CIT 270: SYSTEMS SECURITY I

CHAPTER 12: ACCESS MANAGEMENT

BYU
IDAHO

INTRODUCTION

Remember this presentation does not replace your reading and only covers at best 70% of the chapter material.

Note 📎

Keep any eye out for boxes like this one in your chapter readings. These are note boxes that highlight important information. Your chapter quiz will often have questions that refer directly to one of these.

In this presentation pay special attention to yellow words. These highlighted words denote a topic that will almost always be on your chapter quiz.

WHAT IS ACCESS CONTROL

Access control is the granting or denying approval to use specific resources or in simple terms: controlling access.

Identification: credentials that uniquely identify someone such as a user name on a computer system.

Authorization: granting permission to take an action.

Accounting: a record that is preserved of who accessed the network, what resources they used, and when they disconnected.

BYU IDAHO

WHAT IS ACCESS CONTROL

Basic steps in access control:

Action	Description	Scenario Example	Computer Process
Identification	Review of credentials	Delivery person showing their employee badge	User enter user name
Authentication	Validate credentials as genuine	Gabe reads a badge to determine its real	User provides password
Authorization	Permission granted for admittance	Gabe opens door to allow delivery person in	User authorized to log in
Access	Right given to access specific resources	Delivery person can only retrieve box by door	User allowed to access only specific data
Accounting	Record of user actions	Gabe signs to confirm the package was picked up	Information recorded in a log file.

WHAT IS ACCESS CONTROL

Roles in access control:

Role	**Description**	**Duties**	**Example**
Privacy officer	Manager who oversees data privacy compliance and manages data risk	Ensures enterprise complies with data privacy laws and its own privacy policies	Decides that users can have permission to Salary.xlsx
Custodian / Steward	Individual to whom day-to-day actions have been assigned by the owner	Periodically reviews security settings & maintains records of access by end users	Sets and reviews security settings on Salary.xlsx
Owner	Person responsible for the information	Determines level of security needed for data and delegates security duties as required	Determines that Salary.xlsx can be read only by managers
End User	User who accesses information in the course of routine job responsibilities	Follows organization's security guidelines & does not attempt to circumvent security	Opens Salary.xlsx

ACCESS CONTROL MODELS

Access Control Model: hardware and software that has a predefined framework that the custodian can use for controlling access. Using the appropriate model allows the custodian to configure the necessary level of control for users.

Discretionary Access Control (DAC): least restrictive model where every object has an owner who has total control over that object.

Mandatory Access Control: most restrictive model where users are assigned privileges (access) strictly by the custodians discretion.

- lattice implementation where users receive a rung.
- Bell-LaPadula (BLP) similar to a lattice but with restrictions on object creation and alteration on lower lattice levels.

ACCESS CONTROL MODELS

Role-based Access Control (RBAC): aka. Non-discretionary Access Control is considered *real-world* access because it is based on a users job function within an organization; roles.

Rule-based Access Control (RB-RBAC): aka. Rule-based Role-based Access Control or automated provisioning based on rules established by the custodian or system administrator; each object contains rules.

Attribute-based Access Control: uses more flexible policies that can combine attributes instead of relying on rigid predefined rules; If-Then-Else structure.

ACCESS CONTROL MODELS

Access Control Models overview:

Access Control Models
CompTIA Security+
SY0-501 - 4.3

MANAGING ACCESS THROUGH ACCOUNT MANAGEMENT

Employee Onboarding: the tasks associated with hiring a new employee like setting up their accounts which could include creating location-based policies, creating time-of-day restrictions, and enforcing least privilege.

Employee Offboarding: actions to be taken when an employee leaves the enterprise; plans for unplanned offboarding.

Location-based Policies: establishing geographical boundaries where a mobile device can and cannot be used; geofencing or IP location.

Standard Naming Convention: rules created by your organization that determine a standard convention to use when naming accounts and/ or files.

MANAGING ACCESS THROUGH ACCOUNT MANAGEMENT

Time-of-Day Restrictions: time based restrictions that can limit when a user can login or have access to resources.

Least Privilege: limiting and controlling access to buildings, rooms, devices, and physical or digital resources. Only the minimum amount of privileges necessary to perform a job or function should be allocated.

ACCOUNT AUDITING

Recertification: the process of periodically revalidating a user’s account, access control, and membership role or inclusion in a specific group.

Permission Auditing and Review: examine the permissions that a user has been given to determine if each is still necessary.

Usage Auditing and Review: an auditing process that looks at the applications that the user is provided, how frequently they are used, and how they are being used.

BEST PRACTICES FOR ACCESS CONTROL

Separation of Duties: if the fraudulent application of a business process could result in a security breach then two or more individuals must carry out the duties instead of a single individual.

Job Rotation: instead of one person having sole responsibility of a business function for a long period of time, employees are rotated through job positions ensuring only limited control over business functions; reduces burnout.

Mandatory Vacations: countermeasure that seeks to counter fraud that could occur because a rogue employee is always in a position to cover their tracks.

BEST PRACTICES FOR ACCESS CONTROL

Clean Desk Policy: a policy designed to ensure all confidential or sensitive materials are removed from the users workspace and secured when not in use:

- file cabinets closed and locked
- laptop locked in desk drawer
- external storage devices locked in drawer
- shred all paper documents
- printer print outs removed immediately
- whiteboards cleaned and left empty

IMPLEMENTING ACCESS CONTROL

File System Security: security like Access Control Lists (ACLs) that protect files managed by the OS.

Database Security: security used to protect databases; can be ACLs that protect the database file itself.

Group-based Access Control: permits the configuration of multiple computers by setting a single policy for enforcement.

IDENTITY AND ACCESS SERVICES

RADIUS (Remote Authentication Dial-in User Service): developed in 1992 and originally allowed for remote dial-in access to a business network. A RADIUS server utilizes a central database to authenticate remote users and functions as a client-server protocol, authenticating each user with a unique encryption key when access is granted.

🔗 AAA - The Three Chain Links of RADIUS Security

IDENTITY AND ACCESS SERVICES

Kerberos: an authentication system developed by the Massachusetts Institute of Technology (MIT) in the 1980s and used to verify the identity of network users.

MicroNugget: How Does Kerberos Work

IDENTITY AND ACCESS SERVICES

Read pages 548 – 552.