CSCI 455: Principles of Computer Security

Set 03:

Authentication.

Access Control.

Slide Sources

- Multiple sources including
  - Stallings & Brown textbook materials
    - Relevant parts of Chapters 3, 4
  - Other readings including NIST publications
  - My prior slides
  - Others

Authentication Process

- Authentication
  - Basis for access control and user accountability
- Definition of user authentication
  - "The process of verifying an identity claimed by or for a system entity" (RFC 4949)
- Two steps
  - Identification step
    - Presenting an identifier to security system
  - Verification step
    - Presenting or generating authentication information to corroborate binding between entity and identifier

Means of Authenticating User Identity

Aspect	Example
Something an individual knows	Password, PIN, answers to prior questions
Something an individual possesses (token)	Smartcard, electronic keycard, physical key
Something an individual is (static biometrics)	Fingerprint, retina, face
Something an individual does (dynamic biometrics)	Voice pattern, typing rhythm, handwriting

Risk Assessment for User Authentication

- Assurance level
  - Organization's degree of certainty that a user has presented a credential that refers to his or her identity
    - Degree of confidence in vetting process to establish individual identity
    - The degree of confidence that the individual who uses the credential is the individual to whom the credential was issued
  - 1 means little/no confidence, 2 means some confidence, 3 means confidence, and 4 means very high confidence
- Potential impact of security breach (FIPS 199)
  - Low: limited adverse effect, moderate: serious adverse effect, high: severe or catastrophic adverse effect
- Areas of risk
  - Identify and mitigate risk (later in Stallings, Chapter 14)

Password Authentication

- Widely used line of defense against intruders
  - User provides name/login and password
  - System compares password with the one stored for that specified login
- User ID
  - Checks if user is authorized to access system
  - Determines user's privileges
  - Used in discretionary access control
- Widely used password security technique
  - Hashed passwords and a salt value

Password Vulnerabilities

- Offline dictionary attack
- Specific account attack
- Popular password attack
- Password guessing against single user
- Workstation hijacking
- Exploiting user mistakes
- Exploiting multiple password use
- Electronic monitoring

Password Cracking

- Dictionary attacks
  - Keep a set of possible passwords & try each against password file
  - Each password must be hashed using each salt value and then compared to stored hash values
- Rainbow table attacks
  - Pre-compute tables of hash values for all salts
  - A mammoth table of hash values
  - Countered by a sufficiently large salt value and a hash length
- Password crackers exploit "people choose guessable passwords"
  - Shorter password lengths are also easier to crack
- John the Ripper
  - Open-source password cracker first developed in 1996
  - Uses a combination of brute-force and dictionary techniques

Modern Approaches

- Complex password policy
  - Forcing users to pick stronger passwords
- But password-cracking has also improved
  - Increased processing capacity for password cracking
  - Sophisticated algorithms to generate likely passwords
  - Studying examples and structures of actual passwords
- Alas …
  - GPUs now allow password-cracking programs to work thousands of times faster than just a decade ago
    - One AMD Radeon HD7970 GPU can try on average $8.2 * 10^9$ password combinations per second
    - In one study, over 10% of passwords were guessed in 1010 tries, and 40% within 1013 tries

Password File Access Control

- Can block offline guessing attacks by denying access to encrypted passwords
  - Make available only to privileged users
  - Shadow password file
- Vulnerabilities
  - Weakness in OS that allows access to the file
  - Accident with permissions making it readable
  - Users with same password on other systems
  - Access from backup media
  - Sniff passwords in network traffic

Password Selection Strategies

- User education
  - Users can be told or compelled to choose strong passwords
- Computer generated passwords
  - Users have trouble remembering them
- Reactive password checking
  - System periodically runs its own password cracker to find guessable passwords
- Complex password policy
  - Users allowed to select own passwords, but system checks if password is acceptable, otherwise rejects it
  - Allows guessable passwords to be eliminated while allowing users to select memorable passwords

