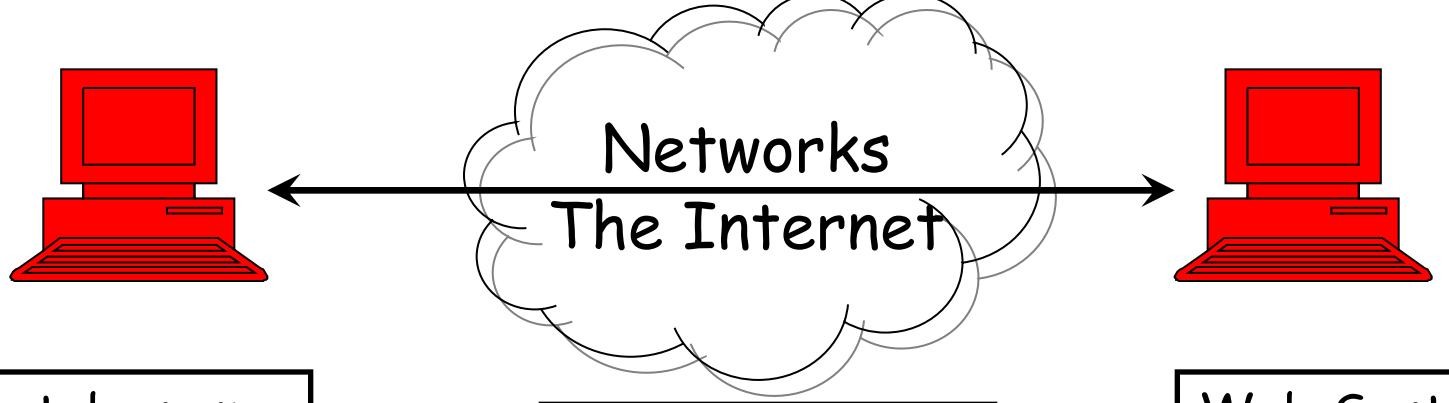
CSCI262 : System Security

Summary



Databases:

Access control
Inference
SQL injection

Environments:

Networks
Computers
OS: Windows
Web Servers
Databases

Web Systems:

Apache
JavaScript
CGI
PHP

Attacks:

Buffer overrun
DoS & DDoS
Malicious Code
Phishing

Fundamentals:

User Authentication
and
Access control

Defence:

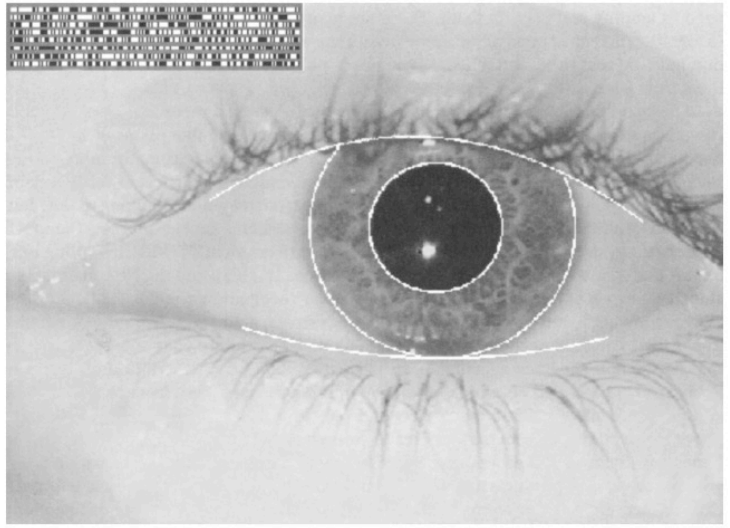
Auditing
Client puzzles
Good coding practices
IDS
Firewalls

SYSTEM SECURITY

User Authentication

- Bases for authentication.
- Errors in authentication
- Passwords.
- Problems with passwords:
  - Poor choices.
  - Brute force.
  - Dictionary attacks.
  - Unix login process:
    - Hashing
    - Salting.
    - Shadowing.
- One-time passwords.

