Protecting Information Assets
- Unit #13 -

Identity Management and Access Control
Agenda

- Identity and Authentication
- Authorization
- Access control models
- Test taking tip and Quiz with solutions - online
- Presentations
Controlling Access to IT Assets

• A central theme of information system security
• Many different security controls work together to provide access control
  – Identity, Authentication, Authorization, Auditing...
• IT Asset includes:
  – Information
  – Systems
  – Devices
  – Facilities
  – Personnel
Identity and Authentication

• First line of defense in battling unauthorized access to network resources and systems

• Broad term covering several types of mechanisms that control access to features of networks, computers and information stored and flowing within them
Authorization: Access to information...

Access is the ability to create a flow of information between user and system

The flow of information between a subject and an object

- **Subject**
  - Always the active entity - requesting access to an object or data within the object
  - Can be users, programs, processes, services, computers...
  - When authorized, subjects can modify objects
- **Object**
  - Always the passive object - providing information to active subjects
  - Can be data files, databases, computers, programs, processes, services, storage media...

E.g. “A *user (subject)* accesses an *object (data file)*”

**Note**: Roles of subject and object can switch during interactions
- e.g. a computer program can be both a data requester and a data provider, switching back and forth
Identification, Authentication, Authorization, and Accountability ("AAA")

To access an information system resource, a user must pass through the following logical steps:
To access a network’s resource, a user must:

Prove their identity (i.e. has the necessary credentials)
Identity Management

Identification and Authentication are distinct functions

**Identification:** Who you say you are

**Authentication:** Confirmation that you are who you say you are
Identification and Authentication

Usually involves a two-step process:

1. **Identification**: Entering public information
   - Method by which a subject (user, program or process) claims to have a specific identity
     - *Username, employee number, account number, or email address*

2. **Authentication**: Entering private information
   - Individual’s identity must be verified during authentication process
   - Method by which subject proves it is who it says it is
     - *Static password, smart token, one-time password, or PIN*
Identification

Method of establishing the subject’s identity

– *Subject can be a human user, program or process*

– **Identity** – A set of attributes that uniquely describe a person within a given context

– Typically a user name, email address or other public information
Identification

Entering public information

– Method by which a subject (user, program or process) supplies identifying information to claim they have a specific identity
  
  • Username, employee number, account number, or email address

– Creating secure identities involves 3 key aspects:
  
  1. **Uniqueness** – every user, program or process must be identified with an identifier (i.e. unique ID) that is specific to the individual for accountability
  
  2. **Non-descriptive** – Identifier should not indicate the purpose of the account nor the user’s position nor tasks done with the account
  
  3. **Issuance** – provided by an authority as a formal/official means of proving identity
Authentication

The process of establishing confidence in the identity of users or information systems

Method of proving identity

– Something a person:

1. **Knows** – a secret password
2. **Has** – a token
3. **Is** or **does** – biometrics
Authentication – Classic 3 factor paradigm

...for authentication systems

Subject provides information to prove it is who it says it is and authentication system verifies the identification information

1. **Something the subject knows** ("authentication by knowledge") – Type 1 factor
   - Examples: password, PIN, combination to a lock...
   - Usually least expensive method to implement
   - Vulnerability: Someone else may acquire this knowledge and gain unauthorized access to a resource

2. **Something the subject has** ("authentication by ownership") – Type 2 factor
   - Examples: Key, swipe card, access card, badge...
   - Common for accessing facilities, sensitive areas, and authenticate holder
   - Vulnerability: Can be lost or stolen and result in unauthorized access

3. **Something the subject is** ("authentication by characteristic") – Type 3 factor
   - Examples: Fingerprint, palm scan, retina scan...
   - Based on biometrics – a way to identify the subject by a unique physical attribute
   - Vulnerability: Can be expensive, cumbersome/troubling to users and associated with false acceptance or rejection
Authentication – something you know

Passwords

– A secret shared between user authentication system
– User name + password most common identification, authentication scheme

• A weak security mechanism – requiring implementation of strong password protections
Authentication

Passphrase

– Is a sequence of characters that is longer than a password
– Takes the place of a password
– Can be more secure than a password because it is more complex
How many unique characters can be produced by the standard US QWERTY keyboard?

