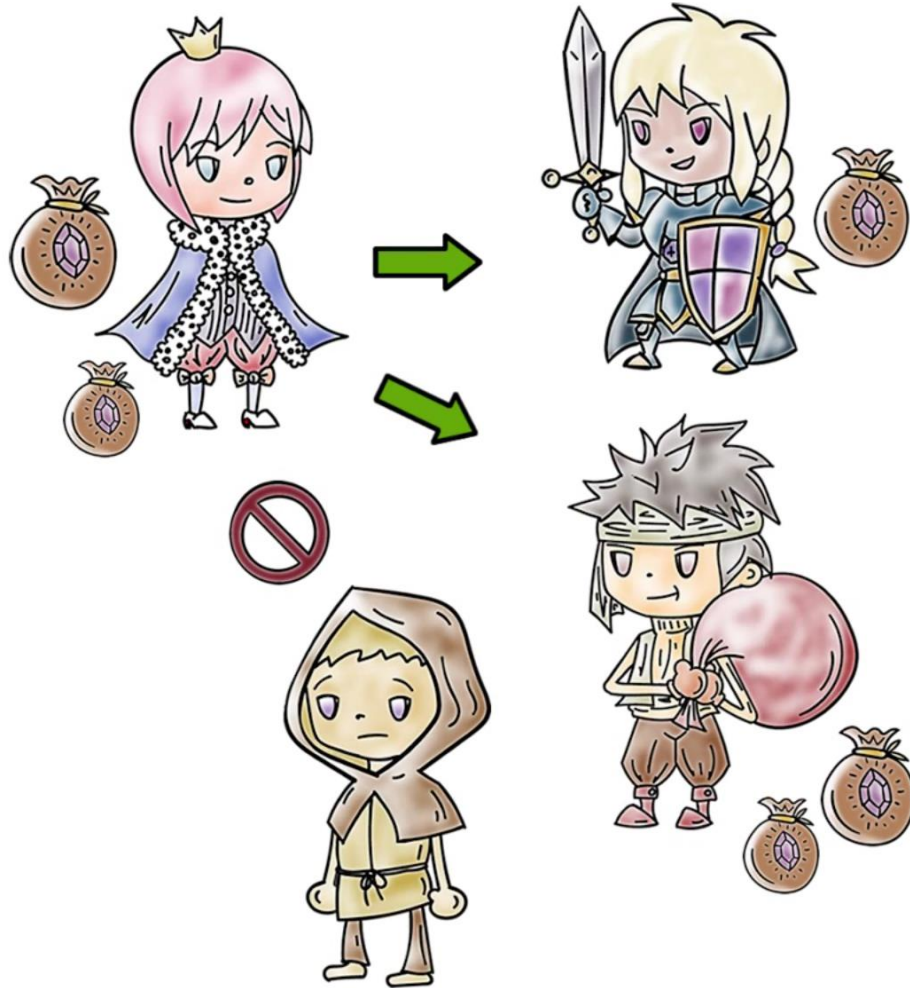


Mandatory Access Control

Lesson Introduction

- Understand need for **mandatory access control (MAC)** and **multi-level security**
 - Explore several **MAC models**
 - Understand **assurance techniques for a trusted computing base (TCB)**
-

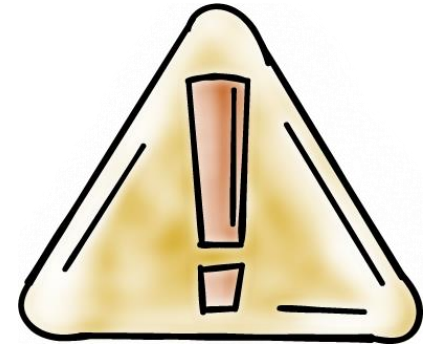
Discretionary Access Control



In discretionary access control (DAC), **owner of a resource decides** how it can be shared

- Owner can choose to give **read or write access to other users**

Discretionary Access Control



Two problems with DAC:

- You cannot control if someone you share a file with will not further share the data contained in it
 - **Cannot control “information flow”**
- In many organizations, **a user does not get to decide how certain type of data can be shared**
 - Typically the employer may mandate how to share various types of sensitive data
 - Mandatory Access Control (MAC) helps address these problems



DAC Quiz

Check the best answer:

In a certain company, payroll data is sensitive. A file that stores payroll data is created by a certain user who is an employee of the company. Access to this file should be controlled with a...

