Joint Interpretation Library

Application of Attack Potential to Hardware Devices with Security Boxes

Version 3.1
November 2023

This page is intentionally left blank.

Table of contents

1 Introduction

1 This document interprets the current version Common Criteria Methodology (CEM), based on evaluation experience in the technical domain “Hardware Devices with Security Boxes” and input from the related industry through the JIL Embedded Devices Subgroup (JEDS) of the SOG-IS. It provides guidance metrics to calculate the attack potential required by an attacker to effect an attack on ICT products of the technical domain “Hardware Devices with Security Boxes”. The underlying objective is to aid in expressing the total effort required to mount a successful attack. This should be applied to the operational behaviour of such ICT product as defined in a related Security Target of the product under evaluation.

1.1 Scope

2 For most of the attacks presented in [AM-SBOX], the attack potential rating is analysed according to the tables included in section 2 Parameters conditioning attacks. These tables are based on the information included in [AP-POI]. Advices for the rating of software attacks and attacks on RNG will be added with later revisions.

NOTE: Further analysis is to be detailed providing ratings for specific real cases and taking into account possible countermeasures implemented to mitigate the attacks.

2 Parameters conditioning attacks

2.1 Scale factor

3 The size is one of the factors conditioning the attacks being performed against devices with security boxes. Depending on the scale of the device, the attack could be different, and the difficulty may increase or decrease depending on such scale.

4 A size categorization can be made in the following manner.

2.1.1 Macroscopic scale

5 This scale surrounds the attacks performed against entire devices with its complete external enclosure. The enclosure may have several components inside such as PCB boards, batteries, etc. so that the aim of an attack is gain access to the internal parts of the enclosure.

2.1.2 Micro- technology

6 In this case, the scale surrounds the attacks performed against assembled electronic components, such as PCB boards containing buses and ICs. The attacks can be made against the buses transmitting data between components, or perhaps against the IC connectors.

2.1.3 Nano-technology

7 This scale contemplates the internals of the ICs. Very precise and specialized tools are needed to perform attacks against the ICs internals. These attacks could have the aim of modifying the IC behaviour, or obtain data stored within the IC.

2.2 Factors for the attack potential calculation

8 Note about CC v3.1 and CC:2022:

9 Starting with Common Criteria version 3.1, there is no more distinction between the identification phase and the exploitation phase. But considering Security Boxes, the risk management performed by the user of CC certificates required clearly to distinct between the cost of “identification” (definition of the attack) and the cost of “exploitation” (e.g. once a script is published). Therefore, this distinction is kept in mind when calculating attack potential for Security Boxes evaluation. Although the distinction between identification and exploitation is essential for the evaluation of a Security Box to understand and document an attack path, the final sum of attack potential will be calculated by adding the points of the two phases, as both phases build the complete attack.

2.2.1 How to compute an attack

10 Attack path identification and exploitation analysis and tests are mapped to relevant factors: attack time, expertise, knowledge of the Security Box, access to the TOE per unit required for the attack, equipment required, or the required window of opportunity to execute an attack.

11 Even if the attack consists of several steps, the identification and exploitation rating needs only to be computed for the entire attack path. It is not allowed to calculate the rating for each step separately and to sum up the points afterwards since in that case different factors would count multiple (e.g. tools and expertise). An entire attack path or full attack starts with the preparation activities for an attack and ends when the attacker could gain access to a TOE asset. A full attack does not end with a violation of a SFR if access to a TOE asset could not be gained.

12 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. It may not be necessary to carry out all of the experiments to identify the full attack, but to provide that it is clear whether the attack actually proves that access could been gained to a TOE asset and that the complete attack could realistically be carried out. One of the outputs from the Identification phase assumes a script giving a step-by-step description of how to carry out the attack – this script is assumed to be used in the exploitation part.

13 Sometimes the identification phase will involve the development of a new type of attack (possibly involving the creation of new equipment) which subsequently could be applied to other TOEs. In such a case, the question arises how to handle 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 rating points for the development of the attack (in terms of time or expertise) can be used in the attack potential calculation.

14 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 assumes to identify the necessary equipment. This means that the elapsed time, expertise and TOE knowledge ratings for exploitation will sometimes be lower for exploitation than for identification.

15 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 need to be documented in the ETR.

