# Database Applications of Role-Based Access Control

**Sylvia Osborn**
**The University of Western Ontario**
**Nov. 12, 2001**



# Outline of Talk

- **Brief Introduction to Access Control Models**
- **Role-Based Access Control (RBAC)**
- **Database Applications of RBAC**

## Basic Definitions

**Subject:** an entity wishing to access an object

**Object:** the entity on which operations take place or on which the subject acts

**Access Mode:** one of the legal operations that can be performed by a subject on an object



## Discretionary Access Control

- The owner of an object can give permissions to others at his/her discretion
- Typical of operating systems and relational databases
- Basic model here is the access matrix

# Example of Access Matrix

| | Objects | | | | |
|---|---|---|---|---|---|
| Subjects | $O_1$ | ... | $O_j$ | ... | $O_m$ |
| $S_1$ | $A[s_1, o_1]$ | | $A[s_1, o_j]$ | | $A[s_1, o_m]$ |
| . | | | | | |
| . | | | | | |
| $S_i$ | $A[s_i, o_1]$ | | $A[s_i, o_j]$ | | $A[s_i, o_m]$ |
| . | | | | | |
| . | | | | | |
| $S_n$ | $A[s_n, o_1]$ | | $A[s_n, o_j]$ | | $A[s_n, o_m]$ |



# Storage of Access Control Information

- **The Access Control matrix is typically sparse**
- **Stored by rows: called a *capability list***
- **Stored by columns: called an *access control list***

## Administration of access control

- As well as having a right, one can have the right to grant it to others
- In discretionary models, this is given to owners of the object
- In some versions of the access matrix model, the grant permission is shown by +



# Example from db2

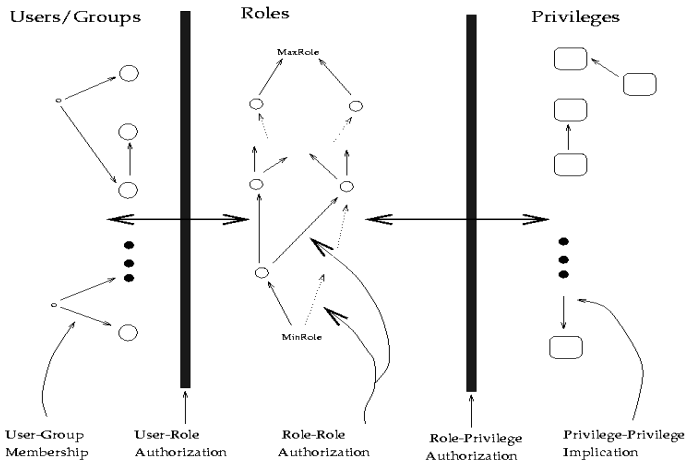
```
db2 => connect to canada

   Database Connection Information

 Database product        = DB2/6000 1.1.0
 SQL authorization ID    = LKR
 Local database alias    = CANADA

db2 => select * from sysibm.systabauth where tcreator <> 'SYSIBM'

GRANTOR  GRANTEE  TCREATOR TTNAME              TABAUTH CONTROLAUTH ALTERAUTH DELETEAUTH INDEXAUTH INSERTAUTH SELECTAUTH UPDATEAUTH REFAUTH
-------- -------- -------- ------------------ ------- ----------- --------- ---------- --------- ---------- ---------- ---------- -------
SYSIBM   LKR      LKR      PROVINCES          -----Y      Y           Y         Y          Y         Y          Y          Y          Y
SYSIBM   LKR      LKR      ANIMALS            -----Y      Y           Y         Y          Y         Y          Y          Y          Y
SYSIBM   LKR      LKR      MUSIC              -----Y      Y           Y         Y          Y         Y          Y          Y          Y
LKR      WELCH    LKR      ANIMALS            -----N      N           N         N          N         Y          N          N          N
LKR      CAM      LKR      ANIMALS            -----N      N           N         N          N         Y          N          N          N
LKR      DSTOKES  LKR      ANIMALS            -----N      N           N         N          N         Y          N          N          N
LKR      TOBAN    LKR      ANIMALS            -----N      N           N         N          N         Y          N          N          N
LKR      WARREN   LKR      PROVINCES          -----N      N           N         N          N         Y          N          N          N
LKR      PETE     LKR      PROVINCES          -----N      N           N         N          N         Y          N          N          N
LKR      WAYNE    LKR      PROVINCES          -----N      N           Y         N          N         N          N          N          N
LKR      YAAMAG   LKR      PROVINCES          -----N      N           Y         N          N         N          N          N          N
LKR      SYLVIA   LKR      PROVINCES          -----N      N           Y         N          N         N          N          N          N
LKR      HANAN    LKR      PROVINCES          -----N      N           Y         N          Y         Y          N          N          N
LKR      MAGI     LKR      PROVINCES          -----N      N           Y         N          Y         Y          N          N          N
LKR      JANICE   LKR      PROVINCES          -----N      N           Y         N          Y         Y          N          N          N
LKR      CURTIS   LKR      PROVINCES          -----N      N           Y         N          Y         Y          N          N          N
LKR      WELCH    LKR      PROVINCES          -----N      N           Y         N          N         Y          N          N          N
LKR      CAM      LKR      PROVINCES          -----N      N           Y         N          N         Y          N          N          N
LKR      DSTOKES  LKR      PROVINCES          -----N      N           Y         N          N         Y          N          N          N
LKR      TOBAN    LKR      PROVINCES          -----N      N           Y         N          N         Y          N          N          N
LKR      BAUER    LKR      MUSIC              -----N      N           N         N          N         Y          N          N          N
LKR      SHAUN    LKR      MUSIC              -----N      N           Y         N          N         Y          N          N          N
LKR      PERY     LKR      MUSIC              -----N      N           N         N          N         Y          Y          N          N
LKR      ROBBINS  LKR      MUSIC              -----N      N           N         Y          N         N          Y          N          N
LKR      KATCHAB  LKR      MUSIC              -----N      N           N         N          N         N          Y          N          N
LKR      BRUCE    LKR      MUSIC              -----N      N           N         Y          N         Y          Y          N          N

  26 record(s) selected.
```

