COMP3052.SEC Computer Security

Session 03: Foundations of Security

ACKNOWLEDGEMENTS

- Some of the materials we use this semester may come directly from previous teachers of this module, and other sources ...

- Thank you to (amongst others):
  - Michel Valstar, Milena Radenkovic, Mike Pound, Dave Towey, …

OVERVIEW

- Key Concepts
- Fundamental Dilemma
- Data vs. Information
- Principles of Computer Security Design
- Summary

KEY CONCEPTS

- Security
- Computer Security
- Confidentiality
- Integrity
- Availability
- Accountability
- Nonrepudiation

SECURITY

- Security:
  - Security is about the protection of assets
  - Knowledge of assets and their value is vital
- Protection measures:
  - Prevention – sometimes the only feasible measure
  - Detection
  - Reaction
    - Recovery? Manual? Automatic?

COMPUTER SECURITY

- Traditionally defined by three areas: **CIA**
  - Confidentiality
    - *prevention of unauthorised disclosure of information*
  - Integrity
    - *prevention of unauthorised modification of information*
  - Availability
    - *prevention of unauthorised withholding of information or resources*

ACTIVITY ...

- Write down a list of as many security measures you can think of relating to:
  - Confidentiality
  - Integrity
  - Availability
- Are there any other areas?
- Which are higher or lower priorities?

CONFIDENTIALITY

- The prevention of unauthorised users reading sensitive (private, secret) information
- Privacy – protection of personal data
- Secrecy – protection of data of an organisation
- Examples:
  - Hide document's content
  - Hide document's existence (Unlinkability and Anonymity)

INTEGRITY

- Informally
  - Making sure everything is as it is supposed to be.
- Formally
  - Integrity deals with the prevention of unauthorised writing.

INTEGRITY

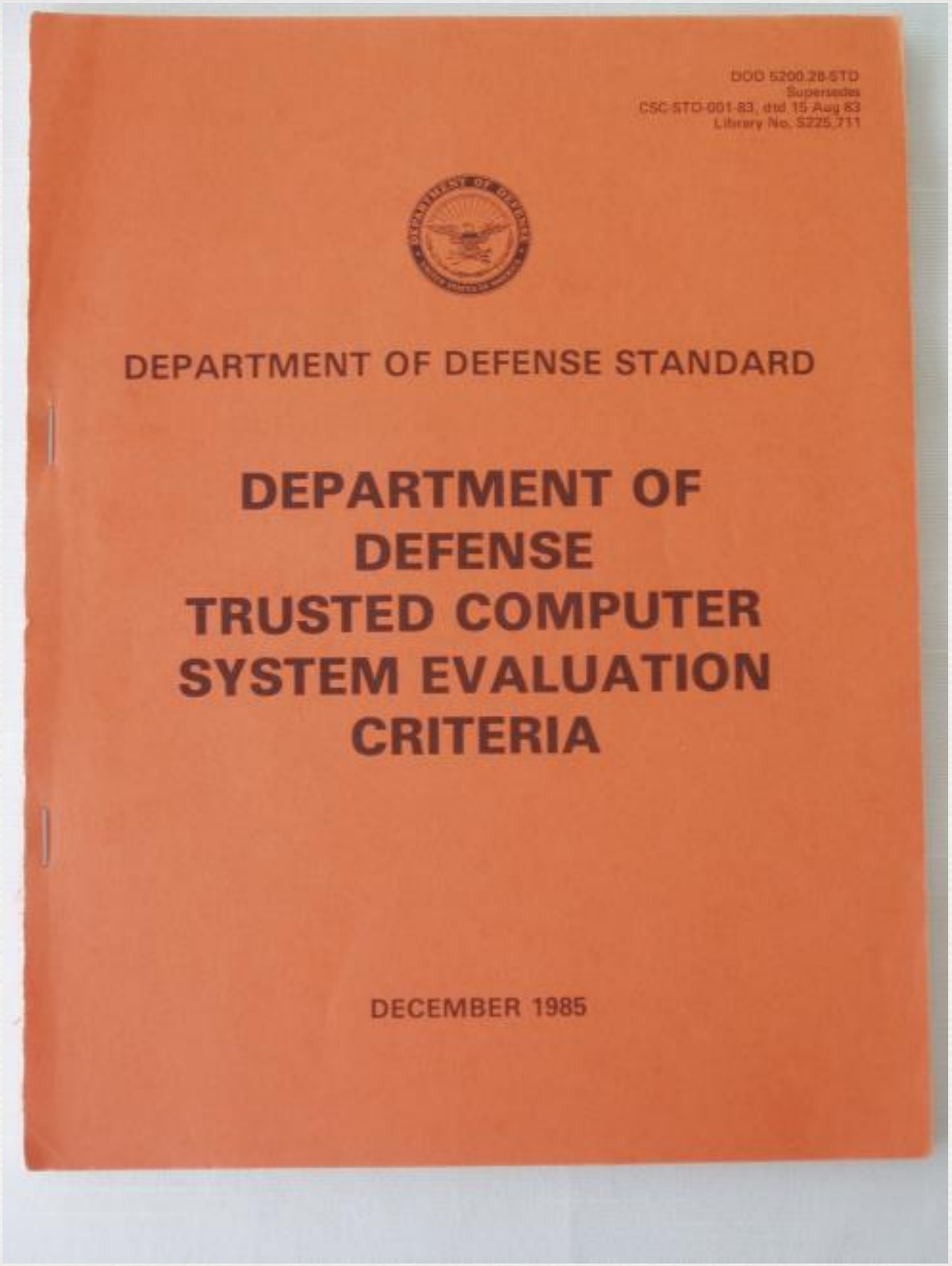
- The prevention of unauthorised modification of data, and the assurance that data remains unmodified
- Examples:
  - Distributed bank transactions
  - Database records

