

Common Criteria: Security Target Level of Detail

*James Arnold/
Jean Petty*

28 September 2007

- Introduction
- Purpose of a Security Target
- Parts of a Security Target
- Level of Detail
- Summary
- Recommendations
- Conclusions

Note that the presentation was developed in accordance with Common Criteria version 3.1, but it substantially applies to version 2.3 as well.

- Common Criteria (CC) Security Targets (STs) are intended to describe security problems and the products, known as targets of evaluation (TOEs), that mitigate those problems.
- STs include several layers of description, including a top-level product/TOE overview, a security problem statement, security objectives, security requirements, and finally, a TOE summary specification (TSS) that describes the security functions that satisfy the requirements.
- The CC includes requirements designed to ensure that the various details are consistent and support each other adequately.
- However, beyond some specific points of reference found in the ST evaluation requirements and guidance found in CCv3.1 Part 1 Annex A, the CC does not specifically dictate the level of detail required throughout the ST.

- Due to a lack of specific guidance about lack of detail, it is common for developers, evaluators, and validators to disagree whether the detail present in a given Security Target (ST) is adequate.
- This presentation explores the appropriate level of detail that should be present throughout an ST, with emphasis on the description of how the product meets the identified requirements.

Purpose of a Security Target (ST)

- Each ST fulfills two general roles:
 - Before and during the evaluation, the ST specifies “what is to be evaluated”
 - After the evaluation, the ST specifies “what was evaluated”
- The ST is not a detailed nor complete specification of the TOE.
- The ST audience changes over time, from evaluators and validators to potential users of the TOE.

Parts of a Security Target (ST)

- In CCv3.1, an ST has seven major parts:
 - Introduction
 - Conformance claims
 - Security problem definition
 - Security objectives
 - Extended components definition
 - Security requirements
 - TOE summary specification
- While these parts are identified and defined in terms of guidance and requirements, an ST does not have to be organized in this manner.
- However, this presentation will address each of these parts in turn, without regard for how an ST might actually be organized with the corresponding information.

- The CC has specific requirements that must be satisfied for each part of the Security Target (ST).
 - This presentation does not represent those requirements, but rather, focuses on areas where the requirements are not specific about the required level of detail.
- The CCv3.1 Part 1 Annex A provides guidance for the specification of STs.
 - This presentation references that guidance, providing additional guidance where it seems necessary.
- Note that while this presentation addresses every part of the ST for completeness, most of the guidance offered is relative to the parts of the ST that have historically had the most problems:
 - The introduction (formerly, in CCv2.3, the TOE description)
 - The requirements
 - The TOE summary specification

- The Introduction in CCv3.1 includes much of the *Introduction* and *TOE description* of CCv2.3.
 - As such, it requires an appropriate introduction to the ST as well as a TOE overview and TOE description.
- CCv3.1 Part 1 Annex A Section A.4 provides good guidance for all parts of this section and no additional guidance seems necessary.
 - Note that the notion of logical and physical boundaries that created problems when evaluating Security Targets with CCv2.3 has been replaced in CCv3.1 to make it more clear:
 - Physical scope – what the TOE is
 - Logical scope – the security features of the TOE

- The conformance claims (of CCv3.1) were included in the *Introduction* in CCv2.3 and include:
 - A summary of Common Criteria conformance
 - Any Protection Profile (PP) claims
 - Any package (e.g., assurance level) claims
- CCv3.1 Part 1 Annex A Section A.5 provides good guidance for conformance claims.

- The security problem definition of CCv3.1 is essentially the same as the *TOE Security Environment* of CCv2.3.
- CCv3.1 Part 1 Annex A Section A.6 provides good guidance for the security problem definition.
 - Note that historically there have been disputes as to whether Organizational Security Policies (OSPs) had to be associated with an actual organization.
 - CCv3.1 resolves that issue by allowing that OSPs can be presumed to be imposed by a hypothetical organization.
 - While the guidance is good, it isn't especially clear that the security problem is what the TOE is intended to solve.
 - As such, the definition of the security problem should not extend to problems that may derive from the TOE itself.

Level of Detail – Security Objectives

- The security objectives of CCv3.1 and CCv2.3 are essentially the same, except that there is no longer a distinction between the IT and non-IT environment of the TOE in terms of objectives.
- CCv3.1 Part 1 Annex A Section A.7 provides good guidance for the security objectives.

- The extended components definition of CCv3.1 was essentially an aspect of the *Security Requirements* in CCv2.3.
- CCv3.1 Part 1 Annex A Section A.8 provides good guidance for the security objectives.
 - Note that the guidance is fairly brief, indicating that this part of the Security Target (ST) must define any extended components (but not the actual requirements).
 - Between this guidance and the requirements for this part of the ST, it seems clear what must be presented.

