Open Smart Card Infrastructure for Europe

v2

Volume 8: **Security and Protection Profiles**

Part 1: **Application of attack potential to smart cards (Common Criteria Supporting Document)**

Authors: **eESC TB3 Protection Profiles, Security Certification**

NOTICE

This eESC Common Specification document supersedes all previous versions.

Neither eEurope Smart Cards nor any of its participants accept any responsibility whatsoever for damages or liability, direct or consequential, which may result from use of this document.

Latest version of OSCIE and any additions are available via www.eeurope-smartcards.org and www.eurosmart.com. For more information contact info@eeurope-smartcards.org.

Supporting document framework

CC Supporting document

Warning

This document is a Common Criteria supporting document. It is not officially endorsed by all the Common Criteria Recognition Arrangement participants, but is endorsed by some certificate-producing participants that use it in a particular field of technology. The use of this supporting document is not mandatory. It can be use by any certification/validation body, evaluation facility and vendors.

Any comments about this document can be sent to the sponsor of the document.

See the CCRA Procedure for Supporting Documents

Document name : Application of Attack Potential to Smartcards
Reference : Version 1.1, July 2002
Object : Smartcards
Sponsor : BSI
Supporters : BSI, CESG, DCSSI, NLNCSA

Supporting document framework

Last update : July 2002(draft indicator deleted, references updated, same content as V1.0)
By : BSI, CESG, DCSSI, NLNCSA

1.General purpose:
This document provides guidance on the application of the current version of Common Criteria Methodology [CEM], part 2, annex B.8. This work has been based on smartcard CC evaluation experience and input from smartcard industry. The document contains guidance metrics to calculate attack potential required by an attacker to effect an attack. The underlying objective is to aid in expressing the total effort required to mount a successful attack. This should be applied to operational behaviour of a smartcard and not to applications specific only to hardware or software.

2.Field of special use: Evaluation of Smartcard Components

3. Body text:

Table of contents

1 Introduction

1 This document interprets the current version of Common Criteria Methodology [CEM], part 2, annex B.8. This work has been based on smartcard CC evaluation experience and input from smartcard industry through Trailblazer 3 working group of eEurope initiative. This replaces chapter 7 of reference [HW-IC-Meth].

2 This chapter provides guidance metrics to calculate attack potential required by an attacker to effect an attack. The underlying objective is to aid in expressing the total effort required to mount a successful attack. This should be applied to operational behaviour of a smartcard and not to applications specific only to hardware or software.

2 Scope

3 This document introduces the notion of an attack path comprised of one to many attack steps. Analysis and tests need to be carried out for each attack step on an attack path for a vulnerability to be realised. Where cryptography is involved, the Certification Body should be consulted.

3 Identification of Factors

3.1 How to compute an attack

4 Attack path identification and exploitation analysis and tests are mapped to relevant factors: elapsed time, expertise, knowledge of the TOE, access to the TOE, equipment needed to prosecute an attack. Even if the attack consists of several steps identification and exploitation need only be computed for the entire attack path.

5 The identification part of an attack corresponds to the effort required to set-up test benches and to demonstrate the attack.

6 The exploitation part of an attack corresponds to achieving the attack on another smartcard using the same analysis and tests as per the identification part of an attack. This could also mean the analysis and test needed to clone a smartcard to emulate the secrets derived from an identification attack.

7 The attack potential calculation requires a more granular analysis in the event that the computed analysis and test be close to a boundary (low/moderate, moderate/high). This shall essentially consist of an impact analysis of the potential changes for each individual factor on an attack path.

3.2 Elapsed Time

8 Additional granularity is introduced into CEM elapsed time. In particular, distinction is drawn between one week and several weeks. Time is divided into the following intervals:

	Identification	Exploitation
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*

Table 1: Rating for Elapsed Time

9 The CEM defines the term *Not Practical* as "the attack path is not exploitable within a timescale that would be useful to an attacker". Example 5.5 illustrates this scenario.

10 In practice an evaluator is unlikely to spend more than 3 months attacking the TOE. At the end of the evaluation the evaluator has to assess the time it would take to carry out the minimum attack path. This computes the estimated time to mount the attack, and not necessarily the time spent by the evaluator to conduct the attack.

11 Where the attack builds on the findings of a previous evaluation, Elapsed Time as well as Expertise have to be taken into account, e.g. a particular attack may have been developed on a smartcard product similar to the TOE. It is not possible to give general guidance.