- ☐ DAC policy that allows the user to share it with others judiciously
- ☐ It must use a MAC model as the company must decide who can access it

Mandatory Access Control (MAC) Models



User works in a company and the **company decides how data should be shared**

- Hospital owns patient records and limits their sharing
 - **Regulatory requirements may limit sharing**
- HIPAA for health information

Mandatory Access Control (MAC) Models

Military and intelligence agencies:



Data has **associated classification level** and users are cleared at various levels

- Top secret, secret, confidential etc.
- Limits on **who can access data at a certain level**
 - User cleared only at secret level should not be able to access top secret data
- Also called **multilevel security (MLS)**

Implementing MAC

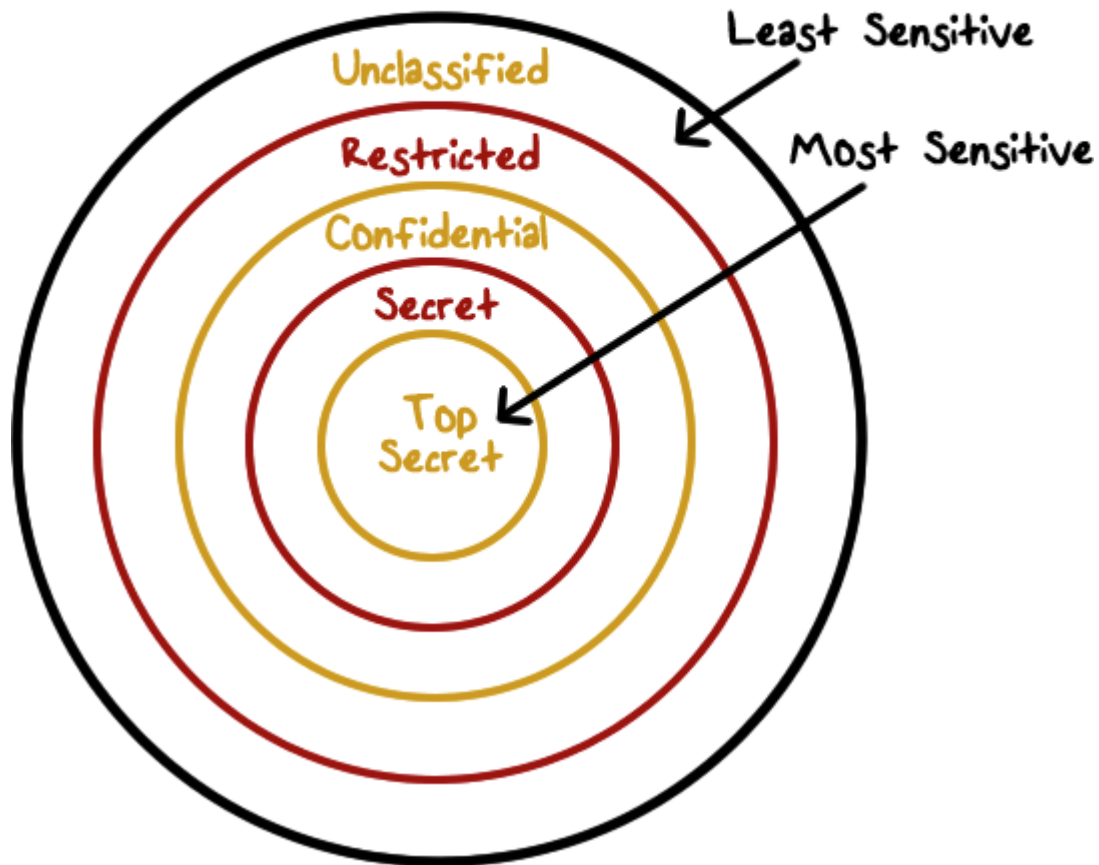


Labels: A Key Requirement for Implementing MAC

- indicate sensitivity/category of data or clearance/need-to-know requirements of users
- TCB associates **labels with each user and object and checks them when access requests are made**
 - Need to relate labels to be able to compare them
- Exact nature of labels **depends on what kind of model/policy is implemented**
 - DoD models include classification/clearance level and a compartment in the label
 - Commercial policies are different but use labels to deal with conflict-of-interest, separation-of-duty etc.

