جامعة المستقبل
AL MUSTAQBAL UNIVERSITY

كلية العلوم

قسم الأمن السيبراني

Lecture: (4)

Isolation, Least Privilege, Compartmentalization

Subject: software security

second Stage

Lecturer: Asst. Lecturer. Suha Alhussieny

Isolation

Isolation in software security refers to the practice of separating different components, processes, or data within a system to enhance security. By isolating these elements, potential security risks are contained, preventing them from spreading to other parts of the system. Isolation is a key strategy in reducing the attack surface and minimizing the impact of security breaches. Here's a Types **of Isolation** in software security:

1. **Process Isolation:** Ensuring that each process runs in its own memory space, separate from other processes. This prevents one process from accessing or interfering with the memory of another.
2. **Virtualization:** Each **Virtual Machines** VM runs its own operating system instance, isolated from other VMs on the same physical host. Hypervisors manage the isolation between VMs.
3. **Network Isolation:** Dividing a network into smaller, isolated segments or zones to control traffic flow and limit the spread of potential attacks. For example, isolating the internal network from the public-facing network.
4. **Privilege Isolation: Principle of Least Privilege (PoLP),** users and processes are granted the minimum level of access rights necessary to perform their tasks, ensuring that higher-privileged functions are isolated from lower-privileged ones.
5. **Database Isolation:** Ensuring that data from different users or tenants is kept separate, especially in multi-tenant environments like cloud services.

6.**Code Isolation:**

- **Module Isolation:** Structuring code into isolated modules or components with well-defined interfaces, limiting the impact of vulnerabilities within a single module.
- **Micro services:** A software architecture where applications are built as a collection of loosely coupled, independently deployable services, each running in its own isolated environment.
- **Benefits:** Enhances maintainability and security by containing vulnerabilities within specific components.

Least Privilege

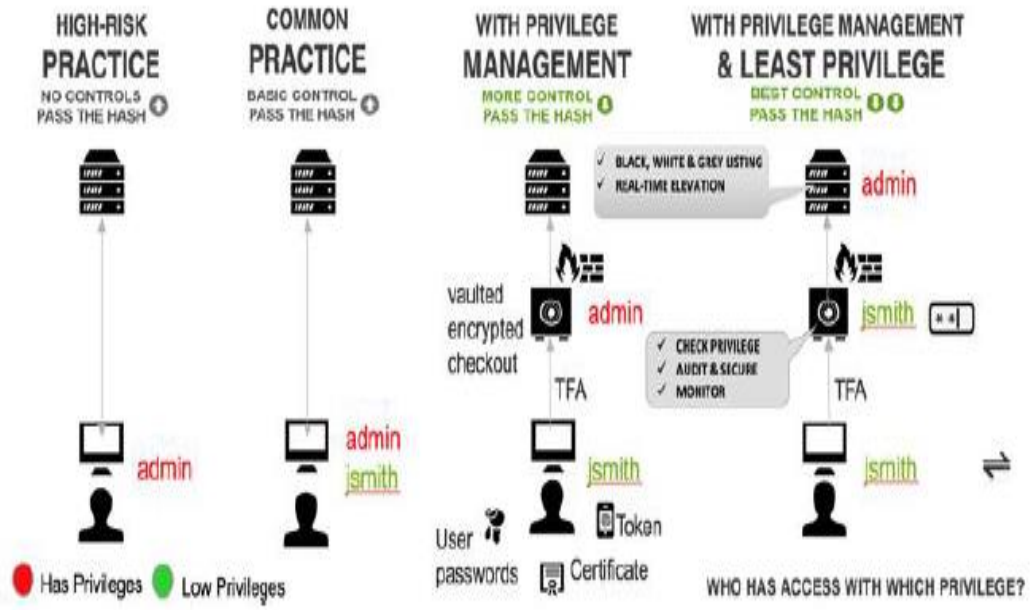
The Principle of Least Privilege (PoLP) is a fundamental concept in software security that advocates for granting users, systems, and processes the minimum level of access or privileges necessary to perform their required tasks. By limiting access rights, the potential attack surface is reduced, minimizing the risk of accidental or intentional misuse of privileges.

