Information Systems Security

Presented By
Dr. Mohamed Marie

3 Chapter

Security Management Concepts and Principles

This chapter presents the following:

Security Management Concepts and Principles
Protection Mechanisms
Change Control/Management
Data Classification

Protection Mechanisms

Another aspect of security solution concepts and principles is the element of protection mechanisms. **These are common characteristics of security controls**. Not all security controls must have them, but **many controls offer their protection for confidentiality, integrity, and availability through the use of these mechanisms**. These **mechanisms** include using **multiple layers or levels of access**, **employing abstraction**, **hiding data**, and **using encryption**.

Protection Mechanisms

Layering

Layering, also known as ***defense in depth***, is ***simply the use of multiple controls in a series***. **No one control can protect against all possible threats.** Using a multilayered solution allows for numerous, different controls to guard against whatever threats come to pass. ***When security solutions are designed in layers, most threats are eliminated, mitigated, or thwarted***.

Using layers in a series rather than in parallel is important.

Performing security restrictions in a series means to perform one after the other in a linear fashion. Only through a series configuration will each attack be scanned, evaluated, or mitigated by every security control. A single failure of a security control does not render the entire solution ineffective. ***If security controls were implemented in parallel, a threat could pass through a single checkpoint that did not address its particular malicious activity***. **Serial configurations are very narrow but very deep, whereas parallel configurations are very wide but very shallow**. ***Parallel systems are useful in distributed computing applications, but parallelism is not often a useful concept in the realm of security***.

Protection Mechanisms

Layering

Think of physical entrances to buildings. A parallel configuration is used for **shopping malls**. There are many doors in many locations around the entire perimeter of the mall. A series configuration would most likely be used in a **bank or an airport**. **A single entrance is provided, and that entrance is actually several gateways or checkpoints that must be passed in sequential order to gain entry into active areas of the building**. Layering also includes the concept that networks comprise numerous separate entities, each with its own unique security controls and vulnerabilities. In an effective security solution, there is a synergy between all networked systems that creates a single security front. **Using separate security systems creates a layered security solution.**

Protection Mechanisms

Abstraction

Abstraction ***is used for efficiency***. ***Similar elements are put into groups, classes, or roles that are assigned security controls, restrictions, or permissions as a collective.*** Thus, the concept of abstraction **is used when classifying objects or assigning roles to subjects**. The concept of abstraction also includes the definition of object and subject types or of objects themselves (that is, a data structure used to define a template for a class of entities). ***Abstraction is used to define what types of data an object can contain, what types of functions can be performed on or by that object, and what capabilities that object has.*** Abstraction simplifies security by enabling you to assign security controls to a group of objects collected by type or function.

Protection Mechanisms

Data Hiding

Data hiding ***is exactly what it sounds like: preventing data from being discovered or accessed by a subject by positioning the data in a logical storage compartment that is not accessible or seen by the subject.***
Keeping a database from being accessed by unauthorized visitors is a form of data hiding, as is restricting a subject at a lower classification level from accessing data at a higher classification level.
Preventing an application from accessing hardware directly is also a form of data hiding. Data hiding is often a key element in security controls as well as in programming.

Protection Mechanisms

Encryption

Encryption ***is the art and science of hiding the meaning or intent of a communication from unintended recipients***.

Encryption can take many forms and be applied to every type of electronic communication, including text, audio, and video files, as well as applications themselves. Encryption is an important element in security controls, especially in regard to the **transmission of data between systems**. There are various strengths of encryption, each of which is designed and/or appropriate for a specific use or purpose.

Change Control/Management

Another important aspect of security management is the control or management of change. **Change in a secure environment can introduce loopholes, overlaps, missing objects, and oversights that can lead to new vulnerabilities**. The only way to maintain security in the face of change is to **systematically manage change**. This usually involves extensive **planning**, **testing**, **logging**, **auditing**, and **monitoring** of **activities related to security controls and mechanisms**. The records of changes to an environment are then used to identify agents of change, whether those agents are objects, subjects, programs, communication pathways, or even the network itself.

The goal of change management is to ensure that any change does not lead to reduced or compromised security. Change management is also responsible for **making it possible to roll back any change to a previous secured state**. Change management can be implemented on any system despite the level of security. Ultimately, **change management improves the security of an environment** by protecting implemented security from unintentional, tangential, or affected diminishments. Although an important goal of change management is to **prevent unwanted reductions in security, its primary purpose is to make all changes subject to detailed documentation and auditing and thus able to be reviewed and scrutinized by management.**

Change Control/Management

Change management should be used to oversee alterations to every aspect of a system, including **hardware configuration and OS and application software**. Change management should be included in **design**, **development**, **testing**, **evaluation**, **implementation**, **distribution**, **evolution**, **growth**, **ongoing operation**, and **modification**. It requires a detailed inventory of every component and configuration. It also requires the collection and maintenance of complete documentation for every system component, from hardware to software and from configuration settings to security features.

Change Control/Management

The change control process of configuration or change management has several goals or requirements:

- **Implement changes in a monitored and orderly manner**. Changes are always controlled.
- **A formalized testing process is included** to verify that a change produces expected results.
- **All changes can be reversed**.
- **Users are informed of changes before they occur** to prevent loss of productivity.
- **The effects of changes are systematically analyzed.**
- **The negative impact of changes on capabilities, functionality, and performance is minimized.**

Change Control/Management

One example of a change management process is a ***parallel run***, **which is a type of new system deployment testing where the new system and the old system are run in parallel**. Each major or significant user process is performed on each system simultaneously to ensure that the new system supports all required business functionality that the old system supported or provided.