# Mandatory access control

- **Subjects have labels called their *clearance***
- **Objects have labels called their *classification***
- **Labels are arranged in a lattice**
- **Access is decided by comparing the two security labels using certain rules (no read up, no write down, etc.)**



# RBAC – 3 planes

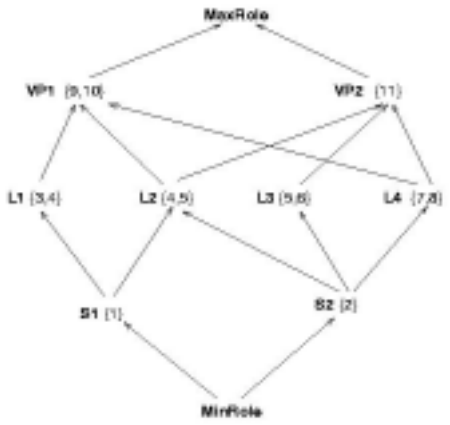


# Some definitions

- **Role: named collection of privileges**
- **Privilege: (object, operand) pair**
- **Group: set of users**
- **Direct privileges: not available to immediate juniors**
- **Effective privileges: direct and all inherited privileges**



# Example Role Graph




**For VP1,**

**Direct privileges are {9,10}**

**Effective are {1,2,3,4,5,7,8,9,10}**

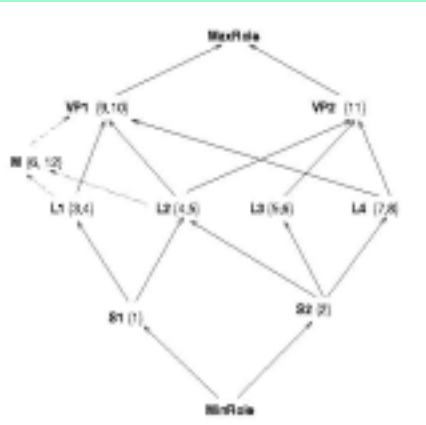
# Algorithms

**Insert a role - 2 algorithms:**

1. **Insert1(role name, direct privs, juniors, seniors)**
2. **Insert2(role name, effective privs)**