- Biometrics briefly
- Token-based authentication.
- CAPTCHA.
  - For authentication and for denial of service.



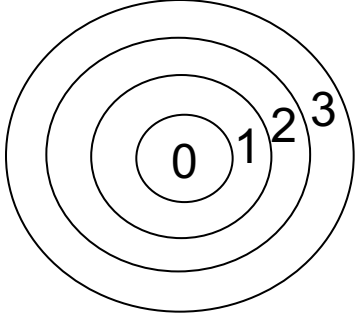
Operating System

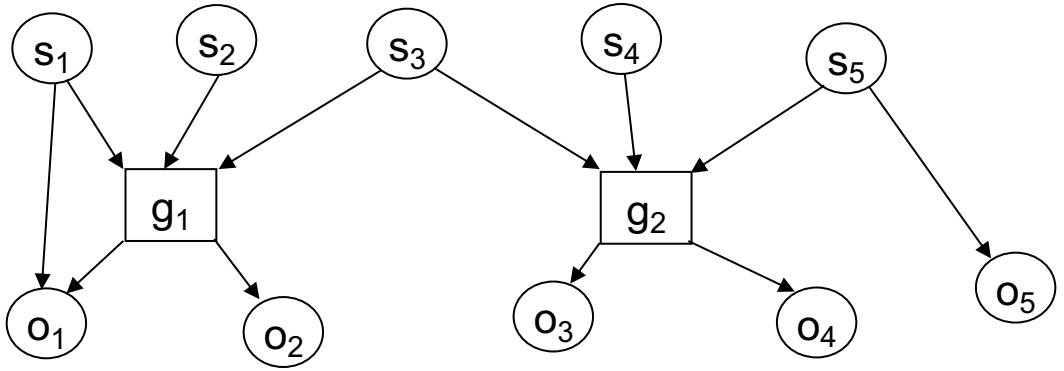
- What is the OS used for?
- Sharing the CPU.
- Executing Apps
- Advantages of Virtual Address Map
- Operating Modes
- OS Isolation.

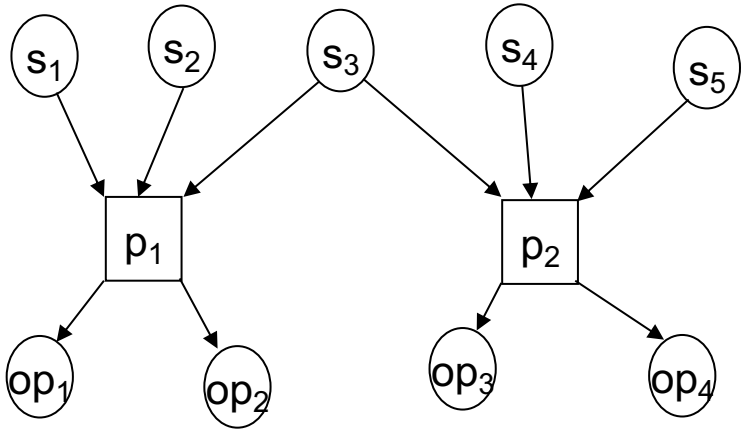
Access control

- What is it?
- Objects and Subjects.
- Representations:
  - Access control matrices.
  - Access control lists.
  - Capabilities.
  - Advantages and disadvantages.

- Types of access control:
  - Discretionary versus mandatory.
  - Based on:
    - Identity.
    - Group.
    - Role.
    - Protection rings.
    - Privileges.
    - Attributes.
- Labels and lattices.





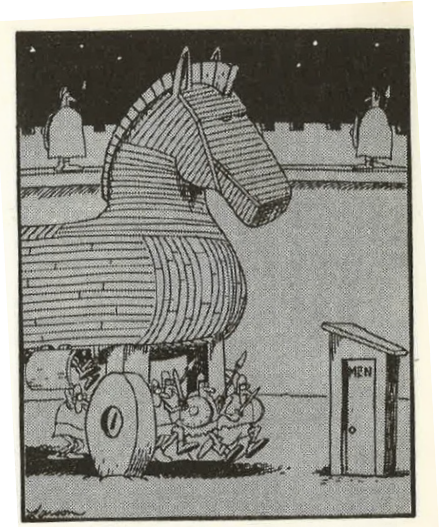


- Properties:
  - ss and *.
- Access control mantras:
  - **BLP**: Confidentiality based:
    - “No write down, no read up!”
  - **Biba**: Integrity based:
    - “No write up, no read down!”

