Access Control

What (Definition)

* ***Access controls*** are security features that control how users and systems communicate and interact with other systems and resources.
* They protect the systems and resources from unauthorized access and can be components that participate in determining the level of authorization after an authentication procedure has successfully completed.
* Access control is a broad term that covers several different types of mechanisms that enforce access control features on computer systems, networks, and information.
* Access control is extremely important because it is one of the first lines of defense in battling unauthorized access to systems and network resources.

Access Control：

Identification

• Subjects supplying identification information - 主体提供身份信息

• Username, user ID, account number - 用户名、用户ID、账号

• Authentication - 验证

• Verifying the identification information - 验证身份信息

• Passphrase, PIN value, biometric, one-time password, password - 密码、PIN 值、生物识别、一次性密码、密码

• Authorization - 授权

• Using criteria to make a determination of operations that subjects can carry out on objects - 使用标准来确定主体可以对客体执行的操作

• Accountability - 问责制

• Audit logs and monitoring to track subject activities with objects - 审计日志和监控以跟踪主题与对象的活动

Access Control Concepts (5个概念):

* Identity (身份)
* Identification and authentication (识别和认证)
* Authorization (授权)
* Accountability (问责制)
* Password management (密码管理)

**Identity (身份)**

Creating or issuing secure identities should include three key aspects

* Uniqueness
* Non-descriptive
* Issuance

Uniqueness

Definition

* Uniqueness refers to the identifiers that are specific to an individual, meaning every user must have a unique ID for accountability.

Examples

* Retina scan
* Fingerprints
* Iris scan

Non-descriptive

Definition (定义）

* Non-descriptive means that neither piece of the credential set should indicate the purpose of that account.

Examples (例子）

* For example, a user ID should not be “administrator,” “backup\_operator,” or “CEO.”

Issuance (发行)

Definition

* These elements are the ones that have been provided by another authority as a means of proving identity.

Examples (例子）

* ID cards are a kind of security element that would be considered an issuance form of identification.

Identification Component Requirements

When issuing identification values to users, the following should be in place:

* Each value should be unique, for user accountability
* A standard naming scheme should be followed.
* The value should be non-descriptive of the user’s position or tasks.
* The value should not be shared between users.

**Identification and Authentication**

* **Identification** describes a method of ensuring that a subject (user, program, or process) is the entity it claims to be. Identification can be provided with the use of a username or account number. Once a person has been identified through the user ID or a similar value, she must be **authenticated**, which means she must prove she is who she says she is.

* Three general factors can be used for authentication:
* something a person knows/ authentication by knowledge
* something a person has/ authentication by ownership
* something a person is/ authentication by characteristic
* Strong authentication contains two out of these three methods: something a person knows, has, or is.
* Strong authentication is also sometimes referred to as **multi-authentication**, which just means that more than one authentication method is used. **Three-factor authentication** is possible, which includes all authentication approaches.

Example:

* User ID,
* MAC address,
* IP address,
* Personal Identification Number (PIN),
* Identification Badges,
* Email Address

**Authorization** (授权)

* Once the subject provides its credentials and is properly identified, the system it is trying to access needs to determine if this subject has been given the necessary rights and privileges to carry out the requested actions.

Eg. Different positions will have different rights and privileges to carry out the requested actions

* For example, a teacher and a student in school will have different rights to access different platforms on a school system. A teacher will be able to carry out certain tasks that a student cannot.
* The system will look at some type of access control matrix or **compare security labels** to verify that this subject may indeed access the requested resource and perform the actions it is attempting. If the system determines that the subject may access the resource, it authorizes the subject.

**Identity Management 身份管理**

* Identity management is a broad and loaded term that encompasses the use of different products to identify, authenticate, and authorize users through automated means.
* The following are many of the common questions enterprises deal with today in controlling access to assets:
* What should each user have access to?
* Who approves and allows access?
* How do the access decisions map to policies?
* Do former employees still have access?
* How do we keep up with our dynamic and ever-changing environment?
* What is the process of revoking access?
* How is access controlled and monitored centrally?
* Why do employees have eight passwords to remember?

**Accountability 问责制**

* Auditing 审计 capabilities ensure users are accountable for their actions, verify that the security policies are enforced, and can be used as investigation tools.
* There are several reasons why network administrators and security professionals want to make sure accountability mechanisms are in place and configured properly:
* to be able to track bad deeds back to individuals
* detect intrusions
* reconstruct events and system conditions
* provide legal recourse material
* produce problem reports
* Audit documentation and log files hold a mountain of information—the trick is usually deciphering it and presenting it in a useful and understandable format.
* Accountability is tracked by recording user, system, and application activities. This recording is done through auditing functions and mechanisms within an operating system or application.
* Audit trails contain information about operating system activities, application events, and user actions.
* Audit trails can be used to verify the health of a system by checking performance information or certain types of errors and conditions.
* After a system crashes, a network administrator often will review audit logs to try and piece together the status of the system and attempt to understand what events could be attributed to the disruption.

What to keep in mind when dealing with auditing

1. Store the audits securely.
2. The right audit tools will keep the size of the logs under control.
3. The logs must be protected from any unauthorized changes in order to safeguard data.
4. Train the right people to review the data in the right manner.
5. Make sure the ability to delete logs is only available to administrators.
6. Logs should contain activities of all high-privileged accounts (root, administrator).

**Password Management**

* Different types of password management technologies have been developed to get these pesky users off the backs of IT and the help desk by providing a more secure and automated password management system. The most common password management approaches are listed next:
* **Password Synchronization -** Reduces the complexity of keeping up with different passwords for different systems. eg. The password of our Axis, Moodle and Computer system accounts are the same.
* **Self-Service Password Reset** - Reduces help-desk call volumes by allowing users to reset their own passwords.
* **Assisted Password Reset** - Reduces the resolution process for password issues for the help desk. This may include authentication with other types of authentication mechanisms (biometrics, tokens).

Password security

* Password generation: system vs user
* Password strength: length, complexity, dynamic…
* Password ageing & rotation
* Limit login attempts