operation > 100 hours
- Tiny truncation errors added up
- Clock error of 0.3433 seconds → tracking error of 687 meters

Patriot Missile Failure


2. Focused target isolation
3. Final tracking: Scud falls outside "range gate"
1. Wide area search
3
2
1
Range gate area
Patriot radar system

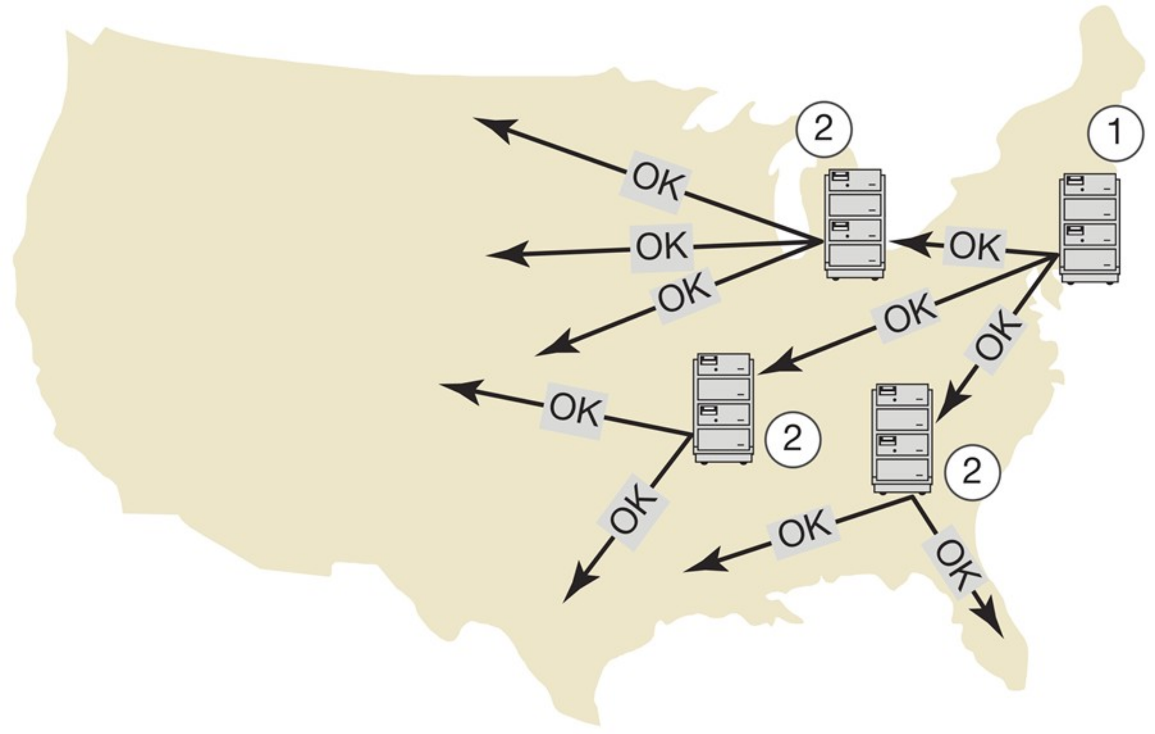
Ariane 5

- Satellite launch vehicle
- 40 seconds into maiden flight, rocket self-destructed
  - $500 million of uninsured satellites lost
- https://youtu.be/PK_yguLapgA
- Statement assigning floating-point value to integer raised exception
- Exception not caught and computer crashed
- Code reused from Ariane 4
  - Slower rocket
  - Smaller values being manipulated
  - Exception was impossible

AT&T Long-Distance Network

- Significant service disruption
  - About half of telephone-routing switches crashed
  - 70 million calls not put through
  - 60,000 people lost all service
  - AT&T lost revenue and credibility
- Cause
  - Single line of code in error-recovery procedure
  - Most switches running same software
  - Crashes propagated through switching network

AT&T Long Distance Network Failure



(1) A single switch in New York City detects an error condition and reboots. When it comes back up, it sends an “OK” message to other switches. (2) Switches in Detroit, St. Louis, and Atlanta are so busy that handling the “OK” message causes them to detect an error condition and reboot. When they come back up, they send out “OK” messages to other switches, causing some of them to fail, and so on.

Robot Missions to Mars

- Mars Climate Orbiter
  - Disintegrated in Martian atmosphere
  - Lockheed Martin design used English units
  - Jet Propulsion Lab design used metric units
- Mars Polar Lander
  - Crashed into Martian surface
  - Engines shut off too soon
  - False signal from landing gear

Denver International Airport

- BAE built automated baggage handling system
- Problems
  - Airport designed before automated system chosen
  - Timeline too short
  - System complexity exceeded development team’s ability
- Results
  - Added conventional baggage system
  - 16-month delay in opening airport
  - Cost Denver $1 million a day

