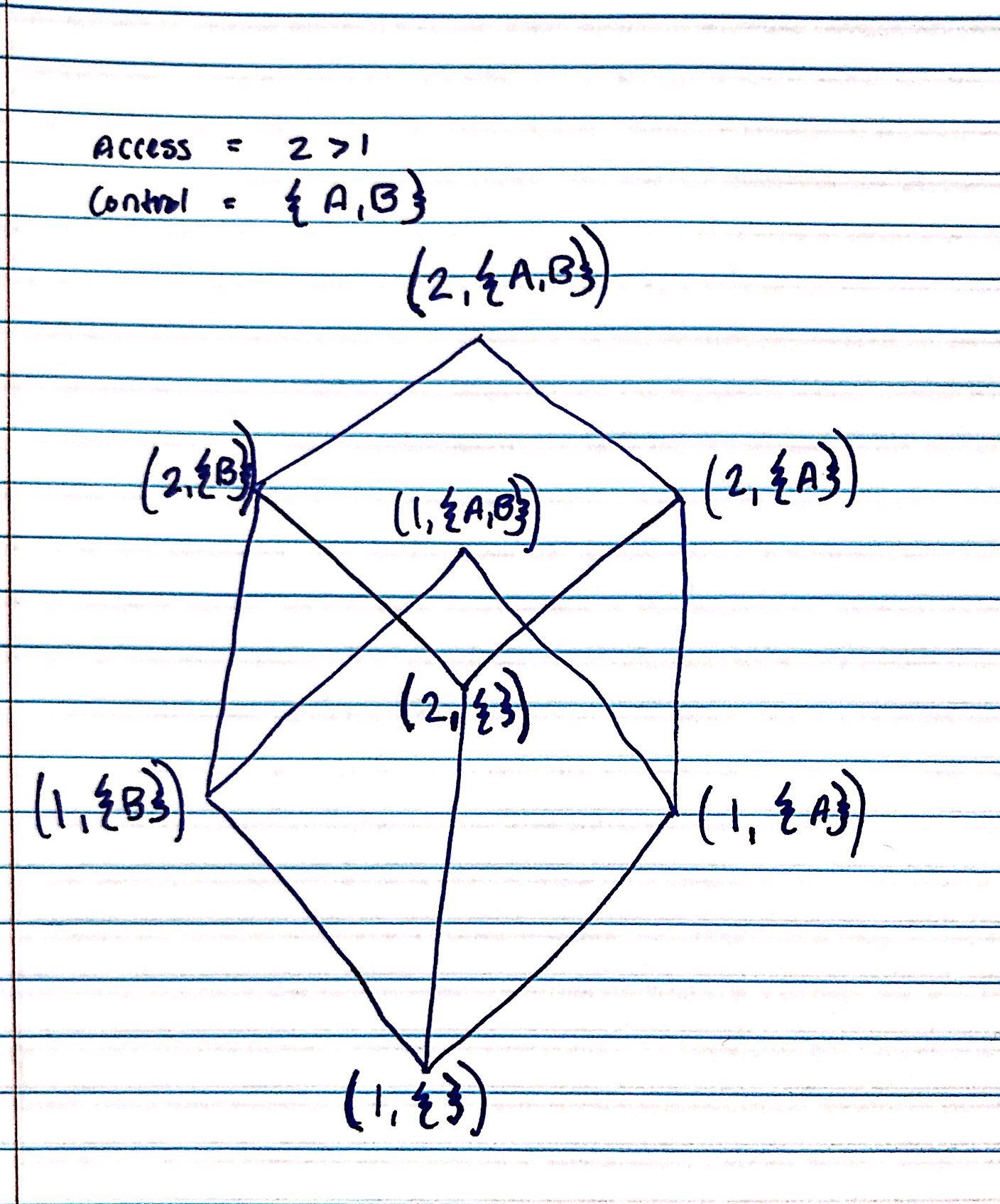
**­­­­­Homework #3**

**Bailey Metz**

**1.  Describe the two rules of the Bell-LaPadula access control model and indicate the information flow in the security lattice enforced by each rule.**1. Simple security property – a subject s is allowed to read an object o only if security label of s dominates the security label of o  
• No read up   
• Applies to all subjects   
  
A user can only read a file if he/she has a security clearance label that is higher than the security clearance label of the file.   
  
E.g., A user with ‘top secret’ level security clearance can read a file with ‘secret’ OR ‘top secret’ level security.  
  
E.g., A user with ‘secret’ level security clearance cannot read a file with ‘top secret’ level security (because his permissions do not allow him to access ‘top secret’ information).  
  
2. Star Property – a subject s is allowed to write an object o only if the security label of o dominates the security label of s.  
• No write down  
• Applies to un-trusted subjects only  
  
Using this property, data with a higher level of security clearance cannot be written down (or copied) to a level of lower security clearance.  
  
E.g., A user with ‘top secret’ level security clearance cannot copy information into a document with ‘secret’ level security clearance. This would violate the star property.

**a)  Why do we say that the BLP rules are necessary but not sufficient conditions?**

• BLP rules are necessary because they keep confidentiality and control of writing (one form of integrity) but fail to address other security principles.   
• Covert channels are stated but not comprehensively addressed.  
• The overall process may take more time than security alternatives.

**2.  Build the security lattice for hierarchical component: 2 > 1   
and domain component: {A, B}**

**3.   Consider the following *role hierarchy*, where R1,R2,R3,R4,R5 are the roles, and p1,p2,p3,p4,p5,p6,p7,p8 are the privileges assigned to the roles by which they are listed.**

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  | | **https://cse.sc.edu/~farkas/csce522/HW3-2018_files/image001.gif** |
|  | **https://cse.sc.edu/~farkas/csce522/HW3-2018_files/image002.gif** |  |
|  |  |  |

**a.  What are *all the privileges* available for R3?**R3’s privileges include P4, P7, P8 since R3 inherits the privileges of R1 as well as its own (R3).

**b.  If a user, cleared for R4, wants to *use privileges p4 and p8*only, at *what roles* (may be multiple roles) should s/he login to limit the number of unneeded privileges?  Why?**  
R3 *(which includes R1 by inheritance)*  
  
While this gives a user access to an additional inherited privilege at R1 (p7), it is the only way to for the user to have privileges p4 and p8. Since the user doesn’t want the privileges of R4, there is no need to give him/her access to R4 even though he/she has been cleared for the role of R4.