

INFO 622

LECTURE NOTES: 1/15/08

- Review Chap. 1 of **Cryptography and Network Security**

- From **Security in Computing** (Pfleeger and Pfleeger, 4th edition), pgs.243 - 257
 - Difference between “secure” and “trusted”
 - Military security policy is based on “need-to-know”; each piece of info has a *classification (security level)* and a *compartment (category)*
 - The *class (security label)* of a piece of info is the combination of $\langle rank; compartments \rangle$
 - The relation \leq (**dominance**) is defined as follows:
 - $s \leq o$ iff $rank_s \leq rank_o$ and $compartments_s \subseteq compartments_o$A subject can read an object only if the subject dominates the object.

- Military policies concentrate on confidentiality, but traditionally aren't concerned as much (if at all) with integrity; commercial security policies are often more concerned with integrity (Clark-Wilson, Chinese Wall).

- Security **models** are used to
 - test a particular policy for completeness & consistency
 - document a policy
 - help conceptualize and design an implementation
 - check whether an implementation meets its requirementsSo, a model enforces a policy decision.

- Bell-La Padula** Confidentiality model defines allowable paths of information flow in a secure system. The system covers a set of subjects S and a set of objects O . Each subject $s \in S$ and each object $o \in O$ have fixed security classes $C(s)$ and $C(o)$. The security classes are ordered by a relation \leq . (The classes may form a lattice, although the model applies to less restrictive situations.) There are two properties characterizing secure flow:

- **Simple security property:** subject s may have *read* access to object o only if $C(o) \leq C(s)$
- ***-Property:** a subject s with *read* access to object o may have *write* access to an object p only if $C(o) \leq C(p)$.

These two properties are referred to as *read-down* and *write-up*.

•**Biba** Integrity model is considered to be the *dual* of the Bell-La Padula model. In this model confidentiality (secrecy) is ignored to concentrate on integrity.

•Subjects are ordered by an integrity classification scheme, denoted by $I(s)$ and $I(o)$. It also has two properties:

- **Simple integrity property:** subject s can modify (have *write* access to object o only if $I(o) \leq I(s)$).
- **Integrity *-property:** If subject s has *read* access to object o with integrity $I(o)$, then s can have *write* access to object p only if $I(p) \leq I(o)$.