

Week 3

BLP Rules

BLP Rules

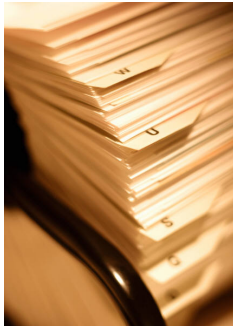
- DS-property
 - Access must be permitted by a discretionary access control matrix, M
 - $(s, o, a) \in M$
 - s : subject; o : object; a : attribute (permission)
 - If the access is defined in the access matrix, consider other rules (SS- and *-properties) for the final decision
 - Otherwise, the access is not allowed

BLP Rules

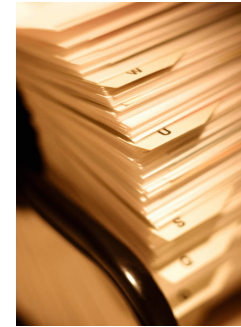
- SS-property (no read up)
 - Subject s can read object o only if $\lambda(s) \geq \lambda(o)$
 - $\lambda(s)$: security level of s
 - $\lambda(o)$: security level of o
 - Information flows from object to subject.
- *-property (no append down)
 - Subject s can append object o only if $\lambda(s) \leq \lambda(o)$
 - Information flows from subject to object

Need for the *-property

High object



Low object



Read

Append



High subject

Information flow
(security violation!)



School of Information Studies
SYRACUSE UNIVERSITY