16 To complete an attack potential calculation, the rating 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 an agreement cannot be reached.

2.2.2 Elapsed time

17 The Elapsed Time is calculated in hours taken by an attacker to identify or exploit an attack. 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 labour 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 cases, where attendance is not required during part of the Elapsed Time, the Elapsed Time has to be taken as expired time divided by 3. The idea behind the division by three is that e.g. a computer is able to work 24 hours per day, not only 8 hours per day.

2.2.3 Expertise

20 Expertise refers to the level of generic knowledge and skills in the application area or product type (e.g. microelectronics, chemistry, skills handling specific drills). For the purpose of Security Boxes three types of experts are defined:

- Laymen are unknowledgeable compared to experts or proficient persons, with no particular expertise or skills in the area.
- Proficient persons are knowledgeable in that they are familiar with the security behaviour of the product, or they have certain (amateur level) expertise handling specific machines or attack techniques to security boxes.
- Experts have a professional experience with specific machines (handling and configuring), security box hardware structures, materials, 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, etc.

	Definition according to CEM	Detailed definition to be used in Security Boxes evaluations
Experts	Familiar with implemented • Algorithms • Protocols • Hardware structures • Principles and concepts of security	Professional experience with • Security boxes hardware structures • Configuration and handling of specific equipment (milling/drills, x-rays, etc.) • Electronic and microelectronic knowledge (sensors, actuators, etc.) and • Techniques and tools for the definition of new attacks
Proficient	Familiar with • security behaviour	Familiar with • Security behaviour and classical attacks to security boxes
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 • Milling machines • Drilling machines • CNC milling machines • X-ray machines • Lasers • Optical Microscope • Chemistry (etching, grinding) • [..]	**Knowledge:** The level of expertise depends on skills and knowledge of • Common Security boxes information • TOE specific hardware structures • Principles and concepts of security • Destructive/ Non-destructive Techniques. • Microelectronics (sensor types and technologies) • [..]

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 and machines manipulation and microelectronics or chemistry.

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

Table 4: Rating for Expertise

2.2.4 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.

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 the Knowledge of the 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).

2.2.5 Access to TOE: Samples

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 - if necessary - the attacker may analyse and/or modify the TOE. Differences are defined in the status and functionality of the device to be analysed/modified/tested. This shall replace the CEM factor "Access to TOE".

- **Non-functional samples** are samples without a final firmware[1] and can be used to study the mechanical design or for supplying spare parts. Basic functionality like active tamper event monitoring may be given.

- **Functional samples** can be used for the assessment of the logical and electrical behaviour of the device including its final firmware, but are not functional within the intended operating environment (e.g. it is no payment transaction possible within a "real world" payment network without real valid cryptographic keys). These functional samples may be optionally loaded with test keys or equivalent.

[1] "Final firmware" means: Released by the manufacturer and approved, if necessary (e.g. by national certification bodies). Typically the evaluator does not examine a final firmware during the evaluation (e.g. it is not approved at the time of evaluation). For the rating it is assumed that a functional sample under "real world" conditions will include a firmware which is a "final firmware" as described before. "Final" does not imply that it is the latest version of the firmware but any version which is released by the manufacturer and approved, if necessary. It may exist different released versions e.g. for different customer groups.

- **Fully operational samples** are fully functional devices, which could be directly used in the intended operating environment. These samples might be used to verify / test an attack method or to actually perform an attack under "real world" conditions.

Access to TOE (Samples)	Identification	Exploitation
Non-functional Sample	1	1
Functional Samples	2	2
Fully Operational Samples	4	4

Table 6: Rating for Access to TOE

31 If more than one sample is required in any category, instead of multiplying the points by the number of samples, the following factors must be used.

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

Table 7: Factor to rate the samples

32 The total number of points is calculated as sum of the points for the samples in the different categories. In exceptional cases the usage of higher-rated samples can lower the total number of points. In such cases the lower rating has to be used.

33 Two examples demonstrate the calculation:

a) Two non-functional and two functional samples are required.
Calculation: 1 x 1.5 + 2 x 1.5 = 4.5 Points

b) One non-functional and three functional samples are required.
Calculation: 1 x 1 + 2 x 2 = 5 Points

But: In both cases the non-functional samples could be substituted by functional samples, meaning that four functional samples could be used instead.
Calculation: 2 x 2 = 4 Points

According the above-mentioned rule the rating for both examples is 4 points, not 4.5 resp. 5 points.

