Identity, Authentication and Authorization

John Slankas
jbslanka@ncsu.edu

Computer Science
NC STATE UNIVERSITY

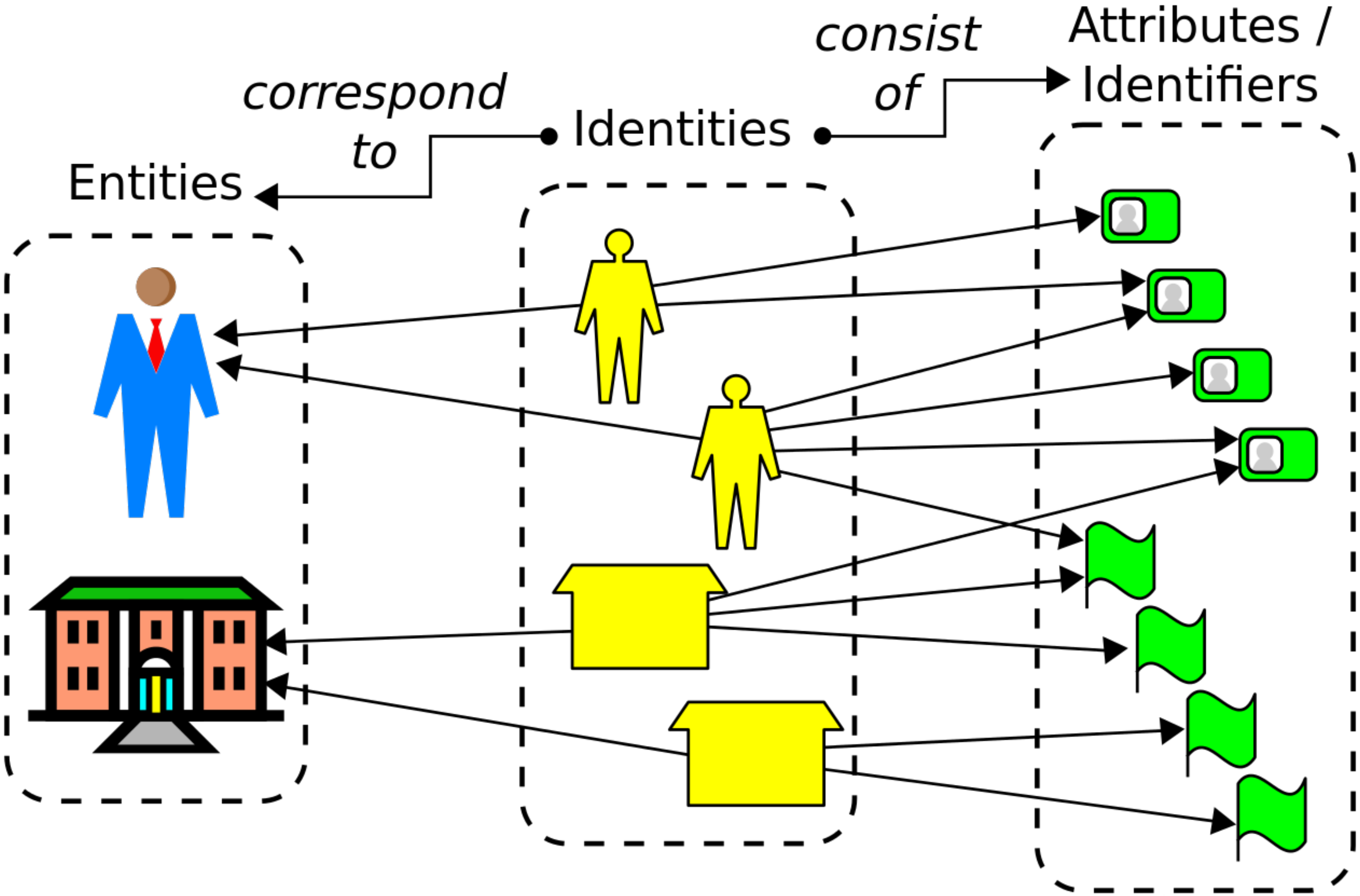
MURDER
ADULTERY
CRAWLING
I HAVE KILLED A BABY
I AM THE SINNER
I RAPED 15 YEARS OLD GUZ
I HAVE FORGOT TO DO MY HOMEWORK
SICK OF IT ALL
ANGER
saddness
go to the heel
i killed a man
one touch
GOBE
KROTEGINI
KILLER
ley

Identity

Who or what a *person* or *thing* is; a distinct impression of a single person or thing presented to or perceived by others; a *set of characteristics* or a description that *distinguishes* a person or thing from others.

Oxford English Dictionary

Identity



https://en.wikipedia.org/wiki/File:Identity-concept.svg

What signifies an identity?

