MODULE 4: PRINCIPLES OF SECURITY DESIGN
WEEK 4

Learning Outcomes:

After completing this course you are expected to demonstrate the following:

1. Illustrate the principles of secure design such as least privilege and isolation

A. Engage

Did you know?

1. Responsible disclosure is also known as vulnerability disclosure.
2. The concept of full disclosure implies the immediate and full publication of all the details of the discovered vulnerability – possibly including an exploit to demonstrate the vulnerability.
3. The vulnerabilities are usually discovered by security researchers who specifically look for them.
4. There are two basic approaches to vulnerability disclosure from the researchers, which are characterized by the terms 'full disclosure' and 'responsible disclosure'.
5. Ethical choices are decisions made by individuals who are responsible for the consequences of their actions.

B. Explore

Video Title: **Design Principles of Security**

YouTube Link: https://www.youtube.com/watch?v=CLHX9S_p-5Q

Video Module Filename: **Week 4-6 - Design Principles of Security**

C. Explain

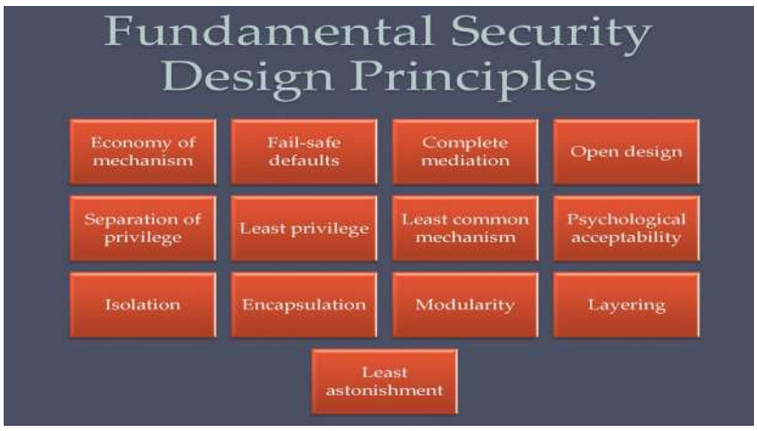

Figure 4.0
Fundamental Security Design Principles

The **security design principles** are considered while designing any security mechanism for a system. These principles are review to develop a secure system which prevents the security flaws and also prevents unwanted access to the system.

D. Elaborate

Least Privilege and Isolation

Least privilege

Least privilege, often referred to as the principle of least privilege (PoLP), refers to the concept and practice of restricting access rights for users, accounts, and computing processes to only those resources absolutely required to perform routine, authorized activities. Privilege itself refers to the authorization to bypass certain security restraints. A least privilege security model entails enforcing the minimal level of user rights, or lowest clearance level, that allows the user to perform his/her role. However, least privilege also applies to processes, applications, systems, and devices (such as IoT), in that each should have only those permissions required to perform an authorized activity.

A Brief Overview of Privileged Accounts & Access

Depending on the system, some privilege assignment, or delegation, to people may be based on attributes that are role-based, such as business unit, (i.e. marketing, HR, or IT) as well as a variety of other parameters (seniority, time of day, special circumstance, etc.). Additionally, various operating systems provide different default privilege settings for different types of user accounts.

1. **Super User Accounts**
   Primarily used for administration by specialized IT employees, may have virtually unlimited privileges, or carte blanche, over a system. Super user account privileges can include full read/write/execute privileges, and the power to render systemic changes across a network, such as creating or installing files or software, modifying files and settings, and deleting users and data.

2. **Standard User Accounts**
   Sometimes called least-privileged user accounts (LUA) or non-privileged accounts, have a limited set of privileges. In a least privilege environment, these are the type of accounts that most users should be operating in 90 – 100% of the time.

3. **Guest User Accounts**
   Have access that is even more restricted than standard user accounts.

In addition to privileged accounts, a least privilege strategy will also need to account for privileged processes within applications, services, etc. For instance, some apps might request access to sensitive resources or require a higher level of privileges to perform a function. As with privileged accounts, applications can be compromised, with the threat actor then able to leverage the elevated privileges of the application in leveraging their attack.

Chief Benefits of Implementing a Least Privilege Model

1. ***A condensed attack surface:*** Limiting privileges for people, processes, and applications means the pathways and ingresses for exploit are also diminished.

2. ***Reduced malware infection and propagation:*** As the malware (such as SQL injections) would be denied the privileges necessary to elevate processes that allow it to install or execute.
3. ***Improved operational performance:*** Limiting the number of privileges to the minimal range of processes to perform an authorized activity reduces the chance of incompatibility issues cropping up between other applications or systems, and helps reduce the risk of downtime.
4. ***Easier path to compliance:*** By restricting the potential activities that can be performed, least privilege enforcement helps create a less complex, and thus, a more audit-friendly, environment. Moreover, many compliance regulations (including HIPAA, PCI DSS, FDDC, Government Connect, FISMA, and SOX) require that organizations apply least privilege access policies to ensure proper data stewardship and systems security.

