Joint Interpretation Library

Application of Attack Potential to POIs

Version 1.0 (for trial use)
9th June 2011

Acknowledgments:

The organisations listed below and organised within the Joint Interpretation Working Group (JIWG) provide JIWG Supporting documents in order to assist the consistent application of the criteria and methods between SOG-IS Evaluation and Certification Schemes.

France:	Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)
Germany:	Bundesamt für Sicherheit in der Informationstechnik (BSI)
Italy:	Organismo di Certificazione della Sicurezza Informatica (OCSI)
Netherlands:	Netherlands National Communications Security Agency (NLNCSA)
Spain:	Centro Criptológico Nacional (CCN)
United Kingdom:	Communications-Electronics Security Group (CESG)

They acknowledge the contribution of the work on the development of this version of this JIWG Supporting document done by evaluation labs, several POI terminal vendors, and other companies organised within the

- Groupe d'Evaluation de la Sécurité des Terminaux électroniques (GESTe)[1] and the
- JIL Terminal Evaluation Methodology Subgroup (JTEMS).

[1] "GESTe (Groupe d'Evaluation de la Sécurité des Terminaux Electroniques) is a French ANR (Agence Nationale pour la Recherche) project started in March 2009 and ending in September 2011, involving the following partners; Ingenico, CEA LETI, EMSE, GIE- Cartes-Bancaires, Maxim, Thales-CESTI, Trusted Labs and University of Caen"

Table of contents

1 Introduction

1 This document interprets the current version of Common Criteria Methodology [CEM] (annex A.8 for CC v2, annex B.4 for CC v3). This work has been based on security evaluations of PIN Entry Devices (PEDs) performed within the Payment Card Industry security evalution scheme as well as other European security evaluation schemes like Currence, UK Payments and ZKA.

2 This chapter provides guidance metrics to calculate attack potential required by an attacker to effect an attack. The metric is equivalent to the metric used introduced in *PCI Payment Card Industry (PCI) POS PIN Entry Device (PED), Version 2.1, Appendix B*. 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 POI and not to applications specific only to hardware or software.

3 This document is compatible with CC v3.

2 Scope

4 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

5 Note about CC v3.1 :

6 With Common Criteria version 3.1, there is no more distinction between the identification phase and the exploitation phase but within the POI community, the risk management performed by the user of CC certificates required clearly to have a distinction between the cost of “identification” (definition of the attack) and the cost of “exploitation” (e.g. once a script is published on the World Wide Web). Therefore this distinction is kept when calculating attack potential for POI evaluation. Although the distinction between identification and exploitation is essential for the POI evaluation to understand and document the attack path, the final sum of attack potential is calculated by adding the points of the two phases, as both phases build the complete attack.

3.1 How to compute an attack

7 Attack path identification and exploitation analysis and tests are mapped to relevant factors: attack time, expertise, knowledge of the POI, access to the TOE per unit required for the attack, equipment required for the attack, specific parts required.

8 Even if the attack consists of several steps identification and exploitation need only be computed for the entire attack path.

9 The identification part of an attack corresponds to the effort required to create the attack, and to demonstrate that it can be successfully applied to the TOE (including setting up or building any necessary test equipment). The demonstration that the attack can be successfully applied needs to consider any difficulties in expanding a result

shown in the laboratory to create a useful attack. For example, where an experiment reveals some bits or bytes of a confidential data item (such as a key or PIN), it is necessary to consider how the remainder of the data item would be obtained (in this example some bits might be measured directly by further experiments, while others might be found by a different technique such as exhaustive search). It may not be necessary to carry out all of the experiments to identify the full attack, provided it is clear that the attack actually proves that access has been gained to a TOE asset, and that the complete attack could realistically be carried out. One of the outputs from Identification is assumed to be a script that gives a step-by-step description of how to carry out the attack – this script is assumed to be used in the exploitation part.

10 Sometimes the identification phase will involve the development of a new type of attack (possibly involving the creation of new equipment) which can subsequently be applied to other TOEs. In such a case the question arises as to how to treat the elapsed time and other parameters when the attack is reapplied. The interpretation taken in this document is that the development time (and, if relevant, expertise) for identification will include the development time for the initial creation of the attack until a point determined by the relevant Certification Body. Once a Certification Body has determined this point, then no points for the development of the attack (in terms of time or expertise) will be used in the attack potential calculation.

