Access Control (访问控制)

What (Definition: 定义）

* ***Access controls*** are security features that control how users and systems communicate and interact with other systems and resources.

Access control 是一种控制users怎么运用其他系统和资源的安全功能

* 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.

它们保护着系统和资源,防止資料 在未 獲授權情況下存取，并且可以是在身份验证过程成功完成后参与确定授权级别的组件.

* 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 是一个广义术语，涵盖了几种不同类型的机制，这些机制在计算机系统、网络和信息上实施访问控制功能

* 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 的重要性在于它是与未经授权访问系统和网络资源作斗争的第一道防线之一

关于Access Control 的单词/词语：

Identification

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

主题(subject)代表着使用者, 物体（object）代表着被使用的事物

Eg. User access interface (用户访问接口)

User is the subject and interface is the object

在不同的情况下，subject和object都不一样，

有些情况下的subject有可能是另一种情况下的object.

• 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 (制定或颁发安全身份的三个关键特征):

* Uniqueness (唯一性)
* Non-descriptive (非描述性的)
* Issuance (发行)

Uniqueness (唯一性)

Definition (定义）

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

唯一性是指特定于个人的标识符，这意味着每个用户都必须具有唯一的 ID 以进行问责。

Examples (例子)

* Retina scan - 视网膜扫描
* Fingerprints - 指纹
* Iris scan - 虹膜扫描

Non-descriptive (非描述性的)

Definition (定义）

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

非描述性意味着凭证集的任何部分都不应指示该帐户的用途

Examples (例子）

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

用户 ID 不应是”管理员”, “备份操作员”或“CEO”

Issuance (发行)

Definition (定义)

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

这些元素是由另一个权威机构提供的，作为证明身份的手段

Examples (例子）

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

身份证是一种安全元素，可被视为身份证明的发行形式

Identification Component Requirements (标识组件要求)

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

向用户发布标识值时，应具备以下条件:

* Each value should be unique, for user accountability

每个值都应该是独特的，以便用户负责

* A standard naming scheme should be followed.

应遵循标准命名方案

* The value should be non-descriptive of the user’s position or tasks.

该值不应描述用户的职位或任务

* The value should not be shared between users.

该值不应在用户之间共享

**Identification and Authentication(**识别和认证)

* **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.

标识描述了一种确保主体（用户、程序或进程）是它声称的实体的方法。可以使用用户名或帐号来提供标识。一旦通过用户 ID 或类似值识别了一个人，就必须对她进行身份验证，这意味着她必须证明她是她所说的那个人。

* Three general factors can be used for authentication:
* something a person knows/ authentication by knowledge (你知道的东西）eg. 妈妈，家乡
* something a person has/ authentication by ownership （拥有的东西）eg. Identification Card 身份证，Passport 护照
* something a person is/ authentication by characteristic (你是什么东西）eg. Uniqueness, Iris Scan虹膜，Fingerprint Scan指纹
* 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.

一旦主体提供了其凭证并被正确识别，它试图访问的系统就需要确定该主体是否已被授予必要的权利和特权来执行所请求的操作。

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.

系统将查看某种类型的访问控制矩阵或比较安全标签，以验证该主体是否确实可以访问所请求的资源并执行它正在尝试的操作。如果系统确定主体可以访问资源，则它授权主体。

**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.

身份管理是一个广泛而丰富的术语，包括使用不同的产品通过自动化方式识别、验证和授权用户。

* 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.

审计功能确保用户对他们的行为负责，验证安全策略是否得到执行，并可作为调查工具使用。

* There are several reasons why network administrators and security professionals want to make sure accountability mechanisms are in place and configured properly: 网络管理员和安全专家要确保问责机制到位并配置得当，有几个原因。
* to be able to track bad deeds back to individuals 能够追溯到个人的不良行为
* detect intrusions 检测入侵行为
* reconstruct events and system conditions 重构事件和系统条件
* provide legal recourse material 提供法律追索材料
* produce problem reports 制作问题报告
* 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.

以一种有用和可理解的形式呈现

* Accountability is tracked by recording user, system, and application activities. This recording is done through auditing functions and mechanisms 机制 within an operating system or application.

通过记录用户、系统和应用程序的活动来跟踪责任制。

* Audit trails contain information about operating system activities, application events, and user actions. 操作系统活动、应用程序事件和用户行动。
* Audit trails can be used to verify the health of a system by checking performance information or certain types of errors and conditions. 审计跟踪可以通过检查性能信息或某些类型的错误和状况来验证系统的健康状况
* 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. 在系统崩溃后，网络管理员通常会审查审计日志，试图拼凑出系统的状态，并试图了解哪些事件可以归因于系统的中断

What to keep in mind when dealing with auditing

1. Store the audits securely. 安全地储存审计结果。
2. The right audit tools will keep the size of the logs under control. 正确的审计工具会使日志的大小得到控制。
3. The logs must be protected from any unauthorized changes in order to safeguard data. 日志必须受到保护，防止任何未经授权的更改，以保护数据
4. Train the right people to review the data in the right manner. 培训正确的人以正确的方式审查数据。
5. Make sure the ability to delete logs is only available to administrators. 确保删除日志的能力只对管理员有效。
6. Logs should contain activities of all high-privileged accounts (root, administrator). 日志应包含所有高权限账户（root、管理员）的活动。

**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:

不同类型的密码管理技术已经被开发出来，通过提供一个更安全和自动化的密码管理系统，让这些讨厌的用户从IT部门和服务台的背上消失。接下来列出了最常见的密码管理方法。

* **Password Synchronization -** Reduces the complexity of keeping up with different passwords for different systems. 密码同步 - 减少了为不同系统保持不同密码的复杂性。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. 自助式密码重设 - 通过允许用户重设自己的密码来减少服务台的呼叫量。
* **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). 辅助密码重置 - 减少服务台解决密码问题的过程。这可能包括用其他类型的认证机制（生物识别技术、令牌）进行认证。

Password security

* Password generation: system vs user 密码生成：系统与用户
* Password strength: length, complexity, dynamic… 密码强度：长度、复杂性、动态...
* Password ageing & rotation 密码的老化和轮换
* Limit login attempts 限制登录尝试