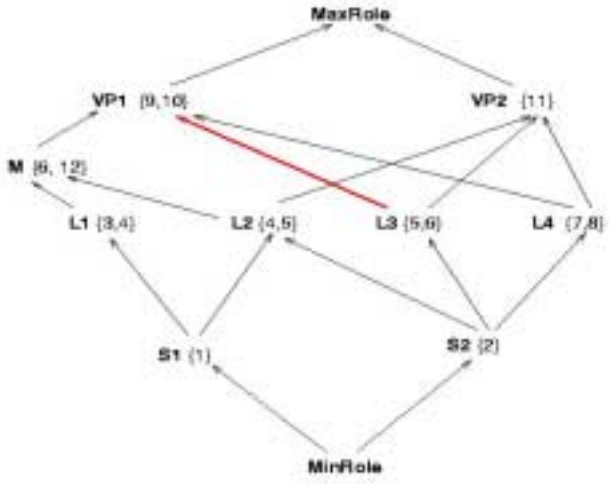
# Example of Insert1




Insert1

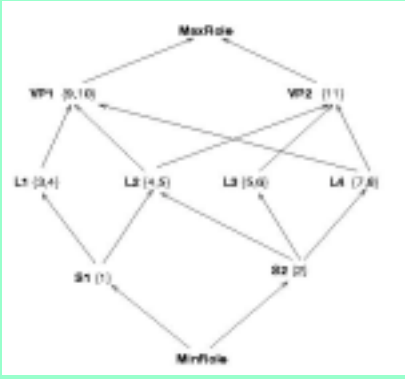
- Role name: M
- Direct: {6, 12}
- Juniors: {L1, L2}
- Seniors: {VP1}

# Result





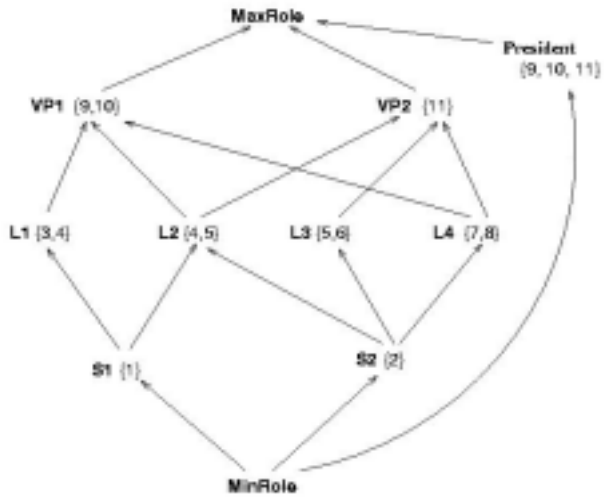

# Example of Insert2




Insert2

- Role name: President
- Effective: {9,10,11}

## Result






## Other Algorithms

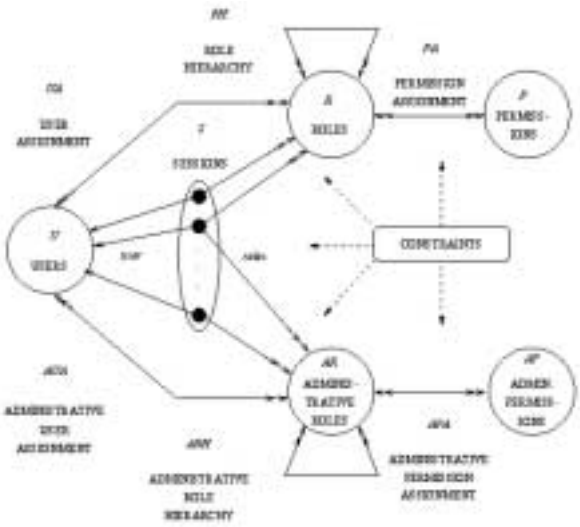
- Delete role
- Add/delete privileges to/from a role
- Add/delete edges

They all restore certain properties:

1. Acyclic (aborts if duplicate roles created)
2. path $r_i \leadsto r_k$ if privs of $r_i \subset$ privs of $r_k$
3. MaxRole and MinRole are always present
4. Display transitive reduction, with MaxRole at top of page, MinRole at bottom, and inheritance of privileges going up the page.

