On Security Evaluation Testing

Kerstin Lemke-Rust

Hochschule Bonn-Rhein-Sieg

Workshop: Provable Security against Physical Attacks
Lorentz Center, 19 Feb 2010
Motivation

1. How does an evaluator identify all applicable physical attacks for (commercial) cryptographic products?
2. How does an evaluator conduct penetration testing?
3. How does an evaluator assess the security level of (commercial) cryptographic products?
4. How is a certification process organized?

Security Evaluation Schemes

Introduction to Security Evaluation Schemes

The Common Criteria Approach
  1. Penetration Testing for Smartcard ICs

The FIPS-140 Approach
  1. Penetration Testing for Multiple Chip Cryptographic Modules

Conclusion
Certification Process

Manufacturer

Evaluation Reports

Product samples and supporting documents

Application for Certification

Accreditation

Evaluation Reports

Certification Body

Review Reports
Why Certification?

Benefits

1. Benefits for Manufacturer:
   - Evidence of compliance to law requirements
   - Consequent assessment of security functions during development
   - Knowledge and minimization of vulnerabilities and risks
   - Improvement of product quality
   - Marketing

2. Benefits for User:
   - Evidence of correct and effective implementation of security functions.
Comparison of the Common Criteria and the FIPS 140 Approach

<table>
<thead>
<tr>
<th>FIPS 140</th>
<th>Common Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>The standard has 4 pre-defined Security Levels.</td>
<td>The standard provides tool boxes for functional and assurance requirements. Extensions are possible.</td>
</tr>
<tr>
<td>Each security level has pre-defined security functions and test requirements for 11 requirement areas (among them: Physical Security, Self Tests, and Mitigation of Other Attacks).</td>
<td>Manufacturer/Sponsor defines security functions and aimed Evaluation Assurance Level (EAL) of the product (also known as Target of Evaluation (TOE)).</td>
</tr>
<tr>
<td></td>
<td>Product-specific requirements are set down in a Security Target (ST).</td>
</tr>
<tr>
<td></td>
<td>Product-class specific requirements are set down in a Protection Profile (PP).</td>
</tr>
</tbody>
</table>
History of Security Evaluation Standards

- Trusted Computer System Evaluation Criteria (TCSEC) or “Orange Book” (USA, 1983)
- Common Criteria (Standard since 1996, Current Version: 3.1)
  - Mutual International Recognition Agreement (CCRA) for Evaluation Assurance Levels (EALs) 1 through 4.
Contents and Principles

Contents

- Part 1: General Information.
- Part 2: Catalogue of Functional Requirements. What are the Security Functions?
- Part 3: Catalogue of Assurance Requirements. How deeply and rigorous are Security Functions evaluated?
- Common Criteria Evaluation Methodology (CEM). How shall the evaluator conduct each evaluation task?

Principles

Impartiality, Objectivity, Repeatability, Reproducibility.
## Common Criteria Evaluation Assurance Level (EAL)

<table>
<thead>
<tr>
<th>Assurance class</th>
<th>Assurance Family</th>
<th>Assurance Components by Evaluation Assurance Level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>EAL1</td>
</tr>
<tr>
<td>Development</td>
<td>ADV ARC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ADV_FSP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ADV_TMP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ADV_INT</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ADV_SPM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ADV_TDS</td>
<td></td>
</tr>
<tr>
<td>Guidance</td>
<td>AGD_OPE</td>
<td>1</td>
</tr>
<tr>
<td>documents</td>
<td>AGD_PRE</td>
<td>1</td>
</tr>
<tr>
<td>Life-cycle</td>
<td>ALC_CMC</td>
<td>1</td>
</tr>
<tr>
<td>support</td>
<td>ALC/cms</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>ALC_DEL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ALC_DVS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ALC_FLR</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ALC_LCD</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ALC_TAT</td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td>ASE_CCL</td>
<td></td>
</tr>
<tr>
<td>Target evaluation</td>
<td>ASE_ECD</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ASE_INT</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ASE_OBJ</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ASE_REQ</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ASE_SPD</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ASE_TSS</td>
<td></td>
</tr>
<tr>
<td>Tests</td>
<td>ATE_COV</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ATE_DPT</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ATE_FUN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ATE_IND</td>
<td></td>
</tr>
<tr>
<td>Vulnerability</td>
<td>AVA_VAN</td>
<td>1</td>
</tr>
<tr>
<td>assessment</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Evaluation Assurance Level:**
- EAL1: functionally tested
- EAL2: structurally tested
- EAL3: methodically tested and checked
- EAL4: methodically designed, tested and verified
- EAL5: semiformal-designed and tested
- EAL6: semiformal verified designed and tested
- EAL7: formally verified and tested

