EUROPEAN UNION AGENCY
FOR CYBERSECURITY

EUCC SCHEME

STATE-OF-THE-ART DOCUMENT

Minimum ITSEF requirements for security evaluations of Hardware devices with security boxes (HDwSB)

Version 1.1, October 2023

DOCUMENT HISTORY

Date	Version	Modification	Author’s comments
October 2022	1.0	Creation	Version submitted to the ECCG Based on JIL-Minimum-ITSEF-Requirements-For-Security-Evaluations-Of-Hardware-Devices-With-Secutity-Boxes-v1.1.pdf
October 2023	1.1	Addition of a document history section with a link to the SOG-IS document the state-of-the-art document is based on, where applicable	Based on ECCG comments received Approved for publication on 20/10/2023 by the ECCG and the European Commission

CONTENTS

1 REQUIRED CAPABILITIES FOR THE PHYSICAL EVALUATION OF HARDWARE DEVICES WITH SECURITY BOXES

1.1 OVERVIEW OF A PHYSICAL EVALUATION

The physical evaluation of hardware devices with security boxes (HDwSB) requires the development of specific skills and knowledge. The aim is to provide a technical guidance for evaluators running an evaluation and to expose the related minimum requirements.

To achieve this, the following sections will encompass:

- The understanding of the secure physical technology, its underlying principles and the development equipment used by manufacturers.
- The knowledge and experience in physical attack techniques that could compromise the hardware and an ability to use the related equipment to stress the hardware layers. This includes the understanding of the underlying physical principles.
- The ability to use the related equipment to conduct physical disruptions and the understanding of the related physical effects on the hardware.
- The knowledge and experience in cryptographic attack techniques and the ability to perform the analysis (including data-capture, signal processing procedures, analysis and rating).

The required tools for performing the various attack techniques can be categorised in standard (basic), specialised and bespoke.

1.2 PHYSICAL TECHNOLOGY

Evaluators must understand typical HDwSB hardware and the underlying principles to the extent necessary to comprehend the design decisions of the manufacturer.

Basic knowledge of the following is required:

- the electrical behaviour of electronic components, e.g. resistors, capacitors, transistors, integrated circuits, RAM, ROM, E2PROM, etc,
- design principles of integrated circuits,
- chemical properties of typical HDwSB hardware.

In addition, evaluators must have detailed knowledge of:

- microcontroller architecture, functionality and packaging,
- architecture and functionality of FPGAs (Field Programmable Gate Array) and ASICs (Application Specific Integrated Circuit),
- physical behaviour of removal and case opening detection switches,
- physical behaviour of sensors (temperature, voltage, …),
- layout principles of PCBs (Printed Circuit Boards),
- physical principles of protective shields (e.g. grid foils, printed grids),
- realisation of standard circuitry as used in micro-controllers,
- dynamic behaviour of digital and analogue circuitry,
- physical behaviour of potting mechanisms.

Evaluators must be able to understand the schematics (block diagrams, schematics).

Evaluators must have knowledge of the design process and must understand the process from the schematics (logical representation of the hardware) to the actual layout (physical representation). They must understand the processes of technology qualification, functional testing, characterisation, and reliability testing.

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

1.3 PHYSICAL SPECIFIC ATTACKS

The following provides an overview about HDwSB specific attacks. This is not a complete list but provides some examples. Detailed information about HDwSB specific attacks can be found in the state-of-the-art document APPLICATION OF ATTACK POTENTIAL TO HARDWARE DEVICES WITH SECURITY BOXES.

Evaluators must have knowledge about standard attack scenarios and in principle be able to develop new ideas for such attacks.

To be more specific, evaluators must know about attack scenarios for HDwSB such as intrusion of sensors, switches and filters, physical manipulation and probing, malfunction attacks, inherent and forced leakage attacks, abuse of test features and cryptographic attacks. A multitude of such attack scenarios – along with quotations – is described in the state-of-the-art document cited above.

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

Evaluators must have knowledge and experience of other HDwSB attacks; side channel attacks (SCA) such as Timing Analysis, Machine Learning based SCA, Simple Power Analysis (SPA), Differential Power Analysis (DPA), Differential EM radiation Analysis (DEMA), Template Attacks (TA); fault injection attacks such as DFA and related attacks) and possess the equipment (physical and analysis tools) necessary to perform such attacks. The ITSEF must own or have unlimited access to the equipment (physical and analysis tools) necessary to perform such attacks according to section 1.4. They must be able to operate this equipment (including data-capture procedures) and to perform the analysis (mathematics). Knowledge and experience in cryptography and standard cryptographic attack techniques is required.