34 The number of samples has to be justified. Especially, a strong justification has to be provided if a higher number of samples is required as typically for this product type. E.g. for payment terminals it is expected that most attacks can be performed with one or two samples in the identification phase and a single sample in the exploitation

phase.

35 It has to be checked if it is possible to reduce the amount of samples and/or the time for identification or exploitation ("Elapsed Time") by "Knowledge of the TOE" with the goal to reduce the total number of points.

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

2.2.6 Equipment and tools

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

38 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 purchased from the Internet. The equipment might consist of simple attack scripts, personal computers, power supplies, or simple mechanical tools like standard drills, common use chemical products, soldering irons, etc.

- **Specialized equipment** is not readily available to the attacker due to its price or size, but could be acquired without undue effort. This could include purchase of moderate amounts of equipment (e.g., specialized test bench, chemical workbench, precise milling/drills, etc.) or development of more extensive attack scripts and proofs.

- **Bespoke equipment** is not readily available to the public as it might need to be specially produced (e.g., very sophisticated tools) or because the equipment is so specialized that its distribution is controlled, possibly even restricted. Alternatively, the equipment may be very expensive (e.g., Abrasive Laser Equipment). Bespoke equipment, which can be rented, might have to be treated as specialized equipment.

39 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**.

40 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

41 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.

42 The border between standard, specialized and bespoke cannot 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
Soldering Iron	Standard
Heat guns	Standard
Glue	Standard
Needle	Standard
Syringe	Standard
Knife	Standard
Steel cutting blades	Standard
Screwdriver	Standard
Hammer	Standard
Standard drill	Standard
Drill press	Standard
Circular saw	Standard
Radial arm saw	Standard
Voltage supply	Standard
Multimeter	Standard
Analogical Oscilloscope	Standard
PC or workstation	Standard
Signal analysis software	Standard
Dental toolkit (mirrors)	Standard
Borescope	Standard
Fiberscope	Standard
Solder paste	Standard
Shunts	Standard
Wires and electrical probes	Standard
Torch	Standard
Micro-cameras	Standard
Microphones	Standard
Chemical products	Standard
Antennas	Standard
Milling Machine	Specialized
Sandblasting Machine	Specialized
CNC Milling Machine	Specialized
Laser Milling Machine	Specialized
Laser Equipment	Specialized
Electrostatic emitting devices	Specialized
Electromagnetic emitting devices	Specialized
Conductive ink printer	Specialized
Signal and function processor	Specialized
Digital Oscilloscope	Specialized

Signal/Protocol Analyser	Specialized
Tools for chemical etching (wet)	Specialized
Tools for chemical etching (plasma)	Specialized
Tools for grinding	Specialized
Climate chamber	Specialized
Anechoic chamber	Specialized
Standard X-ray machine	Specialized
Radio-frequency generator	Specialized
Gamma-ray generator	Specialized
Standard tomography scanner	Specialized
Standard thermal camera	Specialized
FIB systems	Specialized

Table 8: Rating for Tools

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

44 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
X-ray 3-D tomograph	Bespoke
New Tech Design Verification and Failure Analysis Tools	Bespoke

Table 9: Rating for Tools (II)

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

46 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*	3	4
Bespoke	5	6
Multiple Bespoke	7	8

* If clearly different test benches consisting of specialised equipment are required for distinct steps of an attack this shall be rated as bespoke

Table 10: Rating for Equipment

47 Equipment can always be rented but the same quotation applies with one exception:

Bespoke equipment, which can be rented, might have to be treated as specialized equipment.

2.2.7 Window of Opportunity

48 Opportunity is also an important consideration, and has a relationship to the Elapsed Time factor. This factor applies when the identification or exploitation of some vulnerability may require considerable amounts of access to a TOE that may increase the likelihood of detection. Some attack methods may require considerable effort off-line, and only brief access to the TOE to exploit. Access may also need to be continuous, or over a number of sessions.