**Vulnerability Assessment:**
AVA_VAN gives the resistance against attack potential:
1, 2: „basic“
3: „enhanced basic“
4: „moderate“
5: „high“
For each in the operational environment exploitable vulnerability the required attack potential is calculated according to the following factors:

- **Elapsed Time** (0-19 points),
- **Specialist Expertise** (0-8 points),
- **Knowledge of the TOE** (0-11 points),
- **Window of opportunity** (0-10 points),
- **IT hardware/software or other equipment** (0-9 points)

**Final Assessment**

TOE is resistant to

- “basic” attack potential if all attacks require at least 10 points,
- ...
- “high” attack potential if all attacks require at least 25 points.
Estimation of the Attack Potential (for Smartcard Evaluation)

For smartcard evaluation, a specific JIL document “Application of Attack Potential to Smartcards, Version 2.7” applies (see talk of Christophe Giraud).

Main differences are

- Separation in identification and exploitation phase.
- **Window of opportunity** counts number of samples needed.
- Additional category **Open samples**.
- Points per category and phase are different.
- Points needed for certain AVA_VAN level are different to CEM, e.g., TOE is resistant to
  - “high” attack potential if all attacks require at least 31 points.
Penetration Testing Approach

Penetration testing approach considers

- the claimed security functions in the PP/ST,
- the identified threats in the PP/ST, and
- the aimed vulnerability assessment level in the PP/ST.

Notes:

- Only attacks are considered with can be applied in the defined operational environment of the product.
- If the PP/ST does not include requirements for physical security functions physical attacks are not conducted.
- The PP/ST author has the option to restrict to specific physical threats.
- Further restrictions might be made in guidance documents!
Example: Eurosmart Security IC Platform Protection Profile

Security IC Platform Protection Profile Version 1.0, 15.06.2007:

- Authors: Atmel, Infineon Technologies AG, NXP Semiconductors, Renesas Technology Europe Ltd, STMicroelectronics.
- Physical threats are addressed for the end-consumer phase.
- Minimum assurance level is EAL4 augmented with AVA_VAN.5 and ALC_DVS.2.

Note: this Protection Profile covers only the Security IC, composite evaluations are based upon the evaluation of the Security IC and the evaluation of the embedded Software.
Considered Threats

Physical Interface (contact and/or contactless)

1. Electrical stimulation
2. Energy and Particle Exposure (e.g. light)
3. Inspection and Reverse-engineering
4. Physical manipulation
5. Electro-magnetic interaction/radiation and analysis
6. Electrical measurement and analysis
7. Communication
8. Electrical measurement and analysis
9. Glitches, etc.
Considered Threats

**Threat Statement**

- **Inherent Information Leakage** *(e.g., TA, SPA/SEMA, DPA/DEMA,...)*
- **Physical Probing** *(IC failure analysis and IC reverse engineering)*
- **Malfunction due to Environmental Stress** *(e.g., with temperature, glitches, spikes, light,...)*
- **Physical Manipulation** *(IC failure analysis and IC reverse engineering with changes of circuitry)*
- **Forced Information Leakage** *(e.g., FA, DFA, with glitches, spikes, light, ...)*
- **Abuse of Functionality** *(e.g., re-activating functionality of test pads)*
- **Deficiency of Random Numbers** *(e.g., by destruction, manipulation, environmental stress.)*

Main Physical Security Objective is **Tamper Resistance**.
Penetration Testing Approach

Dependencies for Vulnerability Testing according AVA_VAN.5

- Public domain sources (e.g. papers on practical physical attacks)
- Supporting Documents for the TOE:
  - Security architecture description
  - Complete functional specification
  - Basic modular design
  - Implementation representation of the TOE Security Functions
  - Operational user guidance
  - Preparative procedures
  - Testing: basic design

The penetration testing is based on sensitive and even critical information about the TOE (White-box Testing)!
Penetration Testing Approach

Tradeoff between “Elapsed Time” and “Knowledge”

Compensation of time-consuming analysis by

- Sensitive and even critical knowledge of the TOE.

Tradeoff between “Elapsed Time” and “Open Samples”

Compensation of time-consuming analysis by

- Use of special TOE samples (e.g., with built-in trigger signals, deactivated countermasures).

Support by the Manufacturer

Further simplifications for testing are usual (but not well supported in the Common Criteria scheme any longer):

- Joint penetration testing with manufacturer.
- Joint analysis of penetration testing results with manufacturer.
Example: Leakage of Masked Crypto Implementations

Input to Penetration Testing:

- Details of masking scheme are known.
- Details of further side channel countermeasures are known.