- For People
- Machines
- Services
- Messages

Personal Identification

- Name (?)
- Email address
- Identifier
  - Unity ID
  - Social Security Number
- Combination of attributes
- Driver's License / Passport
- ATM card

Sources of Personal Identification

- Authoritative source
  - HR System
  - Student Information Service
- "Trust Chain"
  - Passports and driver's licenses are issues by trusted parties
  - SSL Certificates
  - Phone numbers, credit cards
- Self

Machines

- IP Address
- DNS Names
- SSH Host Keys
- Certificates
- Machine Address Code (MAC)

Services

- Uniform Resource Identifier (URI)
- Certificates
- Images

  (authentication process for some websites)

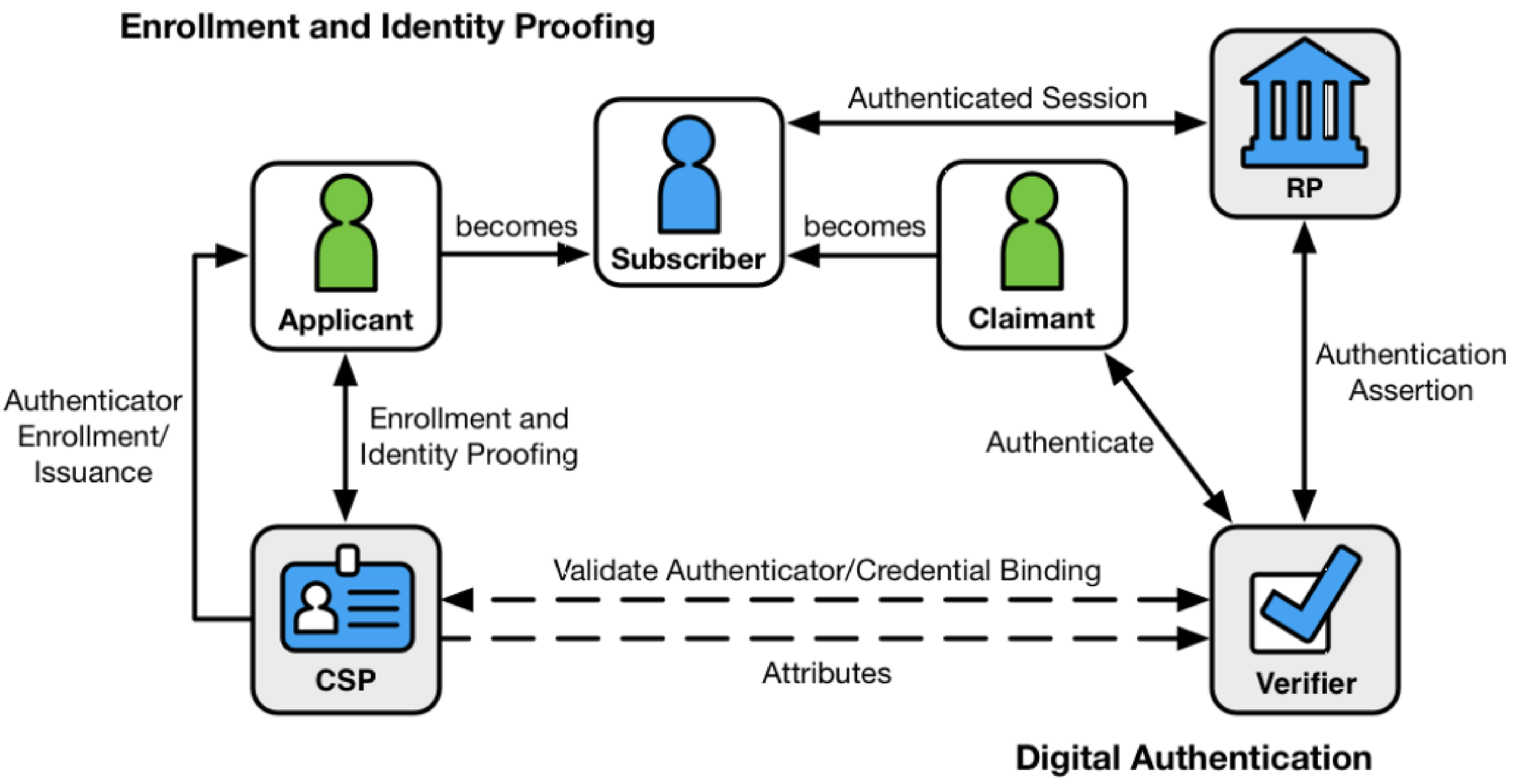
Messages

- Protocol
- Message Authentication Code
- Checksums
  - Provide integrity

Identity Resolution / Record Linkage

- Link identities across different data sources and/or different transactions
- Examples
  - Twitter, e-mail, Facebook, web-page accounts
  - Different sources (vendors and employees, public records)
- Applications
  - Credit history
  - Profiling (e.g., Target)
  - Historical research (including medical)

