Secure Role Activation and Authorization in the Enterprise Environment

Richard W.C. Lui Lucas C.K. Hui
S.M. Yiu

Department of Computer Science
The University of Hong Kong

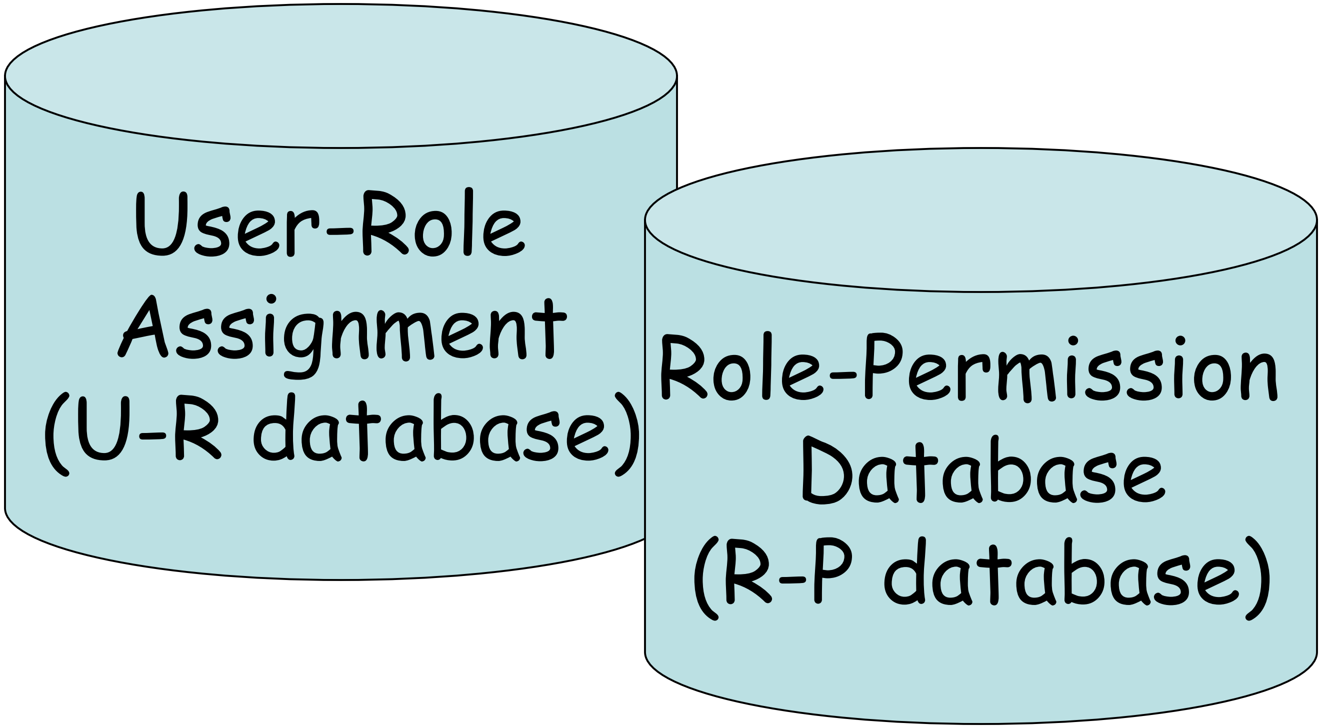
Outline

- Traditional Role Based Access Control
- Additional Constraints for Access Control
- The Proposed Approach:
  - Role Issuing (Assignment)
  - Role Activation
  - Resources Access
- Summary and Future Directions

Role Based Access Control (RBAC)

- Popular Access Control Paradigm
  - Users are assigned to roles based on their responsibility and qualification
  - Roles are assigned to permission.
  - A user who is assigned a role may activate the role (or a junior role) to exercise the associated permission.

Traditional Approach



User-Role Assignment (U-R database)

Role-Permission Database (R-P database)

When a user requests for a resources (e.g. access a data file or execute a function), the system will check with these databases before granting the access.

Additional Constraints for Access Control

Examples:

- A certain role can only be activated within a certain period of time. (e.g. in our dept, examination grade data entry officer)

-The same person may be assigned two *conflicting roles* that cannot be activated at the same time (e.g. Account entry officer and Auditor).

