A methodology to construct Common Criteria security targets through formal risk analysis

Jorge L. Hernandez-Ardieta Pedro Blanco David Vara
Cybersecurity Unit
Security Division
Indra Sistemas S.A., Spain
Email: jlhardieta,pbsainz,dvara@indra.es

***Abstract*—Formal threat and risk analysis methodologies (TRA) are paramount to know and manage the risks to which information systems are exposed, reducing such risks to acceptable levels. On the other hand, Common Criteria (CC) is the reference standard methodology for the evaluation of the security of information technology products. The security target, a primary source document during the evaluation, establishes the security problem that the product intends to resolve as well as the security functional and assurance requirements for such product. This information is used by the evaluator to ascertain if the product resists the attacks with the attack potential determined in the evaluation assurance level (EAL). Though reusing the results of a formal TRA seems a natural and useful approach to derive a security target, current heterogeneity between both worlds impedes it. In this paper we propose a methodology that unites both paradigms, allowing the construction of security targets that contain an accurate security problem, a coherent EAL, and security requirements that effectively counteract the identified threats.**

Keywords: Security, Common Criteria, Formal threat and risk analysis, Security target

I. Introduction

Current best practices for secure software and systems engineering encourage to undertake the identification and formalization of the threats and risks to which the product or system to develop will be exposed [1], [2]. This formal threat and risk analysis (TRA), normally carried out during the analysis stage but also refined during the whole life-cycle of the development, is paramount if effective and appropriate security countermeasures need to be implemented. As a particular case, a TRA is mandatory for products and systems that manage classified information, and where the TRA is usually required to follow standard procedures (e.g. MAGERIT [3], CRAMM [4], HMG IA [5]), depending on the accreditation authority.

On the other hand, Common Criteria (CC) [6], as the standard security evaluation methodology, not only has a positive effect in the product released, in terms of achieved degree of confidence respecting the fulfillment of its security properties, but also improves the development life-cycle. One of the causes is that CC obliges the developer to perform an identification of the assets to protect and the threats considered. In other words, the developer has to carry out a TRA to successfully pass a CC evaluation.

However, this potential benefit of CC is usually undermined as the developer is not required to carry out a formal TRA, but only to define a security problem by listing assets and threats in a purely descriptive and informal manner. In addition, the functionality that the product implements to counteract those threats (represented by the security functional requirements), along with the assurance level at which the product will be evaluated, are typically selected in terms of market opportunity, client claims, or just the developer's own convenience, not the actual risk level to which the product will be exposed.

If standard formal TRAs already exist, why not reusing the results of a formal TRA already carried out (assuming that the developer follows recommended practices) to define an accurate security problem? Why developers perform a secondary and limited informal threat analysis as a requirement for a CC evaluation?

Using the results of a TRA as input to a CC evaluation seems a natural and useful approach that would ease and speed up a CC evaluation, reducing the costs and time-effort inherent to this process. The reason that has prevented it from happening lies in the lack of harmonization between both worlds, as every TRA uses a proprietary catalog of assets, threats and safeguards, and CC establishes a predefined set of countermeasures. Consequently, the results obtained from a formal TRA cannot be used for the definition of the security problem nor the selection of the security requirements. While some contributions that try to resolve this issue can be found in the literature [9], [10], the approach followed has been completely the opposite. To use CC as a catalyst able to harmonize threat and risk analysis methodologies.

In this paper we propose a methodology that permits the developer to reuse the results of a formal TRA in order to compose an accurate security problem, derive a coherent evaluation assurance level according to the risk level to which the assets will be exposed, and derive appropriate and effective security requirements. As this information has to be written by the developer in a particular CC document named security target, the goal of the methodology is thus to aid in the construction of such document. As no homogenization between different TRAs has been achieved so far, our methodology had to be tied to a particular TRA. In our case we selected MAGERIT [3] as it is the Spanish standard TRA, but it is also recognized by important international organizations such as NATO [11],

EDA [12] and ENISA [13]. To the best of our knowledge, this is the first methodology proposed in this direction.

The paper is organized as follows. The next section II explains the background necessary to understand the rest of the paper. Section III presents the methodology and the validation results. Relevant work related to our research is briefly reviewed in section IV. Finally, the conclusions are given in section V.

II. Background

This section introduces formal threat and risk analysis methodologies, in particular MAGERIT, and Common Criteria as the standard security evaluation methodology.