Digital Identity Model



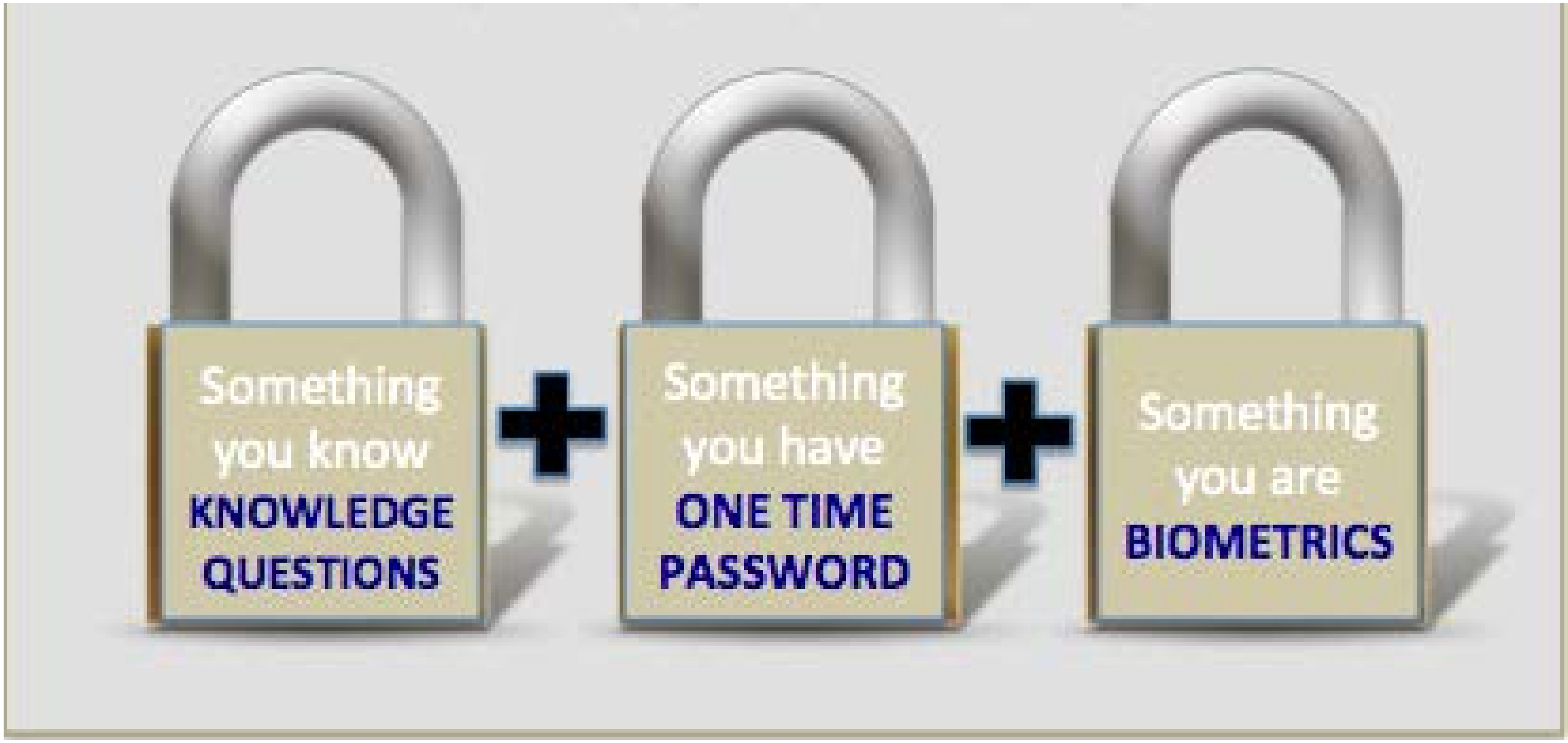
Source: NIST SP-800-63-3: Digital Identity Guidelines

Authentication

Validate an entity's identity

http://www.moillusions.com/optical-illusion-fingerprints/

Authentication Factors



Multifactor - at least two of these categories

Authentication Protocols

- Kerberos
- Transport Layer Security (TLS / SSL)
- Host Identity Protocol
- SAML / OAuth
- ….

- Central topic of 574 – Computer and Network Security

Authentication Best Practices

- Emails
  - Correct form
  - Deliverable
- Hash stored passwords with salts
- Account lockout procedures
- Externalize (e.g., Shibboleth)
- Re-authenticate for sensitive operations
- Effective password management
  - Rules (length, types of characters, …)
  - No defaults
  - Expiration time

Authentication Weaknesses

- Knowledge
  - Easy to guess
  - Written down in a non-secure location
  - Stealing: eavesdropping, social engineering
- Physical devices
  - Stolen
  - Copied
- Biometrics
  - Duplicated

2017 NIST Password Guidelines

- Remove password complexity rules
- Length matters more
- No periodic password resets
- Enable “Show Password”
- Allow Paste in Password Fields

2017 NIST Password Limitations

- Forbid commonly used passwords
- Don’t use password hints or knowledge-based authentication
- Limit the number of password attempts

2017 NIST Password Storage

- Salt passwords with at least 32 bits of data
- Password-based Key Derivation Function 2
  - At least 10,000 iterations
- Stores salts separately

Authorization

What can an entity can do?

Access Control

- Implements authentication and authorization
- Significant, widely-used control mechanism
- Regulates *who* can perform specific *actions* on specific *resources*
- Ensures confidentiality and integrity