Evaluators must at least understand the physical principles, and the usage (as appropriate) of the equipment classed as 'standard', 'specialised' and 'bespoke' as defined in the state-of-the-art document APPLICATION OF ATTACK POTENTIAL TO SMARTCARDS AND SIMILAR DEVICES.

1.4 EQUIPMENT FOR HDWSB PHYSICAL EVALUATION

In order to accomplish the vulnerability and failure analysis, physical manipulations and attack scenarios mentioned in section 1.3, the ITSEF must have unlimited access to and own the majority of the tools of the category 'standard' and shall be able to use them efficiently.

The ITSEF must have unlimited access to tools of the category 'specialized' and shall know how to use them efficiently.

Examples of this equipment and their categorisation are listed in the state-of-the-art document APPLICATION OF ATTACK POTENTIAL TO HARDWARE DEVICES WITH SECURITY BOXES.

The ITSEF must at least possess a basic set of tools (unlimited access is not sufficient) for physical manipulations, side channel analysis, perturbation attacks and supply equipment. The supply equipment is needed for the operation of the TOE during the evaluation.

The basic set consists of the following tools:

- soldering iron, solder paste, heat guns, glue, needles, syringes, knives, steel cutting blades, screwdriver, hammer, standard drill, saws, dental toolkit (mirrors), tools for chemical etching, tools for grinding,
- multimeter, digital oscilloscope, signal/protocol analyser, PC or workstation, signal analysis software, shunts, wires and electrical probes, digital camera, endoscope, microphones, electric torch, antennas,
- voltage supply devices, signal and function generators.

2 REQUIRED CAPABILITIES FOR A LOGICAL HDWSB EVALUATION

2.1 HDWSB LOGICAL DESIGN

Evaluators must understand typical HDwSB logical architectures (e.g. the boot process, operating system, resource management and interfaces) and the underlying principles to the extent necessary to comprehend the design decisions of the HDwSB developer. They must know the typical potential HWSB vulnerabilities and standard test and attack methods, especially domain-specific attack methods.

Evaluators must show their ability to search for new publicly known vulnerabilities.

2.1.1 Source Code

A typical HDwSB runs software on dedicated hardware. Therefore, knowledge of software, how it is designed, compiled and executed and how it utilizes the hardware is important for the evaluation.

A wide array of programming languages can be used to write the software found in a HWSB. They can be categorized into three families:

- Low level: specific to the processor of the HWSB language (ARM assembler, x86 assembler, etc.),
- Intermediate level: compiled code (C, C++, ADA, GO, Rust etc.),
- High level: managed code, running inside a virtual machine or an interpreter (Java, Python, Shell, Perl, PHP etc.).

Now while assembler is less used, managed code, on the opposite, can often be encountered, as well as compiled code. Evaluators need a thorough understanding of the use of C/C++ or Java in the context of the specific hardware architecture. If the HDwSB in evaluation or parts of it are programmed in other languages evaluators need a thorough understanding of these languages, too.

Moreover, for an in-depth security analysis, an understanding of assembler code and intermediate code (like Java Card byte code) is required. In particular, a variety of security impacts and defects cannot be understood on the level of a higher language like C or Java, because they become only apparent in assembler code or byte code. Therefore, the importance of understanding assembler code produced by a compiler and security impacts of generation tools shall be explicitly emphasized – eventually the processor runs on assembler (machine) code, not C, Java or anything else.

In addition, evaluators need to understand the impact of compilers, compiler libraries and interpreters on the security behaviour of the HDwSBs in evaluation. They must know the meaning of the different compiler settings in relation to security aspects (e.g. if an optimization flag removes loops necessary to avoid timing attacks).

2.1.2 Interfaces

Evaluators shall be familiar with the different kind of interfaces which are typically used by HDwSBs, e.g. Universal Serial Bus (USB), Serial, Ethernet port, Near Field Communication (NFC), Wi-Fi and Bluetooth. If a HDwSB uses other kinds of interfaces they shall be familiar with them, too.

They must know if the interfaces allow potentially security-critical behaviour, e.g. direct memory access (DMA) or modes of operations which are not foreseen by the developer. Evaluators must know how to address the HDwSB interfaces at the different ISO OSI layers and how to test their correct function.

They shall also be able, through software, to utilize debug ports available on the PCB, such as JTAG.

Evaluators must have knowledge of penetration tests related to the above mentioned interfaces.

2.1.3 Transport Layer Protocols

Evaluators must have knowledge of the security principles of the encryption schemes to be used for the transport layer protocols like secure messaging at smart card interfaces or TLS or SSH over the interfaces detailed in the above section.

Often these standards allow a high degree of flexibility in the configuration of security options, demanding scrutiny when evaluating a specific choice against a set of prerequisite requirements.

Evaluators must have knowledge of penetration tests related to the above mentioned transport layer protocols.