- All the algorithms are polynomial in the size of the graph and the size of the privilege lists

## Sandhu's RBAC'96 model





## Relationship of DAC, MAC and RBAC

- RBAC can simulate MAC and DAC (Osborn, Sandhu and Munawer, ACM TISSEC, May 2000)
- The DAC simulation uses lots of administrative roles
- The MAC simulation assumes one administrative role, and is very simple

## Issues for Database Security

- More granularity types
- Access to containers implies access to contents
- Also access to schema information
- Access to data implies can read schema
- More operations than simply read/write/execute
- Some notion of administrative roles whether or not there are roles for users: DBA, sysadmin,etc.
- Transactions



## How RBAC fits with relational

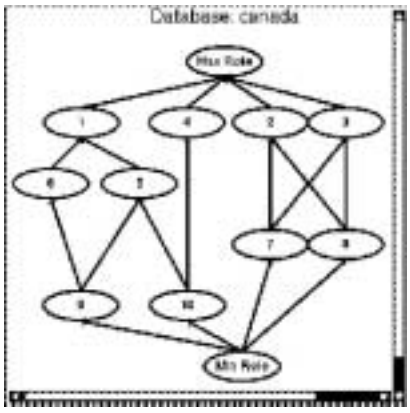
- Can look at the permission information and draw the role graph (next example)
- Role names have to be generated
- Also did a project which converted from a role graph to DB2 (had to turn off table ownership – control privilege)

# That example from DB2

```
db2 => connect to canada

   Database Connection Information

 Database product        = DB2/6000 1.1.0
 SQL authorization ID    = LKR
 Local database alias    = CANADA

db2 => select * from sysibm.systabauth where tcreator <> 'SYSIBM'

GRANTOR  GRANTEE  TCREATOR TTNAME           TABAUTH CONTROLAUTH ALTERAUTH DELETEAUTH INDEXAUTH INSERTAUTH SELECTAUTH UPDATEAUTH REFAUTH
-------- -------- -------- --------------- ------- ----------- --------- ---------- --------- ---------- ---------- ---------- -------
SYSIBM   LKR      LKR      PROVINCES           255 Y           Y         Y          Y         Y          Y          Y          Y
SYSIBM   LKR      LKR      ANIMALS             255 Y           Y         Y          Y         Y          Y          Y          Y
SYSIBM   LKR      LKR      MUSIC               255 Y           Y         Y          Y         Y          Y          Y          Y
LKR      WELCH    LKR      ANIMALS              32 N           N         N          N         N          Y          N          N
LKR      CAM      LKR      ANIMALS              32 N           N         N          N         N          Y          N          N
LKR      DSTOKES  LKR      ANIMALS              32 N           N         N          N         N          Y          N          N
LKR      TOBAN    LKR      ANIMALS              32 N           N         N          N         N          Y          N          N
LKR      WARREN   LKR      PROVINCES            32 N           N         N          N         N          Y          N          N
LKR      PETE     LKR      PROVINCES            32 N           N         N          N         N          Y          N          N
LKR      WHYME    LKR      PROVINCES             4 N           N         Y          N         N          N          N          N
LKR      YHUANG   LKR      PROVINCES             4 N           N         Y          N         N          N          N          N
LKR      SYLVIA   LKR      PROVINCES             4 N           N         Y          N         N          N          N          N
LKR      HANAN    LKR      PROVINCES           152 N           N         Y          N         Y          Y          N          N
LKR      MAGI     LKR      PROVINCES           152 N           N         Y          N         Y          Y          N          N
LKR      JANICE   LKR      PROVINCES           152 N           N         Y          N         Y          Y          N          N
LKR      CURTIS   LKR      PROVINCES           152 N           N         Y          N         Y          Y          N          N
LKR      WELCH    LKR      PROVINCES            36 N           N         Y          N         N          Y          N          N
LKR      CAM      LKR      PROVINCES            36 N           N         Y          N         N          Y          N          N
LKR      DSTOKES  LKR      PROVINCES            36 N           N         Y          N         N          Y          N          N
LKR      TOBAN    LKR      PROVINCES            36 N           N         Y          N         N          Y          N          N
LKR      BAUER    LKR      MUSIC                32 N           N         N          N         N          Y          N          N
LKR      SANDY    LKR      MUSIC                36 N           N         Y          N         N          Y          N          N
LKR      PERY     LKR      MUSIC                98 N           N         N          N         N          Y          Y          N
LKR      ROBBINS  LKR      MUSIC                72 N           N         N          Y         N          N          Y          N
LKR      KATCHAB  LKR      MUSIC                64 N           N         N          N         N          N          Y          N
LKR      BRUCE    LKR      MUSIC               104 N           N         N          Y         N          Y          Y          N

  26 record(s) selected.
```