11 The exploitation part of an attack corresponds to achieving the attack on another instance of the TOE using the analysis and techniques defined in the identification part of an attack. It is assumed that a different attacker carries out the exploitation, but that the technique (and relevant background information) is available for the exploitation in the form of a script or set of instructions defined during the identification of the attack. The script is assumed to identify the necessary equipment and, for example, mathematical techniques used in the analysis. This means that the elapsed time, expertise and TOE knowledge ratings for exploitation will sometimes be lower for exploitation than for identification. For example, it is assumed that the script identifies such things as the timing required for a perturbation attack, and hence in the exploitation phase the attacker does not have to spend significant time to find the correct point at which to apply the perturbation. Furthermore this same information may also reduce the exploitation requirement to one of time measurement, whereas the identification phase may have required reverse engineering of hardware or software information from power data – hence the expertise requirement may be reduced. Similarly, knowledge about the application that was used to achieve the timing of an attack may also be included either directly in the script or indirectly (through data on the timing required).

12 In many cases, the evaluators will estimate the parameters for the exploitation phase, rather than carry out the full exploitation. The estimates and their rationale will be documented in the ETR.

13 To complete an attack potential calculation the points for identification and exploitation have to be added as both phases build the complete attack. When presenting the attack potential calculation in the ETR, the evaluators will make an argument for the appropriateness of the parameter values used, and will therefore give the developer a chance to challenge the calculation before certification. The final attack potential result

will therefore be based on discussions between the developer, the ITSEF and the CB, with the CB making the final decision if agreement cannot be reached.

14 *[…rules for time to be spent on a POI evaluation…]*

15 It is an assumption that the Certification Bodies will ensure that there is harmonisation between national schemes. This is required, for example, where new types of attack are applied and a decision has to be taken as to when the attack is considered 'mature', at which point it will no longer gain points for the time or expertise to develop the attack (as discussed above).

3.2 Elapsed Time

16 The Elapsed Time is given in the time in hours taken by an attacker to identify or exploit an attack.

17 Compared to CEM V2.x 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:

Elapsed Time	Identification	Exploitation
< one hour	0	0
≤ one day	1	2
≤ one week	2	3
≤ one month	3	4
> one month	5	7

Table 1: Rating for Elapsed Time

18 For purposes of calculating time, a day = 8 hours; a week = 40 hours; and a month = 180 hours.

19 If the attack consists of several steps, the Elapsed Time can be determined and added to achieve a total Elapsed Time for each of these steps. Actual labor time has to be used instead of time expired as long as there is not a minimum Elapsed Time enforced by the attack method applied (for instance, the time needed for performing a side channel analysis or the time needed for an epoxy to harden). In those case where attendance is not required during part of the Elapsed Time, the Elapsed Time is to be taken as expired time divided by 3.

3.3 Expertise

20 Expertise refers to the level of generic knowledge of the application area or product type (e.g., Unix operation systems, Internet protocols). For the purpose of POIs three types of experts are defined:

- Laymen are unknowledgeable compared to experts or proficient persons, with no particular expertise.

- Proficient persons are knowledgeable in that they are familiar with the security behavior of the product.
- Experts are familiar with the underlying algorithms, protocols, hardware, structures, etc. implemented in the product or system type and the principles and concepts of security employed;

21 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
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 TOE related knowledge)	
Equipment: The level of expertise depends on the degree to which tools require experience to drive them • Optical Microscope • Chemistry (etching, grinding) • [..]	**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), TOE specific hardware structures, Principles and concepts of security • Developers knowledge

Table 3: Extent of expertise

22 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.

23 A new level "Multiple Expert" was introduced to allow for a situation, where different fields of expertise are required at an Expert level for distinct steps of an attack. It should be noted that the expertise must concern fields that are strictly different like for example HW manipulation and cryptography.

Expertise	Identification	Exploitation
Layman	0	0
Proficient	1	1
Expert	2	3
Multiple Expert	5	6

Table 4: Rating for Expertise

3.4 Knowledge of TOE

24 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.

25 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.

26 The following classification is to be used:

- **Public information** about the TOE (or no information): Information is considered public if it can be easily obtained by anyone (e.g., from the Internet) or if it is provided by the vendor to any customer.
- **Restricted information** concerning the TOE (e.g., as gained from vendor technical specifications): Information is considered restricted if it is distributed on request and the distribution is registered. Suitable example might be the functional specification (ADV_FSP).
- **Sensitive information** about the TOE (e.g., knowledge of internal design, which may have to be obtained by "social engineering" or exhaustive reverse engineering). Suitable example might be High-Level Design (HLD), Low-Level-Design (LLD) information or the Source Code.

