French Scheme CSPN to CC Evaluation

Antoine COUTANT
ITSEF AMOSSYS
4 bis allée du bâtiment 35000 Rennes
antoine.coutant@amossys.fr

Abstract. Since 2008, French certification body created a new scheme for a specific evaluation: CSPN evaluation. For a target of evaluation (TOE), this French certification requires to analyse its security target, test its compliance and perform an intrusion tests in a constrained time. So, this evaluation is performed within certain time and workload constraints so as to meet the requirements for mastering costs and time limits. The goal is to attest that a product (target of evaluation) successfully passed an evaluation by ANSSI licensed evaluation facility.

This kind of evaluation is conducted under the terms of the conformity analysis (verify that a product is conform to its security specifications, see a product as a whole to perform relevant analyses) and analysis of efficiency (rate the theoretical strength of the security functions and mechanisms, identify vulnerabilities).

This paper focuses mainly on introducing the CSPN evaluation and briefly explaining the difference between CSPN and Common Criteria evaluation. Finally, we’ll see that these two schemes are complementary and can be used consecutively.

Keywords: CSPN, CC evaluation

1 Introduction

CSPN\textsuperscript{1} evaluation is a methodology created by the French certification body (called ANSSI). This scheme is the result of a pragmatic response to the civil market needs. Indeed, Common Criteria (i.e. CC) are flexible and robust guides for specifications and requirements of security assurances. CC can provide a methodological evaluation without specific requirements concerning the technical aspect. However, CC evaluation can become a real headache without prior delimitation of the TOE (Target Of Evaluation) functional scope. In addition, security products have heterogeneous and complex basic mechanisms, often beyond the normative framework and more and more integrated with the operating system or the operating environment.

\footnote{\textit{Certification de Sécurité de Premier Niveau} which can be translated by First Level Security Certification}
The implementation of the CSPN scheme meets the needs of the evaluation market for civil security products (constrained time suitable for products versioning, cost-optimized) and also purely technical needs such as technical expertise methodological completeness. The CSPN takes also into account recommendation by French deputy Lasbordes [5].

CSPN certification (implemented on a trial basis from May 2008 to May 2011) is based on criteria [1] and methodology [2] developed by French certification body. The main objective is to verify that a product meets its security requirements.

In brief, the objectives of the CSPN evaluation tasks are:

- Verify that the product is compliant with its security specifications;
- Theoretically rate the mechanisms and list the known vulnerabilities of products of the same type;
- Test the product to try to bypass its security functions.

## 2 CSPN Scheme

To limit functional scope, ANSSI defined categories of products to be evaluated. Procedure for CSPN evaluation [3] defines the following categories (a product may be associated with one or more of these technical fields):

- Intrusion detection;
- Anti-virus and protection against malicious codes;
- Firewall;
- Data deletion;
- Administration security and supervision;
- Identification, authentication and access control;
- Secure communication;
- Secure messaging;
- Secure storage;
- Embedded hardware and software.

This certification process includes sponsor(s), evaluation facility (ITSEF\(^2\) or evaluation facility licensed by the ANSSI in one or more technical areas of expertise), ANSSI certification body and possibly the developers of the product submitted for evaluation.

CSPN is intended to conduct evaluations in a constrained time, thus limiting sponsor budget and, most importantly, adapting the product development life-cycle to the civil market. The sponsor is responsible for providing the security target of the product, the product itself and the product’s documentation if available. If essential security features are implemented using cryptographic mechanisms, the sponsor must ensure that the documentation for these mechanisms is available ([4]).

\(^2\) Information Technology Security Evaluation Facility
The application of this methodology emphasizes technical expertise (balance efficacy/compliance functions) without neglecting methodological aspects. Laboratories responsible for these evaluations are licensed by ANSSI attesting both their competence on the specific technological building blocks (reverse engineering, cryptography, intrusion detection, network security,. . .) but also their independence.

It should be noted that ANSSI may refuse a certification from a sponsor if the product does not implement security functions, has an incomplete security target (not conform or obviously misleading), is too complex to be evaluated, uses cryptographic algorithms not compliant to the standard. . .ANSSI issues a certificate with french scope in light of an Evaluation Technical Report (ETR) issued by a licensed laboratory (ETR is the document containing the results of the evaluation).

The input documents for this work are:

- The security target of the TOE;
- The TOE in the version chosen for the evaluation;
- The public documentation of the evaluated product;
- Installation, configuration and administration manuals;
- The cryptographic specifications of the TOE (if applicable);
- The source code for cryptographic mechanisms of the TOE (if applicable).

Obviously, the laboratory conducting the evaluation must have access to the TOE and to test equipments if they are specific or dedicated. The issued evaluation document is the ETR and the plan is fixed in [2].

The performance of the evaluation relies on the existing documentation, public vulnerability bases to test known vulnerabilities and the product itself (installed on a test platform that is as representative as possible of the foreseen usage environment).

