MODULE 5: PRINCIPLES OF SECURITY DESIGN
WEEK 5

Learning Outcomes:

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

1. Illustrate open design principles in relation to developing and implementing the concept of a secure system

A. Engage

Did you know?

1. Various operating systems provide different default privilege settings for different types of user accounts.
2. While straightforward conceptually, least privilege access can prove complex to effectively implement, depending on the particular variables.
3. Privilege access management (PAM) alternatively referred to as privileged identity management (PIM) or simply Privilege Management
4. Isolation security design principle is considered in three circumstances.
5. Fail safe default state that, unless a subject is given explicit access to an object, it should be denied access to that object.

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

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

Open Design

The principle of ***open design*** states that the security of a mechanism should not depend on the secrecy of its design or implementation.

Designers and implementers of a program must not depend on secrecy of the details of their design and implementation to ensure security. Others can ferret out such details either through technical means, such as disassembly and analysis, or through nontechnical means, such as searching through garbage receptacles for source code listings (called "dumpster-diving"). If the strength of the program's security depends on the ignorance of the user, a knowledgeable user can defeat that security mechanism. The term "security through obscurity" captures this concept exactly.

This is especially true of cryptographic software and systems. Because cryptography is a highly mathematical subject, companies that market cryptographic software or use

cryptography to protect user data frequently keep their algorithms secret. Experience has shown that such secrecy adds little if anything to the security of the system. Worse, it gives an aura of strength that is all too often lacking in the actual implementation of the system.

Keeping cryptographic keys and passwords secret does not violate this principle, because a key is not an algorithm. However, keeping the enciphering and deciphering algorithms secret would violate it.

Issues of proprietary software and trade secrets complicate the application of this principle. In some cases, companies may not want their designs made public, lest their competitors use them. The principle then requires that the design and implementation be available to people barred from disclosing it outside the company.

Example

The ***Content Scrambling System (CSS)*** is a cryptographic algorithm that protects DVD movie disks from unauthorized copying. The DVD disk has an authentication key, a disk key, and a title key. The title key is enciphered with the disk key. A block on the DVD contains several copies of the disk key, each enciphered by a different player key, and a checksum of the disk key. When a DVD is inserted into a DVD player, the algorithm reads the authentication key. It then deciphers the disk keys using the DVD player's unique key. When it finds a deciphered key with the correct hash, it uses that key to decipher the title key, and it uses the title key to decipher the movie. Figure 5.1 shows the layout of the keys. The authentication and disk keys are not located in the file containing the movie, so if one copies the file, one still needs the DVD disk in the DVD player to be able to play the movie.

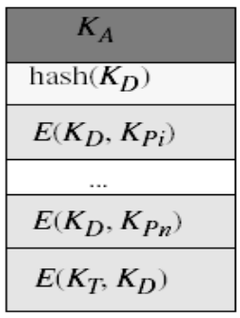

Figure 5.1
Key Layouts

Strong Vs. Weak Argument For Open Design:

1. **Weak:** Don't rely on security through obscurity, because your secrets will leak out eventually

2. **Strong:** Your system will actually benefit from having everyone examine its design/implementation. But being open doesn't automatically make you secure!

Statement: Open design. The security of physical products, machines and systems should not depend on secrecy of the design and implementation.

Rationale: Baran (1964) argued persuasively in an unclassified RAND report that secure systems, including cryptographic systems, should have unclassified designs. This reflects

recommendations by Kerckhoffs (1883) as well as Shannon's maxim: "The enemy knows the system" (Shannon, 1948). Even the NSA, which resisted open crypto designs for decades, now uses the Advanced Encryption Standard to encrypt classified information.

End-to-end security

What is end-to-end encryption?

End-to-end encryption is a secure line of communication that blocks third-party users from accessing transferred data. When the data is being transferred online, only the sender and recipient can decrypt it with a key. In that way, E2EE can help mitigate risk and protect sensitive information by blocking third parties from accessing user data when data is transferred from one source to another.

So, how does E2EE work?

At the basic level, encryption starts with cryptography. ***Cryptography*** is the art of writing code, is used to generate the codes that keep the information encrypted.

To transfer the data, the sender uses an encryption key, which scrambles the information. Only a recipient with the corresponding key can unscramble the data. There are two types of keys available: ***asymmetric and symmetric encryption***.

What are asymmetric and symmetric encryption?

- **Symmetric encryption**, the more conventional mode of encryption, uses the same key to encode and decode information.
- **Asymmetric encryption** utilizes two keys to unlock encrypted information. This is a newer, more complex version of encryption, with a public and a private key. The public key is in fact public, for anyone to use to send a message, but the private key is held by the owner to protect it.

What are the benefits and challenges of E2EE?

One pro of end-to-end encryption is that it's a security measure that's built in to your hardware and software. You don't have to think about it. Your data is protected and no one can access it except the intended recipient.
But there are challenges that come with E2EE. Mainly, while it protects information being transmitted from one recipient to another, it doesn't protect those endpoints.

What are other methods to keep your data safe?

Beyond E2EE, there are other types of data encryption:

1. **Secure Sockets Layer (SSL)** is the more modern version of Transport Layer Security (TLS), and it's the standard for protecting data on the web.

2. **Tokenization** means you're substituting a sensitive data element with a non-sensitive equivalent, referred to as a token. The token has no meaning or value; it just helps map you back to the sensitive data.

3. An **elliptic curve integrated encryption scheme (ECIES)** is a system that independently derives a bulk encryption key and a MAC (message authentication code) key from a "common secret." The data is encrypted under a symmetric cipher. Then the cipher is encrypted under a MAC.

E. Evaluate

ASSESSMENT:

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

CONTENT FOR ASSESSMENT:

1. Utilizes two keys to unlock encrypted information.
2. It has no meaning or value.
3. States that the security of a mechanism should not depend on the secrecy of its design or implementation.
4. The more conventional mode of encryption, uses the same key to encode and decode information.
5. Keeping _____ keys and passwords secret does not violate this principle.

References:

1. *https://slideplayer.com/slide/16969680/(image)*
2. *https://binaryterms.com/fundamental-security-design-principles.html*
3. *https://www.informit.com/articles/article.aspx*
4. *https://people.eecs.berkeley.edu/~daw/teaching/cs261-f07/slides-aug30.pdf*
5. *https://squareup.com/us/en/townsquare/end-to-end-encryption*
6. *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	:	