I promise to pay Dave the
sum of Twenty RMB
Thousand
^

INTEGRITY

- Informally
  - Making sure everything is as it is supposed to be.
- Formally
  - Integrity deals with the prevention of unauthorised writing.
- Data Integrity

  "The state that exists when computerised data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction." [Orange Book]

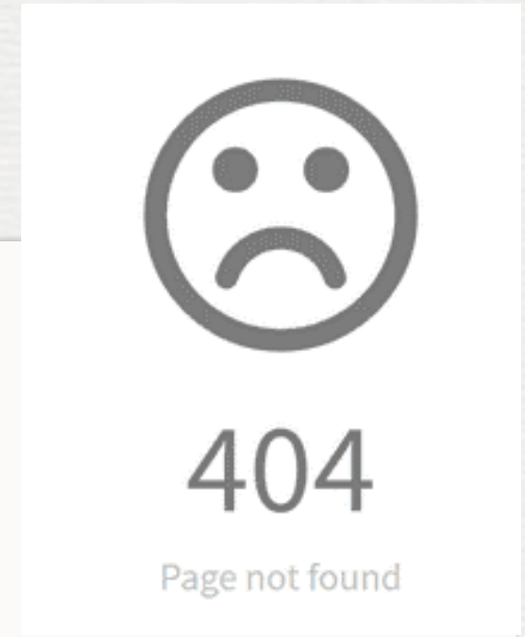

DOD 5200.28-STD
Supersedes
CSC-STD-001-83, dtd 15 Aug 83
Library No. S225,711
DEPARTMENT OF DEFENSE STANDARD
DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA
DECEMBER 1985

AUTHENTICITY

- Just because we have integrity, doesn't mean we have authenticity
  - Can we verify the sender?
  - Does it have freshness?