27 Care should be taken here to distinguish between information required to identify the vulnerability and the information required to exploit it, especially in the area of sensitive information. Requiring sensitive information for exploitation would be unusual.

28 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.

Knowledge	Identification	Exploitation
Public	0	0
Restricted	2	2
Sensitive	3	4

Table 5: Rating for Knowledge of TOE

29 Note: Specialist expertise and knowledge of the TOE are concerned with the information required for persons to be able to attack a TOE. There is an implicit relationship between an attacker's expertise and the ability to effectively make use of equipment in an attack. The weaker the attacker's expertise, the lower the potential to effectively use equipment. Likewise, the greater the expertise, the greater the potential for equipment to be used in the attack. Although implicit, this relationship between expertise and the use of equipment does not always apply—for instance, when environmental measures prevent an expert attacker's use of equipment; or when, through the efforts of others, attack tools requiring little expertise for effective use are created and freely distributed (e.g., via the Internet).

3.5 Access to TOE

30 Access to the TOE is also an important factor. It is assumed here that the TOE would be purchased or otherwise obtained by the attacker and that beside other factors there's no time limit in analyzing or modifying the TOE. Differences are defined in the status

and functionality of the device to be analyzed/tested. This shall replace the CEM factor "Access to TOE".

- **Mechanical samples** are non-functional and are used merely to study the mechanical design or for supplying spare parts.
- **Functional samples** without working keys might be used for the logical and electrical behavior of the device but aren't loaded with working keys and are therefore not functional within a payment network or with real payment cards. Such devices might be regularly purchased.
- **Functional samples** with working keys are fully functional devices, which might be used to verify an attack method or to actually perform an attack. If more than one sample is needed in any category, instead of multiplying the points by the number of samples, the following factors must be used.

Samples	Identification	Exploitation
Mechanical sample	1	1
Functional samples without working keys	2	2
Functional sample with working keys and software	4	4

Table 6: Rating for Access to TOE

31 If more than one unit is required, the values must be multiplied by the factors given below.

Number of Devices	Factor
1	1
2	1.5
3-4	2
5-10	4
>10	5

Table 7: Rating for Access to TOE

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

3.6 Equipment

33 Equipment refers to the equipment that is required to identify or exploit vulnerability.

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

- **Standard equipment** is equipment that is readily available to the attacker, either for the identification of vulnerability or for an attack. This equipment

can be readily obtained—e.g., at a nearby store or downloaded from the Internet. The equipment might consist of simple attack scripts, personal computers, card readers, pattern generators, simple optical microscopes, power supplies, or simple mechanical tools.

- **Specialized equipment** isn't readily available to the attacker, but could be acquired without undue effort. This could include purchase of moderate amounts of equipment (e.g., dedicated electronic cards, specialized test bench, protocol analyzers, oscilloscopes, microprobe workstation, chemical workbench, precise milling machines, etc.) or development of more extensive attack scripts or programs.
- **Bespoke equipment** is not readily available to the public as it might need to be specially produced (e.g., very sophisticated software) or because the equipment is so specialized that its distribution is controlled, possibly even restricted. Alternatively, the equipment may be very expensive (e.g., Focused Ion Beam, Scanning Electron Microscope, and Abrasive Laser Equipment). Bespoke equipment, which can be rented, might have to be treated as specialized equipment. Software that has been developed during the identification phase is considered as bespoke equipment; it must not additionally be considered for in the exploitation phase.

35 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.

36 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

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

38 The procedure to rate buy in of specialist equipment is as following:

39 It is possible that some attacks may require some specialist equipment, such as a PIN disclosing bug. One option, in the attack potential calculation is to score the attacker developing the bug himself, adding points to time, expertise and, possibly, specialist equipment.

40 However, some attackers may seek to source such equipment on the open, possibly criminal, market, and buy in a PIN disclosing bug from a third party. The criminal

market place for purchase of equipment intended to support or enable an attack of some kind is well known.

41 The question is whether this possibility should be addressed separately in the attack potential calculation, possibly by the addition of a cost element, or whether it should remain as a combination of existing elements such as expertise, time and specialist equipment.

