جامعة المستقبل
AL MUSTAQBAL UNIVERSITY

كلية العلوم

قسم الأمن السيبراني

Lecture: (1)

Software and System Security Principles

Subject: software security

second Stage

Lecturer: Asst. Lecturer. Suha Alhussieny

Section One: Software and System Security Principles

Computer software, also called software, is a set of instructions and documentation that tells a computer what to do or how to perform a task. Software includes all different programs on a computer, such as applications and the operating system.

- Applications are programs that are designed to perform a specific operation, such as a game or a word processor.
- The operating system (e.g. Mac OS, Microsoft Windows, Android and various Linux distributions) is a type of software that is used as a platform for running the applications, and controls all user interface tools including display and the keyboard.

The word software was first used in the late 1960s to emphasize on its difference from computer hardware, which can be physically observed by the user. Software is a set of instructions that the computer follows. The word firmware usually refers to a piece of software that directly controls a piece of hardware. The firmware for a CD drive or a modem are examples of firmware implementation.

Software security refers to a set of practices that help protect software applications and digital solutions from attackers. Developers incorporate these techniques into the software development life cycle and testing processes. As a result, companies can ensure their digital solutions remain secure and are able to function in the event of a malicious attack.

Software Security Important: Secure software development is incredibly important because there are always people out there who seek to exploit business data. As businesses become more reliant on software, these programs must remain safe and secure. With strong software security protocols in place, you can prevent attackers from stealing potentially sensitive information such as credit card numbers and trade secrets, and build trust among users. The theft of critical data can be catastrophic for customers and businesses alike. Malicious actors can abuse sensitive information and even steal users' identities. Additionally, companies can face legal penalties in the event of a data breach and suffer reputational harm.

Businesses can work to protect critical data by implementing software security techniques into their development life cycles. Applying security techniques enables organizations to proactively identify system vulnerabilities and better protect their software.

Authentication

Authentication is a fundamental aspect of software security, ensuring that only authorized users or systems can access the software and its resources. It involves verifying the identity of a user, device, or other entity before granting access to the system. Here are the key components and methods of authentication in software security:

1. Password-Based Authentication

Strength and Complexity: Users are required to create strong passwords that combine uppercase and lowercase letters, numbers, and special characters to resist brute-force attacks.

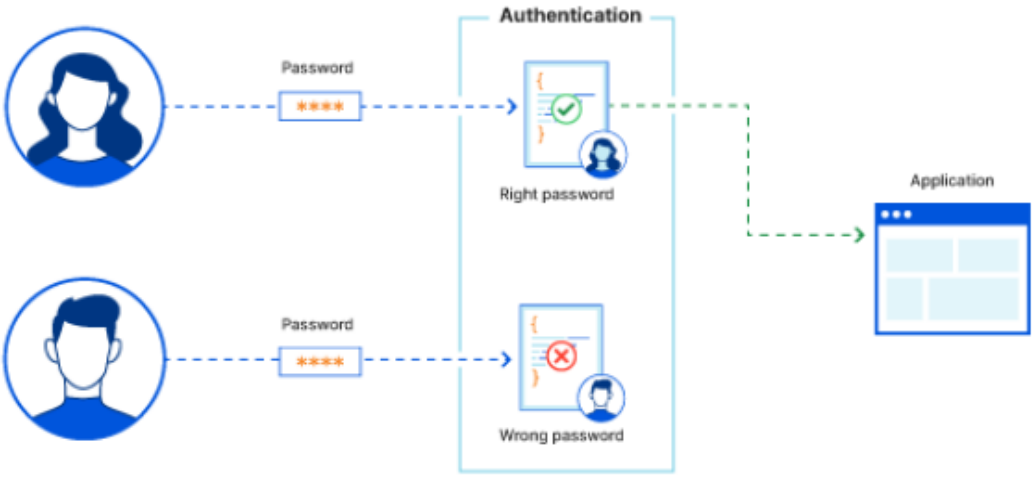
2. Multi-Factor Authentication (MFA)

• **Something You Know:** This is usually a password or PIN.

