Module 3.2
Access Control Models: Alphabet Soup

Ravi Sandhu

Spring 2021
Access Control Models

Discretionary Access Control (DAC) 1970

Mandatory Access Control (MAC) 1970

Role Based Access Control (RBAC) 1995

Attribute Based Access Control (ABAC)

Flexible policy

Fixed policy

2020s (Hopefully)
Access Control Models

Discretionary Access Control (DAC)
1970

Mandatory Access Control (MAC)
1970

Role Based Access Control (RBAC)
1995

Attribute Based Access Control (ABAC)
Encompasses
Relationship-Based Access Control (ReBAC)
Usage Control (UCON)
Rule-Based, Policy-Based, etc
2020s (Hopefully)

Fixed policy

Flexible policy

© Ravi Sandhu

World-Leading Research with Real-World Impact!
(s,o,r) allowed or not?
- s: subject (aka actor)
- o: object (aka target)
- r: right (aka operation)

(s,o,r,c) allowed or not?
- s, o, r: as above
- c: context (aka environment)
(s,o,r) allowed or not?
- s: subject (aka actor)
- o: object (aka target)
- r: right (aka operation)

(s,o,r,c) allowed or not?
- s, o, r: as above
- c: context (aka environment)
Access Decision Function

- (s,o,r) allowed or not?
  - s: subject (aka actor)
  - o: object (aka target)
  - r: right (aka operation)

Access decision triple

- (s,o,r,c) allowed or not?
  - s, o, r: as above
  - c: context (aka environment)

Access decision quad

- c: beyond Access Matrix
  - c integrates well with ABAC
Operational model
- specify the decision function for the access decision triple or quad

Administrative
- specify the model’s dynamics
- dynamics change the system state and modify the outcome of some access decision triple or quads
Operational model

- \((s, o, r)\)?
- authorized iff \(r \in [s, o]\) cell of the matrix

Administrative

- specify the semantics of the administrative rights: own, parent etc
Operational model

- specify the decision function for the access decision triple or quad

Administrative

- specify the model’s dynamics
- dynamics change the system state and modify the outcome of some access decision triple or quads

Our focus
Operational model

- specify the decision function for the access decision triple or quad

Administrative

- specify the model’s dynamics
- dynamics change the system state and modify the outcome of some access decision triple or quads
Access Control
PEI Layers

- Security and system goals (objectives/policy)
  - Necessarily
    - Informal
  - Formally or quasi-formally
    - System block diagrams, protocol flows

- Policy models
  - Enforcement models
    - Implementation models
      - Trusted Computing Technology (mechanisms/implementation)

Big decisions
- Idealized
- Enforceable
- Codeable
- Code
Our focus

Big decisions

Idealized

Enforceable

Codeable

Code

Security and system goals

Formally

quasi-formal

System block diagrams, Protocol flows

Pseudo-code

Actual Code

Trusted Computing Technology

(mechanisms/implementation)

Implementation models

Pseudocode

Actual Code

Policy models

Necessarily Informal

Formal/ quasi-formal

Codeable

Enforceable

Idealized

Big decisions

Our focus

Security and system goals (objectives/policy)
Enforcement Models

**PUSH MODEL**

- Client
- Authentication + Authorization Credentials
- Server

**PULL MODEL**

- Client
- Authentication Credentials
- Server
- Authorization Credentials