Buffer overflow

- What is it?
- When is it likely to occur?
  - And how can we avoid it?
- What are the likely effects?
- You wouldn't be asked to write code but might have to read & interpret, or correct some.
  - This is true throughout the exam.
- Some development guidelines.
- Shellcode.
  - Significance of setuid.

Malware



Gary Larson

- What is malware?
- Types:
  - Viruses.
  - Worms.
  - Trojan Horses.

  How do they move? On and between computers.
- Virus components:
  - Infection mechanism, payload, trigger.

Classification of Viruses

- … and according to the method of concealment.
  - Encrypted.
  - Stealth.
  - Polymorphic.
  - Metamorphic.
- These are effectively technologies used by the virus.
- The transport mechanism is related to the target but can also be used as a means of classification.

- Protection against malware:
  - Certification, Rights reduction, Sandboxing.
  - Detection: Signatures, patterns, behaviour.
- Digital Immune System.

Denial of Service

- What is it and what does it threaten?
- Specific system targets:
  - Memory.
  - Processors.
  - Communication bandwidth.
- May not be purely brute force.
  - Attacks on poorly configured devices or software, or poorly developed protocols.
  - TCP SYN flooding.
  - Ping of death.
- Distributed DOS.
  - Reflection
  - Amplification

Protecting against DOS

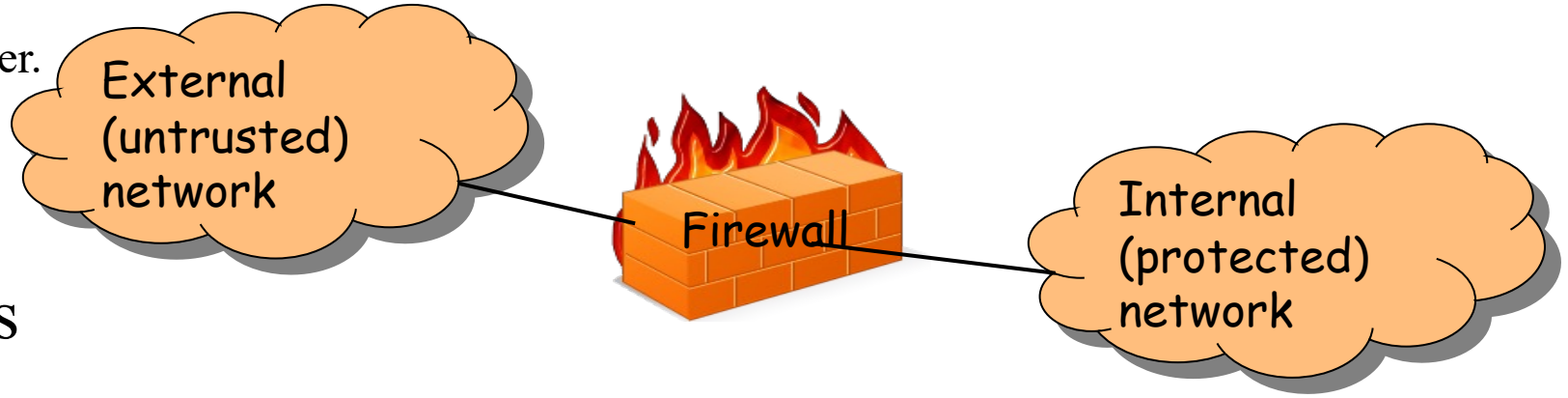
- Tricky business ☹
- Time-out.
- Random dropping.
- (SYN)-cookies.
- Puzzles:
  - Juels and Brainard mechanism with sub-puzzles. Hash-based.
  - Without requiring hashes in the generation → Aura et al.