- Standard US Qwerty keyboards have 101, 104 or 107 keys which can produce 96 unique characters
- 26 lower case letters
- 26 upper case letters
- 10 numbers
- 32 visible symbols
- 2 Windows and Menu keys

“The name comes from the order of the first six keys on the top left letter row of the keyboard (Q W E R T Y). The QWERTY design is based on a layout created for the Sholes and Glidden typewriter and sold to E. Remington and Sons in 1873. It became popular with the success of the Remington No. 2 of 1878, and remains in widespread use.” -- Wikipedia
Authentication - Passwords

How many unique characters can be produced by the standard US QWERTY keyboard?

Standard US Qwerty keyboards have 101, 104 or 107 keys which can produce 96 unique characters:

• 26 lower case letters
• 26 upper case letters
• 10 numbers
• 32 visible symbols
• 2 Windows and Menu keys

“The name comes from the order of the first six keys on the top left letter row of the keyboard (Q W E R T Y). The QWERTY design is based on a layout created for the Sholes and Glidden typewriter and sold to E. Remington and Sons in 1873. It became popular with the success of the Remington No. 2 of 1878, and remains in widespread use.” — Wikipedia
How to create a password that is hard to crack:

• The longer the password, the harder it is to crack
• Always use a combination of characters, numbers and special characters
• Variety in passwords on different apps and systems...

https://resources.infosecinstitute.com/10-popular-password-cracking-tools/#gref

• 1 character password: 96 tries to crack
• 2 characters: 96 *96 = 9,216
• 3 characters: 96 * 96 * 96 = 884,736
• 4 characters $96^4 = 84,934,656$
• ... 
• 8 characters $96^8 = 7,213,895,789,838,336$
Techniques to attack passwords

- Guessing
- Social engineering
- Dictionary attacks
- Electronic monitoring
- Access the password file
- Brute force attacks
- Rainbow tables

https://resources.infosecinstitute.com/10-popular-password-cracking-tools/#gref
Authentication - Something you have
e.g.
- Your phone
- Card
- Synchronous token
  - Time Based
  - Counter Synchronization
Authentication – Something you are or do ("Biometrics")

- Verifies an identity by analyzing a unique person attribute or behavior
- Most expensive way to prove identity, also has difficulties with user acceptance
- Many different types of biometric systems
Authentication

Most common biometric systems:
Authentication – Biometric Systems

During identity verification (i.e. authentication) the biometric system scans personal’s physiological attribute or behavioral trait and compares the captured data to a record created in an earlier enrollment process.

- **Enrollment**
  - Present Biometric
  - Capture → Process → Store
  - No Match

- **Verification**
  - Present Biometric
  - Capture → Process
  - Match
Authentication – Biometric Systems

- Must be capable of repeatedly taking accurate measurements of anatomical or behavioral characteristics
- Error types:
  - **False negative (Type I error)** – incorrect rejection of the identity of authorized individual
    - *False Rejection Rate (FRR)* is a measurement of the likelihood that biometric device will result in Type I errors
  - **False positive (Type II error)** – incorrect match and identity acceptance of unauthorized individual ("imposter")
    - *False Acceptance Rate (FAR)* is a measurement of the likelihood that biometric device will result in Type II errors

Organizations’ security requirements will dictate how many Type I and Type II errors are acceptable.

Extreme tradeoffs:
- Prioritizing confidentiality would accept a certain Type I error rate to achieve no Type II errors
- Prioritizing convenience would accept certain Type II error rate to achieve no Type I errors

*Calibration of biometric systems would enable lowering Type II error rate by adjusting system sensitivity which will increase Type I error rate*
Authentication – Biometrics

Crossover error rate (CER) also called Equal error rate (EER)

- Objective measurement of biometric system accuracy, useful for comparing different biometric system products
- Stated as a percentage (%)
- **CER** is the point at which false rejection rate equals the false acceptance rate: FRR = FAR
- *Most important metric in determining a biometric system’s accuracy!*
Multi-factor authentication refers to use of >1 factor:
  - Something the subject knows ("authentication by knowledge")
  - Something the subject has ("authentication by ownership")
  - Something the subject is ("authentication by characteristic")

Authentication system strength determined by the number of factors incorporated into the systems
  - Implementations that use 2 factors are considered stronger than those that only use 1 factor
  - Systems that incorporate all 3 factors are stronger than systems that incorporate 2 factors
Authorization

Determines that the proven identity has some set of characteristics associated with it that gives it the right to access the requested resources
Authorization

Advantages of centralized administration and single sign on:

– User provisioning
– Password synchronization and reset
– Self service
– Centralized auditing and reporting
– Integrated workflow (increase in productivity)
– Regulatory compliance
Access Control Models

1. Discretionary (DAC)
2. Mandatory (MAC)
3. Role-Based (RBAC)
4. …other methods
Discretionary Access Control (DAC)

– Access control is at the discretion of the owner
– Used in Windows, Linux, Unix, OSX...