The goal is Least Privilege to reduce security risks by limiting the potential damage that could result from security breaches or errors. This minimizes the opportunities for malicious actors or malware to exploit elevated privileges.

Implementation Least Privilege in Different Contexts

- **User Accounts:**
  - ✓ Regular users should have access only to the files, applications, and systems needed for their job. Administrative privileges should be restricted to a few trusted individuals who need them to perform specific tasks.

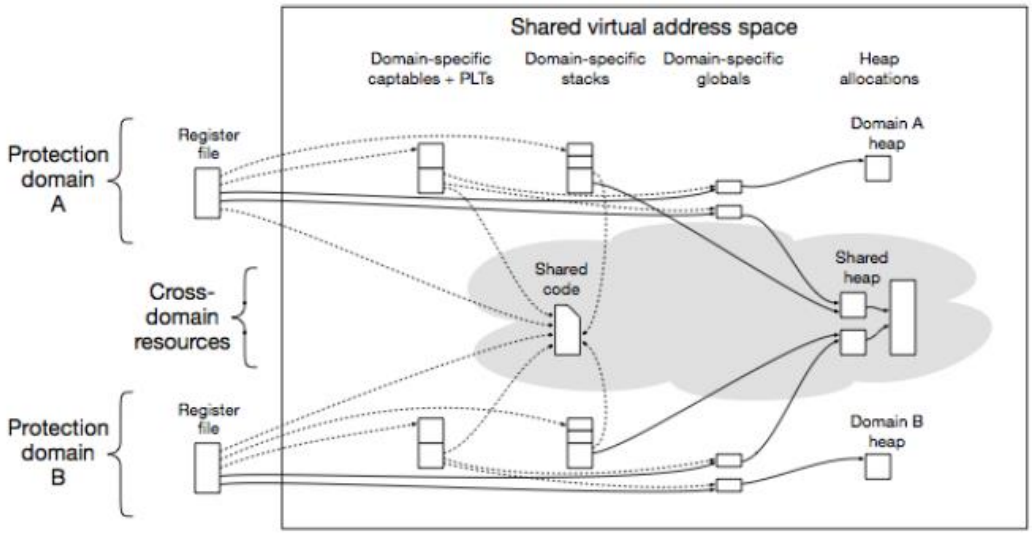
- **System Processes:**
  - ✓ System services and applications should run under dedicated service accounts with minimal privileges, rather than under accounts with full administrative rights.
- **Applications:**
  - ✓ Applications should request only the permissions necessary to perform their functions. For example, a messaging app should not require access to the device's camera unless it supports video calling.
- **Network Access:**
  - ✓ Network resources should be segmented, and access should be restricted based on the principle of least privilege, ensuring that users or systems can only access the parts of the network they need.



Compartmentalization

Compartmentalization in software security refers to the practice of dividing a system into distinct, isolated sections or compartments, each with specific functions, data, and access controls. The purpose is to limit the impact of a security breach by ensuring that if one compartment is compromised, the others remain unaffected. This approach enhances security by reducing the attack surface and containing potential threats. **Examples of Compartmentalization in Practice**

- **Military and Government Systems:**
  - ✓ Sensitive information in military and government systems is often compartmentalized based on classification levels (e.g., Confidential, Secret, Top Secret), with strict access controls and isolation between compartments.
- **Cloud Environments:**
  - ✓ In cloud computing, multitenant architectures use compartmentalization to ensure that each tenant's data and applications are isolated from others, protecting against cross-tenant data breaches.
- **Web Applications:**
  - ✓ Web applications often compartmentalize user sessions, isolating them from each other to prevent session hijacking and cross-site attacks.