Proactive Password Checking

- Rule enforcement
  - Specific rules that passwords must adhere to
- Password cracker
  - Compile a large dictionary of passwords not to use
- Bloom filter
  - Builds a table based on hash dictionary
  - Check desired password against this table

Memory Cards

- Can store but do not process data
  - Use of a magnetic stripe card
  - Can include an internal electronic memory
- Can be used alone for physical access
  - Hotel room, ATMs, many US credit cards
- Improves security with a PIN or password
- Drawbacks of memory cards
  - Requires a special reader
  - Loss of token
  - User dissatisfaction

Smart Tokens

- Physical characteristics
  - Include an embedded microprocessor
  - A smart token that looks like a bank card
  - Can look like calculators, keys, small portable objects
- Interface
  - Manual interfaces include a keypad and display for interaction
  - Electronic interfaces communicate with a compatible reader/ writer
- Authentication protocol (three categories)
  - Static
  - Dynamic password generator
  - Challenge-response
- Smart cards

Electronic Identity Cards (eID)

- Use of a smart card as a national identity card for citizens
  - Can support purposes where a national ID card or a driver's license
- Provides stronger proof of identity for a variety of apps
  - In effect, is a smart card that has been verified by the national government as valid and authentic
- Most advanced deployment is the German card neuer Personalausweis
  - Has human-readable data printed on its surface
    - Personal data
    - Document number
    - Card access number (CAN)
    - Machine readable zone (MRZ)

Biometric Authentication

- Attempts to authenticate an individual based on unique physical characteristics
- Based on pattern recognition
- Is technically complex and expensive when compared to passwords and tokens
- Physical characteristics used include
  - Facial characteristics, fingerprints, hand geometry, retinal pattern, iris, signature, voice

Remote User Authentication

- More complex to authenticate over a network, Internet, or a communications link
  - Additional security threats
    - Eavesdropping, password capture, replaying a previously observed authentication sequence
- Generally need to rely on some form of
  - Challenge-response protocol to counter threats

Authentication Security Issues

- Eavesdropping
  - Tries to learn password by an attack that involves physical proximity of user and adversary
- Host Attacks
  - Directed at user file at host containing passwords/tokens/ biometric templates
- Replay
  - Tries a previously captured user response
- Client Attacks
  - Tries user authentication without access to the remote host or the intervening communications path
- Trojan Horse
  - Masquerades as an authentic application or device for capturing a user password/ passcode/biometric
- Denial-of-Service
  - Attempts to disable a user authentication service by flooding the service with numerous authentication attempts

Access Control Principles

Computer security:

"Measures that implement and assure security services in a computer system, particularly those that assure access control service." (RFC 4949)

Authorization

- Subjects
  - Active entities such as users or processes
- Objects
  - Passive entities manipulated by a subject such as a records, relations, or files

Access Control

- Why
  - It helps to protect objects from unauthorized disclosure (confidentiality), and unauthorized modification (integrity)
- What
  - It is an approach to regulate access requests by subjects to objects to perform certain operations through a set of access policies
- How
  - Based on subject's identity, job function, or a set of identifiable attributes

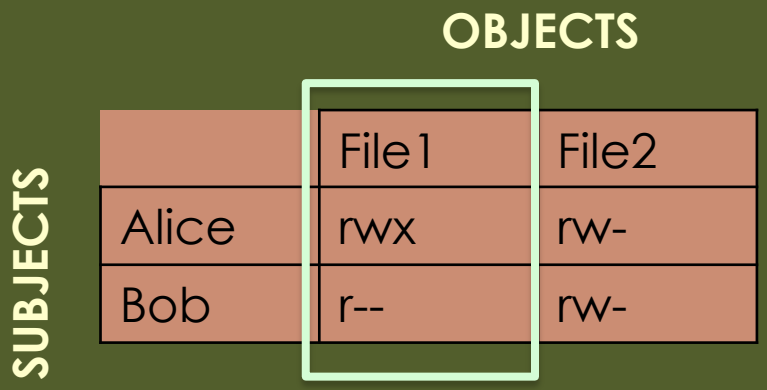
Authorization Management

- Granting and revoking access rights
- Centralized v. decentralized administration
  - Security officer v. locally autonomous systems
  - Hierarchical administration
    - Security officer > dept admin > local admin
- Ownership based
  - Owner of data may grant access to others to data (possibly with grant option)
- Cooperative authorization
  - Predefined groups of users or predefined number of users may access data