Level of Detail – Security Requirements



- The security requirements of CCv3.1 and CCv2.3 are essentially the same.
- CCv3.1 Part 1 Annex A Section A.9 provides useful guidance for the security requirements.
 - The guidance suggests that the requirements are an “exact” description of how the TOE is to be evaluated.
 - This is not true, since even though it is standardized, it is still informal and subject to interpretation.
 - A common problem today is that evaluators are often face with validation issues, insisting that the requirements are not detailed enough, and this guidance doesn’t mitigate that problem.
 - It should be more clear that the requirements do not have to include any specific implementation details.
 - The guidance suggests that requirements serve as a basis for comparing TOEs through their Security Targets.
 - This is good, though a concept not generally accepted among the validation community – who insist comparison is supported only via Protection Profiles.

Level of Detail – TOE Summary Specification



- The TOE summary specification (TSS) of CCv3.1 and CCv2.3 are essentially the same.
- TSS
 - Unfortunately, there is no guidance that might curtail the all-too-common level of detail problems related to this part of the ST.
- The Common Criteria indicates that the level of detail of this specification should enable potential consumers to understand the general form and implementation of the TOE.
 - This means that, for example, the Security Target (ST) might indicate that a password is used for authentication, but not that the ST should delve into how that password mechanism is actually implemented within the TOE.
 - The meaning of implementation in this context is ambiguous.

- A common criticism of the TOE summary specification (TSS) is that it describes *what* the TOE does and not *how* the TOE does it.
 - However, the distinction between “what” and “how” isn’t particularly helpful, since the actual meaning depends on perspective.
 - For example,
 - The requirements define what must be met, and the TSS summarizes how that is done.
 - The TSS summarizes what the TOE does, and the underlying design documents explain how that happens.
 - In general, when this comment appears, it really means, quite simply, that the reviewer wants more detail.
 - What additional detail is being requested, and is that appropriate?

Level of Detail – TOE Summary Specification



- The following guidance is offered for specification of the TOE summary specification (TSS) at an appropriate level of detail.
 - The TSS must have at least as much detail as the corresponding requirements.
 - If the requirements are sufficiently detailed, repeating or paraphrasing the requirements should suffice.
 - The TSS generally should be limited to details about the TOE that could be perceived or determined by a user of the TOE.
 - For example:
 - Users would know how they authenticate themselves.
 - Users could figure out the rules for access decisions, though they may be unaware of how the applicable attributes are actually realized inside the TOE.
 - Users should be aware of the cryptographic algorithm used by the TOE when they interact with the TOE using non-TOE applications, but they might be unaware of algorithms used exclusively between TOE components.
 - In other words, the TSS should focus on user-visible details of how the TOE works to fulfill the requirements.

Level of Detail – Rationale

- Note that rationale has not been identified as a part of the ST since in CCv3.1 rationale is included within each part that requires rationale, rather than leaving it to the end of the Security Target.
- In each case, CCv3.1 Part 1 Annex A provides useful guidance for the corresponding rationale.

- CCv3.1 Part 1 Annex A represents a good improvement in guidance from the corresponding CCv2.3 Part 1 Annex C.
- However, most issues regarding level of detail have been related to the TOE summary specification, and CCv3.1 actually provides less guidance than CCv2.3 in this regard.

Recommendations

- CCv3.1 Part 1 Annex A should generally be used as a guide for appropriately developing the content of Security Targets (STs).
- This presentation has offered guidance that should be applied consistently when developing STs:
 - Security problem definitions should be limited to the problem the TOE is intended to solve, and the ST author, evaluators and validators should not be looking to the TOE in order to identify additional problems to specify.
 - Requirements should be specified without TOE-specific implementation details, in order to promote comparability and increase the likelihood of reusing requirements from ST to ST.
 - The TSS should be presented to address the requirements while being limited to user-visible design details, where possible.
- Furthermore, the CCv3.1 Part 1 Annex A should be revised to extend the guidance to help mitigate historical problems.

Conclusions

- For the most part, CCv3.1 Part 1 Annex A serves as a useful guide when determining how to develop a suitable Security Target.
- The most common problems related to level of detail have not been addressed in CCv3.1.
 - Without additional agreed upon guidance, those problems will continue to plague evaluations.

Contact



James Arnold

SAIC Accredited Testing & Evaluation Labs
AVP/Technical Director

James.L.Arnold.Jr@saic.com

Jean Petty

SAIC Accredited Testing & Evaluation Labs
Senior Product Evaluator

Jean.E.Petty@saic.com

<http://www.saic.com/infosec/cctl.html>