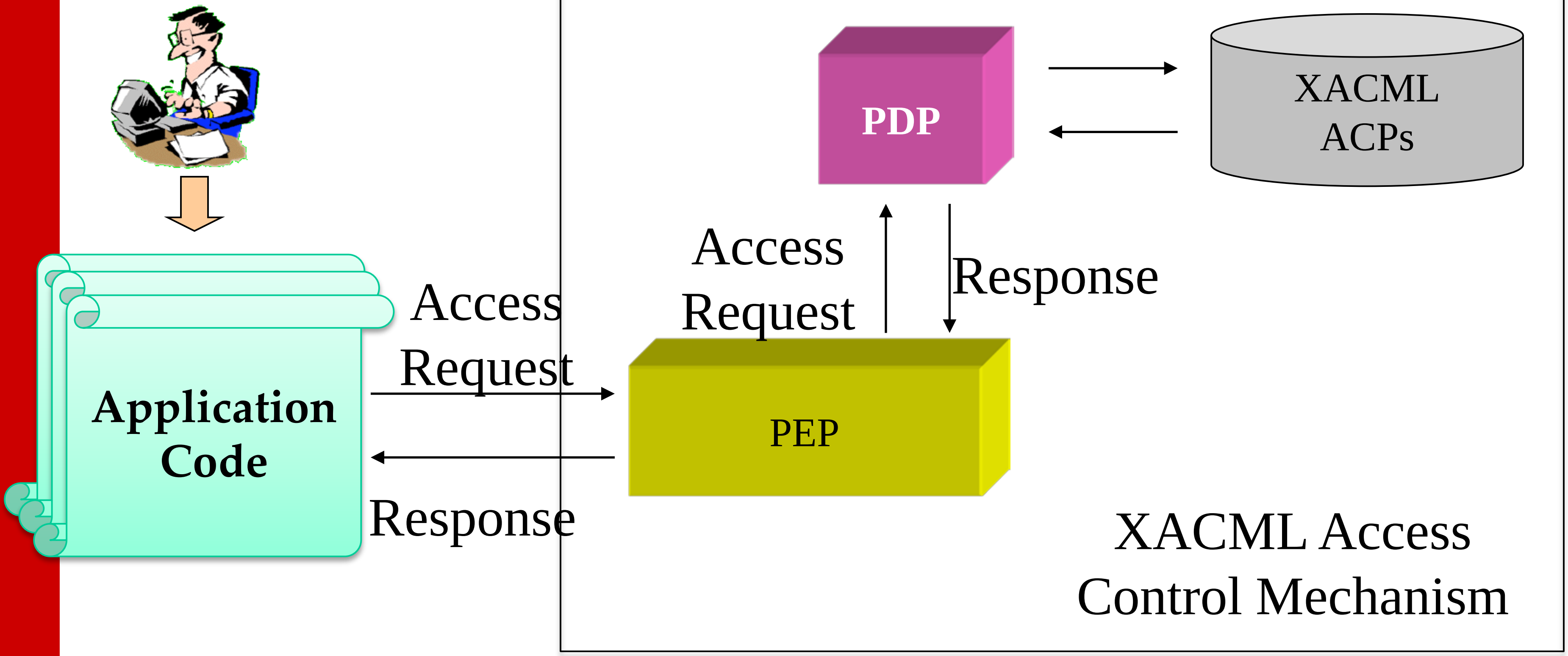
Security Objectives

Objective	Relation
Confidentiality	Allow and prohibit specific individuals and processes from reading specific data
Integrity	Prohibit improper modification
Availability	Ensured by limiting access to a system or parts of a system
Identification & Authentication	(self-defining)
Non-repudiation	Who originated (performed) an action?
Privacy	Limit who can see what data and for what purposes

Access Control Policy

- An access control policy is composed of a sequence of rules that specify under what conditions a user/actor can access specified resources.
- Describes a sequence of rules to decide whether access requests are allowed or denied
  - Policy …. Deals with subject, object, action

Access Control Mechanism



XACML: eXtensible Access Control Markup Language
PDP = Policy Decision Point
PEP = Policy Enforcement Point
ACP = Access Control Policy

Access Control Models

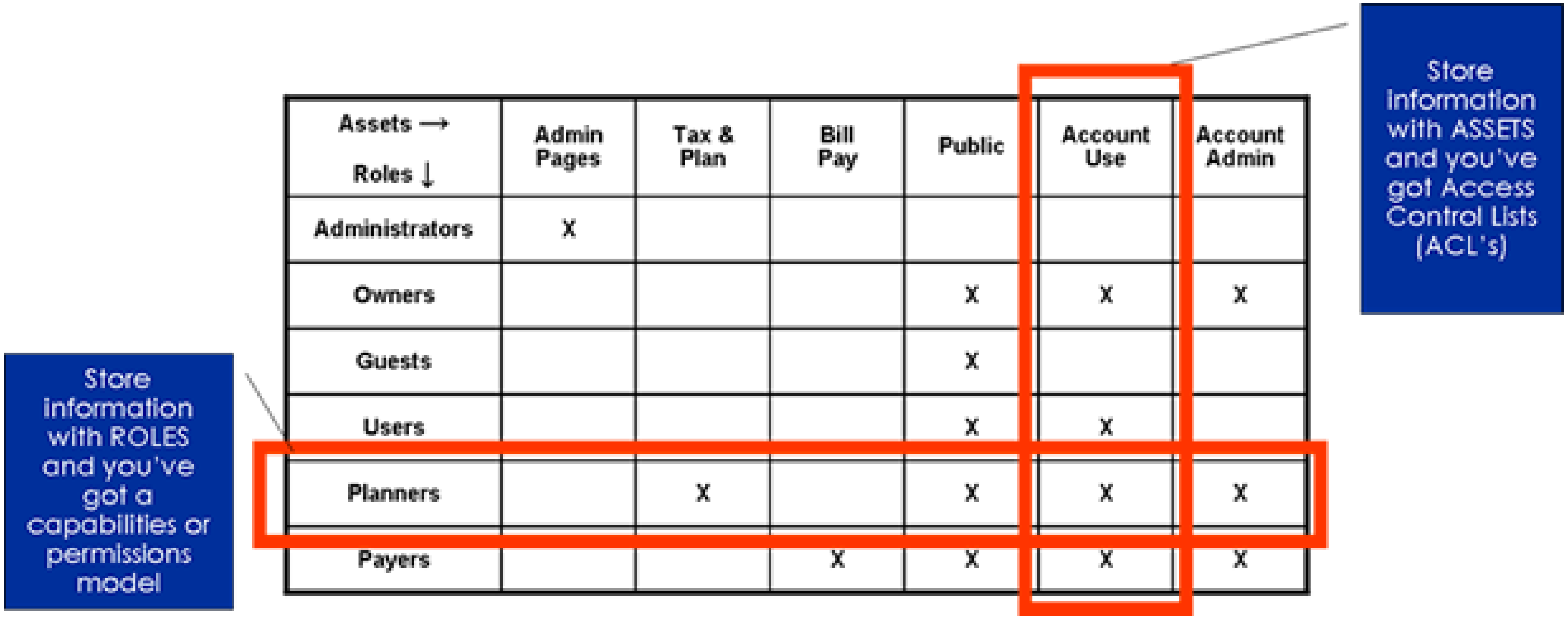
Most models contain rules with –

- Subject (actor)
- Resource (object)
- Action

“Clark-Wilson access control triple”