When using DAC method, the **owner decides** who has access to the resource - decisions are made directly for each user

Access Control Lists (ACL) and File system permissions are used to control access

The permissions identify the actions the subject can perform on the object

E.g. DAC method in NTFS permissions on Windows operating systems

• On NTFS file system each file and folder has an owner
• The owner can use ACL and decide which users or group of users have access to the file or folder
• Many operating systems use DAC method to limit access to resources
### Linux/OSX/Unix File Permissions

```bash
[root@localhost home]# ls -l
total 16
drwx------. 5 ali sales 4096 May 10 22:30 ali
-rw-r--r--. 1 root root 0 May 20 20:33 file.txt
-rw-r--r--. 1 root root 0 May 26 15:32 fileuid.txt
drwx------. 5 root itdepartment 4096 May 26 15:51 itdepartment
drwx------. 3 mohtork mohtork 74 May 9 10:20 mohtork
drwx------. 14 mtork mtork 4096 May 26 15:24 mtork
drwx------. 5 ramy ramy 4096 May 26 15:25 ramy
drwx------. 3 root sales 50 May 16 19:53 sales
```

<table>
<thead>
<tr>
<th>File Type</th>
<th># of Hard Links</th>
<th>File size</th>
<th>Owners</th>
<th>Last Modify Time</th>
<th>File name</th>
</tr>
</thead>
<tbody>
<tr>
<td>-rwxr-x---</td>
<td>1 walbert</td>
<td>0</td>
<td>support</td>
<td>Oct 31 11:06</td>
<td>test</td>
</tr>
</tbody>
</table>

#### File Permissions Diagram

```
Root Directory (/)
- Directory
  - Directory
    - Directory
      - Directory
        - File
        - File
      - Directory
        - File
  - Directory
    - File
```

- **File Type**: The first character indicates the file type (d for directory, - for regular file).
- **# of Hard Links**: The number of hard links to the file.
- **File size**: The size of the file in bytes.
- ** Owners**: The user and group ownership of the file.
- **Last Modify Time**: The date and time the file was last modified.
- **File name**: The name of the file.
Discretionary Access Control (DAC)

Provides a huge tradeoff:

— **Strengths**
  
  • Flexibility to user
  
  • Less administrative overhead to IT

— **Weaknesses**
  
  • Achilles’ heel (i.e. weakness) to the operating system
  
  • Malware can work under the identity (security context) of the user
    
    — If a user opens an virus infected file, code can install itself in the background without user awareness
    
    — Code inherits all rights and permissions of the user, can carry out all activities the user can on the system
      
      » Send copies of itself to all contacts in user’s email client, install a back-door, attack other systems, delete files on hard drive...
      
      » If the user is a local administrator or has root accounts then once installed malware can do anything
Discretionary Access Control (DAC)

Security administrators can counter downside of DAC and protect critical assets by removing user control by implementing “nondiscretionary access control” within a DAC Operating System by:

– Setting up workstations with pre-configured and loaded user profiles specifying the level of control the user does and does not have:

  • With permissions on files (including Operating System command files) and folders set to block discretionary access control to users from:
    – Changing the system’s time
    – Altering system configuration files
    – Accessing a command prompt
    – Installing unapproved applications
    – ...
Access Control Models

1. Discretionary
2. Mandatory
3. Role-based
Mandatory Access Control (MAC)

• Used in very specialized systems by government-oriented agencies:
  – To protect and maintain highly classified data
  – For focused and specific purposes – and nothing more
• Users do not have discretion to determine who can access objects
• Systems are “locked down” for security purposes with
  – Reduced amount of user rights, permissions and functionality
    • Users cannot install software, change file permissions, add new users

DAC systems are discretionary and MAC systems are considered non-discretionary because users are unable to make access decisions based on their own choice (discretion)
  – Exam Tip
Mandatory Access Control (MAC)

Based on a system of multi-level security policies and security labels

– Subjects (e.g. users) and objects (i.e. resources) are classified and labeled with their classification:
  • For example: Top Secret, Secret, Confidential, Restricted, Official, Unclassified...