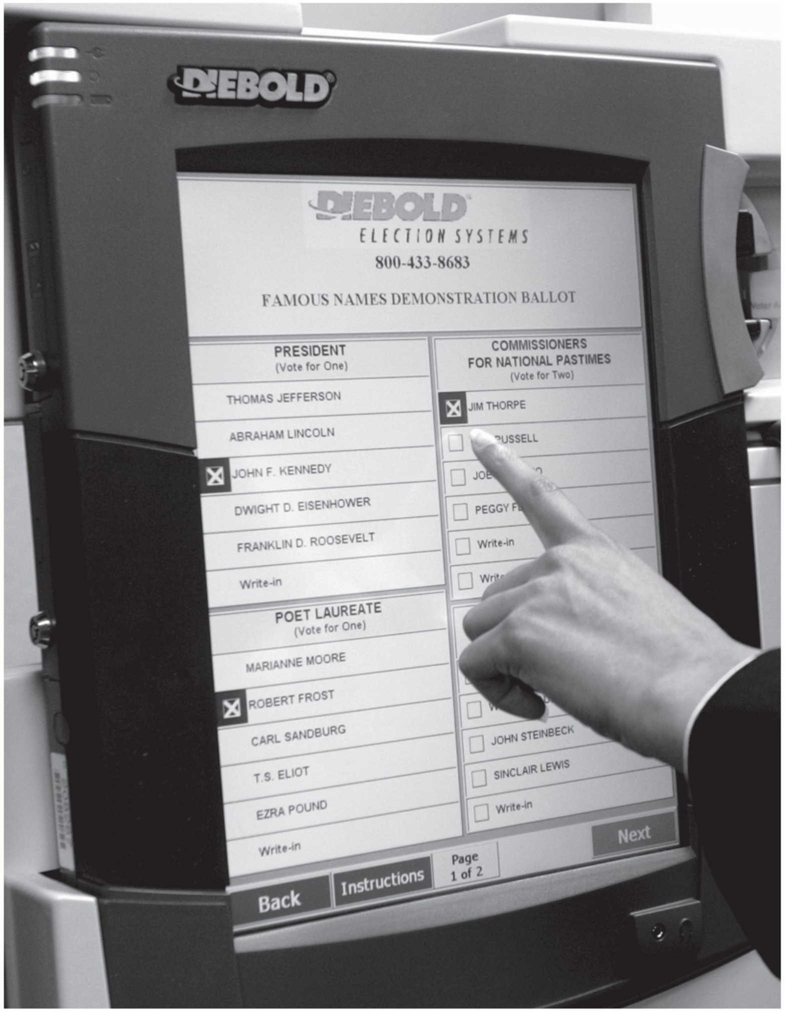
Tokyo Stock Exchange

- First day of trading for J-Com
- Mizuho Securities employee mistakenly enters order to sell 610,00 shares at 1 yen, instead of 1 share at 610,000 yen
- Employee overrides computer warning
- After sell order posted on exchange’s display board, Mizuho tries to cancel order several times; software bug causes attempts to fail
- Mizuho loses $225 million buying back shares

Direct-Recording Electronic Voting Machines

- After problems with 2000 election, Congress passed Help America Vote Act of 2002
- HAVA provided money to states to replace punch card voting systems
- Many states used HAVA funds to purchase direct recording electronic (DRE) voting machines
- Brazil and India have run national elections using DRE voting machines exclusively
- In November 2006 one-third of US voters used DRE voting machines

Direct-Recording Electronic Voting Machine



Issues with DRE Voting Machines

- Voting irregularities
  - Failure to record votes
  - Overcounting votes
  - Misrecording votes
- Lack of a paper audit trail
- Vulnerability to tampering
- Source code a trade secret, can’t be examined
- Possibility of widespread fraud through malicious programming

Back to Paper

- States had second thoughts about DRE voting machines
- May 2007: Florida legislature voted to replace DRE voting machines with optical scan ballots
- Optical scan ballots
  - Voters fill in bubbles next to names
  - Machines count ballots
  - Paper ballots allow for auditing of election results
- By November 2017, 70% of Americans using some form of paper ballot

Genesis of the Therac-25

- AECL and CGR built Therac-6 and Therac-20
- Therac-25 built by AECL
  - PDP-11 an integral part of system
  - Hardware safety features replaced with software
  - Reused code from Therac-6 and Therac-20
- First Therac-25 shipped in 1983
  - Patient in one room
  - Technician in adjoining room

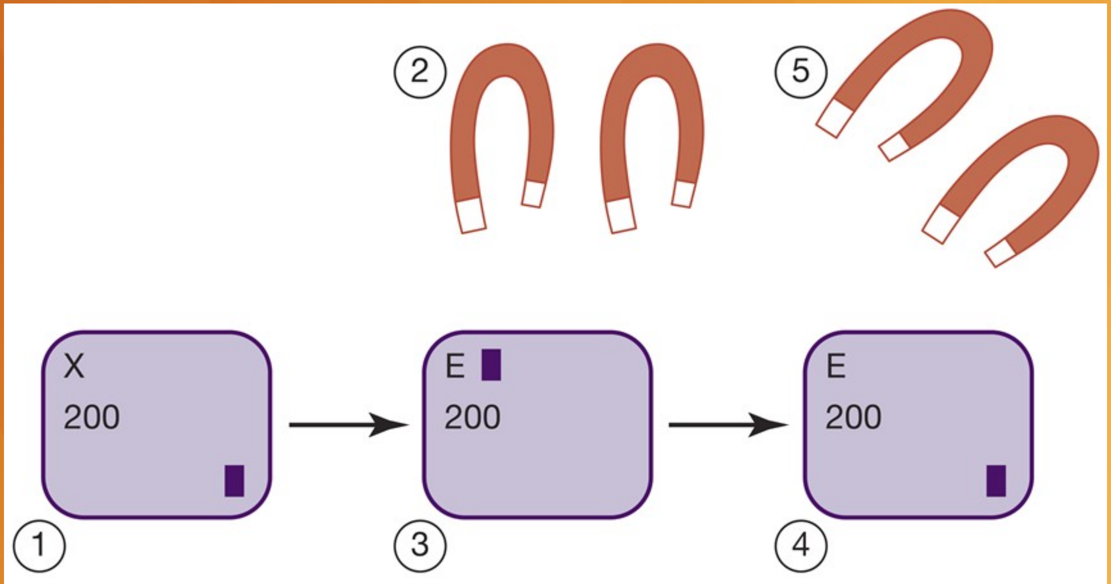
Chronology of Accidents and AECL Responses

- Marietta, Georgia (June 1985)
- Hamilton, Ontario (July 1985)
- First AECL investigation (July-Sept. 1985)
- Yakima, Washington (December 1985)
- Tyler, Texas (March 1986)
- Second AECL investigation (March 1986)
- Tyler, Texas (April 1986)
- Yakima, Washington (January 1987)
- FDA declares Therac-25 defective (February 1987)