Often extended with various contexts (time, location, …)

Access Control Matrix



Assets → Roles ↓	Admin Pages	Tax & Plan	Bill Pay	Public	Account Use	Account Admin
Administrators	X					
Owners				X	X	X
Guests				X		
Users				X	X	
Planners		X		X	X	X
Payers			X	X	X	X

Store information with ROLES and you've got a capabilities or permissions model

Store information with ASSETS and you've got Access Control Lists (ACL's)

https://www.owasp.org/index.php/Access_Control_In_Your_J2EE_Application

Discretionary Access Control (DAC)

- Users to grant or revoke access, ownership, and delegation of rights to any of the objects under their control.
- Advantage: flexible
- Disadvantage: no control of information dissemination; complete trust of security policy administration given to user

http://csrc.nist.gov/groups/SNS/rbac/documents/design_implementation/Intro_role_based_access.htm

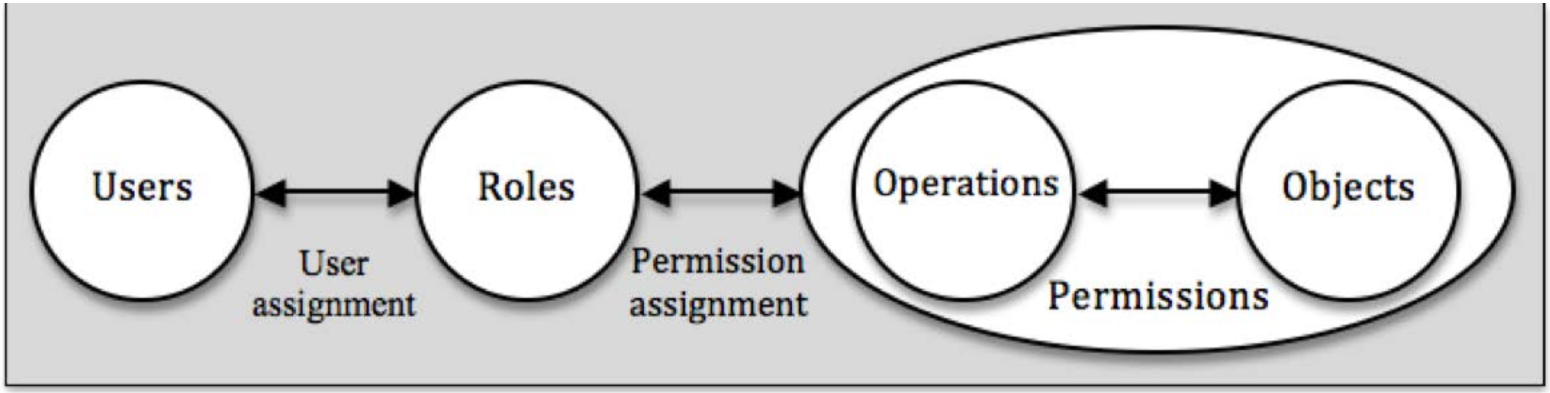
Mandatory Access Control (MAC)

- Restrict access to objects based on the sensitivity of the objects and the formal authorization (i.e. clearance) of subjects to access information of such sensitivity.
- Often used for highly sensitive government and military information
- Advantages:
  - Access to an object is based on the sensitivity of the object
  - Access based on need to know is strictly adhered to and scope creep has minimal possibility
  - Only an administrator can grant access
- Disadvantages:
  - Difficult and expensive to implement
  - Not agile

http://csrc.nist.gov/groups/SNS/rbac/documents/design_implementation/Intro_role_based_access.htm