<table>
<thead>
<tr>
<th>Problem (standard TOE sample)</th>
<th>Simplification (special TOE sample)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resynchronization of测量ment traces might be difficult.</td>
<td>Built-in trigger signals at the crypto operation. Resynchronization is no longer required.</td>
</tr>
<tr>
<td>Detection of leakage of masks and masked values is usually limited to second-order DPA. Profiling need to be done in unsupervised mode with limited efficiency.</td>
<td>Output of masks. This enables advanced multivariate side channel analysis in supervised mode: templates and stochastic methods using masks.</td>
</tr>
<tr>
<td>Additional countermeasures might make the analysis difficult.</td>
<td>Deactivation of additional countermeasures. The number of traces needed for analysis is reduced.</td>
</tr>
</tbody>
</table>
Example: Leakage of Masked Crypto Implementations

**Assessment**

**Case 1:** No leakage detected with special TOE samples. **Assessment:** attack is not practical in the operational environment.

**Case 2:** (Partial/Complete) Leakage detected with special TOE samples. Further penetration tests need to be carried out to verify if the attack is practical in the operational environment with standard TOE samples:

- How big is the resynchronization effort needed?
- How big is the effort to deal with additional countermeasures?

**Assessment:** according to the attack potential calculation for the different adversaries considered. The setting with the minimum number of points determines the attack potential.
Example: Physical Probing

**Input to Penetration Testing:**
- Access to details of chip layout (typically at the manufacturer’s site).
- Details of probing countermeasures (e.g., active shield, bus and memory encryption) are known.

**Tools for Penetration Testing:**
- Focused Ion Beam (Microprobing is prevented because of active shield and shrinked technology.)

**Questions for Penetration Testing:**
- Can (single-point of) contacts be identified in the layout which leak sensitive information?
- Are these (single-point of) contacts in top metal layers?
- Can a (single-point) probing attack be successfully put in practice?

**Assessment:** according to the test results and the attack potential calculation.
Rough Classification of Considered Threats

<table>
<thead>
<tr>
<th>Threat Classes</th>
<th>Expertise, Knowledge of the TOE, Equipment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inherent Information Leakage</td>
<td>Proficient to Expert (2/5 + 2/4), Several Types of Knowledge (0/9 + 0/5),</td>
</tr>
<tr>
<td>Malfunction due to Environmental Stress</td>
<td>Standard to Specialised Equipment (1/3 + 2/4).</td>
</tr>
<tr>
<td>Forced Information Leakage</td>
<td></td>
</tr>
<tr>
<td>Abuse of Functionality</td>
<td></td>
</tr>
<tr>
<td>Deficiency of Random Number Testing</td>
<td></td>
</tr>
<tr>
<td>Physical Probing</td>
<td>Expert (5+4), very critical hardware design knowledge in Identification (9), critical</td>
</tr>
<tr>
<td>Physical Manipulation</td>
<td>knowledge in Exploitation (5), Bespoke Equipment (5+6).</td>
</tr>
</tbody>
</table>

- “Elapsed Time”, “Access to TOE”, and “Open Samples” are add-on.
- Physical Probing and Physical Manipulation usually require “beyond high” attack potential, unless the required knowledge can be gained in another way and elapsed time is sufficiently short!
- Certification Body makes the final decision if interpretation is needed.
Some Thoughts on Penetration Testing Approach

On estimating attack potential

From above the attack path may look simpler as it really is...
Some Thoughts on Penetration Testing Approach

**On Absolute Guarantees**

- Of course, penetration testing cannot give an absolute guarantee that indeed all vulnerabilities are detected and assessed by an evaluator.
- However, the experience gained in smartcard testing over the last 15 years should give a certain guarantee that the required penetration tests are appropriately conducted.

**On “Beyond High” Attack Potential**

- Industry might not be interested to invest in additional efforts to resist “Beyond High” attack potential.
- Users might be interested in lifting the attack potential thresholds.
History of FIPS 140

- FIPS 140-1 (1994, developed by a government and industry working group)
- FIPS 140-2 (2001, supersedes FIPS 140-1)
- Draft FIPS 140-3 (Revised Draft 09/11/09, will supersede FIPS 140-2)

Further documents

- Derived Test Requirements for FIPS PUB 140-2
- Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program
## Physical security requirements (Draft FIPS 140-3)

