Computer Security and Privacy (COM-301)

Week 2: Security Principles

Malware

- Rob accidentally downloaded a malware that leverages ambient authority. That malware uploaded all Rob's files (both on their laptop and accessible as shared folders) to a cloud. The company discovers later that during the same leak, documents in other departments, that Rob was not working on, also got leaked due to the malware.
- **Which security principle(s) were incorrectly applied by the company's system administrators that manage the shared folders and allowed the full leak?**
- Separation of Privilege
- Least Privilege
- Psychological Acceptability
- Fail-Safe Default

- **Least privilege –> incorrectly applied**: Rob's account had access to many more shared folders than his role required.
- **Separation of privilege –> incorrectly applied**: a single set of credentials was sufficient to access all of these folders.
- **Psychological acceptability –> not relevant**: the use of security measures was not the cause of the breach.
- **Fail-Safe Default –> not relevant**: the problem was not the default access setting, but the fact that Rob already had broad permissions.

PubliBike

After listening to the COM-301 lecture on Security Principles, you are enthusiastic about analysing the security of systems you use every day and to what extent they fulfil the eight main principles. You start by analysing the PubliBike system in which a registered user can rent a bike at a fixed hourly rate through a mobile application.

Which of the following statements is correct?

- The fact that anyone can download the mobile application from the app store satisfies the open design principle.
- The fact that I have to pay for every bike rental after I have returned it to a docking station satisfies the complete mediation principle.
- The fact that payment occurs after a bike rental satisfies the economy of mechanism principle.
- The fact that bikes are locked unless a user enters a valid code to unlock a bike satisfies the fail-safe defaults principle.

Correct answer:

- **Fail-Safe Defaults**: Bikes are locked by default and only unlock when a valid code is entered.

Wrong answers:

- **Open Design**: Publishing the application does not imply publishing its source code; in this case, the security of the system cannot be openly examined to verify that it is not based on secrecy.
- **Complete Mediation**: Paying after returning a bike is not an example of checking every access request.
- **Economy of Mechanism**: Payment timing does not relate to keeping the system design simple.

Hiding the Horcruxes

The Dark Lord Voldemort has created seven distinct horcruxes that he wishes to protect from being discovered. He decides to conceal each of the seven horcruxes in seven distinct vaults whose security mechanisms are only known to Voldemort himself. He selects his seven most loyal followers. He locks each horcrux in a vault and gives the key to one of these trusted followers. Then, the dark lord personally takes the vaults to seven hidden locations across the world. The trusted followers keep the key entrusted to them.

Among the following security principles, name two which hold in this system. Justify your answer.

- fail-safe default
- open design
- least privilege
- complete mediation
- separation of privilege

- **Least Privilege –> holds**: Each follower only has the key to one vault, limiting their access to a single horcrux.
- **Separation of Privilege –> holds**: Access to a horcrux requires two independent factors: the vault's location (known only to Voldemort) and the key (held by a follower).
- **Fail-Safe Default –> holds not**: The scenario does not describe a default-deny system that requires explicit permission.
- **Complete Mediation –> holds not**: Once someone has the key, access is not re-checked each time.
- **Open Design –> holds not**: The system's security relies on secrecy of the vault locations and mechanisms.