Access Control Policies

- Discretionary access control (DAC)
- Mandatory access control (MAC)
- Role-based access control (RBAC)
- Attribute-based access control (ABAC)
- Others
  - Context-based
  - Content-based
  - History-based

Access Control Matrix: ACLs



If a subject *s* requests to perform an operation *m* over *o*, the reference monitor checks if *m* is listed in M[s,o]:
Yes -> request is granted
No -> request is denied

- Access Control List (ACL)
  - Each object maintain a list of access rights of subjects

Access Control Matrix: Capabilities

OBJECTS

SUBJECTS

	File1	File2
Alice	rwx	rw-
Bob	r--	rw-

If a subject *s* requests to perform an operation *m* over *o*, the reference monitor checks if *m* is listed in M[s,o]:
Yes -> request is granted
No -> request is denied

- Capabilities List
  - Each subject has a list of capabilities for each object

Access Control Policies

- Discretionary access control (DAC)
  - Based on requestor identity and on access rules (authorizations) stating what requestors are (or are not) allowed to do
- Mandatory access control (MAC)
  - Based on comparing security labels with security clearances
- Role-based access control (RBAC)
  - Based on user roles within system and on rules stating what accesses are allowed to users in given roles
- Attribute-based access control (ABAC)
  - Based on user attributes, the resource to be accessed, and current environmental conditions

Subjects, Objects, Access Rights

- Subject
  - An entity capable of accessing objects
  - Three classes
    - Owner, Group, World
- Object
  - A resource to which access is controlled
  - Entity used to contain and/or receive data
- Access right
  - Describes how a subject may access an object
  - Could include:
    - Read, Write, Execute, Delete, Create, Search

Discretionary Access Control (DAC)

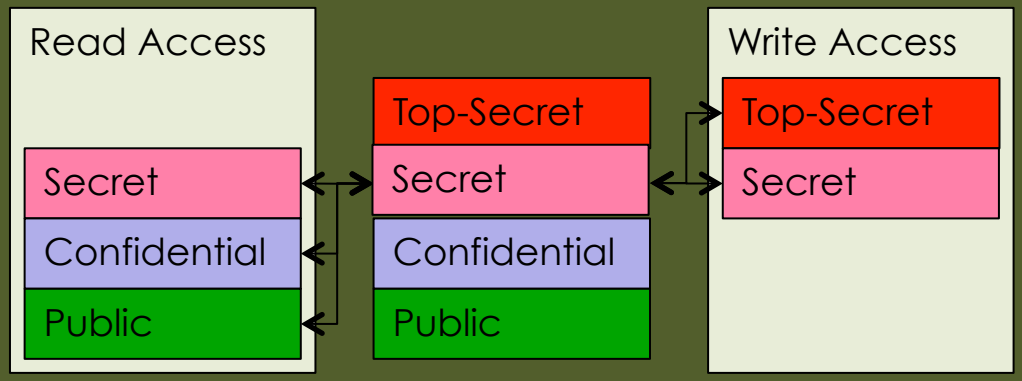
- Scheme in which an entity may enable another entity to access some resource
  - Often provided using an access matrix
    - One dimension consists of identified subjects that may attempt data access to resources
    - The other dimension lists objects that may be accessed
  - Each entry in matrix indicates access rights of a particular subject for a particular object

Traditional UNIX File Access Control

- "Set user ID"(SetUID), "Set group ID"(SetGID)
  - System temporarily uses rights of file owner/group in addition to real user's rights when making access control decisions
  - Enables privileged programs to access files/resources not generally accessible
- Sticky bit
  - When applied to a directory, it specifies only owner of a file in the directory can rename, move or delete that file
- Superuser
  - Is exempt from usual access control restrictions
  - Has system-wide access

