

S -> Subject O -> Objects
 L(S) -> Security clearance of S
 L(O) -> Security classification of O

Simple security condition (Read)

S can read O if and only if $L(O) \leq L(S)$ and S has DAC read access to O.

*-Property (Write)

S can write O if and only if $L(S) \leq L(O)$ and S has DAC write access to O.

Informally: Read down, write up

Compartments

Feeds from principle of least privilege
 Further sub-divide access

Levels: Top Secret, Classified, ...
 Compartment: US, Europe, Asia

Dominance

Security level (L,C) dominates the security level (L',C') if and only if $L' \leq L$ and C' is a subset of C.

In other words, to dominate an object, one must have better security classification

Examples:

Compartments/categories NUC, US, EUR
 Access TS, S, C, UC

User striegel (L,C) = (TS, {NUC, US})

Can striegel access (TS, {US})?
 $TS \geq TS$ Yes
 NUC, US superset of US Yes OK

Can striegel access (C, {EUR, NUC})?
 $TS \geq C$ Yes
 NUC, US superset of EUR, NUC No Cannot access

View it as a lattice structure
 NUC, EUR, US

NUC, EUR	NUC, US	EUR, US
NUC	EUR	US

{ }

Confidentiality with Compartments

Simple Security

S can read O if and only if S dominates O and S has DAC read access to O.

*-Property

S can write to O if and only if O dominates S and S has DAC write to O.

Theorems to Prove Security

Let X be a system with a secure initial state of State0

Let T be a set of state transformations

If every element of T preserves the simple security condition and the *-property, then every StateI, $I > 0$ is secure.

MAC -> Confidentiality	Subject labeling of classification
	Object labeling of classification
DAC -> User-level	Can only restrict further beyond MAC
	Cannot bypass MAC

Who enforces security?

TCB or Trusted Computing Base
Complete Mediation

All system calls to read/write files are processed by the OS and passed through the MAC and DAC control mechanisms

Tranquility

Strong tranquility	Cannot change security levels
Weak tranquility	Can change within rules of system

Discussion: Is this model sufficient for all cases?