Software Errors

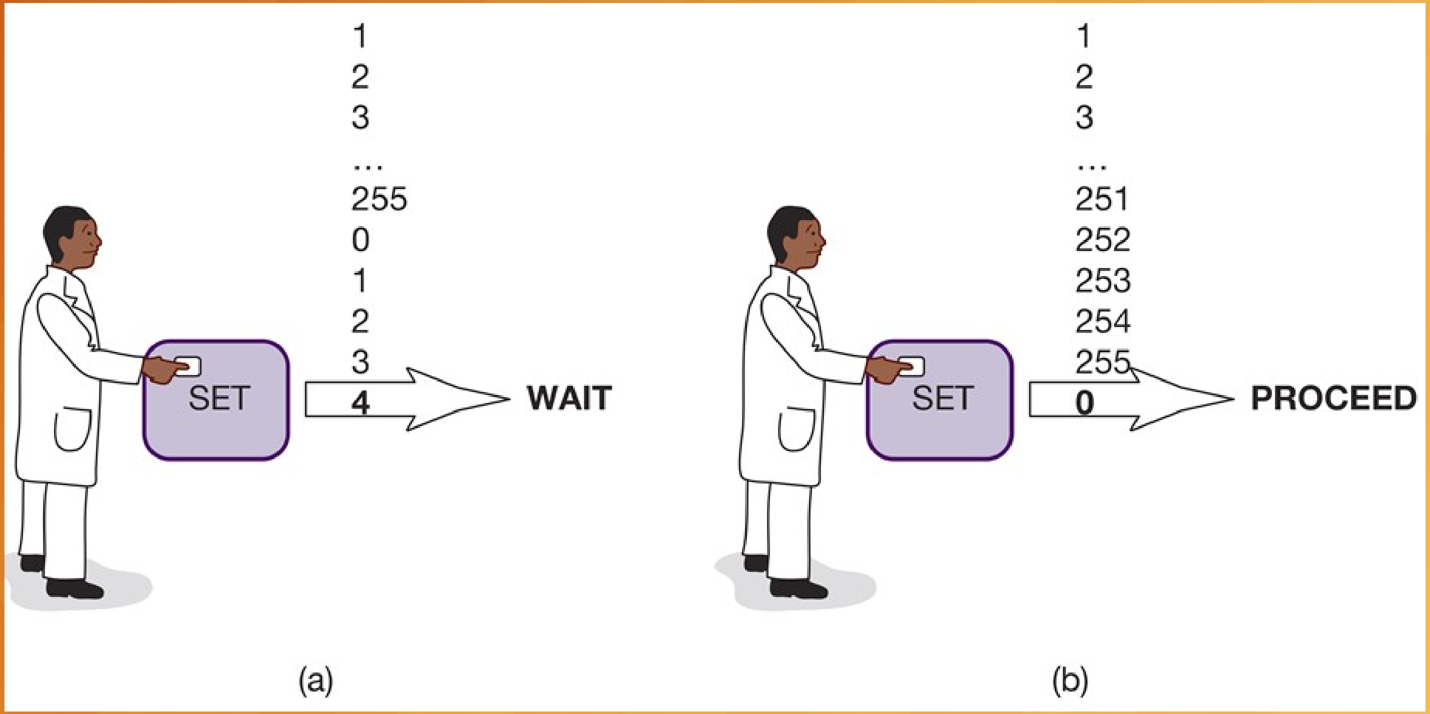
- Race condition: order in which two or more concurrent tasks access a shared variable can affect program's behavior
- Two race conditions in Therac-25 software
  - Command screen editing
  - Movement of electron beam gun

Race Condition Revealed by Fast-Typing Operators



(1) The operator finishes filling in the form. The software knows the form is filled in because the cursor is in the lower right-hand corner of the screen. (2) The software instructs the magnets to move into the correct position. While the magnets are moving, the software does not check for screen edits. (3) The operator changes the prescription from X-ray to electron beam. (4) The operator finishes the edit, returning the cursor to the lower right-hand corner of the screen. (5) The magnets finish moving. The software now checks the screen cursor. Since it is in the lower right-hand corner, the program assumes there have been no edits.

Race Condition Caused by Counter Rolling over to Zero



As long as the electron beam gun was out of position, a software task kept incrementing an 8-bit variable. (a) Usually when the operator hit the SET button, the variable was not zero and the system would wait, just as it was supposed to. (b) If the operator his the SET button just as the variable rolled over from 255 to 0, the system would administer radiation, even though the gun was out of position.

Post Mortem

- AECL focused on fixing individual bugs
- System not designed to be fail-safe
- No devices to report overdoses
- Software lessons
    - Difficult to debug programs with concurrent tasks
    - Design must be as simple as possible
    - Documentation crucial
    - Code reuse does not always lead to higher quality
- AECL did not communicate fully with customers

Moral Responsibility of the Therac-25 Team

- Conditions for moral responsibility
  - Causal condition: actions (or inactions) caused the harm
  - Mental condition
    - Actions (or inactions) intended or willed –OR-
    - Moral agent is careless, reckless, or negligent
- Therac-25 team morally responsible
  - They constructed the device that caused the harm
  - They were negligent

Postscript

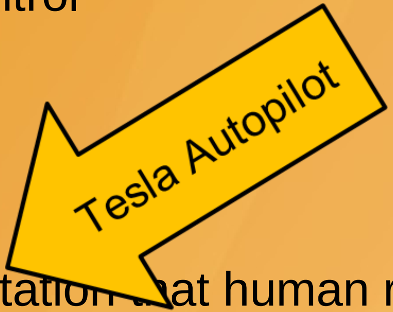
- Computer errors related to radiation machines continue to maim and kill patients
- Investigation by the **New York Times**
  - Scott Jerome-Parks, New York (2006)
  - Alexandra Jn-Charles, New York (2006)

Introduction

- October 2014: Tesla introduces technology package
  - Ultrasonic sensors
  - Camera
  - Front radar
  - Digitally controlled brakes
  - Enabled car to brake before collisions
- October 2015: Tesla releases Version 7.0 (Autopilot)
  - Software to control speed and steer
  - Tesla: “Like the systems that airline pilots use when conditions are clear”
  - Tesla: “Driver still responsible” and supposed to keep hands on steering wheel

Automation of Driving (SAE International)

