ISO/IEC TR 5891:~~2021~~2023(E)

ISO JTC 1/SC 27/WG 3

Date: ~~2022-11-09~~2023-05-17

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

Style Definition ...
Formatted: Font: 11 pt
Formatted ...
Formatted: zzCover, Left
Formatted ...
Formatted: Font: Not Bold
Formatted: zzCover, Left, Space After: 0 pt
Formatted: Font: 11 pt
Formatted: zzCover, Line spacing: single, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Font: 11 pt, Not Bold

~~Technical Report~~

~~Warning for WDs and CDs~~

~~This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.~~

~~Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.~~

~~A model manuscript of a draft International Standard (known as "The Rice Model") is available at https://www.iso.org/iso/model_document-rice_model.pdf~~

Formatted: Font: 11 pt, Font color: Blue
Formatted: Indent: Left: 0 cm, Right: 0 cm, Border: Left: (No border), Right: (No border)
Formatted: Font: 11 pt, Font color: Blue
Formatted: Font: 11 pt, Font color: Blue
Formatted: Font: 11 pt, Font color: Blue
Formatted: Font: 11 pt, Font color: Blue
Formatted: Font: 11 pt
Formatted: Font: 11 pt, Font color: Blue
Formatted: Indent: Left: 0 cm, First line: 0 cm, Right: 0 cm, Border: Left: (No border), Right: (No border)
Formatted: Font: 11 pt, Font color: Blue
Formatted: Font: 11 pt, Font color: Blue
Formatted: Font: 11 pt, Font color: Blue
Formatted: Font: 11 pt, Font color: Blue
Formatted: Indent: Left: 0 cm, First line: 0 cm, Right: 0 cm, Border: Bottom: (No border), Left: (No border), Right: (No border)
Formatted: Font: 11 pt, Font color: Blue
Formatted: Font: 11 pt, Font color: Blue

Contents

Foreword

The ISO (the International Organization for Standardization) is a and IEC (the International Electrotechnical Commission) form the specialized system for worldwide federation of national standardsstandardization. National bodies (that are members of ISO member bodies). The workor IEC participate in the development of preparing international standards is normally carried outInternational Standards through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International 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 nongovernmentalnon-governmental, in liaison with the ISO and IEC, also take part in the work. The ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documentsdocument 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 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

Attention is drawnISO and IEC draw attention to the possibility that some of the elementsimplementation of this document may beinvolve the subjectuse of (a) patent rights. ISO(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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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 and for, as well as information about the ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee *for Project Committee]* ISO/IEC JTC1JTC 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.htmlwww.iso.org/members.html and www.iec.ch/national-committees.

Introduction

Hardware components and the computing ecosystem are becoming increasingly complex. ~~As hardware becomes increasingly complex.~~As a result, it becomes increasingly difficult to evaluate ~~its~~the security of hardware. Even in the design stage, it is quite difficult to identify abnormal parts that ~~may~~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 ~~this~~these means, the evaluation ~~may~~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— General framework for runtime 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~~— the monitored target is for the ~~postsilicon~~post-silicon phase, not for the design-house phase (e.g~~.~~, an RTL or netlist design~~).~~);

— ~~Monitoring~~— 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~~:2009~~, *Information ~~technology — Security techniques~~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~~:2009~~, ISO/IEC TS 30104~~:2015~~ 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/

Formatted: Section start: New page, Different first page header
Formatted: Font color: Blue
Formatted: Space Before: 20 pt, After: 38 pt, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Font: Bold, Font color: Blue
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: Body Text, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: List Continue 1, Indent: Left: 0 cm, First line: 0 cm, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.7 cm, Left + 1.4 cm, Left + 2.1 cm, Left + 2.8 cm, Left + 3.5 cm, Left + 4.2 cm, Left + 4.9 cm, Left + 5.6 cm, Left + 6.3 cm, Left + 7 cm, Left
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: std_publisher
Formatted: RefNorm, Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers, Tab stops: 0.7 cm, Left + 1.4 cm, Left + 2.1 cm, Left + 2.8 cm, Left + 3.5 cm, Left + 4.2 cm, Left + 4.9 cm, Left + 5.6 cm, Left + 6.3 cm, Left + 7 cm, Left
Formatted: std_docNumber
Formatted: std_docPartNumber
Formatted: std_docTitle, Font: Not Italic
Formatted: std_docTitle, Font: Not Italic
Formatted: Font: Not Italic
Formatted: std_publisher
Formatted: std_documentType
Formatted: std_docNumber
Formatted: std_year
Formatted: std_docTitle, Font: Not Italic
Formatted: Don't adjust space between Latin and Asian text, Don't adjust space between Asian text and numbers
Formatted: std_publisher
Formatted: std_docNumber
Formatted: std_docPartNumber
Formatted: std_publisher
Formatted: std_documentType
Formatted: std_docNumber
Formatted: Font: Cambria, 11 pt
Formatted ...
Formatted: English (United States)
Formatted: English (United States)
Formatted: Font: Cambria

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

3.2
~~Runtime~~runtime hardware-behaviour-based security
~~A tool~~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~~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~~

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

Formatted: Normal, Space After: 36 pt, Line spacing: Exactly 12 pt
Formatted: Font: 12 pt
Formatted: Font: 11 pt
Formatted: Space After: 0 pt, Line spacing: single

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, but not inside, 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. ThereAmong these, there are no relevant hardware standards.

5.2 Relationship to ISO/IEC 15408-3

In ISO/IEC 15408-3, vulnerability assessment (AVA category) is defined. In ISO/TR 5891, we aimThis document aims to survey technologies to support hardware vulnerability assessment that can be done at runtime.

5.3 Relationship to ISO/IEC TS 30104

ISO/TR 5891This document aims to supplement ISO/IEC TS 30104:2015, subclauses 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

Formatted: Normal, Right, Space After: 36 pt, Line spacing: Exactly 12 pt
Formatted: Font: 12 pt
Formatted: Font: 11 pt
Formatted: Space After: 0 pt, Line spacing: single