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

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

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

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

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