Chapter 13

Trusted Computing and Multilevel Security

Computer Security Models

Two fundamental computer security facts:

All complex software systems have eventually revealed flaws or bugs that need to be fixed

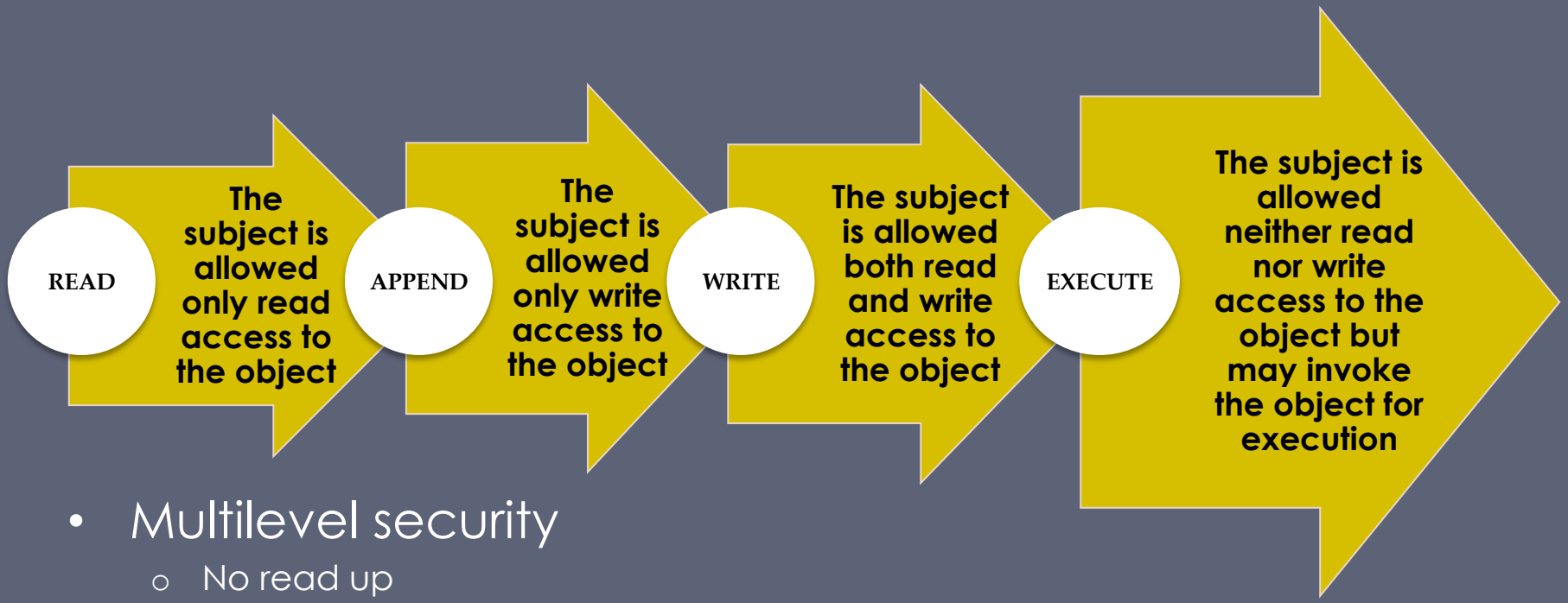
It is extraordinarily difficult to build computer hardware/ software not vulnerable to security attacks

- Problems involved both design and implementation
- Led to development of formal security models
  - Initially funded by US Department of Defense
- Bell-LaPadula (BLP) model very influential

Bell-LaPadula (BLP) Model

- Developed in 1970s
- Formal model for access control
- Subjects and objects are assigned a *security class*
  - Top secret > secret > confidential > restricted > unclassified
  - Form a hierarchy and are referred to as security levels
- A subject has a security clearance
- An object has a security classification
- Security classes control the manner by which a subject may access an object

Bell-LaPadula (BLP) Model Access Modes



- Multilevel security
  - No read up
    - Subject can only read an object of less or equal security level
    - Referred to as the simple security property (ss-property)
  - No write down
    - A subject can only write into an object of greater or equal security level
    - Referred to as the *-property

