Group 06

SOSEC Assignment 2

https://www.commoncriteriaportal.org/files/ppfiles/ANSSI-CC-profil_PP-2012-01en.pdf

2020-09-11

Ranjana Ghimire
Justas Narusas
Efstathios Psyllakis
Oskar Elfving Söderström
Faith Onwumere
Motti Aimé

Group 06 Charter

2020-09-11

Member Roles and Responsibilities

Team Member	Roles/Responsibilities
All	Basic understanding of Common Criteria and protection Profiles and what they do
Ranjana Ghimire	- Read over chosen Policy Protection document - Find some strengths/weaknesses - Go over Common Criteria Chapter 7, General Model
Justas Narusas	- Read over chosen Policy Protection document - Find some strengths/weaknesses - Go over Common Criteria Chapter 9, Protection Profiles and Packages
Efstathios Psyllakis	- Read over chosen Policy Protection document - Find some strengths/weaknesses - Go over Common Criteria Chapter 6, Overview
Oskar Elfving Söderström	- Read over chosen Policy Protection document - Find some strengths/weaknesses - Go over Common Criteria Chapter 8, Tailoring Security Requirements
Faith Onwumere	- Read over chosen Policy Protection document - Find some strengths/weaknesses - Go over Common Criteria Chapter 10 B. Specification of Protection Profiles (pg 85,86,87, 92-97)
Aimé Motti	- Read over chosen Policy Protection document - Find some strengths/weaknesses - Go over Common Criteria Chapter 10 Evaluation Results (pg 59-64)

Time Allocation

Task	Hour allocation / person
Zoom discussion meeting for team charter and finalising the team charter on 09-11-2020 at 13:00	1 hr (Completed)
Going over the Common Criteria	1 hr 30 min(Completed)
Basic understanding of PP	1 hr 30 min(Completed)
Studying the allocated work for Secure Smartcard Reader with Human Interface Protection Profile	2 hr(Completed)
Overview and discussion of SAMM 2.0	30 min(Completed)
Studying step similarities/differences between SAMM and CC	1 hr(Completed)
Team meeting with Alan presenting all the findings on 09-15-2020 at 13:00	2 hr(Completed)
Documentation of the overall work on 09-15-2020 at 11 AM	2 hr(Completed)
Finalising the documentation on 09-15-2020 at 6 PM	30 min(Completed)
Total Time Spent:	**12hr**

What are the strengths (security or otherwise) of the product or PP as described in this document?

- The PP defines both technical and non-technical issues that can be present in the device, i.e. should be visible if the device has been tampered.
- Defined the TOE in not too ambiguous terms, but not so precise it would limit the usage of the PP too much.
- They have also defined some attack scenarios that has to be considered when developing a TOE meeting this PP.
- The PP highlights the protection of pin from disclose and modification.
- The PP makes sure of providing proper manual and guidelines to the consumers.
  (*ANSSI-CC-Profil_PP-2012-01en.Pdf*, 2011)

What are the weaknesses (security or otherwise) of the product or PP as described in this document? Anything in the ST or PP or in the CC itself that seems to you unusual, and why.

- TOE, used with smartcards having to be inserted in the TOE, now there exist smartcards using other techniques such as NFC, which are not included thus making it too specific of a PP.
- Does not discuss about virus attack when attached to the computer, eg. brute force attack, trojan attacks, ddos.
- The PP could have more specifications and limitations on what can enter the device from the connected PC.
  (*ANSSI-CC-Profil_PP-2012-01en.Pdf*, 2011)

Other thoughts on the PP to discuss:

- Have they managed to cover the important threats and attack scenarios?
  - No disclosure on important threats and the resolution to the mentioned scenario is also not satisfactory.
- We know that everything around the TOE can be potentially dangerous, because they are out of scope of the TOE, so can there be any vulnerabilities despite the very comprehensive checkpoints?
- Why is protection of the device limited only to the device while not to the potential attacks from the connected devices?
- Does not provide any cryptographic service unless specified.
  (*ANSSI-CC-Profil_PP-2012-01en.Pdf*, 2011)

Stemming from your work on an ST/PP, the group's reflections on the strengths and weaknesses of the CC as a whole.

- If using CC compared to i.e. SAMM as a starting point for development: does it need to have an existing defined PP for that product? While using a method like SAMM, the models can be applied when starting developing anything?
- CC provides a good framework for assurance, due to certification and such? (*CCPART1V3.1R5.Pdf*, 2017)

Embarrassing questions to CC proponent:

- The evaluation process is very costly, isn't this risking shutting out smaller projects/companies with less resources, ending up in fewer secure software?
- Other models support updates. In CC, every update of a product has to be evaluated and certified. Does this make organisations less prone to update software? (*CCPART1V3.1R5.Pdf*, 2017)

Embarrassing questions to SAMM proponent:

- How could we be sure that the software meets all our requirements when no external party reviews it, as they do in CC?
- With this fast paced developmental practice, no organization is willing to spend an extra amount in defining proper requirements and a proper operational defect management process. The basic criteria is if your code is written to just work in specific cases only then it doesn't vary between multiple operational platforms thus removing that dependency. Why is SAMM not adaptable to face paced and small scale projects? . (*OWASP SAMM v2.0 Released*, 2020)

References

CCPART1V3.1R5.pdf. (n.d.). Retrieved September 15, 2020, from https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf

OWASP SAMM v2.0 Released. (2020, September 15). https://owasp.org/2020/02/11/SAMM-v2.html

ANSSI-CC-profil_PP-2012-01en.pdf. (n.d.). Retrieved September 15, 2020, from https://www.commoncriteriaportal.org/files/ppfiles/ANSSI-CC-profil_PP-2012-01en.pdf