Implementing MAC

Example of Labels/MAC in a DoD Environment:



1. **Label** = (sensitivity level, compartment)

1. Let us consider highly sensitive documents that have information about various arms stockpiles.

L1 = (TS, {nuclear, chemical})

L2 = (S, {nuclear, conventional})

1. Providing confidential access to documents (Bell and La Padula or BLP Model)



Health Data Quiz

Check the best answer:

A hospital is found to be lax in securing access to patient records after it suffers a major breach. It may have violated the following policy:

☐

HIPAA

☐

BLP



Security Clearance Quiz

Check the best answer:

Highly sensitive defense or intelligence information should only be accessed by cleared personnel. Approximately, how many people in the United States have various types of clearances?

☐

10,000

☐

1,000,000

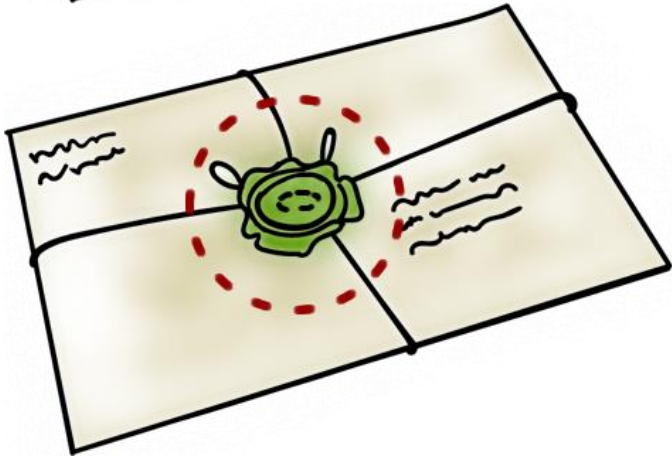
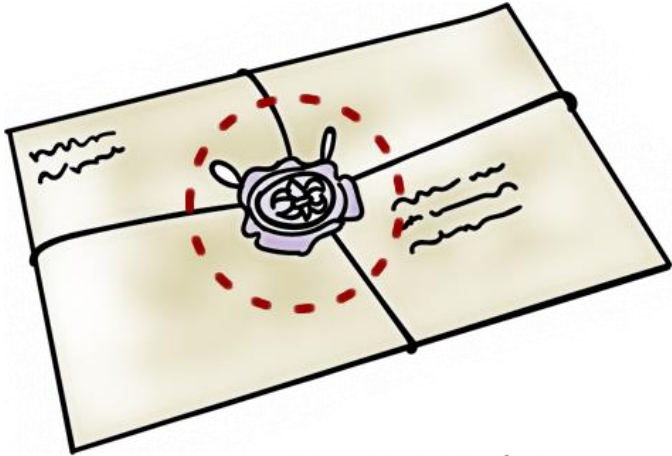
☐

100,000

☐

5,000,000

Comparing Labels



- Assume **sensitivity levels are totally ordered**
($TS > S > C > U$)
- Compartments are sets which can only be partially ordered
- **How do we order labels?**

Comparing Labels

$$L_1 = (X_1, \text{Comp}_1), L_2 = (X_2, \text{Comp}_2)$$

- L_1 dominates L_2 : $l_1 > l_2$ and $\text{Comp}_1 \geq \text{Comp}_2$
- or L_1 is dominated by L_2 : $l_1 < l_2$ and $\text{Comp}_1 \leq \text{Comp}_2$
- or $L_1 = L_2$: $l_1 = l_2$ and $\text{Comp}_1 = \text{Comp}_2$
- or L_1 and L_2 are not comparable : $L_1 \not\geq L_2$ and $L_1 \not\leq L_2$
and $L_1 \neq L_2$

Ordering Among Labels

Ordering among labels defines a structure called a lattice:

Example:

Partial Order

$$L_1 = (TS, \{A, B, C\})$$

$L_1 > L_2?$ Yes

$$L_2 = (S, \{A, B\})$$

$L_2 < L_1?$ Yes

$$L_3 = (S, \{B, C, D\})$$

L_1 and L_3
are not compared



Order Quiz

Select the best answer:

The “<” relation among all real numbers defines a...

