Common Criteria Recognition Arrangement

Management Committee

Policies and Procedures

Document Number: 2009-03-003

Date: [March, 2009]

Subject: Requirements to perform Integrated Circuit Evaluations

1 Rationale

The CCRA requires Evaluation Facilities to be accredited according to the requirements of EN 45001 or ISO Guide 25 (now superseded by ISO 17025), unless the Evaluation Facility has been established under a law or statutory instrument. Furthermore the CCRA requires Evaluation Facilities to demonstrate to the satisfaction of the CB that it is technically competent in the specific field of IT security evaluation.

Requirements for the accreditation are described in ISO/IEC 17025 [1] and specifically in chapter 5, there are requirements for the technical skills and the necessary equipment to be available.

This procedure is intended to provide guidelines for the technical accreditation and licensing of Evaluation Facilities for performing integrated circuit evaluations.

2 Introduction

In order to ensure credible results from the evaluation of smartcard integrated circuits (ICs) according to the Common Criteria, an IT-Security Evaluation Facility (ITSEF) must have a minimum set of capabilities. These capabilities differ from those required for software systems in both the equipment required and the skills and knowledge needed by the evaluator.

3 Required Knowledge and Skill

3.1 Overview

The required knowledge and skill of the evaluator can be grouped as follows:

- understanding of the smartcard design and production process in general and of the IC design and manufacturing process (refer to section 3.2),
- understanding of smartcard IC technology, its underlying principles and the development equipment used by IC manufacturers (refer to section 3.3),
- knowledge of smartcard fraud and attack scenarios,

- knowledge and experience in IC failure analysis, an understanding of the underlying physical principles and an ability to use the related equipment (refer to section 3.4),
- knowledge and experience in cryptographic attack techniques and the ability to perform the analysis (including data-capture and signal processing procedures) (refer to section 3.4).

In addition, the ITSEF will need equipment pertinent for IC failure analysis, diverse other smartcard attacks and cryptographic attack techniques (refer to section 3.4). The required tools can be categorised in standard (basic), specialised and bespoke (refer to section 3.5).

3.2 IC Design and Production Process

IC hardware and software is in general developed by different companies. These components are then integrated and additional security relevant data is injected into the card.

The security objectives for an IC are twofold:

- Ensure a level of security for the card in the field.
- Maintain the level of security throughout the development and production process.

Although many specialists concentrate on security in the field (since the smartcard is delivered into a hostile, unregulated environment and may be subject to tampering), security during the development, production and personalization process is also important. The security objectives, that a smartcard component are assessed against, will depend very much on the application context which can be dependent upon the production and personalization process. In particular, personalization affects the security functionality to be provided by the smartcard.

The Common Criteria depict an ideal development process starting with a definition of the requirements followed by the design process, implementation, test, acceptance, delivery and usage. When looking at the components of a composite product this process must be interpreted and rearranged.

For instance, the chip manufacturer develops the design of the chip hardware and the software for testing. He receives the software from the software developer to create the ROM image. Then the mask files are sent to the mask manufacturer. The masks or reticles are returned to the chip manufacturer. After wafer production the chips are tested and initialisation data (transport keys, traceability data) are injected into the E2PROM (or other non-volatile memory). The initialisation data are defined by the card manufacturer. Operational dies are delivered or directly embedded into modules. The protection of die delivery can be complex: The authentication mechanism is realised by the software manufacturer but used by the card manufacturer (or personalisation centre). The keys are generated by the card manufacturer but injected into the card by the chip manufacturer using a procedure (for diversification etc.) defined by the card manufacturer.

These examples show that a real development process can be more complex than the assumed one by the Common Criteria. Inputs and outputs are not always as simple as expected by the Common Criteria. As a result, the corresponding assurance components of the Common Criteria (for instance delivery) must be interpreted, refined, and rearranged if

needed. In addition, it must be ensured that the processes of different components (and their description in terms of Common Criteria assurance components) fit together.