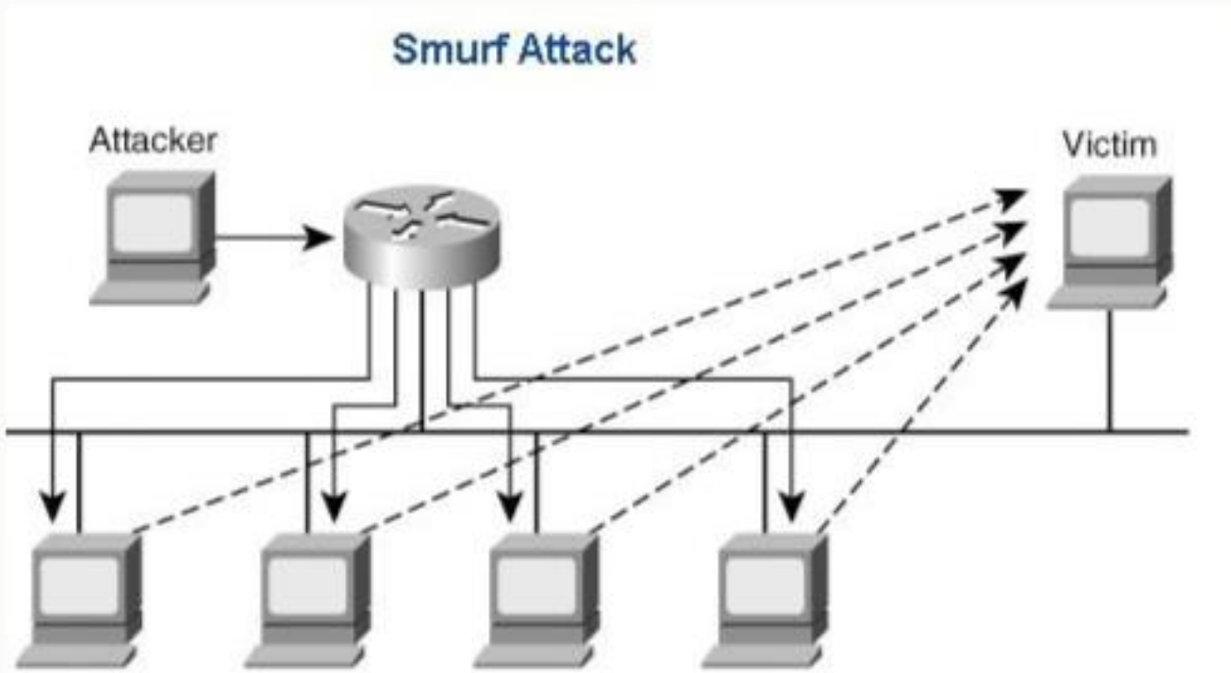
- Authenticity = Integrity + Freshness
- Freshness may seem trivial, but it's pretty important in bank transactions!

AVAILABILITY



- Availability
  - *"The property of being accessible and useable upon demand by an authorised entity."*
- We want to prevent denial of service (DoS):
  - *"The prevention of authorised access to resources or the delaying of time-critical operations."*

