CSCI262
System Security

Revision

User Authentication

- Bases for authentication.
- False positive/negative
- Passwords.
  - Dictionary attacks.
  - Brute force.
  - Entropy
  - Hashing
  - Salting
  - Rainbow table
- One-time passwords.

Access control

- Access control vs Authentication
- Representations:
  - Access control matrices.
  - Access control lists.
  - Capabilities.

- Types of access control:
  - Discretionary versus mandatory.
  - Based on:
    - Identity.
    - Group.
    - Role.
    - Attribute
    - Ring
    - Level

- Access control security models
  - BLP
    - No read up, no write down
  - Biba
    - No wirte up, no read down
  - Clark-Wilson
  - Lattice
    - Least upper bound
    - Greatest lower bound
  - Lippner
  - Chinese wall

Denial of Service

- What is it and what does it threaten?
- Specific system targets
- Protecting against TCP SYN flooding
  - Time-out.
  - Random dropping.
  - (SYN)-cookies.
  - Puzzles.
- Distributed DOS.
- Reflection & Amplification

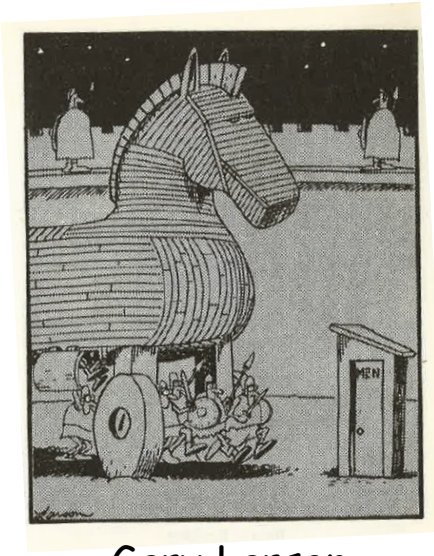
Buffer overflow

- What is it?
- When is it likely to occur?
- What are the likely effects?
- How to avoid it?

Secure mobile code

- HTTP Authentication
- JavaScript
- PHP
- XSS – Cross-site scripting

Malware



Gary Larson

- Types:
  - Viruses.
  - Worms.
  - Trojan Horses.
- Classification
- Virus structure & components
- Virus concealment methods

- Protection against malware:
  - Information flow metrics, Sandboxing
  - Detection: Signatures, integrity.
- Digital immune system

Intrusion detection systems (IDS)

- The role of IDS.
- False positive/negative (again)
- IDS Models:
  - Anomaly-based
  - Signature/Misuse-based.
- Architecture: Agents (host or network based), director, notifier.
- Honeypot

Firewalls

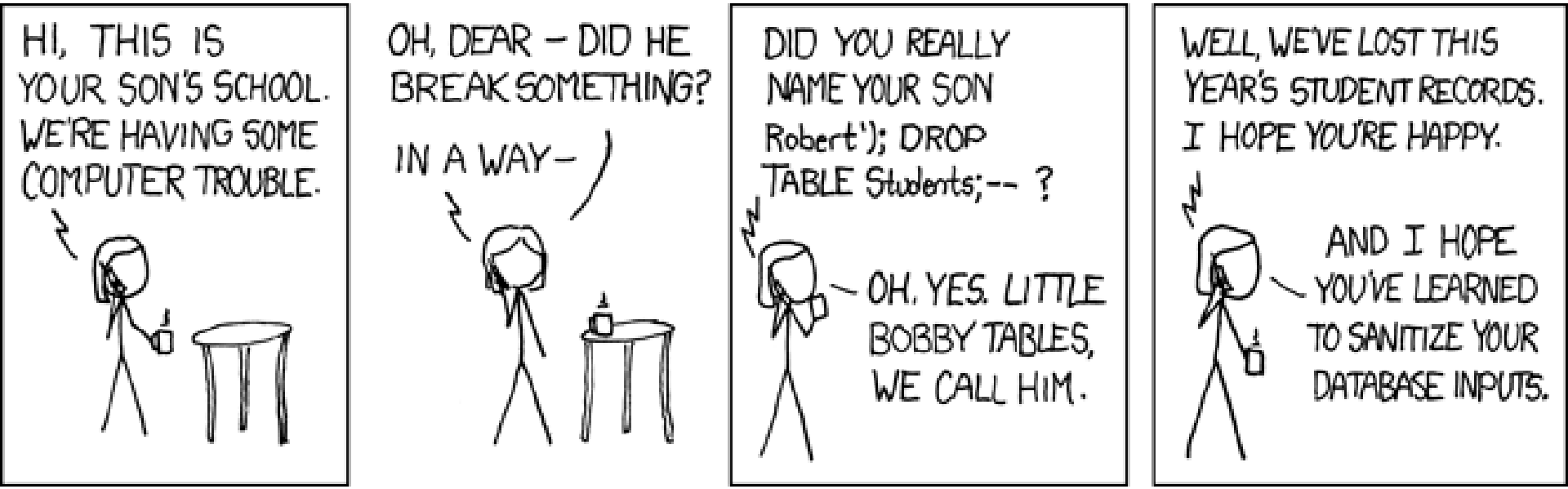
- Type of firewalls.
  - Packet-filtering firewall.
    - Stateful inspection firewalls.
  - Application-level gateway.
    - Also called proxy server.
  - MAC layer firewalls.
- Firewall architecture
- Firewall limitations

Statistical databases

- An aggregate-query interface.
- Inference: The derivation of sensitive information from non-sensitive (aggregated) data.
- Direct vs Indirect attacks
- Protection: Query set restriction, data perturbation, output perturbation.

SQL injection

- It's often about checking input!



http://xkcd.com

Exam overview

- Duration: *3 hour*
- Marks: **60*, worth 60%***.
  - Remember, you need at least 45% to pass the exam, i.e. **27/60**.
- You are not allowed calculators, computers, dictionaries or notes...
- You will not be asked to write any program or SQL statement, although you may need to explain particular coding problems

Exam overview

- Question types
  - Fill in the blank
    - Put your answer in the answer booklet, not on the exam sheet!
    - These questions should not each take very long to answer, e.g.,

"Examples of each of the main authentication bases are ___, ___ and ____."

"Online" and "offline" attacks differ in that _____

The C library function strcpy() is considered unsafe because it may result in _____.

Exam overview

- Short answer questions: concepts, principles, etc.

What is salting? Where can we use it?

Describe the general program structure of a virus.

Describe the two types of error that can occur in intrusion detection systems.

Consider the following statements and answer the subsequent questions:

Alice can climb trees and push walls.

Bob can climb trees, push walls and jump walls.

Chris can push Alice, push walls and climb walls.

Dan can climb trees and push walls.

- What are the subjects, objects and actions for this scenario?
- Draw an access control matrix for this scenario.

Describe two methods for protecting against inferential attacks at the query level in the context of statistical databases.

Select * from employee where dept = %d

Use the above SQL statement as an example to describe how SQL Rand works.

- Look at the UOW exams from previous years!
  - Go to https://ereadingsprd.uow.edu.au/ and enter CSCI262

Good Luck!