Some limits of Common Criteria certification

DUSART Pierre
XLIM - UMR CNRS 6172,
Université de Limoges - Faculté des Sciences et Techniques,
123 avenue Albert Thomas, 87060 Limoges, France
pierre.dusart@unilim.fr

SAUVERON Damien
XLIM - UMR CNRS 6172,
Université de Limoges - Faculté des Sciences et Techniques,
123 avenue Albert Thomas, 87060 Limoges, France
damien.sauveron@unilim.fr

TAI-HOON Kim
Dept. of Multimedia, Hannam University,
133 Ojeong-dong, Daedeok-gu, Daejeon, 306-819, Korea
taihoonn@hnu.kr

Abstract

The Common Criteria evaluation and certification is one of the most commonly used process to improve the trust in the security of evaluated products. Nevertheless this methodology has a lot of problems and side-effects that lead to limitations of which the end-user should be aware. The aim of this paper is to develop some of these limits.

1. Introduction

Nowadays whereas the security concerns are ubiquitous, users want to be confident of security of the products which they use.

To claim that a product is secure is not an enough proof to provide trust for the user of this product. More formal processes should be applied to check the security level that product provider thinks to reach and to maintain a chain of trust from the manufacturer to the user (banks, mobile phone companies, end-user, etc.). Indeed, without this assurance there would be serious economic risks for information processing systems which are essential in the day to day life (payment cards for the banking structure, SIM card in the world of mobile telephony, health card, protection of the networks with the firewalls, etc.). To satisfy the need of trust in the security of the IT products, he industrialists (with the help of governments) have thus set up the mechanisms of control to ensure such a chain of trust For example in the world of the IT products, the security can be assessed and ensured through methodologies of evaluations/certification like the Common Criteria (CC – ISO 15408) [1, 2, 3] or ITSEC [4]. The paper will focus on the most commonly used : the Common Criteria. Despite the positive aspects of this methodology, it will be shown that there are some limitations that could be dangerous if the user is not aware of them. The aim of this paper is thus to briefly point some limits of common criteria.

The paper follows this organization. Section 2 presents why the current schemes of security certification have some interesting aspects. Then, an overview of the operation and

the context of the certification scheme according to Common Criteria are given section 3. Section 4 illustrates few limits of the CC security assurance scheme in the current state.

2. Benefits of the CC certification

For the manufacturer, the main goal of security evaluation is to obtain a degree (CC certificate) which validates the security level of his product. Although getting this certificate is prestigious, the security benefits are real. More and more manufacturers follow the Common Criteria approach to improve their product quality. The first benefit is clearly for marketing and business: an evaluated product will be easily sold than a non evaluated one. The certificate is an advantage on the competitive market. Moreover some specialized markets (banking for example)need a minimal security level for theirs products (*e.g.* high security level, noted EAL4+, for EMV credit cards).Hence manufacturers are inclined (even obligated) to prove the security quality to access to the market. The chosen products are better distributed and sold. Hence the second benefit is the access to closed or specialized markets. The evaluation process is completely independent and conform to a methodology (CEM [5]). An evaluator team works on product, security rational and documentation to hunt an error or a security fault. This third benefit is that the end-user could expect (since the evaluation process tries to mitigate the security threats in the product). For high security levels, audits complete the global vision of quality production. With this agreement the manufacturer is confident that his approach is correct. If not, he can correct the faults with the help of the evaluation report. This analysis is not free but it's only a key to access to security market and prove the card security. The advantages of certification are:

• to certify a minimal level of confidence for security of IT product (confidentiality, integrity, availability);

• to allow the customers to compare the various products on the market in a objective way;• to allow the manufacturers to prove their competence, to make a marketing argument and so to widen their markets;

• to allow the governmental certification bodies to make sure that products used in their countries are secured and that, consequently, there is no major risk of attacks against their IT systems. If, as we have just seen it, the security certification has advantages, the perverse corollary is that any initiative of certification allows the manufacturer to clear its responsibility in case of discovery of problems. The level of security (*i.e.* the assurance level) is chosen by the one who requests the certificate according to the demand of the market, the state of the art and the trust that he puts in his product and his teams. The company chooses the limits in terms of perimeter and potential of attack to its product in a document called Security Target (ST). The product is then assessed according to a scheme of certification, presented in the following section.