The evaluators must understand the smartcard supply chain and its integration into the application context in order to be able to interpret the Common Criteria assurance requirements in an appropriate way. In particular, these assurance requirements are:

- Guidance,
- Delivery,
- Installation, Generation and Start-Up,
- Tools and Techniques,
- Life-Cycle Definition, and
- Development Security.

In addition, differences between the evaluation of smartcard ICs and the evaluation of software means that the interpretation of the Common Criteria assurance components of the classes ASE, ADV, ATE and AVA is also required.

These interpretation of the Common Criteria assurance components and additional guidance are described in several CC Supporting Documents for Smartcards and similar devices that are published on www.commoncriteriaportal.org website.

Note that the evaluator also needs to understand the smartcard IC design and manufacturing process since it can not be expected that each IC manufacturer will describe their processes and security measures without assuming such an understanding.

3.3 Smartcard Integrated Circuit Technology

The evaluator must understand smartcard integrated circuit technology and the underlying principles to the extent necessary to comprehend the design decisions of the IC manufacturer. Basic knowledge is required of:

- electron theory of semiconductors (physics) and the electrical behaviour of semiconductors and transistors,
- physical and electrical behaviour of all standard materials used in integrated circuit manufacturing (for instance silicon, poly-silicon, metal, and isolating and passivation material),
- physical layout (implementation on the semiconductor surface) of standard cells (simple gates), memory cells (E2PROM, RAM, ROM) and memory blocks,
- layout principles and methods of routing and layering,
- production steps and the resulting layer structure on the chip's surface.

In addition, the evaluator must have detailed knowledge of:

- digital and analogue circuit engineering (digital gates of different complexity and standard analogue circuitry),

- static and dynamic behaviour of digital and analogue circuitry,
- microcontroller architecture and functionality,
- realisation of standard circuitry as used in micro-controllers.

The evaluator must be able to understand the schematics (block diagrams, schematics on gate and transistor level). The functional components can be described in the form of standard schematics or in VHDL-sources.

The evaluator must have knowledge of the VLSI design process and must basically understand the process from the schematics or VHDL-sources (logical representation of the chip) to the actual layout and dice/wafers (physical representation). The evaluator must understand the processes of technology qualification, functional testing, characterisation, and reliability testing.

The evaluator must understand the development equipment used by the manufacturers for micro-controller software. This includes simulators, emulators, and special evaluation software masks. The evaluator must be able to read micro-controller source code and to develop software for penetration testing and other investigations. Therefore, the evaluator must understand the CPU instruction set, the memory map and use of other peripheral units of the micro-controller.

3.4 Smartcard Specific Attacks

The following provides an overview about smartcard specific attacks. This is not a complete list but provides some examples. Detailed information about smartcard specific attacks can be found in 'Annex A: Examples for Smartcard specific Attacks' of this procedure.

The evaluator must know about standard smartcard fraud and attack scenarios and in principle be able to develop new ideas for such attacks. In addition, the evaluator must know about attack scenarios for ICs such as physical manipulation and probing, malfunction attacks, inherent and forced leakage attacks, abuse of test features, cryptographic or software attacks, which are not described here.

The evaluator must be able to adapt and combine these attack scenarios for the individual chip being subject to evaluation. During vulnerability analysis the evaluator must be able to find possible weaknesses (in schematics and their realisation on the chip and the combination thereof) and be able to use the standard techniques to assess them.

The evaluator must have knowledge and experience in IC failure analysis to be used for physical manipulation and probing. The evaluator must at least understand the physical principles, and the usage (as appropriate) of the equipment classed as 'standard' and 'specialised' (in section 3.5). Moreover, the evaluator must be able to use the 'bespoke' tools with the help of trained operators. The evaluator must know how these tools and techniques can be used during vulnerability analysis in order to assess the IC’s security properties and functions. The method and purpose of using the equipment (especially Focused Ion Beam (FIB), Scanning Electron Microscope (SEM) or E-beam Tester) during the vulnerability assessment should not necessarily correspond to the expectations of the operating personnel. The evaluator should instruct the operating personnel.

