Role Based Access Control Slide Set - May 1995

Janet Cugini and David Ferraiolo

National Institute of Standards and Technology

Technology Administration

U.S. Department of Commerce

Gaithersburg, MD 20899 USA

cugini@csmes.ncsl.nist.gov

ABSTRACT

This set of slides gives our definition for Role-Based Access Control, gives some historical background, and describes our current NIST RBAC projects. These projects include an NSA R23 sponsored project whose tasks include the development of an RBAC formal model and an implementation of RBAC on R23's Mach microkernel-based distributed operating system called Synergy. This set of slides also gives the motivation for RBAC and the preferred environment of use. As opposed to other access control policies, RBAC actually models how an enterprise functionally allows access by those in various job positions to the objects that the enterprise owns, and RBAC greatly eases system administration. We show these principals in the model through our definitions for a role, role actions, role types, job positions, organization units, and resource sets, and by defining system administration actions. Also, in this set of slides the list of model components is given and various model properties are highlighted. These properties include the Role Type Inheritance property which shows how role types form a lattice and shows multiple inheritance of attributes, the Separation of Duty properties, and the Conflict of Interest properties, all of which are fundamental to our definition of Role-Based Access Control. Then, the state dependent, state independent, and state properties are listed as well as the final theorem that provides a proof for the properties. This set of slides also includes a description of the possible cooperative agreements that NIST can have with industry. Since RBAC is particularly suited for the non-classified environment, we here at NIST are very interest in forming alliances with industry to create a standard definition for RBAC and for furthering this work. Finally, the advantages of RBAC are summarized.

Role Based Access Control

Janet Cugini, David Ferraiolo

Security Division, Computer Systems Lab, NIST

Building 224/A24, Gaithersburg, MD 20899

Phone: (301) 975-4524

Fax: (301) 926-2733

cugini@csmes.ncsl.nist.gov

RBAC Definition

- A mechanism which allows and promotes an organization-specific access control policy based on roles
- **Non-discretionary**:
  - users do not “own” objects for which they are allowed access
  - protection policies are unavoidably imposed on all users
  - does not deal with information flow

NIST RBAC Background

- Study of security needs of commercial and civil organizations [1991-92]
- D. Ferraiolo, R. Kuhn paper: *Role-Based Access Control*, NIST/NSA National Computer Security Conference, 10/92
- Re-presented paper at OSF DME/DCE working group meeting [1993]

Current NIST RBAC Projects

- NIST Small Business Innovative Research (SBIR): Seta Corp.
- NSA R23 R&D Other Agency (OA) to NIST
- NIST Advanced Technology Program (ATP)

SBIR Tasks

- **Phase 1:** assess user needs, develop theoretical model and specification, explore approaches to implementation, describe how RBAC can be administered
- **Phase 2:** further define and prototype RBAC, demonstrate RBAC concepts, provide implementation guidance

NIST R23 RBAC Research Effort

- develop formal model
- develop architecture for NSA's distributed Mach-based OS Synergy
- Implementation and administrative interface
- Two "real world" demos
- Requirement specification (protection profile)

RBAC Motivation

- Simplify existing access control management functions (e.g., user accesses to a group of objects with a certain property)

- Provide functions not readily available in other methods of access control management (e.g., review of access rights of a subject, secure state determination)

RBAC Preferred Environment of Use

- **User Characteristics:** large number of users, few security administrators, frequent change of job responsibility
- **Data and Application Characteristics:** large number of data objects, sharing based on job functions
- **Enterprise Characteristics:** data owned by enterprise, controlled by security administrators, before and after the fact audit and periodic assessment of access control policy enforcement necessary.

Role

- Defines a set of functional responsibilities within an organization which implies a set of permitted actions &/or resources.
- Examples: in a hospital system, roles might be: doctor, nurse, and pharmacist.