How to Implement Least Privilege

While straightforward conceptually, least privilege access can prove complex to effectively implement, depending on the particular variables, which may include:

1. Heterogeneous systems (Windows, Mac, Unix, Linux, etc.)
2. The expanding number and types of applications and endpoints (desktops, laptops, tablets smart phones, IoT, etc.)
3. Diverse computing environments (cloud, virtual, on-prem, hybrid)
4. The many different types of user roles
5. Third-party/vendor access

Organizations looking to implement least privilege environments typically rely on automated privileged access management (PAM) solutions, firewalling, network segmentation, and other tools and tactics. Here's a brief breakdown of each:

1. **Privilege access management (PAM)**
   Alternatively referred to as privileged identity management (PIM) or simply Privilege Management, involves the creation and deployment of solutions and strategies to manage and secure accounts, and control privilege delegation and escalation activities for users, applications, services, processes, tasks, etc.
2. **Network segmentation**
   Such as the creation of different zones through firewall configuration and rules, enables the enforcement of least privilege in broad strokes. By controlling access and movement between zones, which may have a different mix of applications and services, firewalls can restrict users broadly based on privileges.
3. **Separation of privilege**
   It involves separating different types of privileged and non-privileged accounts and activities, as well as compartmentalizing privileges for different application and system sub-tasks or processes. This essentially creates moats around users and system/application processes, condensing the attack surface by reducing the ability for lateral movement.
4. **Systems hardening**
   Entails the elimination of unnecessary programs, accounts, and services, A common systems hardening use case is the closing of un-needed firewall ports.

Statement: Least privilege

Rationale: Every program and user should operate while invoking as few privileges as possible. This is the rationale behind Unix "sudo" and Windows User Account Control, both of which allow a user to apply administrative rights temporarily to perform a privileged task.

Implications: This principle has impact on the system, software components, but also on procedures used.

Isolation

This security design principle is considered in three circumstances. The **first condition**, the system that has critical data, processes or resources must be isolated such that it restricts public access. It can be done in two ways.

The system with critical resources can be isolated in two ways ***physical*** and ***logical isolation***.

1. The **physical isolation** is one where the system with critical information is isolated from the system with public access information.

2. In **logical isolation**, the security services layers are established between the public system and the critical systems.

The **second isolation condition** is that the files or data of one user must be kept isolated with the files or data of another user. Nowadays the new operating system has this functionality.

Each user operating the system have an isolated memory space, process space, file space along with the mechanism to prevent unwanted access.

And the **third isolation condition** is where the security mechanism must be isolated from such that they are prevented from unwanted access.

Statement: Isolate public access systems from mission critical resources (e.g., data, processes, etc.).

Rationale: While the trend toward shared infrastructure has considerable merit in many cases, it is not universally applicable. In cases where the sensitivity or criticality of the information is high, organizations may want to limit the number of systems on which that data is stored and isolate them, either physically or logically. Physical isolation may include ensuring that no physical connection exists between an organization's public access information resources and an organization's critical information. When implementing logical isolation solutions, layers of security services and mechanisms should be established between public systems and secure systems responsible for protecting mission critical resources.

Implications: Isolation measurements must be tested regularly. An audit report from a third party is required (in case of cloud sourcing).

Fail-Safe Defaults

The principle of **fail-safe defaults** states that, unless a subject is given explicit access to an object, it should be denied access to that object.

This principle requires that the default access to an object is none. Whenever access, privileges, or some security-related attribute is not explicitly granted, it should be denied. Moreover, if the subject is unable to complete its action or task, it should undo those changes it made in the security state of the system before it terminates. This way, even if the program fails, the system is still safe.

Example:

If the mail server is unable to create a file in the spool directory, it should close the network connection, issue an error message, and stop. It should not try to store the message elsewhere or to expand its privileges to save the message in another location, because an attacker could use that ability to overwrite other files or fill up other disks (a denial of service attack). The protections on the mail spool directory itself should allow create and write access only to the mail server and read and delete access only to the local server. No other user should have access to the directory.

In practice, most systems will allow an administrator access to the mail spool directory. By the principle of least privilege, that administrator should be able to access only the subjects and objects involved in mail queuing and delivery. As we have seen, this constraint minimizes the threats if that administrator's account is compromised. The mail system can be damaged or destroyed, but nothing else can be.

Statement: Fail Safe Defaults

Rationale: A mechanism that, in the event of failure, responds in a way that will cause no harm, or at least a minimum of harm, to other devices or danger to personnel.

Implications: Stress under load and hard failure situations must be incorporated in the security test suite. Default system configuration at start-up is secure.

E. Evaluate

ASSESSMENT:
Instructions: You may write your answer on the Answer Sheet (AS) provided in this module.

CONTENT FOR ASSESSMENT:

1. One where the system with critical information is isolated from the system with public access information.
2. Security model entails enforcing the minimal level of user rights, or lowest clearance level, that allows the user to perform his/her role.
3. This principle requires that the default access to an object is none.
4. Involves separating different types of privileged and non-privileged accounts and activities.
5. Have access that is even more restricted than standard user accounts

Activity No.2

Instruction: To be pass by next meeting. Do a reseach on the following and analyze it for recitation next meeting:

1. Open design principle of security design
2. End-to-end security

References:

1. *https://slideplayer.com/slide/16969680/(image)*
2. *https://binaryterms.com/fundamental-security-design-principles.html*
3. *https://www.beyondtrust.com/resources/glossary/least-privilege*
4. *https://www.informit.com/articles/article.aspx?p=30487&seqNum=2*
5. *https://security-and-privacy-reference-architecture.readthedocs.io/en/latest/08-security-principles.html#isolate-public-access-systems-from-mission-critical-resources*

Facilitated By:		
Name	:	
MS Teams Account (email)	:	
Smart Phone Number	:	