Technical Report

ISO/IEC TR 5891

First edition
2024-04

Information security, cybersecurity and privacy protection — Hardware monitoring technology for hardware security assessment

Sécurité de l'information, cybersécurité et protection de la vie privée — Technologie de surveillance des matériels pour l'évaluation de leur sécurité

Reference number
ISO/IEC TR 5891:2024(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

Hardware components and the computing ecosystem are becoming increasingly complex. As a result, it becomes increasingly difficult to evaluate the security of hardware. Even in the design stage, it is quite difficult to identify abnormal parts that can cause flaws from among millions of source code lines or billions of transistors, as well as the physical connections between them. Other areas of technology use monitoring to assist with the evaluation aiming to mitigate such difficulties. In those technologies, runtime activities such as changes in internal or external status can be monitored to identify deviations from normal behaviour patterns, and by these means, the evaluation can focus on a small set of patterns that the monitored subject typically works with. This method now becomes an available option to assist in hardware security assessment. In such cases, either the target of security assessment is supposed to be "runtime hardware-behaviour-based security", or introduced as a proactive approach to security.

Many evaluation and assessment standards, such as ISO/IEC TS 30104, ISO/IEC 19790 and ISO/IEC 17825, focus on physical security (invasive/nonintrusive) at the hardware boundary. However, they do not focus on the monitoring data, either offline or in real time.

Information security, cybersecurity and privacy protection — Hardware monitoring technology for hardware security assessment

1 Scope

This document surveys and summarizes the existing hardware monitoring methods, including research efforts and industrial applications. The explored monitoring technologies are classified by applied area, carrier type, target entity, objective pattern, and method of deployment. Moreover, this document summarizes the possible ways of utilizing monitoring technologies for hardware security assessment with some existing state-of-the-art security assessment approaches.

The hardware mentioned in this document refers only to the core processing hardware, such as the central processing unit (CPU), microcontroller unit (MCU), and system on a chip (SoC), in the von Neumann system and does not include single-input or single-output devices such as memory or displays.

The hardware monitoring technology discussed in this document has the following considerations and restrictions:

— the monitored target is for the post-silicon phase, not for the design-house phase (e.g. an RTL or netlist design);

— monitoring is only applied to the runtime system.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 15408-1, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC/TS 30104:2015, *Information Technology — Security Techniques — Physical Security Attacks, Mitigation Techniques and Security Requirements*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 15408-1, ISO/IEC TS 30104 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
hardware monitoring
hardware or software component allowing an individual to monitor devices connected to a computer

3.2
runtime hardware-behaviour-based security
function of a hardware that protects running physical devices from harm caused by abnormal or unexpected state transitions

Note 1 to entry: Such transitions come from vulnerability, non-declarations, or malicious logic.

4 Abbreviated terms

CPU	central processing unit
DRAM	dynamic random-access memory
EDA	electronic design automation
FSM	finite state machine
I/O	input/output
MCU	microcontroller unit
NIC	network interface controller
RAS	reliability availability and serviceability
RTL	register transfer level
SoC	system on a chip
JTAG	Joint Test Action Group
IP	intellectual property
CISC	complex instruction set computer
QoS	Quality of Service
ISA	instruction set architecture
ECC	error checking and correction
ROM	read-only memory
EEPROM	electrically erasable programmable ROM
VMM	virtual machine manager
FPGA	field programmable gate array

5 Relationship to existing standards

5.1 Standards of security assessment

Existing security assessments and technical standards face challenges in addressing hardware uncontrollability. ISO/IEC TS 30104, ISO/IEC 19790, and ISO/IEC 17825 focus on (invasive/nonintrusive) physical security at the hardware boundary, but not over the boundary. ISO/IEC TR 20004 complements the vulnerability analysis of ISO/IEC 15408-3 from the perspective of software. Among these, there are no relevant hardware standards.

5.2 Relationship to ISO/IEC 15408-3

In ISO/IEC 15408-3, vulnerability assessment is defined. This document aims to survey technologies to support hardware vulnerability assessment that can be done at runtime.