- SAE Level 0 – No automation
- SAE Level 1 – Driver Assistance
  - Example: anti-lock brakes, dynamic cruise control
- SAE Level 2 – Partial Automation
  - Steering and acceleration/deceleration
- **SAE Level 3 – Conditional Automation**
  - All aspects of dynamic driving task with expectation that human responds to request for intervention
- S A E Level 4 – High Automation
  - All aspects of dynamic driving task, even if human does not respond to request for intervention
- S A E Level 5 – Full Automation


Tesla Autopilot

May 7, 2016 Fatal Accident

- Tesla S traveling east on US-27A, a divided highway in Florida
- Semitrailer truck, driving west on highway, turned left in front of Tesla
- Car struck trailer, killing driver Joshua Brown
    - Car traveling 74 miles per hour (posted speed limit 65 mph)
    - Autopilot engaged for 37 minutes before collision
    - Brown’s hands on wheel only 25 seconds during that time
    - System provided Brown with 7 warnings to put hands on wheel
    - Brakes not applied
        - Trailer was white, making it difficult to see
        - Trailer was tall, making radar signature similar to signature of an overhead sign

The Hand-Off Problem

- Drivers get bored when they have nothing to do
- Hand-off problem
  - Takes 3-7 seconds on average for drivers to regain attention and take control
  - In many emergency situations, accident happens in less than 3 seconds
- Ford, Volvo, Google all skipping SAE Level 3 automation
  - Going to straight to SAE Level 5
  - Avoiding hand-off problem

Assigning Moral Responsibility

- How to allocate moral responsibility for Joshua Brown’s death among
  - Truck driver
  - Engineers and managers at Tesla Motors
  - Brown himself
- Driver of truck
  - Turned left in front of Brown
  - Generally, that would put driver at fault
  - However, Brown’s car was speeding
  - In those cases, some or all blame shifts to driver of speeding car

Assigning Moral Responsibility

- Joshua Brown
  - Set cruise control for 74 mph, 9 mph above speed limit
  - Did not keep hands on steering wheel as instructed by Tesla
  - Did not keep eyes on road ahead (or he would have hit the brakes)
- Engineers and managers at Tesla Motors
  - Automatic Emergency Braking failed to see trailer in path of car
  - While Autopilot in beta version, could have restricted it use to freeways with no lateral crossing traffic
  - Allowed Autopilot to operate even when car speeding
  - Allowed Autopilot to stay engaged even when driver not paying attention

Assigning Moral Responsibility

- Conclusion
  - Moral responsibility must be shared among truck driver, Joshua Brown, and engineers and managers of Tesla Motors
  - Truck driver failed to yield right-of-way
  - Joshua Brown did not keep hands on steering wheel, did set cruising speed at 74 mph, and did not remain attentive
  - Tesla Motors released a product with SAE Level 3 automation without solving the hand-off problem

Introduction

- Travis Kalanick, former CEO of Uber, held that…
  - Development of autonomous vehicles an existential threat to Uber
  - Vital for Uber to be among first companies to develop autonomous-vehicle technology
- Uber's effort to catch up with Tesla and Waymo
  - Opened R&D center in Pittsburgh, Pennsylvania
  - Hired 50 researchers from Carnegie Mellon University
  - Quickly developed test vehicles

Uber Begins Self-Driving Car Pickups

- Pittsburgh, Pennsylvania
  - Started offering pickups in September 2016
  - Uber engineers in front seat to monitor system, take over when necessary
- San Francisco, California
  - Started offering pickups in December 2016
  - Experiment lasted only a week
  - Video of Uber car running red light on day 1
  - California Department of Motor Vehicles revoked registrations of Uber’s self-driving cars
- Arizona governor welcomes Uber to his state

Shift to One Human Safety Operator

- Two safety operators in initial tests
  - One behind the steering wheel, responsible for taking control of vehicle if necessary
  - Other responsible for monitoring system performance and logging significant events on a laptop
- Operators assigned to 8-hour shifts
  - Repeatedly traversed same route
  - 30-minute lunch break
- Fall 2017: Uber removes second safety operator
  - Operators complained it would be harder for them to stay alert
  - Scientific research demonstrates legitimacy of concerns

“Bad Experiences”

- In March 2018 Uber’s test vehicles still gave passengers frequent “bad experiences,” such as braking too quickly
- Autonomous vehicles subject to false positives – identifying a danger when there is none
  - Car exhaust
  - Steam
  - Litter
- Quickly braking for no reason a serious problem
  - Disconcerting to passengers
  - Car may get rear-ended
- Eliminating false positives can lead to false negatives – failing to identify a dangerous situation – and that is worse

Effort to Eliminate “Bad Experiences”

- Uber chose to reduce “bad experiences” by turning off emergency braking of self-driving cars
  - Human safety operator responsible for emergency braking and steering
  - Engineers did not implement a way for system to alert operator when emergency braking needed
    - This sounds bad, but it actually makes sense. Why?
- Volvo X C90s in Arizona test fleet came equipped with automatic emergency braking as standard equipment
  - System de-activated when car under control of self-driving system
  - Otherwise, two active systems could give conflicting commands

March 18, 2018 Accident

- Uber test vehicle running predetermined test route in Tempe, Arizona
  - Dark conditions (time was 9:58 p.m.)
  - Car northbound in rightmost lane of N Mill Avenue, traveling at 43 mph (2 mph below speed limit)
- Female pedestrian began crossing N Mill Avenue from west to east, pushing a bicycle
  - Pedestrian wearing dark clothes
  - Some illumination from streetlights
  - No crosswalk, signs warning pedestrians not to cross
  - Nearest crosswalk 360 feet to north

March 18, 2018 Accident

- NTSB preliminary report with a figure showing the location of the crash

https://www.ntsb.gov/investigations/AccidentReports/Reports/HWY18MH010-prelim.pdf

March 18, 2018 Accident

- Response of self-driving system to pedestrian
  - First detected moving object six seconds before collision
  - Had trouble classifying the object
  - When car 80 feet from pedestrian (1.3 seconds before impact), it determined emergency braking required
  - System did not alert driver because there was no alert mechanism

