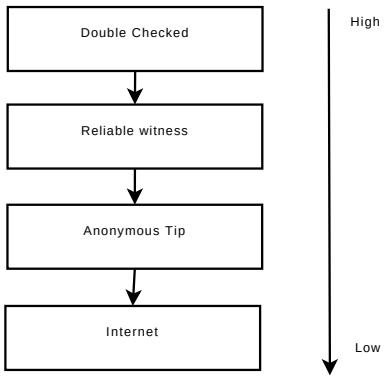
1 Biba Integrity Model

Unlike Bell-LaPadula, which the secrecy level goes from low to high, Biba Integrity Model has the integrity level that goes from high to low.



Example: Christianity vs. Islam. Compartments mean "is believed by

In Biba Integrity Model, for (l_o, C_o) and (l_s, C_s) where o stands for object and s for subject:

$$\text{read:} l_o \geq l_s; C_o \supseteq C_s$$
$$\text{write:} l_o \leq l_s; C_o \subseteq C_s$$

2 Role-Based Access Control (RBAC)

- Enterprise may have thousands of employees
- Dozens or hundreds of roles may exist in an institution
  - Auditor
  - Teller
  - Branch manager
  - CEO
  - CSR
  - "AND" Qualified Roles (e.g. Branch Manager of Branch X)
  - In this example, $teller \subset branchmanager \subset CEO$ in what they can do
- Represent ACM(access control matrix) in terms of roles

There are two different types of separation of duties:

1. Static Separation of duties: auditor conflicts CEO.
2. Dynamic Separation of duties: must switch between roles

3 Chinese Wall Model

- Objects in the system were partitioned into domains $d_1, ..., d_n$
- Initially user can access any domain
- As soon as user access some domain d_i, he loses access to all conflicting domains

Example: Untrusted code
As soon as applet reads hard drive, it permanently loses network write access.

Although the mechanism of this model is simple, it's hard to implement because the difficulty of absolutely insulating each domain. For example, the following may be used to bypass the insulation or used as a side channel:

- IPC
- Shared memory
- Input
- Fans

Also, some covert channels may contains information such as CPU usage, memory, CPU temperature.

4 Implementation/Organization of access control information

Commonly OS FS: metadata on file (e.g. linux has privilege for owner, group and other. R/W/X for each)

4.1 ACLs

- stored with the object
- indicate who can access and how
- Positive vs Negative rules
  - Positive: simple to understand
  - Negative: may enable succinct policy description

In Unix:
fd = open(filename, 'r')

What kernel does is checking:

1. uid,gid
2. Supplemental gids

An old bug happened in lpr - setuid
s: setuid privilege
rwsrwxr-x root root lpr

lpr now has root privilege!