ISO/IEC TR 6114:2023-10 (E)

Cybersecurity - Security considerations throughout the product life cycle

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