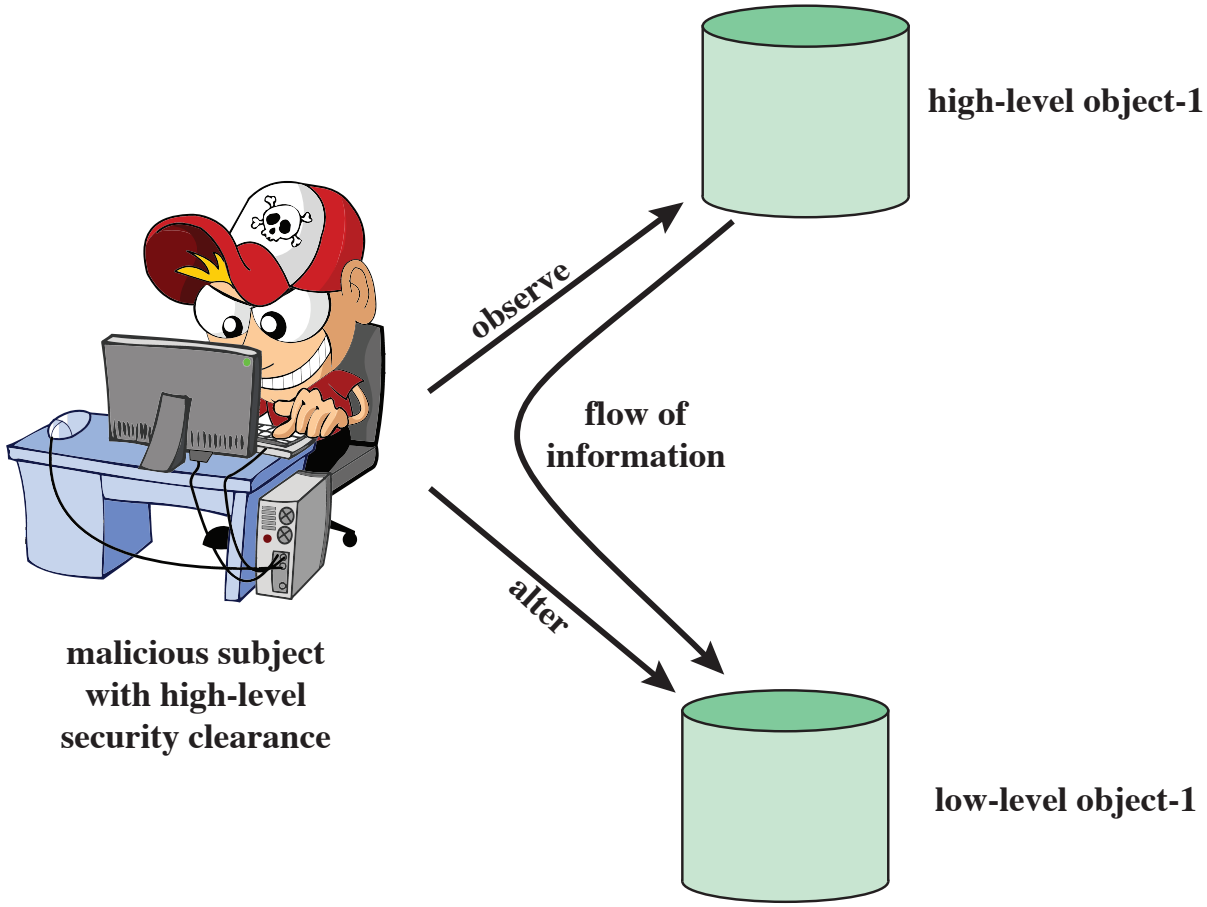


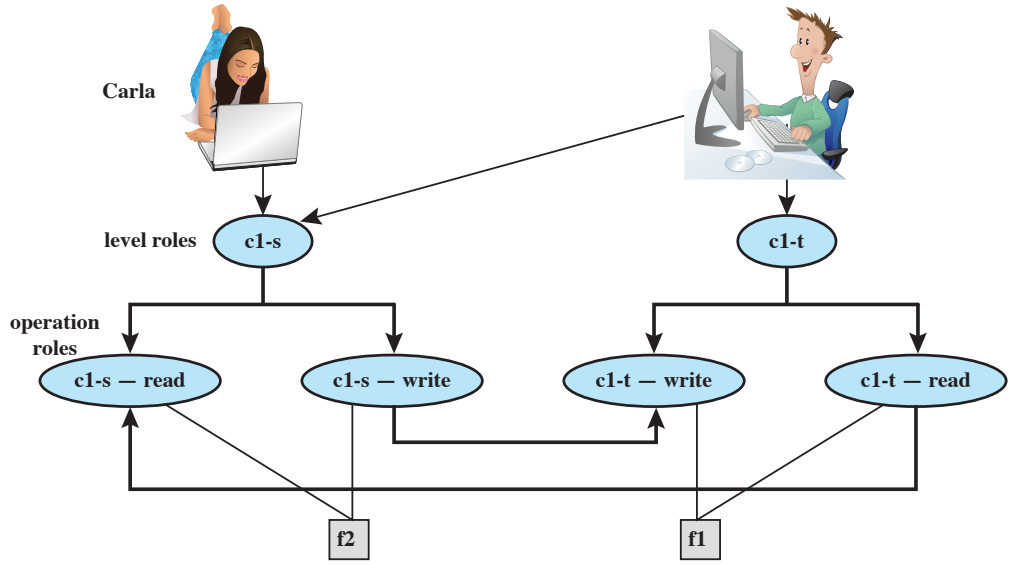
Figure 13.1 Information Flow Showing the Need for the *-property