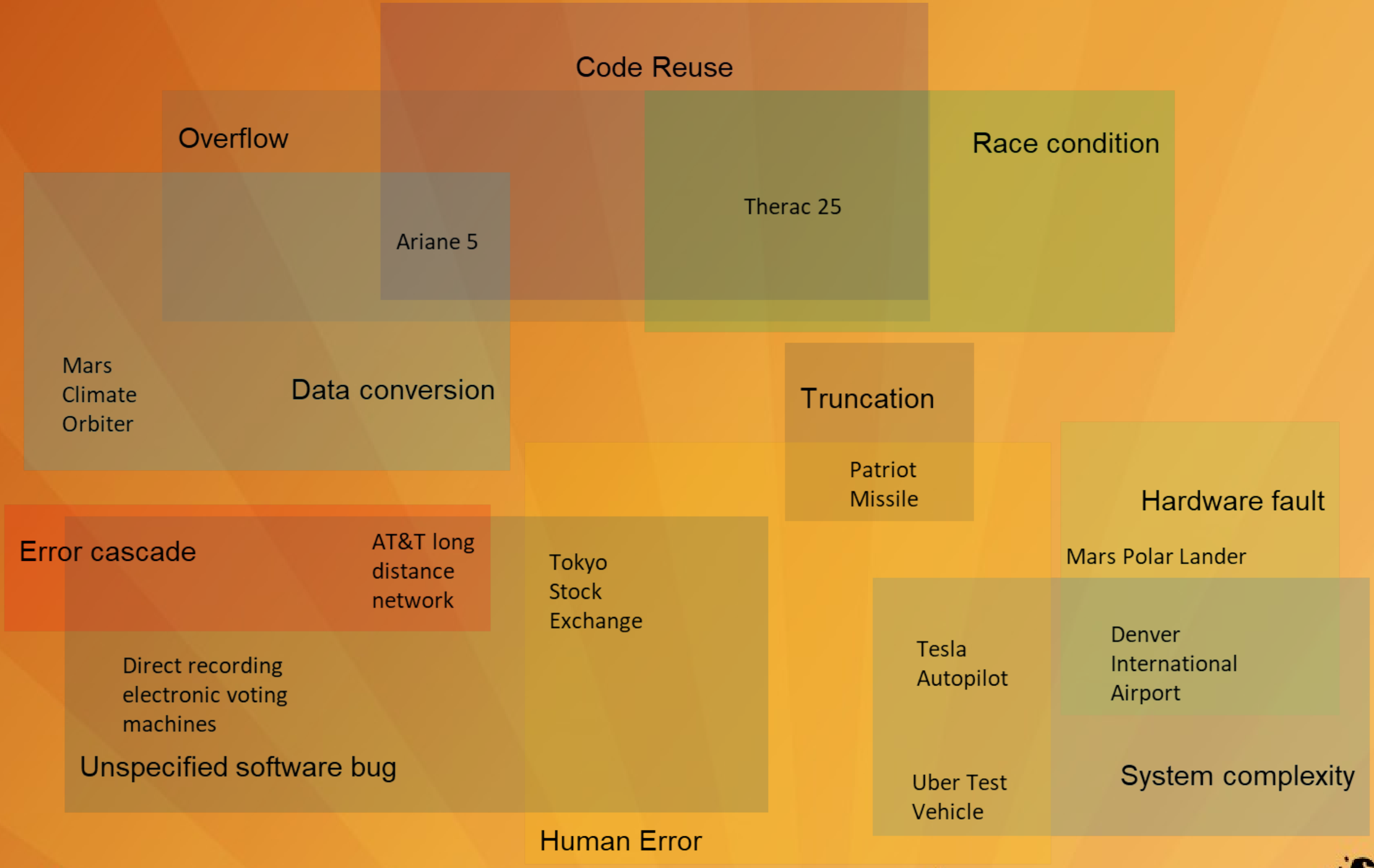
March 18, 2018 Accident

- Actions of safety operator
  - Had not been keeping gaze fixed on road ahead
  - Told police she was looking at computer interface
  - However, according to police report, driver had been streaming talent show “The Voice” to her smartphone
  - Put hands on steering wheel and began to turn just before impact
  - Braked vehicle less than 1 second after impact
- Effects of collision
  - Vehicle hit pedestrian at 39 mph
  - Pedestrian died

March 18, 2018 Accident

- Actions of pedestrian before impact
  - Did not look in direction of oncoming car until just before it hit her
  - May have assumed there were no cars on road
    - Volvo may not have been visible to her when she stepped off curb, due to distance, bend in road, and foliage
  - Her judgment may be been impaired
    - Toxicology tests returned positive results for methamphetamine and marijuana
- Consequences of accident
  - Arizona governor suspended Uber’s testing program
    - Said public safety should have been Uber’s top priority
  - Uber shut down Arizona testing facility
    - Terminated 300 safety operators in Arizona