A. Formal Threat and Risk Analysis Methodologies: MAGERIT

A formal threat and risk analysis methodology (TRA) is a systematic methodology that allows organizations to know the risk to which their information systems are exposed, and, as a result, to manage them, reducing such risks to acceptable levels. By means of a comprehensive TRA the applicable threats are identified, and, consequently, appropriate countermeasures can be designed and implemented.

MAGERIT [3] is a TRA recognized by the Spanish Government as the standard TRA for the Spanish Public Administration, and has also been selected by NATO (North Atlantic Treaty Organization) and included into the ENISA (European Network and Information Security Agency) and EDA (European Defence Agency) catalog of formal TRAs. MAGERIT is based on the characterization of the assets of the organization, the threats on them, and the existent safeguards that protect those assets from the identified threats. From that information, MAGERIT derives the level of risk (function of the probability or frequency of the threat and the impact caused) for each security dimension (availability, data integrity, data confidentiality, users and data authenticity, service and data traceability) of each asset. Thereby, MAGERIT permits to observe how the current risk is reduced with the increment of the number of safeguards and their maturity level, reaching a level of risk called objective or residual.

A threat and risk analysis based on MAGERIT follows three stages: potential risk assessment, actual risk assessment and residual or objective risk assessment.

During the potential risk assessment stage, the following steps are carried out:

1) **Assets Characterization**, including their interrelationships and their value (what cost-damage would be caused by their degradation). Asset valuation can follow qualitative or quantitative approaches.
2) **Threats characterization**, identifying those applicable to the selected assets, and considering their frequency (number of occurrences of the threat over a specific period, e.g. annually) and the degradation caused on the asset should the threat appears.
3) **Potential impact estimation**, defined as the damage to the asset arising from the occurrence of the threat. It includes the accumulated value and the deflected value.
4) **Potential risk estimation**, defined as the rate of exposure of a threat to appear, causing an impact, and considering the absence of safeguards. It includes the accumulated value and the deflected value.

The actual risk assessment stage implies the selection of the safeguards (and their maturity level) already incorporated in the IT system under analysis. A safeguard can reduce the risk from the potential level to the actual level by reducing the frequency of threats, limiting the impact caused in case the threat occurs, or both.

Finally, during the residual risk assessment stage, the analyst is able to incorporate new safeguards or improve the maturity level of the current ones, until the actual level of risk is reduced to a residual and acceptable level. Figure 1 depicts the relationship between safeguards and the different types of risk levels.

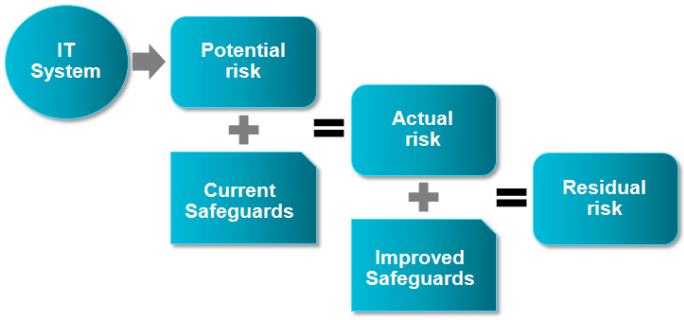

Fig. 1. Relationship between safeguards and types of risk levels

B. Common Criteria

Common Criteria (CC) [6] is an international formal methodology for the evaluation of the security of information technology products, implemented either in hardware, software or firmware. The evaluation process, carried out by an independent laboratory accredited by an authoritative evaluation scheme, establishes a level of confidence in that the security functionality of the evaluated product and the assurance measures applied to this product meet these requirements. For the purpose of compatibility and recognition between evaluation results, CC offers a common catalog of requirements for security functionality [7] and assurance measures [8]. Also, the evaluator follows a well-defined evaluation methodology [14], guaranteeing the recognition of evaluation results amongst the different evaluation schemes.

In CC terminology, the part of the product that is evaluated is called Target of Evaluation (TOE), and can range from the whole product to a tiny part of it (e.g. access control functionality of a monolithic operating system). During the evaluation process, the developer of the product has to provide the laboratory with a set of evidence, including the TOE itself and technical documents regarding the TOE design, guidance

Attack potential	Applicable EALs
Basic attack potential	EAL1, EAL2, EAL3
Enhanced-Basic attack potential	EAL4
Moderate attack potential	EAL5
High attack potential	EAL6, EAL7

TABLE I
RELATIONSHIP BETWEEN ATTACK POTENTIAL AND EVALUATION ASSURANCE LEVEL

documents, life-cycle support, test procedure and test results. The laboratory then evaluates the evidence to assess if the TOE meets the security functional and assurance requirements.