• **Something You Have:** A physical token, smartphone, or a one-time password (OTP) generated by an authenticator app.

• **Something You Are:** Biometric authentication, such as fingerprint, facial recognition, or iris scanning.

• MFA adds an additional layer of security by requiring two or more forms of authentication.



Access Rights

Access control policies are a fundamental component of software development that governs the permissions and restrictions placed on users accessing a system or its resources. These policies define the rules and guidelines for granting or denying access to different functionalities, data, or areas within the software. There are several types of access control policies that can be implemented in software development to manage and enforce access to resources. These policies determine how permissions are granted or denied based on various factors, such as user roles, attributes, or predefined security levels.

1. Role-Based Access Control (RBAC). In RBAC, access rights are assigned to users based on their roles within the system. For example, an administrator may have full access to all functionalities, while a regular user may only have access to specific features.

2. Attribute-Based Access Control (ABAC) is another type of access control policy that considers additional attributes or characteristics of users when granting or denying access. These attributes can include user location, time of access, device used, or any other relevant information.

Q1/

1. What is computer software?

A. A physical component of a computer
B. A set of instructions and documentation that tells a computer what to do
C. A type of hardware that controls the computer

D. A device used to store data
E. A tool for repairing computers

2. Which of the following is an example of an operating system?

A. Microsoft Word
B. Google Chrome
C. Mac OS
D. Adobe Photoshop
E. Fortnite

3. What is the primary purpose of software security?

A. To increase the speed of software
B. To protect software applications from attackers
C. To reduce the cost of software development
D. To improve the user interface of software
E. To make software compatible with all devices

4. When was the term "software" first used?

A. 1950s
B. Late 1960s
C. 1980s
D. Early 2000s
E. 1990s

5. What is firmware?

A. A type of hardware that cannot be updated
B. A piece of software that directly controls hardware

C. A type of malware that infects computers
D. A tool for creating software
E. A type of operating system

6. Why is secure software development important?

A. To make software more expensive
B. To prevent attackers from stealing sensitive information
C. To reduce the size of software files
D. To make software run faster
E. To increase the number of software users

7. What is the purpose of authentication in software security?

A. To increase the speed of the software
B. To verify the identity of a user or system before granting access
C. To improve the user interface of the software
D. To reduce the cost of software development
E. To make software compatible with all devices

8. Which of the following is NOT a component of Multi-Factor Authentication (MFA)?

A. Something you know
B. Something you have
C. Something you are
D. Something you want
E. A one-time password (OTP)

9. What is the purpose of strong and complex passwords?

A. To make it easier for users to remember their passwords
B. To resist brute-force attacks
C. To reduce the need for authentication
D. To make software run faster
E. To increase the number of users

10. What is Role-Based Access Control (RBAC)?

A. Access rights are assigned based on user location
B. Access rights are assigned based on user roles within the system
C. Access rights are assigned based on the time of access
D. Access rights are assigned based on the device used
E. Access rights are assigned randomly

11. Which of the following is an example of "Something You Have" in MFA?

A. A password
B. A fingerprint
C. A physical token
D. A username
E. A security question

12. What is Attribute-Based Access Control (ABAC)?

A. Access control based on user roles
B. Access control based on user location, time, or device
C. Access control based on the size of the software
D. Access control based on the cost of the software
E. Access control based on the speed of the software

13. Which of the following is a potential consequence of a data breach?

A. Increased software speed
B. Legal penalties and reputational harm
C. Reduced software cost
D. Improved user interface
E. Increased number of users

14. What is the main function of an operating system?

A. To perform specific tasks like word processing
B. To serve as a platform for running applications and control user interface tools
C. To directly control hardware components
D. To store sensitive data
E. To create software applications

15. Which of the following is an example of biometric authentication?

A. A password
B. A one-time password (OTP)
C. Fingerprint scanning
D. A physical token
E. A security question