The evaluation process is divided into nine phases described below.

2.1 Step #1 - Security Target Analysis

The evaluator should verify, in detail, that the security target contains the expected elements identified in the ANSSI methodology [2]. The required contents of a security target are:

1. An unambiguous identification of the product to evaluate (the TOE);
2. A product rationale describing in natural language for what purpose the product was designed, by whom and in what context it is supposed to be used;
3. The precise technical environment where the product runs/operates (computer model, operating system, . . .);
4. The sensitive assets that the product must protect;
5. Protection offered against identified threats;
6. Security functions implemented by the product to counter identified threats (these functions will be subject to evaluation).
2.2 Step #2 - TOE Installation

The installation is done following the documentation provided by the sponsor. As a CC evaluation, the architecture of the platform evaluation is consistent with that proposed in the Security Target. The main objective of this task is identify non-compliances with the provided documentation, confirm that documentation is clear and unambiguous, identify any particular parameterization of the underlying system.

2.3 Step #3 - Analysis of compliance

The objective of this task is verify that the product is assessed according to its specifications. According with the CSPN evaluation process, the compliance study will be based on an analysis of existing documentation to advise on its readability and completeness, compliance testing of security functions identified in the Security Target and a review of source code (if applicable). The documents to be analyzed are mainly those provided by a developer and/or sponsor. The evaluator should identify the level of documentation features.

This step will also assess the security of programming code to ensure that rules of good practice, in terms of specification and design, have been met (use consistent naming conventions, structure and modularity for source code, clarity and presence of relevant comments).

2.4 Step #4 - Resistance Analysis for Functions and Mechanisms

There are two ways to define mechanism robustness:

- **Theoretical rating.** This phase measures the efficiency and robustness of theoretical mechanisms specified by the TOE. Typically, for cryptographic mechanisms, a known quantitative metric exists to rate the theoretical robustness of different algorithms (e.g.: based on the computational complexity).

- **Empirical rating.** This task measures the actual resistance for mechanisms specified by the target of evaluation. Like the previous step, this task is performed in both black box and white box through code review.

The evaluator will have to identify mechanisms implementing the security features of the evaluated product and analyze the operation of each mechanism. The evaluator will have to provide a listing of each mechanism. Thus, the evaluator can estimate the strength of functions based on the mechanisms and the overall strength of the product in terms of security.

2.5 Step #5 - Vulnerability Analysis

Evaluator must identify known vulnerabilities (intrinsic, constructional, operational) based on their own skills and the exploitation of vulnerability databases.
The task is to extract relevant vulnerabilities and verify whether and how they can be exploited. Two types can be addressed: specific to the product ones and generic ones, potentially applicable. The objective is to identify vulnerabilities to evaluated product (not with in an official patch, or a workaround to limit effects of the vulnerability), identify known vulnerabilities for products in the same category, implement, test and validate some vulnerabilities (according to feasibility, operability, no patch...).

This vulnerability synthesis will then identify those applicable to the audited code. The identification of vulnerabilities will be based on a three-step process:

1. Identification of public vulnerabilities;
2. Architecture and source code analysis (emphasis on critical functions);
3. Use of static analysis and test code tools by generating random data (fuzzing).

2.6 Step #6 - Ease of Use

For this step, the evaluator must identify when the product can be configured or used in any unsafe way, identify possible non-intrinsically safe functionalities that should not be used if they contribute to lead to an exploitable vulnerability. Finally, evaluator provides, when possible, recommendations for safe use of the TOE despite its potential vulnerabilities.

2.7 Step #7 - Evaluation of Cryptographic Mechanisms (if applicable)

Cryptographic mechanisms are evaluated in relation with ANSSI cryptology lab. This step has two axes:

- Check compliance of cryptographic mechanisms to ANSSI cryptographic standard requirements. This verification is done by analyzing the documentation which must contain at least the description of cryptographic functions, reference algorithms, key size, key distribution, key generation, key transmission, the description of pretreatment before encryption, the description of post-processing after encryption;
- Check implementation conformity of these mechanisms in relation to their description by comparing product results to a reference implementation and analyze source code with optionally unit tests of some functions.

2.8 Step #8 - Developers Interview (optional)

Wherever possible (and if necessary), evaluator contacts product developers. The main goal of these discussions is to retrieve or dig additional information or some interesting points that are not detailed in the documentation provided with the product.
2.9 Step #9 - Synthesis

Evaluator writes an expert opinion which summarizes obtained results during these different steps. This summary is addressed for technical readers.

3 CSPN to CC Evaluation

3.1 CSPN feedbacks

According to CSPN scheme emitted by ANSSI, the necessary workload for this analysis is 25 man days with 10 man days added if the product implements cryptographic mechanisms. The time limit is 8 calendar weeks. For a CSPN, the average time is approximately 2 months while for a CC evaluation, the average time is 1 year. The CSPN certification provides useful recommendations for use to overcome the possible limitations of an evaluated product.