3. Short overview of the CC-based certification scheme

The process of certification is a complex procedure involving several independent actors:

• the initiator of the evaluation who wishes to obtain a certificate for its product or its system of Information Technology (IT);

• the evaluation center (*i.e.* ITSEF: Information Technology Security Evaluation Facility) which manages the tasks of evaluation of the security of the product according to the methodology chosen by the initiator(*e.g.* the Common Criteria or ITSEC), of the level of

assurance chosen by the initiator, the elements of proof brought by the initiator and its own technical expertise;

• the certification body which evaluates the technical relevance of reports written by the evaluation center and which in view of the Evaluation Report, decides or not to issue the certificate.

In every step, elements of proof are produced to guarantee the good progress of the evaluation, the exhaustiveness and the quality of the works led by the evaluation center. So the certificate of an IT product has for vocation to establish the minimum reliable security level of the product (that is the level of assurance) that a customer (banks, phone operators, etc.) can have.

To develop the certification of IT products but also to guarantee the trust in their system of certification, the administrators of certification schemes of several countries made agreements of mutual recognition of certificates emitted by them at the international level.

3.1. The French scheme

The French scheme follows an organization rather similar to the one that we have just described higher. It is presented in figure 1. The certification body is a governmental body called "Direction Centrale de la Sécurité des Systèmes d'Information" (DCSSI) [6]. This body belongs in fact to the "Secrétariat Général de la Défense Nationale" (SGDN) which is a service placed directly under the responsability of the French Prime Minister. Thus, it is the DCSSI which delivers the approval to an evaluation center on its demand.

To obtain this approval the ITSEFs have to set up very strict policies of security to guarantee the safety of the information which they manipulate. So, the access to office must be checked, documents must be kept in safes, the engaged staffs must be declared to the SGDN to undergo possible inquiries of morality, etc. In other words, all the means to guarantee a confidential level like security Defense one must be operated. Furthermore to be authorized to perform an evaluation, the ITSEFs must be accredited by the accreditation body, the COFRAC (French Committee of Accreditation) [7], for all the aspects connected to Quality. Indeed, we saw previously that during an evaluation, there was certain number of proofs which were produced by the evaluation center; so that they can be verified by the body of certification, it is necessary that the quality of these proofs is also checked (*e.g.* tools have to be calibrated, without that, the measures are false and thus the results are not reproducible).

Products certified within the French scheme benefit from European mutual recognition agreement: SOG-IS who allows the recognition between the signatory states of a certificate delivered by any certification authority. There is also an international mutual agreement of recognition according to the Common Criteria: CC-MRA (Common Criteria Mutual Recognition Arrangement). He allows the recognition, by the signatory countries of the agreement, of certificates delivered by certification schemes following the Common Criteria. The mutual recognition applies until the EAL4 evaluation level.

