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.

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 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?