



Lecture 19

Computer and Network Security

Addison-Wesley
is an imprint of

PEARSON

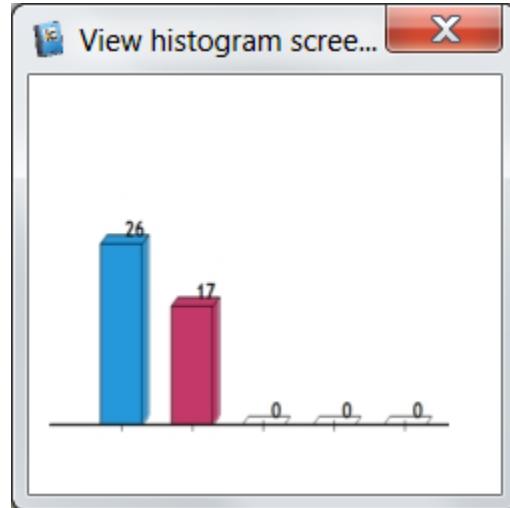
Based on slides © 2011 Pearson Education, Inc. Publishing as Pearson Addison-Wesley

Participation Quiz

1. What is the French word for “eggplant?”
 - A. のみもの
 - B. すきやき
 - C. Aubergine
 - D. デザート
 - E. \$&%()@@

Computer Reliability

“The manufacturer of a self-driving car should not be held responsible for crashes in bad weather, such as snow storms.”



Final Projects

- Due Thursday, midnight, Turnitin++
- Some comments
 - Don't take scores on previous essays *too* seriously
 - Use and cite references (don't plagiarize!)
 - Most important is to make a clear, convincing argument

Computer Reliability

- Data-Entry and Retrieval errors
 - Voter logs
 - Long gun registry
 - False arrests
 - Credit records
- What responsibility does the maintainer of a database have for the integrity of the data in it? What rights should the people about whom data is stored have to access it, and to have the data corrected?

Software and Billing Errors

- System Malfunctions
 - Huge bills in the mail
 - Errors in government statistics
 - Mail undelivered
 - Rent system charged people too much
- System Failures
 - 911 system had huge delays
 - Errors in stock exchange platforms
 - Air traffic control systems
 - Emergency room scheduling systems
 - Airline scheduling software crash leads to 1100 canceled flights
 - Boeing 777 autopilot malfunction led to erratic flying

Embedded Systems

- Patriot missiles
 - Accumulating floating point truncation errors led them not to fire at incoming missiles
- Ariane 5
 - Floating point to integer conversion error led rocket to explode
- Mars climate orbiter
 - Imperial/metric unit conversion led to crash
- Denver International Airport
 - \$311 million automated baggage system never worked, eventually replaced with a \$71 million traditional system
- Tokyo stock exchange
 - Accepted an order for selling 610,000 shares at 1 yen, instead of 1 share at 610,000 yen. Then wouldn't cancel the order.

More Embedded Systems

- Electronic Voting Machines
 - Fails to record various ballots
 - Records way too many votes
 - Records way too few votes
 - Votes recorded correctly but counted wrong (integer overflow)
 - Votes were changed at the confirmation screen
- Therac-25
 - A linear accelerator used to for cancer radiation therapy
 - Occasionally gave patients way too much radiation
 - Traced to various software errors, including two race conditions
- How much should be done to prevent such problems?
- How should we decide that a system is safe?

Computer Simulations

- Simulations are used to answer questions about scenarios that can't be easily observed in the real world
 - Nuclear explosions
 - Climate change
 - Car crashes
- Models are only useful if they accurately describe reality
- What would you need to see to trust a simulation? How accurate does a simulation have to be to be useful?

Software Warranties

- Software companies tend to write license agreements saying that the software may not perform as promised
 - “we expressly disclaim ... the implied warranties of merchantability and fitness for a particular purpose”
- Why is this reasonable?
 - Software is expensive
 - Other expensive goods are backed up by warranties
- Should software come with warranties? If so, what should these warranties cover?
- Do software makers have a moral obligation to produce software that does what it promises?