The evaluator must have knowledge and experience of other smartcard attacks (such as Differential Power Analysis (DPA), Differential EM radiation Analysis (DEMA) and related attacks) and possess the equipment (physical and analysis tools) necessary to perform such attacks. The evaluator must be able to operate this equipment (including data-capture procedures) and to perform the analysis (mathematics). Knowledge and experience in cryptography and standard cryptographic attack techniques is required. The principles of timing and other attacks (such as Differential Fault Analysis (DFA)) must be understood. The evaluator must be able to find vulnerabilities related to such attacks.

The evaluator must be able to develop software to communicate with the smartcard. Therefore, the evaluator must understand the I/O protocol being supported, the operating conditions and the external command interface if being used or attacked.

The evaluator must know how to handle chip card readers and be able to modify them in order to use the chips in different packages and to apply non-standard operating conditions. Therefore, the evaluator must be able to use standard equipment such as voltage supply, signal and function generators, oscilloscopes, and soldering irons.

3.5 The IT-Security Evaluation Facility (ITSEF)

The IT-Security Evaluation Facility (ITSEF) must be well organised and provide instructions for the evaluator. These instructions must describe physical, procedural and organisational security measures or refer to other documents, which describe them. A Quality Management System must exist. The requirements of ISO/IEC17025 must be met. In order to accomplish the vulnerability and failure analysis, physical manipulations, and attack scenarios mentioned in section 3.4, the IT-Security Evaluation Facility must have unrestricted access to the tools necessary to perform those attacks and shall be able to use them efficiently. Examples of these equipments and their categorisation are listed below. Please refer to the CC Supporting Document ‘Application of Attack Potential to Smartcards’ for an up-to-date list of necessary equipment with their categorisation.

Standard equipment, e.g.:

- UV-light emitter
- Flash light
- Low-end visible-light microscope
- Climate chamber
- Voltage supply
- Analogue oscilloscope
- Chip card reader
- PC or work station
- Signal analysis software
- Signal generation software

Specialised equipment, e.g.:

- High-end visible-light microscope and camera
- UV light microscope and camera
- Microprobe work station
- Laser cutter
- Signal and function processor
- High-end digital oscilloscope
- Signal analyser
- Tools for chemical etching (wet)
- Tools for chemical etching (plasma)
- Tools for grinding

Bespoke equipment, e.g.:

- Scanning electron microscope (SEM)
- E-beam tester
- Atomic Force Microscope (AFM)
- Focused Ion Beam (FIB)
- New technical design verification and failure analysis tools

The optical microscope and a camera must give sufficient magnification and resolution for the technology being assessed. The Microprobe Workstation must be equipped with appropriate needles. Supply equipment (voltage supply, signal and function generators) must be available.

For the equipment categorised as 'bespoke', the evaluator must have a good understanding of the underlying physical principles and of the capabilities of the tools. If the ITSEF uses other facilities, appropriate security measures must be applied to protect the chip vendor's information and samples, and the know-how of the ITSEF. If the ITSEF hires bespoke equipment, the evaluator must be present and must instruct the operating personnel.

3.6 Subcontracting with a specialised IT-Security Evaluation Facility

When an ITSEF subcontracts work, this work shall be placed with a competent subcontractor. A competent subcontractor is one that, for example, complies with the International Standard for the work in question. ISO/IEC 17025 permits subcontracting of work subject to certain conditions.

4 Summary

This document has described the knowledge, skills and facilities required by an ITSEF before it can be capable of preparing and carrying out an evaluation of smartcard integrated

circuits. These capabilities are not limited to having access to sophisticated types of equipment and the knowledge of how to use them. Moreover, the ITSEF evaluator should completely comprehend the smartcard design and production process and have the ability to develop and test for new attack scenarios. This knowledge cannot be gathered through short-term training but requires years of relevant experience.

If an ITSEF is known to meet the guidelines in this document, then a level of confidence will be provided to both the manufacturers (paying for the evaluation) and to the customers (accepting a certificate). Without these guidelines, that confidence can only be deduced by examining the detailed information from evaluation reports (although that still remains the ultimate measure of the ITSEF's performance).