Multilevel Security (MLS)

- Allows handling of multiple sensitivity levels
  - Public, Confidential, Secret, Top-Secret
- Permits simultaneous data access by users with different clearance levels and needs-to-know
- Prevents users from obtaining access to information for which they lack authorization



Mandatory Access Control Model

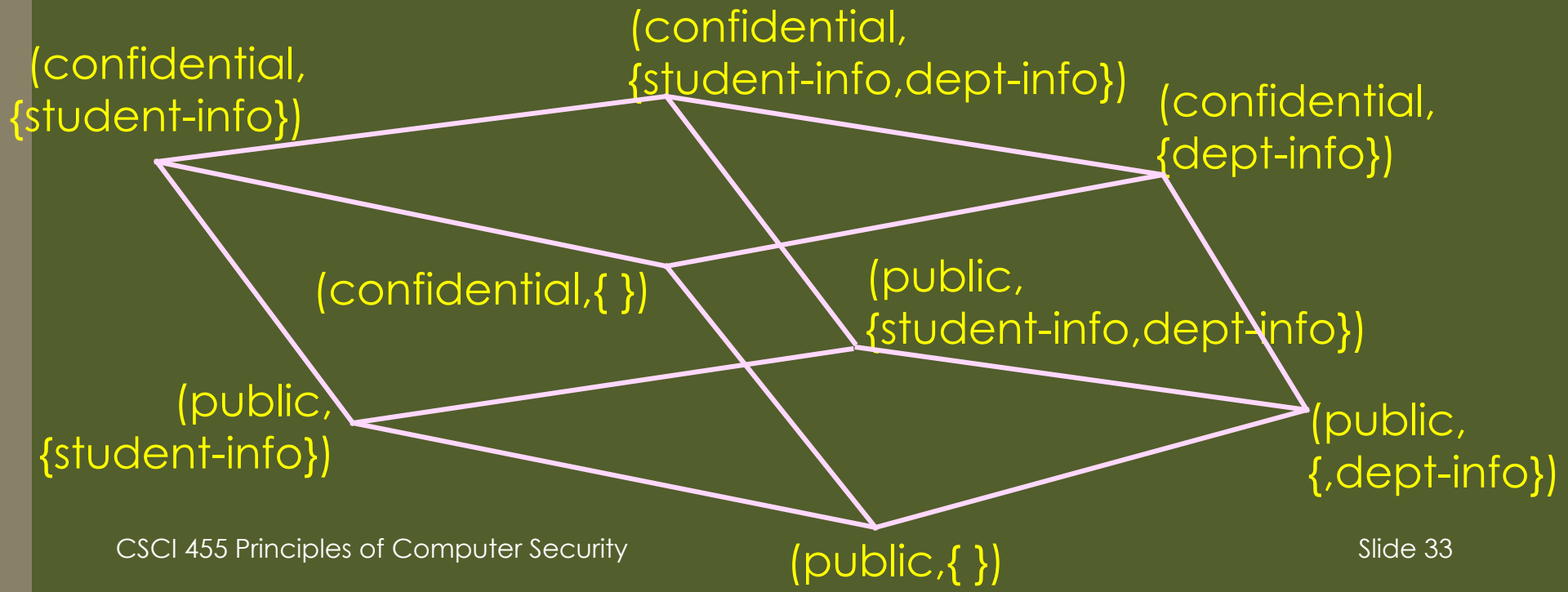
- Sometimes known as Non-Discretionary Model
- Works with Multi-level Security
- Labels
  - Subjects have labels called "clearance"
  - Objects have labels called "classification"
- Labels arranged in a lattice
- User access determination
  - Based on subject and object label comparison rules
    - No read up, no write down, and so on