BLP Formal Description

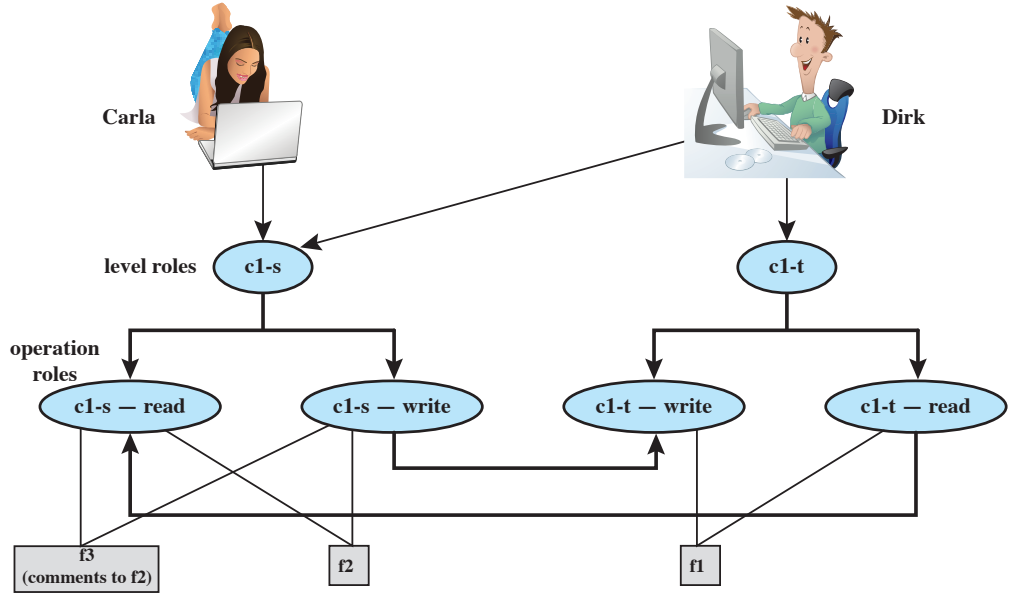
- Based on current state of system (b, M, f, H):
  (current access set b, access matrix M, level function f, hierarchy H)
- Three BLP properties:
  ss-property: (S_i, O_j, read) has $f_c(S_i) \geq f_o(O_j)$.
  *-property: (S_i, O_j, append) has $f_c(S_i) \leq f_o(O_j)$
  and
  (S_i, O_j, write) has $f_c(S_i) = f_o(O_j)$
  ds-property: (S_i, O_j, A_x) implies $A_x \in M[S_i$
- BLP give formal theorems
  - Theoretically possible to prove system is secure
  - In practice usually not possible

BLP Rules

1. Get access
2. Release access
3. Change object level
4. Change current level
5. Give access permission
6. Rescind access permission
7. Create an object
8. Delete a group of objects