5.3 Relationship to ISO/IEC TS 30104

This document aims to supplement ISO/IEC TS 30104:2015, 7.2 and 7.3.

6 Background

6.1 Complexity and security

Modern circuits are very complex, and their complexity, amplified by time-to-market pressure, is increasing rapidly in modern computing environments. Consequently, design houses frequently use external IPs, and most IC design enterprises are fabless.

The complexity of modern systems increases the attack surface. Because the semiconductor industry has shifted to a horizontal business model for the integrated circuit supply chain, malicious hardware (hardware Trojans) can be implanted in untrusted phases or components, e.g. commercial IP cores, EDA tools, fabrication, and assembly services. Such malicious modifications to the original circuitry are inserted by adversaries to exploit hardware or to use hardware mechanisms to create backdoors in the design.

6.2 Challenges in defining hardware security assessment techniques

It is difficult to address all such security risks because of the complexity of processes and components, outsourcing of design and fabrication, and the increase in the sophistication of potential attacks.

For a given piece of hardware, especially a complex system such as a modern SoC, it is also difficult to identify small malicious modifications to the original design (e.g. at the gate-level netlist). Even with trusted source code, a piece of hardware cannot be guaranteed to be Trojan-free in the post-silicon phase. Traditional tests (e.g. function coverage tests, fault tests, and random case tests) are less likely to help with such detection because hardware Trojans are typically activated, i.e. designed to be activated, by specified conditions, such as specific sequences of instructions, particular combinations of external signals, a timer, or a temperature threshold. Adversaries can make the Trojan active and launch attacks, then switch it off during hardware runtime. In other words, traditional methods of auditing the source code or performing manufacturing fault detection are ineffective for hardware security assessment.

A hardware Trojan is a malicious inclusion or modification of hardware. A hardware Trojan consists of a trigger circuit and a payload circuit. The trigger circuit activates the payload circuit under a specific condition, and the payload circuit implements the malicious behaviour of the hardware Trojan. The hardware Trojan can leak secret information in the hardware or bypass or disable the security functions of the hardware.

Hardware Trojan detection is applicable in multiple phases of hardware production and distribution. For example, detection based on the netlist can be applied in the designing phase. Side-channel and logic approaches can be applied during the manufacturing or in-use phase. Focusing on the fact that a hardware Trojan alters the behaviour of the circuit, the side-channel approach detects abnormal behaviour from the side-channel information. The logic-test-based approach generates test patterns to detect hardware Trojans via the output. Some state-of-the-art approaches use machine learning technologies to detect hardware Trojans from the netlist or side-channel information of the hardware.

Hardware flaws, such as Meltdown, Spectre and a series of newly revealed flaws,[99-101] are a result of pursuing performance, for instance, parallelism, during microarchitecture development. First, they are difficult to fix, and the fixes can cost more than the gains from hardware optimization. Second, some of these flaws exist for approximately 10 to 15 years before they are revealed. Traditional detection in the pre-silicon phase would be unlikely to help since flaws are not malicious modifications. It is claimed that some advanced security verification techniques are able to find such flaws by chance early in the design lifecycle.[102] However, rather than being used in an evaluation approach, such techniques are more likely to assist

in design and are probably not available to third parties. For hardware products with commercial IPs, it is extremely difficult to apply security assessment to the microarchitecture because of the need to preserve commercial secrets.

7 Hardware monitoring technologies

7.1 Overview

Hardware monitoring technology began in the computer boom period in the 1980s. It was first used to assist with debugging and later developed into applications in various fields. However, with the rapid development of computing hardware and networks, especially the emergence of multicore processors and complex systems, including multicore processor systems, hardware monitoring technology has also undergone tremendous changes. While the fast-developing software and hardware environment has led to complex application functions, it also faces increasingly complex security challenges. In cloud computing-based systems, runtime stability and security are highly important, as they provide online services nonstop. The unique runtime characteristics of hardware monitoring technology give it a natural advantage in coping with these scenarios.

Hardware monitoring has made considerable progress in academic fields and industrial applications. It is widely used in/for the following areas/purposes:

— security

— debugging and testing

— performance analysis, evaluation, and optimization

— system fault tolerance and reliability

— physical parameter measurement and early warning

Although the focus of this document is hardware security assessment, monitoring techniques used for other purposes have implications for building assessment models. For example, the technology used for commissioning and reliability analysis is similar to the technology used for replay in the safety assessment process; the technology used for performance analysis has some consistency with runtime Trojan-based hardware detection technology. Therefore, in this document, keywords such as “debug” and “performance” are widely used in literature searches.

7.2 Research in academic areas

On the academic side, different studies have reviewed monitoring technologies from different perspectives.

Ian Cassar et al.[1] divided runtime monitoring instrumentation techniques into offline and online categories. Detailed online segmentation ranges from tightly coupled completely synchronous (CS) monitoring instrumentation approaches, to loosely coupled completely asynchronous (CA) monitoring approaches.

Heidar Pirzadeh et al.[2] divided monitoring technologies into software and hardware monitoring technologies and subdivided software monitoring technologies into add-on monitoring, manual instrumentation, online instrumentation, instrumenting compilers, interpreter instrumentation and OS instrumentation. In terms of security, cost, flexibility intrusiveness, performance and broadness, various monitors were compared horizontally.

Lihua Gao et al.[3] and Frank Cornelis et al.[4] separately subdivided software runtime monitoring technology. Reference [3] classifies and discusses the different levels of monitoring objectives (functional, module, architecture, and subsystem), while Reference [4] focuses on non-deterministic events and addresses the needs of various technologies for external resources (time, order, language, etc.) for subdivision comparison.

Georgios Kornaros et al.[5] focused on on-chip monitoring technology in a multicore SoC system and discussed the monitoring technology in detail from the perspective of function and methodology.

7.3 Industrial cases

In terms of industrialization, mainstream chip manufacturers and IT service providers also use hardware monitoring technology in their products.

Since 2013, Intel®[1)] has introduced technology in commercial processors that can be enormously helpful in debugging because it exposes an accurate and detailed trace of activity and has triggering and filtering capabilities to help with isolating the important traces.

AMD®[2)] has provided a similar technology for monitoring and controlling processors. This custom-built tool is designed specifically for a proprietary line of devices, thus indicating that the hardware and utility designers work together to provide the best service for their products.

ARM®[3)] designed a set of utilities, including various trace macrocells, system and software measurements for the ARM processor, and a complete set of IP blocks, to debug and trace the most complex multicore SoC.

There are also hardware monitoring programs that are used to read the main health sensors of PC systems: voltages, temperatures, powers, currents, fan speed, utilization, and clock speeds during runtime.

Hardware security is a complex concept. The types of hardware are very complex. Figure 1 shows a comprehensive description of hardware monitoring technologies from five perspectives: target entity, purpose, carrier, objective patterns and deployment.

1) This tradename is provided for reasons of public interest or public safety. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO or IEC.

2) This tradename is provided for reasons of public interest or public safety. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO or IEC.

3) This tradename is provided for reasons of public interest or public safety. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO or IEC.