49 For the purposes of this document:

- **Unlimited:** access means that the attack does not need any kind of opportunity to be realised because there is no risk of being detected during access to the TOE.
- **Easy:** means that access is required for less than an hour.
- **Moderate:** means that access is required for less than a day.
- **Difficult:** means that access is required for at least a week or more.
- **None:** means that the opportunity window is not sufficient to perform the attack (the length for which the asset to be exploited is available or is sensitive is less than the opportunity length needed to perform the attack - for example, if the asset key is changed each week and the attack needs two weeks).

Consideration of this factor may result in determining that it is not possible to complete the exploit, due to requirements for time availability that are greater than the opportunity time.

Window of Opportunity	Identification	Exploitation
Unlimited	0	0
Easy	1	1
Moderate	2	3
Difficult	4	5
None	-*	-*

* Indicates that the attack path is not exploitable due to other measures in the intended operational environment of the TOE.

Table 11: Rating for the Windows of Opportunity

2.2.8 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		
Public	0	0
Restricted	2	2
Sensitive	3	4
Access to TOE (Samples)		
Non-functional Samples*	1	1
Functional Samples*	2	2
Fully Operational Samples*	4	4
Equipment		
None	0	0
Standard	1	2
Specialized**	3	4
Bespoke	5	6

Factors	Identification	Exploitation
Multiple Bespoke	7	8
Window of Opportunity		
Unlimited	0	0
Easy	1	1
Moderate	2	3
Difficult	4	5
None	-***	-***

* Table 7 contains an factor to rate the number of devices.

** If clearly different test benches consisting of specialized equipment are required for distinct steps of an attack this shall be rated as bespoke

*** Indicates that the attack path is not exploitable due to other measures in the intended operational environment of the TOE.

Table 12 Final table for the rating factors

2.2.9 Range for CC v3.1 and CC:2022

50 The following table replaces table 4 of section B.4 of CEM v3.1 R5 resp. table B.3 of CEM:2022 for the domain “Hardware Devices with Security Boxes”.

Range of Values*	TOE resistant to attackers with attack potential of
0 – 13.5	No rating
14 – 15.5	Basic
16 – 24.5	Enhanced – Basic
25 – 34.5	Moderate
35 and above	High

* Final attack potential = identification + exploitation

Table 13 Rating of vulnerabilities for CC v3 .1 R5 and CC:2022

3 Application of attack potential

51 The attack potential rating is performed following the strategy presented in **section 2: Parameters conditioning attacks.** The calculation of the attack potential will be performed by adding the ratings of two phases: identification and exploitation.

52 For every attack described in the following sections, special annotation, called **Rating hint**, has been added. This note consists in several hints, which may help the evaluator to determine the proper attack potential rating to be calculated, taking into account the different scenarios that the attacker will face.

3.1 Physical security invasive attacks

3.1.1 Attacks to external Enclosures

3.1.1.1 Manual Material Removal Attacks

53 The following attacks bypass any external enclosure in order to disclose critical design information or secret data (data travelling through any bus):

- De-attach tamper evident stickers: open a security box, sealed with tamper evidence stickers, leaving no tamper evidence e.g. applying hot air on a sticker until it gets sticky, and then just carefully remove it.
- Bypass tamper screws: the special-head screws can be sometimes remove by mechanical procedures e.g. drilling the head of the screw and then remove the screw with pliers.
- Remove (glued) covers: heat can make the glue become malleable e.g. heating the glue with a hairdryer will make it sticky and easy to remove.
- Brain surgery: the attacker attempts to remove material, in a lot amount of time and very carefully, from a potted or sealed container while stopping short of tripping a sensor e.g. using a knife or any other accurate cutting tool.

54 Rating hint: take into account that depending on the type of seals used to leave tamper evidence, the attacker can remove the stickers from easy by using only a hairdryer to difficult process trying to leave no evidence when a really specialized tamper evident sticker is used. In addition, the brain surgery attack must not be underestimated, if the attacker has good hand-eye coordination and is plenty of time, extremely delicate work can be accomplished.

55 The main impacts are:

- Disclosure of the PCB internals.
- Disclosure of any plaintext data sent through the tracks of the PCB.

3.1.1.2 Mechanical Machining Attacks

56 The following attacks bypass any external enclosure in order to disclose critical design information or secret data (data travelling through any bus):

- Automatic material removing: remove potting material in an automatic way e.g. milling out the epoxy resin to discover any underneath device.