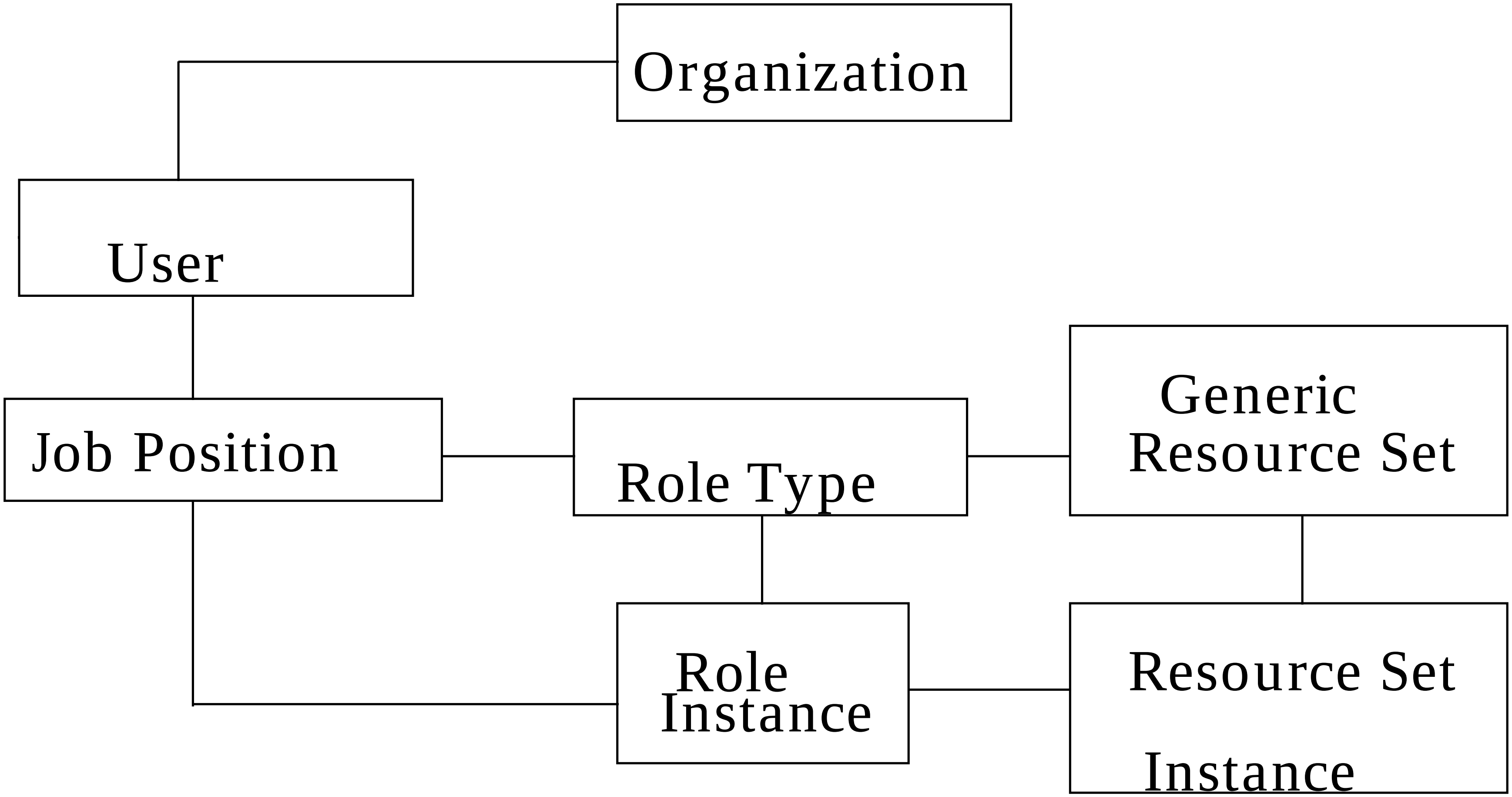
Role Actions

- Actions are selectively associated with roles
- The role of a pharmacist may include transactions to dispense, but not prescribe, prescription drugs
- Binding associated with the role and the actions that are associated with the role

RBAC Model Definitions

- **Role Types:** captures generic functions of the enterprise.
- **Role Instances:** captures the specific organizational context for each role type
- **Job Positions:** captures the constraints on user enrollment in different functions
- **Organization Unit:** captures the constraints placed on job positions and enterprise structure.

Enterprise Authorization Model



RBAC Formal Model

- Based on Seaview Formal Security Policy Model for for multilevel secure data bases.
- This model is based on a security theorem that states that if the initial state of a system is secure, and all subsequent operations are secure, then the system is secure.

RBAC Model Components

- **M_o:** Describes RBAC authorization
- **$M_{1:}$** Describes RBAC policy attribute management
- **Subcomponents of $M_{i:}$**

  o A set of TYPES, together with functions on these types

  o A set of STATES, which are defined by a set of state dependent functions.