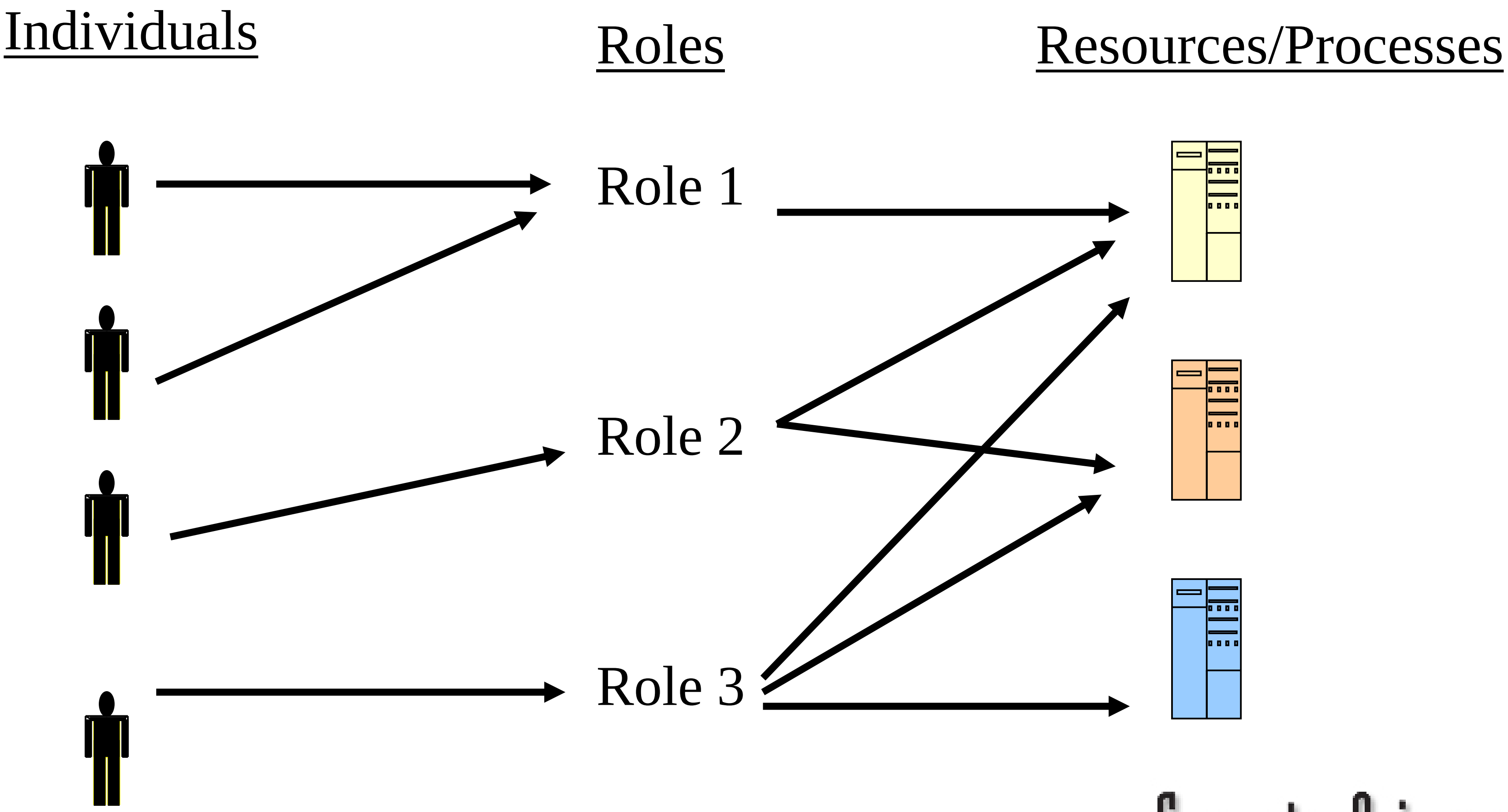
Role-Based Access Control (RBAC)

- Access to an object based on the assigned role.
- Roles are often defined based on job functions.
- Privileges are defined based on job authority and responsibilities within a job function. ("need to know")
- Operations on a resource are invocated based on the permissions associated with the privilege.
- The object is concerned with the user's role and not the user.



csrc.nist.gov/rbac/alvarez.ppt and http://courses.cs.ut.ee/2010/is/uploads/Main/RBAC-for-UML.pdf

Role-Based Access Control



Individuals

Roles

Resources/Processes

Role 1

Role 2

Role 3

User's change frequently, roles don't

From: csrc.nist.gov/rbac/alvarez.ppt

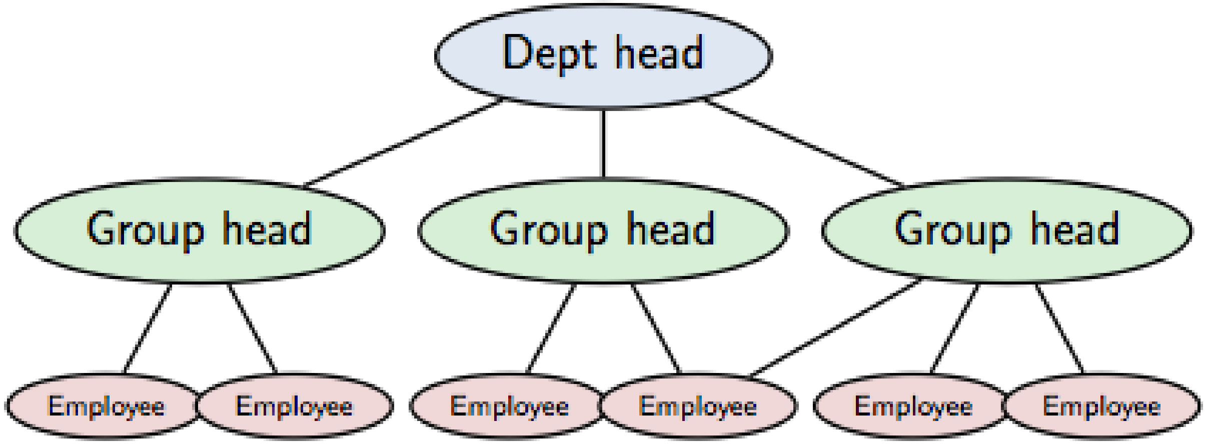
RBAC is Many-to-Many

- Users may be assigned many roles
- Roles may have many users assigned to them
- Roles may be assigned to many other roles
- Roles may be assigned many permissions
- Permissions may be assigned to many roles
- Permissions may be granted to perform many different types of operations on an object

www.sans.edu/resources/student_projects/200608_002.ppt

Hierarchies are possible … and can be complicated

- … and can be complicated
- … and can present conflicts



http://www.icg.isy.liu.se/courses/tsit02/lectures/cseclecture03.pdf

Principle of Least Privilege

- Roles are engineered based on the principle of least privilege.
- A role contains the minimum amount of permissions.
- A user is assigned to a role that allows him or her to perform only what's required for that role.
- No single role is given more permission than the same role for another user.

