

# 【作业1】 计算机安全十大准则

唐亚周 519021910804

Describe the computer security design principles and their implications.

1. **Economy of mechanism.** This principle stresses simplicity in the design and implementation of security measures.
2. **Fail-safe defaults.** This principle states that the default configuration of a system should have a conservative protection scheme.
3. **Complete mediation.** The idea behind this principle is that every access to a resource must be checked for compliance with a protection scheme.
4. **Open design.** According to this principle, the security architecture and design of a system should be made publicly available.
5. **Separation of privilege.** This principle dictates that multiple conditions should be required to achieve access to restricted resources or have a program perform some action.
6. **Least privilege.** Each program and user of a computer system should operate with the bare minimum privileges necessary to function properly.
7. **Least common mechanism.** In systems with multiple users, mechanisms allowing resources to be shared by more than one user should be minimized.
8. **Psychological acceptability.** This principle states that user interfaces should be well designed and intuitive, and all security-related settings should adhere to what an ordinary user might expect.
9. **Work factor.** According to this principle, the cost of circumventing a security mechanism should be compared with the resources of an attacker when designing a security scheme.
10. **Compromise recording.** Finally, this principle states that sometimes it is more desirable to record the details of an intrusion than to adopt more sophisticated measures to prevent it.