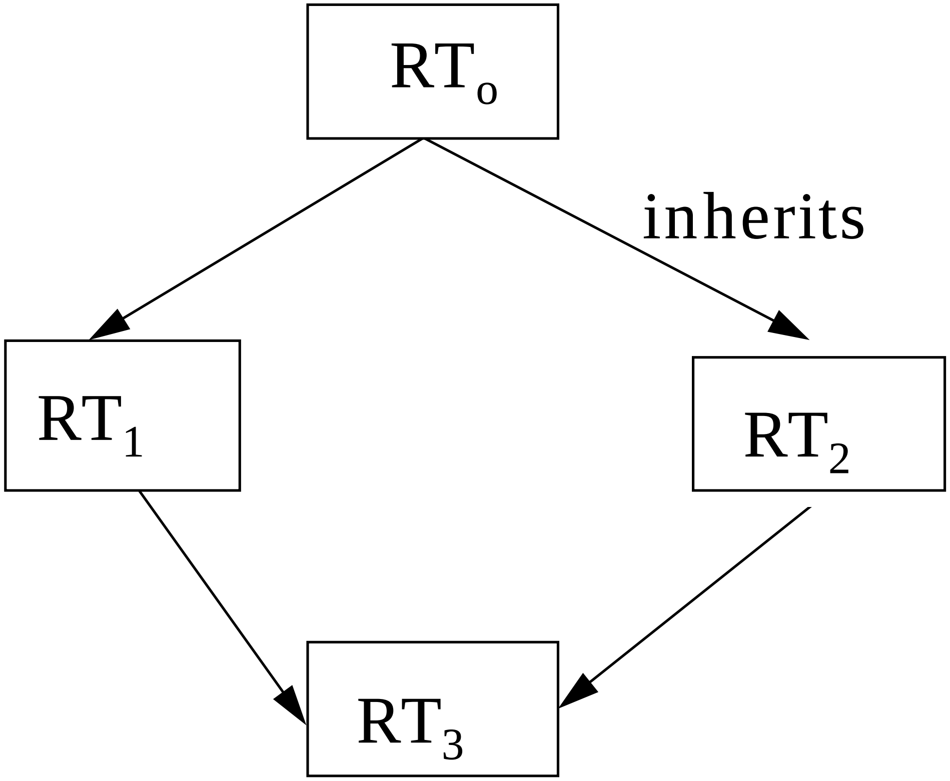
  o A set of COMMANDS of the form:

  $$op(s_1, S, x_1....x_n \text{ -> } s_2)$$

  o A set of command sequences.

  o A set of axioms, properties, and theorems.

Role Type Inheritance Property



Therefore, RT_3 dominates all other RTs

Separation of Duty Properties

- Two or more job positions have no common roles

- (**Strict**): Two or more job positions have no common access to any objects

Conflict of Interest Properties

- Two or more job positions are in conflict if they have incompatible roles

- (**Dynamic**): A user is not authorized to access an object in two job position roles

  -if he accessed the object in one role, he may not access the object in the other role

RBAC Type Property

- Is satisfied if and only if all state independent properties are satisfied, namely:

Active Role-Type Property
Role-type Instantiation Property
Separation of Duty Property
Conflict of Interest Property
Organization Attribute Property
Organization Object-Set Property

RBAC State Property

- Is satisfied if and only if all state-dependent properties are satisfied, namely:
  Initial Authorization Property   *Null Access Property*
  Active Access Property   *Role Inheritance Property*
  Role Authorization Property
  Active Job-Position Property
  Job-Position Authorization Property
  Strict Separation of Duty Property
  Dynamic Conflict of Interest Property
  Active Organization Unit Property
  Organization Unit Authorization Property

RBAC Transition Property

- Is satisfied if and only if all transition properties are satisfied, namely:

  Status Property *Discretionary Access Property*
  Create RB Object Property *Implicit Authorization Property*
  Create Role Type Object Property
  Role Type Deletion Property *Role Type Update Property*
  Create Job Position Object Property
  Job Position Deletion Property *Job Position Update Property*
  Discretionary Authorization Property
  Discretionary Revocation Property
  Create Organization Unit Object Property
  Organization Unit Deletion Property
  Organization Unit Update Property