- The same role in different departments (domains) in the same company may have different constraints.

Role Assignment, Activation and Authorization

Role Assignment: A user is assigned a set of roles.

Role Activation: A user requests to activate a particular role

Role Authorization: The user is authorized to activate the role (thus can access certain resources) if all constraints for activation are satisfied.

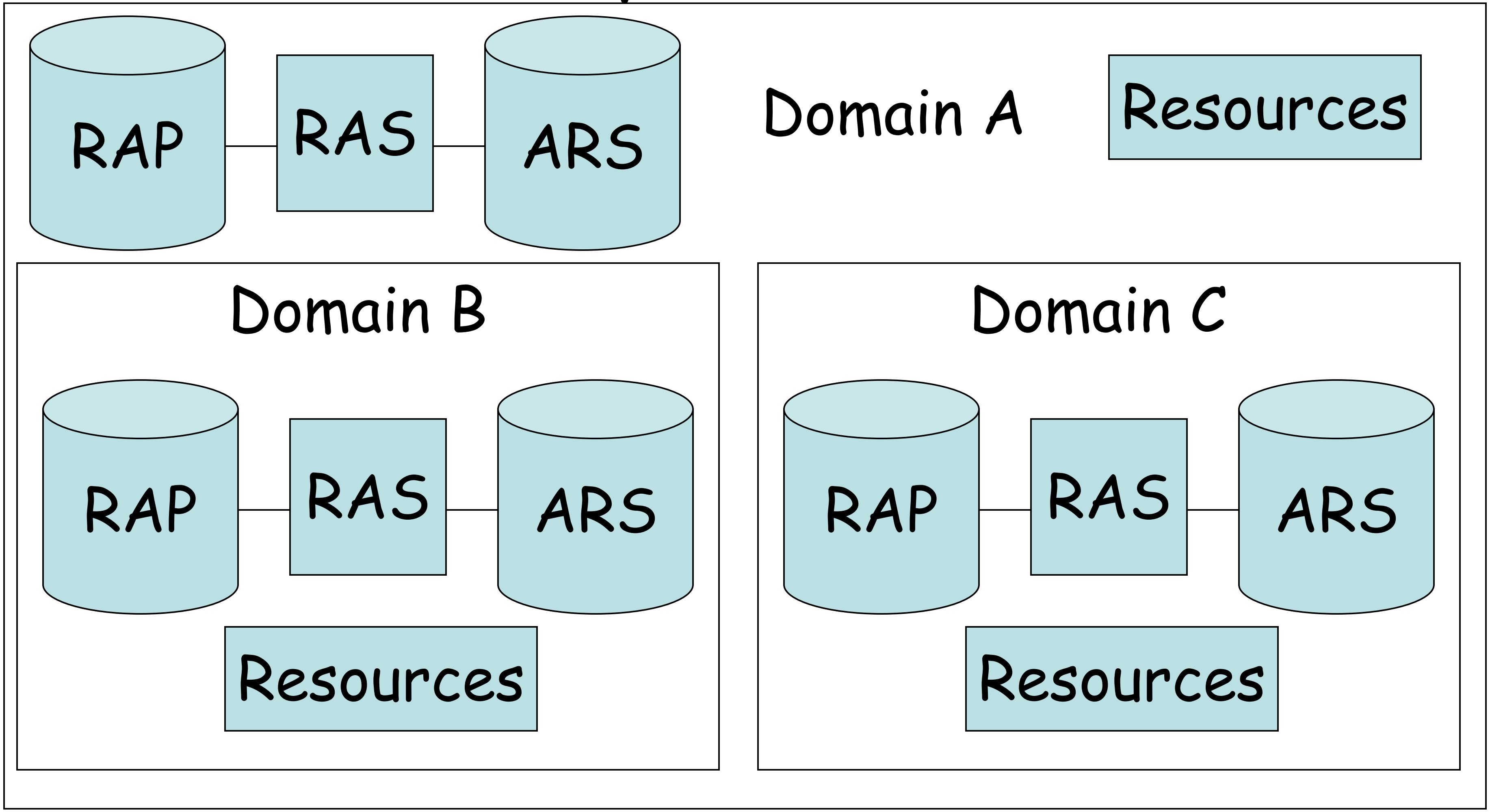
Note: RBAC may not be easily extended to handle the complicated constraints.

