Mini-Exam 1, Most Repeated Errors

September 15, 2021

General Advice

- Answer the question. Do not provide a mitigation to an attack if you are only asked about the attack. If the proposal is wrong it will result in negative points.
- Read the question carefully. If you are uncertain about details, spell this out clearly in your answer. For example, if you are not sure what are the assumptions about the threat model in the question, state in your answer how you interpreted the question.

Question: Security Principles

Strategy 1: "All invited participants will receive a badge before the start of the conference and only people carrying a badge will be allowed in. Guards securing the entries to the venue will check that every person entering the venue has a personalised badge. Furthermore, a list of invited participants is distributed to the guards and the guards will check the name of every person entering the venue in addition to the validity of badges."

Strategy 2: "Because climate activists are often young, no one below the age of 18 will be allowed into the venue and guards securing the entries to the venue will enforce this policy. Furthermore, there will be random checks by additional security guards patrolling the venue to ensure that activists who managed to sneak past the entry guards will be detected."

Error 1: Strategy 1 as specified follows a separation of privilege principle.

Many stated that Strategy 1 follows the separation of privilege principle because the entry guards will conduct two checks. This is arguable, however, because Consultant 1 suggests that these two checks are conducted by the same entity and so could easily be breached simultaneously. This would violate the separation of privilege principle which mandates that no security-critical action depends on one entity.

If the answer specified that the name list check was conducted through a separate ID document other than the name on the badge, or that the answer assumed that there was a separate group of guards at the entry, it was counted

as a correct answer. But this specification was important.

Error 2: Strategy 2 as specified does not follow the complete mediation principle.

Many argued that Strategy 2 does not follow the complete mediation principle because it follows a blacklist approach and the checks inside the venue are random.

In this case, both strategies satisfy complete mediation as under both strategies every request to enter the venue will go through a security check. The difference between the two strategies is in what property is checked. While Strategy 1 follows a fail-safe default principle and checks for a positive permission, Strategy 2 applies a blacklist approach. The age condition might not be the best way to filter out activist, however, it is applied following the complete mediation principle (Note "guards securing the entries to the venue will enforce this policy.").

Question: ACL and Capabilities

Error 1: ACL are easier to check at the entrance.

Many stated that ACL would be easier to check at the entrance of the room. Note that, when you are checking one permission (one student in one room), the check is **equally** easy in Capabilities and ACLs. The difference is when you want to know full rows (all permissions for one student – easier with capabilities) or full columns (all permissions for a room – easier with ACL).

Error 2: A student letting others enter or lending others their CAMIPRO is an instance of confused deputy.

Many stated that CAMIPRO-based access control is subject to confused deputy because students with rights to enter a room can let others come into the room. If the student with rights does this *willingly* there is no confusion. This is **not** a confused deputy, but a problem with the hardness of checking rights transference in this scenario!

To argue that there is a confused deputy case, you would need to explain that the student with the rights is tricked by another student that does not have the right to let them come in.

Question: Threat model

Error 1: Not specifying threat, vulnerability, or harm.

Some answer included all three without naming them. A major part of this question is identifying and distinguishing these three from each other. If you do not specify that a part of the response is threat, vulnerability or harm, then you will not get the point.

Error 2: Threat is the same as threat model.

Threat is something which can go wrong with the system, while threat model determines the capability of the adversary.