Information Flow

Should you press "send error report" ?

Some Concepts

Who may access data?

How may data be used?

user control

- Discretionary Access Control

management control

- Mandatory Access Control

- Decentralised Label Model (Myers)

- Information Flow (Denning, Volpano)

concrete access operations

abstract security operations

Discretionary Access Control

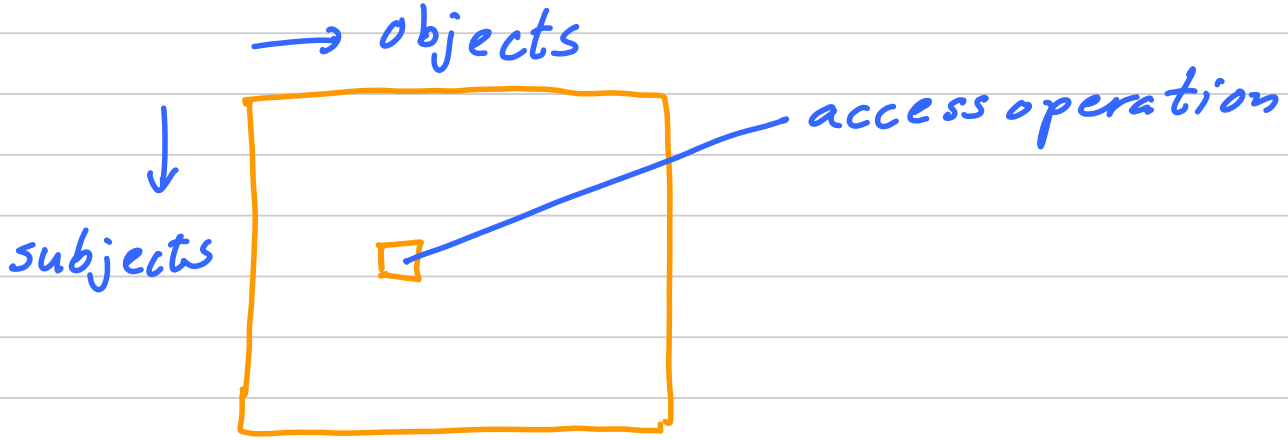
Subjects or principals denote users, programs

Objects denote files, data, ressources

Access denotes operations like read, write,
execute, append, ..., change owner, ...

E.g. UNIX: file: rwxrwxrwx
owner group other

Access Control Matrix



Access Control list: a column

at each object: for (group of) subjects the list of accesses

Capability List : a row

at each subject: for (group of) objects the list of accesses

Mandatory Access Control

Discretionary Access Control is flexible but it is hard to get the matrix right. So we add:

Add security classification
- for each subject
- for each object

Impose security policy for each access

Bell LaPadula: "No read up No write down"

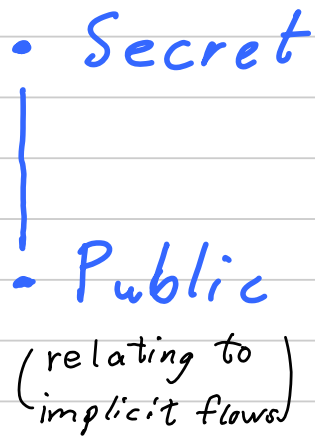
if read then

level (subject) ≥ level (object)

if write then

level (object) ≥ level (subject)

plus some more "technical" conditions (relating to implicit flows)



this should ensure that secret data never ends up in public files

Information Flow

Information Flow applies the security classification of mandatory access control at a lower level of granularity so that a subject can operate on variables at many levels.

The focus is on

- explicit flows: where can sensitive data move?
- implicit flows: under what conditions can data move?

Why do we need to use program analysis techniques like flow analysis and type systems?

Because the obvious alternative of using an execution monitor (a generalised reference monitor) is too weak!

Example:

l := 1; if h = 0 then l := 0 else skip fi

if you block here you leak that h = 0

if you block here you would also need to block

if h = 0 then skip else skip

and this is too restrictive

If you do not block you leak whether or not h = 0