Role-Based Authorization and Access Control

Vance Heron
Security Architect
Institutional Computing & Information Systems
Jet Propulsion Laboratory
California Institute of Technology

Role Based Access Control (RBAC)

One of the most challenging problems in managing large networked systems is the complexity of security administration.

Today, security administration is costly and prone to error because administrators usually specify access control lists for each user on the system individually.

Role based access control (RBAC) is a technology that is attracting increasing attention, particularly for commercial applications, because of its potential for reducing the complexity and cost of security administration in large networked applications.

- NIST

How RBAC Works

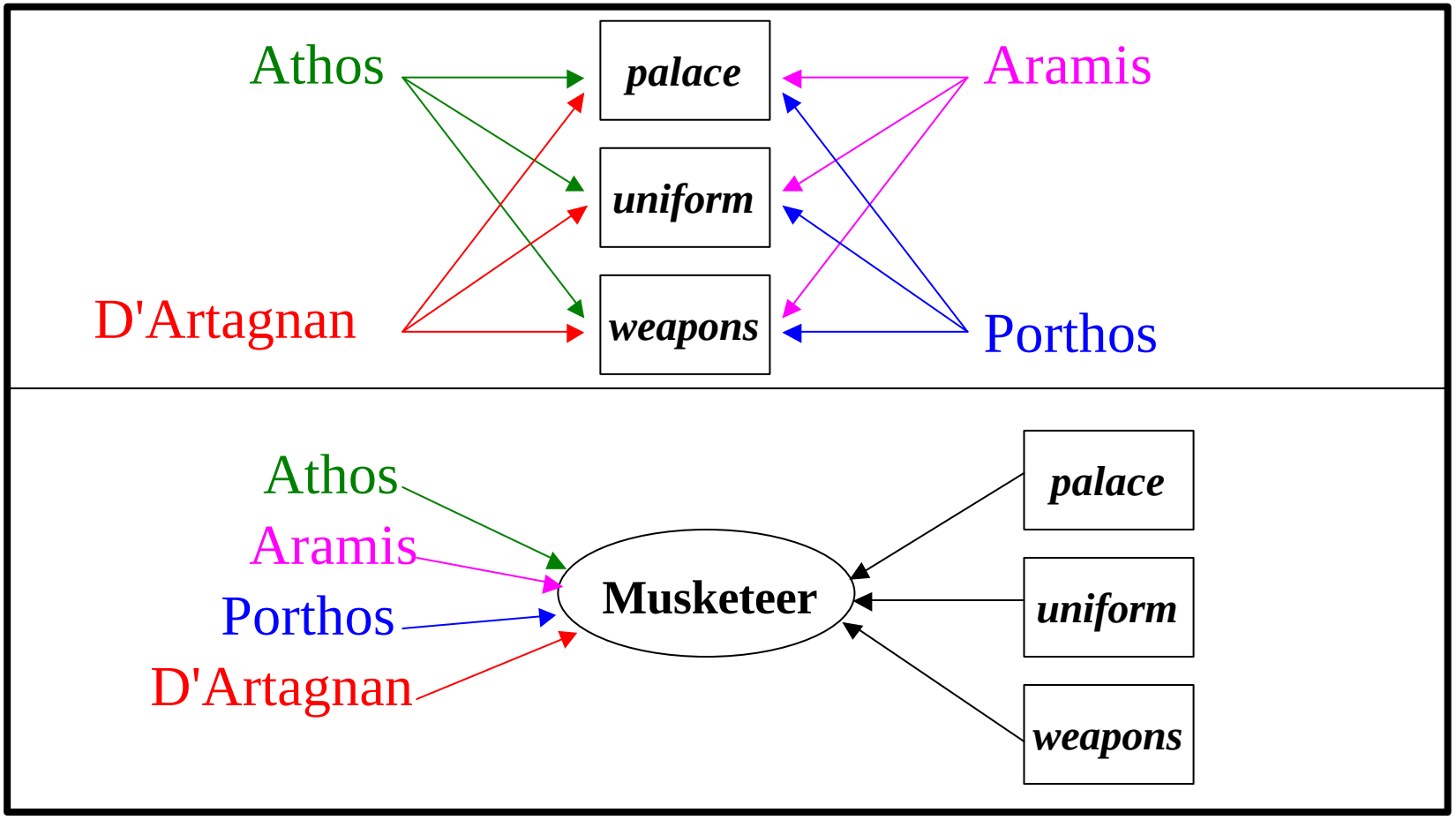
- Identities are assigned to roles
  - Can be many to many
  - Can be managed hierarchically
- Roles are granted Privileges
  - Many to Many relationship
- Can be constrained to enforce “Separation of Duties” requirements
  - Static constraints (Teller/Auditor)
  - Dynamic constraints (Teller/Customer)

Benefits of RBAC

- Reduce number of relationships
- Reduce changes to access control info
- Reduces duplication of access control info
- Reduces management costs
- Improves accuracy of access control information

Example from OMG CORBAmed Security Working Group Meeting Presentation

Used with permission of John Barkley
National Institute of Standards and Technology
http://csrc.nist.gov/rbac/



Example from OMG CORBAmed Security Working Group Meeting Presentation

Used with permission of John Barkley
National Institute of Standards and Technology
http://csrc.nist.gov/rbac/

Quantifying RBAC Advantage

- For each job position, let:

$U =$ Number of individuals in job position

$P =$ Number of permissions required for job position

$$(U + P) < (U \cdot P) \Rightarrow \text{RBAC advantage}$$

$$U, P > 2 \Rightarrow (U + P) < (U \cdot P)$$

- For all job positions,

$$\sum_{i}^{n_{jp}} (U_i + P_i) < \sum_{i}^{n_{jp}} (U_i \cdot P_i) \Rightarrow \text{RBAC advantage}$$

Function of IT Security in managing Role Information

- Facilitate collection and dissemination
  - does not own this information
  - use existing data sources/processes
  - create illusion of consistency
- Work with providers and users
  - primary customers are service providers
- Help improve existing processes
  - reduce (eliminate) duplication of effort

What we’re doing at JPL

- Roles kept as groups in the directory
  - some groups generated based on attributes
- Role info maintained with direct interfaces, and meta-directory software
  - Pull, Push, and Synchronize
- Currently using for three network services
  - several more in process

Implementation Issues

- Multiple sources of role information
  - with different management interfaces
  - often out of date (contain stale references)
- Management of role information
  - List role/identity relationships
  - List role/privilege relationships
  - Assign/Remove role info
    - Removal of roles on job change is a challenge

Implementation Issues (cont.)

- Transitioning existing identity based system
  - Where possible, retain existing mgmt interfaces
  - User education
- Multiple definitions of same role
  - Good use for role hierarchies
  - May require renaming existing roles