Examples for the Calculation of Attack Potential for Smartcards

Thomas Schröder, T-Systems GEI GmbH
on behalf of the JHAS working group

T - Systems

Introduction
Basis for the examples

- The work is based on a collection of attack methods

- The examples are based on theoretical designs including public known countermeasures to
  - identify general steps of the attack methods
  - protect the properties of hardware developers

- Examples may be used in evaluations, however the evaluator must take care that attack methods that cannot be completely assessed based on the evaluation of the implementation must be additionally analysed by penetration tests. Furthermore a demonstration of the attack is required to show the applicability of the attack to the TOE.

List of attack methods taken from:
“Attack Methods for Smartcards and Related Products”

- Physical Attacks
- Overcoming sensors and filters
- Perturbation Attacks
- Retrieving keys with DFA
- SPA/DPA – Non-invasive retrieving of secret data
- Higher Order DPA
- EMA Attacks
- Exploitation of Test features
- Attacks on RNG
- Ill-formed Java Card applications
- Software Attacks

Physical Attack Example: Probing Attack

Key Properties of the attack

- Description of Attack
  - Physically access signal lines or memories
- Effect of Attack
  - Read or manipulate data transferred on internal signal lines
- Impact on the TOE
  - Attack against the hardware platform
  - Often independent of the embedded software
  - Access to secret data or forcing internal signals
- Characteristics of the Attack
  - Devices without countermeasure
  - Skill of the attacker depends on the complexity of the design
  - The tools required to uncover and analyse metal lines are considered as specialised equipment

Probing Attack
Example Rating

Factor	Comment	Ident.	Exploit.
Elapsed Time	Ident. less than a month and exploit. less than a week	3	4
Expertise	Expert for Identification	5	2
Knowl. of TOE	Knowledge of commands	2	0
Open Sample	Not required	0	0
Access to TOE	Less than ten samples	0	0
Equipment	Specialised equipment	3	4
Points		13 + 10 = 23	

Probing Attack
Results

- Resistance of the TOE
  - The TOE is resistant to an attacker with low attack potential (VLA.2)
- Required Demonstration of attack to justify the rating
  - provide the signal of one line and demonstrate that the other lines are accessible by probing
- State of the art
  - Active shield and advanced routing techniques are two countermeasures that can increase the attack potential

Perturbation Attack
Key Properties of the attack

- Description of Attack
  - Operate the IC outside the specified operating environment
  - Applying an external source of energy during the operation of the IC
- Effect of Attack
  - Change the intended behaviour of an IC to create an exploitable error in the operation of the TOE
- Impact on the TOE
  - Modifying the program flow, changing the access rights to files
  - Enable differential fault analysis of cryptographic keys
  - Attack against the hardware platform or a composite product
- Characteristics of the Attack
  - Device without specific sensors
  - The attacker requires expert skill
  - Example tools are a microscope and a photo flash light

Perturbation Attack

Example Rating

Factor	Comment	Ident.	Exploit.
Elapsed Time	Ident. less than a month and exploit. less than a week	3	4
Expertise	Expert for Identification	5	2
Knowl. of TOE	Knowledge of commands	2	0
Open Sample	Not required	0	0
Access to TOE	Less than ten samples	0	0
Equipment	Specialised equipment	3	4
Points		13 + 10 = 23	

Perturbation Attack
Results

- Resistance of the TOE
  - The TOE is resistant to an attacker with low attack potential (VLA.2)
- Required Demonstration of attack to justify the rating
  - prove that the error is exploitable e.g. allows access to a file that cannot be accessed without the perturbation
- State of the art
  - Various sensors are countermeasures that can improve the resistance.
  - In most cases a combination of countermeasures implemented in the hardware and the embedded software are required to avert such attacks.

Power Analysis
Key Properties of the attack

- Description of Attack
  - The power consumption of a device can be measured using a digital storage oscilloscope and a resistor
  - The measurement can be applied without damaging the TOE
- Effect of Attack
  - Exploiting information leaked through characteristic variations in the power consumption of electronic components
- Impact on the TOE
  - SPA analysis can be used to detect specific operations of the TOE
  - SPA and DPA can be applied in general to all cryptographic algorithms
- Characteristics of the Attack
  - Preconditions for SPA and DPA analysis are well known
  - The attacker requires detailed knowledge of the cryptographic algorithms
  - The assessment is based on the usage of an open sample

Power Analysis
Example Rating

Factor	Comment	Ident.	Exploit.
Elapsed Time	Data collection and analysis of at least 100.000 traces	3	4
Expertise	Expert for the identification	5	2
Knowl. of TOE	Knowledge of commands	2	0
Open Sample	Appropriate control of open samples	4	0
Access to TOE	Less than ten samples	0	0
Equipment	Specialised equipment	3	4
Points		17 + 10 = 27	

Power Analysis
Results

- Resistance of the TOE
  - The TOE is resistant against an attacker with medium attack potential (VLA.3)
- Required Demonstration of attack to justify the rating
  - if the key is known it is possible to determine the remaining size of the key space that is left for a brute-force search
- Progress
  - Current Balancing, Current Smoothing, Randomised Clock, and Blinding are countermeasures that can improve the resistance

Exploitation of Test features
Results

- Most published attacks to re-use test features are at the limit between no rating and resistant to low attack potential
- Possible attack scenarios depend on the product specific countermeasures implemented to prevent such an attack
- Possible impacts are:
  - access to the content of non-volatile memory
  - re-configuration of life cycle data or error counters

Software Attacks
Attack Techniques

- There are many attacks that are based only on the embedded software
- Most software attacks arise from errors (bugs) either in design or implementation
- The identification is split into the analysis of the implementation and penetration testing
- In most cases these issues cause a TOE to fail the evaluation
- Attack techniques that may exploit vulnerabilities
  - Editing commands
  - Direct protocol attacks
  - Man-in-the-middle attacks
  - Replay attacks

Combined Attack
Key Properties of the attack

- Description of Attack
  - Hardware perturbation attack to accept a illicit command request
- Effect of Attack
  - Enable modified commands within an application context
- Impact on the TOE
  - The effects depend on the application
- Characteristics of the Attack
  - Setup for perturbation attacks
  - The attacker requires basic knowledge of the application
  - The assessment is based on the usage of an open sample

Combined Attack
Assessment

- Elapsed time
  - Time spent for both attack steps during the identification could not simply be added because parts can be done in parallel
- Expertise
  - The attack requires an expert for the identification
- Knowledge of the TOE
  - The knowledge is limited to the commands of the application
- Open samples
  - If the hardware platform and the embedded software include countermeasures against such attacks they are used to reduce the complexity.
- Access to the TOE
  - The number of samples depends on the countermeasures
- Equipment
  - Such an attack requires in most cases specialised equipment for the perturbation step. For the exchange of application commands normally standard equipment is sufficient that does not add points

Summary
Objectives of the examples

- Comparable objectives on penetration testing by different labs
- Common understanding of the rating for composite evaluation
- Comparable ratings by different labs controlled by the certification bodies