Week 7 - Monday

COMP 4290

Last time

- What did we talk about last time?
- Quantum cryptography and transmission
- Program security
- Non-malicious software flaws

Questions?

Project 2

Ashley Gutierrez Presents

Exam 1 Post Mortem

Back to non-malicious program errors

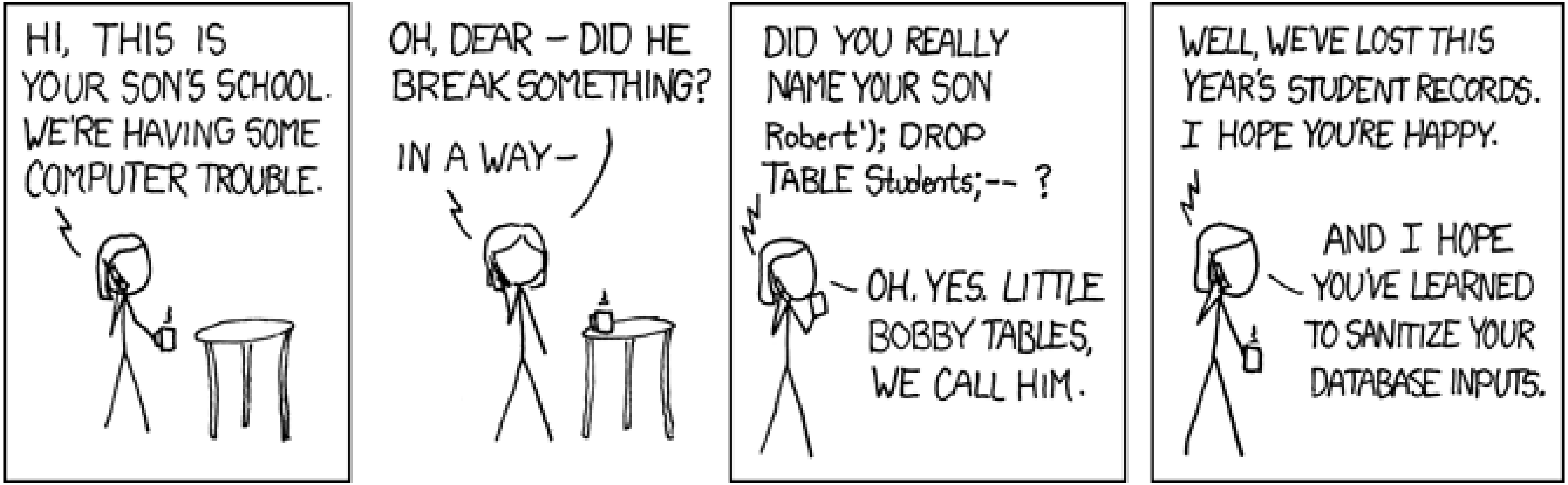
Incomplete mediation

- **Incomplete mediation** happens with a system does not have complete control over the data that it processes
- Example URL:
  - `http://www.security.com/query.php?date=2025September29`
- Wrong URL:
  - `http://www.security.com/query.php?date=2000Hyenas`
- The HTML generates the URL, but the URL can be entered manually

Incomplete mediation security

- For a website, a carelessly altered URL might just mean a 404 error
- For a program, bad data could cause any number of faults and failures
- Malicious attackers could change data or mount an SQL injection attack to destroy, change, or reveal database internals
- Values should always be checked and sanitized

Bobby Tables


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

Time-of-check to time-to-use

- A **time-of-check to time-to-use flaw** is one where one action is requested, but before it can be performed, the data related to the action is changed
- The book's example is a man who promises to buy a painting for $100 who puts five $20 bills on the counter and pulls one back when the clerk is turning to wrap up the painting
- In this flaw, the first action is authorized, but the second may not be

Time-of-check to time-to-use

- It seems like things happen instantly in a computer
- Many operations, especially those on files, may be put into a queue of work
- Imagine you give the OS a data structure with this command:

File	Command
MyFile.txt	Change byte 4 to 'A'

- After it is authorized but before it can be executed, you change it to:

File	Command
YourFile.txt	Delete file

Undocumented access point

- A program might have a way to access its private internal data
- These access points are called **backdoors** or **trapdoors**
- During development, these backdoors can be really useful for debugging
- In production, they cause a security risk, either because the developers can have control they shouldn't or because other attackers can exploit the backdoor

General programming errors

- Integer overflow and underflow
  - Someone ordered -2 billion oranges?
- Unterminated C-style string
  - A C-style string ends with the null character (`'\0'`)
  - Without the null character, string processing functions might keep reading (or writing) into memory
- Race conditions
  - In multi-threaded environments, data can be updated by multiple threads, leading to inconsistent (and unpredictable) results

Ticket out the Door

Upcoming

Next time…

- Kyle Hinkle presents
- Therac-25
- Malicious code
- Countermeasures
- Start web security

Reminders

- Read sections 4.1 – 4.4
- Work on Project 2