Access Management

IAAAA - Identification, Authentication, Authorization, Access, Accounting

- *Object* - resource
- *Subject* - a user, or function acting on behalf of a user
- *Operation* - the action taken by a subject, over an object
- *Privacy Officer* - oversees privacy compliance
- *Custodian or Steward* - reviews security settings and makes audit trails
- *Owner* - person responsible for the information
- *End user* - person who accesses the information

Accounts

Types of Accounts:

- User Accounts
- Service Accounts
- Privileged Accounts

Initial Set-Up

- Employee Accounts
- Location Based Settings
- Standard Naming Conventions
  - aclark, athan.clark, clarkaem, clark.al.aem
- Time-Of-Day Restrictions
- Enforcing Least-Privilege
- Routine Auditing
  - Recertification
  - Permission auditing & review
  - Usage auditing & review

Offboarding

- Backup of employee's data
- Archive email & hide record in address book
- *orphaned* vs. *dormant*

Access Control Model

Properly configuring accounts is first step in security

Name	Explanation	Description
MAC	End user cannot set controls	Most restrictive
DAC	Subject has total control over objects	Least restrictive
RBAC	Assigns users and objects to role hierarchy	Real-World
RB-RBAC	Dynamically assigns roles based on rules	Managing user access to multi-systems
ABAC	Uses policies that can combine attributes	Most flexible

Discretionary Access Control (DAC)

- Least Restrictive
- Every Object has an Owner
- Owners have total control
- Owners can give permission to subjects
- Used in operating systems

Weakness

- Relies on decisions of end user to set proper security
- Security permissions are inherited by processes

Mandatory Access Control (MAC)

- Most restrictive - has no control to change security policy
- Military settings
- *Labels* - every object is assigned a classification label, subjects assigned a clearance label
- *Levels* - hierarchy of labels
- major implementations: Lattice Model, Bell-LaPadula Model
  - In Bell-LaPadula, subjects may not create objects or perform operations on lower level objects
- Windows uses Mandatory Integrity Control (MIC)
  - User Access Control (UAC) and security ids (SID)

Role Based Access Control (RBAC)

Non-Discretionary Access Control

- Access permissions are based on user's job function
- i.e. user groups

Rule Based Access Control

Rule-Based Role-Based Access Control (RB-RBAC)

- Dynamically assigns roles to subjects based on a set of rules set by custodian
- Used for managing system access to one or more systems - business changes → rule changes → access changes

Attribute-Based Access Control

- Most flexible
- More flexible policies than RB-RBAC - can combine policies
- Policies can take advantage of object, subject, and environment attributes
- Can be formatted with control flow (`if .. else`)

Best Practices for Access Control

Separation of Duties

Two keys at opposite ends of a room to launch nuke

If necessary process was operated fraudulently could cause catastrophic failure, then distribute operation of process to two or more parties

Job Rotation

- Move individuals between job responsibilities
- Limits time for committed fraud, exposes avenues for fraud
- Reduces employee "burnout"

Mandatory Vacations

- Limits fraud, because perp needs to be present
- Audits usually scheduled during absence

Clean Desk Policy

Ensures all confidential and sensitive material is secured when not in use

- computers are locked and turned off at end of day
- confidential documents are locked in desk
- keys for file cabinets are properly maintained
- use of locking cables

Implementing Access Control

- ACL is attached to objects - system checks object ACL when subject performs operation

  - file permissions, SQL and relational databases
- Each *entry* - ACE
- ACE Windows structure:
  - SID for user, group, or logon session
  - Access mask specifies access rights controlled by ACE
  - Flag indicates type of ACE (allow / deny)
  - Flags indicating inheritance of permissions (i.e. by folder structure)

Group-Based Access Control

Configures multiple computers by single security policy

- Windows Group Policy for users of Active Directory, settings stored in Group Policy Objects
  - Local Group Policy - fewer options, not for AD

Identity and Access Services

Feature	RADIUS	TACACS+
Transport Protocol	UDP	TCP
Authentication & Authorization	Combined	Separate
Communication	Unencrypted	Encrypted
Kerberos?	Nope	Yep!
Network Devices?	Nope :(	Yep!

RADIUS

Remote Authentication Dial In User Service

- 1992
- Client typically a wireless AP
- Typically users are stored in central DB
- Advantages: Increased security due to single audit trail, easier billing and network stats
- XFINITY remote login?
- IEEE 802.1x port security

Kerberos

- Developed at MIT
- Crypto tickets
- Like using a driver's license to cash a check

Terminal Access Control Access Control Systems+ (TACACS+)

- Similar to RADIUS

- commonly used on UNIX
- central server
- current version is TACACS+

Lightweight Directory Access Protocol (LDAP)

- Information about users and network devices
- Network resources and users' privileges to those resources
- **X.500** → defines DAP
- TCP/IP subset of DAP, simpler than X.500
- LDAPS - over SSL/TLS
- Susceptible to LDAP injection attacks (like SQL injection when input isn't sanitized)

Security Assertion Markup Language

- XML, allows web domains to exchange user auth data
- used in e-commerce business-to-business and business-to-customer transactions
- 3rd party identity providers

Authentication framework protocols More secure alternative to:

- Challenge-Handshake Authentication Protocol (CHAP)
- MS-CHAP
- Password Authentication Protocol (PAP)

  Extensible Authentication Protocol (EAP)

- Four packets - Request, Response, Success, Failure