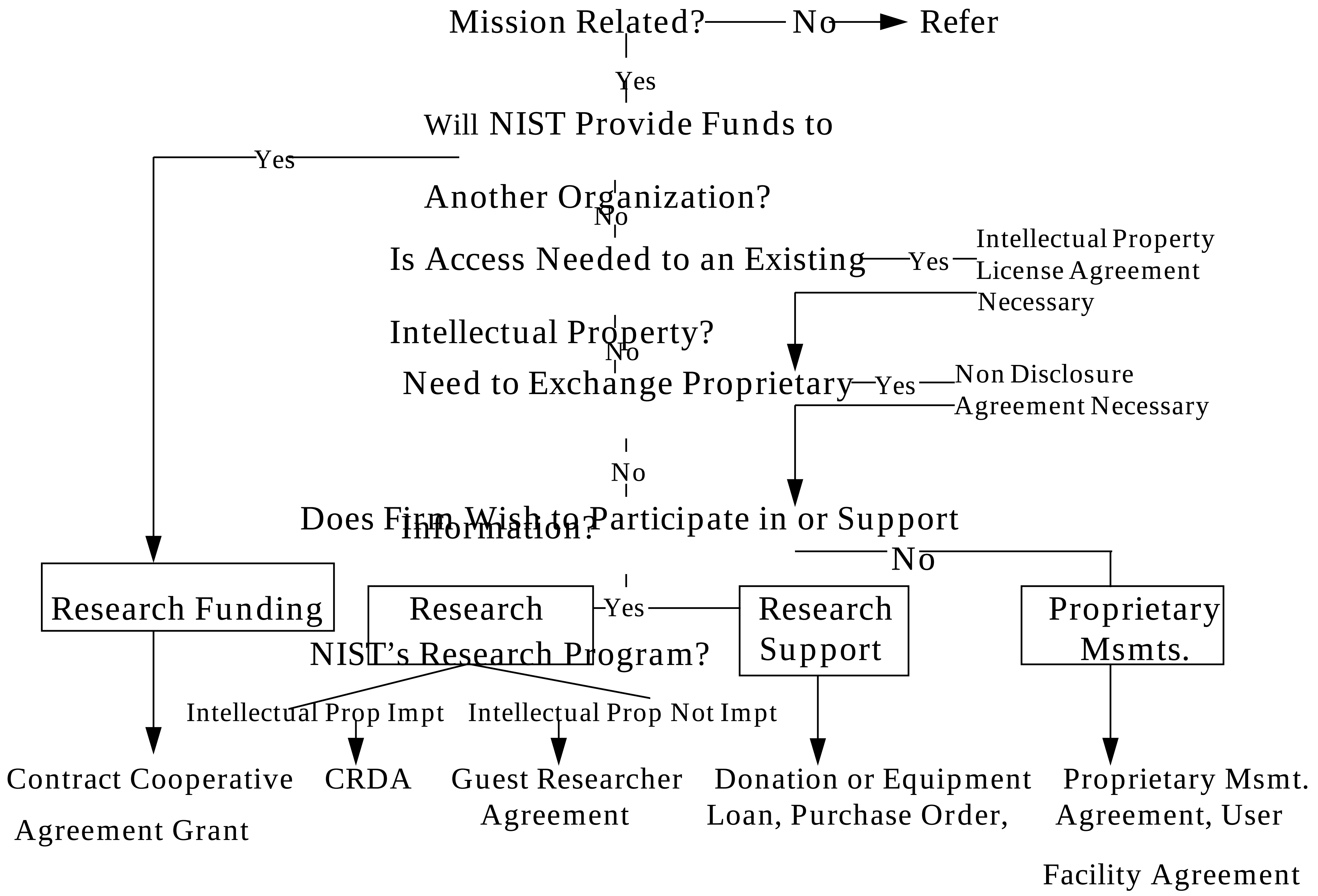
Theorem: RBAC Secure System

- If a system satisfies the RBAC Type Property, the initial state satisfies the RBAC State Property, and all commands satisfy the RBAC Transition Property, then the system is secure.

NIST Cooperative Agreements

- CRADAs: Cooperative Research and Development Agreement
- Guest Researchers
- Proprietary Measurement Agreement
- User Facility Agreement
- Donations/gifts/loans
- Research Support via Purchase Order
- Licenses
- Non-disclosure Agreements
- None - company comments on our work

Selecting the Agreement



Mission Related? No → Refer

Yes

Will NIST Provide Funds to Another Organization?

Yes

No

Is Access Needed to an Existing Intellectual Property?

Yes

Intellectual Property License Agreement Necessary

No

Need to Exchange Proprietary Information?

Yes

Non Disclosure Agreement Necessary

No

Does Firm Wish to Participate in or Support NIST’s Research Program?

Yes

No

Research Funding

Research

Research Support

Proprietary Msmts.

Intellectual Prop Impt

Intellectual Prop Not Impt

Contract Cooperative Agreement Grant

CRDA

Guest Researcher Agreement

Donation or Equipment Loan, Purchase Order,

Proprietary Msmt. Agreement, User Facility Agreement

Summary: RBAC Advantages

- More closely models enterprises and user actions than other types of access control (non-discretionary, user does not own objects)
- Allows per-subject (role) as well as per-object access review
- Greatly eases system administration