SMURF

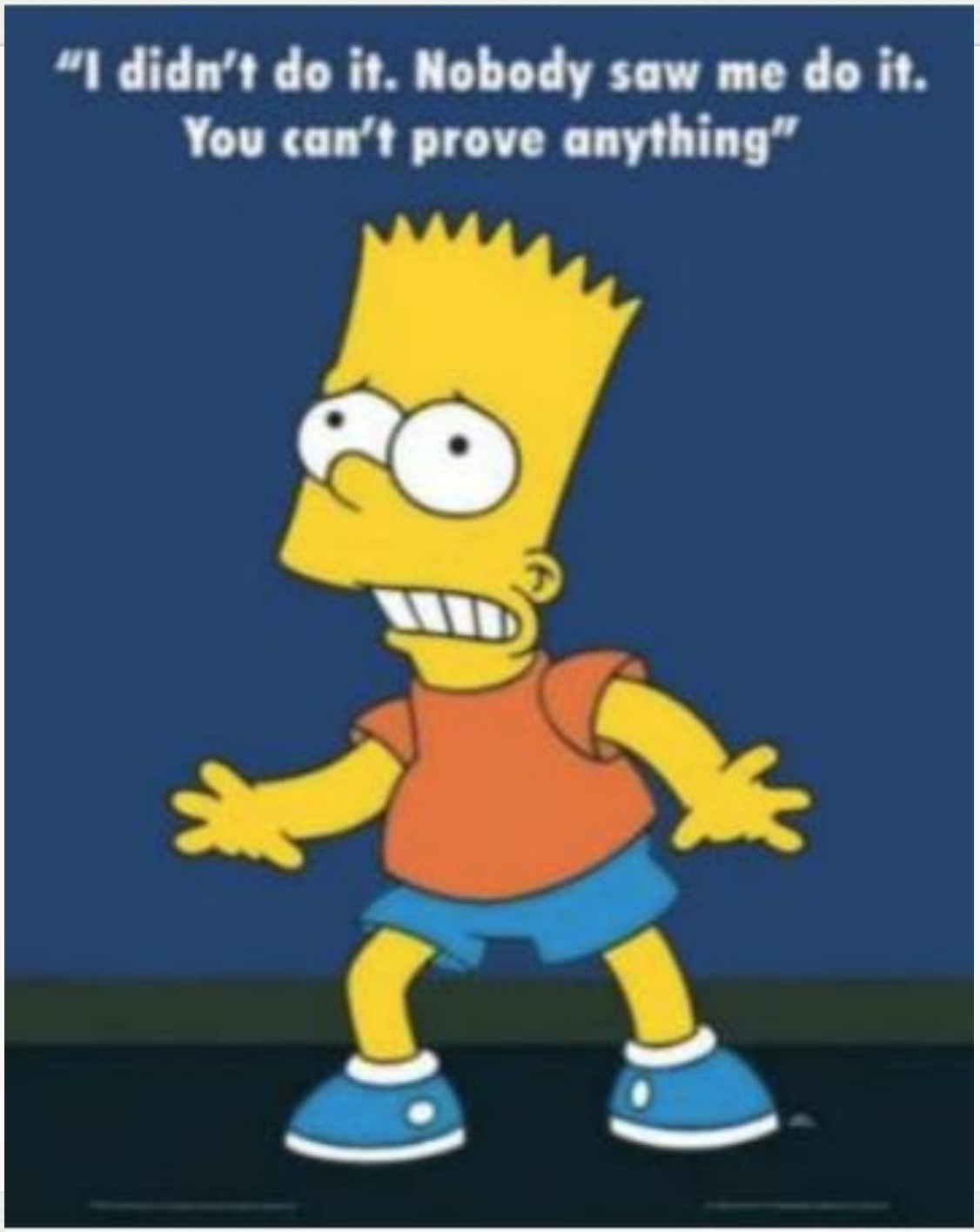


- Attacker sends ICMP echo request (ping) to broadcast address of a network, spoofing the sender address to be that of the victim

ACCOUNTABILITY

- Users should be held responsible for their actions
- System should identify and authenticate users
- Audit trail should be kept
- *"Audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party"*

NON-REPUDIATION



NON-REPUDIATION

- Non-repudiation provides un-forgeable evidence
- Evidence verifiable by a third party
  - E.g., notaries, digital certificates, …
- Nonrepudiation of:
  - origin – sender identification
  - delivery – delivery confirmation
- Relate to physical security (keycards,…)

RELIABILITY

- Reliability - against (accidental) failures
- Safety - impact of system failures on their environment
- Security is an aspect of reliability, and *vice versa*!
- Dependability

  "The property of a computer system such that reliance can justifiably be placed in the service it delivers"

OUR DEFINITION

- Computer Security – What?

  "Deals with the prevention and detection of unauthorised actions by users of a computer system"

- Computer Security – Why?

  "Concerned with the measures we can take to deal with intentional actions by parties behaving in some unwelcome fashion"

REMEMBER

- No single definition of security exists
- When dealing with security material, do not confuse your notion of security with that used in the material

FUNDAMENTAL DILEMMA

"Security-unaware users have specific security requirements but usually no security expertise."

- Trade-off between security and ease of use

FUNDAMENTAL DILEMMA

- In contrast, conflict between security and ease of use:

- Engineering trade-off:
  - Security mechanisms need increased computational resources
  - Security interferes with working patterns of users
  - Managing security is work – thus better (G)UI wins

DATA VS INFORMATION

- Security is about controlling access to information and resources
  - This can be difficult, thus controlling access to data is more viable
  - Data – Means to represent information
  - Information – (subjective) interpretation of data
- Problem of inference …

PROBLEM OF INFERENCE

- Focusing on data can still leave information vulnerable
- Consider a medical database
  - Medical records ***cannot*** be queried
  - Aggregates like prescription totals ***can*** be
- Carefully chosen queries can narrow down who has what conditions
  - A covert channel
  - Compare:
    - "Joe's criminal record not found in the DB"
    - "You do not have permission to access to Joe's criminal record"

SECURITY DESIGN: PRINCIPLES

- Computer security is NOT rocket science if:
  - approached in a systematic, disciplined & well planned manner
  - from the inception of a developed / designed system

- However:
  - if added as an afterthought to an existing, complex system -> TROUBLE!