3.3 Expertise

12 For the purpose of smartcards two types of experts are defined:

- an expert with the ability to define new attacks for smartcards (hardware, software, cryptography) and the necessary tools, and
- an expert with a commensurate level of knowledge of the TOE to that of the developer (e.g. knowledge of product standards and specifications).

13 Expertise necessary to carry out an attack may cover several disciplines: chemical, ability to drive sophisticated tools, cryptographic.

	Definition according to CEM	Detailed definition to be used in smartcard evaluations
a) Experts	Familiar with implemented • Algorithms • Protocols • Hardware structures • Principles and concepts of security	Familiar with • Developers knowledge namely algorithms, protocols, hardware structures, principles and concepts of security and • Techniques and tools for the definition of new attacks

	Definition according to CEM	Detailed definition to be used in smartcard evaluations
b) Proficient	Familiar with • security behaviour	Familiar with • security behaviour, classical attacks
c) Laymen	No particular expertise	No particular expertise

Table 2: Definition of Expertise

Extent of expertise (in order of spread of equipment or smartcard related knowledge)	
Equipment: The level of expertise depends on the degree to which tools require experience to drive them • Optical Microscope • Chemistry (etching, grinding), Microprober • Laser Cutter, Radiation • Plasma (etching, grinding), Focused Ion Beam (FIB) • Scanning Electron Microscope (SEM), • Scanning Force Microscope (SFM)	**Knowledge:** The level of expertise depends on knowledge of • Common Product information • Common Algorithms, Protocols • Common Cryptography • Differential Power Analysis (DPA), Differential Fault Analysis (DFA), Smartcard specific hardware structures, Principles and concepts of security • Developers knowledge

Table 3: Extent of expertise

14 It may occur that for sophisticated attacks, several types of expertise are required. In such cases, the higher of the different expertise factors is chosen.

	Identification	Exploitation
Layman	0	0
Proficient	2	2
Expert	5	4

Table 4: Rating for Expertise

3.4 Knowledge of TOE

15 The CEM states “to require sensitive information for exploitation would be unusual”, however it shall be clearly understood that any information required for identification shall not be considered as an additional factor for the exploitation.

16 Since all sensitive and critical design information must be well controlled and protected by the developer, it may not be obvious how it assists in determining a dedicated attack path. Therefore, it shall be clearly stated in the attack potential calculation why the required critical information cannot be substituted

by a related combination of time and expertise, e.g a planning ingredient for a dedicated attack.

17 The following classification is to be used:

- Public: this is information in the public domain,
- Restricted: this corresponds to assets which are passed about during the various phases of smartcard development. Suitable examples might be the functional specification (ADV_FSP), guidance documentation (AGD) or administrative documents usually prepared for smartcard issuers/customers. (See [CC-IC App])
- Sensitive: HLD and LLD information.
- Critical: Implementation representation (Design and Source Code).

18 In this way knowledge shall distinguish between access to high level design, low-level design on the one hand and source code/ schematics of the product on the other by taking into account two types of information (HLD/LLD and Implementation Level). (See [CC-IC App])

19 It may occur that for sophisticated attacks, several types of knowledge are required. In such cases, the higher of the different knowledge factors is chosen.

	Identification	**Exploitation**
Public	0	0
Restricted<	2	2
Sensitive	4	3
Critical	6	5

Table 5: Rating for Knowledge of TOE

3.5 Access to TOE

20 Availability of samples (in terms of time and cost) needs to be taken into account as well as the number of samples needed to carry out an attack path (this shall replace the CEM factor “Access to TOE“).

21 The attack scenario might require access to more than one sample of the TOE because:

- the attack succeeds only with some probability,
- the attacker needs to collect information from several copies of the TOE. In this case, TOE access is taken into account using the following rating:

	Identification	**Exploitation**
< 10 samples	0	0
< 100 samples	2	4

	Identification	**Exploitation**
> 100 samples	3	6
Not practical	*	*

Table 6: Rating for Access to TOE

22 Not practical is explained as following:

- For identification: not practical starts with 2000 samples or the largest integer less than or equal to n/(1+(log n)^2), n being the estimated number of products to be built.
- For exploitation: not practical starts with 500 samples or the largest integer less or equal to n/(1+(log n)^3), n being the estimated number of products to be built.

23 The Security Policy as expressed in the Security Target should also be taken into account.

3.6 Equipment

24 In order to clarify equipment category, price and availability has to be taken into account.

- None
- Standard
- Specialized (this type of equipment shall be considered as the type of expensive equipment which universities have in their possession.)
- Bespoke
  - Expensive [CEM]
  - Difficult to keep confidential [CEM] such as PC's linked across Internet.