MAC Example

- Security labels form a partially ordered set
  - label1=(confidential,{student-info})
  - label2=(public,{student-info})
  - label3=(public,{student-info,dept-info})
- Objects: security classification
  - grades=(confidential, {student-info})
- Subjects: security clearances
  - Pooh=(confidential, {student-info})
- Dominance: label l=(H,C) dominates l'=(H',C') iff H ≥ H' and C ⊆ C'
  - label1 dominates label2 because confidential ≥ public and {student-info} ⊆ {student-info}) BUT (confidential, {student-info}) DOES NOT dominates (public,{student-info,dept-info})

MAC Lattice

- Labels or security classes: (A, C)
  - A is the total order authority level
    - Confidential > public
  - C is the set of categories
    - {student-info, dept-info}



MAC: In a Nutshell

- Compare security classification of requested objects with security clearance of subject
  - Subject can read object only if label(subject) dominates label(object)
- Access permitted if access rules are satisfied
  - Pooh wants to read grades
    - label(Pooh)=(confidential,{student-info})
    - label(grades)=(confidential,{student-info})
  - Pooh permitted to read grades

Comparison	Access
If subject label and object label cannot be compared	NOT allowed
If labels can be compared	Based on rules re. relationship between labels

MAC Models

- Object-subject classification
  - Bell-La Padula, 1973 (major milestone)
    - Still dominates MAC implementations
  - Biba, 1977
  - Dion, 1981
- Information flow system
  - Denning, 1976
- Polyinstantiation (see Abrams Essays)
  - MULTICS: Hinke and Schaefer, 1975
  - Sea View: Denning, et al. 1986
  - Sandhu and Jajodia, 1991

MLS Models

- Bell-LaPadula
  - Designed to protect confidentiality
  - TS, Secret, Confidential, Public
  - No Read Up, No Write Down
  - Trusted subject allowed to violate insert, update, delete MACs
- Biba
  - Designed to protect integrity
  - Top Secret, Secret, Confidential, Public
  - No Read Down, No Write Up
  - Trusted subject allowed to violate insert, update, delete MACs

Bell-La Padula (BLP) Model

- Confidentiality protection
- Lattice-based access control
  - Subjects, objects, and security labels
- Supports decentralized administration
- Captures military classification
- Uses finite state machine
- Formally define a state to be secure, then consider transitions (that maintain security)

BLP Model

- Based on the subject-object paradigm
  - Subjects are active elements that can execute actions
  - Objects are passive elements that can contain information
- 4 access modes for subjects on objects
  - Read-only or read
  - Append (writing without reading)
  - Execute (executes an object /program)
  - Read-write or write

BLP Levels

- Classification levels
  - For subjects/programs and objects/resources
    - 1 Top secret
    - 2 Secret
    - 3 Confidential
    - 4 Unclassified
- Security levels
  - L1 = (C1, S1), L2 = (C2, S2),
    - Where S1 and S2 are categories
  - L1 is higher or equal to L2 iff C1 > C2 AND S1 $\subseteq$ S2

BLP Operations

- Get access
  - Initiate access to object in given mode
- Release access
  - End access previously started by get
- Give access
  - Grant access mode on an object to a subject
- Rescind access
  - Revoke access granted with "give"
- Create object
  - Takes an inactive object and adds to object hierarchy
    - Note: an object may be inactive or active
- Delete object
  - Deactivates an active object
- Change subject security level
- Change object security level

BLP Reference Monitor

- All accesses are controlled by the reference monitor
  - Cannot be bypassed
- Access is allowed if and only if
  - Resulting system state satisfies all security properties
- Trusted subjects
  - Subjects trusted not to compromise security

BLP Axioms (or Properties)

Simple security property

- A subject s is allowed to read object o only if s's security label dominates o's security label
  - (b,M,f,H) satisfies this property iff for every read in M[s,o], f(s) ≥ f(o), where ≥ is the dominance relation
  - No read up
  - Applies to all subjects

A subject can only read objects at or below its level

*-property

- A subject s is allowed to write object o only if o's security label dominates s's security label
  - (b,M,f,H) satisfies the *-property iff for every write in M[s,o], f(o) ≥ f(s), where ≥ is the dominance relation
  - No write down
  - Applies to untrusted subjects only