SECURITY DESIGN: PRINCIPLES

- Fundamental Design Principles:
  - Focus of Control
  - Complexity vs. Assurance
  - Centralised or Decentralised Controls
  - Layered Security

FOCUS OF CONTROL

- **1st Design Decision**:

In a given application, should the protection mechanisms in a computer system focus on:

Data

Operations

Or users?

Permitted manipulation of data e.g. consistency check

Permitted invocations e.g. transfermoney()

Permissions for specific users
e.g. /home/name/

COMPLEXITY VS ASSURANCE

- **2nd Design Decision**:

Do you prefer simplicity- and higher assurance- to a feature-rich security environment?

This decision is linked to the fundamental dilemma!

Feature-rich security systems and high assurance do not match easily

(DE) CENTRALISED CONTROLS

- **3rd Design Decision**:

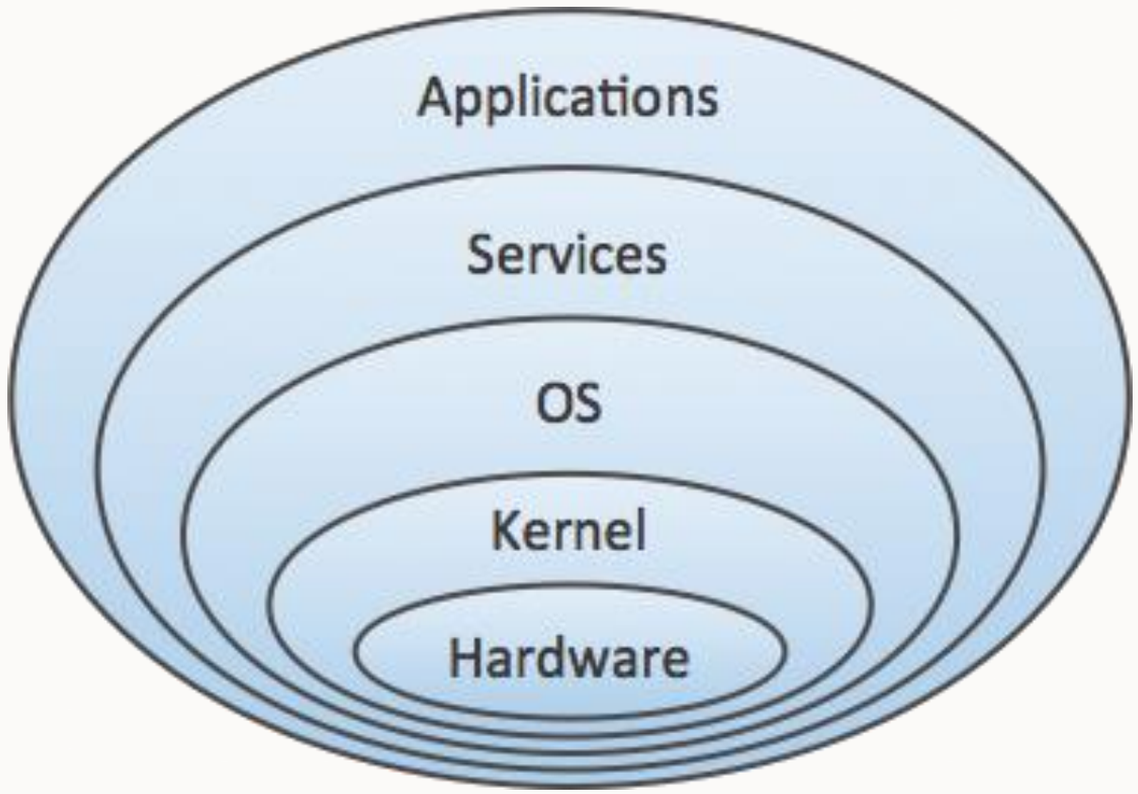
Should the tasks of defining and enforcing security be given to a central entity or should they be left to individual components in a system?