25 In an ideal world definitions need to be given in order to know what are the rules and characteristics for attributing a category to an equipment or a set of equipment. In particular, the price, the age of the equipment, the availability (publicly available, sales controlled by manufacturer with potentially several levels of control, may be hired) shall be taken into account. The tables below have been put together by a group of industry experts and will need to be revised from time to time.

26 The range of equipment at the disposal of a potential attacker is constantly improving, typically:

- Computation power increase
- Cost of tools decrease
- Availability of tools can increase
- New tools can appear, due to new technology or to new forms of attacks

27 It may occur that for sophisticated attacks, several types of equipment are required. In such cases, the higher of the different equipment factors is chosen.

3.6.2 Tools

Tool	Equipment
Laser equipment	Standard
UV-light emitter	Standard
Climate chamber	Standard
Voltage supply	Standard
Oscilloscope analogue	Standard
Chip card reader	Standard
PC or work station	Standard
Signal analysis software	Standard
Signal generation software	Standard
Visible light microscope and camera	Specialized
UV light microscope and camera	Specialized
Micro-probe Workstation	Specialized
Laser cutter	Specialized
Signal and function processor	Specialized
Oscilloscope digital	Specialized
Signal analyzer	Specialized
Tools for chemical etching (wet)	Specialized
Tools for chemical etching (plasma)	Specialized
Tools for grinding	Specialized

Table 7: Categorisation of Tools (1)

3.6.2 Design verification and failure analysis tools

28 Manufacturers know the purchasers of these tools and their location. The majority of the second hand tools market is also controlled by the manufacturers.

29 Efficient use of these tools requires a very long experience and can only be done by a small number of people. Nevertheless, one cannot exclude the fact that a certain type of equipment may be accessible through university laboratories or equivalent but expertise in using the equipment is quite difficult to obtain.

Tool	Equipment
Scanning electron microscope	Bespoke
E-beam tester	Bespoke
Scanning Force Microscope (SFM)	Bespoke
Focused Ion Beam (FIB)	Bespoke
Laser beam	Bespoke
New Tech Design Verification and Failure Analysis Tools	Bespoke

Table 8: Categorisation of Tools (2)

30 Note, that using bespoke equipment should lead to a moderate potential as a minimum.

	Identification	**Exploitation**
None	0	0
Standard	1	2
Specialized	3	4
Bespoke	5	6

Table 9: Rating for Equipment

31 Equipment can always be rented but the same quotation applies.

4 Final Table

Factors	**Identification**	**Exploitation**
Elapsed time		
< one hour	0	0
< one day	1	3
< one week	2	4
< one month	3	6
> one month	5	8
Not practical	*	*
Expertise		
Layman	0	0
Proficient	2	2
Expert	5	4
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	4	3
Critical	6	5
Access to TOE		
< 10 samples	0	0
< 100 samples	2	4
> 100 samples	3	6
Not practical	*	*
Equipment		
None	0	0
Standard	1	2
Specialized	3	4
Bespoke	5	6

Table 10: Final table for the rating factors

32 * Indicates that the attack path is not exploitable within a timescale that would be useful to an attacker. Any value of * indicates a High rating.

33 The following table replaces table B.4 of CEM, para 1873 for smartcards.

Range of values	**Resistance to attacker with attack potential of:**	**SOF rating**
0-15	No rating	No rating
16-24	Low	Basic
25-30	Moderate	Medium
31 and above	High	High

Table 11: Rating of vulnerabilites

5 Examples of use of this document

34 The following examples have been constructed during the development of this document and only reflect the current state of the art situation of that period (Q4/01). For each particular TOE these types of calculations need to be carried out for each attack path and the results of the calculations may differ from those shown below, e.g. because the design and use of the TOE may be different.

5.1 Basic DPA

35 Definition of the Attack: basic DPA. The evaluation lasts less than one month, including sampling less than 10 cards, with knowledge of the set of commands of the smartcard.

- Equipment: standard.
  Rated 1 for identification; 2 for exploitation.
- Access to TOE:
  Identification of vulnerabilities can be done on attacker's own card (one sample). Undetectable. Rated 0; exploitation on the current sample. Rated 0.
- Knowledge of the TOE:
  Restricted for identification, Rated 2 and 0 for exploitation (public information).
- Expertise:
  Attacker needs to know cryptographic algorithms (public) + attacks (public). Proficient. Rated 2.
- Elapsed Time:
  Identification within days. Rated 2; exploitation within hours. Rated 3.