A subject can only write objects at or above its level

BLP: Discretionary Property

- ds-property
  - Every current access must be present in access matrix
    - A subject can exercise only accesses for which it has the necessary authorization
  - A system state satisfies discretionary property if and only if for all subjects s, objects o, and access mode m
    - $\langle s, o, m \rangle \in b \Rightarrow \; m \in M[s,o]$

Tranquility and Changing of Security Labels

- Tranquility principle
  - Subjects can't change active objects' levels
  - Not atomic, i.e., read and write sequences that may or may not be interrupted

Strong tranquillity	Weak tranquillity
When security labels of never change during an operation, usually over system lifetime	When security labels never change in violation of security policy
State always satisfies security requirements, but this approach is inflexible	High watermark for a subject is during reads when it may upgrade its security clearance, and for an object is during writes when its classification may be upgraded

BLP: Issues With Trusted Subjects

- Are trusted subjects needed?
  - Strict enforcement of *-property impractical
  - User may need to extract an UNCLASSIFIED paragraph from a CONFIDENTIAL document
  - User creates a TOP SECRET message, then decides that the message should be SECRET
- Subjects trusted not to compromise security
  - Does this violate *-property?
- Makes security policy difficult to understand
- Does user confirmation of security-relevant operations to prevent security violations hold?

BLP: Lessons

- Axioms may be overly restrictive
- Trusted subjects are not sufficiently restrictive
- Using axioms and trusted subjects together complicates security policy being enforced

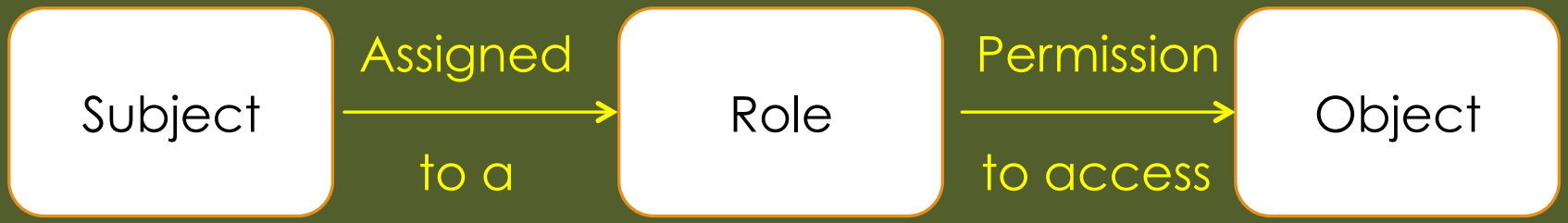
- Carl Landwehr
  - Problem isn't in what BLP allows but what it doesn't
  - Many secure operations are disallowed by BLP so systems face a choice
    - Obey BLP but impose severe functionality constraints, OR
    - Rely heavily on trusted processes for desired functions