☐

Total order

☐

Partial order



Label Domination Quiz

Select the best answer:

If $L1 = (\text{secret}, \{\text{Asia}, \text{Europe}\})$ and $L2 = \{\text{top-secret}, \{\text{Europe}, \text{South-America}\}\}$,

☐

L1 dominates L2

☐

L2 dominates L1

☐

Neither L1 nor L2 dominates the other one



Sensitive Data Quiz

Select the best answer:

Assume that label L1 or a document D1 dominates label L2 of document D2 when these labels are defined by (sensitivity level, compartment).

☐

D1 contains more sensitive data than D2.

☐

D2 is more sensitive than D1.

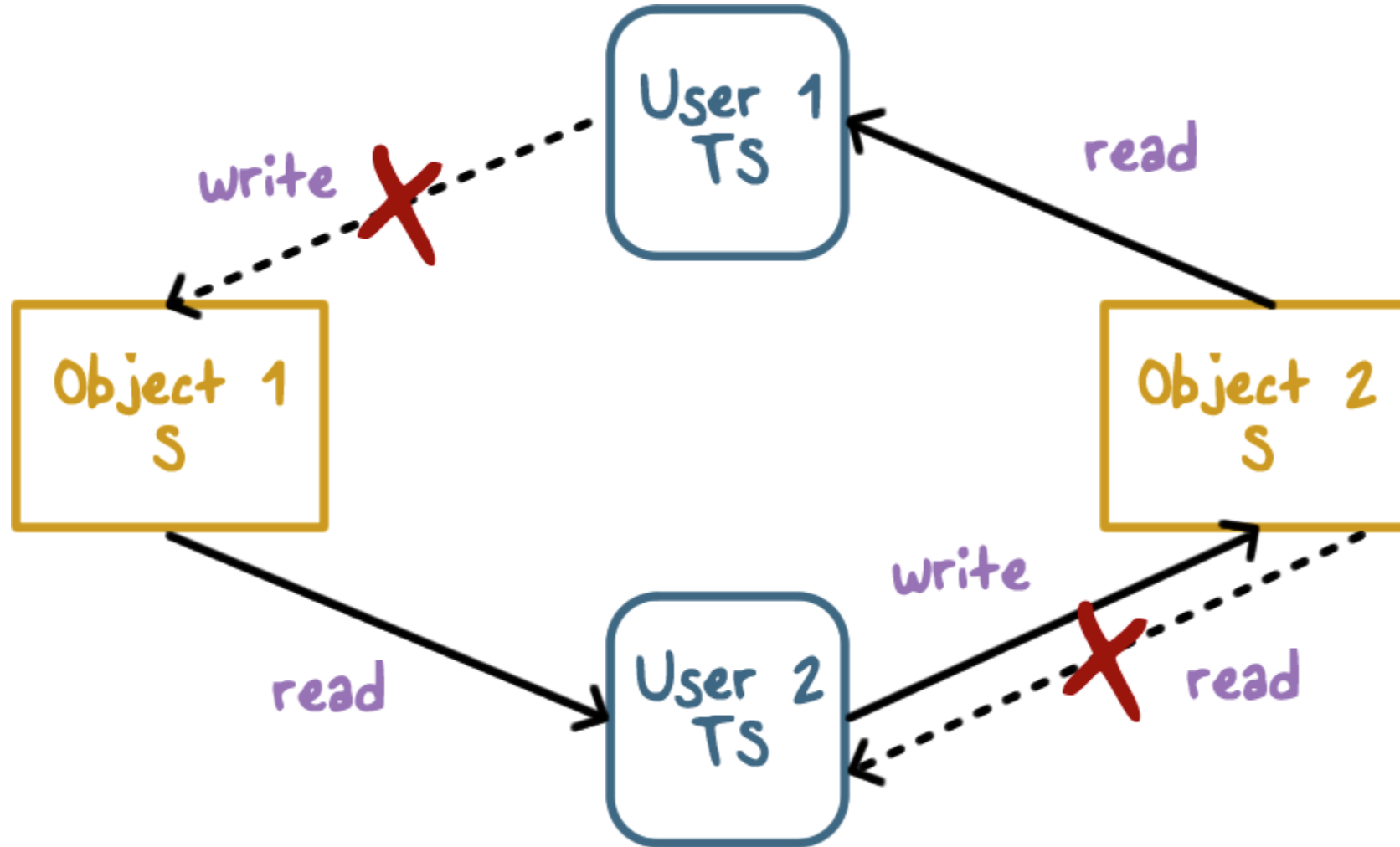
☐

The data contained in D2 has a narrower scope as defined by its compartment

Using Labels for MAC: Confidentiality

- **Bell and La Padua or BLP Model** (Developed by DoD)
 - Assumes classification of data (TS, S, C, U) and clearances for subjects
- **Read/write rules**
 - User with label L1 can read document with label L2 only when L1 dominates L2
 - **Read-down rule (simple security property)**
 - User with label L1 can write document with label L2 when L1 is dominated by L2
 - **Write-up rule (star property)**

Preventing Information Flow with BLP





Unclassified Documents Quiz

Select the best answer:

Since an unclassified document contains no sensitive information, it can be read or written by anyone in a system that implements BLP

☐

True

☐

False



Classified Data Quiz

Select the best answer:

BLP allows an unclassified user to write a top secret document.

☐

True

☐

False



BLP Model Quiz

Select the best answer:

Tranquility principle in the BLP model states that classification of a subject or object does not change during a session. This principle is needed to avoid...

☐

Information flow that may violate confidentiality requirements defined by BLP

☐

To reduce overhead associated with change of classification level

Other MAC Models



- Biba is dual of BLP
- Focuses on integrity rather than confidentiality
- Read-up and write-down rules

Example:

- Integrity level could be high, medium or low
- Compartment could be similar to BLP and captures topic(s) of document
- Low integrity information should never flow up into high integrity documents

Policies for Commercial Environments



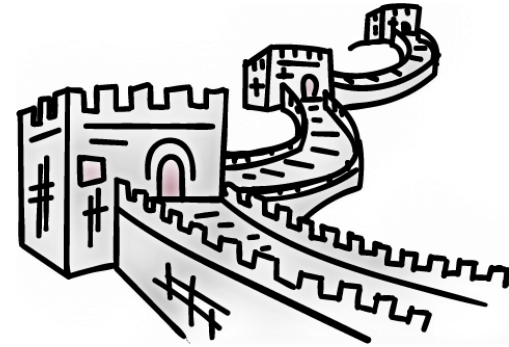
- **User clearance is not common**
- Other requirements exist
 - **Data only be accessed by certain application** (e.g., payroll)
 - **Separation-of-duty and conflict-of-interest requirements**

