ASCAA Principles for Next-Generation Role-Based Access Control

Ravi Sandhu
Executive Director and Endowed Chair
Institute for Cyber Security
Univ of Texas at San Antonio
ravi.sandhu@utsa.edu
www.profsandhu.com
The State of Cyber Security

- We are in the midst of big change in cyber space
- Nobody knows where we are headed
- So far we have done a pretty bad job in cyber security
- There is hope
  - New services will not be held back
  - Need for security will remain
  - “Good enough” security is achievable
OLD THINK:
We had it figured out. If the industry had only listened to us our computers and networks today would be secure.

REALITY:
Today’s and tomorrow’s cyber systems and their security needs are fundamentally different from the timesharing era of the early 1970’s.
Change Drivers

Stand-alone computers → Internet

Vandals → Criminals

Enterprise security → Mutually suspicious yet mutually dependent security

Few standard services → Many and new innovative services
DAC: Discretionary Access Control

- The owner decides who gets access
- Anyone with read access can copy and owns the copy
- The classic formulation of DAC is fundamentally broken
- Solving the owner-control problem correctly is high priority (but a different lecture)

First emerged: early 1970s
First models: early 1970s
MAC: Mandatory Access Control

- Who gets access is determined by security labels
- A user’s security label is assigned by a security officer
- Copies are automatically labeled correctly by the security system

First emerged: early 1970s
First models: early 1970s
MAC: Mandatory Access Control

Lattice of security labels:
- TS
- S
- C
- U

Information Flow
– There is MAC (good)
– There is DAC (weak)
– Don’t need anything else
RBAC: Role-Based Access Control

- Access is determined by roles
- A user’s roles are assigned by security administrators
- A role’s permissions are assigned by security administrators
- Control on copies determined by configuration of roles

Is RBAC MAC or DAC or neither?

First emerged: mid 1970s
First models: mid 1990s
Fundamental Theorem of RBAC

- RBAC can be configured to do MAC
- RBAC can be configured to do DAC
- RBAC is policy neutral

RBAC is neither MAC nor DAC!
Example Role Hierarchy

Director (DIR)

- Project Lead 1 (PL1)
  - Production 1 (P1)
  - Quality 1 (Q1)
  - Engineer 1 (E1)

- Project Lead 2 (PL2)
  - Production 2 (P2)
  - Quality 2 (Q2)
  - Engineer 2 (E2)

Engineering Department (ED)

Employee (E)

Inheritance hierarchy
Example Role Hierarchy

Director (DIR)

- Project Lead 1 (PL1)
  - Production 1 (P1)
  - Engineer 1 (E1)
  - Quality 1 (Q1)

- Project Lead 2 (PL2)
  - Production 2 (P2)
  - Engineer 2 (E2)
  - Quality 2 (Q2)

Engineering Department (ED)

Employee (E)

Inheritance and activation hierarchy
Permission-role review is advanced requirement

Inheritance and/or activation

Limited to separation of duties

Overall formal model is more complete

Institute for Cyber Security
Founding Principles of RBAC96

- **Abstraction** of Privileges
  - Credit is different from Debit even though both require read and write

- **Separation** of Administrative Functions
  - Separation of user-role assignment from role-permission assignment

- **Least Privilege**
  - Right-size the roles
  - Don’t activate all roles all the time

- **Separation of Duty**
  - Static separation: purchasing manager versus accounts payable manager
  - Dynamic separation: cash-register clerk versus cash-register manager
ASCAA Principles for Future RBAC

- **Abstraction** of Privileges
  - Credit vs debit
  - Personalized permissions
- **Separation** of Administrative Functions
- **Containment**
  - Least Privilege
  - Separation of Duties
  - Usage Limits
- **Automation**
  - Revocation
  - Assignment: (i) Self-assignment, (ii) Attribute-based
  - Context and environment adjustment
- **Accountability**
  - Re-authentication/Escalated authentication
  - Click-through obligations
  - Notification and alerts
Usage Control: The UCON Model

- unified model integrating
  - authorization
  - obligation
  - conditions
- and incorporating
  - continuity of decisions
  - mutability of attributes

Mutability of Attributes

Continuity of Decisions

before-usage ongoing-Usage after-usage

pre-decision ongoing-decision

pre-update ongoing-update post-update

• unified model integrating
  • authorization
  • obligation
  • conditions
• and incorporating
  • continuity of decisions
  • mutability of attributes
Conclusion

– RBAC is here to stay
  • ABAC will still use roles as one attribute
  • Attribute-based assignment to roles

– Access control needs agility
  • Usage limits
  • Automation (self-administration)
  • Accountability

– This is already happening
  • Our models have fallen behind

– ASCAA principles apply beyond RBAC
  • UCON model incorporates ASCAA