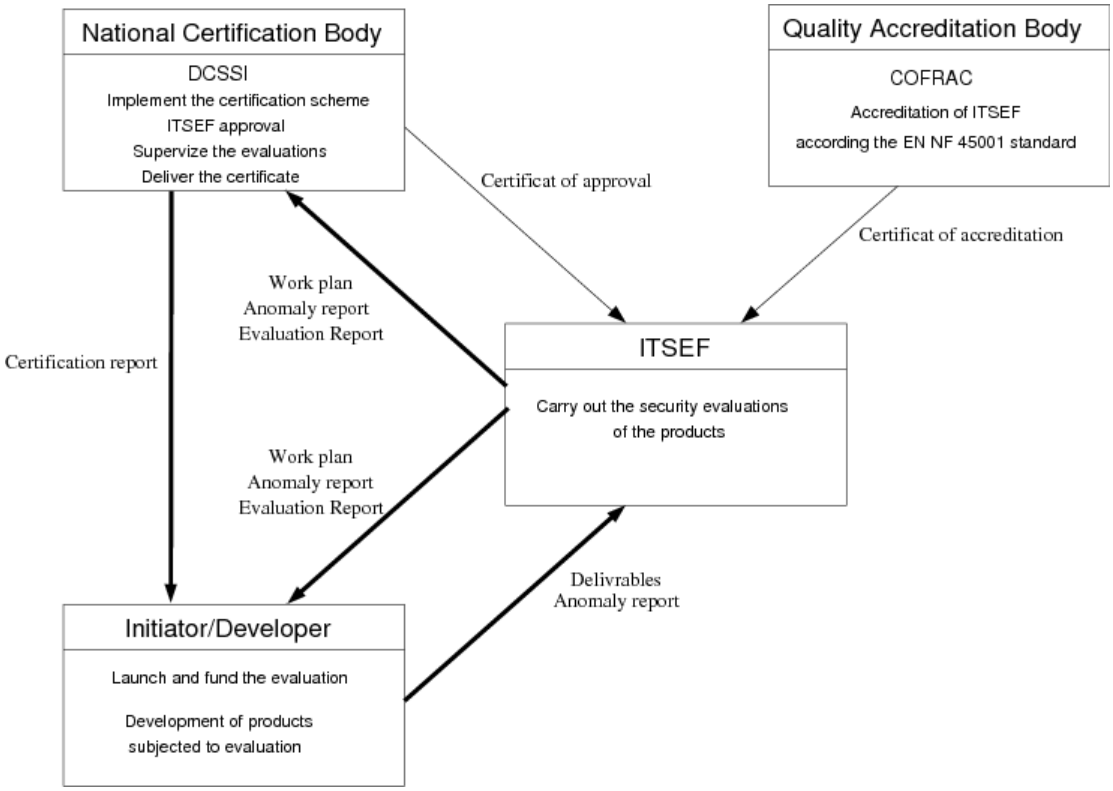

Figure 1: Roles of various actors and exchanges of information.

3.2. Common Criteria

The Common Criteria (CC) [8] is a standard which has for vocation to be used as base for the evaluation of the properties of security of products and systems of Information Technologies (IT). They are defined by the Common Criteria Interpretations Management Board (CCIMB) [9] and are for some years a ISO standard named ISO/IEC 15408 [1, 2, 3].

Before the appearance of CC, countries used different criteria of evaluation:

- Orange Book [10] for United States;
- ITSEC [4] for France, Germany, the United Kingdom and Netherlands;
- CTCPEC [11] for Canada.

3.3. Audience

Three categories of persons are interested in a general way in the evaluation of the properties of security of products and IT systems: users of Target Of Evaluation (TOE), developers of TOE and TOE evaluators.

3.4. Application Field

Common Criteria deal with the protection of the information against their disclosure, their modification or their loss of usage. The types of protection towards these three sorts of failures of security are called in the practice respectively confidentiality, integrity and availability. Common Criteria cover the security measures of the IT implemented in the

equipment, firmware or software. They are thus useful as guide for the development of TOE. They also allow to compare the results of security evaluations independently carried out. On the other hand, they do not deal either with the methodology of evaluation or with the administrative and legal frame in which the criteria can be used by the authorities of evaluation.

4.Limits of the CC security assurance scheme

4.1. Limit in perimeter

One very famous limit of the common criteria is that an initiator can voluntarily restrict the scope of the TOE in order to exclude some part of the IT product that would be subjected to some flaws. Indeed, the initiator very often starts the security evaluation of the overall IT product and in the same time that the security evaluation is conducted, some flaws are found and he reduces the scope of the TOE. It is thus of the responsibility of the customer to verify the scope that the certificate covers.

Two other limits of the common criteria are still focused on the scope of the TOE. First limit, the scope of the TOE is very static after the issuance of the certificate and each change in the scope of the product implies to evaluate again the product. To cope with this problem, a process of maintenance has been set up to follow each modification in an IT product. Second limit, even if the product is a software platform able to support several applications (like Java Card could be) and that this platform is certified, it is not allowed to make the composition of it with a new application that could have been already certified. However in the fictive example aforementioned both the platform (more precisely its scope) and the application (its scope too) have been certified. Since it is allowed to do such composition, the national body forbids evaluating an application alone independently of the platform on which it will run. We can summarize this problem as a lack of dynamicity of the scope and even if the common criteria security evaluation. It is a pity since it will be helpful to reduce the overall cost and time of the security evaluation. It would be nice to reach the time to market needs.

This limit regarding the short lifecycle of the certificate is very close of the static aspect of the scope of the TOE. Indeed, the certificate is only valid at the time of its issuance. This short delay is explained by the possibility that new attacks could have been discovered just at the time of the issuance or just after.

4.2. Integrating flaws or new attacks

Even if the product could be finally not sensitive to theses new attacks, with a fixed context, some new attacks haven't taken into account in the product conception. To limit this delay, the conception and the evaluation must be scheduled in parallel way. But with this method, flaws must be corrected in time and all depending process must be re-evaluated.

Moreover during this additive delay for evaluation, the market requirements can change. A new component can appear with more capacities, more security and with a lower price. Hence the delay between the product conception and the sale must be as short as possible.

4.3. Product distribution

When a product is certified, it is deployed on the market. However an analysis of what happens starting to the deployment time shows that any element enabling to ensure the

traceability and thus to maintain the chain of trust, have been set up. In the following, the problems can be raised and will be illustrated using as example the smart card products.