57 Rating hint: The mechanical machining process, from dummy tools to computer numerical control (CNC) machines, extremely depends on the scale factor of the security box. A research may allow the evaluator to assess the required precision for the attack so that he can determine which kind of machine is needed and how much time it takes.

58 The main impacts are:

- Disclosure of the PCB internals.
- Disclosure of any plaintext data sent through the tracks of the PCB.

3.1.1.3 Water Machining Attacks

59 The following attacks bypass any external enclosure in order to disclose critical design information or secret data (data travelling through any bus):

- Water machining: remove potting material using a water jet cutter e.g. removing the epoxy material layer by layer.

60 Rating hint: The water jet cutter process extremely depends on the scale factor of the security box. A research may allow the evaluator to assess the required precision for the attack so that he can determine which kind of machine is needed and how much time it takes.

61 The main impacts are:

- Disclosure of the PCB internals.
- Disclosure of any plaintext data sent through the tracks of the PCB.

3.1.1.4 Laser Machining Attacks

62 The following attacks bypass any external enclosure in order to disclose critical design information or secret data (data travelling through any bus):

- Laser machining: remove potting material using a Laser cutter e.g. removing the epoxy material layer by layer.

63 Rating hint: The Laser cutting process extremely depends on the scale factor of the security box. A research may allow the evaluator to assess the required precision for

the attack so that he can determine which kind of machine is needed and how much time it takes.

64 The main impacts are:

- Disclosure of the PCB internals.
- Disclosure of any plaintext data sent through the tracks of the PCB.

3.1.1.5 Sandblasting Attacks

65 The following attacks bypass any external enclosure in order to disclose critical design information or secret data (data travelling through any bus):

- Sandblasting machining: remove potting material using sandblasting machining e.g. removing the epoxy material layer by layer.

66 Rating hint: The sandblasting machining process extremely depends on the scale factor of the security box. A research may allow the evaluator to assess the required precision for the attack so that he can determine which kind of machine is needed and how much time it takes.

67 The main impacts are:

- Disclosure of the PCB internals.
- Disclosure of any plaintext data sent through the tracks of the PCB.

3.1.2 Switches deactivation attacks

3.1.3 Sensors removal and deactivation

68 The following attacks bypass any sensor in order to disclose critical design information or secret data (data travelling through any bus):

- Bypass the sensor: those sensors based in all-or-nothing detection, can by bypassed depending on its constructive nature e.g. soldering the pads, between them, of a micro switch detector.
- Remove the sensor: the sensor can be mechanically removed from its position e.g. carefully hammering the sensor with a pry tool.
- Deactivate the sensor: the sensor can be disconnected from its measuring source e.g. covering an ambient light sensor with black epoxy.

69 Rating hint: The evaluator may take into account the specific topology of the sensors. The scale factor must be considered as a critical factor in the calculation of the attack potential. When the attacker is facing any macroscale sensor, the attack methodology is going to be less time consuming then other types. Since the integration of IC is becoming extremely common, the attacker will face in many cases sensor sizes

around the nanometers.

70 The main impacts are:

- Disclosure of the PCB internals.
- Disclosure of any plaintext data sent through the tracks of the PCB.

3.1.4 Attack to a tamper respondent sensor networks

71 The following attacks bypass any sensor network in order to disclose critical design information or secret data (data travelling through any bus):

- Sniff the network: The sensor network can be monitored using an external device such as bus readers/analysers e.g. if the sensor is externally accessible, it can be monitored using any bus reader.
- Modify the sensor behaviour: The sensor can be modified by adding a fixed value to its data register e.g. the data register can be accessed using any JTAG which may allow the attacker to fix the measured value.

72 Rating hint: The evaluator has to take into account that some of the implementation can be easier to sniff than others. If the bus (I2C, SPI, RS232, etc.) is encrypted, the effort will be extremely higher compare to those buses in plaintext.

73 The main impacts are:

- Disclosure of the PCB internals.
- Disclosure of any plaintext data sent through the tracks of the PCB.

3.1.5 Removing and penetration potting materials

74 The following attacks bypass any enclosure based in epoxy materials in order to disclose critical design information or secret data (data travelling through any bus):

- Solve the epoxy material: the epoxy resin can be removed by using chemical products e.g. injecting the proper chemical solvent over the epoxy material.
- Remove the epoxy material mechanically: the epoxy resin can be removed mechanically, removing layer by layer e.g. carefully hammering the epoxy with a pry tool.

