



Joint Interpretation Library

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

Version 1.1

July 2003

Table of Contents

- 1 Examples of Smartcard Specific Attacks 4**
 - 1.1 Physical modification 4
 - 1.2 Reverse engineering (observation) 6
 - 1.3 Cryptanalysis (DPA, DEMA, DFA)..... 7
 - 1.4 Protocol attacks..... 10
 - 1.5 Observation Attacks..... 11
 - 1.6 Software Attacks..... 13
 - 1.7 Perturbation Attacks 14

- 2 Abbreviations 15**

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	<ul style="list-style-type: none"> • Physical Probing of the IC: T.P_Probe; • Physical Alteration of the IC: T.P_Alter;
BSI-PP-0002	<ul style="list-style-type: none"> • Physical Manipulation: T.Phys-Manipulation • Forced Information Leakage: T.Leak-Forced
PP/9911	<ul style="list-style-type: none"> • 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

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

JIL

- 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	<ul style="list-style-type: none"> • Physical Probing of the IC: T.P_Probe; • Physical Alteration of the IC: T.P_Alter; • Cloning: T.Clon.
BSI-PP-0002	<ul style="list-style-type: none"> • Physical Probing: T.Phys-Probing • Physical Manipulation: T.Phys-Manipulation • Forced Information Leakage: T.Leak-Forced
PP/9911	<ul style="list-style-type: none"> • 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:

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

JIL

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	<ul style="list-style-type: none"> • 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-0002	<ul style="list-style-type: none"> • Inherent Information Leakage: T.Leak-Inherent • Abuse of Functionality: T.Abuse-Func

	<ul style="list-style-type: none">• Malfunction due to Environmental Stress: T.Malfunction
PP/9911	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none"> • 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-0002	<ul style="list-style-type: none"> • Abuse of Functionality: T.Abuse-Func
PP/9911	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Insertion of faults: T_Flt_ins • Information Leakage: T.I_Leak • Linkage of multiple sources: T.Link
BSI-PP-0002	<ul style="list-style-type: none"> • Inherent Information Leakage: T.Leak-Inherent
PP/9911	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none">• Invalid inputs: T.Inv_Inp• Forced reset: T_Forced_rst• Load bad software: T.Bad_load
BSI-PP-0002	Smartcard embedded software not in the scope of the PP.
PP/9911	<ul style="list-style-type: none">• Unauthorised Modification: T.MOD_DEL, 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 perturbing 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	<ul style="list-style-type: none"> • Environmental Stress: T.Env_Strs
BSI-PP-0002	<ul style="list-style-type: none"> • 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