42 The current methodology, whereby expertise, time and specialist equipment are considered, is sufficient, because, to a great extent, these points may represent the value to the attacker of the purchase of a PIN disclosing bug and that market forces (even criminal market forces) will ensure that the price that the attacker has to pay for the device reflects the value of the device in terms of the attack, and that this can be considered to equate to the points awarded under the current attack potential methodology.

3.7 Tools

43 The border between standard, specialized and bespoke can not be clearly defined here. The rating of the tools is just a typical example. It is a case by case decision depending on state of the art and costs involved. The following tables are just a general guideline.

Tool	Equipment
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 equipment	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 8: Rating for Access to TOE

3.7.1 Design verification and failure analysis tools

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

45 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 (SEM)	Bespoke
E-beam tester	Bespoke
Atomic Force Microscope (AFM)	Bespoke
Focused Ion Beam (FIB)	Bespoke
New Tech Design Verification and Failure Analysis Tools	Bespoke

Table 9: Categorisation of Tools (2)

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

47 The level "Multiple Bespoke" is introduced to allow for a situation, where different types of bespoke equipment are required for distinct steps of an attack.

Equipment	Identification	Exploitation
None	0	0
Standard	1	2
Specialized (1)	3	4
Bespoke	5	6
Multiple Bespoke	7	8

Table 10: Rating for Equipment

(1) If clearly different testbenches consisting of specialised equipment are required for distinct steps of an attack this shall be rated as bespoke.

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

3.8 Parts

49 Parts refer to components required to hide the signs of an attack; to otherwise replace components that have been broken during an attack, like a case part, a display or a printer; to created data-monitoring or communicating bug; or otherwise are needed to perform the attack. If the same part may be used for identification and exploitation, it must only be accounted for once.

- **Standard parts** are readily available to the attacker, either by purchasing them from a supply store or by re-using parts from a mechanical sample of the same device.
- **Specialized parts** are not readily available to the attacker but could be acquired without undue effort. These might be parts that can be ordered

from the stock but require long delivery time or a certain minimum component count for purchase.

- **Bespoke parts** are not readily available and have to be specifically manufactured. It is very unlikely that an attack requires bespoke spare parts.

Parts	Identification	Exploitation
None	0	0
Standard	1	1
Specialized	2	2
Bespoke	4	4

Table 11: Rating for Parts

3.9 Final Table

Factors	Identification	Exploitation
Elapsed time		
< one hour	0	0
< one day	1	2
< one week	2	3
< one month	3	4
> one month	5	7
Expertise		
Layman	0	0
Proficient	1	1
Expert	2	3
Multiple Expert	5	6
Knowledge of the TOE		
Public	0	0
Restricted	2	2
Sensitive	3	4
Access to TOE		
Mechanical sample	1	1
Functional samples without working keys	2	2

Factors	Identification	Exploitation
Functional sample with working keys and software	4	4
Equipment		
None	0	0
Standard	1	2
Specialized (1)	3	4
Bespoke	5	6
Multiple Bespoke	7	8
Parts		
None	0	0
Standard	1	1
Specialized	2	2
Bespoke	4	4

Table 12: Final table for the rating factors

(1) If clearly different testbenches consisting of specialised equipment are required for distinct steps of an attack this shall be rated as bespoke.

3.10 "Partial" or "Complete" Attacks

50 Each attack shall be identified as either "Partial", meaning that other attacks have to be completed in order to compromise POI assets, or "Complete" in which case a successful attack directly compromises one or more assets.

51 An example of a "Partial" attack would be to attack a PCB switch, but usually there are other security barriers which must be overcome before an asset is compromised.

52 An example of a "Complete" attack would be to monitor keyboard sounds as this attack directly compromises the PIN, which is one of the defined POI assets.

53 In the case of a "Complete" attack the attack potential calculation gives the attack potential for the whole attack.

54 There should be an approach defined for combining attack potentials, in cases where two or more "Partial" attacks need to be combined in order to compromise an asset. A suggested method is identified below.

3.11 Combination of "Partial" Attack Potentials

55 Where multiple attack steps have to be combined in order to comprise an attack which compromises an asset the overall attack potential should be calculated as follows:

56 Initially add the attack potential ratings of each "Partial" attack step required. Scores for Identification and Exploitation should be maintained separately as well as an overall total.

