

# ISA662 Homework 2

Due March 07

February 23, 2006

1. Consider a BLP system with the following clearances (classifications) and category sets: 3 clearances/classifications: U S TS 3 category sets: ASIA, EUR, US, EUR, US, US (do not consider other unlisted category sets, like ASIA or EUR. They won't appear in the system)

1.1 List all the security levels in the system.

1.2. By Denning's axioms, those security levels form a lattice. Draw the lattice in full details (with all the security levels you have listed above; don't write something like lattice1 lattice2).

1.3. Assuming Alice is assigned the security level (U, ASIA, EUR, US), list all the security levels (of objects) that she can read and all the security levels (of objects) that she can write by BLP policy.

1.4. The two conditions of BLP can be summarized as 'read down' (a subjects  $s$  can read an object  $o$  if and only if  $s$  dominates  $o$ ) and 'write up' (a subjects  $s$  can write an object  $o$  if and only if  $o$  dominates  $s$ ). Explain why 'no read up' and 'no write down' are insufficient to describe BLP (hint: see what levels Alice cannot read).

2. Page 150, Number 2.

3. Page 150, Number 7.

4. In order to support separation of duty in RBAC, we use a constraint saying that any user can only play one of the two roles that are to be separated, such as cashier and sales assistant (page 61 of the our handouts details this approach). Describe another way to support separation of duty in RBAC (hint: instead of using the subject-to-role relationship, looks at the other half of the model).