The company considered here could be a bank, a mobile operator, in short a large company which has an important need of smart cards. In general this company will be directly provided by the chosen manufacturer and not by the retailers. Moreover this major company is very often the initiator of the evaluation (or at least the privileged target of the manufacturer for which it has funded itself the evaluation). At the time of the products reception phase, several types of problems can exist or even to coexist:

• problems due to a negligence: there is an error in the batches or in the production line and the company does not receive the good cards. Normally the procedures of delivery defined by the CC (ADO/DEL) and of audit of the production sites make it possible to be sure that such a trouble is not possible (in theory).

• problems due to an ill will of economical type: to save money the manufacturer has used more powerful (hardware/software) components during the evaluation and lost-cost and less powerful components in production. Once again the procedures of delivery and audit make it possible to counter this trouble (in theory).

• problem due to an ill will of mischievous type: for example, modification by the manufacturer of a batch of cards for specific reasons (desire to mischief, backdoor to keep the possibility to correct possible security problems later). As for the previous case, there cannot theoretically occur.

• distribution problem: according to procedures of delivery defined by the CC, the company receives from the manufacturer the good ordered cards (same model that that evaluated) and it is perfect.

Nevertheless, for these various cases, how a company can have the proof that it received the good cards? Would not be better to have a mechanism making it possible to ensure in a more systematic way that each product sample is identical to that evaluated in order to maintain the existence of the chain of trust?

At end-user level, the same problem appears. How can he be sure that the proposed product is secure? It seems important since for example, in the case of the banking world, its own money depends on the card security. He should trust his service supplier whereas this one is perhaps not able itself to have a full trust in its product.

Clearly the limits of trust in CC certification are related to the absence of proof attached to the product.

4.4. Conformity of penetration tests.

To verify the security of the product, some tests are achieved in the Vulnerability analysis part. Vulnerability analysis consists of the identification of flaws potentially introduced in the different refinement steps of the development. It results in the definition of penetration tests through the collection of the necessary information concerning: the completeness of the security functions (does the security functions counter all the postulated threats?), the dependencies between all security requirements and whether any of the security requirements can be undermined through unexpected behavior of the system. These potential vulnerabilities are assessed through penetration testing to determine whether they could, in practice, be exploitable to compromise the security of the system.

The number and the complexity of theses tests depend on the assurance level indicated in the main document (Security Target document). One must verify that the security functions are efficient through these tests. Some attack paths use different kind of attack and knowledge. But the execution of theses tests is made in different ways by the ITSEF Centers. There is no homologated set of attack but what the evaluator wants to do or what he can do. The effective level of the vulnerability tests depend on the center quality and knowledge. Hence a same product can be evaluated as good by one center and as bad by another center.

However theses differences are limited by the certification authority which asks for complementary tests if doubts on security level appear. This choice of management facilitates the mind of initiative to create / to invent new tests. If the list of attacks was fixed as for tests of validity, it would not correspond to the reality of the reel world.

4.5. Problems of interpretation

The problems of interpretation are split in two sorts:

- difficulties in the intrinsic comprehension of the criteria: it is exactly the same thing that the laws (a paper can understand differently according to the situation, the use, the past abuses, etc.): it is necessary to legislate. An international committee exists to limit this kind of difficulty (http://www.commoncriteriaportal.org/interpretations.html)

- difficulties in terms of translation in the language of the country. The used terms do not necessarily exist and can be understood or felt in a different way. (Ex: the term "freedom" will not be understood / felt in the same way into different countries)

5.Conclusion

To summarize, a Common Criteria certificate is the recognition of a quality level reached at a certain moment. So, it helps the buyers of big quantities to make their choices. On his side, the end-user has no word to say on the final choice.

In the paper, we have shown that the chain of delivery is not secure until the end. A priori the manufacturer delivers best of its products because that it is not more expensive. Nevertheless, an additional digital certificate registered during a secure phase would make it possible to cover the end of the chain (potentially supplemented by a self test function for the embedded system) and thus, to enforce and expand the trust to the end-user.

6. References

[1] International Organization for Standardization. Information Technology – Security Techniques — Evaluation Criteria for IT Security – Part 1: Introduction and General Model, ISO-IEC 15408-1. ISO, 1999. http://www.iso.ch/

[2] International Organization for Standardization. Information Technology – Security Techniques — Evaluation Criteria for IT Security – Part 2: Security Functional Requirements, ISO-IEC 15408-2. ISO, 1999. http://www.iso.ch/

[3] International Organization for Standardization. Information Technology – Security Techniques — Evaluation Criteria for IT Security – Part 3: Security Assurance Requirements, ISO-IEC 15408-3. ISO, 1999. http://www.iso.ch/

[4] ITSEC. http://www.ssi.gouv.fr/site documents/ITSEC/ITSEC-fr.pdf

[5] CCIMB. Common Methodology for Information Technology Security Evaluation. janvier 2004. http://www.ssi.gouv.fr/site documents/CC/CEMv2.2.pdf