57 Individual elements of each attack step should then be reviewed to identify whether there is overlap between steps. For example, if the same "Expert" is involved in more than one step this score should only count once. If the "Expert" is different in each step then the "Expert" score should, remain for each step.

58 If the same "Expert" is required in multiple steps, then these cannot be paralleled, and the timescales should reflect consecutive working rather than parallel. If the "Expert" is different then attack steps may be run in parallel and the overall timescale score for the complete attack should be reduced accordingly.

59 Similarly, if specialist equipment is required, but the same specialist equipment is required in multiple steps, the score for this should only be counted once.

60 In this way an overall score for a complete attack can be constructed.

61 An example of a two step attack is shown below, with individual step attack potentials, and a combined attack potential rating. It should be noted that each combination of steps should be treated on its own merits, and that there is no direct mathematical way to establish the overall attack potential resulting from multiple attack steps.

62 **Example Calculation**

63 Suppose that a combination of Steps 1 and 2 compromise one or more assets. That is to say that the two "Partial" attacks (step 1 and step 2) combine to form a "Complete" attack. This is not necessarily the case, but the example serves to demonstrate the method for combining attack potentials.

64 Step 1 - Removal Sensor Deactivation

Factor	Comment	Ident'n	Exploit'n
Elapsed Time	Elapsed time to identify the switch configuration and train attacks. Exploit time will cover removal bug insertion and replacement	≤ one week 2	≤ one day 2
Expertise	Any skilled amateur or professional modeller.	Proficient 1	Proficient 1
Knowledge of TOE	No private knowledge required	Public 0	Public 0

Factor	Comment	Ident'n	Exploit'n
Access to TOE (per unit)	Mechanical sample(s) required to identify the switch configuration and train attacks. Field device required to finally mount the attack.	Mechanical Sample 1	Functional sample with working keys 4
Equipment	Equipment is readily available in any hardware store.	Standard 1	Standard 2
Parts	No parts required	None 0	None 0
Sub Total		**5**	**9**
Total		**14**	

65 Step 2 - Case Switch Deactivation

Factor	Comment	Ident'n	Exploit'n
Elapsed Time	Elapsed time to identify the switch configuration and train attacks. Exploit time will cover removal bug insertion and replacement	≤ one week 2	≤ one day 2
Expertise	The attack requires excellent mechanical skills for any decent success rate.	Expert 2	Expert 3
Knowledge of TOE	No private knowledge required	Public 0	Public 0
Access to TOE (per unit)	Mechanical sample(s) required to identify the switch configuration and train attacks. Field device required to finally mount the attack.	Mechanical Sample 1	Functional sample with working keys 4
Equipment	Equipment is readily available in any hardware store.	Standard 1	Standard 2
Parts	Selection of glues, material to build a mould	Standard 1	None 0
Sub Total		**8**	**11**

Total	18

66 Thus the initial combined attack potential would be:

Identification: 8 + 5 = 13

Exploitation: 9 + 11 = 20

Overall total: 33

67 However, on inspection it may be considered that the same "Expert" (modeller or person with excellent mechanical skills) can perform both attacks and, therefore, the Expert scores should only be included once. In this case the higher scores remain, but the lower scores, for step 1, are subtracted from the overall scores, leaving:

Identification: (8 - 1) + 5 = 12

Exploitation: (9 - 1) + 11 = 19

Overall total: 31

68 However, it is not likely that any reduction can be made for paralleling the timescales, especially if the same expert is used, so the full ratings for Identification and Exploitation of the attack remain.

69 It should be noted that this is only intended to be an example of how to combine attack ratings, and that each combination of attack steps should be treated on its own merits, and the reasons for modifying scores should be well documented.

3.12 Range for CC v3

70 The following table replaces table B.4 of CEM, para 1988 for POIs.

Range of values*	TOE resistant to attackers with attack potential of:
0-13	No rating
14-15	POI-Basic
16-24	POI-Low
25-34	POI-Moderate
35 and above	POI-High

Table 13: Rating of vulnerabilites for CC v3

*final attack potential = identification + exploitation.

4 Examples of Attacks

71 The following examples have been compiled by a group of security experts representing the different actor groups involved in the development, production, security evaluation and distribution of a POI product (hardware vendors, POI vendors, OS provider, evaluation labs, certification bodies, service providers).

72 The collection represents the current state of the art at that time (Q3/08). As state of the art is not static this document is under review of the same expert group and will be updated if necessary.