A TOE that successfully passes an evaluation obtains a CC certificate recognized amongst the members of the Common Criteria Recognition Agreement (CCRA). Depending on the level of depth and detail in the evidence provided by the developer, and the effort allocated by the evaluator to inspect those evidences, the TOE is granted a CC certificate bound to a certain evaluation assurance level. CC Part 3 [8], establishes a catalog of assurance components upon which to base assurance requirements for TOEs, and defines seven pre-defined assurance packages which are the so called Evaluation Assurance Levels (EALs). The higher the EAL, the more confidence is gained in that the TOE meets the claimed security functional requirements and assurance measures. For instance, EAL1 provides a basic level of confidence, being limited to the correct operation of the TOE (functionally tested). The level of confidence is increased as the EAL increases. The highest level, the EAL7, assures that the TOE design has been formally verified and the TOE formally tested.

Each EAL considers an attack potential that is taken into account by the evaluator during the evaluation. The attack potential can be calculated following the formula given by CC in the Common Criteria Evaluation Methodology (CEM) [14], or supporting documents prepared by sectors of the industry [15], [16]. CEM describes the attack potential as a function of expertise, resources and motivation. In particular, CEM recommends five reference factors for the attack potential calculation: time taken to identify and exploit; specialist technical expertise required; knowledge of the TOE design and operation; window of opportunity; and IT hardware/software or other equipment required for exploitation.

Therefore, there exists a clear relationship between the attack potential that the TOE is able to resist, and the EAL at which the TOE can be evaluated. This relationship can be seen in Table I.

As a result, a TOE that needs to resist sophisticated attacks (i.e. high attack potential), and thus need to provide high assurance respecting the protection of its assets, shall be evaluated against a high EAL, i.e. EAL6 or EAL7. On the contrary, a TOE that claims resistance against basic threats shall be evaluated only up to EAL3.

The nature of the TOE also influences the maximum EAL at which it can be evaluated, independently of the developer's desires. For instance, the experience gained after hundreds of evaluations[1] demonstrates that software products that consider attackers with capability of accessing the execution environment cannot resist attacks of medium or high potential, reducing the EAL to EAL4.

The security target (ST) is the primary source document in a CC evaluation. A ST is written by the developer and contains important information for the evaluator. In particular, a ST contains:

- A description of the TOE, including an overview, the TOE usage, its major security features and the logical and physical boundaries.
- A security problem definition where the assets to be protected by the TOE, the threats to those assets, the organizational security policies in place and the assumptions made by the developer are specified. In other words, this section describes the security problem that is considered by the developer. Therefore, threats not included may not be counteracted by or applicable to the TOE.
- The security objectives to be met by the TOE and the operational environment, and that counteract the identified threats and fulfill the existent policies and assumptions.
- The security functional requirements (SFR) that permit to achieve the aforementioned security objectives for the TOE (the security objectives for the operational environment are excluded).
- The security assurance requirements (SAR) that establish the EAL for the evaluation.
- A TOE summary specification where the developer explains how the SFR are implemented by the TOE.

The ST is paramount as it delimits the scope of the evaluation, conditioning the attacks that the evaluator can perform during the vulnerability analysis as well as the depth of inspection during the evidence examination.

III. A METHODOLOGY TO CONSTRUCT SECURITY TARGETS THROUGH FORMAL RISK ANALYSIS

This Section describes a methodology to construct a security target using the output produced by a MAGERIT-based threat and risk analysis on the TOE and its operational environment. First, the approach and overall strategy followed are presented. The stages of the methodology are then specified. Finally, the validation of the methodology in a real case is presented.

A. Approach

The methodology proposed in this paper assumes that a threat and risk analysis (TRA) based on MAGERIT has been carried out to the IT product to be evaluated as well as its operational environment. Once the TRA is completed, the obtained potential risk indicates the risk to which the assets are exposed in the absence of safeguards, while the selected technical safeguards that reduce the potential risk to the residual-acceptable level represent the security functionality that the product should implement.