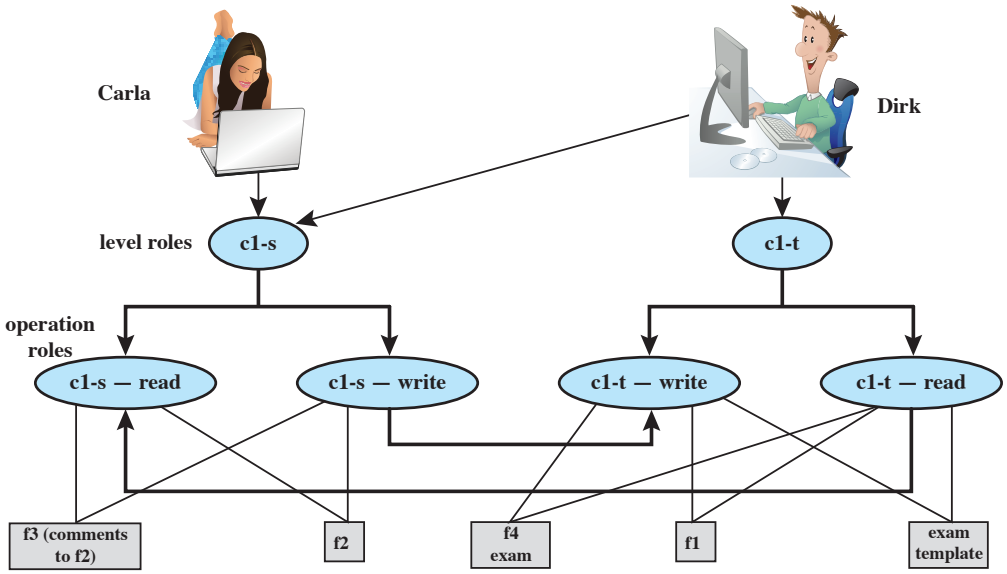


(a) Two new files are created: f1: c1-t; f2: c1-s

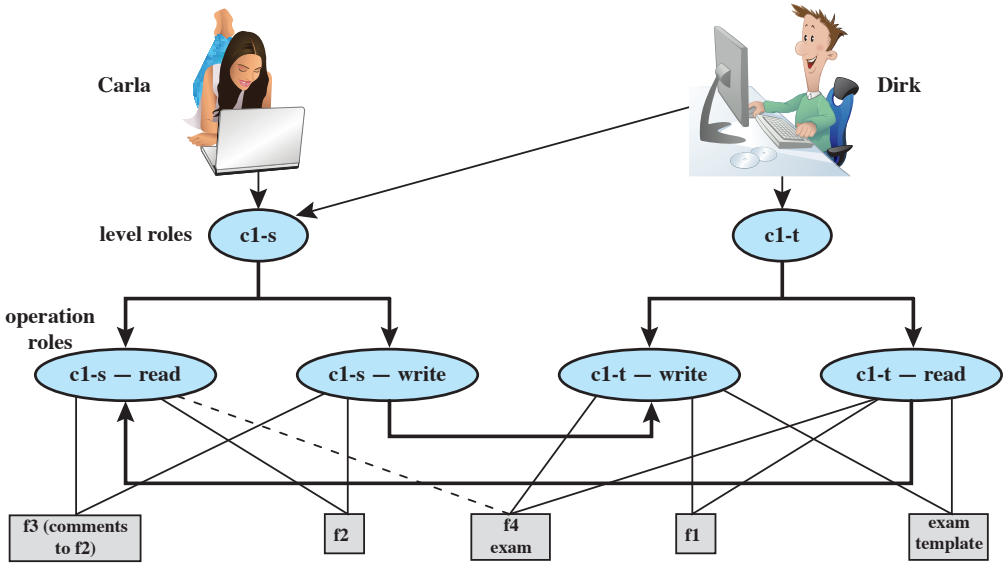


(b) A third file is added: f3: c1-s

Figure 13.2 Example of Use of BLP Concepts (page 1 of 3)