Actually, the ratio of successful CSPN evaluations is about 50%. Main conclusion of these evaluations are that developers tend to focus on their core business and do not provide a comprehensive security in the design. Thus, many vulnerabilities (design, construction or operation) can be identified by laboratories performing CSPN. This scheme is selective enough to filter out the less safe products, it provides a good overview of the security level for security products, offers good guarantees of success for a developer (or sponsor) wishing to target a CC certification but has yet to evolve to facilitate the expertise reproducibility.

It can be advised, for the latter, that it should be necessary to develop a specific methodology for each category as well as an industrialized conformity and vulnerability analyzes. Indeed, for example, the needs of CSPN tasks for an application developed in Java are totally different than a digital tablet. Today, the results of different CSPN certification tend to this conclusion.

3.2 Two complementary evaluations

The evaluation approach according to Common Criteria starts with the Security Target Evaluation and continues with the Product Evaluation which can be divided in two parts: development documents with source code analysis (if applicable) and product testing (conformity, efficiency, vulnerabilities). Results are also described on an ETR. This document is used to emit the certificate provided by certification body. The figure below (figure 1) is a generic example of CC evaluation.

Security target (ST) evaluation is a prerequisite for all others activities. Indeed, ST is the reference document for evaluator and mandatory to understand the following steps for the evaluation. In practice, security target is used and controlled throughout the evaluation. For example, development analysis and life-cycle are linked: source management can show the used modularity approach. User documentation analysis is done in parallel to these two tasks. Finally, test analysis (developer tests plan) and vulnerabilities analysis are strongly linked.
The following table draws a parallel between concerned Common Criteria classes and CSPN works.

<table>
<thead>
<tr>
<th>CC classes</th>
<th>CSPN works</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASE</td>
<td>Security Target Analysis</td>
</tr>
<tr>
<td>AGD_OPE</td>
<td>Ease of Use</td>
</tr>
<tr>
<td>AGD_PRE</td>
<td>TOE Installation</td>
</tr>
<tr>
<td>ATE_IND</td>
<td>Analysis of compliance</td>
</tr>
<tr>
<td>AVA_VAN</td>
<td>Resistance Analysis</td>
</tr>
<tr>
<td></td>
<td>Vulnerability Analysis</td>
</tr>
<tr>
<td></td>
<td>Cryptographic Evaluation</td>
</tr>
</tbody>
</table>

A Common Criteria evaluation, as well as the CSPN, aims to ensure that the security services announced by a TOE are actually achieved. There are similarities between entries of these two types of evaluation. Four basic proof elements are the target of evaluation, the scope of evaluation, guides (use and/or administration) and the expression of security functions. In both evaluation schemes, these elements help an evaluator to understand the TOE, help his analysis and to prepare its final report. Vulnerability research, testing and source code audit (if applicable) are seminal works of the evaluation activity.

Common Criteria provide an additional perspective on matters relating to the TOE development (life-cycle, development environment, . . . ) or the shape of which is exposed the security issue (for example, no SFR\(^3\) definition for CSPN

\(^3\) Security Functional Requirements
works). This finding helps to understand the form of inclusion between CSPN and CC evaluation (at constant perimeter).

In the practice, we can observe that CSPN works done before CC evaluation are intended to reduce effects for an inadequate consideration of the security issue by the TOE and, finally, prepare the TOE to a future analysis on the background with Common Criteria.

Moreover, in this context, it is possible to reduce from 20 to 30% the cost of a CC evaluation, following a CSPN evaluation, on the same product. This solution has already been successfully by ITSEF with clients who have chosen to begin their certification process by a CSPN in order to progress to CC.

4 Conclusion

The CSPN approach is complementary to Common Criteria evaluation. The philosophy is the "quick-win" so reliable results in constrained time. Analyzes are primarily intended to ensure the robustness of a TOE.

For a developer and/or sponsor willing to begin a certification process, CSPN works followed by CC works are a good compromise for a certificate as soon as possible. Indeed, CSPN works can "roughing" a TOE by addressing vulnerabilities within constrained time. Following CSPN works, a developer can potentially improve the security of its own product (based on CSPN analysis) before starting the CC process which will focus on life-cycle development, architecture,

CSPN scheme is a methodology focused primarily on technical side allowing to have a relative confidence in a product. CSPN certificate certifies that a product has successfully passed an evaluation by a laboratory licensed by the French certification body (ANSSI). This scheme is characterized by balanced analytical works between efficiency and compliance, evaluation tasks completed in a constrained time, the opportunity to conduct an evaluation without strong involvement for developer and, at the end, a certificate with national validity range which is issued by ANSSI.

However, it appears that, in a (near?) future, specific methodologies according to analyzed products must be implemented. This will streamline workloads on the product analyzed.

References