# Becomes this role graph




| Role | Users | Effective Privileges |
|---|---|---|
| MaxRole | LKR | Provinces: All; Animals: All; Music: All |
| Role 1 | BRUCE | Music: Update, Select., Index |
| Role 2 | HANAN, MAGI, JANICE, CURTIS | Provinces: Select, Delete, Insert |
| Role 3 | CAM, WELCH, DSTOKES, TOBAN | Provinces: Select, Delete; Animals: Select |
| Role 4 | SANDY | Music: Delete, Select |
| Role 5 | PERY | Music: Update, Select |
| Role 6 | ROBBINS | Music: Update, Index |
| Role 7 | WARREN, PETE | Provinces: Select |
| Role 8 | WHYME, YHUANG SYLVIA | Provinces: Delete |
| Role 9 | KATCHAB | Music: Update |
| Role 10 | BAUER | Music: Select |
| MinRole | None | None |

## Oracle's roles

- A permission can be assigned to a user or to a role
- Roles can be assigned to roles
- Thus can get role hierarchies, but
  - not obliged to have only roles
  - no role graph or algorithms



## Integrating Two Systems

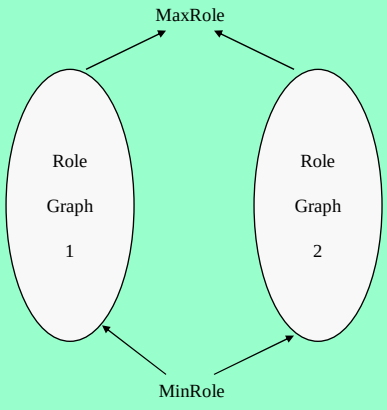
- Users - which have names
- Roles - which have names
- Privileges - data and operator
  - integrated by database integration techniques

# Basic Algorithm

- **Insert one role graph into the other**
  - **possibly with some intervention by Security Administrator**
- **Users get mapped to roles they had before**
  - **possibly with some intervention by Security Administrator**



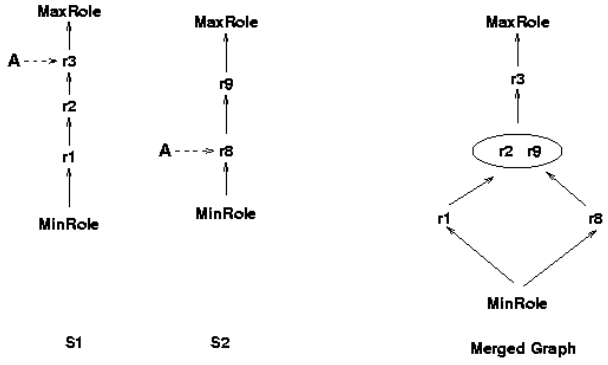
# Roles and Privileges Disjoint



## Privilege sets not disjoint, role names are, users may or may not be disjoint

- If a role from RG1 has equal privilege set to a role in RG2, merge the two roles in the result.
- Keep track of the mapping of the two roles to the merged role
- Map users in RG1 to same roles (or what they are mapped to)
- Do the same for RG2 - may need human intervention