73 For the evaluation of a TOE at least these examples have to be considered. This does not mean that in any case all attacks have to be carried out. For each TOE the evaluation laboratory conducting the evaluation has to select the appropriate attacks from this catalogue in agreement with the certification body. This selection will be dependent on the type of the TOE and additional tests may also be required.

74 In this document only a general outline of the attacks is given. For more detailed descriptions and examples, please refer to the certification bodies. They can also provide examples as reference for rating.

75 POIs may be implemented by different electronic architectures, different electronic components may exist within a POI: Printed Circuit Boards (PCBs), Integrated Circuits like CPUs or memory elements, resistors, sensors, switches, … In the following a PCB includes any component and circuit on it. Components may be ICs, memory elements, switches, circuits, … Note: A POI may consist of different PCBs.

4.1 Minimal Invasive or Non-Invasive Physical Attacks

76 The following attacks bypass any tamper-responsive mechanism in order to disclose unciphered secret data (Plaintext-PIN) or secret keypad entries.

- Insert PIN disclosing bug using a flexible Printed Circuit Board (PCB): The interface to the IC card is tapped to disclose unciphered secret data when transferred via the interface. The flexible PCB is inserted into the slot of the IC card reader.
- Wire attacks: The I/O pin of an IC card reader is contacted with a wire to disclose unciphered secret data when transferred. This can be done e.g. by inserting the wire through the slot of the IC card reader.
- Attack unused keys to tap the keypad matrix in order to disclose secret data during entry.
- Monitoring keypad entries by scanning POI power supply in order to disclose secret data during entry.

77 The main impacts is:

- Disclosure of the Plaintext-PIN (flexible PCB, wire attacks).
- Disclosure of any PIN (unused keys at keypad, scanning POI power supply).

4.2 Intrusion of Sensors, Switches and Filters

78 This attack covers ways of deactivating or avoiding the different types of sensors amd filters that a POI may use to monitor the environmental conditions and to protect itself from conditions that would threaten correct operation of the TOE. Switches are used to recognise tampering.

79 Hardware or software may use the outputs from sensors, filters and switches to take action to protect the TOE.

80 The main impacts are:

81 Sensors, filters and switches may be overcome by:

- Disconnection
- Deactivation (switches)
- Changing the behaviour of the sensor and switch
- Finding gaps in the coverage of the monitored condition (e.g. voltage), or of the timing of monitoring.

82 Sensors may also be misused, in order to exploit activation of a sensor as a step in an attack. This misuse of sensors is a separate attack.

83 The different types of sensors and filters include:

- Voltage (e.g. high voltage or voltage spike)
- Frequency (e.g. high frequency or frequency spike)
- Temperature

84 The different types of tamper responsive switches include:

- Mechanical switches (case, keypad)
- Logical switches (e.g. connectors)

85 The main impacts are:

86 The correct operation of a POI (and its security module) can no longer be guaranteed outside the safe operating conditions when sensors and filters are overcome. The impact of operating under these conditions may be of many sorts. For example:

- Contents of memory or registers may be corrupted
- Program flow may be changed
- Failures in operations may occur (e.g. CPU, coprocessors, RNG)
- Change of operating mode and/or parameters (e.g. from user to supervisor mode)
- Change in other operating characteristics (e.g. changed leakage behaviour; enable other attacks like RAM freezing).

Overcoming switches allows to access further parts of the POI like ICs or circuits. This can be used for further attacks. The misuse of a switch is a separate atck.

4.3 Physical Attacks to Retrieve Secret Data

87 Physical attacks may consist of penetrating a security grid or potting material. If the penetration is succesfull, ethe attacker has access e.g. to the PCB of the security module with its ICs, circuits or any other component. Having access to these electronic componets the attacker e.g. could physically access memories. Such attacks are often independent of the embedded software (i.e. it could be applied to any embedded software and is independent of software counter measures).

88 Architectures exist where the functionality of a security module is embedded in a IC (e.g. in a Application Specific Integrated Circuit, ASIC). Here physical attacks as known to attack smart card ICs can be applied. Microelectronic tools enable to either access or modify such an IC by removing or adding material (etching, etc). Depending on the tool and on its use the interesting effect for the attacker is to extract internal signals or manipulate connections of the IC by adding or to cutting wires. Physical attack are related to characteristics of a Ball Grid Array design (BGA) accessing the contact of the BGA IC to the PCB.