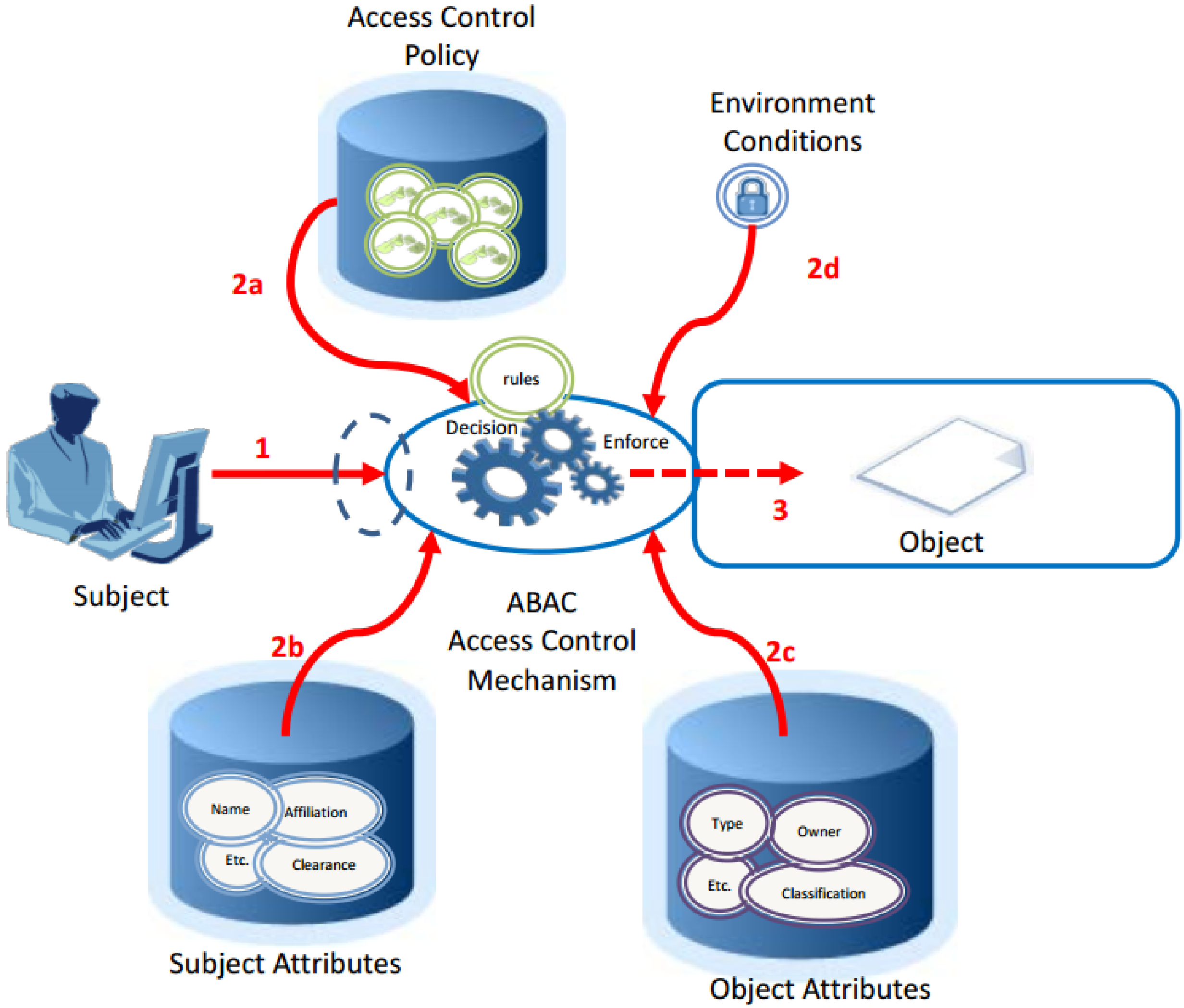
From: csrc.nist.gov/rbac/alvarez.ppt

Attribute Based Access Control

Controls access to objects by evaluating rules against the attributes of entities (subject and object), operations, and the environment relevant to a request

