Overview of TCSEC Trusted System Divisions [A]

The *Trusted Computer System Evaluation Criteria* (TCSEC) divides trusted systems into four divisions called A, B, C, and D, with A being the most trusted and D the least trusted. These divisions are hierarchical (as shown in Figure 14); that is, protection provided in division C must be incorporated into a division B system's additional security mechanisms, and so on. The following sections describe the TCSEC security policy and accountability requirements for each division.

A.1 Division D criteria

Division D systems provide minimal protection. This division is reserved for systems that have been evaluated, but failed the requirements for a higher division rating.

A.2 Division C criteria

Division C systems provide discretionary protection and are divided into two classes: C1 and C2. C1 systems provide discretionary security protection by using the following security mechanisms:

- Security policy
  - Discretionary access controls (for example, `owner/group/world` permissions)
- Accountability
  - User identification (for example, a login procedure) and user authentication (for example, passwords)

C2 systems provide controlled access protection by adding the following security mechanisms (shown in boldface type) to the C1 mechanisms:

- Security policy
  - Discretionary access controls (for example, owner/group/world permissions)

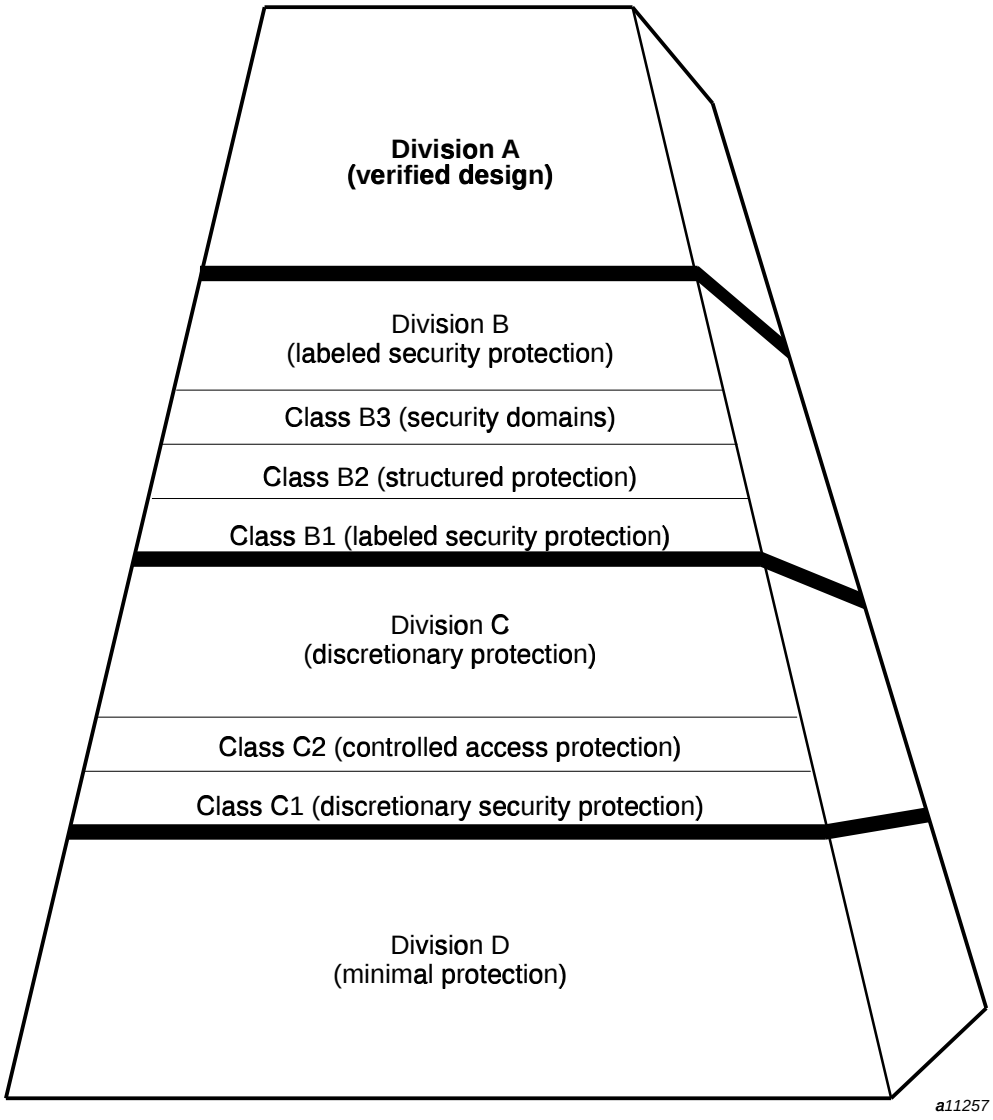

Figure 14. Divisions

- Accountability
  - User identification (for example, a login procedure) and user authentication (for example, passwords)

  - **Individual accountability**
  - **Audit trail (all subject access to an object is logged in the security log)**

A.3 Division B criteria

Division B systems provide mandatory access controls and are divided into three classes: B1, B2, and B3.

B1 systems provide labeled security protection by adding the following security mechanisms (shown in boldface type) to the division C mechanisms:

- Security policy
  - Discretionary access controls (for example, owner/group/world permissions)
  - Finer discretionary access controls (for example, to the granularity of a single user)
  - Object reuse capability (objects are scrubbed before accessed)
  - **Security labels for each subject and object**
  - **Mandatory access controls, which are enforced for every subject's access to an object**
- Accountability
  - User identification (for example, a login procedure) and user authentication (for example, passwords)
  - Individual accountability
  - Audit trail (all subject access to an object is logged in the security log)

B2 systems provide structured protection by adding the following security mechanisms (shown in boldface type) to division C and B1 mechanisms:

- Security policy
  - Discretionary access controls (for example, owner/group/world permissions)
  - Finer discretionary access controls (for example, to the granularity of a single user)
  - Object reuse capability (objects are scrubbed before accessed)

  - Security labels for each subject and object **and use of labels extended to include devices (for example, terminals, consoles, printers, and disks)**
  - Mandatory access controls, which are enforced for **all resources**
- Accountability
  - User identification (for example, a login procedure) and user authentication (for example, passwords)
  - Individual accountability
  - Audit trail (all subject access to an object is logged in the security log)
- Assurance
  - **Trusted facility management provided to divide system administrator functions between system operators and system administrators**

B3 systems provide security domains by adding the following security mechanisms (shown in boldface type) to division C, B1, and B2 mechanisms:

- Security policy
  - Discretionary access controls (for example, owner/group/world permissions)
  - Finer discretionary access controls (for example, to the granularity of a single user)
  - Object reuse capability (objects are scrubbed before accessed)
  - Security labels for each subject and object
  - Mandatory access controls, which are enforced for all resources
  - Use of security labels extended to include devices (for example, terminals, consoles, printers, and disks)
- Accountability
  - User identification (for example, a login procedure) and user authentication (for example, passwords)
  - Individual accountability
  - Audit trail (all subject access to an object is logged in the security log)

- Assurance
  - Trusted facility management provided to divide system administrator functions between system operators, system administrators, **and security administrators**

A.4 Division A criteria

Division A systems provide verified protection and are functionally equivalent to a B3 system. The following is needed to acquire a division A rating:

- Formal design specifications and techniques
- Formal proof of the security policy
- Stringent configuration management techniques