5 Literature

[1] ISO/IEC 17025: General requirements for the competence of testing and calibration laboratories

Requirements to perform Integrated Circuit Evaluations
Annex A:
Examples for Smartcard Specific Attacks

1 Examples of Smartcard Specific Attacks

The objective of this paper is to provide some examples of attacks that an ITSEF should be able to execute during the evaluation. The reader should realise that this is not a complete list.

The following attacks are not applicable for all kind of evaluations (e.g. a pure smartcard hardware will undergo other tests than an IC with certain SW on it).

A short description on the generic categories of smartcard potential attacks is given hereafter in order to have an understanding on these attacks.

1.1 Physical modification

Characteristics of the attack:

The attack is invasive and the chip is physically changed.

Objectives of the attack:

Two main directions:

A) extracting information without authorisation

B) changing the behaviour of the IC

Generic method:

The attacker removes physical layers (either totally or locally), lays open the target device or wire, contacts it. Additionally, he may change wiring or devices (cutting, new connections) to get a new behaviour of the circuitry (as in case B).

Targets are active devices and connecting lines. In many cases the attacker must apply these physical manipulations without destroying the device.

To successfully apply these methods in most cases re-engineering (at least partially) of the device has to be done.

Skills and tools:

Basically for both cases the needed skills and tools are the same. Depending on technology and layout details (e.g. number of layers, layout dimensions, density of design) of the attacked device the selection and the sophistication of the required skills and tools can vary greatly. Case B attacks require deeper knowledge about the functioning of the attacked device.

Skills:

- selective removal (total or local) of IC layers for example mechanically (grinding), chemically (dry or wet etching), locally evaporating (laser)
- applying contact pads to devices and connecting lines
- contacting devices and connecting lines in possibly locally very restricted areas (either directly or via applied contact pads)
- rewiring of circuitry or connecting lines (mainly in case B attacks)
- applying and analysing of electrical signals

Tools:

- etching equipment (great variation from simple wet etching equipment to high sophisticated plasma etching equipment)
- probe station (from simple to very sophisticated for new technologies with very small dimensions)
- microscope
- oscilloscope
- laser cutter
- FIB
- logic analyser
- PC and software (for addressing the device)
- interface hardware (mostly customised for the device and the attack)

PP Examples:

SCSUG-SCPP/ BSI-PP-0003	Physical Probing of the IC: T.P_Probe; Physical Alteration of the IC: T.P_Alter;
BSI-PP-0035	Physical Manipulation: T.Phys-Manipulation Forced Information Leakage: T.Leak-Forced
PP/9911	Unauthorised disclosure: T.DIS_ES2

References:

- Usenix Workshop on Smartcard Technology 1999: *Design Principles for Tamper-Resistant Smartcard Processors*. Markus Kuhn, Oliver Kömmerling. ISBN1-880446-34-0
- F.Beck: *Integrated Circuit Failure Analysis – A Guide to Preparation Techniques*. John Wiley & Sons, 1998
- T.W. Lee:, S.V. Pabbisetty: *Microelectronic Failure Analysis, Desk Reference*. 3rd edition, ASM International, Ohio, 1993, ISBN 0-87170-479-X
- R.J. Anderson, M.G. Kuhn: *Tamper Resistance – a Cautionary Note*. In *The Second USENIX Workshop on Electronic Commerce Proceedings*, pp. 1 – 11, Oakland, California 1996
- J.H. Daniel, D.F. Moore, J.F. Walker: *Focused Ion Beam for Microfabrication*, Engineering Science and Education Journal, pp 53 – 56, April 1998

1.2 Reverse engineering (observation)

Characteristic of the attack:

This type of attack aims to identify the internal structure of the chip, the location and functionality of building blocks of the chip as well as their interconnections.

Objectives of the attack:

The main objective is trying to identify the structure of the chip as well as detailed information on the internal operation of the chip's building blocks and their interconnections.

Thus preparatory work is done for physical attacks (probing, disconnect security functions, extracting internal information, changing behaviour).