Policies for Commercial Environments

- Clark-Wilson Policy

Users → Programs
(transactions) → Objects

- Same user cannot execute two programs that require separation-of-duty

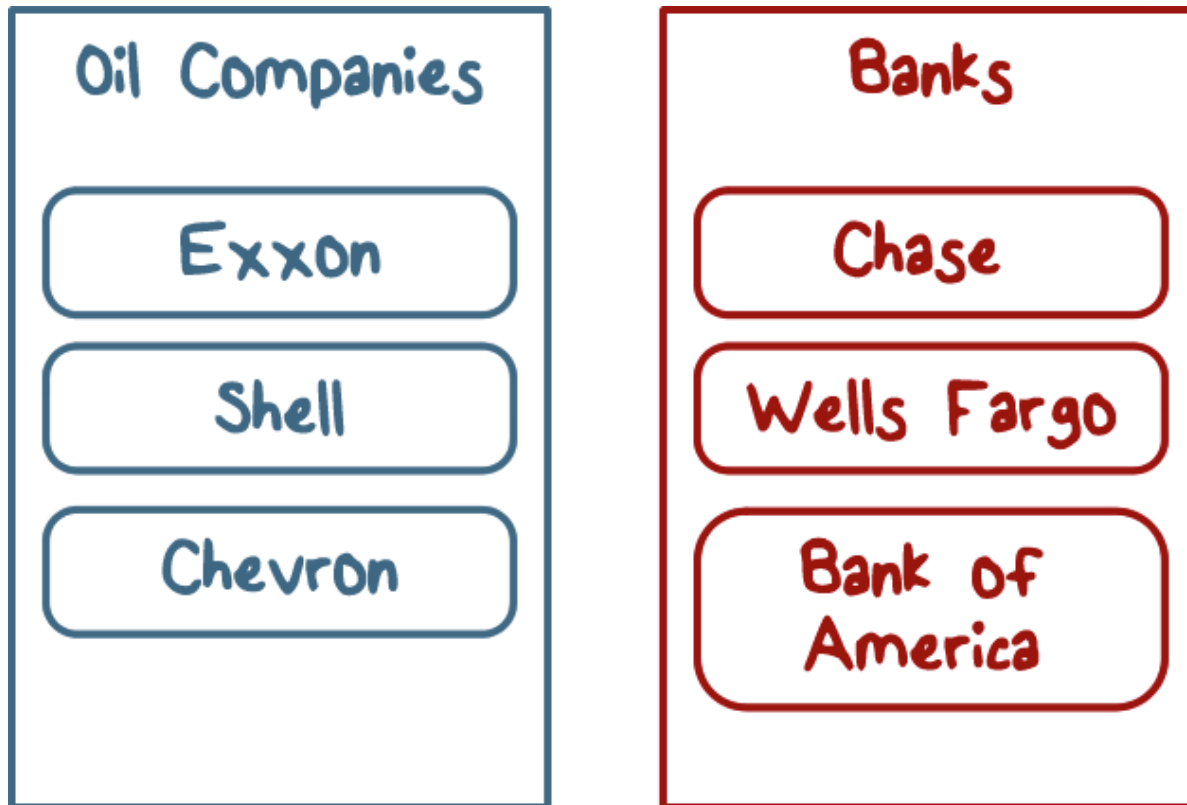


- Chinese Wall Policy

- Deals with conflict of interest

Chinese Wall Policy (Conflict of Interest)

Objects are put into conflict classes:



The user **can access any object** as long as he/she has not accessed an object from another company **in the same conflict class**.

Policies for Commercial Environments

Oil Companies

Exxon

Shell

Chevron

Banks

Chase

Wells Fargo

Bank of
America



Clark-Wilson Quiz

Select the best answer:

Clark-Wilson is a mandatory access control policy because...

☐

Any user in a company can decide what files can be accessed by a program

☐

Only the company can decide (e.g., sysadmin) what files can be accessed by a program.



Col Quiz

Select the best answer:

A large law firm currently has two client companies that compete with each other. Thus, its lawyers working on cases related to one company must not be able to access documents related to the other company. To ensure proper access control, which policy should the law firm use?

☐

Clark-Wilson

☐

Chinese Wall



RBAC Quiz

Select the best answer:

Role-based access control (RBAC) is often used in a commercial setting. RBAC is an example of MAC because...

- ☐ File permissions are associated only with roles and not users
- ☐ Only the company can decide roles of its employees



MAC Support Quiz

Select the best answer(s):

Which of the following operating systems supports a BLP-like model?

☐

SELinux

☐

MacOS

☐

Windows

☐

SCOMP

Trusted Computing Bases (TCB)

Revisiting Trusted Computing Base (TCB)



- How do we know TCB can be trusted?
- **Secure vs. trusted. vs high assurance**
 - Set of all hardware and software trusted to operate securely
 - Required for all other trust in the system security policy


Trusted Computing Bases (TCB)

Trusting Software:

- **Functional correctness**
 - Does what it was designed to do
- **Maintains data integrity**
 - Even for bad input
- **Protects disclosure of sensitive data**
 - Does not pass to untrusted software
- **Confidence**
 - Experts analyze program & assure trust
- **Statement giving security we expect system to enforce**
 - Do this formally when and where possible



TCB Design Principles

- **Least privilege for users & programs**
 - **Economy**
 - Keep trusted code small as possible, easier to analyze & test
 - **Open design**
 - Security by obscurity does not work
- 
- **Complete mediation**
 - Every access checked, attempts to bypass must be prevented
 - **Fail-safe defaults**
 - Default deny
 - **Ease of use**
 - Users avoid security that gets in their way



Least Privilege Quiz

Select the best answer:

Least privilege is useful for damage containment when something goes wrong. Is this principle applicable to a TCB that must be trusted?