Data Classification

Data classification ***is the primary means by which data is protected based on its need for secrecy, sensitivity, or confidentiality***. It is inefficient to treat all data the same when designing and implementing a security system because some data items need more security than others. ***Securing everything at a low security level means sensitive data is easily accessible. Securing everything at a high security level is too expensive and restricts access to unclassified, noncritical data***. Data classification is used to determine how much effort, money, and resources are allocated to protect the data and control access to it.

The primary objective of data classification schemes is to formalize and stratify the process of securing data based on assigned ***labels*** of importance and sensitivity. **Data classification is used to provide security mechanisms for storing, processing, and transferring data**. It also addresses how data is removed from a system and destroyed

Data Classification

The following are benefits of using a data classification scheme:

- It demonstrates an organization's commitment to protecting valuable resources and assets.
- It assists in identifying those assets that are most critical or valuable to the organization.
- It lends credence to the selection of protection mechanisms.
- It is often required for regulatory compliance or legal restrictions.
- It helps to define access levels, types of authorized uses, and parameters for declassification, and/or destruction of no longer valuable resources.

Data Classification

The criteria by which data is classified vary based on the organization performing the classification. However, you can glean numerous generalities from common or standardized classification systems:

- **Usefulness** of the data
- **Timeliness** of the data
- **Value** or **cost** of the data
- **Maturity** or **age** of the data
- **Lifetime** of the data (or when it expires)
- **Association** with personnel
- **Data disclosure damage assessment** (that is, how the disclosure of the data would affect the organization)
- **Data modification damage assessment** (that is, how the modification of the data would affect the organization)
- **National security implications** of the data
- **Authorized access to the data** (that is, who has access to the data)
- **Restriction from the data** (that is, who is restricted from the data)
- **Maintenance and monitoring** of the data (that is, who should maintain and monitor the data)
- **Storage** of the data

Data Classification

Using whatever criteria is appropriate for the organization, data is evaluated, and an appropriate data classification label is assigned to it. In some cases, the label is added to the data object. In other cases, labeling is simply assigned by the placement of the data into a storage mechanism or behind a security protection mechanism. ***To implement a classification scheme, you must perform seven major steps or phases***:

- Identify the custodian, and define their responsibilities.
- Specify the evaluation criteria of how the information will be classified and labeled.
- Classify and label each resource. (The owner conducts this step, but a supervisor should review it.)
- Document any exceptions to the classification policy that are discovered, and integrate them into the evaluation criteria.
- Select the security controls that will be applied to each classification level to provide the necessary level of protection.
- Specify the procedures for declassifying resources and the procedures for transferring custody of a resource to an external entity.
- Create an enterprisewide awareness program to instruct all personnel about the classification system.

Data Classification

Declassification is often overlooked when designing a classification system and documenting the usage procedures. ***Declassification is required once an asset no longer warrants or needs the protection of its currently assigned classification or sensitivity level***. In other words, if the asset were new, it would be assigned a lower sensitivity label than it currently is assigned. When assets fail to be declassified as needed, security resources are wasted, and the value and protection of the higher sensitivity levels is degraded.

Data Classification

The two common classification schemes are **government/military classification** and **commercial business/private sector classification**.

There are five levels of **government/ military classification** (listed here from highest to lowest):

Top secret ***The highest level of classification***. The unauthorized disclosure of top-secret data will have drastic effects and cause grave damage to national security.

Secret ***Used for data of a restricted nature***. The unauthorized disclosure of data classified as secret will have significant effects and cause critical damage to national security.

Confidential Used for data of a confidential nature. The unauthorized disclosure of data classified as confidential will have noticeable effects and cause serious damage to national security. This classification is used for all data between secret and sensitive but unclassified classifications.

Sensitive but unclassified Used for data of a sensitive or private nature, but the disclosure of this data would not cause significant damage.

Unclassified The lowest level of classification. This is used for data that is neither sensitive nor classified. The disclosure of unclassified data does not compromise confidentiality or cause any noticeable damage.

Data Classification

The classifications of **confidential**, **secret**, and **top secret** are collectively known or labeled as ***classified***. Often, revealing the actual classification of data to unauthorized individuals is a violation of that data. Thus, the term ***classified*** **is generally used to refer to any data that is ranked above the sensitive but unclassified level.** All classified data is exempt from the Freedom of Information Act as well as many other laws and regulations. The U.S. military classification scheme is most concerned with the sensitivity of data and focuses on the protection of confidentiality (that is, the prevention of disclosure). You can roughly define each level or label of classification by the **level of damage** that would be caused in the event of a confidentiality violation. **Data from the top-secret level would cause grave damage to national security, while data from the unclassified level would not cause any serious damage to national or localized security**.

Data Classification

The ***four levels*** of **commercial business/private sector classification** (listed highest to lowest) are as follows:

Confidential The highest level of classification. This is used for data that is extremely sensitive and for internal use only. A significant negative impact could occur for a company if confidential data is disclosed. Sometimes the label *proprietary* is substituted for *confidential*.

Private Used for data that is of a private or personal nature and intended for internal use only. A significant negative impact could occur for the company or individuals if private data is disclosed.

Sensitive Used for data that is more classified than public data. A negative impact could occur for the company if sensitive data is disclosed.

Public The lowest level of classification. This is used for all data that does not fit in one of the higher classifications. Its disclosure does not have a serious negative impact on the organization.