Generic method:

- A number of steps are performed:
- remove the chip from the housing; thus the die surface of the chip becomes available for visual inspection
- determine the number of layers, metal shielding, bus design (scrambling), sensors
- remove layer after layer
- image the separate layers
- interpret and combine the images of the layers and derive the function of the separate components (CPU, memory, I/O, security logic, sensors) as well as their interrelationships

Skills and tools:

- knowledge on chip design and architecture

- knowledge on etching techniques – etchants, decapsulator, polishing wheel
- microscope
- photography or image processing – microphotography equipment, image processing equipment

PP Examples:

SCSUG-SCPP/ BSI-PP-0003	Physical Probing of the IC: T.P_Probe; Physical Alteration of the IC: T.P_Alter; Cloning: T.Clon.
BSI-PP-0035	Physical Probing: T.Phys-Probing Physical Manipulation: T.Phys-Manipulation Forced Information Leakage: T.Leak-Forced
PP/9911	Unauthorised full or partial cloning of the TOE: T.CLON Unauthorised disclosure: T.DIS_INFO, T.DIS_DEL, T.DIS_ES1, T.DIS_TEST_ES, T.DIS_ES2

References:

- Usenix Workshop on Smartcard Technology 1999: *Design Principles for Tamper-Resistant Smartcard Processors*. Markus Kuhn, Oliver Kömmerling. ISBN1-880446-34-0
- F.Beck: *Integrated Circuit Failure Analysis – A Guide to Preparation Techniques*. John Wiley & Sons, 1998
- T.W. Lee:, S.V. Pabbisetty: *Microelectronic Failure Analysis*, Desk Reference. 3rd edition, ASM International, Ohio, 1993, ISBN 0-87170-479-X
- R.J. Anderson, M.G. Kuhn: *Tamper Resistance – a Cautionary Note*. In *The Second USENIX Workshop on Electronic Commerce Proceedings*, pp. 1 – 11, Oakland, California 1996
- J.H. Daniel, D.F. Moore, J.F. Walker: *Focused Ion Beam for Microfabrication*, Engineering Science and Education Journal, pp 53 – 56, April 1998

1.3 Cryptanalysis (DPA, DEMA, DFA)

Characteristics of the attack:

This type of attack aims at retrieving sensitive data (generally secret and private keys) while observing the smartcard. Two classes of techniques are discussed: DPA/DEMA and DFA.

1.3.1 DPA/DEMA

Objective of the attack:

Two main objectives:

- getting access to information by observing the power consumption or the electromagnetic emanation of the smartcard
- retrieving sensitive data, secret & private keys

Generic method:

The method is not invasive. The method records useful information such as power absorbed by the card or electromagnetic radiation emanated by the card. Subsequently, these recorded signals (traces) are processed using statistical techniques.

Skills and tools:

- voltage supply
- signal and function processor
- oscilloscope analogue
- oscilloscope digital
- chip card reader
- PC or workstation
- signal analyser
- signal acquisition & processing tools
- antenna for EM radiation (DEMA)

It needs generic laboratory equipment for signal processing. Performing DEMA requires a sensor for obtaining and measuring relevant electromagnetic signals. The required knowledge refers to cryptography, signal analysis, EM radiation characteristics. The required level of knowledge and skill depends on the nature of the attack and on the precise method. It may vary from a medium level to an expert level if advanced techniques are used.

Also required for DPA /DEMA are (i) intense knowledge of the cryptographic algorithm to be attacked, (ii) special software for signal acquisition and processing and (iii) knowledge and software for statistical analyses.

1.3.2 DFA

Objective of the attack:

The attack aims at retrieving secret keys from the smartcard.

Generic method:

The method aims to retrieve secret information from the smartcard by inducing an error while the smartcard is performing a cryptographic calculation. Thus, two kinds of cryptograms are obtained: wrong cryptograms (cryptograms resulting from a disturbed cryptographic operation) and correct cryptograms.

Comparison of both types of cryptograms may reveal information about the used cryptographic key.

