Confidentiality Policy: The Bell-La Padula Model

by

Amit Konar

Dept. of Math and CS, UMSL

What is a confidentiality policy?

A **confidentiality policy**, also called an **information flow policy** prevents the unauthorized disclosure of information.

Example: The navy must keep confidential the date on which a troop ship will sail. If the enemy knows the date of sailing, the ship could be sunk.

Recapitulation: Military/Governmental Security Policy

A **security policy** is a statement that partitions the states of the system into a set of authorized or secure states and a set of unauthorized or non-secure states.

A **military/governmental security policy** is a security policy developed primarily to provide confidentiality.

The Bell-La Padula Model

The **Bell-La Padula model** corresponds to military style classification model **to segregate the secure and non-secure states**.

It combines **mandatory** (system based compulsory) and **discretionary** (user-set) access controls. **S has discretionary read/write access to O means were the mandatory control not existent, S would be able to read/write O.**

Characteristics of the Model

1. The model provides a set of security clearance levels of subject set S and security classification for Object set O.
2. Let L(s) =l_s be the security clearance level of subject s and L(O) = l_o be the security classification for object o, then

   s can read o if and only if l_o <= l_s and s has discretionary read access to o. (simple security condition)

Characteristics (Contd.)

3. S can write o if and only if $l_s <= l_o$, and s has discretionary write access to o. (*-property)
4. Let $\sum$ be a system with a secure initial state Q_o, and T be a set of transformations. If every element of T preserves the simple security condition and the *-property, then every state Q_i is secure.

Example: Illustrating characteristics

Top Secret (TS)	Tamara,Thomas	Personnel Files
Secret(S)	Sally, samuel	E-mail files
Confidential (C)	Claire, Clarence	Activity Log files
Unclassified(UC)	Ulaley,Ursula	Telephone list files

Claire/Clarence cannot read personnel files;
Tamara/Thomas cannot write on E-mail files.