89 Also the keypad used for PIN entry can be physically attacked monitoring the keys when pressed by the cardholder. For this purpose the keypad has to be manipulated without leaving traces.

90 The main impacts are:

- Access to secret data such as secret cryptographic keys or PINs by extracting internal signals transferring secret data
- Disconnecting security features to make another attack easier (DPA, perturbation)
- Forcing internal signals
- Even unknown signals could be used to perform some attacks

91 The potential use of these techniques is manifold and has to be carefully considered in the context of each evaluation.

4.4 Perturbation Attacks

92 Perturbation attacks (e.g. glitches) change the normal behaviour of a POI in order to create an exploitable error in the operation of a TOE. The behaviour is typically changed by operating the POI or part of the POI (e.g. the security module) outside its intended operating environment (usually characterised in terms of temperature, Vcc and the externally supplied clock frequency).

93 Chapter 4.3 concerns itself more with the methods to induce meaningful faults whereas Chapter 4.4 describes how these induced faults may be used to extract keys from cryptographic operations.

94 The attack will typically aim to make cryptographic operations weaker by creating faults that can be used to recover keys or PINs, or to avoid or change the results of checks such as authentication or else change the program flow.

95 Perturbations may be applied to either the PCB and its components of a POI or a software/composite TOE (an OS or application running on a POI).

96 The main impacts are:

97 For attackers, the typical external effects on a PCB running a software are as follows:

- Modifying a value read from memory during the read operation: The value held in memory is not modified, but the value that arrives at the destination (e.g. CPU or coprocessor) is modified. This may concern data or address information.
- Changing the characteristics of random numbers generated (e.g. forcing RNG output to be all 1's) – see Attacks on RNG 4.5 for more discussion of attacks on random number generators.
- Modifying the program flow: the program flow is modified and various effects can be observed:
    - Skipping an instruction
    - Inverting a test
    - Generating a jump
    - Generating calculation errors

98 It is noted that it is relatively easy to cause communication errors, in which the final data returned by an IC on a PCB is modified. However, these types of errors are not generally useful to an attacker, since they indicate only the same type of errors as may naturally occur in a communication medium: They have not affected the behaviour of the PCB while it was carrying out a security-sensitive operation (e.g. a cryptographic calculation or access control decision).

99 The range of possible perturbation techniques is large, and typically subject to a variety of parameters for each technique. This large range and the further complications involved in combining perturbations means that perturbation usually proceeds by investigating what types of perturbation cause any observable effect, and then refining this technique both in terms of the parameters of the perturbation (e.g. small changes in power, location or timing) and in terms of what parts of software are attacked. For example, if perturbations can be found to change the value of single bits in a register, then this may be particularly useful if software in a TOE uses single-bit flags for security decisions. The application context (i.e. how the TOE is used in its intended operating environment) may determine whether the perturbation effect needs to be precise and certain, or whether a less certain modification (e.g. one modification in 10 or 100 attempts) can still be used to attack the TOE.

4.5 Front Side Attacks

100 Front Side Attacks are physical attacks to the PED consisting in monitoring key entry, especially the PIN entry by the cardholder. The cryptographic key is not the objective of this attack. Key entry shall be monitored without beeing detected by the cardholder or by the merchand.

4.6 EMA and Sound Attacks

101 When a POI is operating, each individual element will emit electromagnetic radiation (e.g. microwave) in the same way as any other conductor with a current flowing through it. Due to the change of the data processed, small changes in the current flow will be the result. These current flow changes lead to an electromagnetic emission depending on the processed data.

102 Electromagnetic Analysis (EMA) attacks measure these electromagnetic emissions from a POI during its operation and inferences to the data processed.

103 The attack will typically aim to recover secret cryptographic keys or PINs.

104 When keys of the keypad are pressed sounds is emitted. Also this can be monitored in order to detect PINs when entered.

4.7 Attacks on RNG

105 Attacks on RNGs aim in general to get the ability to predict the output of the RNG (e.g. of reducing the output entropy) which can comprise:

- past values of the RNG output (with respect to the given and possibly known current values),
- future values of the RNG output (with respect to the possibly known past and current values),
- forcing the output to a specific behaviour, which leads to:
    - known values (therefore also allowing for the prediction of the output),
    - unknown, but fixed values (reducing the entropy to 0 at the limit),
    - repetition of unknown values either for different runs of one RNG or for runs of two or more RNGs (cloning) .

