

Question 1: Scenarios (20 min)

In class we discussed 16 design principles for security:

- DP1: economy of mechanism
- DP2: fail-safe defaults
- DP3: complete mediation
- DP4: open design
- DP5: separation of privilege
- DP6: least privilege
- DP7: least common mechanism
- DP8: psychological acceptability
- DP9: time-tested tools
- DP10: evidence production
- DP11: remnant removal
- DP12: reluctant allocation
- DP13: security by design
- DP14: security is economics
- DP15: defence in depth
- DP16: know your adversary

For the following situations, identify which principle or principles are relevant.

1. A car has a valet key intended for valet drivers who park your car for you. The key opens the door and turns on the ignition, but it does not open the trunk or the glove compartment.
2. A 2D barcode on a print-at-home concert ticket is scanned before granting admittance.
3. Social insurance numbers are frequently used as a form of authentication (e.g., at a bank, to access tax data), but they were not originally for this purpose and are easily learned by others.
4. A Digital Rights Management (DRM) scheme is used to copy-protect media and seems secure until someone reverse engineers how it works.

5. A ground floor of a building has metal bars over the windows while the further floors do not.
6. A laptop owner encrypts their hard drive, uses a password with a lock screen, and a physical lock cord attached to their desk.
7. A mountain bike owner uses a metal cord through their wheels along with a U-lock for the frame.
8. A corporation maintains their tax records the required seven years and then shreds them.
9. A lock and key is used to secure most physical buildings.
10. An undercover police officer on a stakeout ignores a nearby call of distress.
11. A building with electric key card locking system opens all doors if the fire alarm is triggered.
12. A library records your name and the book you are withdrawing.

Question 2: Design Principles (25 min)

Consider the world of home security. People may have locks, keys, access codes, shared gates, shared entryways, guard, keyed elevators, camera, spare keys, hidden keys, someone to water the plants when on holiday, locked cabinets, hidden wall safes, outbuildings with padlocks, animal door flaps, etc.

Relate aspects of home security to the design principles discussed in class, either by following or by violating the principle.

Consider different access control mechanisms to the house, e.g., keys shared with others, keys that access different areas, animal door flaps, etc. Consider them as security mechanisms and describe the assumptions that are made in their context.