[6] DCSSI. http://www.ssi.gouv.fr/fr/dcssi/ index.html

[7] COFRAC. http://www.cofrac.fr/

[8] International Common Criteria, home page. http://www.commoncriteriaportal.org/

[9] CCIMB. http://www.commoncriteriaportal.org/

[10] National Computer Security Center, Department of Defense Trusted Computer System Evaluation Criteria (TCSEC or Orange Book). http://csrc.nist.gov/secpubs/rainbow/std001.txt 1983

[11] Canadian System Security Center, The Canadian Trusted Computer Product Evaluation Criteria. ftp://ftp.cse-cst.gc.ca/pub/ criteria/CTCPEC/CTCPEC.ascii january 1993

[12] Thomas S. Messerges, Ezzy A. Dabbish and Robert H. Sloan, "Investigation of Power Analysis Attacks on Smartcards", Proceedings of the USENIX Workshop on Smartcard Technology (Smartcard '99).

Authors

Dr. Dusart received his Ph.D. in Mathematics and Applications from the University of Limoges, France. After working with the SERMA ITSEF Center for 2 years as researcher and evaluator of security products, he is currently now an associate professor of the University of Limoges. He was a program committee of ISA 07, ISA 08, WISTP 07, WISTP 08. He makes as lecturer many courses in Cryptography and Smartcards. His research area is the evaluation of information security products or systems with Common Criteria and the attack improvement for security enhancement. He researches also some parts of mathematics which can be usable in security area.

Dr. Damien Sauveron is Assistant Professor at the XLIM Laboratory (UMR CNRS 6172) of the University of Limoges (France). He is vice-chair of IFIP WG11.2 Small System Security and member of: IFIP WG 8.8 Smart Cards, IEEE, IEEE Broadcast Technology Society, IEEE Communications Society, IEEE Computer Society, IEEE Systems, Man, and Cybernetics Society, IEEE Vehicular Technology Society, IEEE Standards Working Groups, etc. From 01/02/2006 to 31/03/2006, he was invited researcher at the ISG-SCC (Information Security Group - Smart Card Centre) of the Royal Holloway, University of London (RHUL). Then, from the 01/04/2006 to 10/08/2006 he was in a postdoctoral position at the ISG-SCC of the RHUL.

From 03/09/2001 to 02/09/2004, he worked during three years for the ITSEF of SERMA Technologies on the Java Card security. He obtained his Ph.D at the University Bordeaux 1 (France) in December 2004. During his thesis that he carried out in the Distributed Systems and Objects team of the LaBRI he was one of the main developers of a Java Card emulator, he introduced the concept of pre-persistance in Java Card and he highlighted a new category of attacks on the open multiapplication smart cards. More information on: http://damien.sauveron.fr/

Dr. Tai Hoon Kim received his M.S. degrees and Ph.D. in Electrics, Electronics & Computer Engineering from the Sungkyunkwan University, Korea. After working with Technical Institute of Shindoricoh 2 years as a researcher and working at the Korea Information Security Agency as a senior researcher 2 years and 6 months, he worked at the DSC (Defense Security Command) about 2 years. After working with E-wha Woman University a half year as a research professor, now he is currently a professor of Hannam University. He wrote sixteen books about the software development, OS such as Linux and Windows 2000, and computer hacking & security. And he published about 100 papers by 2006. He was a program committee of SNPD 2004, SERA 2004, SERA 2005, ISNN 2006, ICCS 2006, ICCSA 2006, ICIC 2006, RSTK 2006, SERA 2007, SmarTel 2007, SIN 2007. He was a special session and workshop chair of ICCSA 2004, PCM 2004, KES 2004, PARA 2004, ICCMSE 2004, SCI 2004, ICCSA 2005, ICIC 2005, RSFDGrC 2005, KES 2005, ICCMSE 2005, ICCSA 2006, ICIC 2006, KES 2006, ISNN 2006, ICCMSE 2006, ICCSA 2007, ICIC 2007, KES 2007, ISNN 2007, ICCMSE 2007. He was a General Chair of ICHIT 2006 and MUE 2007, Steering Committee Chair of FBIT 2007, FGCN 2007, SH 2007 and IPC 2007, and Publicity Chair of JRS 2007. He was a Guest Editor of AJIT and FGCS Journal, and now he is an EIC of JSE and IJSIA Journal. He researched security engineering, the evaluation of information security products or systems with Common Criteria and the process improvement for security enhancement. In these days, he researches also some approaches and methods making IT systems more secure.