<table>
<thead>
<tr>
<th>Security Level</th>
<th>General Requirements for all Embodiments</th>
<th>Single-Chip Cryptographic Modules</th>
<th>Multiple-Chip Embedded Cryptographic Modules</th>
<th>Multiple-Chip Standalone Cryptographic Modules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>Production-grade components.</td>
<td>No additional requirements.</td>
<td>If applicable, production-grade enclosure or removable cover.</td>
<td>Production-grade enclosure.</td>
</tr>
<tr>
<td>Level 2</td>
<td>Evidence of tampering. Opaque covering.</td>
<td>Opaque tamper-evident coating on chip or enclosure.</td>
<td>Opaque tamper-evident encapsulating material or opaque enclosure with tamper-evident seals or pick-resistant locks for doors or removable covers.</td>
<td>Opaque enclosure with tamper-evident seals or pick-resistant locks for doors or removable covers.</td>
</tr>
<tr>
<td>Level 3</td>
<td>Tamper response and zeroization circuitry. Protection from probing.</td>
<td>Hard opaque tamper-evident coating on chip or strong opaque removal-resistant and penetration resistant enclosure.</td>
<td>Hard opaque potting material encapsulation of multiple chip circuitry embodiment or applicable Multiple-chip standalone security Level 3 requirements.</td>
<td>Hard opaque potting material encapsulation of multiple chip circuitry embodiment or strong opaque enclosure with removal/penetration attempts causing serious damage.</td>
</tr>
<tr>
<td>Level 4</td>
<td>Either EFP or EFT for temperature and voltage.</td>
<td>Hard opaque removal-resistant coating on chip.</td>
<td>Tamper detection envelope with tamper response and zeroization capability.</td>
<td>Tamper detection envelope with tamper response and zeroization capability.</td>
</tr>
</tbody>
</table>
Physical security - Non-Invasive Attacks (Draft FIPS 140-3)

- New Chapter “Non-Invasive Attacks” in Draft FIPS 140-3, refers to Annex F for non-invasive attacks and their associated security functions addressed by this standard.
- Annex F: The addressed non-invasive attack methods are: SPA/SEMA, DPA/DEMA, TA and some extensions such as template attack, CPA, higher-order DPA.
- Requirements shall be applicable to single-chip cryptographic modules and single-chip components of hybrid modules.
- Requirements are optional for all other hardware module embodiments.
<table>
<thead>
<tr>
<th>Security Level 1-2</th>
<th>no requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Level 3</td>
<td>At Security Level 3, the cryptographic module shall protect the module’s CSPs against all of the applicable non-invasive attacks Annex F specifies and associates with Approved or Allowed security functions. Documentation shall specify the mitigation techniques employed against these attacks and how these techniques mitigate access to the module’s CSPs. The effectiveness of the mitigation techniques shall be specified.</td>
</tr>
<tr>
<td>Security Level 4</td>
<td><strong>In addition to the requirements for Security Level 3, the module shall undergo testing</strong>, and shall meet the requirements defined by the validation authority, for each of the applicable non-invasive attacks and the Approved or Allowed security functions which are relevant to those attacks, as specified in Annex F.</td>
</tr>
</tbody>
</table>
Penetration testing approach considers

- the aimed Security Level,
- the hardware embodiment, and
- the documentation for the cryptographic module.

Notes:

- The vendor can explicitly exclude components from security requirements provided that a rationale is given and the component, even if malfunctioning or misused, cannot cause a compromise under any reasonable condition.
- Verdict of test procedure is pass or fail.
- Some sophisticated test procedures can be either done at the tester’s facility, the vendor facility, or the tester supervises vendor performing tests at vendor facility.
Security Construction: Multiple Chip Cryptographic Module (Security Level 4)
Security Construction: Multiple Chip Cryptographic Module (Security Level 4)

Main Requirements: Tamper response and zeroization circuitry

- Tamper response and zeroization circuitry continuously monitors the tamper detection envelope.
- Tamper detection detects means such as cutting, drilling, milling, grinding, or dissolving of the potting material or disclosure.
- Tamper detection leads immediately to the zeroization of plaintext secret and private cryptographic keys.

Main Physical Security Objective is Tamper Response.
Penetration Testing Approach: Tamper response and zeroization circuitry

Test Procedures
- The tester shall breach the tamper detection envelope barrier and then verify that the module zeroize all plaintext secret and private keys.

Some Detailed Test Questions
- Can the tamper detection envelope be penetrated without any tamper detection?
- How fast does the zeroization start and how long does it take?
- Can the zeroization process be deactivated or stopped?
- Are there “burned-in” effects in the battery backed RAM?
- Are there remanence effects at minimum operating temperature?
- Does the circuitry detect when the internal battery becomes undercharged?
Test requirements are under continuous development, many research results of the previous years are taken into account for penetration testing.

Penetration testing approaches and outcomes depend on the competence and experience of personnel in evaluation labs.

(National and international) Harmonisation of penetration testing approaches depends on the Certification Bodies.