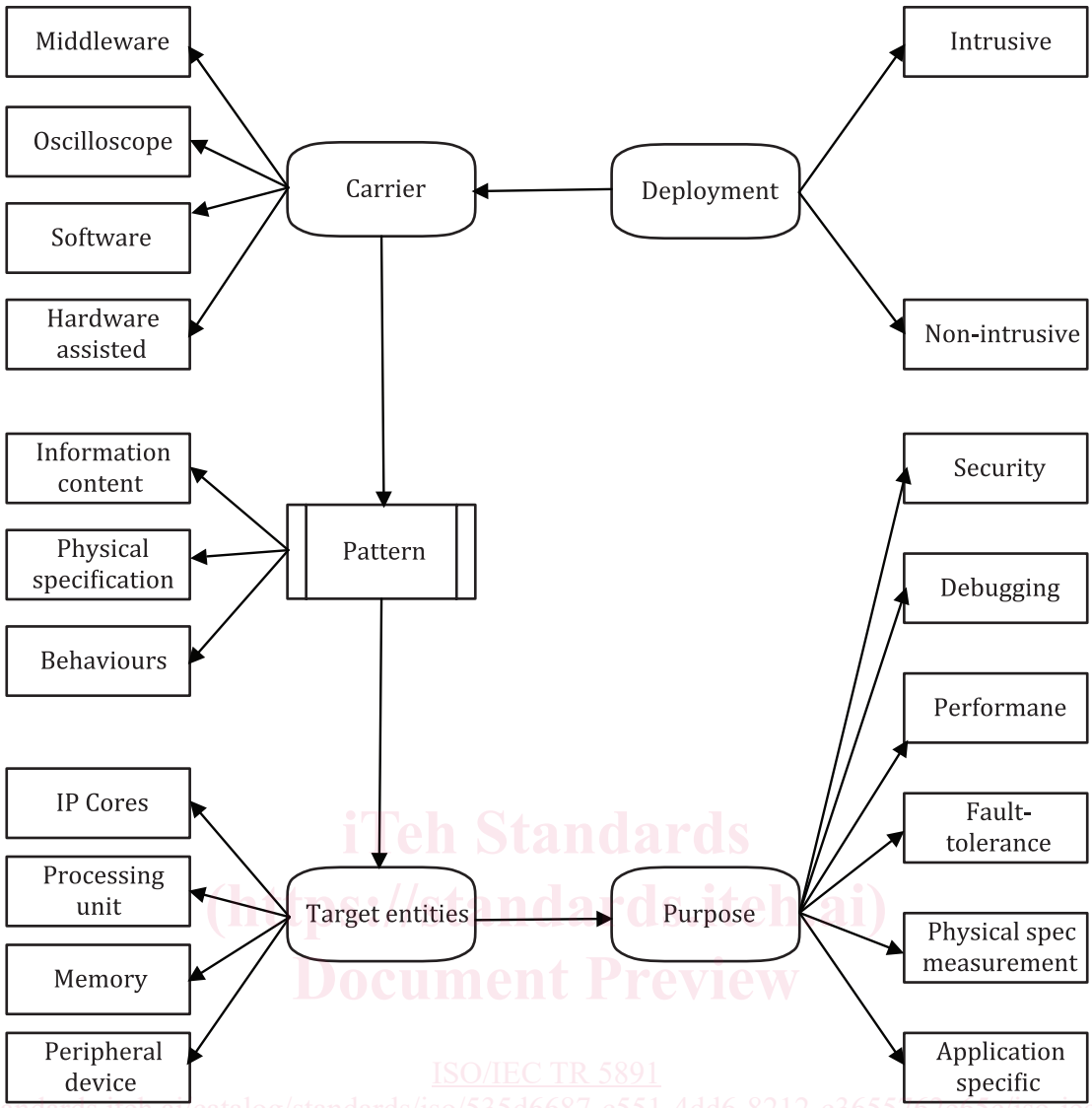

Figure 1 — Taxonomy of hardware monitoring technologies

7.4 Purpose

7.4.1 Security

The application of hardware monitoring technology for security purposes mainly aims to compare whether the running behaviour matches expectations. Then, security control is performed based on the matching results. Security control can terminate the operation of the system, re-execute the target module, or only record the current events and status to provide offline analysis or security audits.

According to the various monitoring objectives, different monitoring methods are adopted. From the scope of division, these methods can be divided into those that monitor a certain key hardware in the system and those that help ensure the safe operation of the entire system. The security of critical hardware can be divided into the implementation monitoring of malicious Trojan horses and the vulnerability security protection of hardware operation mechanisms.

Architecture monitoring support for security usually focuses on achieving tamper resistance and encryption. Some built-in on-chip technologies, such as control-flow integrity (CFI),[6] can assist users with high-performance integrity verification. They focus on the anti-attack capability of the core hardware itself. Some technology[7] can help defend against control-flow hijacking malware, for example, indirect branch