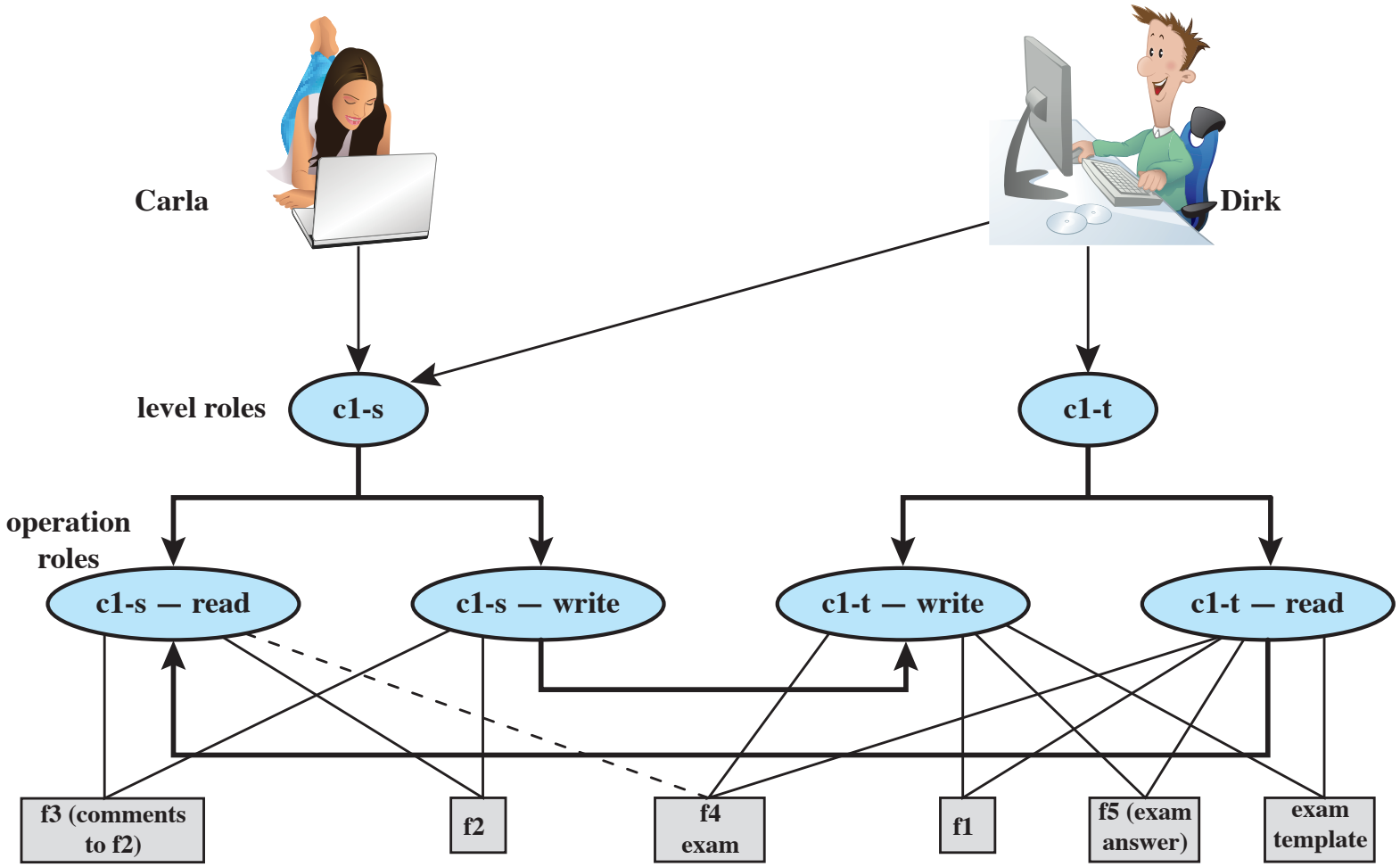


(c) An exam is created based on an existing template: f4: c1-t



(d) Carla, as student, is permitted acess to the exam: f4: c1-s

Figure 13.2 Example of Use of BLP Concepts (page 2 of 3)



(e) The answers given by Carla are only accessible for the teacher: f5: c1-t

Figure 13.2 Example of Use of BLP Concepts (page 3 of 3)

Limitations to the BLP Model

- Incompatibility of confidentiality and integrity within a single MLS system
  - MLS can work either for *powers* or for *secrets* but not readily for both
  - This mutual exclusion excludes some interesting power and integrity centered technologies from being used effectively in BLP style MLS environments
- *Cooperating conspirator* problem in the presence of covert channels
  - In the presence of shared resources the *-property may become unenforceable
  - In essence, the BLP model effectively breaks down when (untrusted) low classified executable data are allowed to be executed by a high clearance (trusted) subject

Biba Integrity Model

- Various models dealing with integrity
- Strict integrity policy:
  - Simple integrity: $I(S) \geq I(O)$
  - Integrity confinement: $I(S) \leq I(O)$
  - Invocation property: $I(S_1) \geq I(S_2)$

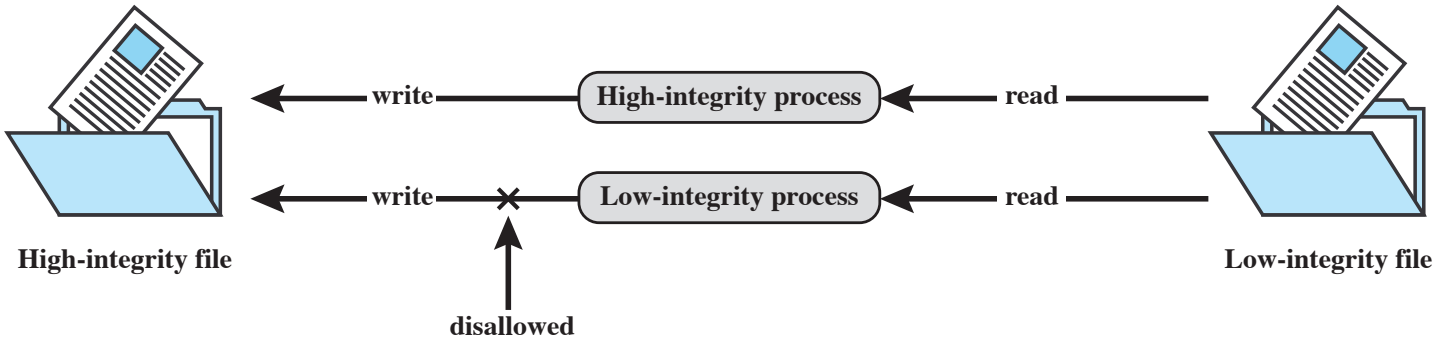


Figure 13.4 Contamination With Simple Integrity Controls [GASS88]

