Access Control Methodologies

Chapter 2

Lecturer: Pei-yih Ting

Overview

- Basic Principles
- Controls
- Access Control Designs
- Access Control Administration
- Accountability
- Access Control Models
- Identification and Authentication Methods
- Single Sign-On Systems
- File and Data Ownership
- Attacks

Basics of Access Control

- Access control is a collection of methods and components
  - Supports confidentiality (protects information from unauthorized disclosure)
  - Supports integrity (protects information from unauthorized modification)
- Goal: to allow only authorized subjects to access permitted objects

Access Control Basics (cont'd)

- Subject
  - The entity that requests access to a resource
  - Active
- Object
  - The resource a subject attempts to access
  - Passive

How do we partition subjects / objects for efficient management?

Access Control Basics (cont'd)

- Least secure philosophy (permissive policy)
  - Any object access not prohibited is granted by default.
  - Ineffective maintenance leads to authorization creep
- Least privilege philosophy (prohibitive policy)
  - A subject is granted permissions needed to accomplish required tasks and nothing more

Controls

- Mechanisms put into place to allow or disallow object access
  - Any potential barrier to unauthorized access
  - Locks, guards, passwords…
- Controls organized into different categories
- Common categories
  - Administrative (enforce security rules through policies, ex. procedures, usage monitoring, security training)
  - Logical/Technical (implement object access restrictions, ex. identification / authentication / segregated network)
  - Physical (limit physical access to hardware)

Access Control Techniques

- Choose techniques that fit the organization's needs
- Considerations include
  - Level of security required
  - Environmental impact of security measures
  - User convenience
- Techniques differ in
  - The way objects and subjects are identified
  - How decisions are made to approve or deny access

Access Control Designs

- Access control designs define rules for users accessing files or devices
- Three common access control designs
  - Mandatory access control (MAC)
  - Discretionary access control (DAC)
  - Non-discretionary access control

Mandatory Access Control

- A unified (mandatory) way to assign a security label to each subject and object in a system.
- Matches label of subject to label of object to determine when access should be granted
- A common implementation is rule-based access control
  - Often requires a subject to have a need to know in addition to proper security clearance
  - Need to know indicates that a subject requires access to object to complete a particular task
  - Example rule:

    subject's security clearance > object's security label

MAC (cont'd)

- Common military data classifications
  - Unclassified
  - Sensitive but Unclassified (SBU)
  - Confidential
  - Secret
  - Top Secret
- Common commercial data classifications
  - Public
  - Sensitive
  - Private
  - Confidential

Discretionary Access Control

- Access to an object is defined by the object owner.
- Uses identity of subject to decide when to grant an access request
- Most common design in commercial operating systems
  - Generally less secure than mandatory control
  - Generally easier to implement and more flexible
- Includes
  - Identity-based access control: ex. UNIX file permission
  - Access control lists (ACLs): ex. WINNT

    allows group of objects / subjects to be controlled together

Non-discretionary Access Control

- Uses a subject's role or a task assigned to subject to grant or deny object access
  - Also called role-based or task-based access control
- Works well in environments with high turnover of subjects since access is not tied directly to subject
- Lattice-based control is a variation of non-discretionary control
  - Relationship between subject and object has a set of access boundaries that define rules and conditions for access

Access Control Administration

- Can be implemented as centralized, decentralized, or hybrid
- Centralized access control administration
  - All requests go through a central authority
  - Administration is relatively simple
  - Single point of failure, sometimes performance bottlenecks
  - Common packages include Remote Authentication Dial-In User Service (RADIUS), Challenge Handshake Authentication Protocol (CHAP), Terminal Access Controller Access Control System (TACACS)

Access Control Administration (cont'd)

- Decentralized access control administration
  - Object access is controlled locally rather than centrally
  - More difficult administration
    - Objects may need to be secured at multiple locations
  - More stable and robust
    - Not a single point of failure
  - Usually implemented using security domains

A security domain is a *sphere of trust*, including a collection of subjects and objects with defined access rules or permissions

Accountability

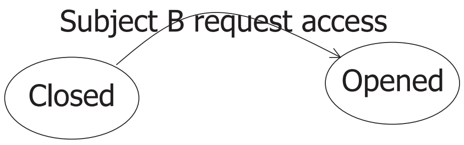
- System auditing used by administrators to monitor
  - Who is using the system
  - What users are doing
- Logs can trace events back to originating users
- Process of auditing can have a negative effect on system performance
  - Must limit data collected in logs
  - Clipping levels set thresholds for when to start collecting data

Access Control Models

- Provide conceptual view of security policies
- Map goals and directives to specific system events
- Provide a formal definition and specification of required security controls
- Usually many different models and combinations of models are used in a secure system

State Machine Model

- A collection of defined states and transitions
- Modifications change objects from one state to another
- A state represents the characteristics of an object at a point in time
- Transitions represent the modifications that can be made to objects to change from one state to another
- Ex.



