A Comparison of Commercial and Military Computer Security Policies

David D. Clark & David R. Wilson

Contribution

- Distinct set of security polices related to integrity which are different from disclosure.

- Separate mechanisms are required for enforcement of these policies.

History

- In the early 1980s the Department of Defence is concerned about the confidentiality of classified information on computers with multiple users.

- This gives rise to the rainbow series – a set of security standards developed by the DoD. The “Orange Book” was the first in the series.

Trusted Computer System Evaluation Criteria aka “Orange Book”

- Published by the National Computer Security Center (NCSC) in 1983, revised & released in 1985.
- Documented mechanisms that should be found in a computer system that enforces privacy of data.
- It was superseded by the common criteria.

BLP Lattice Model

- This is a Mandatory Control Access model

- Developed in 1973 to formalize the US DoD multilevel security policy.

- Focuses on the confidentiality of classified information

Orange Book Ratings

Ratings	Sub Category	Description
D		System which couldn’t attain a higher classification.
C	**C1** - Discretionary Security Protection **C2** - Controlled Access Protection	Provides for discretionary protection.
B	**B1** - Labeled Security Protection **B2** - Structured Protection **B3** - Security Domains	Specifies that protection systems should be mandatory, not discretionary.
A	**A1** – Verified Protection	Highest security division. Extensive documentation is required to demonstrate that the computer system meets the security requirements.

Notion of Integrity within a Commercial Environment

- Well formed transaction:

  A user should not manipulate data arbitrarily, but in a constrained way that preserves/ensures integrity of data

- Separation of duty.

Notion of integrity in the context of computer systems

- Well formed transactions - data items can only be manipulated by a specific set of programs.
- Separation of Duty - each user permitted to use only certain sets of programs.

Military vs. Commercial Mechanisms

Military	Commercial
Data item associated with a particular level	Data item associated by a set of programs permitted to manipulate it
Users constrained by what they can read and write	Users constrained by which programs they are allowed to execute

Commercial Evaluation Criteria

- System must separately authenticate and identify every user, so that their action can be controlled and audited.

- System must ensure that specified data items can be manipulated only by a restricted set of programs.

Commercial Evaluation Criteria

- System must associate with each user a valid set of programs to be run.
- System must maintain an auditing log that records every program executed and the name of the authorizing user.