Intrusion detection systems (IDS)

- The role of IDS.
- IDS Models: Anomaly, Misuse, Specification-based.
- Architecture: Agents (host or network based), director, notifier.
- Handling intrusions.
- Honeypots.

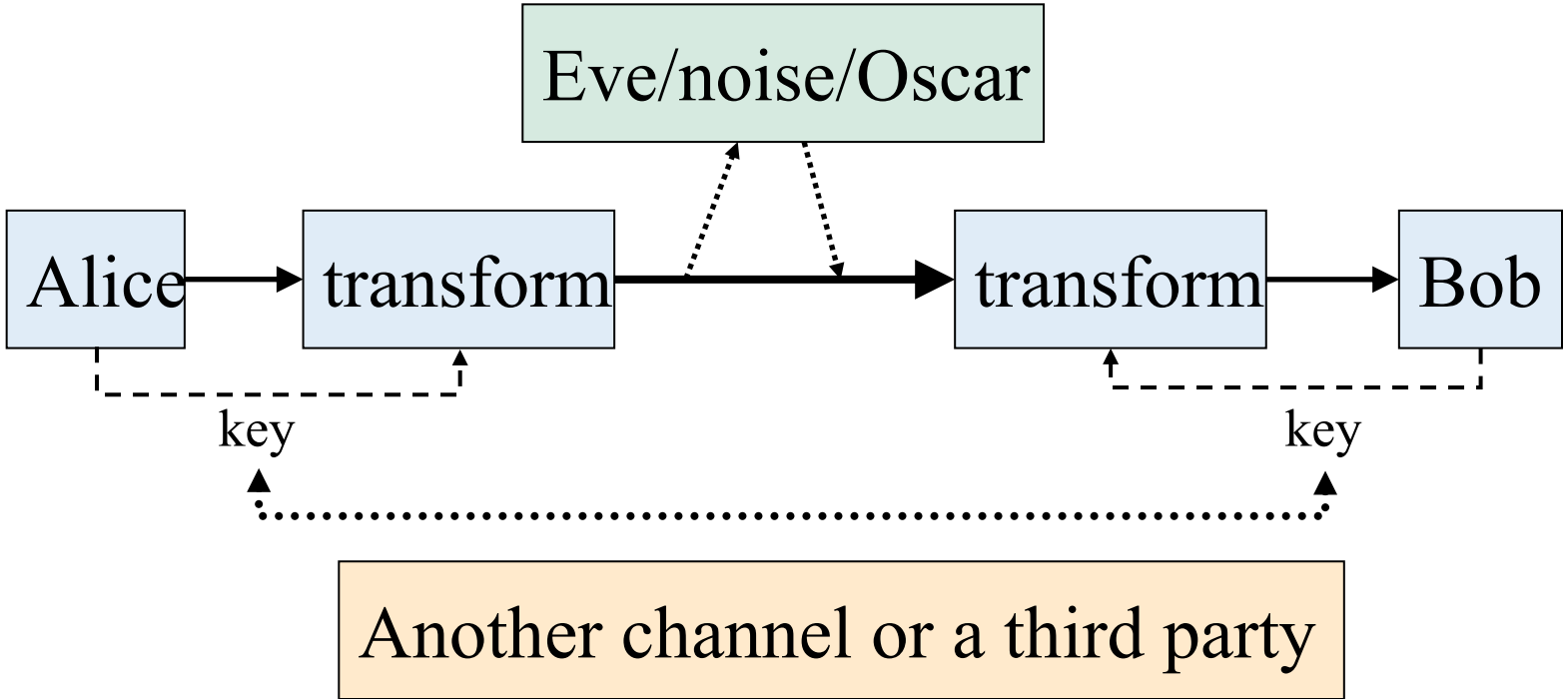
Firewalls

- Assumptions regarding the use of firewalls.
- The role of firewalls.
- Type of firewalls.
  - Packet-filtering firewall.
    - Stateful inspection firewalls.
  - Application-level gateway.
    - Also called proxy server.
  - MAC layer firewalls.
- Bastion hosts.
- Firewall architectures



Side channel attacks?