[1]See evaluation results of certified products in Common Criteria portal at http://www.commoncriteriaportal.org

These safeguards are thus the TOE security functionality (TSF) that shall be CC evaluated, and where a relation between TSF and security functional requirements (SFR) exists. In addition, the EAL at which those safeguards shall be evaluated depends upon the potential risk that each of them reduces. That is, the higher the potential risk is, the more confidence should be gained in that the related safeguards behave as expected. If such confidence is achieved, it means that the TOE will operate within its operational environment under a level of risk equal to the residual one.

In order to formalize these relationships, correlation tables have been developed. These tables map the elements of the TRA with the elements from CC Part 2 [7], i.e. security functional requirements, and CC Part 3 [8], i.e. security assurance requirements, as outlined in Fig. 2.

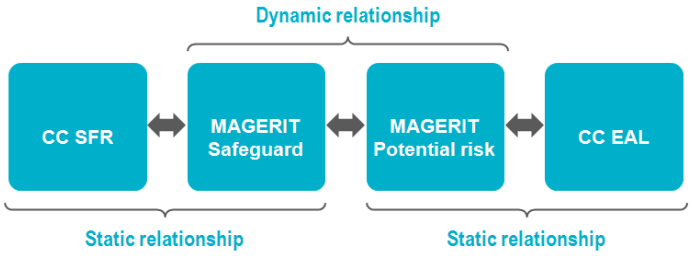

Fig. 2. Relationships between MAGERIT elements and CC

As explained above, there is a strong relationship between the technical safeguards and the security functional requirements. This relationship is, actually, independent of the particular TRA or TOE, as both MAGERIT and CC provide a predefined set of elements. Therefore, this static relationship has been developed as a fixed correlation table where each MAGERIT technical safeguard has been mapped to the corresponding CC SFRs. We have filtered the hundreds of MAGERIT safeguards, reducing them to 87 that can be mapped to CC SFR. Due to lack of space, the table has not been included in the paper.

It should be noted that the mapping is one-to-many, being one safeguard related to one or more SFR. The reason stems from the different levels of abstraction used in MAGERIT and CC, thus being possible that more than one SFR is conceptually equivalent to the same safeguard.

Similarly, the relationship between the potential risk indicated by MAGERIT and the EAL levels can also be fixed without considering the particular TRA or TOE. For that purpose, we also developed a fixed correlation table where such static relationship is captured (see Annex A).

Finally, a safeguard is bound to a certain level of risk, which is, on the contrary, always dependent on the specific TRA. In this case, the relationship between safeguards and potential risks is established at the end of the TRA, and thus shall be completed on a case-by-case basis.

A template table with a structure similar to the one shown in Table II is provided to the analyst in order to facilitate the application of the methodology.

B. *Formalized Steps*

This Section presents the steps that have to be applied by the analyst to construct a security target for the TOE and derive the EAL of the CC evaluation using our methodology.

1) Security problem definition derivation
   In this step the analyst composes the security problem definition section of the security target. For this purpose, the assets to be protected by the TOE can be directly obtained from the TRA. However, a refinement shall be done to select only those applicable to the TOE.
   The TRA also provides the threats to the assets. Again, a refinement shall be done to select only those threats applicable to the TOE.
   Finally, the technical, physical, organizational and personnel safeguards are also provided by the TRA. A selection of those applicable to the TOE operational environment shall be done, and from which the assumptions and organizational security policies of the security target can be derived.

2) Safeguards and risks association
   The analyst has to extract the technical safeguards and the risks that they reduce, along with the affected assets. With this information the analyst is able to complete the dynamic relationship between safeguards and potential risk levels, filling in the columns C2 and C3 of the template table.

3) Identification and association of SFR with safeguards
   In this step, and using the correlation table between MAGERIT technical safeguard and CC SFRs, the analyst has to identify the CC SFRs associated with each technical safeguards extracted in Step 2, and incorporate them in column C1 of the template table.

4) EAL derivation
   Using the correlation table of Annex A, the analyst must identify the EAL for each potential risk extracted in Step 2, and incorporate them in column C4 of the template table.
   After this step, the analyst has obtained the SFRs of applicability to the TOE, as well as the EAL(s) at which such SFRs shall be evaluated. Next Table II depicts an example of the set of associations produced at this time.

5) Normalization
   If no composite evaluation is needed, the analyst shall homogenize the EAL at which the TOE will be evaluated. With this regard, a specific policy of the organization, or other criteria, may indicate how to proceed. For instance, one possibility is to homogenize the EAL to highest value possible, though a TOE (e.g. software product) may not be capable to pass a EAL5 or above, unless the underlying platform is under control (e.g.