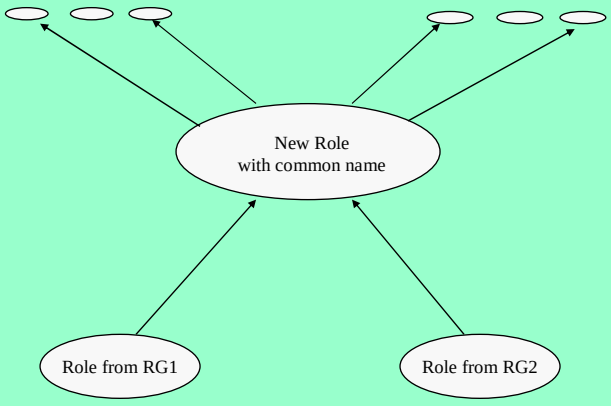




## Some duplicate role names, no duplicate privileges

- Needs human intervention
- Security admin can decide to rename one of them - back to first case
- Security admin can decide to keep the common role
  - rename two original roles - keep track of mapping to new role names
  - Insert new role with common name, and union of the privileges of the two original roles
  - The new role has no direct privileges

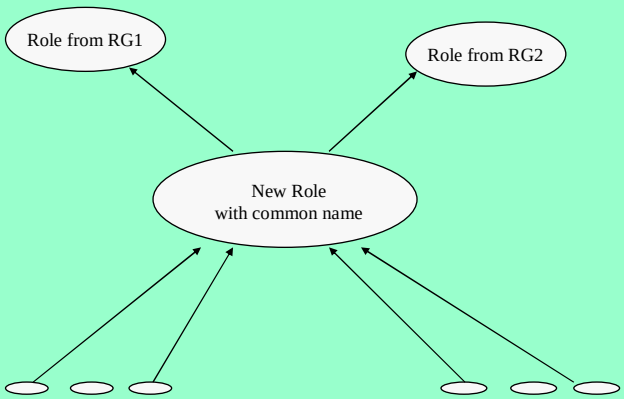




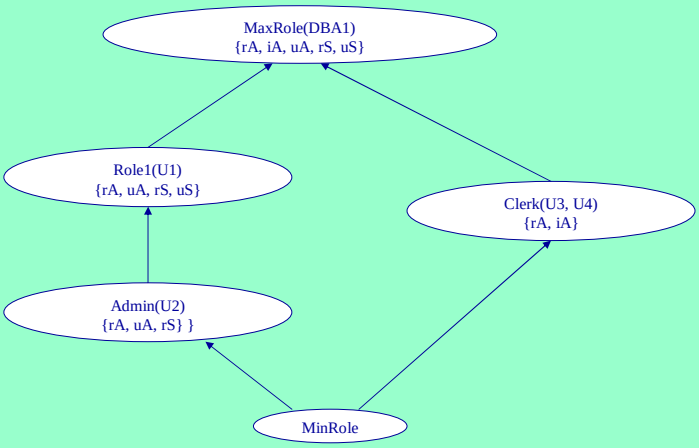
## Duplicate role names, duplicate privileges

- Completely disjoint privileges -- previous case
- Completely duplicate privileges -- just merge and map one of the names
- some overlap of privileges -- create a common junior with the intersection of privileges