- It's useful to know what side channels are first!
- There is a standard communication channel…
  - Side channels are another source of information, likely dependent on the implementation and likely the cryptographic device, rather than the ciphertext and plaintext/ciphertext relations.



- An example timing attack:
  - With target key k and input x:

```
If ( k[i] == 1 & x[i] == 1 )
  do a modulo operation.
else
  don't do a modulo operation.
Endif
```

Relatively costly...

Databases

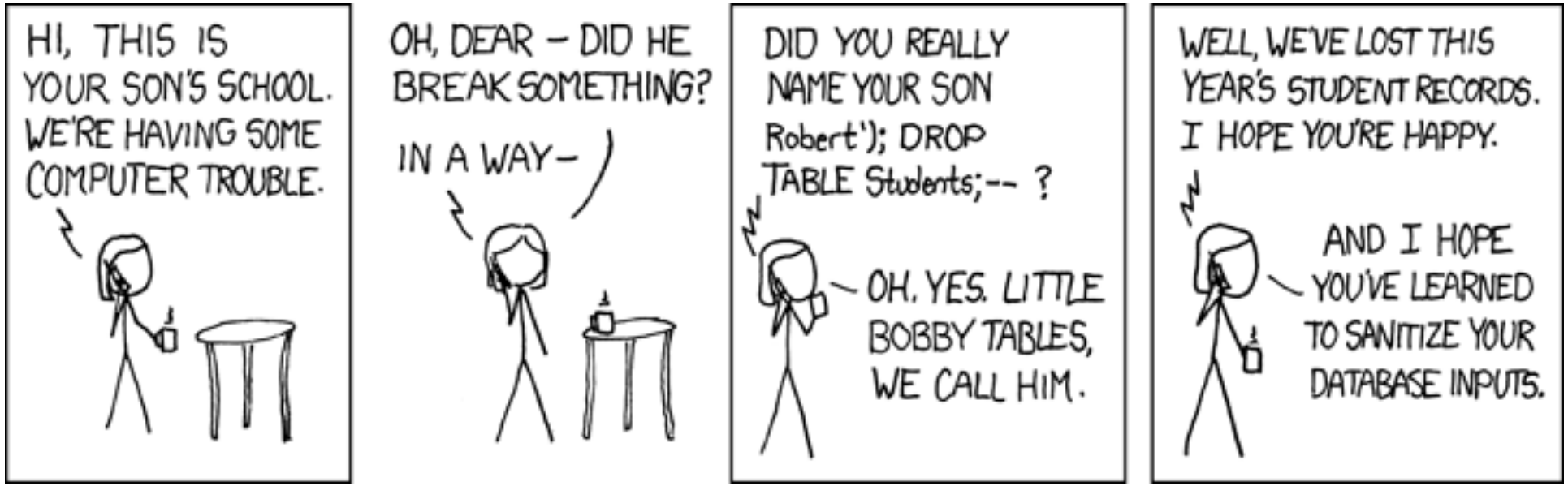
- Databases are an environment where we can see explicit examples of some of the security concerns mentioned.
- We started by looking at the difference between data and information, and we difference between file systems and databases.
- We briefly described some of the types of information we might want to protect, and mentioned the basic security properties: CIA.

Statistical databases

- An aggregate-query interface.
- A variety of different levels of disclosure.
  - We might not want people getting certain aggregate date either.
- Inference: The derivation of sensitive information from non-sensitive (aggregated) data.
- Attacks: Direct, indirect, trackers …
- Protection: Query set restriction, data perturbation, output perturbation, …

SQL injection

- It's often about checking input!



http://xkcd.com

Exam

- Duration: 3 hours
- 3 parts
  - Part A: filling the blanks
  - Part B: short questions & answers
  - Part C: questions with sub-questions.

Exam overview

- Marks: **60, *worth 60%***.
  - Remember, you need at least 40% to pass the exam, i.e., **24/60**.
- 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
    - 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.

Good Luck!