2.1.4 Application Layer Protocols

Evaluators must have knowledge of the security behaviour of application layer protocols, e.g. for POI knowledge of payment protocols like EPAS, IFSF (online) and EMV. Further examples are the processing of GNSS data in digital tachograph environment and the usage of the PACE protocol in smart meter gateways. They must know the security related state machines of these protocols as well as the underlying cryptographic mechanisms. They must be able to use test suites implementing such protocols to test security features of these protocols.

Evaluators must have knowledge of the typical PIN encryption schemes.

They must know the security principles of key management, HDwSB management protocols and software download mechanisms.

2.1.5 Operating System, Content and Resource Management

The defining task of an operating system is the management of computational resources (like persistent and volatile memory, internal I/O, external interface components, display, keyboard, etc.) and the administration of access (interface) to such resources.

While the previous paragraphs dealt with the communication between a HDwSB and the outside world, the focus shall lie here on the resource management inside the HDwSB itself.

At first, evaluators need to understand the different types of operating systems and their specifics, e.g. a real-time OS will not behave the same way as a standard desktop OS. Also the file structure and file access rights administration within these various operating systems will differ. Knowledge of the memory types (EE, Flash, ROM, RAM), special dedicated RAM (like Crypto-RAM, Buffer-RAM) and memory management procedures (e.g. access limitations) are required.

The concept of domain separation and application isolation needs to be profoundly understood. This is especially relevant for application management, which refers to the secure loading, administration, deletion of application as well as the access rights of such applications to the HDwSB's resources. This concept of separation is typically assisted by the underlying hardware/firmware platform, such as with the Trusted Execution Environment (TEE). It is important for the evaluator to have knowledge in this specific area.

The concept of boot-up processes for embedded devices, e.g. of multi-stage bootloaders, and the various possibilities of updating firmware and operating systems needs to be profoundly understood. Boot-up and update processes are potential targets for an attacker.

Another potential attack path might be the error handling e.g. in case of unexpected or misaligned expression as input. The evaluator must be able to analyse the error handling and to conduct appropriate tests.

2.1.6 Random Number Generator

The evaluator must have knowledge of and experience with evaluation methodologies for random number generators, in particular according to ISO/IEC 20543[1].

For the evaluation of physical RNGs the evaluator must have sufficient knowledge in probability theory and design principles of physical RNGs. The evaluator must be able to identify and analyse those characteristics of a system or a process that have significant impact on the distribution of random numbers and to rate the randomness of number generation.

This analysis shall be quantified by a stochastic model. The stochastic model shall allow to verify a lower entropy bound per random bit. The stochastic model in particular comprises a family of distributions that contains the true (but unknown) distribution(s) of the raw random numbers (or at least of random numbers in an early stage of the generation process) during the life time of a physical RNG, even for defective states, e.g. unacceptable outputs. The stochastic model shall be justified by technical arguments. Furthermore, also the effectivity of online tests (also known as "health tests") shall be verified on the basis of the stochastic model.

2.2 EQUIPMENT FOR HDWSB LOGICAL EVALUATION

In order to accomplish the vulnerability and failure analysis and attack scenarios mentioned in section 1.3, the ITSEF must have unrestricted access to the following categories of tools necessary to perform those analysis and attacks:

- Environment control equipment (e.g. to control communication, voltage, clock and temperature);
- Chemical and mechanical lab equipment (i.e. for sample preparation and analysis);
- Imaging equipment (e.g. cameras, microscopes);
- Logical test tools (e.g. for interface testing, vulnerability scanning, operating system testing, randomness analysis, source code analysis, circuit layout analysis, fuzzing tools).

Evaluators shall be able to operate the equipment to perform independent tests and attacks.

3 ITSEF ORGANISATION

3.1 LIFE CYCLE

Evaluators have to know the main phases of the life cycle which are the following: Development and manufacturing, initial software loading, delivery, installation and operation (including loading of software updates and additional software),and end-of-life (e.g. controlled erasure of keys and destruction or re-use of hardware).

[1] ISO / IEC 20543:2019: Information Security - Security Techniques - Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408.

3.2 SUBCONTRACTING, THIRD PARTY FACILITIES AND EQUIPMENT

Some attack methods for HDwSB may require specific chip know how and bespoke chip equipment. In that case this kind of work may be, with the consent of the Certification Body, subcontracted to an ITSEF competent for the Technical Domain related to smartcards and similar devices.

4 ACRONYMS

EMV	Europay, MasterCard and Visa
EPAS	Electronic Protocols Application Software
HDwSB	Hardware Device with Security Box
IFSF	International Forecourt Standards Forum
OSI	Open Systems Interconnection
PIN	Personal Identification Number
SSH	Secure Shell
TLS	Transport Layer Security

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu