TOPIC

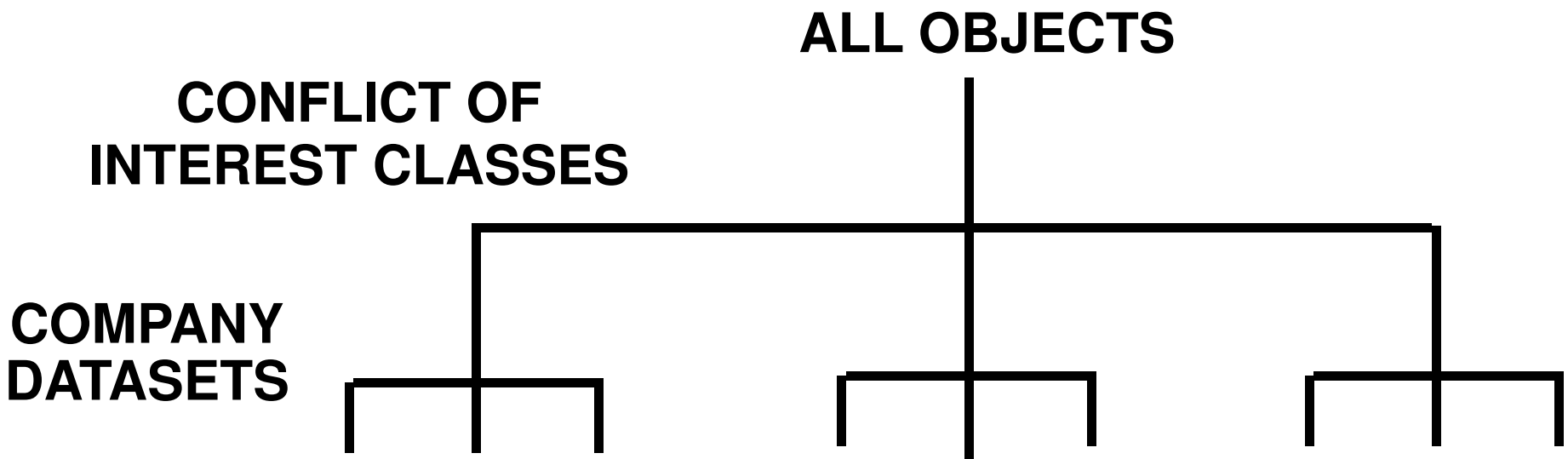
THE CHINESE WALL LATTICE

Ravi Sandhu

CHINESE WALL POLICY

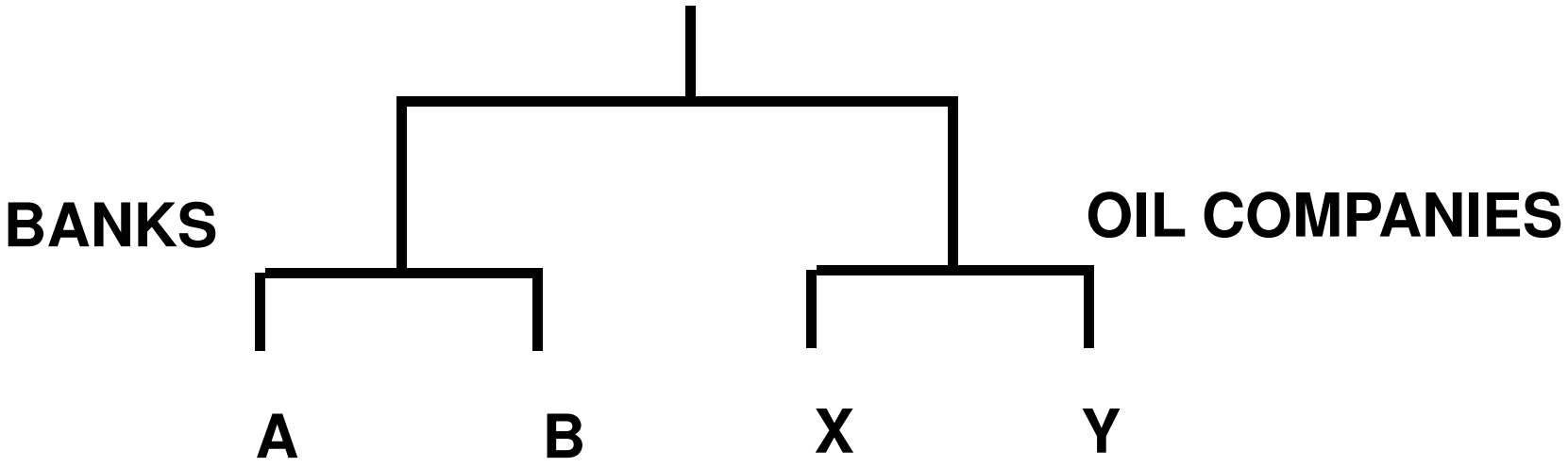
- **Example of a commercial security policy for confidentiality**
- **Mixture of free choice (discretionary) and mandatory controls**
- **Requires some kind of dynamic labelling**
- **Introduced by Brewer-Nash in Oakland '89**

CHINESE WALL POLICY



A consultant can access information about at most one company in each conflict of interest class

CHINESE WALL EXAMPLE



READ ACCESS

BREWER-NASH SIMPLE SECURITY

S can read O only if

- **O is in the same company dataset as some object previously read by S (i.e., O is within the wall)**

or

- **O belongs to a conflict of interest class within which S has not read any object (i.e., O is in the open)**

WRITE ACCESS

BREWER-NASH STAR-PROPERTY

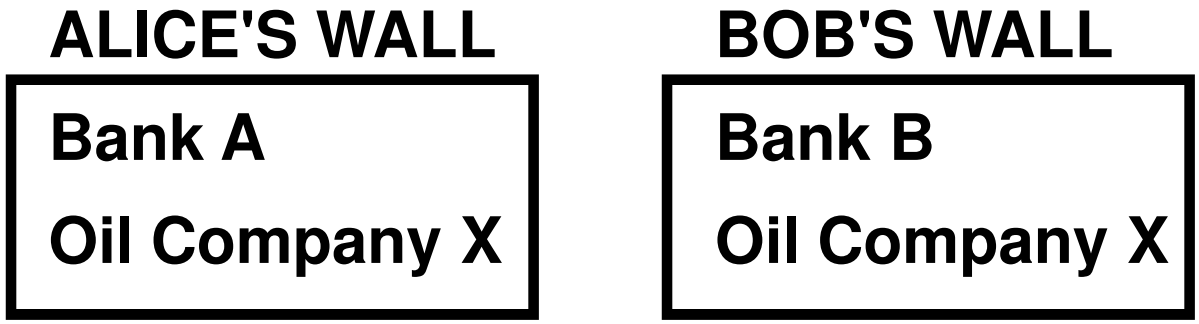
S can write O only if

- **S can read O by the simple security rule**

and

- **no object can be read which is in a different company dataset to the one for which write access is requested**

REASON FOR BN STAR-PROPERTY



- **cooperating Trojan Horses can transfer Bank A information to Bank B objects, and vice versa, using Oil Company X objects as intermediaries**

IMPLICATIONS OF BN STAR-PROPERTY

Either

- **S cannot write at all**

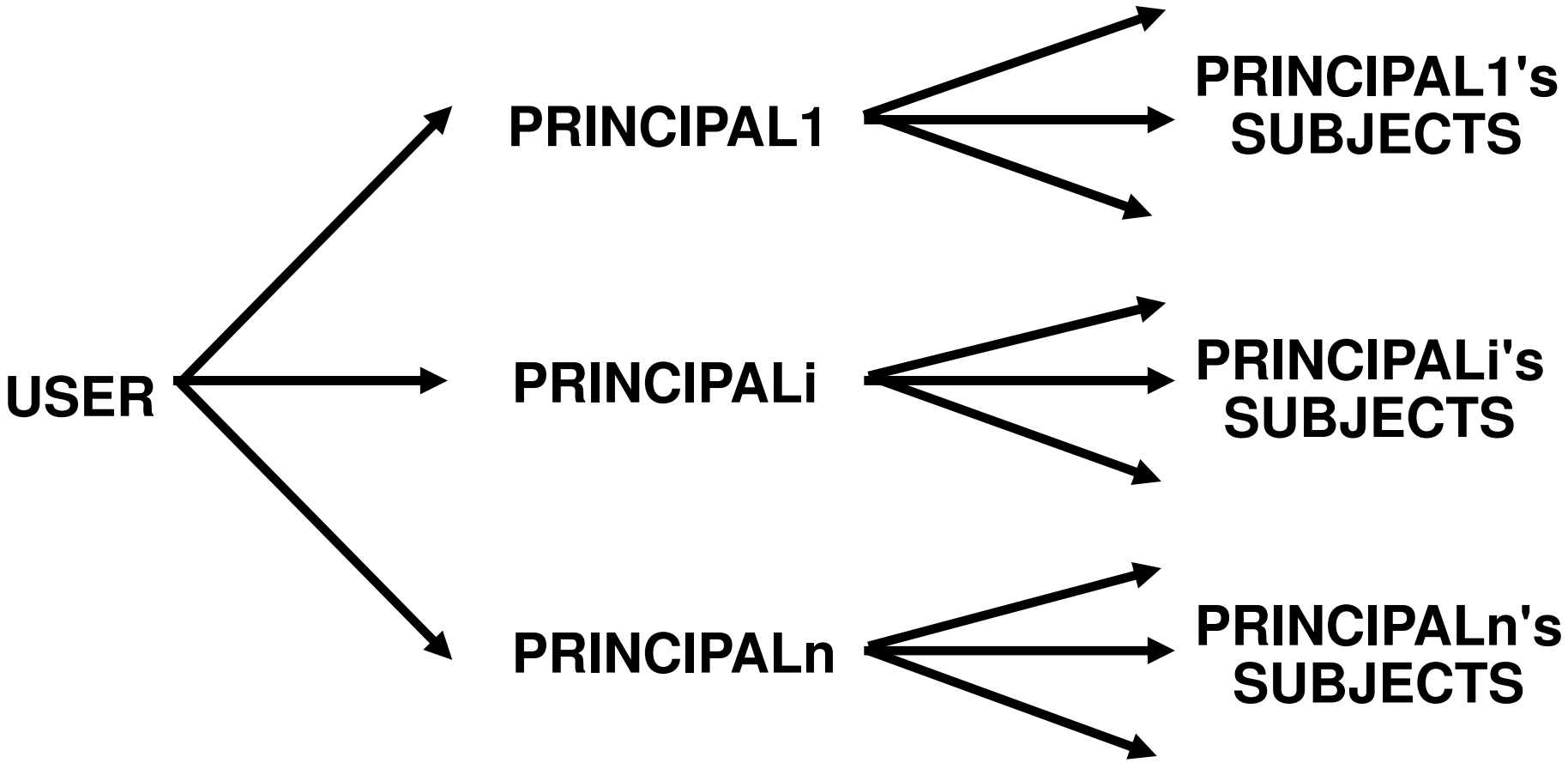
or

- **S is limited to reading and writing one company dataset**

WHY THIS IMPASSE?

Failure to clearly distinguish user labels from subject labels.

USERS, PRINCIPALS, SUBJECTS

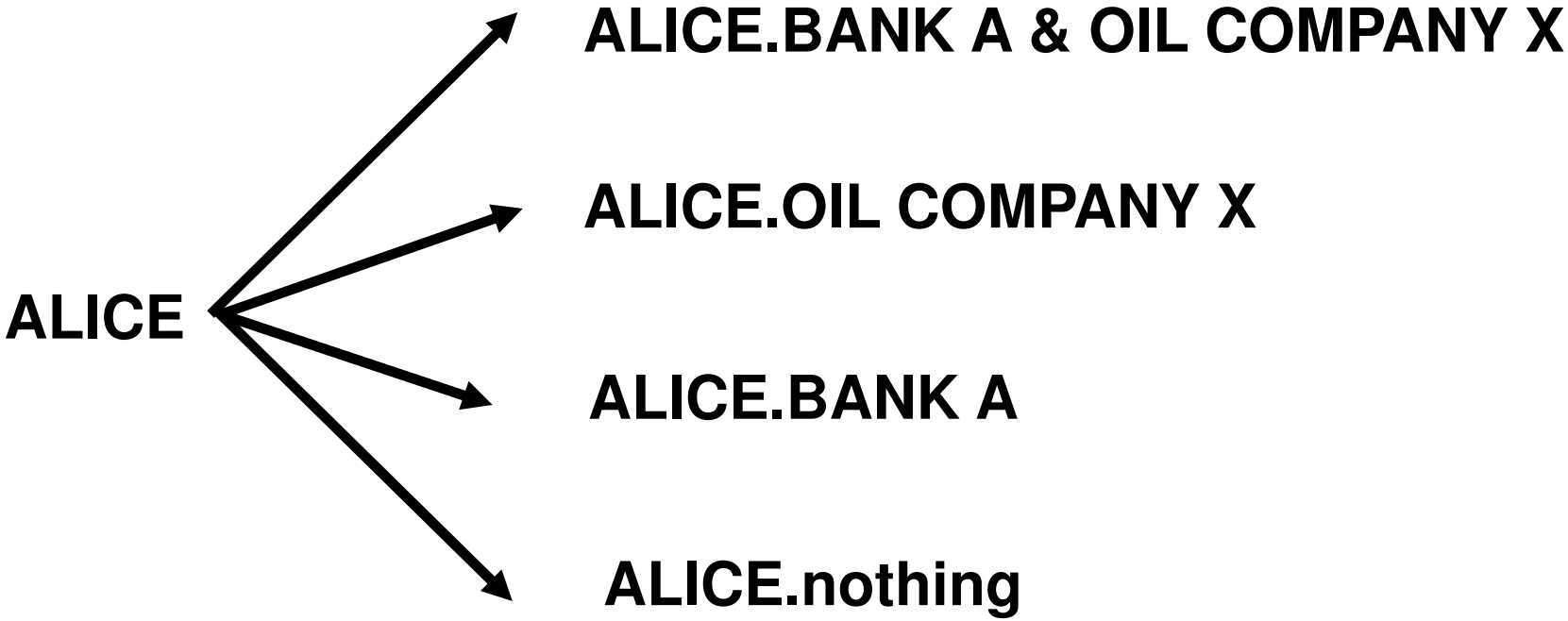


USERS, PRINCIPALS, SUBJECTS

- **Principals are subjects**
- **Users are not subjects**

  Users are collections of principals (subjects)