☐

No, because a TCB is guaranteed to function correctly

☐

Yes, because TCB only provides high assurance and not a guarantee



TCB High Assurance Quiz

Select the best answer:

A TCB vendor claims its proprietary techniques help ensure high assurance, but cannot be disclosed. What principle does it violate?

☐

Complete mediation

☐

Open design



Design Principle Quiz

Select the best answer:

A home wireless router comes with a setting that does not encrypt traffic unless security settings are explicitly enabled. This violates...

☐

Ease of use principle

☐

Fail-safe default principle

How Do We Build a TCB: Support Key Security Features



- **Must implement certain security relevant functions**
 - Authentication
 - Access control to files & general objects
 - Mandatory access control (SELinux)
 - Discretionary access control (standard file permissions)

How Do We Build a TCB:

Support Key Security Features

- **Protection of data used by OS** (OS must protect itself)
 - Security features of trusted OSes
 - Object reuse protection
 - Disk blocks, memory frames reused
 - Process can allocate disk or memory, then look to see what's left behind
 - Trusted OS should zero out objects before reuse
 - **Secure file deletion**: overwrite with varying patterns of zeros & ones
 - **Secure disk destruction**: degaussing, physical destruction

How Do We Build a TCB:

Support Key Security Features

- **Complete mediation of accesses**
- Trusted path from user to secure system
 - Prevents programs from spoofing interface of secure components
 - Prevents programs from tapping path (e.g. keyloggers)
- **Audit log showing object accesses** – only useful if you /look/ at the log
 - Detect unusual use of the system

Kernel Design



- Security kernel **enforces all security mechanisms**
- **Good isolation, small size for verifiability, keeps security code together**
- Reference monitor controls access to objects (monitors all references to objects)
- **Tamperproof** [impossible to break or disable]
- **Un-Bypassable** [always invoked, complete mediation]
- **Analyzable** [small enough to analyze & understand]

Kernel Design

What is included in the trusted computing base (TCB)?



- **All parts of OS needed** for correct enforcement of security policy
 - Handles primitive I/O, clocks, interrupt handling, hardware capabilities, label checking
- **Virtualization**
 - Virtual machine provides hardware isolation, logical OS separation

Revisiting Assurance



Assurance: Ways of convincing ourselves that a model, design, & implementation are correct

Methods of assurance validation:

- Testing /Penetration testing
- Formal verification Validation
- Checking that developers have implemented all requirements
- Requirements checking, design & code reviews, system testing

Revisiting Assurance



Testing:

- Demonstrate existence of problem
- Cannot demonstrate absence of problem
- **Regression testing**: ensure that alterations do not break existing functionality / performance (regression: “going backwards”)

Revisiting Assurance



Challenges:

- Test case generation
- Code coverage
- Exponential number of different executions
- Different execution environments

Penetration testing:

- Ethical hackers attempt to defeat security measures
- Cannot demonstrate absence of problem

Revisiting Assurance



Formal verification: Checking a mathematical specification of program to ensure that security assertions hold.

- **Model checking**, automated theorem proving
- State variables w/ initial assignment, program specification describing how state changes, boolean predicates over state variables
- **Difficulty:** exponential time & space worst case complexity
- Model checking pioneers won the 2007 Turing Award



Reducing TCB Size Quiz

Check all applicable answers:

We discussed the need for reducing the size of the TCB.
This helps with...

☐

Testing of the TCB

☐

Verification of the TCB

☐

Isolation of the TCB



Testing TCB Quiz

Check the correct answer:

Testing is challenging for a complex system like a TCB because of...

☐

It is hard to cover all executions

☐

It can show both existence and absence of problems



Model Checking Quiz

A key problem with model checking is...

