Week 12: Computer and Network Security, Computer Reliability
March 29, 2018
8.1 Introduction

- Computer systems are sometimes unreliable
  - Erroneous information in databases
  - Misinterpretation of database information
  - Malfunction of embedded systems

- Effects of computer errors
  - Inconvenience
  - Bad business decisions
  - Fatalities
8.2 Data-Entry or Data-Retrieval Errors
Two Kinds of Data-related Failure

• A computerized system may fail because wrong data entered into it
• A computerized system may fail because people incorrectly interpret data they retrieve
Disfranchised Voters

- November 2000 general election
- Florida disqualified thousands of voters
- Reason: People identified as felons
- Cause: Incorrect records in voter database
- Consequence: May have affected election’s outcome
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?
Class Activity 1: Should NCIC continue to maintain a centralized database of stolen vehicles? Discuss from an act utilitarian perspective.
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 $\rightarrow$ more false arrests
• Accuracy of NCIC records more important than ever
8.3 Software and Billing Errors
Errors When Data Are Correct

- Assume data correctly fed into computerized system
- System may still fail if there is an error in its programming
Comair Cancelled All Flights on Christmas Day, 2004

AP Photo/Al Behrman, File
Other System Malfunctions

• Hackers taking control of systems:
  • At Black hat Conference in Las Vegas, computer
    security researcher Jay Radcliffe show how he
    could wirelessly hack into and control the insulin
    pump he was wearing
  • In July 2015, two researchers demonstrated that
    they could hack into a Jeep Cherokee with a
    touch screen to gain control of the vehicle’s vital
    functions
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
Class Activity 2: Was Amazon.com wrong in refusing to fill the orders on the wrong price of the iPAQs? Discuss from a rule utilitarian and Kantian perspective.
8.4 Notable Software System Failures
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 $\rightarrow$ tracking error of 687 meters
Patriot Missile Failure

Figure from SCIENCE 255:1347. Copyright ©1992 by The American Association for the Advancement of Science. Reprinted with permission.
Tokyo Stock Exchange

• First day of trading for J-Com
• Mizuho Securities employee mistakenly enters order to sell 610,000 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 1/3 of U.S. voters used DRE voting machines
Diebold Electronic Voting Machine

© AP Photo/Rogelio Solis
Class Activity 3: What could be potential problems with EVMs?
8.8 Software Warranties and Vendor Liability
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
Class Activity 4a: Should companies and programmers take responsibility of software malfunctions or errors?
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
Class Activity 4b: When someone is bullied on Facebook (by a person they don’t know in the offline world) and this person then dies by suicide, is Facebook responsible for having somehow “caused harm”? 
Extras
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: $500,000/year
- 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 $445,000/year
- Conclusion: Good to have NCIC stolen vehicles database
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
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
Moral Responsibility of Software Manufacturers

- If vendors were responsible for harmful consequences of defects
  - Companies would test software more
  - They would have to purchase liability insurance
  - Software would cost more
  - Start-ups would be affected more than big companies
  - Less innovation in software industry?
  - Software would be more reliable?

- Making vendors responsible for harmful consequences of defects may be a bad idea, but…

- Consumers should not have to pay for bug fixes