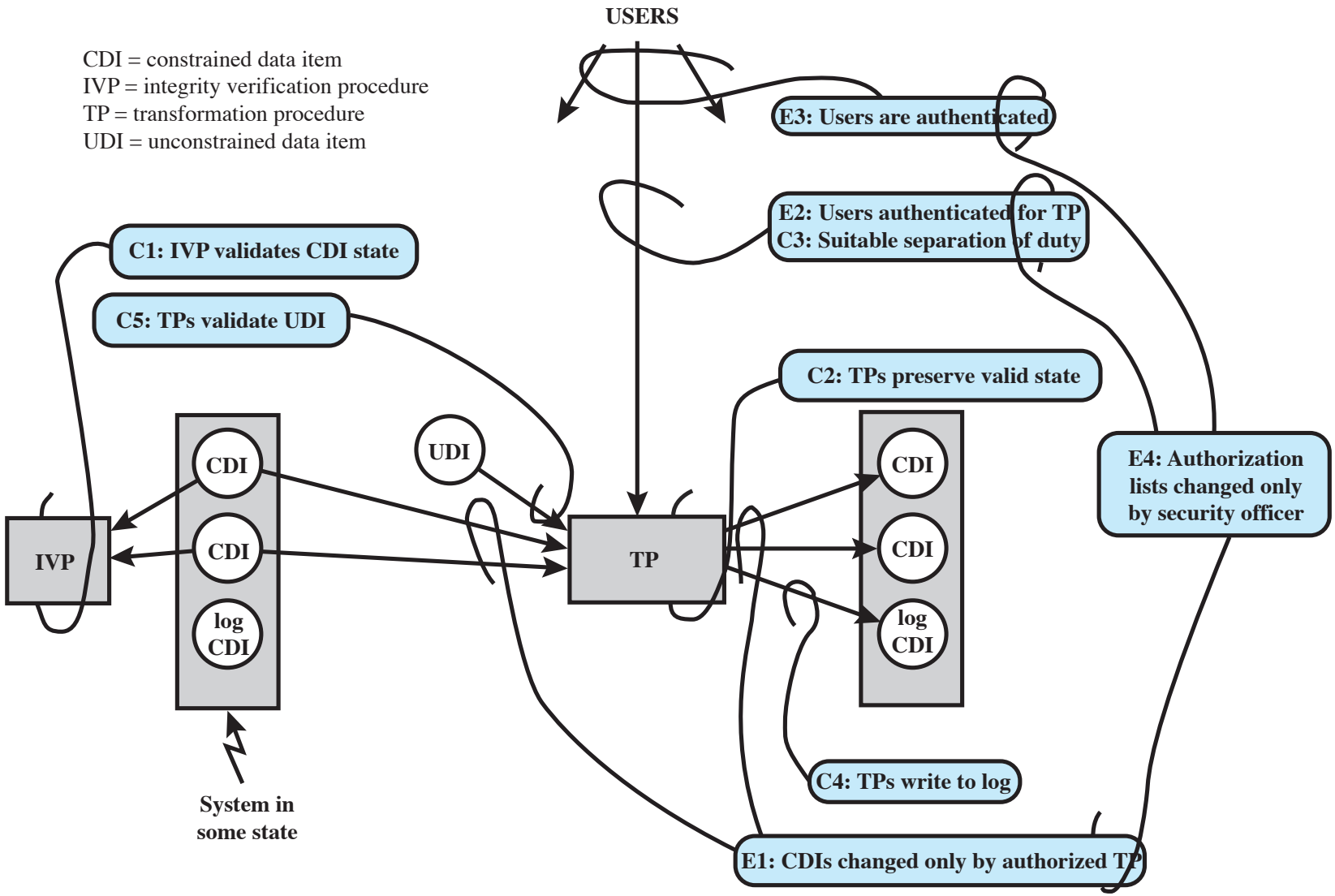


Figure 13.5 Summary of Clark-Wilson System Integrity Rules [CLAR87]