C1: CC SFR	C2: MAGERIT Safeguards (technical)	C3: MAGERIT Potential risk		C4: CC EAL
		Asset	Risk	
FCS Cryptographic support FCS_CKM Cryptographic key management FCS_CKM.1 Cryptographic key generation	[S] Service protection [S7] Use of cryptographic services [S72] Key management [S722] Key generation	[A1] Identification and Authentication service	{7.5}	EAL6, EAL7
FTP Trusted path/channels FTP_ITC Inter-TSF trusted channel	[SW] Protection of computer applications (SW) [SWa] Production [SWa] Security of mechanisms between processes	[A3] Data flow System1-System2	{4.0}	EAL5

TABLE II
EXAMPLE

smart card). Other criteria may be to split the TOE into different sub-TOEs, and perform different evaluations with different EALs with the goal to achieve a further composite evaluation.

As can be seen in Table II, two possible EALs have been identified for FCS_CKM.1 Cryptographic key generation SFR, while the EAL5 has been asigned to FTP_ITC Inter-TSF trusted channel. In the former, the analyst could decide to select the highest one (i.e. EAL7) if such criteria was of applicability.

C. Validation

We have validated the applicability and usefulness of our methodology by integrating it into a real-case. In particular, the methodology has been applied to construct the security target of a complex product that manages classified information within the defence sector. Due to the nature of the project and the product itself, we cannot provide further details. In our case, the large set of SFRs obtained intend to counteract the threats that were identified during the formal TRA using MAGERIT. The EAL derived (after normalization, and following the threshold for software products) corresponds to EAL4.

The results obtained permit to gain some confidence in the correctness of the method, though a complete validation has not been achieved so far due to time constraints. We cannot ascertain that the methodology has been successfully put into practice until the CC evaluation of the product is completed. At that moment, we will be able to observe if the security target was precisely constructed or some deficiencies and improvements are needed. Currently, the product development is being completed, so we expect that the evaluation should finalize in two years from now on.

We have also observed that this approach permits to address a precise evaluation assurance level (EAL), even without calculating the attack potential as established by CC (see Section II-B). By knowing the threats and their characterization (including the attacker's capability, i.e. attack potential) provided by the TRA, as well as the safeguards that positively impact on them reducing the potential risk to acceptable levels, it could be possible to derive the EAL for each safeguard (or set of safeguards). Consequently, a TRA can help to calculate the EAL for the evaluation in an accurate manner according to the potential risk to which the TOE will be exposed, significantly simplifying the process and avoiding to carrying out an adhoc attack potential calculation.

IV. Related Work

The synergies between Common Criteria (CC) and threat and risk analysis (TRA) have already been explored in some relevant initiatives, but with the goal of using CC as a common framework to harmonize and facilitate current threat and risk analysis (TRA).

In 2002, the Communications Security Establishment (CSE) Canada undertook an initiative to develop a baseline mapping of TRA safeguard areas to the CC assurance and functionality classes and families, using the qualitative descriptions and structured terminology of controls and safeguards available in CC as guidance within TRA. In this sense, a threat mapping was developed, where TRA threats were mapped to CC threats[2]. A safeguard mapping was also carried out, where the TRA safeguard functionality were mapped to a set of CC SFRs. Finally, a mapping between the TRA asset valuation and threat level of a specific threat scenario to an EAL was also performed.

Though this project seemed to have achieved some contributions also proposed in this paper, the results are not publicly available, and only a description of the achievements can be found (and described herein).

The same approach was presented in [9], where the concepts and vocabulary of CC were identified as a possible candidate to homogenize the disparate terminologies of the existent TRA approaches. The report concludes highlighting the need of further research in order to link the CC to TRA methodologies.

NATO technical report [10] feeds from the aforementioned studies to analyze possible links between Common Criteria and risk analysis, trying to find a way to leverage on CC to find a common TRA framework. However, only a brief discussion, and not a detailed methodology, was provided.

