TECHNICAL ISO/IEC TR

First edition
2023-10

Cybersecurity — Security considerations throughout the product life cycle

Cybersécurité — Considérations relatives à la sécurité tout au long du cycle de vie du produit

Reference number
ISO/IEC TR 6114:2023(E)

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 ... **v**

Introduction ... **vi**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**

4 Abbreviated terms ... **2**

5 Security considerations throughout the product life cycle ... **3**
5.1 Security considerations throughout the product life cycle overview ... 3
5.2 Information and communication technology threat model ... 5
5.3 Classes of threats ... 5
5.4 Structure of the report ... 5

6 Phase 1: Concept ... **6**
6.1 General ... 6
6.2 Summary of concept threats and controls ... 6
6.2.1 Workflow toolchain tampering ... 6
6.2.2 Unauthorized operations ... 7
6.2.3 Integrity faults ... 7
6.2.4 Theft or loss ... 7

7 Phase 2: Development ... **7**
7.1 General ... 7
7.2 Summary of development threats and controls ... 7
7.2.1 Attacks on development tools and/or network ... 7
7.2.2 Malicious embedded firmware ... 7
7.2.3 Malicious hardware ... 8
7.2.4 Malicious software (driver) ... 8
7.2.5 Counterfeit ... 8

8 Phase 3: Source and manufacture ... **9**
8.1 General ... 9
8.2 Source ... 9
8.3 Manufacture ... 9
8.4 Summary of production threats and controls ... 9
8.4.1 Attack on production tools, data exchange tools and/or network ... 9
8.4.2 Unauthorized disclosure ... 9
8.4.3 Reverse engineering / theft of design ... 10
8.4.4 Improper system settings ... 10
8.4.5 Design alteration ... 10
8.4.6 Insertion of malicious and/or counterfeit components ... 10
8.4.7 Falsification of test results ... 11
8.4.8 Product theft ... 11
8.4.9 Code insertion or replacement (firmware, operating system, software) ... 11
8.4.10 System replacement (spoof device) ... 11

9 Phase 4: Transport ... **12**
9.1 General ... 12
9.2 Summary of production threats and controls ... 12
9.2.1 Product theft ... 12
9.2.2 Code insertion or replacement (firmware, operating system, software) ... 12
9.2.3 Insertion of malicious components ... 12
9.2.4 System replacement (spoof device) ... 12
9.2.5 Physical attack in storage and transit ... 12

10 Phase 5: Utilization and support ... **12**

10.1 General ... 12
10.2 Provision ... 13
10.3 Utilization ... 13
10.4 Support ... 13
10.5 Summary of utilization threats and controls ... 13
10.5.1 Unknown provenance ... 13
10.5.2 Spoofed system (replaced system) ... 13
10.5.3 Undetected tampering ... 14
10.5.4 Build data store tampering ... 14
10.5.5 Non-current device/product (firmware, operation system, application, drivers) ... 14
10.5.6 Unauthorized changes (firmware, operating system, software) ... 14
10.5.7 Unauthorized component swap ... 14
10.5.8 Insertion or replacement with malicious component ... 15
10.5.9 Product data store tampering ... 15

11 Phase 6: Retirement ... 15
11.1 General ... 15
11.2 Summary of retirement threats and controls ... 15
11.2.1 Inaccurate hardware return ... 15
11.2.2 Incomplete data removal ... 16

Annex A (informative) **Product security threat mapping to SCLC phases ... 17**

Annex B (informative) **Typical threats for hardware ... 21**

Annex C (informative) **Typical threats for software ... 30**

Annex D (informative) **Typical threats for data ... 36**

Annex E (informative) **Use of tagalongs ... 40**

Annex F (informative) **Software tampering ... 41**

Bibliography ... 44

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

The globalization of technology design, development, manufacturing, and distribution has created an environment of complicated supply chains with limited transparency. This presents an incredible challenge for the industry and highlights a growing need to ensure product integrity for all stages of the information and communications technology (ICT) product life cycle.

The call for assurance across the supply chain landscape has evolved over several decades. More recently, policy makers around the world have begun to focus on supply chain risks in new ways: from policies considering supply chain security risks for government procurement to various initiatives adding security considerations such as trust and transparency in the supply chain for ICT.

Vendors have been doing their part as well. Over the past several years, ICT suppliers have taken important steps towards increasing supply chain transparency. These steps include sourcing conflict-free minerals,[1] and implementing a set of policies, procedures and tools at factories to improve security consideration throughout the supply chain by validating where and when each component of an ICT product was manufactured.

These are important first steps, however they primarily focus on the production stage, just one stage of the ICT product life cycle. In today's complex environment, hardware platform providers are expected to enable a full range of tools and solutions that improve security consideration across the entire life cycle, from design and sourcing to secure retirement.

Security considerations throughout the product life cycle (SCLC) establish an end to end framework that can be applied to the multi-year life cycle of ICT products to comprehend and address potential risks for improved transparency and higher levels of security assurances. By enabling transparency and assurances across the ICT product life cycle, supply chain owners can improve platform integrity, resilience and security. The life cycle phases are both iterative and recursive in nature.