H.W

Q1/

Isolation

1. **What is the primary goal of process isolation in software security?**
    - A. To increase system performance
    - B. To prevent one process from accessing or interfering with the memory of another
    - C. To reduce the cost of hardware
    - D. To allow processes to share memory space
    - E. To improve user interface design
2. **Which of the following is an example of network isolation?**

- A. Running multiple applications on the same server
- B. Dividing a network into smaller, isolated segments to control traffic flow
- C. Allowing all users to access all network resources
- D. Using a single password for all network devices
- E. Sharing network credentials publicly

3. **What is the role of a hypervisor in virtualization?**
   - A. To manage the isolation between virtual machines
   - B. To increase the speed of the physical host
   - C. To reduce the number of operating systems running
   - D. To allow all virtual machines to share the same memory space
   - E. To eliminate the need for network isolation
4. **Which of the following is a benefit of code isolation in software security?**
   - A. It reduces the need for user authentication
   - B. It enhances maintainability and security by containing vulnerabilities within specific components
   - C. It allows all users to access all parts of the code
   - D. It eliminates the need for network segmentation

- E. It increases the complexity of the system

5. **What is the purpose of database isolation in multi-tenant environments?**
   - A. To allow all users to access all data
   - B. To ensure that data from different users or tenants is kept separate
   - C. To reduce the cost of database management
   - D. To eliminate the need for user accounts
   - E. To increase the speed of database queries

Least Privilege

6. **What is the Principle of Least Privilege (PoLP)?**
   - A. Granting users full access to all system resources
   - B. Granting users, systems, and processes the minimum level of access necessary to perform their tasks
   - C. Allowing all users to have administrative privileges
   - D. Eliminating the need for user accounts
   - E. Increasing the attack surface of the system
7. **Which of the following is an example of implementing the Principle of Least Privilege for user accounts?**

- A. Granting all users administrative privileges
- B. Restricting administrative privileges to a few trusted individuals
- C. Allowing all users to access all files and applications
- D. Sharing user credentials publicly
- E. Eliminating the need for user authentication

8. **Why should system processes run under dedicated service accounts with minimal privileges?**
   - A. To increase the speed of the system
   - B. To reduce the risk of accidental or intentional misuse of privileges
   - C. To allow all processes to share the same memory space
   - D. To eliminate the need for network isolation
   - E. To reduce the cost of hardware
9. **Which of the following is an example of applying the Principle of Least Privilege to applications?**
   - A. Allowing a messaging app to access the device's camera even if it doesn't support video calling
   - B. Requesting only the permissions necessary for the app to perform its functions
   - C. Granting all apps full access to the device's resources

- D. Sharing app credentials publicly
- E. Eliminating the need for user authentication

10. **How does the Principle of Least Privilege apply to network access?**
    - A. By allowing all users to access all parts of the network
    - B. By segmenting network resources and restricting access based on necessity
    - C. By sharing network credentials publicly
    - D. By eliminating the need for user accounts
    - E. By increasing the attack surface of the network

Compartmentalization

11. **What is the primary purpose of compartmentalization in software security?**
    - A. To increase system performance
    - B. To limit the impact of a security breach by isolating sections of the system
    - C. To allow all users to access all parts of the system
    - D. To reduce the cost of hardware
    - E. To eliminate the need for user authentication

12. **Which of the following is an example of compartmentalization in military and government systems?**
    - A. Sharing sensitive information publicly
    - B. Compartmentalizing information based on classification levels with strict access controls
    - C. Allowing all users to access all classified information
    - D. Eliminating the need for access controls
    - E. Increasing the attack surface of the system

13. **How is compartmentalization used in cloud environments?**
    - A. By allowing all tenants to access each other's data
    - B. By isolating each tenant's data and applications from others
    - C. By eliminating the need for user accounts
    - D. By increasing the cost of cloud services
    - E. By reducing the need for network segmentation

14. **What is the benefit of compartmentalizing user sessions in web applications?**
    - A. To allow all users to access each other's sessions
    - B. To prevent session hijacking and cross-site attacks
    - C. To eliminate the need for user authentication

- D. To increase the complexity of the system
- E. To reduce the cost of web application development

15. **Which of the following is a key advantage of compartmentalization in software security?**
    - A. It increases the attack surface of the system
    - B. It reduces the impact of a security breach by containing threats within specific compartments
    - C. It allows all users to access all parts of the system
    - D. It eliminates the need for user accounts
    - E. It reduces the cost of hardware