Central entity – could mean a bottleneck

Distributed solution – more efficient but harder to manage

THE ONION MODEL

- We can visualise our security model in layers
- Each layer protects a boundary, and relies on the security of the layers below



THE LAYER BELOW

- Every protection mechanism has a defined security perimeter

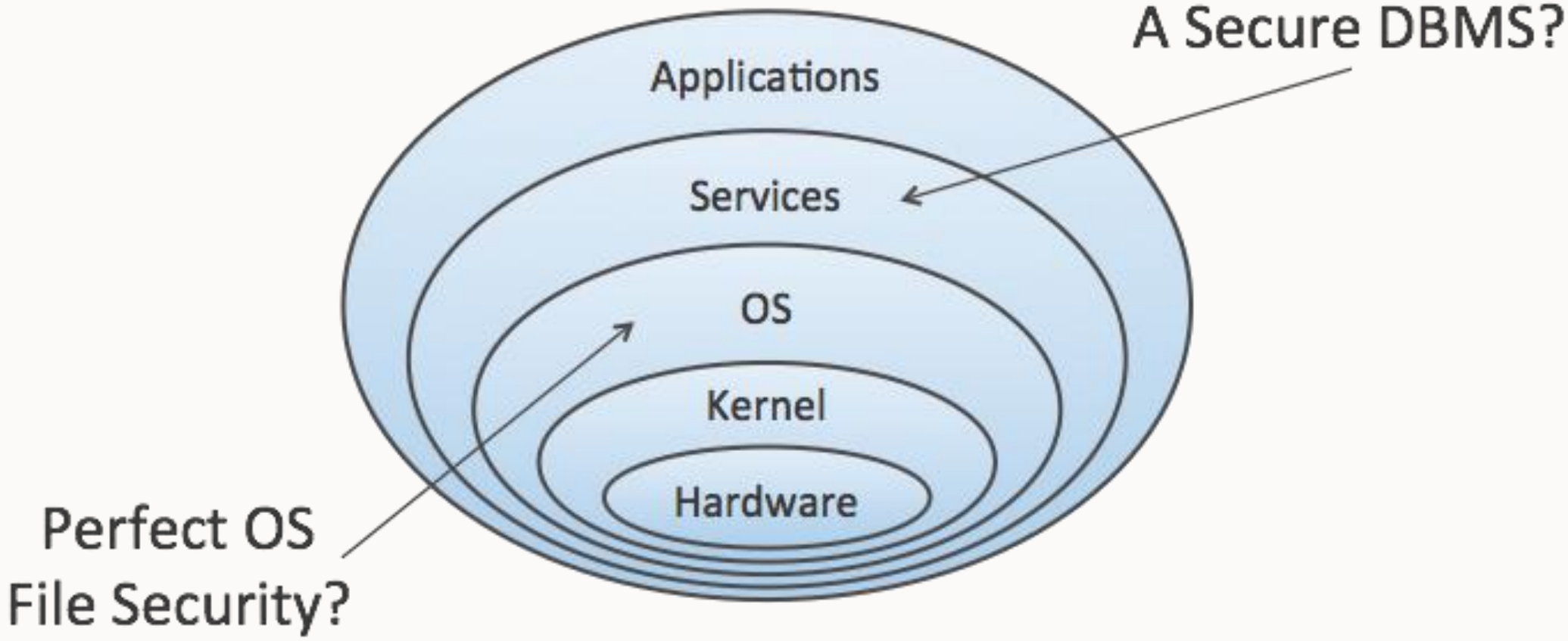
Security perimeter – parts of a system that can be used to disable the protection mechanism lying within

4th Design Decision:

How can you prevent an attacker getting access to a layer below the protection mechanism?

THE LAYER BELOW

- A good security layer built upon an insecure layer is useless



SUMMARY

- Summary:
  - Definitions
  - Fundamental Dilemma
  - Data vs. Information
  - Principles of Computer Security
  - The Layer Below

Read:

1. Gollman: Chapter 3
2. Anderson: Section 1.7