– MAC OS systems decide whether or not to fulfill a request to access an object based on:
  • Its security policy (e.g. confidentiality or integrity), and
  • Clearance of the subject and classification of the object
Mandatory Access Control (MAC)

Security policy models

- **Bell-LaPadula** model enforces **confidentiality** in access control
  - Goal: Prevent secret information from unauthorized access
    - Provides and addresses confidentiality only
      » Who can and cannot access the data, and what operations can be carried out on the data
      » Does not address integrity of data the system maintains
  
  - First mathematical model for multilevel security policy – based on modes of access and provides rules of access

  - A system based on Bell-LaPadula model is called a “multilevel security system” because its users have different clearances and it processes data at different classification levels
Mandatory Access Control (MAC)

Security policy models

- Bell-LaPadula model enforces confidentiality in access control

  - 3 main rules:
    1. “No read up” rule
       A subject at a particular security level cannot read data that resides at a higher security level
    2. “No write down” rule
       A subject in a given security level cannot write information to a lower security level
    3. Strong star property rule
       A subject who has read and write capabilities can only perform both functions at the same security level; nothing higher and nothing lower
       For a subject to be able to read and write to an object, the subject’s clearance and the object classification must be equal
Mandatory Access Control (MAC)

Security policy models

- **Biba** model enforces integrity of data within a system
  - Goal: Prevents data at any integrity level from flowing to a higher integrity level
  - Uses integrity levels
  - Is not concerned with security levels nor confidentiality
Biba model enforces **integrity** of data within a system

3 main rules:

1. **“No write up” rule**
   A subject cannot write data to an object at a higher integrity level

2. **“No read down” rule**
   A subject cannot **read** data from a lower integrity level

3. **Invocation property**
   A subject cannot **communicate** by calling on or initializing another subject (invoke a service) at a higher integrity. Subjects are only allowed to invoke services at a lower integrity level
Mandatory Access Control (MAC) - Security policy models

Bell-LaPadula versus Biba

- Both information flow models concerned with data flowing from one security level to another
  - Bell-LaPadula uses security levels to provide data confidentiality
    - “no read up” “no write down”
  - Biba uses integrity levels to provide data integrity
    - “no write up” “no read down”
Brewer and Nash Model (“Chinese Wall”) – Mandatory Access Control Model

- Applies to a single integrated database
- Creates security domains around data that are used to block conflicts of interest
  - E.g. someone works for Company A should not also be allowed access to similar data from Company B if the two companies compete with each other
DAC versus MAC Systems

Administrators cannot simply switch on MAC and switch off DAC in an operating system

• DAC systems
  – System access decisions by comparing subject’s identity to the ACL on the object (i.e. resource)
  – Very flexible and dynamic
  – Malware usually targets
  – Viruses, worms, and rootkits can be installed and run as applications on DAC systems

• MAC systems
  – System access decisions by comparing subject’s clearance to the object’s security label
  – Are very constrained and have very limited functionality
  – OS does block users from installing software including malware
  – Special types of Unix systems are developed based on the MAC model
    • SE Linux is a publicly released MAC system developed by NSA and Secure Computing
    • Trusted Solaris is a product based on the MAC model
Access Control Models

1. Discretionary
2. Mandatory
3. Role-based
Role-Based Access Control (RBAC)

To resolve issues with access control administration based on DAC model resulting from:

- Access control specified explicitly to subjects at the object level with ACLs
- Complexity
  - As administrators translate organizational policy into ACL configuration permissions
  - As number of objects and users grow, and users change responsibilities, users tend to be granted or retain unnecessary access to some objects
    - Violating least-privilege rule, increasing organizational risk
  - Addressed by Role-Based Access Model...
Role-Based Access Control (RBAC)

Benefits

• Uses a centrally administered set of controls to determine how subjects and objects interact
• Roles defined in terms of operations and tasks the role will carry out
• Access to resources is implicitly assigned (inherited) based on the role the user holds within the organization
• Best system for organizations with high employee turnover
  – Assignment of users to roles is changed by administrators
  – Administrators do not need to continually change the ACLs on individual objects
Authorization concepts

- Authorization Creep
- Default to Zero – start with no access
- Principle of “Need to Know”
- Access Control List (ACL)
Test Taking Tip

Look at the facts and ask yourself, so what?

• The issue that jumps out is likely to be the issue that the correct response addresses

• Non-relevant answers can be eliminated more readily

• Especially useful in questions that ask for the “Best” answer
Quiz