Skills and tools:

- electronics able to inject single faults during a cryptographic operation of the card
- voltage supply
- signal and function processor
- oscilloscope analogue
- oscilloscope digital
- chip card reader
- PC or workstation
- signal acquisition & processing tools
- signal generation software

The required knowledge refers to sophisticated knowledge on cryptography, signal analysis and internal chip operation.

PP Examples:

SCSUG-SCPP/ BSI-PP-0003	Insertion of Faults: T.Flt_Ins Information Leakage: T.I_Leak Linkage of Multiple Observations: T.Link Linked Attacks: T.Lnk_Att Cloning: T.Clon
BSI-PP-0035	Inherent Information Leakage: T.Leak-Inherent Abuse of Functionality: T.Abuse-Func Malfunction due to Environmental Stress: T.Malfunction
PP/9911	Unauthorised disclosure: T.DIS_ES2 Theft or unauthorised use: T.T_ES, T.T_CMD

References:

P.Kocher, J.Jaffe, B. Jun, *"Differential Power Analysis"*, in Proceedings of Advances in Cryptology – CRYPTO99, Springer-Verlag, 1999, pp 388-397,

TS.Messerges, E.A. Dabbish and Robert H.Sloan, *"Investigations of Power Analysis Attacks on SmartCards"*, in Proceedings of Usenix Workshop on SmartCard Technology, May 1999, pp. 151-161,

E.Biham, A.Shamir, *Differential Fault Analysis of Secret Key Cryptosystems*, in Proceedings of CRYPTO'97, Lecture Notes in Computer Science, Vol. 1294, Springer, pp 513-528, 1997.

R.Anderson, M.Kuhn, *Low Cost Attacks on Tamper Resistant Devices*, in Proceedings of Security Protocols, 5th International Workshop, Paris, France, April 7-9, 1997, Lecture Notes in Computer Science, Vol. 1361, Springer, pp. 125-136, 1997.

1.4 Protocol attacks

Characteristic of the attack:

This type of attack looks for flaws in the protocol implementation of the smartcard.

Objectives of the attack:

A smartcard protocol specifies the possibilities for communication with a smartcard. It defines the conditions under which the smartcard executes sensitive operations.

The main objective is to find functionality of the smartcard not conforming to the protocols the smartcard supports. In other words, it is investigated if the smartcard executes sensitive operations not specified by the protocol.

Generic method:

In this framework attention is paid to:

- replay attacks
- interrupting the smartcard while it is executing a command
- undocumented commands (are there 'dangerous' commands the smartcard executes but which are not documented?)
- file scanning (are the access controls to the files implemented as stated?)
- undocumented sequences of commands (does the smartcard support sequences of commands not allowed by the protocol?)

Skills and tools:

- knowledge on smartcard protocols
- PC, smartcard reader, test software

PP Examples:

SCSUG-SCPP/ BSI-PP-0003	Forced Reset: T.Forced_Rst; Invalid Input: T.Inv_Inp; Replay Attack: T.Reuse;

	Brute Force Data Space Search: T.Brute-Force; Invalid Access: T.Access; Use of Unallowed Application Functions: T.App_Ftn; Use of Unallowed Life Cycle Functions: T.LC_Ftn; Linkage of Multiple Observations: T.Link; Linked Attacks: T.Lnk_Att; Cloning: T.Clon
BSI-PP-0035	Abuse of Functionality: T.Abuse-Func
PP/9911	Theft or unauthorised use: T.T_ES, T.T_CMD

1.5 Observation Attacks

Characteristics of the attack:

The attack is non invasive (the chip is not changed).

This type of attack is aiming at retrieving sensitive data (generally secret and private keys, depending on the nature of defined assets) while observing the smartcard.

There are various techniques to obtain knowledgeable information from direct observation of the smartcard, e.g. timing attacks (timing observation), SPA, DPA type of attacks.

SPA attacks are described below.

Example : SPA attacks (Simple Power Analysis)

This attack corresponds to a direct analysis of the power consumption of the smartcard. The objective of this attack is to determine for example secret or private key values from the power consumption levels, which set of CPU instructions are being processed, under which parameters (input/output). It may be the case that with a naive smartcard implementation, the cryptographic algorithm parts will be externally visible. This knowledgeable information may be useful to retrieve the values of the secret and/or private keys.