Role-Based and Attribute-Based Access Control

RBAC and ABAC

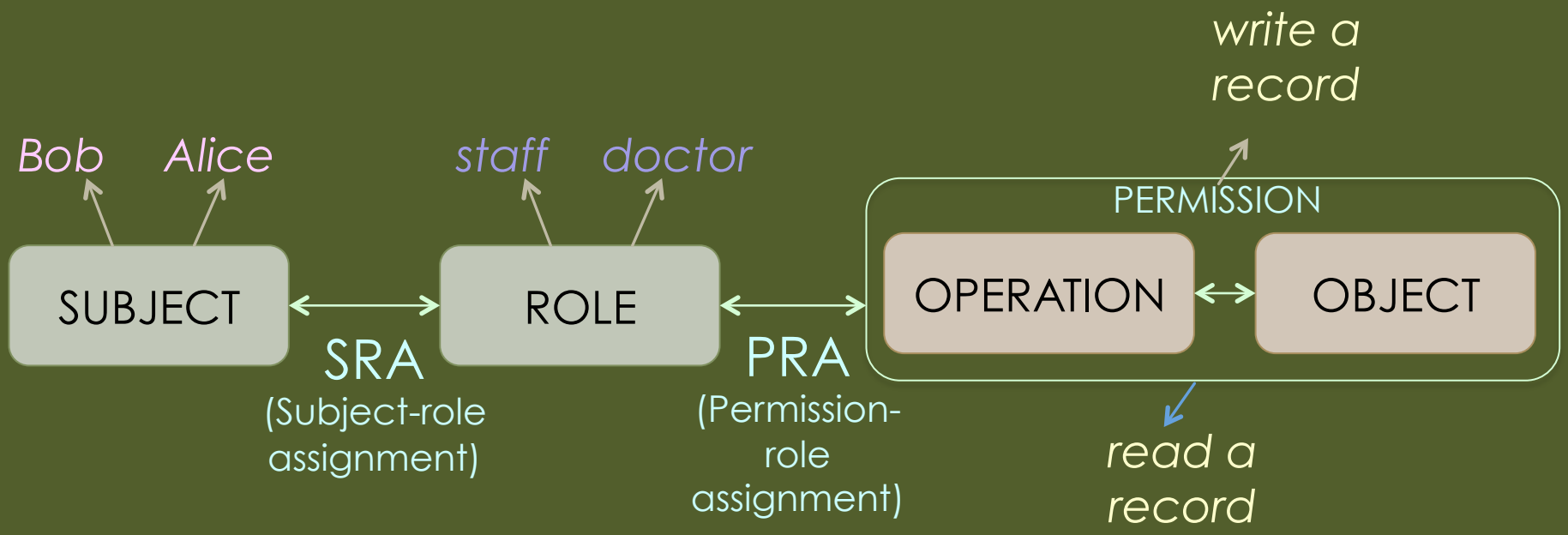
RBAC Overview

- A subject has access to an object based on assigned role
- Roles typically defined based on job functions
- Permissions defined based on job authority and responsibilities within a job function
- Operations on an object invoked based on permissions
- Object access depends on subject's role, not the subject



From Suhair Alshehri

Role-Based Access Control (RBAC)



