# Questions

1. In a few sentences, explain the security design goal of non-repudiation.
2. In a few sentences, explain the security design concept of anonymity.
3. For each of the following, explain how non-repudiation and anonymity may or may not apply.
   1. Use of an ATM (automated teller machine).
   2. Buying a movie ticket for an X-rated film.
   3. Purchasing an item at a retail store with cash.
4. Match each security design principle to its appropriate description.

|  |  |  |
| --- | --- | --- |
| **Security Design Principle** |  | **Matching Description** |
| Be reluctant to trust |  |  |
| Complete mediation |  |  |
| Compromise recording |  |  |
| Defend in depth |  |  |
| Economy of mechanism |  |  |
| Fail-safe defaults |  |  |
| Least common mechanism |  |  |
| Least privilege |  |  |
| Open design |  |  |
| Promote privacy |  |  |
| Psychological acceptability |  |  |
| Secure the weakest link |  |  |
| Separation of privilege |  |  |
| Use your resources |  |  |
| Work factor |  |  |

1. Be skeptical of security protections that are not within your software system (i.e., trust but verify).
2. Cost of compromising a security mechanism should be compared with the resources of an attacker when designing a security scheme.
3. Default setting/action should be to favor security over usability. When in doubt, deny access.
4. Each user and program should operate with minimum set of privileges necessary to accomplish the job. Every user should not have “admin” rights.
5. Every request to access data/system should be checked for adherence to a protection scheme. Strike a balance with performance (e.g., speed, power usage) and usability requirements.
6. It may be more desirable to record the details of an intrusion rather than designing more sophisticated prevention mechanisms.
7. Keep your design as simple as possible. Allows quality assurance methods the greatest chance of finding security vulnerabilities.
8. Minimize security mechanisms being shared/used by more than one user or system.
9. Publish your design for anyone to review. No one person is an expert in all things security-related!
10. Separate components of a system to reduce damage when a security breach occurs in any one component.
11. Suite of security mechanisms being used are only as good as the weakest security mechanism being used.
12. Talk to others about design choices you are making. Have experts with different backgrounds review your design.
13. User interfaces related to security mechanisms should be designed based on what a user expects.
14. Your design needs to consider types of personal information you are collecting from a user. Do you really need to persistently store this data? Do you really need to send this data over a network?
15. Your design should include redundancy and layers of defense.
16. What are the benefits and limitations of *complete mediation*?
    1. Benefits:
    2. Limitations:
17. When thinking about *compromise recording* and *secure the weakest link* :
    1. What do these have in common?
    2. How are these different?
18. When thinking about *separation of privilege* and *least privilege* :
    1. What do these have in common?
    2. How are these different?