Objectives of the attack:

Two main objectives:

- getting access to information by observing the smartcard output signals
- retrieving sensitive data, secret & private keys using straight forward methods or sophisticated statistical methods

Generic method:

Usually the method is the recording of useful information such as time, I/O, power signals at specific occurrences and the exploiting and analysis of these records.

It needs generic laboratory equipment for signal processing and knowledge of general signal processing techniques.

Skills and tools:

Usually the tools involved are the following:

- voltage supply
- signal and function processor
- oscilloscope analogue
- oscilloscope digital
- chip card reader
- PC or work station
- signal analyser
- signal analysis software
- signal generation software

The required skills depend on the nature of the attack and on the precise method, it may vary from a proficient level up to an expert level if advanced techniques are being used.

PP Examples:

SCSUG-SCPP/ BSI-PP-0003	Insertion of faults: T_Flt_ins Information Leakage: T.I_Leak Linkage of multiple sources: T.Link
BSI-PP-0035	Inherent Information Leakage: T.Leak-Inherent
PP/9911	Unauthorised disclosure: T.DIS_ES2

1.6 Software Attacks

Characteristics of the attack:

This type of attack is looking into software malfunctions of the smartcard.

There are various techniques to execute these attacks, among them malicious software loading, bad formatted commands, all of them exploiting security flaws of the smartcard.

Objectives of the attack:

The main objective is trying to circumvent smartcard security mechanisms and exploit software security flaws.

Generic method

An attacker may load improper software (operating system, executable files) or security data (authentication information, keys, access control information) onto the TOE that could modify or expose software (e.g., security functions) or data on the TOE.

An attacker exploits code delivered by a system or application developer that does not perform according to specifications, contains security flaws, or is not appropriate for operational use.

An attacker or authorised user of the TOE may compromise the security features of the TOE through the introduction of invalid inputs.

Skills and tools

Usually the tools involved are the basic tools to invoke commands to the smartcard and requires a large panel of skills, from low level expertise to high advanced engineering techniques.

PP Examples:

SCSUG-SCPP/ BSI-PP-0003	Invalid inputs: T.Inv_Inp Forced reset: T_Forcd_rst Load bad software: T.Bad_load
BSI-PP-0035	Smartcard embedded software not in the scope of the PP.
PP/9911	Unauthorised Modification: T.MOD_DEL, T.MOD, T.MOD_LOAD, T.MOD_EXE, T.MOD_SHARE, T.MOD_SOFT

1.7 Perturbation Attacks

Characteristics of the attack:

Any IC under stress condition can operate in an unplanned way. Normal behaviour of the software can be changed.

Objectives of the attack:

By putting the IC in stress conditions (e.g. on the power supply or by illuminating it) the normal behaviour of the software can be changed. The effects could be inverting a test, generating a jump, modifying read values from memory, etc.. These modifications could enable an attacker to for example gain access to protected memories or gain rights to perform protected operations.

Generic method:

The generic method in applying a perturbation is the same as the DFA attacks. Various methods for perturbating the IC are available such as glitches, light, laser. Special equipment for heating up or cooling down the smartcard outside the normal temperature range is used as well.

Skills and tools:

- electronics able to inject single faults during a cryptographic operation of the card
- voltage supply
- signal and function processor
- oscilloscope analogue
- oscilloscope digital
- chip card reader
- PC or workstation
- signal acquisition & processing tools
- signal generation software
- flash light generator, laser equipment

PP Examples:

SCSUG-SCPP/ BSI-PP-0003	Environmental Stress: T.Env_Strs
BSI-PP-0035	Malfunction due to Environmental Stress: T.Malfunction Forced Information Leakage: T.Leak-Forced

2 Abbreviations

IC:	Integrated Circuit
FIB:	Focused Ion Beam
DPA:	Differential Power Analysis
DEMA:	Differential EM radiation Analysis
DFA:	Differential Fault Analysis
EM:	Electromagnetic
SPA:	Simple Power Analysis