Bob	doctor
Alice	nurse

doctor	write a record read a record
nurse	read a record
staff	read a record

Complex initial role structuring and lack of granularity and flexibility

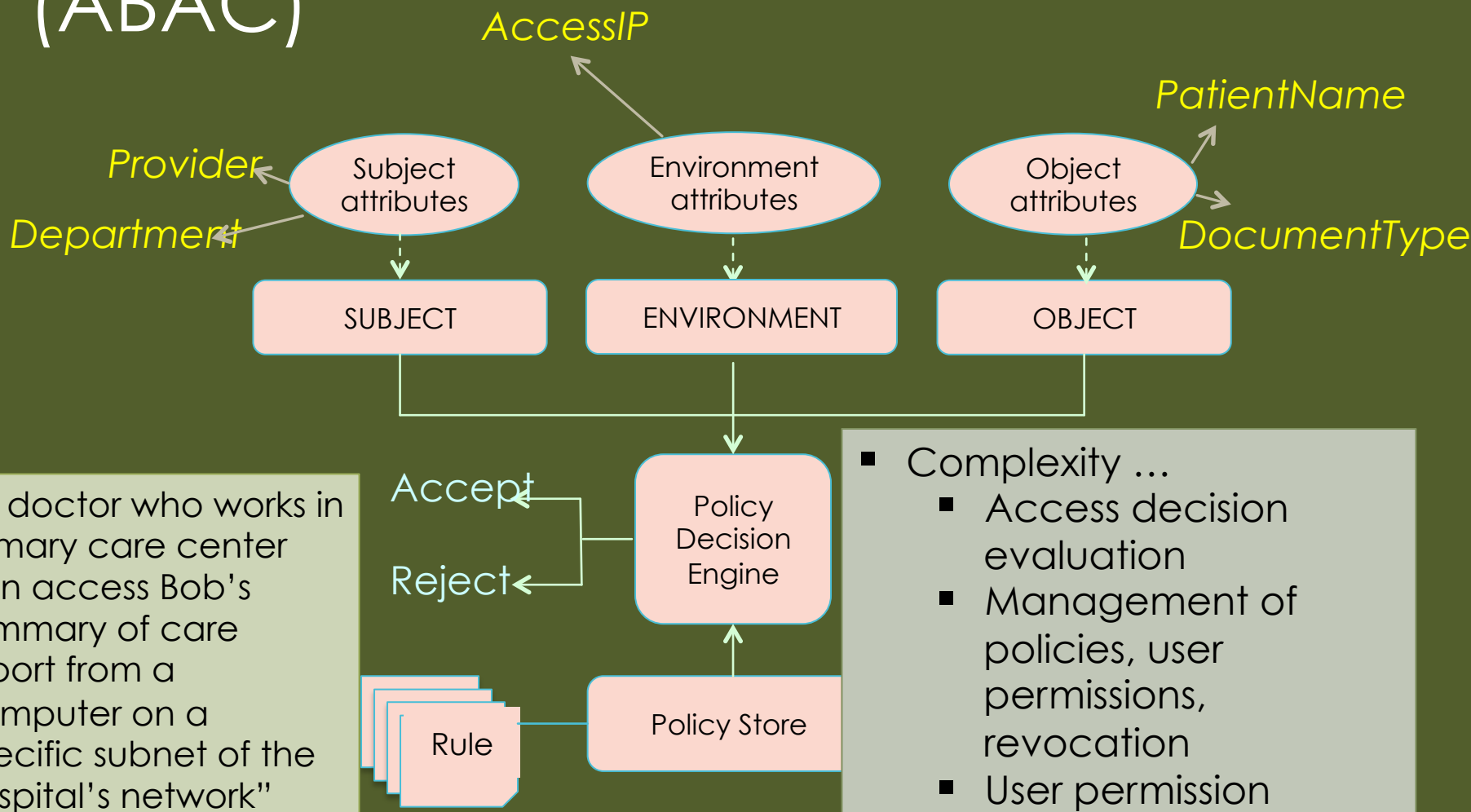
Attribute-Based Access Control (ABAC)

- Can define authorizations that express conditions on properties of both the resource and the subject
- Strength is its flexibility and expressive power
- Main obstacle to its adoption in real systems
  - Performance impact concerns evaluating predicates on both resource and user properties for each access
- Web services have been pioneering technologies through introduction of the
  - eXtensible Access Control Markup Language (XAMCL)
- Considerable interest in applying model to cloud services

ABAC Model: Attributes

- Subject attributes
  - A subject is an active entity that causes information to flow among objects or changes the system state
  - Attributes define identity and characteristics of subject
- Object attributes
  - An object (or resource) is a passive information system-related entity containing or receiving information
  - Objects have attributes that can be leverages to make access control decisions
- Environment attributes
  - Describe operational, technical, situational environment or context in which information access occurs
  - Largely ignored in most access control policies

Attribute-Based Access Control (ABAC)



"A doctor who works in Primary care center can access Bob's summary of care report from a computer on a specific subnet of the hospital's network"

- Complexity …
  - Access decision evaluation
  - Management of policies, user permissions, revocation
  - User permission review
- Potential privacy issues.

ABAC

- Distinguishable as it controls access to objects by evaluating rules against attributes of entities, operations, and environment relevant to a request
- Relies upon the evaluation of attributes of the subject, attributes of the object, and a formal relationship or access control rule defining the allowable operations for subject-object attribute combinations in a given environment
- Systems are capable of enforcing DAC, RBAC, and MAC concepts
- Allows an unlimited number of attributes to be combined to satisfy any access control rule

RBAC versus ABAC

RBAC

- Static
- Coarse-grained
- Access decisions made in advance
- Simple policy and permission modifiability, revocability, and user permission reviewability
- Complex setup

ABAC

- Dynamic
- Fine-grained
- Access decisions made at run-time
- Complex policy and permission modifiability, revocability, and user permission reviewability
- Simple setup