USERS, PRINCIPALS, SUBJECTS



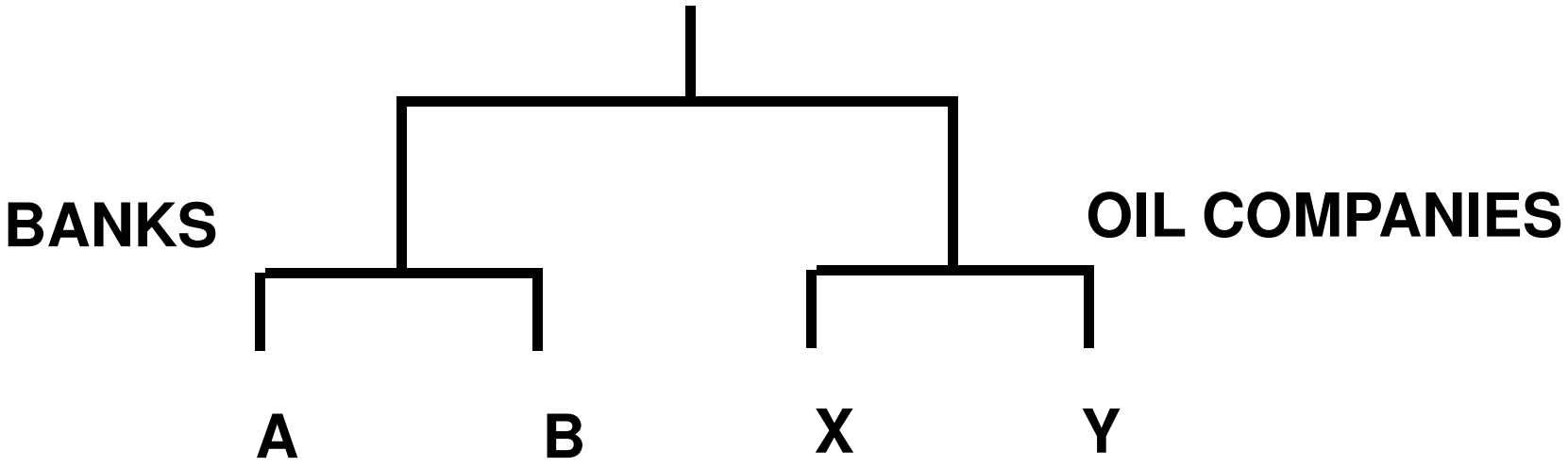
LATTICE INTERPRETATION

- **dynamic creation of principals**

  rather than

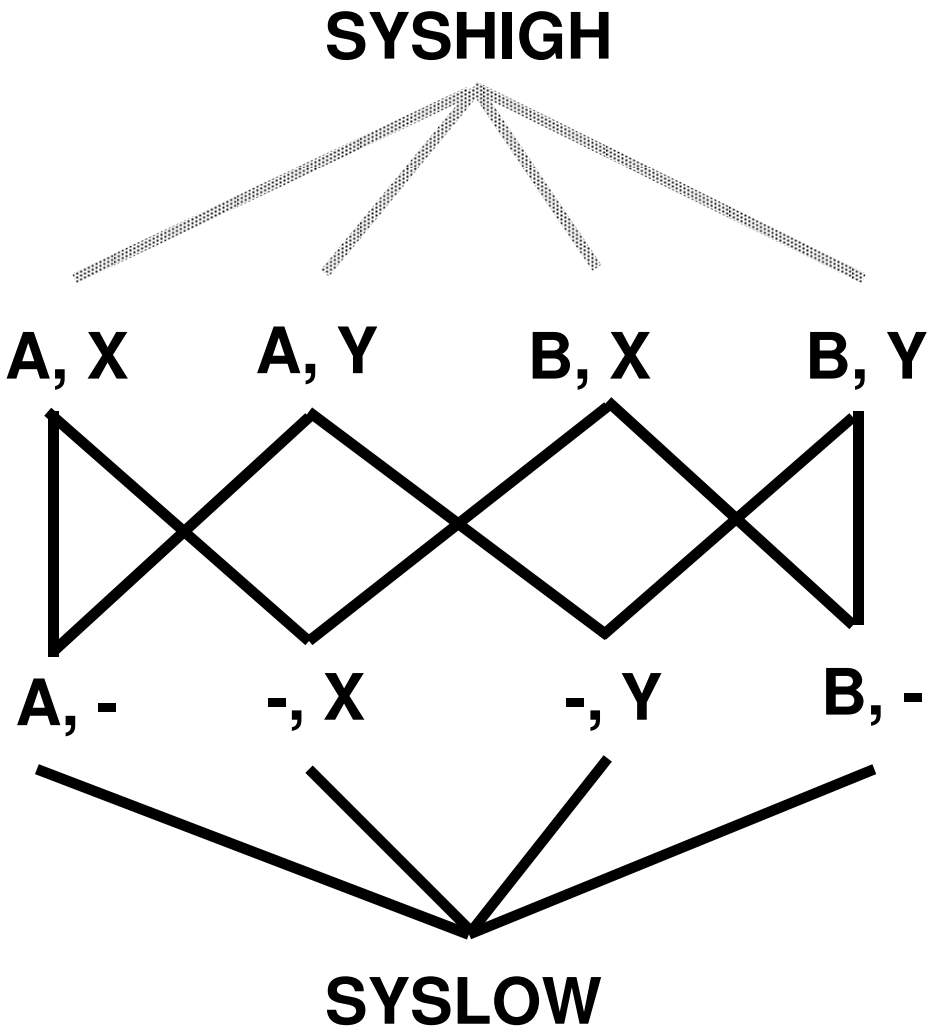
  dynamic labelling of subjects

CHINESE WALL EXAMPLE

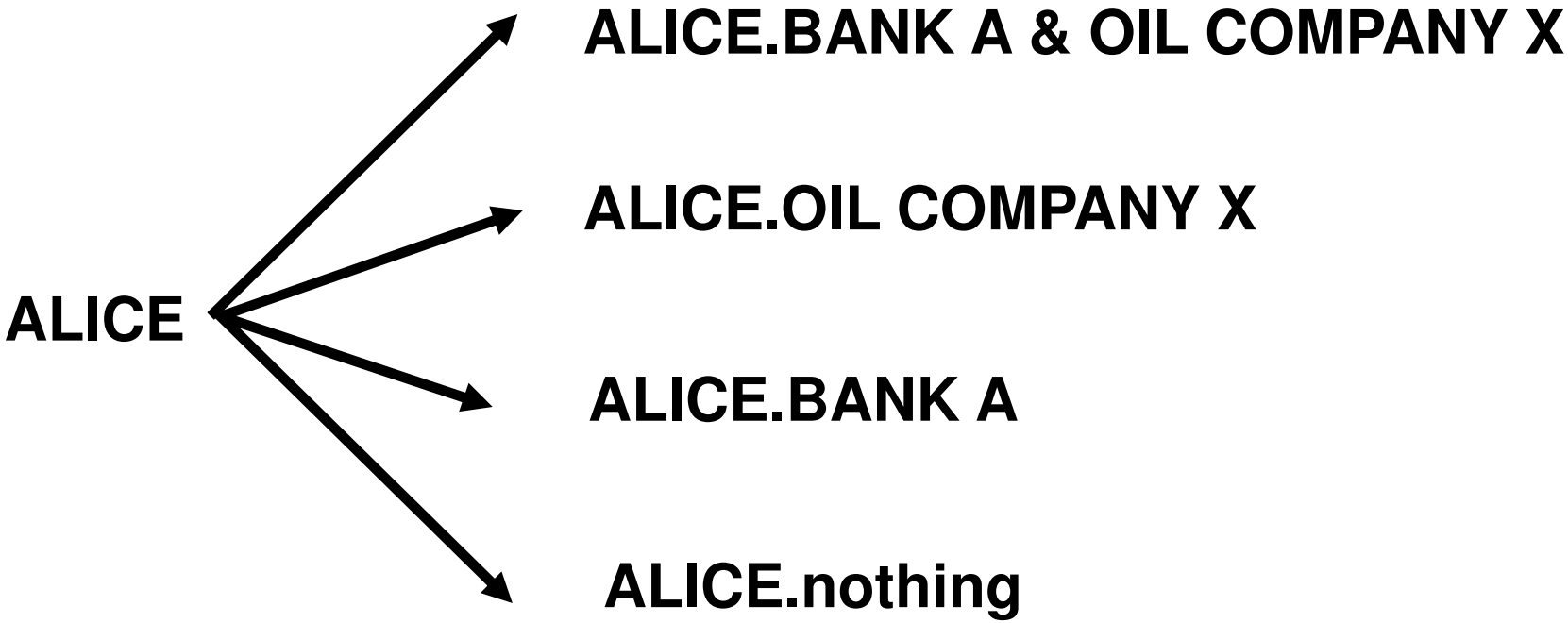


CHINESE WALL LATTICE

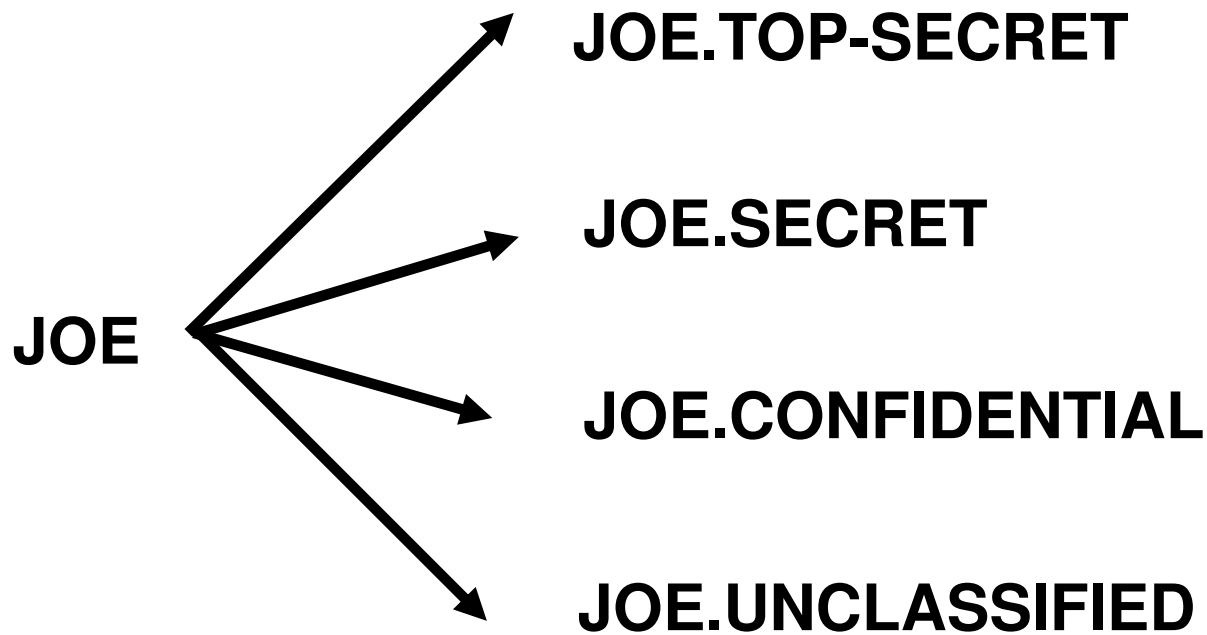
The high water mark of a user's principal can float up so long as it remain below SYSHIGH



USERS, PRINCIPALS, SUBJECTS



USERS, PRINCIPALS, SUBJECTS



USERS, PRINCIPALS, SUBJECTS

- **The Bell-LaPadula star-property is applied not to Joe but rather to Joe's principals**
- **Similarly, the Brewer-Nash star-property applies not to Alice but to Alice's principals**

CONCLUSION

- **The Chinese Wall policy is just another lattice-based information flow policy**
- **To properly understand and enforce Information Security policies we must distinguish between**
  - **policy applied to users, and**
  - **policy applied to principals and subjects**