Computer Security and Privacy (COM-301)

Security Principles

Interactive exercises II

Sick guard security

To secure the entrance to an intimate concert of One Direction, the organizers decide that the best way to control the fans is to only open one door to the venue and hire one big, strong, guard to check the tickets.

However, the guard has a cold and from time to time, he needs to sneeze several times. During this time, fans without a ticket slip in. This mechanism is obviously not good and does not follow many principles; but which one does it follow?

(a) Separation of Privilege

(b) Fail-safe default

(c) Economy of mechanism

(d) Least common mechanism

(c) The mechanism is not good, but it is very simple.

(b) additional note on not fail safe. Example of what would be: door is always closed until the bouncer opens it.

Security fails

Scenario A) A security engineer is designing a system. To ensure that no unauthorized user can log into the system, he implements an access control mechanism in which the decision to grant access depends on the state of the operating system. This state is composed by thousands of variables (such as temperature of the system, time of the day, …). A hacker takes advantage of inconsistencies between these variables to get access to the system.

1) Name one computer security principle that has been violated to get to this situation.

2) Propose an alternative security mechanism that follows that principle

For example, economy of mechanism. Secure access is based on a very complex state. Can't be checked properly.

Alternative mechanism: base access on few well-understood that are not on the OS which is always very complex and hard to predict.

Security wins

Scenario B) 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.

1) Name one security principle which hold in this system

- complete mediation: the vault can only be opened with the key
- economy of mechanism: the mechanism is simple
- separation of privilege: unlocking each horcrux requires a key from the follower and a location from the dark lord
- psychological acceptability: the mechanism is intuitive

Security fails

Scenario C) A computer system uses the same port to serve access control and to download documents. When access control is not available for 10 minutes, the computer system allows users to access documents. A user starts the download of a very large file in order to gain access to the documents without valid credentials

1) Name one computer security principle that has been violated to get to this situation.

2) Propose an alternative security mechanism that follows that principle

Least common mechanism: all users use the same port, when one user blocks the port, the system is not available for the other users (availability is not achieved anymore)

Alternative: Separate the access control to another port. This way, even if files take long, access control is always accessible.

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 CSAM known 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. One authorized Apple employee revises these images and if indeed they are CSAM reports it to the corresponding authorities.

Which security principles does this system follow/not follow?

https://www.apple.com/child-safety/ -- by now this project has been discontinued

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 compares to the same database. 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.