Total:
- identification 1+0+2+2+2 = 7
- exploitation 2+0+0+2+3 = 7
Total is 14.

36 This means that the TOE is not resistant to an attacker with a low attack potential.

5.2 Basic SPA

37 Definition of the Attack: basic SPA.

- Equipment:
  Standard. Rated 1 for identification; 2 for exploitation.
- Access to TOE:
  Identification of vulnerabilities can be done on attacker's own card (one sample). Undetectable. Rated 0;
  exploitation on the current sample. Rated 0.

- Knowledge of the TOE:
  Public Rated 0/0.
- Expertise:
  Attacker needs to know cryptographic algorithms (public) + attacks (public). Proficient. Rated 2.
- Elapsed Time:
  Identification less than one day : Rated 1;
  exploitation less than one hour ; Rated 0

Total:
- identification 1+0+0+2+1 = 4
- ploitation 2+0+0+2+0 = 4

Total is 8.

38 This means that the TOE is not resistant to an attacker with a low attack potential.

5.3 Physical Probing

39 Definition of the Attack: successful attack using physical probing with FIB, without any knowledge of the smartcard (IC and/or Mask).

- Equipment:
  Bespoke. Rated 5 for identification;specialized, rated 4 for exploitation.
- Access to TOE:
  Identification of vulnerabilities can be done on attacker's own card (one sample). Undetectable. Rated 0;
  exploitation on the current sample. Rated 0.
- Knowledge of the TOE:
  Restricted for identification, rated 2 ; restricted for exploitation, rated 3.
- Expertise:
  Expert for identification and proficient for exploitation, rated 5 and 2.
- Elapsed Time:
  Identification Month : Rated 5; Exploitation rated 4.

Total:
- identification 5+0+2+5+5 = 17
- exploitation 4+0+3+2+4= 13

Total is 30.

40 For this type of attack the TOE is resistant to an attacker with a moderate attack potential. This does not automatically mean that the TOE is resistant to an attacker with a moderate attack potential because there may be other attack paths which are easier.

5.4 Combined Attack

41 Definition of the Attack : Use of a perturbation to modify the execution of a program (with software source code)

Identification = to find a critical instruction within the program: analysis of the software source code
Exploitation = Perturbation of the instruction

- Elapsed time:
  Identification: <1 month: 3;
  Exploitation: <1 week: 4
- Expertise
  Identification: Expert in software development: 5;
  Exploitation: Proficient: 2
- Knowledge of the TOE:
  Identification: Software source code: 6
  Exploitation: Card Commands: 0
- Access to the TOE
  Identification: No: 0;
  Exploitation: Few samples: 0
- Equipment
  Identification: PC: 1
  Exploitation: Perturbation source: 4

Total:
15+10 = 25

42 For this type of attack the TOE is resistant to an attacker with a moderate attack potential. This does not automatically mean that the TOE is resistant to an attacker with a moderate attack potential because there may be other attack paths which are easier.

5.5 "Non-practical" Time Attack

43 In section 3.2 the question of "Non Practical" is raised and this may depend on the specific attack scenario as the following two examples show:

(a) Assume a smartcard used for an online system, where the card contains only individual keys and assume further that these keys are deactivated in the system within days after loss of a card was reported. In this case an attack is not even practical for an attacker if he can extract the keys in one week.

(b) Assume a smartcard, which contains system-wide keys, which might be used for fraud even if use of the individual card is blocked after loss. In this case an attack may be successful for the attacker even if it takes a year.

44 So if a general assumption on a time for "Non Practical" is needed, something about 3-5 years is a better worst-case oriented time frame. (This is the time after which a card generation is normally exchanged and system wide keys may be changed in a comparable time frame). However, the best rule seems to decide on the meaning of "Non practical" only in a specific attack scenario.

6 References

[CC] Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999

[CEM] Common Methodology for Information Technology Security Evaluation (CEM), Part 1, Version 0.6; Part 2: Evaluation Methodology, Version 1.0, August 1999

[CC-IC App] CC Supporting Document, The Application of CC to Integrated Circuits, Version 1.2, July 2002.

[IC-HW-Meth] Joint Interpretation Library, Integrated Circuit Hardware Evaluation Methodology, Vulnerability Assessment, Version 1.3, April 2000