75 Rating hint: The more time spent studying the epoxy formulae the more efficient solvent will be found for the chemical removing process. In addition, sometimes a tamper mesh, usually a very long loop of wire, is embedded in the epoxy. If the wire material is similar to the epoxy chemical formulae, the solvent applied will destroy the tamper detection wire at the same time, causing a high risk of tamper detection or destruction of the internals.

76 The main impacts are:

- Disclosure of the PCB internals.
- Disclosure of any plaintext data sent through the tracks of the PCB.

3.1.6 Penetration of tamper respondent meshes

77 The following attacks bypass any tamper response mesh in order to disclose critical design information or secret data (data travelling through any bus):

- Open a hole by adding and cutting pieces of the conductive tracks: bypassing some of the conductive tracks of the mesh may allow drilling a hole directly on the mesh e.g. by inserting a needle in between two tracks.
- Short-circuit the connector of the mesh: If the tracks to the connector between the mesh and the PCB are reachable, the conductive tracks can be short-circuited adding any conductive material e.g. soldering the connector pads between each other.

78 Rating hint: The time spent studying the track layout inside the mesh will allow the attacker to increase the opportunity of success when inserting a needle or similar. On the other hand, some tamper respondent meshes may contain conductive tracks with a very similar composition to the isolating layers at the mesh. This issue may increase the risk of tampering detection in case of mechanical removal or penetration of the mesh.

79 The main impacts are:

- Disclosure of the PCB internals.
- Disclosure of any plaintext data sent through the tracks of the PCB.

3.1.7 Direct attack to the Anti-tamper processor

80 The following attacks bypass any anti-tamper processor in order to disclose critical design information or secret data (data travelling through any bus):

- Shaped charge shooting: Extremely high precision shooting of shaped charges can penetrate a package causing its circuits to be disabled before they can respond e.g. a memory zeroing circuit can be disabled before the energy can be removed from the memory.
- Energy attacks: By focusing a high-energy beam on the processor its functionality can be modified or stopped e.g. shooting an electromagnetic pulse focused on the anti-tamper processor.

81 Rating hint: In this kind of attacks, another attack path may be considered. Since it is necessary to determine the exactly location of the processor inside the PCB,

tomography or X-ray technologies may apply. On the other hand, some cases may include anti reverse engineering methods, 3D mapping or X-ray imaging protection. This issue can be solve by probing the internals of the box through a slit or hole, which belong to the design, or maybe has been manually created bypassing other kind of tamper detections. Notice, the attack will increase its potential rating since other protections may be active e.g. light detectors on the top of the PCB may detect the light coming from a small hole.

82 The main impacts are:

- Disclosure of the PCB internals.
- Disclosure of any plaintext data sent through the tracks of the PCB.

3.1.8 Direct attack to the auxiliary battery

83 The following attacks bypass any anti-tamper processor, which depends on an external power supply, in order to disclose critical design information or secret data (plaintext buses):

- Deactivating the auxiliary power supply: interrupting the power supply which maintains the security processor running when the external power supply is gone e.g. cutting the wire or track of the auxiliary external battery supply.
- Extremely power consumption: by focusing a high energy beam on the auxiliary battery location e.g. shooting an electromagnetic pulse focused on the auxiliary battery.

84 Rating hint: In this kind of attacks, another attack path may be considered. Since it is necessary to determine the exactly location of the battery inside the PCB, tomography or X-ray technologies may apply. On the other hand, many cases may include an external auxiliary battery; in such cases cutting the power supply becomes extremely easy. However, the attacker may consider that the elapsed time between the action of cutting the wire and the zeroization of the memory can be extremely short.

85 The main impacts are:

- Disclosure of the PCB internals.
- Disclosure of any plaintext data sent through the tracks of the PCB.

3.2 Physical security semi-invasive attacks

3.2.1 Perturbation attacks

86 The following attacks bypass any anti-tamper processor, which depends on an external power supply, in order to disclose critical design information or secret data

(data travelling through any bus):

- Permanent environment perturbations: An attacker may need to change the environment conditions during the whole time that the attack is performed e.g. increase/decrease the temperature of the execution environment until the maximum/minimum allowed temperature is reached trying to obtain information from a RAM module.