Summary: Classifying Notable Software System Failures



Code Reuse

Overflow

Race condition

Ariane 5

Therac 25

Mars Climate Orbiter

Data conversion

Truncation

Patriot Missile

Hardware fault

Error cascade

AT&T long distance network

Tokyo Stock Exchange

Mars Polar Lander

Denver International Airport

Tesla Autopilot

Direct recording electronic voting machines

Unspecified software bug

System complexity

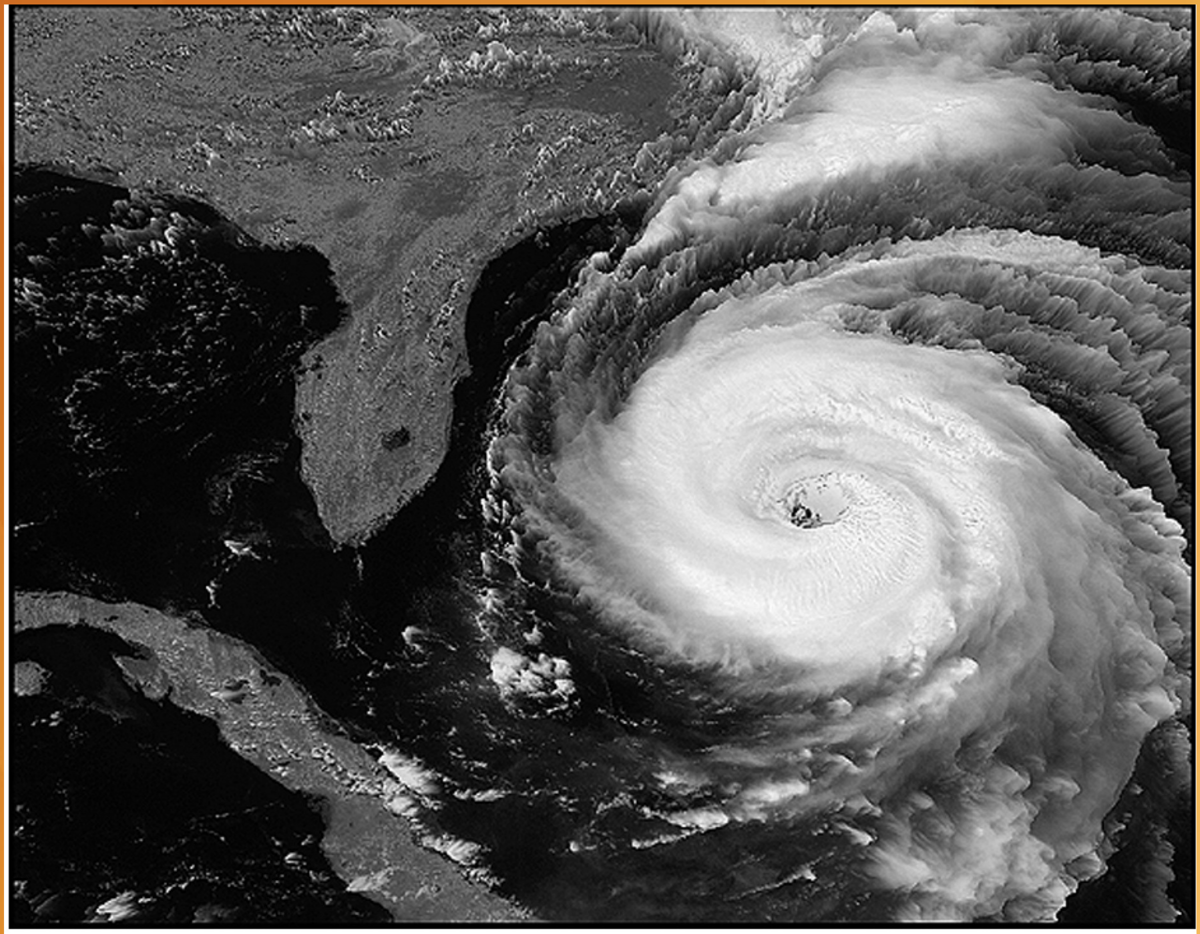
Uber Test Vehicle

Human Error

Uses of Simulations

- Simulations better than physical experiments when …
  - experiment too expensive or time-consuming
  - experiment unethical
  - experiment impossible
- Applications of simulations
  - Model past events
  - Understand world around us
  - Predict the future

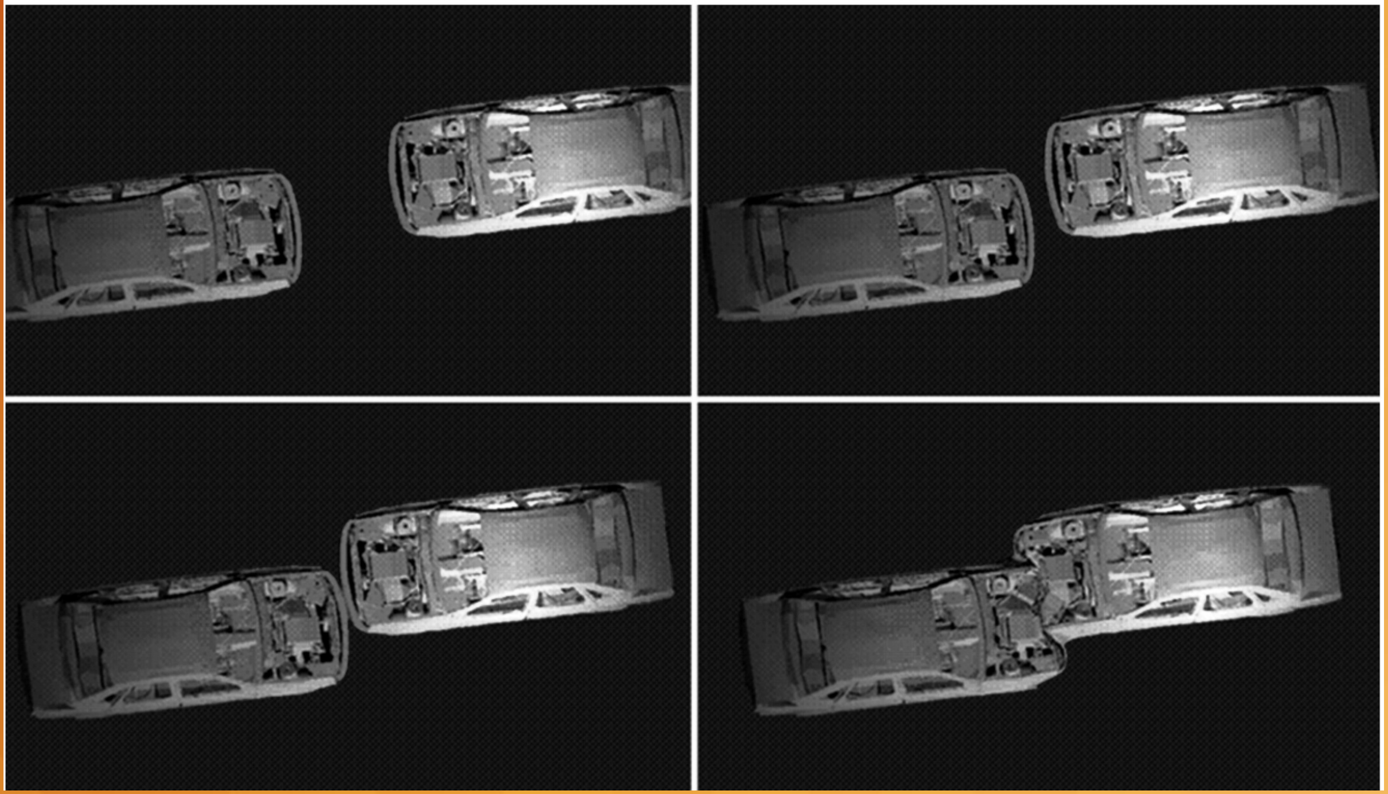
Computer Simulations



Validating Simulations

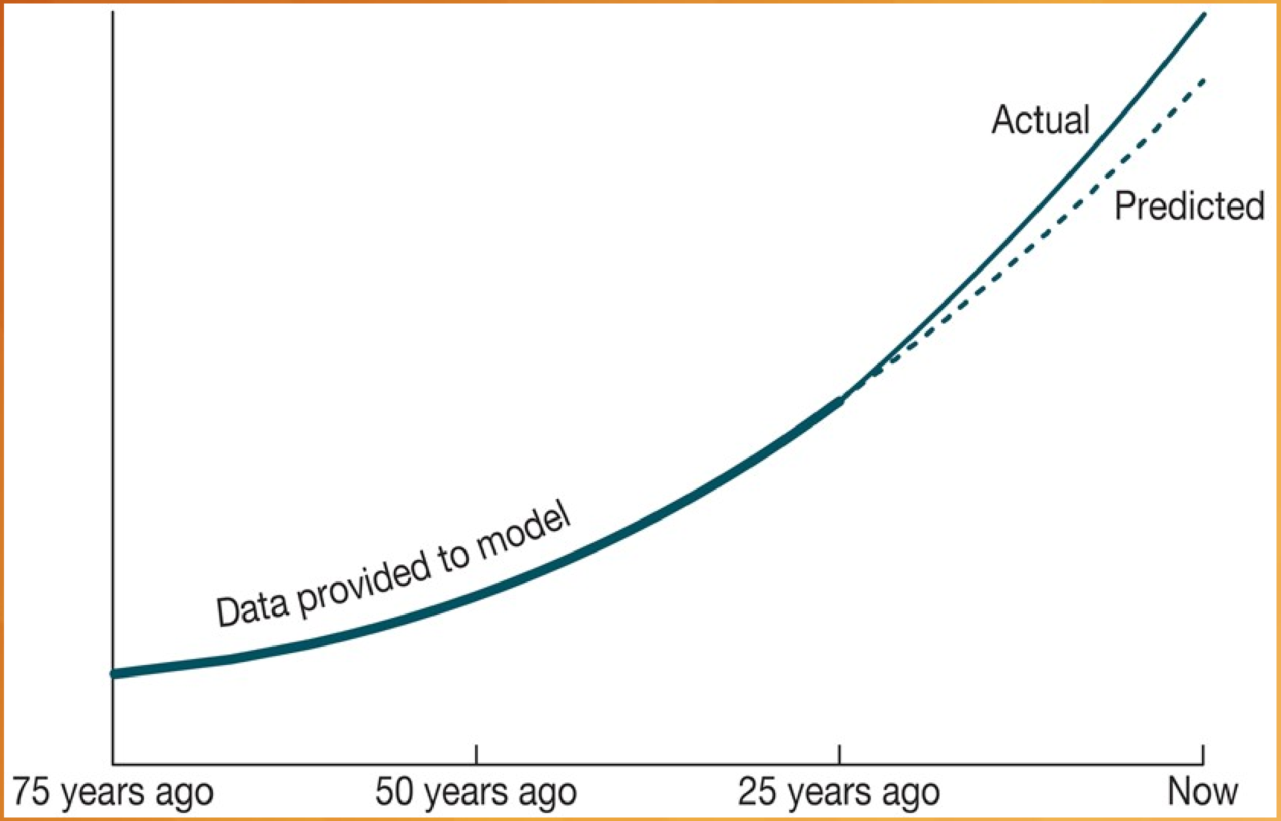
- Verification: Does program correctly implement model?
- Validation: Does the model accurately represent the real system?
- Validation methods
  - Make prediction, wait to see if it comes true
  - Predict the present from old data
  - Test credibility with experts and decision makers

Validating a Model



A computer simulation of an automobile accident can reveal roughly the same information as an actual crash test, and it is far less expensive. (Courtesy of Oak Ridge National Laboratory, US Dept. of Energy)

“Predicting the Present”



You can validate a model’s ability to predict 25 years into the future by using it to “predict the present” with data 25 or more years old. You can then compare the model’s prediction of the present with current reality.

Specification

- Determine system requirements
- Understand constraints
- Determine feasibility
- End products
  - High-level statement of requirements
  - Mock-up of user interface
  - Low-level requirements statement

Development

- Create high-level design
- Discover and resolve mistakes, omissions in specification
- CASE tools to support design process
- Object-oriented systems have advantages
- After detailed design, actual programs written
- Result: working software system

