Grading Instructions Project E, Trusted Camera

History

2017-10-20 First version
2017-10-21 Corrected how to grade number of attacks, minimum raised to 8

General

When grading do not use your own report as baseline for comparison. Your own project work should have made you familiar with the problem and the way of thinking. Because this project has few parts where only one answer of approach is correct, it will be more challenging to grade this report than the project C on TPM. This guide is to give you guidance in the grading work. The project should have a number of mandatory parts

1. Front page, with group name at least. (1 page)
2. Description of your product and considered design requirements (0.5 page)
3. Assumptions for your product that affect security (0.5 page)
4. High-level architectural overview. (2-3 pages)
5. Security evaluation of the design and short summary (2 pages)

Pictures are excluded from the page count.

It is allowed if a report has more pages if these are appendices that function as reference in combination with other references. Appendices are not counted and you do not have to include these in your grading effort.

It is not necessary that section headings map exactly to the above parts. However it should be clear from the section headings where material of the said parts can be located. For example, Section 1 Product description, Section Design requirements and assumptions, etc.

When it comes to the size 25% more text is ok. 25% less text is not OK as with the given limits it becomes too short. 40% more text will cap result to end result 6.

Grading

Below follow 5 blocks with evaluation and grading instructions. These block give at most 26 points together. Divide the sum of the points and divide by 3 and use the integer part as the score, for example sum=25/3 = 8, 18/3 = 6, 20/3=6

In the below you cannot deduct more per block than the given max points for the blcok (Report structure is a block)

A Report structure – 2p

Check if the report contains the part that asked for and that the sectioning is such that the parts are rather easy to locate in the report.

If parts are missing do the following. If part 1 or part 2 is missing deduct 1 p for each. If other parts missing give 0 p. If parts are present but it is hard to identify the parts in the report deduct 1

B Description of your product and considered design requirements - 3p

There should be a short description of what the target customers for the TC are. 1P. These should be a list of considered requirements, deduct 1p if missing or lacking those that are later in the report used.. In case other than the given requirements are used there should be a motivation of these. Lacking motivation give a 1p penalty. If product use with its environment and people using it is not stated/described deduct 2p

C Assumptions for your product that affect security - 3p

It is unlikely that one does not need to make assumptions to make this project effort reasonable. On the other hand one can use so many assumptions that it the security is almost entirely addressed by assumptions. If one identifies the use of assumptions that are not listed deduct 1 p per missing named assumption with at most 3 deductions for this.

D High-level architectural overview - 9p

D1 General – 4p

A description of the components of the product and statement if they have security relevance. It is OK to opt out TPM and use only Trustzone, also the radio and SIM card can be left out

If components are later used and not mentioned in the overview deduct 2p. If life-cycle management is not mentioned deduct 1p. If TPM is used for storage of keys but need to handle of secret/auth values is not mentioned deduct 1p. Jtag is used but no protection of its used is mentioned deduct 2p.

Use of SRTP is skipped and one relies on LTE security deduct 2p.

D2 TOE and ST - 5p

If TOE or ST are not mentioned but their content is reflected in the report deduct 1p

If TOE is absent deduct 5, If ST is absent deduct 2p. If TOE or ST is unclear deduct 1p per unclear/incorrect formulated item.

E Security evaluation of the design and short summary – 9p

E1 General -5p

Description of how evaluation is done is lacking deduct 2p. Unclear description of how evaluation is supposed to work deduct 1p

Summary missing deduct 2p, Unclear about result/final rationale, deduct 1p. If life-cycle management is chosen as in report figure 2 (with repair) a security solution should be present otherwise deduct 1p.

At least 8 distinct threats should be mentioned and they should have a realistic nature (of happening) , if not deduct 1p for each threat missing, counting from 8 downwards, do not deduct more than 6.

E2 Evaluation -4p

Table missing where threats are given and covered by countermeasures or assumptions, deduct 4p.

Not all threats are covered, deduct 2p

There are more countermeasure than needed, deduct 2p

Countermeasure use parts/mechanisms that are not part architecture description, deduct 2p.