Can We Trust the Computer
RISKS

- What can go wrong
  - Questions about Reliability and Safety
    - Almost anything can go wrong.
    - Complexity makes an error free system essentially impossible to create.
    - Computer glitches and system failures have a myriad of causes including:
      - faulty design

- sloppy implementation
- careless or insufficiently trained users
- poor user interfaces
- multiple factors

- Most systems and programs normally work fine.
  - How do we define acceptable risk
  - We play several roles:
    - computer user

    - computer professional
    - educated member of society

- Categories of Failures (e.g.):
    - cause
    - seriousness of effects
    - application area
- Scope of effects of failures:
    - individuals (usually as consumers)
    - system failures affecting many (excluding safety issues)

    - safety critical systems

- Problems for Individuals:
  - Billing errors
    - solutions:
      - test ranges
      - test degree of change from previous
      - educate users
    - gross errors caught quickly
  - Database accuracy problems

  - ∗ errors may propagate
  - ∗ corrections may not propagate
  - ∗ incorrect input
  - ∗ differing code meanings between databases
  - ∗ insufficient information to distinguish multiple instances or to identify inconsistencies
  - ∗ identity theft
- – Consumer hardware and software
  - ∗ first releases often exhibit serious errors

        - software routinely sold with known flaws
        - complexity often culprit
        - Pentium bug infamous because of management reaction
        - testing VS time to market

- System Failures
    - Communications
    - Business & Financial

- businesses destroyed

- systems delayed or abandoned
  - e.g. Denver airport baggage system
    - real-word problems
    - problems with other systems & interface
    - software errors
    - insufficient development & testing time allotted
    - specs changed after project commenced

- Safety Critical Applications

- e.g. military, power plant, aircraft operation & traffic control, trains, factory automation, medical, ...