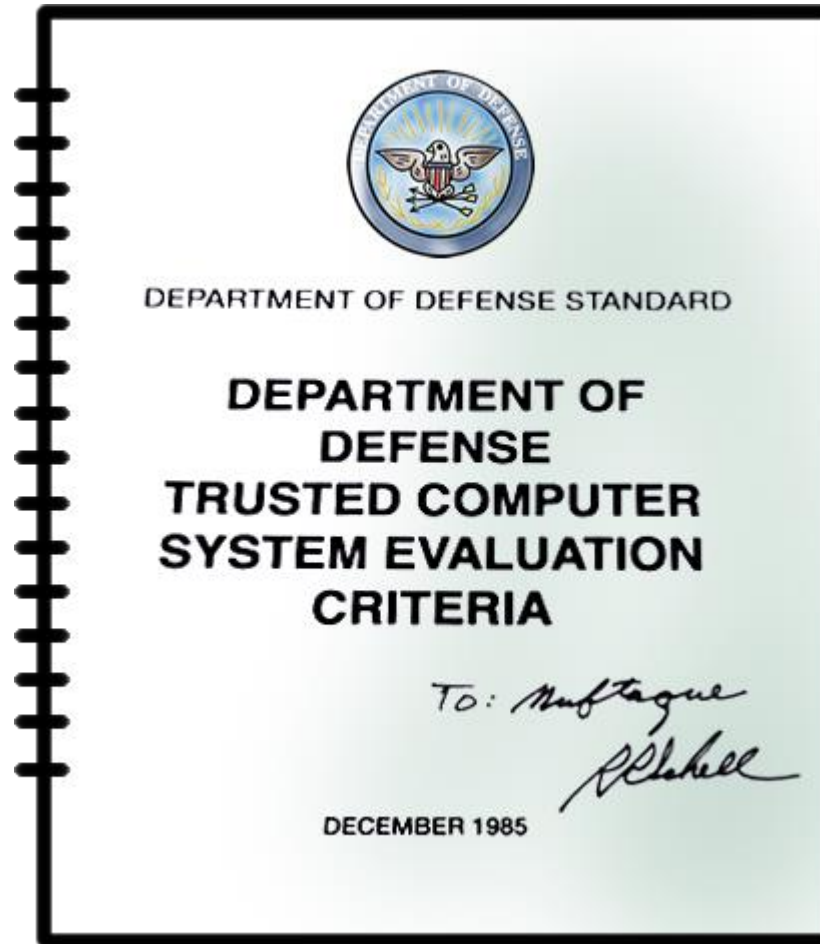
☐

It cannot show absence of a problem

☐

It does not scale to practical large size systems

Security Evaluations



Government Security Evaluations

- **U.S. Orange Book (late 1970's)**
- $D < C1 < C2 < B1 < B2 < B3 < A1$
 - **D**: no protection
 - **C**: discretionary protection
 - **B**: mandatory protection
 - **A**: Verified protection
- C1, C2, B1: security features common to commercial OSes
- B2: Proof of security of underlying model, narrative spec of TCB
- B3, A1: Formal design & proof of TCB





Government Security Evaluations

Common Criteria (2005) international standard

replaced orange book

- Originated out of European, Canadian, and US standards
- **Idea:** users specify system needs, vendors implement solution and make claims about security properties, evaluators determine whether vendors actually met claims
- **Evaluation assurance level** (EAL) rates systems
 - EAL1 most basic, EAL7 most rigorous



TCSEC Divisions Quiz

Many widely used operating systems **do not support MAC** and hence cannot be in a TCSEC division higher than...

☐ D

☐ C



Earning an EAL4 Certification Quiz

How did **VMware vCloud Networking and Security v5.5** system receive an EAL4+ certification?

- ☐ The system developers used formal techniques in its design and testing
- ☐ A systematic review and testing process was used by the system developers



Cost-Benefit Certification Tradeoffs Quiz

Many OS vendors **do not aim for the highest certifications** because...

☐

There is no market demand for such certifications

☐

Cost/benefit tradeoffs dictate the highest certification

Mandatory Access Control

Lesson Summary

- Provides enterprises **an ability to control how sharing** of sensitive information can be controlled
 - Can address both **confidentiality and integrity** but require added functionality with labels
 - **High level of assurance** for trusted systems is challenging
-