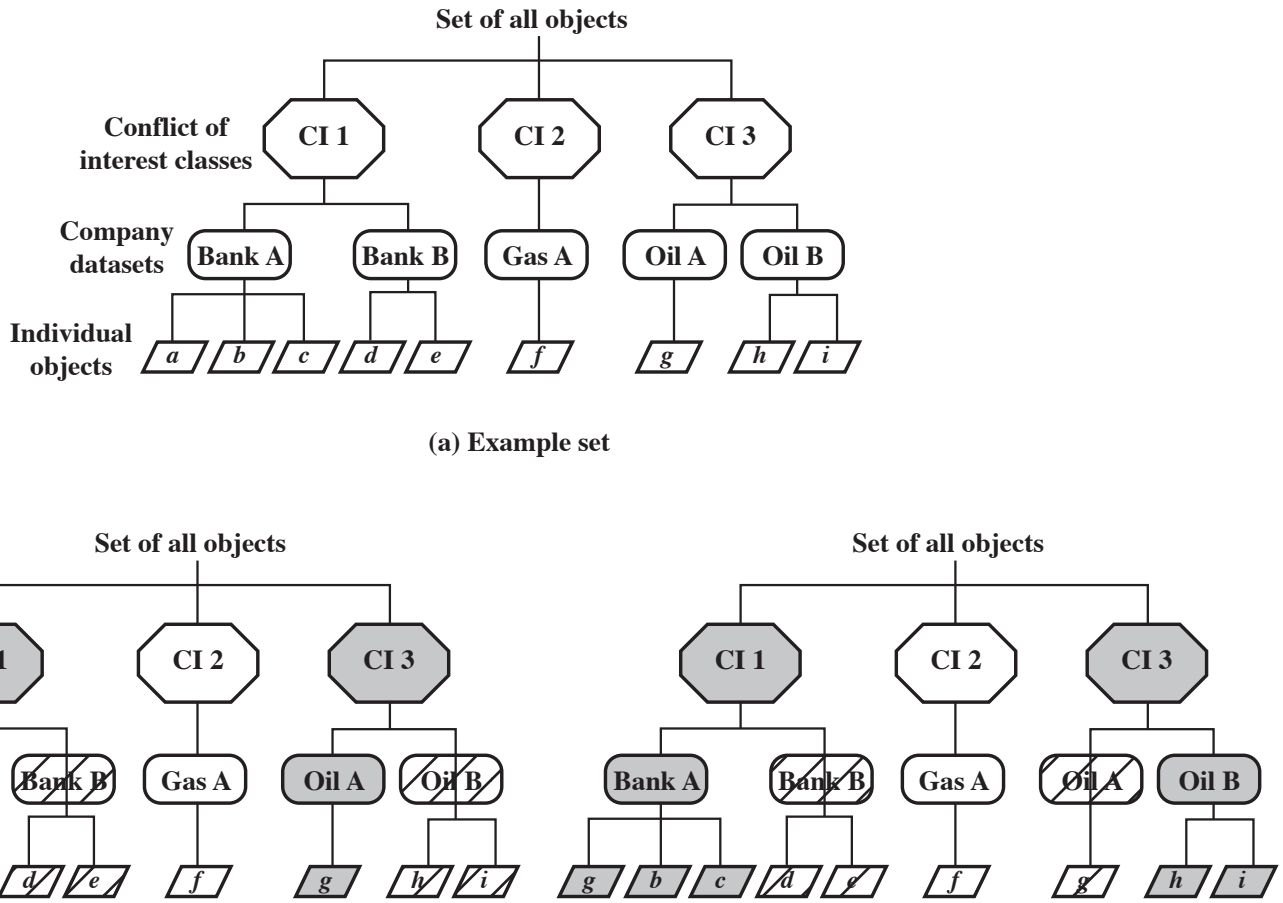


Figure 13.6 Potential Flow of Information Between Two CIs

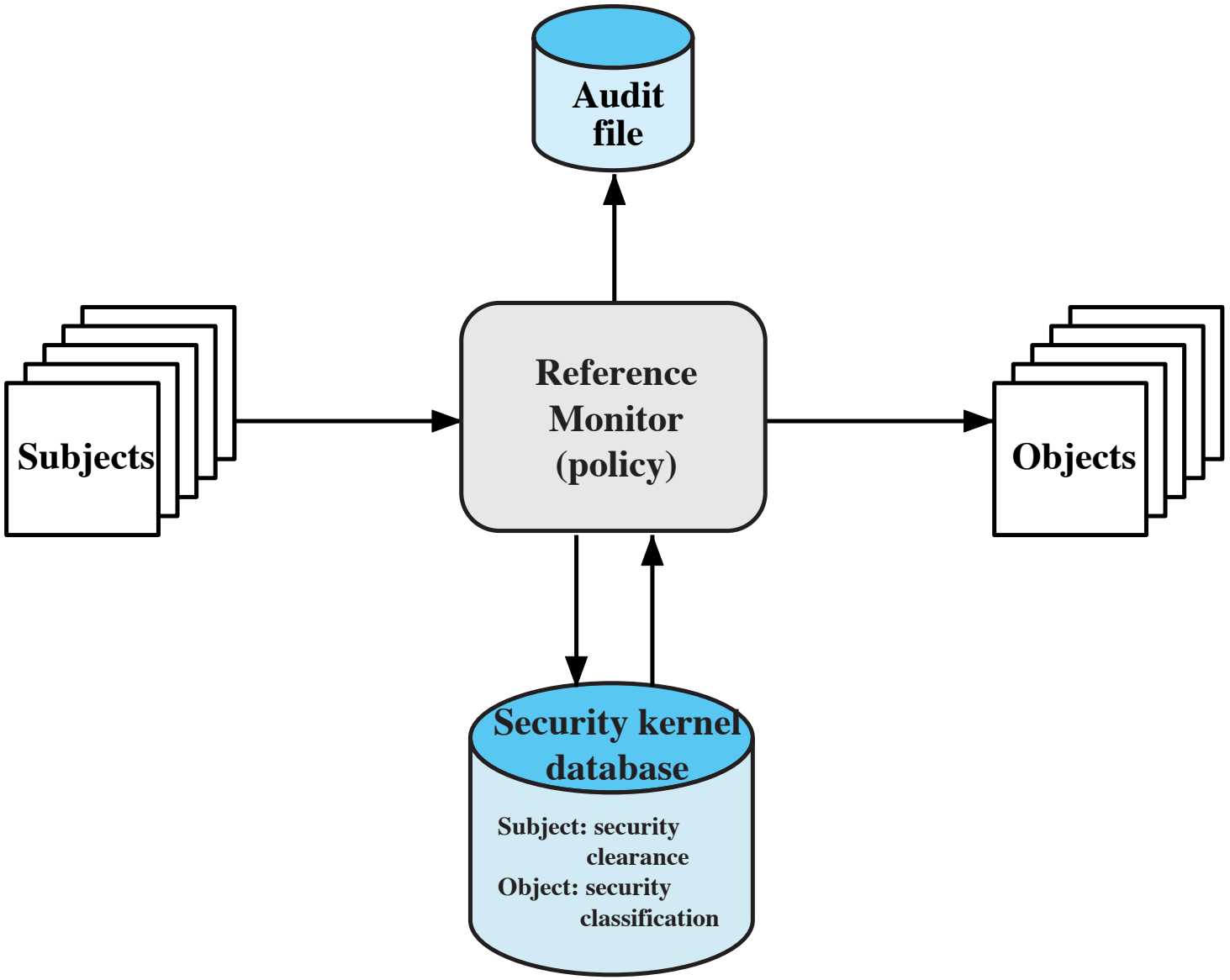


Figure 13.7 Reference Monitor Concept

Properties of the Reference Monitor

- Complete mediation: The security rules are enforced on every access, not just, for example, when a file is opened.
- Isolation: The reference monitor and database are protected from unauthorized modification.
- Verifiability: The reference monitor's correctness must be provable. That is, it must be possible to demonstrate mathematically that the reference monitor enforces the security rules and provides complete mediation and Isolation.