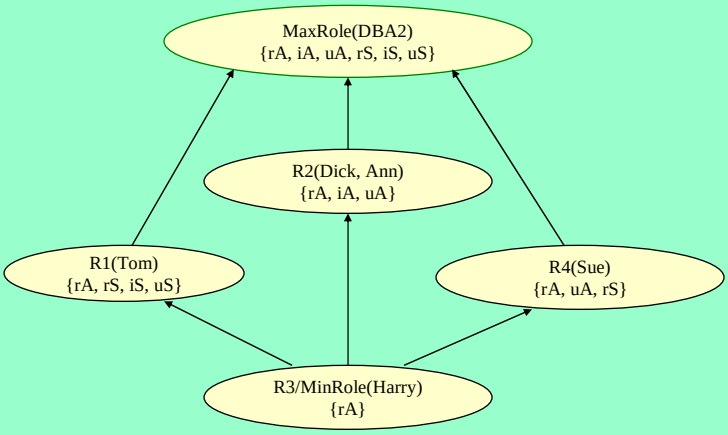


# System 1, Oracle e.g.

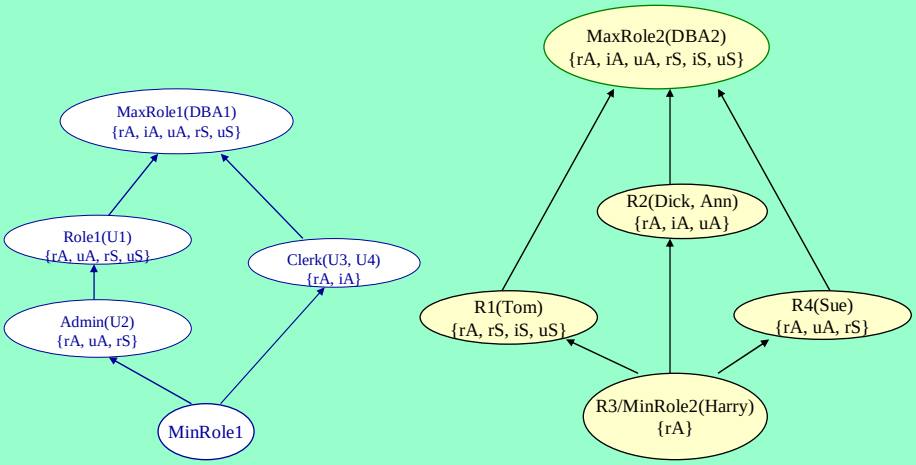





# System 2, automatically generated

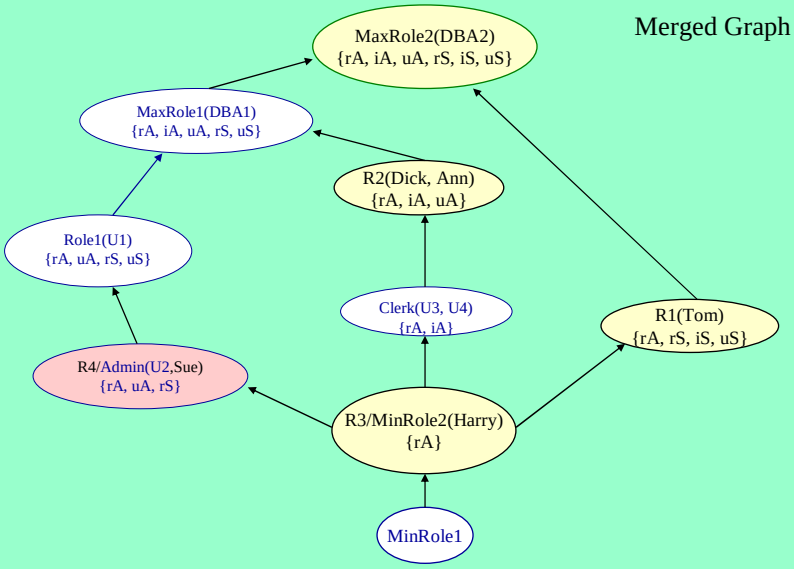


## Merging Role Graphs

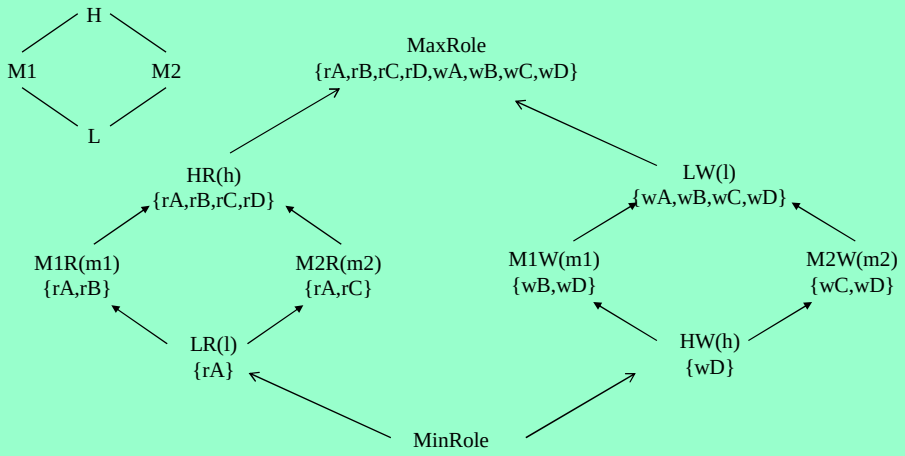





## Merged Graph

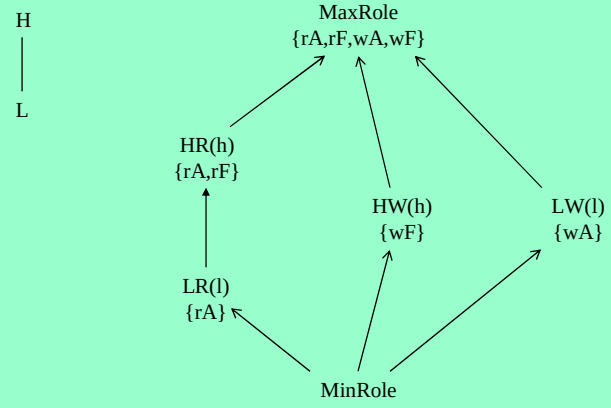


## Two Mandatory Systems

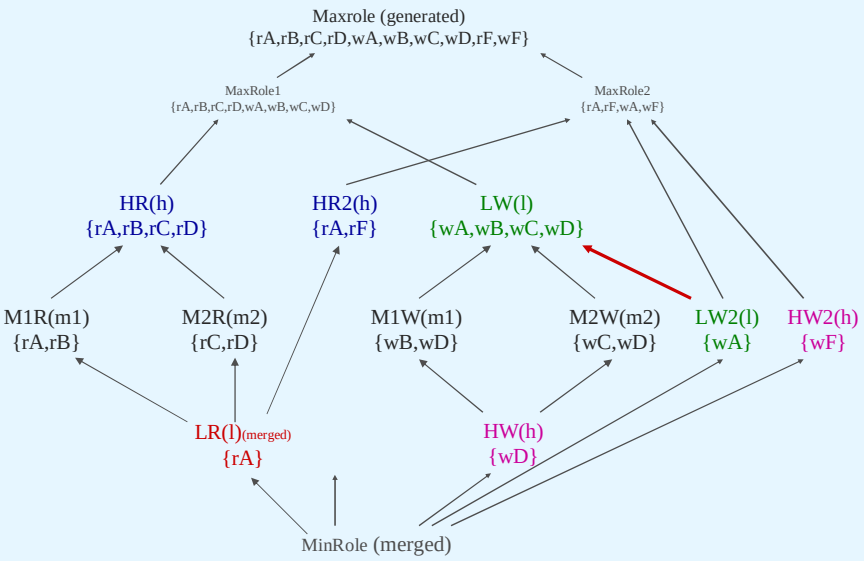



Liberal *-Property






Strict *-Property






# Conclusions

- **RBAC is a more natural, flexible way of expressing access control than traditional methods**
- **Managing a complex role hierarchy can be efficient**
- **Roles are available in relational packages**
- **Merging of role graphs can provide a general way to integrate security information**

# References


- Sylvia@csd.uwo.ca
- NIST: http://csrc.nist.gov/rbac/
- Ravi Sandhu's web page(draft NIST standard is there): http://ite.gmu.edu/list/sandhu/
- S. Osborn, R. Sandhu and Q. Munawer. Configuring Role-Based Access Control to Enforce Mandatory and Discretionary Access Control Policies.ACM TISSEC, vol.3, no. 2, (2000) 85-106.
- M. Nyanchama and S. Osborn,The Role Graph Model and Conflict of Interest, ACM TISSEC, vol.2, no. 1, (1999) 3-33.
- S. Osborn. Database Security Integration using Role-Based Access Control. in Data and Applications Security Developments and Directions, Thuraisingham, van de Riet, Dittrich and Tari, editors. Kluwer, 2001. 245-257.
- S. Osborn, L.K. Reid and G.J. Wesson. On the Interaction Between Role-Based Access Control and Relational Databases,Proceeding of the IFIP WG11.3 Tenth Annual Working Conference on Database Security,Chapman \& Hall, Samarati and Sandhu eds., July, 1996, 275--287.