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)

COPYRIGHT PROTECTED DOCUMENT

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*