- Transient perturbations: by changing the environment condition values in short times of the running period e.g. increasing the voltage in the power supply suddenly, anomalies can be detected in the behaviour of a system.

87 Rating hint: In this kind of attacks, the evaluator may consider the knowledge of the system required to perform such perturbations. For example, if the system has a temperature sensor fixed to certain value, the effort of getting the value must be considered in terms of: available source code (open source), reverse engineering methods, etc.

88 The main impacts are:

- Disclosure of any critical security information.

3.3 Physical security non-invasive attacks

3.3.1 Reverse engineering

3.3.1.1 Imaging technologies

89 The following attacks bypass any anti-reverse engineering system in order to disclose critical design information or secret data (plaintext stored data):

- Visual / Optical recognition: Probably all the reverse engineering methodologies begin with this step, the attacker will try to recognise the structure of the security box by visual recognition e.g. having a look through a hole with the help of a torch.

- X-ray snapshot: The x-ray recognition will help the attacker guessing the structure of the internals protected by the box e.g. taking an x-ray of the security box will sometimes reveal the internals design.

- Ultrasound Attacks: Ultrasound imaging is carried out by means of sound waves with frequency beyond the range of 20,000 Hz. This technique is useful to see wires, hardware components, chemical protections, etc. and to detect breaches and gaps in surfaces.

- Tomography Attacks: Taking a tomogram of a system, the attacker can obtain very critical information about the different levels of the internal design of a system e.g. the attacker will take a tomogram of a multi-layer PCB, this will allow the attacker guessing the internals of the PCB.

- Thermography Attacks: During execution time, the attacker will take a thermal image, which can be used to guess the internal structure e.g. the attacker will take the thermal image trying to obtain the disposition of the main ICs.

90 Rating hint: For every method described above, the evaluator has to take into account the measures taken in the design of the system. Some anti-reverse engineering protection mechanisms will obfuscate the components layout increasing severely the identification of the ICs used in the implementation. On the other hand, if the system is protected against x-ray, tomography or any other kind of 2D/3D scanning methodology, the evaluator has also to take into account the necessary effort to be apply in case of bypassing or deactivating such mechanisms.

91 The main impacts are:

- Disclosure of the PCB internals.
- Disclosure of the stored plaintext data.

3.3.2 Power consumption analysis

92 The following attack has been designed to try to disclose critical secret data (key ciphered data):

- Power consumption analysis: Power consumption measurements are collected, from the power supply line, during cryptographic operations e.g. the attacker will insert any small resistor in series with the power input, then the voltage difference across the resistor divided by the resistance value yields the current value.

93 Rating hint: The evaluator may consider that this kind of analysis is highly difficult. The number of samples to be taken and the study to be implemented after taking the measurements is based in complex differential analysis. The evaluator should consider the expertise required to the attacker in order to get some valuable information such as the key used in the calculations.

94 On the other hand, as the security box protects properly the accessibility to the internals, the power consumption analysis shall be performed using a TOE external interface.

95 The main impacts are:

- Disclosure of the stored ciphered data.
- Disclosure of the secret keys.

3.3.3 Emanation analysis

96 The following attack has been designed to try to disclose critical secret data (secret keys or ciphered data):

- Emanation analysis: An antenna sited close to the chip will read the electromagnetic field variations induced in the surrounding area of the device e.g. the attacker will attach an antenna close to the IC and analyse the wave form depicted in the oscilloscope during a time.

97 Rating hint: The evaluator may consider that this kind of analysis is highly difficult. The number of samples to be taken and the study to be implemented after taking the measurements is based in complex differential analysis. The evaluator should consider the expertise required to the attacker in order to get some valuable information such as the key used in the calculations.

98 On the other hand, as the security box protects properly the accessibility to the internals, the emanation analysis shall be performed locating an antenna outside the security box boundary.

99 The main impacts are:

- Disclosure of the secret keys.

3.3.4 Timing analysis

100 The following attack has been designed to try to disclose critical secret data (secret keys or ciphered data):

- Execution time analysis: an analysis of the variations of execution time of an operation in a cryptographic algorithm, which may reveal knowledge of or about a critical security parameter such as a PIN or cryptographic key e.g. the attacker will execute different cryptographic functions while measuring the spent time.