A particular Object A

State Machine Model (cont’d)

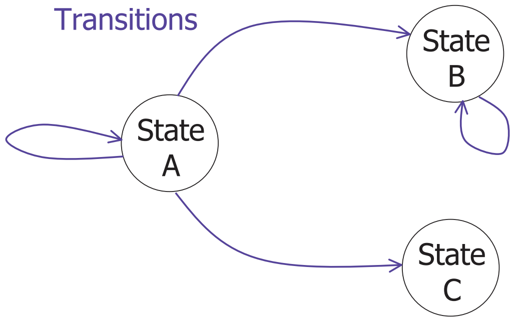


Figure 2.1 Simple state machine

Bell-LaPadula Model

- 1970s by US military
- Focus on confidentiality
- A state machine model that uses *security labels*

1. Top Secret
2. Secret
3. Confidential
4. Sensitive but Unclassified
5. Unclassified

- Each object is given a security level and each subject is given a security clearance
- Two basic properties to *evaluate access requests*
  - Simple security rule: no read up
  - *-property: no write down

Biba Model

- After Bell-LaPadula
- Focuses on integrity controls
- A state machine model that uses *integrity labels*
- Each object or subject is given an integrity level
- Two basic properties to *evaluate access requests*
  - Simple integrity property: no read down
  - *-property: no write up
- Popular with businesses because its main focus is to ensure that unauthorized subjects cannot change objects

Clark-Wilson Model

- Developed after the Biba model
- Not a state machine model
- Restricts all accesses to a small number of tightly controlled access programs
  - Integrity verification procedure (IVP): verifies the integrity of a data item
  - Transformation procedure (TP): makes authorized changes to a data item
  - After subject is properly authenticated and cleared to access the object, all modifications are first validated by the IVP, and then the modification takes place by the TP.
- Works well in commercial applications

Non-interference Model

- Often an addition to other models
- Ensures that changes at one security level do not bleed over into other levels
- Maintains both data integrity and confidentiality

Identification and Authentication Methods

- Two-factor authentication uses two phases
  - *Identification* : a subject claims to be a specific entity by presenting identifying credentials
  - *Authentication* : verifies that the subject really is who she claims to be
- Usually there will be an *authorization* phase followed by successful authentication where system evaluates the specific rights or permissions for the subject

Identification and Authentication Methods (cont'd)

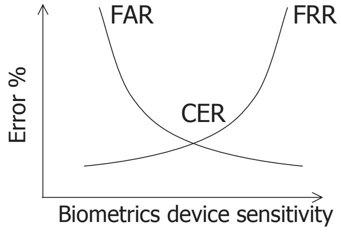
- Security practices often require input from multiple categories of authentication techniques
  - What you know:
    - Password, passphrase, PIN, lock combination
  - What you have:
    - Smartcard, token device
  - What you are: Biometrics
    - fingerprint, palm print, hand geometry, retina / iris pattern, voice pattern, signature, keyboard dynamics

Identification and Authentication Methods (cont’d)

- Strong password policy
  - At least six characters in length
  - Contain at least one number or punctuation characters
  - Do not use dictionary words or combinations of dictionary words
  - Do not use common personal data, such as birth date, social security number, family member or pet name, or favorite song or hobby
  - Never write down your password or send it as clear text
  - Do not use key mapping of MBCS input methods (Chang-Jie, Da-I, Ju-In, BoShaMe, …)
- Try to make your password easy to remember but hard to guess

Identification and Authentication Methods (cont’d)

- Biometrics: detection and classification of a subject’s physical attributes
  - most complex authentication mechanism
  - most difficult to fake
  - most expensive to implement
  - most difficult to maintain
- Imperfect nature of biometrics analysis
  - False rejection rate (FRR)
  - False acceptance rate (FAR)
  - Corssover error rate (CER)



Single Sign-On

- Used to avoid multiple logins
- Once a subject is positively identified, authentication information can be used within a trusted group
- Great for users in a LAN environment since they can sign on once and use multiple resources
- Requires additional works for administrators
- Several good SSO systems in use, Kerberos is one example

Kerberos

- Uses symmetric key cryptography for messages
- Provides end-to-end security through authentication and key exchange protocol
  - Intermediate machines between the source and target cannot read contents of messages
- Used in distributed environments but implemented with centralized servers
- Includes an authentication server and a ticket-granting server
- Weaknesses include
  - Single point of failure, performance bottleneck
  - Session key lives on client machines for a small amount of time, can be stolen

File and Data Ownership

- Different layers of responsibility for ensuring security of organization's information
- Data owner
  - Bears ultimate responsibility, sets classification levels, delegate day-to-day responsibility of maintenance to the data custodian
- Data custodian
  - Enforces security policies, often a member of IT department. Maintains appropriate controls, taking backups, and validating the integrity of the data
- Data user
  - Accesses data on a day-to-day basis, responsible for following the organization's security policies

Related Attacks

- Brute force attack
  - Try all possible combinations of characters to satisfy Type 1 authentication (password guessing)
  - War dialing
- Dictionary attack
  - Subset of brute force attack
  - Instead of all possible combinations, try common passwords from a list, or a dictionary
- Spoofing attack
  - Create fake login program, prompt for User ID, password
  - Return login failure message, store captured information
- Social engineering attack

Summary

- Use access control to ensure that only authorized users can view/modify information
- Access control designs define rules for accessing objects
  - Mandatory, discretionary, non-discretionary
- Access control administration defines the mechanisms for access control implementation
  - Centralized, decentralized, hybrid
- Administrators use system logs to monitor access

Summary (cont'd)

- Access control models
  - Provide a conceptual view of security policies
  - One common example is the state machine model
- Identification and authentication methods
  - Used to identify and validate a user
  - Include passwords, smart cards, and biometrics
  - Single sign-on systems allow trusted groups to share authenticators and authorizations (e.g., Kerberos)

Summary (cont’d)

- Responsibility for information access is shared
  - Data owners, custodians, users
- Attack types related to access controls include
  - Brute force attacks, dictionary attacks, login spoofing

Assignments

- Reading: Chapter 2
- Practice 2.11 Challenge Questions

- Next week, turn in Challenge Exercise 2.3 and the following question
- Write down an access control policy for protecting personnel records in a business. Should employees be able to access their own records? Other people’s records? Should managers be able to access all records? Come up with a consistent policy. Try to build a state machine model to describe this policy.