4.8 Software Attacks

106 Most of the examples of attacks in this document require hardware attack steps for all or part of the attack. However, it is clear that there are many relevant attacks that can be made on software alone. This section considers some of these attacks. In many cases software attacks start with source code analysis.

107 In general, it is important to note that most software attacks arise from errors (bugs) in the TOE, either in design or implementation. In these cases, the error will generally result in a failure to meet the requirements of one (or more) of the ADV families (e.g. ADV_IMP.1.2E: The evaluator shall determine that the least abstract TSF representation provided is an accurate and complete instantiation of the TOE security functional requirements). Hence an error of this sort will cause the TOE to fail evaluation (or, more usually, will require a modification to the TOE to correct the error).

108 In some other cases, a design's specification may be insufficient to meet the TOE security objectives: for example, a protocol specification might itself contain critical vulnerabilities. This would also cause a TOE to fail the evaluation.

109 This section therefore lists a number of attack steps that may be used to discover software errors, but no attack potential examples are given, since if any error is discovered then it must be corrected if the TOE is to pass evaluation.

110 In the text below we consider first an information gathering attack step, which may be relevant to a number of different types of attack. We introduce five specific attack techniques that may exploit software vulnerabilities:

- Editing commands
- Direct protocol attacks
- Man-in-the-middle attacks
- Replay attacks
- Buffer overflow

111 The attacks are of a logical nature, the test environment consists of a POI connected to a PC via the IC card interface or via any other security relevant interface, e.g. the online interfaces. The PC runs communication software, a protocol analyser and some development tools to modify communication. This tool set is considered to be standard equipment. Tools for the IC card interface are available as freeware on the Internet, and they can be modified quite easily to fit the attackers' needs. Usually the online interface also meets an open standard but probably tools are not available via the internet.

112 To perform such attacks, it is necessary to have:

- a means to listen to message sequences (reader, traffic analyser)
- a means to create messages (information on external API, pattern generator)
- a means to interrupt messages without detection (protocol dependent)

113 Setting up a test environment and identifying an attack is quite simple, as the tools are standard (IC card interface) and therefore public knowledge. This holds also for theo online interface. In case of a proprietary change, the expertise needed is slightly higher because the communication must be interpreted. However, in most cases this would be expected to be relatively straightforward, and this type of 'security by obscurity' would not be considered a valid defence against attack.

4.9 PIN and Cryptographic Key Related Protocol Attacks

114 Because of PIN entry and processing and PIN related cryptographic key import and export specific protocol attacks can be identified for POIs. These attacks are related to the disclosure of PINs by successfully compromising encrypted PIN blocks or functions to import resp. export PIN related cryptograpic keys.

5 References

[CC] *Common Criteria for Information Technology Security Evaluation*, Version 3.1, Revision 3, July 2009.

[CEM] *Common Methodology for Information Technology Security Evaluation (CEM)*, Version 3.1, Revision 3, July 2009.

[CASPOIPP] *Point of Interaction Protection Profile*, Version 2.0, 26th November 2010, Common Approval Scheme POI Working Group

[AttackPotIC] *Joint Interpretation Library, Application of Attack Potential to Smartcards*, Version 2.7, February 2009

[AttackMethIC] *Joint Interpretation Library, Application of Attack Potential to Smartcards*, Version 2.0, February 2011

[AttackMethPOI] *Joint Interpretation Library, Attack Methods for POIs*, Version 1.0, 9th June 2011

[CEM POI] *Joint Interpretation Library, CEM Refinements for POI Evaluation*, Version 1.0, 9th June 2011

[PCI_CoAT] *Collection of Attack Techniques Confidential Security Analysis & Testing*, Table of Contents, Payment Card Industry (PCI)

[RNGPCI] *Payment Card Industry (PCI) POS PIN Entry Device (PED), Version 2.1, Appendix C*

Rukhin, Andrew, et al., "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", NIST SP800-22, revisions dated May 15, 2001.

Kim, Song-Ju, et al., "Corrections of the NIST Statistical Test Suite for Randomness".

Bassham, Larry (NIST). "Validation Testing and NIST Statistical Test Suite" presentation, dated July 22, 2004.

Hill, Joshua (InfoGard Labs). "ApEn Test Parameter Selection".