V. Conclusions

In this paper, a comprehensive methodology to partially construct the security target of a product to be evaluated

[2]It should be noted that Common Criteria has never released a formal catalog of threats, and thus this statement relates to threats obtained from the experience rather than from a formalized knowledge.

against Common Criteria has been proposed. The methodology reuses the outputs generated in a formal threat and risk analysis (TRA) performed with MAGERIT in order to facilitate the analyst the definition of the security problem, as well as the selection of the security functional and assurance requirements. As a result, the stated security problem is accurate, the derived evaluation assurance level coherent, and the security requirements that counteract the identified threats, effective. In particular, the methodology permits:

- Derive the Security Problem Definition, using the assets and threats information provided after the potential risk assessment stage.
- Derive the Security Functional Requirements (SFR), based on the final list of safeguards selected after the residual risk assessment stage.
- Calculate the security barriers assurance level, in terms of EAL, for each SFR. This achievement would aid composite evaluations, where different parts of a product can be evaluated independently.
- Recommend the EAL for the evaluation.

Figure 3 represents the coverage of the security target using the methodology proposed in this paper (boxes without dark grey background).

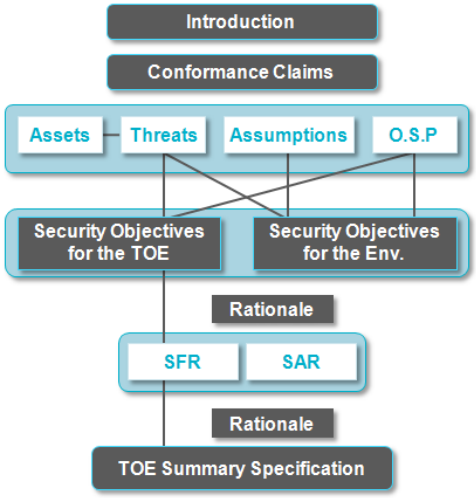

Fig. 3. Security target coverage

The methodology has been successfully put into practice during the development of a complex product which manages classified information. However, a full validation has not been achieved as the evaluation has not been completed yet.

In addition, and until full interoperability is achieved between TRAs, the catalog of threats and safeguards depends on the particular TRA (in our case, MAGERIT).

Also, there is still some work to be done. The methodology will be complemented with an automated tool to assist during the process, and to ease the writing task and support the decisions-making during the refinements.

REFERENCES

[1] M. Howard. Building More Secure Software with Improved Development Processes. IEEE Security & Privacy, 2(6) (2004)
[2] J. Viega and G. McGraw. Building Secure Software. Addison-Wesley Professional Computing Series, New York (2001)
[3] MAGERIT - version 2. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Spanish Ministry of Public Administration (2006)
[4] CCTA Risk Analysis and Management Method (CRAMM). Available at http://www.cramm.com
[5] IA Standard No. 1 Technical Risk Assessment. Issue No: 3.51 (2009)
[6] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. Version 3.1 R3 Final. CCMB-2009-07-001 (2009)
[7] Common Criteria for Information Technology Security Evaluation. Part 2: Security functional components. Version 3.1 R3 Final. CCMB-2009-07-002 (2009)
[8] Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance components. Version 3.1 R3 Final. CCMB-2009-07-003 (2009)
[9] Common Methods For Security Risk Analysis. Technical Report prepared by Cinnabar Networks Inc. for Defence R&D Canada (DRDC) (2004)
[10] Improving Common Security Risk Analysis. RTO Technical Report TR-IST-049, NATO (2008)
[11] North Atlantic Treaty Organization (NATO). Available at http://www.nato.int/cps/en/natolive/index.htm
[12] European Defence Agency (EDA). Available at http://www.eda.europa.eu/
[13] European Network and Information Security Agency (ENISA). Available at http://www.enisa.europa.eu/
[14] Common Methodology for Information Technology Security Evaluation. Evaluation methodology. Version 3.1 R3 Final. CCMB-2009-07-004 (2009)
[15] T. Schröder. Examples for the Calculation of Attack Potential for Smartcards. JHAS working group.
[16] Application of Attack Potential to Smartcards v2.1. Joint Interpretation Library (2006)

APPENDIX

Next Table III contains the static relationship between MAGERIT potential risk and CC EAL.

MAGERIT Potential risk	CC Attack potential	CC EAL
{0.0-0.9} Negligible	–	Not required
{1.0-1.9} Low	Basic attack potential	EAL1, EAL2, EAL3
{2.0-2.9} Medium	Enhanced-Basic attack potential	EAL4
{3.0-3.9} High	Moderate attack potential	EAL5
{4.0-4.9} Very high	Moderate attack potential	EAL5
{5.0-10.0} Critical	High attack potential	EAL6, EAL7

TABLE III
RELATIONSHIP BETWEEN MAGERIT POTENTIAL RISK AND CC EAL