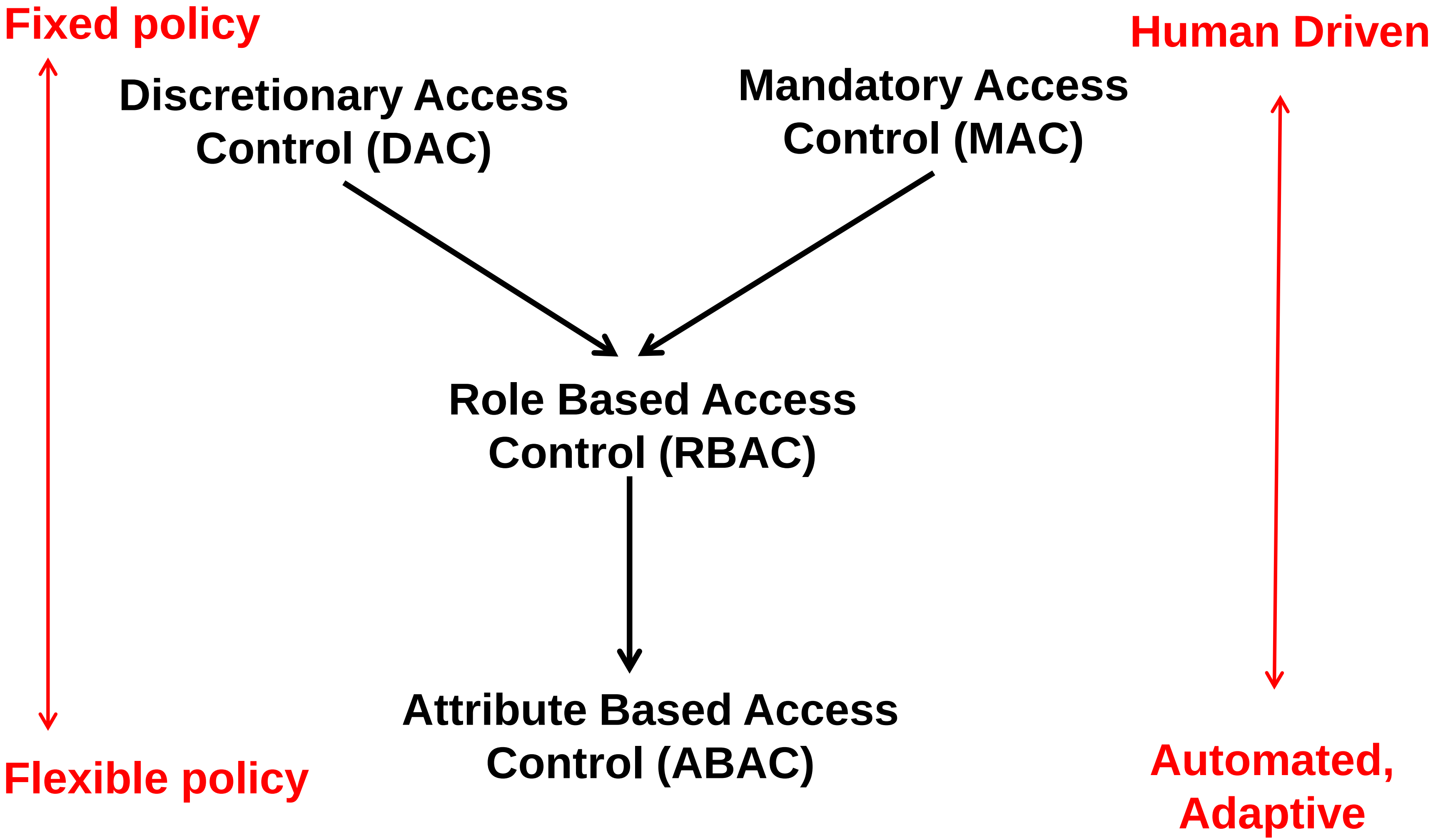
- Attributes are name:value pairs
  - possibly chained
  - values can be complex data structures
- Associated with users, subjects, objects, contexts
- Converted by policies into rights just in time

Attribute Based Access Control



1. Subject requests access to object
2. Access Control Mechanism evaluates a) Rules, b) Subject Attributes, c) Object Attributes, and d) Environment Conditions to compute a decision
3. Subject is given access to object if authorized

Access Control Genealogy



Fixed policy

Flexible policy

Discretionary Access Control (DAC)

Mandatory Access Control (MAC)

Role Based Access Control (RBAC)

Attribute Based Access Control (ABAC)

Human Driven

Automated, Adaptive

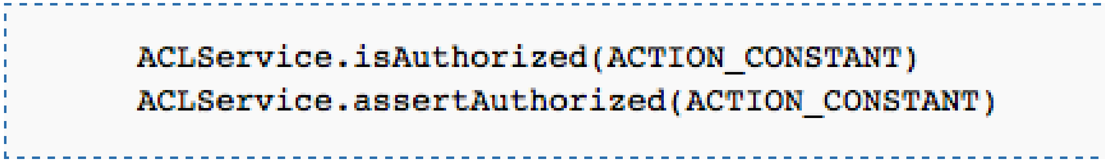
http://profsandhu.com/miscppt/pst_120716.pptx

Computer Science

NC STATE UNIVERSITY

Best Practices for Access Control

- Policies should be persisted and centralized
- Use a policy language (XACML)
- Have a centralized Access Controller



```
ACLService.isAuthorized(ACTION_CONSTANT)
ACLService.assertAuthorized(ACTION_CONSTANT)
```

- Controller manages conflicts, hierarchies, negative permissions
- Keep user identity in session
- Load entitlements server side from trusted source
- Force authorization checks on all requests
- Deny by default

https://www.owasp.org/index.php/Access_Control_Cheat_Sheet

Design Principles for Access Control

- Economy of mechanism: Keep the design as simple and small as possible.
- Fail safe defaults: Base access decisions on permission rather than exclusion (“no” by default)
- Complete mediation: Every access to every object must be checked for authority.
- Separation of privilege: When appropriate, use two keys to unlock privileges.
- Least privilege: Role contains the minimum amount of privileges; user is assigned to a role that allows him or her to perform only what’s required for that role.

Testing for Access Control

- Very few automated techniques useful
- Attempt to access administrative components or functions as an anonymous or regular user
  - Scour HTML source for "interesting" hidden form fields
  - Test web accessible directory structure for names like admin, administrator, manager, etc (i.e. attempt to directly browse to "restricted" areas)
- Determine how administrators are authenticated. Ensure that adequate authentication is used and enforced
- For each user role, ensure that only the appropriate pages or components are accessible for that role.
- Login as a low-level user, browse history for a higher level user's cache, load the page to see if the original authorization is passed to a previous session.

Overcoming the lack of state ….

SESSION MANAGEMENT

Session IDs

- Random
- Long (16 bytes +)
- No details exposed
  - Name
  - Content

Session Management

- Use built-in frameworks
- New sessions after any privilege change
- Never cross HTTP / HTTP**S**
- Cookies
  - Only sent over SSL (TLS)
  - HttpOnly attribute
  - SameSite attribute
- Session Expiration
  - Automatic
  - Manual