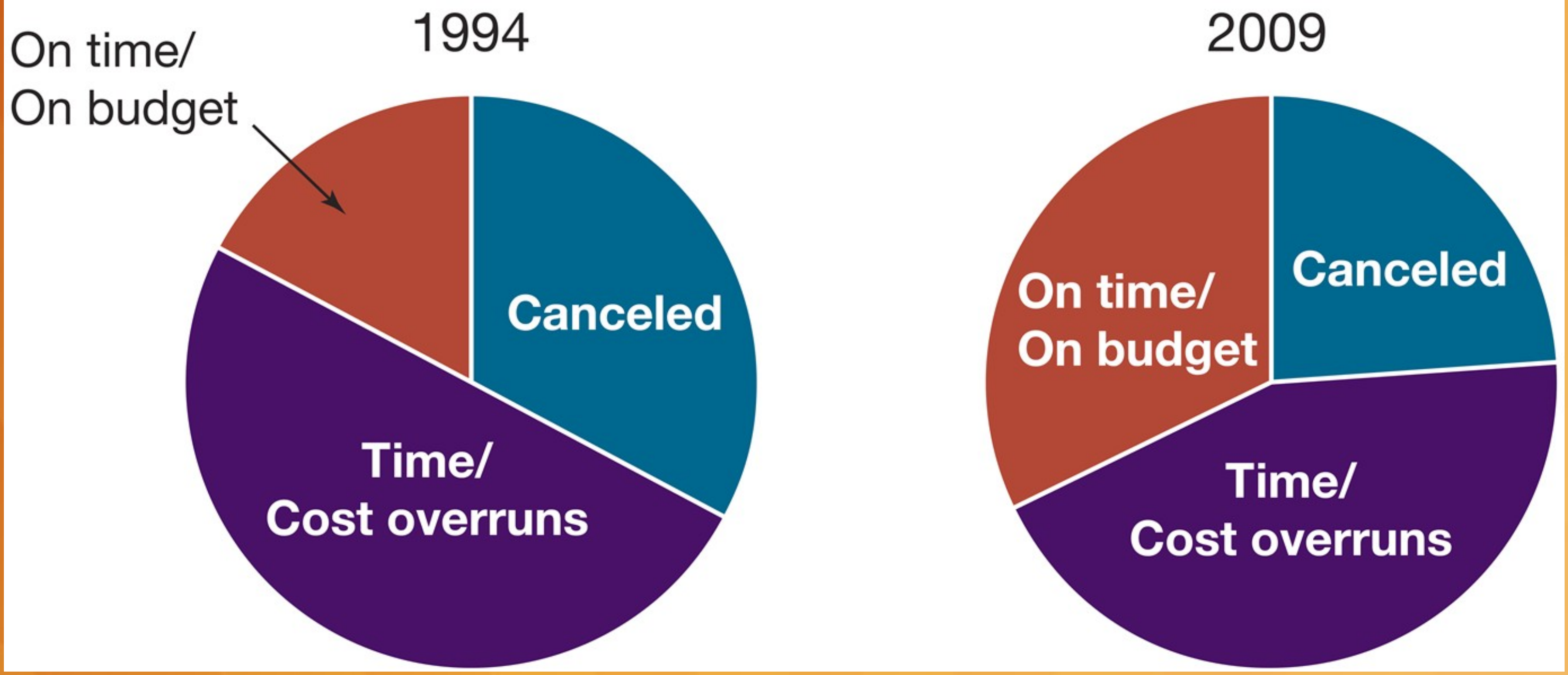
Validation (Testing)

- Ensure software satisfies specification
- Ensure software meets user's needs
- Challenges to testing software
  - Noncontinuous responses to changes in input
  - Exhaustive testing impossible
  - Testing reveals bugs, but cannot prove none exist
- Test modules, then subsystems, then system

Software Quality is Improving

- Standish Group tracks I T projects
- Situation in 1994
  - 1/3 of projects canceled before completion
  - 1/2 projects had time and/or cost overruns
  - 1/6 projects completed on time and on budget
- Situation in 2009
  - 1/4 of projects canceled before completion
  - 5/12 projects had time and/or cost overruns
  - 1/3 projects completed on time and on budget

Success of IT Projects over Time



Research by the Standish Group reveals that the success rate of IT projects in 2009 was twice that of 1994. Today, about one-third of software projects are completed on time and on budget.

Gender Bias

- In male-dominated fields, unconscious gender bias can affect important design decisions
  - Example: seatbelts don’t work well for pregnant women and their unborn children because crash dummies are modeled after men
- Men and women have different approaches to writing and debugging software and using programming tools
- Even if women present, their voices may not be heard
  - Voting suppresses minority views
  - Many decisions made under time pressure
- Solutions
  - Attract more women by improving job postings
  - Assign mentors, eliminate sexual harassment

Bias in Training Sets for Artificial-Intelligence Systems

- When AI system trained with biased data set, can affects its performance across a diverse population
- Example: Facial-recognition systems
  - Training data: 75% of faces are male and 80% of faces are white
  - Resulting performance
    - Misidentified fair-skinned males 1% of time
    - Misidentified gender of darker-skinned females up to 35% of time
- Example: Google Photos mislabeled black people as “gorillas”
- Example: Photos of people cooking in kitchen
  - 67% of training photos showed women cooking
  - Trained system correctly identified gender of men in photos less than 50% of time

Shrinkwrap Warranties

- Some say you accept software “as is”
- Some offer 90-day replacement or money-back guarantee
- None accept liability for harm caused by use of software

Are Software Warranties Enforceable?

- Mass-marketed software and software included in sale of hardware likely to be considered a good by a court of law
- Uniform Commercial Code applies to goods, despite what warranties may say

Key Court Cases

- Step-Saver Data Systems v. Wyse Technology and the Software Link
  - Court ruled that provisions of Uniform Commercial Code held
- Pro CD v. Zeidenberg
  - Court ruled shrinkwrap licenses are enforceable
- Mortenson v. Timberline Software
  - Court ruled in favor of Timberline and licensing agreement that limited consequential damages

Should Software Be Considered a Product?

- If software a product, then…
  - theory of strict liability would apply to software maker
  - maker would be liable for personal injury or property damage (but not economic loss) caused when product used as intended
  - primary impact would be when software in an embedded system, e.g., medical device or automobile
- Courts have resisted treating software as a product
  - A software-controlled device may cause harm through no fault of the programmer
  - Strict liability puts too much liability on programmer

Case Study: Incredible Bulk

- Peter downloads Incredible Bulk for $49.95
- Game usable, but has annoying bugs
- Company never releases software patches
- Next year company releases Incredible Bulk II for $49.95
- New game fixes all major bugs in original game

Ethical Analyses

- Kantian analysis
  - Company did no wrong
  - It never promised to release bug fixes
  - Peter could have read reviews before purchasing game
- Social contract theory analysis
  - Peter not actually purchasing software, he purchased license to use software
  - At some point before releasing Incredible Bulk II the company fixed the bugs
  - At that point it should have made the patches freely available to users

Next Time

- Professional Ethics
  - Read 9.1-9.4
- Happy Halloween
  - Don’t eat too much candy