Computer Security and Privacy (COM-301)

Week 2: Security Principles

Interactive Problem Solving

Dragon Egg Security

Dany and Jorah decide to hide a dragon egg inside a crypt. The crypt has two locks and can be opened only if both locks get unlocked. Dany has the key to one lock and Jorah has the key to the other.

Question: For each of the following security principles, argue whether Dany and Jorah's mechanism design does or does not follow this principle?

(a) Open design.
(b) Least privilege.
(c) Complete mediation.
(d) Separation of privilege.

(a) Open design: Can be yes and no. Not discussed here. Whether there mechanism follows principle is orthogonal to how the mechanism is build.
(b) There is no least privilege, as once you open the crypt you can do anything with the egg.
(c) There is no complete mediation as only access is checked. Afterwards, any egg-security operation is not validated
(d) Separation of privilege: neither Dany nor Jorah, on their own, can breach the security policy.

Concert Security

Imagine the following: You are in charge of the entrance security for an intimate concert by Harry Styles. The organisers tell you that it is very important that only fans with a valid ticket enter the venue.

Question: Describe a security policy for this scenario. Clearly define the principals and assets of the system. What are the security properties you need to maintain?

Concert Security

A friend of yours, who has taken COM-301 last year, suggests you the following: " It's easy. Open only one door to the venue and hire one big, strong, guard to check the tickets."

You follow your friends advice. However, on the evening of the concert the guard has a cold. From time to time, he thus needs to sneeze. While sneezing, he is distracted and some fans without a ticket slip in.

Question: For each of the following security principles, argue whether your friend's mechanism design does or does not follow thisprinciple.

(a) Separation of Privilege
(b) Fail-safe default
(c) Economy of mechanism
(d) Least common mechanism

(a) There is no separation of privilege here. Only one door with a faulty mechanism.
(b) DOes not apply which is shown by the problem of the sick guard
(c)Yes, the mechanism is bad but it is simple (to analyse)
(d) No

A good Apple?

Back in 2021, Apple proposed a new system for CSAM (Child Sex & Abuse Material) detection. The method runs locally on all users iPhones scanning all photos the user wants to backup on iCloud. These photos are compared to a list of known CSAM images using complex advanced cryptography so that the list of known images can be kept encrypted. The comparison algorithm is perceptual hashing, a fuzzy hashing that also detects close images (e.g., rotated).

If the scanning detects more than 30 CSAM images, then the IDs of these images are reported to the cloud. An Apple employee revises these images and if indeed they are CSAM reports it to the corresponding authorities.

Question: Which security principles does this system follow/not follow?

Economy of mechanism: no, the mechanism is very complicated. It relies on complex cryptography + hashing algorithm. The TCB includes the phone OS, those providing the CSAM images, and the employees checking. All of them must behave correctly for the system to be secure. Hard to prove.

Separation of privilege: no, there are two steps in the system but in the end, there is no more than one **entity** doing security **decisions**. All depends on Apple.

Fail safe default: no, if the system fails, CSAM is not detected and can pass.
Note: privacy is important but it should be clear that the goal of the system is to detect CSAM-> fail safe arguing about "employee revises photos that are not CSAM" is not good.

Least common mechanism: no, all phones have the same iPhone. If the mechanism fails, everything fails.

Least Privilege: yes, if we think about the mechanism only accesses photos that would be backup. No, if we think about the mechanism only providing access to CSAM. While only CSAM are detected, the mechanism has access to all photos. Nothing says that the list of known images can change to find, e.g., LGBT material, or terrorist material, or political material. The scanning runs with high privileges

Open design: not in this slide. but no, the algorithm is not open, nor is the code. This is Apple

Complete mediation: not enough information in this slide, looks like it but we need more information on the system.

Psychological acceptability: not really, it is impossible for an average user to understand what are the security implications and when they are safe backing up images.