101 Rating hint: Usually this kind of analysis can be performed by using the external interfaces of the system. However, if the cryptographic timing is not reachable from the outside, an extra effort must be taking into account, for example trying to determine the time consumed by an internal cryptographic library performing calculations.

102 The main impacts are:

- Disclosure of critical security information.

4 References

[PHY] ISO/IEC TS 30104:2015 Information technology - Security techniques - Physical security attacks, mitigation techniques and security requirements

[AM-SBOX] Attack Methods for Hardware Devices with Security Boxes, Version 3.0, February 2020

[AP-POI] Joint Interpretation Library, Application of Attack Potential to POIs, Version 1.0, 9th June 2011

[AM-POI] Joint Interpretation Library, Attack Methods for POIs, version 1.95, 2nd February 2015

[CC] Common Criteria for Information Technology Security Evaluation, see https://www.commoncriteriaportal.org/cc/ for valid versions

[CEM] Common Methodology for Information Technology Security Evaluation (CEM), see https://www.commoncriteriaportal.org/cc/ for valid versions

Annex A Point Of Interaction

A.1 Overview

103 This annex will include information regarding concrete attack methodology to be applied against Points of Interaction.

104 See [AP-POI].

Annex B Hardware Security Module (HSM)

B.1 Overview

105 This annex will include the attack potential rating to be applied against HSMs according to the attacks defined in [AM-SBOX].

B.2 Electromagnetic and sounds analysis

106 The following attack has been designed to try to disclose critical secret data (secret keys or ciphered data):

- PIN-pad entry: The secret PIN number can be guessed during the code entering procedure e.g. the attacker will attach a small microphone close to the PIN-pad, will record the sound of the hit keys and later on guess the secret number.

- Emanation analysis: An antenna sited close to the chip will read the electromagnetic field variations induced in the surrounding area of the device e.g. the attacker will attach an antenna close to the IC and analyse the waveform depicted in the oscilloscope during a time.

107 Rating hint: The evaluator may consider the effort when trying to hide any electrical device in case of recording sounds. For example, it might be easy to hide a nano-microphone in the PIN-pad. Hints regarding the emanation analysis are given in section 3.3.3.

108 The main impacts are:

- Disclosure of the secret keys.

Annex C Tachograph

C.1 Overview

109 This annex will include the attack potential rating to be applied against Tachographs according to the attacks defined in [AM-SBOX].

C.2 PIN-based (keyboard) authentication

C.2.1 Electromagnetic and sounds analysis

110 The following attack has been designed to try to disclose critical secret data (secret keys or ciphered data):

- PIN-pad entry: The secret PIN number can be guessed during the code entering procedure e.g. the attacker will attach a small microphone close to the PIN-pad, will record the sound of the hit keys and later on guess the secret number.

- Emanation analysis: An antenna sited close to the chip will read the electromagnetic field variations induced in the surrounding area of the device e.g. the attacker will attach an antenna close to the IC and analyse the wave form depicted in the oscilloscope during a time.

111 Rating hint: The evaluator may consider the effort when trying to hide any electrical device in case of recording sounds. For example, it might be easy to hide a nano-microphone in the PIN-pad. Hints regarding the emanation analysis are given in section 3.3.3.

112 The main impacts are:

- Disclosure of the secret keys.

C.2.2 Printer drawer

113 The following attack has been designed to try to disclose critical design data:

- Printing paper replacement: For those tachographs including a printing device, paper replacement becomes a challenge. In many situations, the drawer containing the replaceable paper leaves a big opening. An attacker can insert almost any tool through this hole making the internals of the printer reachable e.g. the attacker will probe the internals of the tachograph using a fiberscope camera through the printing drawer hole.

114 Rating hint: The evaluator may consider if the opening leave by the printer drawer is easily reachable or not. If the drawer opening is filled with black epoxy, other machining methods must be used, therefore additional rating must be considered.

115 The main impacts are:

- Disclosure of secret design information.

Annex D Smart Meters

D.1 Overview

116 This annex will include the attack potential rating to be applied against Smart Meters according to the attacks defined in [AM-SBOX].