Some Possible Solutions

- Let the applications handle it
  - May have to repeat the same checking for different applications.
  - The security relies on the application programmers.
- Use a centralized server
  - The server will be heavily loaded.
  - Domain-specific constraints are not easy to handle by the enterprise-level server.

Note: Also, the U-R database may provide a single attack point for attackers.

The Proposed Model



RAS: Role Activation Server
RAP: Role Activating Policy
ARS: Activated Role Set

Remarks

- Each user belongs to a domain. To activate a role, it approaches the corresponding RAS.
- Basic security requirements:
  - A user should not be able to activate a role without being assigned to the role.
  - A user should not be able to access a resource without successfully activating the corresponding role.
- Offloads the applications: no need to check a lot of conditions before allowing a resource to be used.

- Try to make sure that the U-R information cannot be easily modified.
- Three issues (or protocols) to be handled:
    - Role Issuing (or Assignment)
    - Role Activation
    - Resources Access

Digital Credentials

- We propose to use digital credentials to handle the problems (In fact, we borrow the idea of Kerberos and makes use of PKI).
- Digital Credential
  - assertion to bind a user to a role.
  - activate the role for that user.
  - Integrity protected by digital signature
    - The U-R relationship is signed

The Proposed Approach

- Assumptions
  - Each user and RAS in the organization is associated with a public/private key pair.
  - There is a role-assignment key pair for the organization to assign roles to users. (Role assignment administrator)

Role Issuing (Assignment):

- A role activation certificate (RAC)
  - to bind a user's public key to a role he/she may activate
  - Signed with the role-assignment private key
  - only the user who has the knowledge of the user's private key may activate the role

Role Activation:

- To activate a role r at a RAS
  - the user should authenticate himself and present the RAC for r
  - RAS evaluates the defined RAP
- If the role activation is authorized, the RAS generates an access certificate (AC)
  - signed using the private key of the RAS
  - to certify that the user has activated a certain role

Resource Access:

- To access resources (which requires the role r to be activated)
  - the user should authenticate himself/herself.
  - and present the *AC* to the resource to show that he/she has activated r.
  - In addition, he/she should present the RAC for r to prove his/her membership in the activated role

Note: no need for applications to check the activation policy or access policy.

A Brief Discussion on Security

- RAC is signed with the role-assignment private key.
  - The role assignment private key is recommended to be kept offline after use or in a separate server.
  - As long as the signature scheme is secure, the attacker cannot easily modify any of the existing U-R assignments.

- Consider the compromise of the RAS
  - The private key of the RAS cannot be kept offline because it is required to sign the AC for role activation.
  - the role assignment private key is not known by the attacker
  - the attacker will not be able to generate any new RAC for himself/herself although the attacker may be activate the role even if it does not satisfy the RAP

Other Issues

Revocation

- The binding between users and roles in a RAC may become invalid as the responsibility of the user changes.
- roles may be deactivated by the user when he/she completes a task or intends to activate a conflicting role to perform another task.
- Possible Approaches
  - Expiry time
  - Online revocation server

Role-Hierarchy

- A user assigned to a certain role r will also be indirectly assigned to all the junior roles.
- A user issued a RAC for role r will also be issued the RACs for all roles r'< r (< means junior).
- This approach allows the RAS and resources to verify the user's membership in a role directly or indirectly assigned without managing a local copy of the role hierarchy.

Summary & Future Work

- In this paper, we highlight the problems of role activation and authorization especially in an enterprise environment in which there are complicated constraints governing whether a role can be activated.
- We proposed to use digital credentials to handle the problems and give details on how to process role assignment, role activation, and resource access.
- We mainly point out the problems, but not yet provide a satisfactory solution to the problems.

- Some possible future directions include
  - Design better models/schemes for this role activation and authorization problem.
    - More secure
    - More efficient
    - More general

  In fact, in the paper, we have provided another set of protocols for performing role assignment, role activation, resource access based on the idea of proxy signature.

- Whether the existing RBAC systems can be extended to handle the problems.

- We did not cover the details of RAP (Role Activating Policy), it deserves more effort on it, for examples, how to specify this policy, whether a language should be defined for it.

< Thank you >