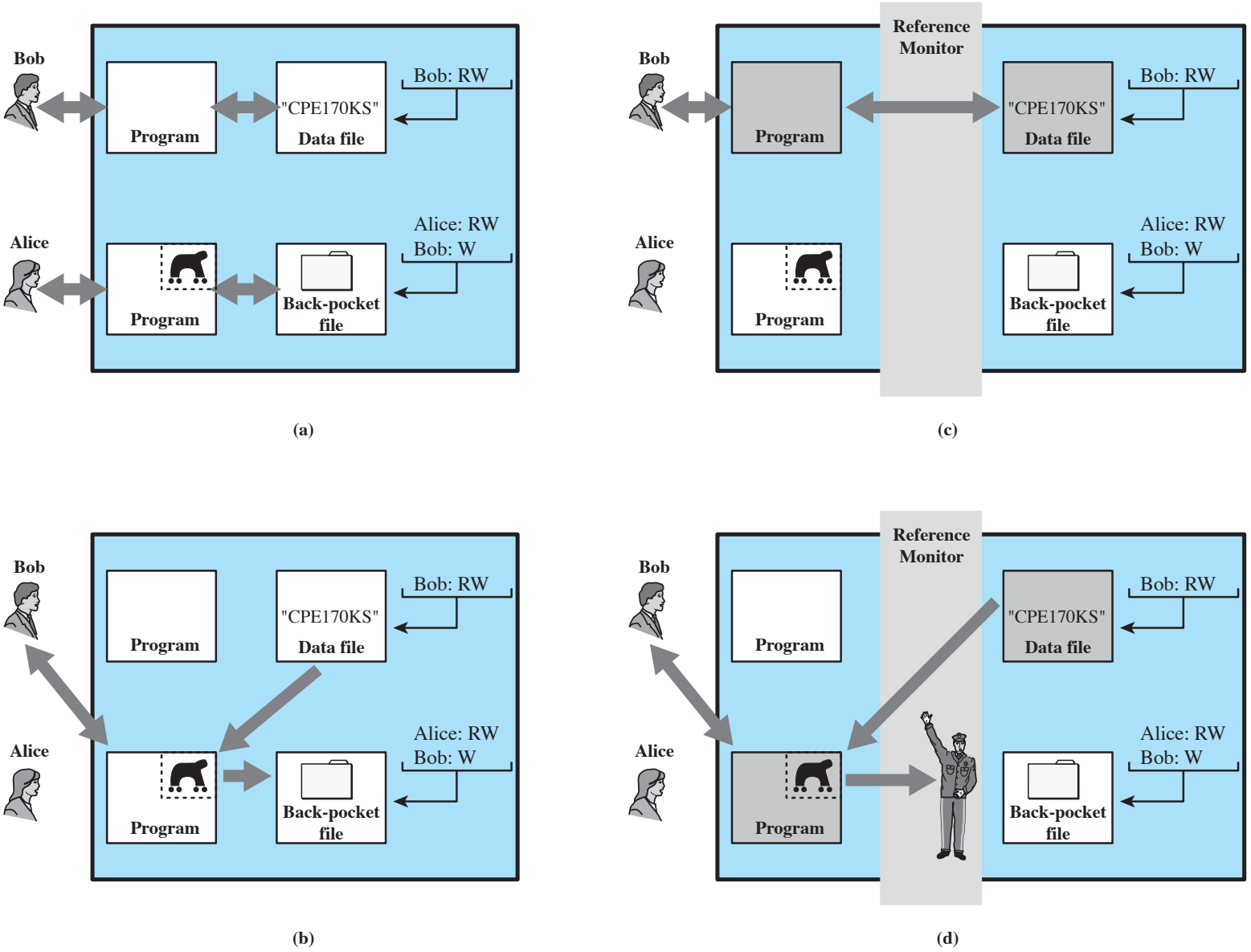


Figure 13.8 Trojan Horse and Secure Operating System

Summary

- The Bell-LaPadula model for computer security
  - Computer security models
  - General description
  - Formal description of model
  - Abstract operations
  - Example of BLP use
  - Implementation example-multics
  - Limitations to the BLP model
- Other formal models for computer security
  - Biba integrity model
  - Clark-Wilson integrity model
  - Chinese wall model

- The concept of trusted systems
  - Reference monitors
  - Trojan horse defense